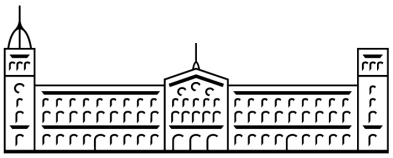

Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques
Universitat de Barcelona

Resolubilitat efectiva per radicals de les quíntiques sobre cossos p-àdics

Autor: Marc Caelles i Vidal

Director: Dr. Artur Travesa i Grau
Realitzat a: Departament d'Àlgebra i Geometria

Barcelona, 17 de gener de 2016

Abstract

Since every finite extension over a p-adic field is solvable, any degree 5 polynomial can be solved by radicals over the p-adic numbers. Using Panayi's algorithm we describe a method for expressing any root of an irreducible quintic over $\mathbb{Q}_p$ as a $\mathbb{Q}_p$-linear combination of radical expressions over the rationals.

Resum

Com que tota extensió finita sobre un cos p-àdic és resoluble, qualsevol polinomi de grau 5 és resoluble per radicals sobre els nombres p-àdics. Utilitzant l'algoritme de Panayi, descrivim un mètode que permet expressar qualsevol arrel d'una quíntica irreductible sobre $\mathbb{Q}_p$ com una $\mathbb{Q}_p$-combinació lineal d'expressions radicals sobre els racionals.

Agraïments

Primer de tot, agraeixo al Dr. Artur Travesa per proposar-me aquest projecte i animar-me a endinsar-me en el món dels p-àdics. Li dóno les gràcies també per les hores que m'ha dedicat i la guia que m'ha procurat durant tot aquest temps.

En segon lloc, dono les gràcies a tots els companys de facultat, amics i familiars que m'han ajudat a arribar fins aquí.

Índex

Part III : Estudi de les quíntiques en $\mathbb{Q}_p$

1 Introducció

El projecte

És ben conegut que Abel va demostrar la impossibilitat de resoldre per radicals el polinomi general de grau 5 i que Galois va donar un criteri per decidir quan una quíntica és resoluble per radicals. Ara bé, tota extensió finita d'un cos de nombres p-àdic és resoluble i, per tant, tots els polinomis en una indeterminada són resolubles per radicals sobre $\mathbb{Q}_p$. El projecte consisteix en un estudi exhaustiu de la resolubilitat efectiva per radicals de les equacions quíntiques i irreductibles sobre els cossos de nombres p-àdics.

Tot i que hi ha fórmules generals per a la resolució de les quíntiques que són resolubles, l'estudi de les equacions de les extensions de grau 5 sobre $\mathbb{Q}_p$ ens permet fixar un objectiu: poder expressar les arrels d'un polinomi de coeficients racionals, irreductible sobre $\mathbb{Q}_p$, com $\mathbb{Q}_p$-combinacions lineals d'expressions radicals sobre $\mathbb{Q}$. En la memòria presentem tota la maquinària per poder assolir aquest objectiu.

Estructura de la Memòria

Estructurem la memòria en tres parts ben diferenciades.

En la primera part s'exposa la teoria necessària per demostrar que tota extensió finita sobre $\mathbb{Q}_p$ és resoluble. A més a més, presentem la teoria que necessitarem per tal de poder dur a terme un estudi exhaustiu de les quíntiques en $\mathbb{Q}_p$.

La segona part la dediquem a la resolubilitat de les quíntiques, i en ella exposem la primera resolució completa de les quíntiques resolubles, donada per Dummit l'any 1991, per contrastar-la amb la resolució publicada el 2014 per Faggal i Lazard, que obtenen fórmules molt més senzilles.

L'última part se centra en l'estudi de les quíntiques en els nombres p-àdics, on reproduïm la feina feta per Pauli i Roblot per tal de determinar polinomis generadors de totes les extensions de grau 5 sobre $\mathbb{Q}_p$. Amb l'ajuda de l'algoritme de Panayi, som capaços de determinar polinomis, resolubles per radicals sobre els racionals, que generen totes aquestes extensions. Això ens permet assolir l'objectiu fixat.

Conclusions

Aquest projecte ens ha permès estudiar amb detall els cossos de nombres p-àdics i les seves extensions. Tot i que en el treball ens centrem en les extensions de grau 5, es tenen resultats anàlegs per a extensions de grau un nombre primer. El fet de considerar el 5 només ens ajuda en el fet que el nombre d'extensions que obtenim sigui petit.

Quant a la resolubilitat de polinomis de grau un nombre primer, tindríem resultats anàlegs, però s'obtindrien unes fórmules cada vegada més complicades, a mesura que augmentem el nombre primer. D'altra banda, la resolució que acabem obtenint per als polinomis de grau 5 evidencia la impossibilitat de resoldre per radicals sobre els racionals qualsevol quíntica.

Per últim, notem que en el projecte només ens centrem en els polinomis de grau 5 que són irreductibles sobre $\mathbb{Q}_p$. Obtenir una resolució similar per a les arrels d'un polinomi que descompon sobre $\mathbb{Q}_p$ comportaria bastanta més feina a nivell de càlculs.

Part I : Cossos $\mathfrak{p}$-àdics

2 Enters algebraics

Ens centrem en l'estudi de la ramificació dels ideals primers de l'anell dels enters d'un cos de nombres. Comencem introduint l'anell dels enters d'un cos de nombres i establim certes propietats dels seus ideals. A més a més, introduïm el concepte de discriminant i acabem fixant-nos en els anells de valoració discreta.

Tots els anells que considerem són commutatius i amb element unitat. Anomenarem domini tot anell commutatiu amb element unitat i sense divisors de zero. Els resultats, amb les seves demostracions, es poden trobar en [17], [18] o [25]. L'apartat d'anells de valoració discreta també està basat en [23].

2.1 Anell dels enters d'un cos de nombres

Definició 2.1.1. *Siguin $A \subseteq B$ dos anells. Es diu que $b \in B$ és* **enter** *sobre A si b és arrel d'un polinomi mònic de coeficients en A. Quan tot element de B és enter sobre A, diem que B és enter sobre A (o que l'extensió $B|A$ és entera).*

Proposició 2.1.2. *Sigui $B|A$ una extensió d'anells. Aleshores, un element $b \in B$ és enter sobre A si, i només si, existeix un A-mòdul $M \subseteq B$ no nul i finitament generat tal que $bM \subseteq M$.*

Enunciem algunes propietats bàsiques dels elements enters.

Proposició 2.1.3. *Siguin $A \subseteq B$ dos anells, i sigui B enter sobre A.*

(1) Siguin A un domini i K el seu cos de fraccions. Si x és algebraic sobre K, aleshores existeix un element $a \in A$, $a \neq 0$, tal que ax és enter sobre A.

(2) Si C és un anell enter sobre B, aleshores C també és enter sobre A.

(3) Si σ és un homomorfisme de B, aleshores $\sigma(B)$ és enter sobre $\sigma(A)$.

Definició 2.1.4. *Sigui $B|A$ una extensió d'anells. Els elements de B que són enters sobre A conformen un anell que s'anomena* **clausura entera** *de A en B.*

Es diu que A és íntegrament tancat en B quan tot element de B enter sobre A és de A. Es diu que un domini és **íntegrament tancat** quan ho és en el seu cos de fraccions. Com que en un domini els coeficients d'un polinomi són polinomis simètrics en les arrels, podem obtenir el resultat següent.

Proposició 2.1.5. *Siguin A un domini íntegrament tancat, K el seu cos de fraccions i $L|K$ una extensió finita. Per a qualsevol element $b \in L$ enter sobre A, el polinomi minimal $\mathrm{Irr}(b, K)$ de b sobre K és de coeficients en A.*

És fàcil demostrar que tot domini de factorització única i, per tant, tot domini d'ideals principals, és íntegrament tancat. A més a més, les extensions enteres tenen un bon comportament per localització.

Proposició 2.1.6. *Siguin $B|A$ una extensió entera d'anells i S un subconjunt multiplicativament tancat de A. Aleshores, l'anell localitzat de B en S, $S^{-1}B$, és enter sobre $S^{-1}A$. Si A és íntegrament tancat, aleshores $S^{-1}A$ també ho és.*

Si $\mathfrak{p}$ és un ideal primer de A, anomenem **localitzat de A en $\mathfrak{p}$** l'anell $A_{(\mathfrak{p})}$ localitzat de A en $A - \mathfrak{p}$. Aquest anell és un domini local, és a dir, té un únic ideal maximal: $\mathfrak{p}$.

Es diu que un domini és **noetherià** si tota cadena creixent d'ideals és estacionària. Per a extensions $L|K$ separables es té un resultat fonamental pel fet que la forma bilineal traça $\mathrm{T}_{L|K} : L \times L \longrightarrow K$, definida per $\mathrm{T}_{L|K}(x, y) = \mathrm{Tr}_{L|K}(xy)$, és no degenerada.

Proposició 2.1.7. *Siguin A un domini noetherià i íntegrament tancat, K el seu cos de fraccions, $L|K$ una extensió finita i separable, i B la clausura entera de A en L. Aleshores, B és un A-mòdul finitament generat.*

Corol·lari 2.1.8. *Si, a més, A és un domini d'ideals principals, llavors B és un A-mòdul lliure de rang $[L : K]$.*

Considerem l'anell $\mathbb{Z}$ dels enters racionals. Un cos extensió finita dels nombres racionals $\mathbb{Q}$ s'anomena **cos de nombres**, i la clausura entera de $\mathbb{Z}$ en un cos de nombres K s'anomena l'**anell dels enters** de K, i es denota per $\mathcal{O}_K$. En virtut d'aquest corol·lari, l'anell $\mathcal{O}_K$ d'un cos de nombres K és un $\mathbb{Z}$-mòdul lliure de rang el grau de l'extensió $K|\mathbb{Q}$.

2.2 Ideals i anells de Dedekind

Siguin $A \subseteq B$ dos anells, $\mathfrak{P}$ un ideal primer de B i $\mathfrak{p} = \mathfrak{P} \cap A$ la seva contracció a A. La inclusió $A \hookrightarrow B$ indueix una injecció entre els anells $A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}$, de manera que l'ideal $\mathfrak{p}$ és un ideal primer de A. A més a més, el següent diagrama commuta:

$$\begin{array}{ccc} B & \twoheadrightarrow & B/\mathfrak{P} \\ \uparrow & & \uparrow \\ A & \twoheadrightarrow & A/\mathfrak{p}. \end{array}$$

Per l'apartat (3) de 2.1.3, si B és enter sobre A, llavors $B/\mathfrak{P}$ és enter sobre $A/\mathfrak{p}$.

Lema 2.2.1 (Nakayama)**.** *Siguin A un anell, $\mathfrak{a}$ un ideal contingut en tots els ideals maximals de A, i M un A-mòdul finitament generat. Si $\mathfrak{a}M = M$, aleshores $M = 0$.*

Proposició 2.2.2. *Siguin A un anell, $\mathfrak{p}$ un ideal primer, i $B|A$ una extensió entera d'anells. Aleshores, $\mathfrak{p}B \neq B$ i existeix un ideal primer $\mathfrak{P}$ de B tal que $\mathfrak{p} = \mathfrak{P} \cap A$.*

Notem que si B és enter sobre A i $\mathfrak{b}$ és un ideal no nul de B, aleshores $\mathfrak{b} \cap A \neq 0$. La demostració de 2.2.2 es fa per a l'anell localitzat de A en $\mathfrak{p}$, ja que la proposició 2.1.6 permet reduir la demostració al cas en què l'anell A és un anell local. El lema de Nakayama permet concloure la prova. De 2.2.2 se'n deriva el resultat següent.

Proposició 2.2.3. *Sigui $B|A$ una extensió entera d'anells. Sigui $\mathfrak{P}$ un ideal primer de B i $\mathfrak{p}$ la seva contracció a A. Aleshores, $\mathfrak{P}$ és maximal si, i només si, $\mathfrak{p}$ ho és.*

Un dels resultats més útils pel que fa a ideals és el teorema xinès del residu.

Teorema 2.2.4 (Teorema xinès del residu)**.** *Siguin A un anell i $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals coprimers dos a dos, és a dir, tals que $\mathfrak{a}_i + \mathfrak{a}_j = A$, si $i \neq j$. Donats $x_1, \ldots, x_n \in A$, existeix un element $x \in A$ tal que $x \equiv x_i \pmod{\mathfrak{a}_i}$ per a tot i.*

Definició 2.2.5. *S'anomena* **anell de Dedekind** *tot domini noetherià, íntegrament tancat, que no és un cos i en què tot ideal primer no nul és maximal.*

Observació 2.2.6. Del corol·lari 2.1.8 es dedueix que l'anell dels enters $\mathcal{O}_K$ d'un cos de nombres K és un domini noetherià i íntegrament tancat, i la proposició 2.2.3 ens assegura

que tot ideal primer no nul és maximal, ja que l'extensió $\mathcal{O}_K|\mathbb{Z}$ és entera i en $\mathbb{Z}$ tenim aquesta propietat. Així, l'anell dels enters d'un cos de nombres és un anell de Dedekind.

Definició 2.2.7. *Siguin $\mathfrak{a}, \mathfrak{b} \subseteq A$ dos ideals. Es diu que l'ideal $\mathfrak{b}$ divideix l'ideal $\mathfrak{a}$ si existeix un ideal $\mathfrak{c} \subseteq A$ tal que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.*

Definició 2.2.8. *Siguin A un domini i K el seu cos de fraccions. Un ideal fraccionari $\mathfrak{a}$ de K és un A-submòdul de K per al qual existeix un element $a \in A$, $a \neq 0$, tal que $a\mathfrak{a} \subseteq A$.*

Teorema 2.2.9. *Siguin A un anell de Dedekind i K el seu cos de fraccions. Els ideals fraccionaris no nuls de A conformen un grup abelià lliure respecte de la multiplicació de A-submòduls de K. A més, els ideals primers no nuls de A formen un sistema de generadors lliure d'aquest grup, i un ideal $\mathfrak{b} \subseteq A$ divideix un ideal $\mathfrak{a} \subseteq A$ si, i només si, $\mathfrak{a} \subseteq \mathfrak{b}$.*

Així doncs, per als anells de Dedekind tenim un anàleg del teorema fonamental de l'aritmètica a nivell d'ideals.

Proposició 2.2.10. *Tot anell de Dedekind amb un nombre finit d'ideals primers és un domini d'ideals principals.*

Proposició 2.2.11. *Sigui A un anell de Dedekind i S un subconjunt multiplicativament tancat de A. Aleshores, $S^{-1}A$ és un anell de Dedekind i l'aplicació $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ és un morfisme exhaustiu del grup dels ideals fraccionaris de A en el dels de $S^{-1}A$, que té per nucli els ideals fraccionaris de A que tenen intersecció no buida amb S.*

2.3 Ramificació

Siguin K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. En l'apartat anterior hem vist que si $\mathfrak{p}$ és un ideal primer no nul de $\mathcal{O}_K$, aleshores $\mathfrak{p} \cap \mathbb{Z}$ és un ideal primer no nul de $\mathbb{Z}$, és a dir, existeix un nombre primer p tal que $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. A més a més, pel teorema 2.2.9, l'ideal primer $\mathfrak{p}$ divideix l'ideal $p\mathcal{O}_K$. Ens interessa estudiar la descomposició de l'ideal $p\mathbb{Z}$ en producte d'ideals primers de l'anell $\mathcal{O}_K$.

Més generalment, si K és un cos de nombres i $L|K$ és una extensió finita, ens interessa estudiar la descomposició dels ideals primers de $\mathcal{O}_K$ en producte d'ideals primers de l'anell $\mathcal{O}_L$. Ja sabem que $\mathcal{O}_K$ i $\mathcal{O}_L$ són anells de Dedekind, però de fet, tenim encara més.

Proposició 2.3.1. *$\mathcal{O}_L$ és la clausura entera de $\mathcal{O}_K$ en L.*

Del teorema 2.2.9 deduïm que si $\mathfrak{p} \subset \mathcal{O}_K$ és un ideal primer no nul, aleshores l'ideal extensió $\mathfrak{p}\mathcal{O}_L$ (per la proposició 2.2.2, $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$) descompon en producte d'ideals primers de manera única. Si $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$, on els $\mathfrak{P}_i$ són ideals primers diferents de $\mathcal{O}_L$ i els e_i són enters positius, és aquesta descomposició, l'exponent e_i s'anomena **índex de ramificació** de $\mathfrak{P}_i$ sobre $\mathfrak{p}$, i el denotem per $e_{\mathfrak{P}_i|\mathfrak{p}}$.

Com que l'ideal $\mathfrak{p}$ és maximal, l'anell $\mathcal{O}_K/\mathfrak{p}$ és un cos, que s'anomena el **cos residual** de $\mathcal{O}_K$ en $\mathfrak{p}$, i el denotem per $\kappa_\mathfrak{p}$. Si $\mathfrak{P}$ és un ideal primer no nul de $\mathcal{O}_L$ que divideix $\mathfrak{p}$, l'extensió de cossos residuals $\kappa_\mathfrak{P}|\kappa_\mathfrak{p}$ és finita i, atès que $\mathbb{Z}/p\mathbb{Z}$ és un cos finit, aquesta extensió és de cossos finits. El grau d'aquesta extensió s'anomena el **grau residual** en $\mathfrak{P}$ de $L|K$ i el denotem per $f_{\mathfrak{P}|\mathfrak{p}}$.

Proposició 2.3.2. *Els índexs de ramificació i els graus residuals són multiplicatius per a cadenes d'extensions.*

Definició 2.3.3. *Es defineix la* **norma** *de $\mathfrak{P}$ com $\mathrm{N}_{L|K}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}|\mathfrak{p}}}$ i s'estén a tots els*

ideals per multiplicativitat. Si l'ideal $\mathfrak{P}$ és principal, generat per un element $\Pi \in B$, llavors $\mathrm{N}_{L|K}(\mathfrak{P}) = \mathrm{N}_{L|K}(\Pi)B$.

El bon comportament dels anells de Dedekind (2.2.11) i dels cossos residuals per localització permet definir tots aquests conceptes per a anells localitzats dels anells d'enters.

Proposició 2.3.4. *Sigui S un subconjunt multiplicativament tancat de $\mathcal{O}_K$. Aleshores,*

$$e_{\mathfrak{P}|\mathfrak{p}} = e_{S^{-1}\mathfrak{P}|S^{-1}\mathfrak{p}} \quad i \quad f_{\mathfrak{P}|\mathfrak{p}} = f_{S^{-1}\mathfrak{P}|S^{-1}\mathfrak{p}}.$$

Definició 2.3.5. *Siguin $A := S^{-1}\mathcal{O}_K$ i $B := S^{-1}\mathcal{O}_L$, i siguin $\mathfrak{P}$ un ideal primer no nul de B i $\mathfrak{p} = \mathfrak{P} \cap A$ la seva contracció a A.*

Es diu que $\mathfrak{P}$ **ramifica** *en l'extensió $B|A$ quan $e_{\mathfrak{P}|\mathfrak{p}} > 1$. En cas contrari es diu que $\mathfrak{P}$ no ramifica en $B|A$.*

Es diu que $\mathfrak{p}$ ramifica en l'extensió $B|A$ quan existeix algun primer $\mathfrak{P}$ de B que divideix $\mathfrak{p}$ que hi ramifica. En cas contrari es diu que $\mathfrak{p}$ no ramifica en $B|A$.

Proposició 2.3.6. *Siguin $n = [L : K]$, $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ la descomposició de $\mathfrak{p}B$ en factors primers de B i f_i el grau residual en $\mathfrak{P}_i$ de l'extensió $L|K$. Aleshores,*

$$\sum_{i=1}^{g} e_i f_i = n. \tag{2.1}$$

Per tal de demostrar aquesta igualtat, primer es redueix la demostració al cas en què A és un anell local. Llavors, B només té un nombre finit d'ideals primers i, per la proposició 2.2.10, és principal. Amb el teorema xinès del residu, s'observa que n'hi ha prou de demostrar que $B/\mathfrak{P}_i^{e_i}$ és de dimensió $e_i f_i$ sobre $A/\mathfrak{p}$ i, per últim, que $[\kappa_{\mathfrak{P}} : \kappa_{\mathfrak{p}}] = n$.

2.4 El discriminant

Un invariant molt important d'extensions de cossos de nombres és l'ideal discriminant. Siguin K un cos de nombres, A un localitzat del seu anell d'enters, $L|K$ una extensió finita i de grau n, i B la clausura entera de A en L.

Definició 2.4.1. *Sigui $\{b_1, \dots, b_n\}$ una K-base de L. El* **discriminant** *de $\{b_1, \dots, b_n\}$ és l'element de K^* definit per*

$$d(b_1, \dots, b_n) := \det(\mathrm{Tr}_{L|K}(b_i b_j)).$$

Observació 2.4.2. Els discriminants de K-bases de L diferents coincideixen mòdul quadrats de K^*, ja que fem un canvi de base a la forma bilineal traça.

Proposició 2.4.3. *Sigui $\alpha \in L$ un element primitiu de l'extensió $L|K$ i sigui $f(X) = \mathrm{Irr}(\alpha, K)(X)$ el polinomi minimal de α sobre K. Aleshores,*

$$\mathrm{disc}(f) = d(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_{L|K}(f'(\alpha)),$$

on $\mathrm{disc}(f)$ denota el discriminant de f i f' denota el polinomi derivat de f.

Definició 2.4.4. *Es defineix el* **discriminant** *de l'extensió $B|A$ com l'ideal $\Delta_{B|A}$ de A generat pels discriminants $d(b_1, \dots, b_n)$, quan els conjunts $\{b_1, \dots, b_n\}$ recorren totes les possibles K-bases de L formades per elements de B. Quan no hi ha confusió de l'extensió d'anells que considerem, el denotem per $\Delta_{L|K}$.*

Si S és un subconjunt multiplicativament tancat de A, aleshores se satisfà la igualtat $S^{-1}\Delta_{B|A} = \Delta_{S^{-1}B|S^{-1}A}$.

Proposició 2.4.5. *Si A és un domini d'ideals principals, aleshores l'ideal $\Delta_{B|A}$ està generat pel discriminant de qualsevol A-base de B.*

El discriminant permet caracteritzar els ideals primers de A que ramifiquen.

Proposició 2.4.6. *Sigui $\mathfrak{p}$ un ideal primer no nul de A. L'ideal $\mathfrak{p}$ ramifica en l'extensió $B|A$ si, i només si, divideix el discriminant $\Delta_{B|A}$.*

Per demostrar aquest resultat, es redueix la demostració al cas local i es fa l'estudi del discriminant mòdul $\mathfrak{p}$, on el paper de la forma bilineal traça torna a ser clau.

Corol·lari 2.4.7. *Només un nombre finit d'ideals primers de A ramifiquen en $B|A$.*

2.5 Extensions de Galois de cossos de nombres

Siguin K un cos de nombres, A un localitzat del seu anell d'enters, $L|K$ una extensió finita i de Galois, G el seu grup de Galois i B la clausura entera de A en L. Siguin també $\mathfrak{P}$ un ideal primer no nul de B i $\mathfrak{p} = \mathfrak{P} \cap A$ la seva contracció a A. Per a qualsevol $\sigma \in G$, $\sigma(\mathfrak{P})$ és un ideal primer no nul de B i $\sigma(\mathfrak{P}) \cap A = \sigma(\mathfrak{P} \cap A) = \sigma(\mathfrak{p}) = \mathfrak{p}$, de manera que $\sigma(\mathfrak{P})$ també divideix $\mathfrak{p}$. A més, se satisfà el resultat següent.

Proposició 2.5.1. *El grup de Galois G opera transitivament en el conjunt dels ideals primers $\mathfrak{P}$ de B que divideixen $\mathfrak{p}$.*

D'altra banda, la igualtat (2.1) se simplifica de la manera que enunciem a continuació.

Proposició 2.5.2. *Tots els ideals primers de B que divideixen l'ideal primer $\mathfrak{p} \subset A$ tenen el mateix índex de ramificació e i el mateix grau residual f. Per tant,*

$$efg = n. \tag{2.2}$$

Definició 2.5.3. *Si $\mathfrak{P}$ és un ideal primer no nul de B, el subgrup d'isotropia de $\mathfrak{P}$,*

$$D_{\mathfrak{P}|\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

s'anomena el **grup de descomposició** *de $\mathfrak{P}$ en l'extensió $B|A$.*

Proposició 2.5.4. *L'extensió de cossos residuals $\kappa_{\mathfrak{P}}|\kappa_{\mathfrak{p}}$ és normal i el morfisme de grups $D_{\mathfrak{P}|\mathfrak{p}} \longrightarrow \mathrm{Gal}(\kappa_{\mathfrak{P}}|\kappa_{\mathfrak{p}})$, definit de manera natural, és exhaustiu.*

Es defineix el **grup d'inèrcia** de $\mathfrak{P}$ en $B|A$ com el nucli d'aquest morfisme.

Observació 2.5.5. Per la fórmula de les òrbites de l'acció d'un grup en un conjunt, el nombre $g_{\mathfrak{p}}$ d'ideals primers diferents de B que divideixen $\mathfrak{p}$ és l'índex del grup de descomposició $D_{\mathfrak{P}|\mathfrak{p}}$ en el grup de Galois G de l'extensió. Així doncs, $\#D_{\mathfrak{P}|\mathfrak{p}} = ef$. Com que el grau de l'extensió residual de cossos finits $\kappa_{\mathfrak{P}}|\kappa_{\mathfrak{p}}$ coincideix amb l'índex del grup d'inèrcia en el grup de descomposició de l'extensió, aleshores $\#I_{\mathfrak{P}|\mathfrak{p}} = e$.

2.6 Anells de valoració discreta

Un **anell de valoració discreta** és un domini d'ideals principals que conté un únic ideal primer $\mathfrak{p}$ no nul. En un domini d'ideals principals A, els ideals primers no nuls són de

la forma πA, on π és un element irreductible. Per tant, si A és un anell de valoració discreta, A conté un únic element irreductible π mòdul multiplicació per unitats i $\mathfrak{p} = \pi A$. L'element π s'anomena un **uniformitzant** de A.

Els ideals no nuls de A són de la forma $\pi^r A$ i si $a \in A$ és no nul, podem posar $a = \pi^r u$, amb $r \in \mathbb{Z}_{\geq 0}$ i $u \in A^\times$ una unitat. L'exponent r s'anomena la **valoració $\mathfrak{p}$-àdica** de a, el denotem per $v_\mathfrak{p}(a)$ (o simplement $v(a)$) i no depèn de l'uniformitzant escollit.

Si ara considerem el cos de fraccions K de A, i prenem $x = a/b$ un element de K^*, podem posar $x = \pi^r u$, amb $r = v(x) \in \mathbb{Z}$ i, clarament, $v(x)$ no depèn de l'elecció de a i b. D'aquesta manera, tenim un morfisme de grups exhaustiu $v : K^* \longrightarrow \mathbb{Z}$ que satisfà:

$$v(x+y) \geq \inf\{v(x), v(y)\}, \quad \forall x, y \in K^*. \tag{2.3}$$

Amb el conveni $v(0) = +\infty$, podem estendre aquesta aplicació a tot el cos K. Amb aquesta valoració definida, $A = \{x \in K : v(x) \geq 0\}$ i $\pi A = \{x \in K : v(x) > 0\}$.

Definició 2.6.1. *Tot morfisme de grups exhaustiu $v : K^* \longrightarrow \mathbb{Z}$ verificant (2.3) s'anomena* **valoració discreta**. *El conjunt $v(K^*)$ s'anomena el* **grup de valors** *de la valoració.*

Si v és una valoració discreta definida en un cos K, els elements $x \in K$ de valoració no negativa conformen un anell de valoració discreta: podem considerar un element $\pi \in K$ tal que $v(\pi) = 1$ i, llavors, tot element $a \in A$ s'escriu de la forma $a = \pi^{v(a)}u$, amb $v(u) = 0$.

És clar que tot anell de valoració discreta és un anell de Dedekind i, per 2.2.10, tot anell de Dedekind amb un únic ideal primer és un anell de valoració discreta. Si A és un anell de Dedekind i $\mathfrak{p}$ és un ideal primer, llavors el localitzat de A en $\mathfrak{p}$, $A_{(\mathfrak{p})}$, és un anell de valoració discreta i tenim definida una valoració discreta en el cos de fraccions K de A.

Donada una valoració discreta $v_\mathfrak{p}$ en un cos K, podem definir un valor absolut $|\cdot|_\mathfrak{p} : K \longrightarrow \mathbb{R}$ associat a aquesta valoració com $|x|_\mathfrak{p} = e^{-v_\mathfrak{p}(x)}$, $\forall x \in K^*$ i $|0|_\mathfrak{p} = 0$. Per (2.3), aquest valor absolut és un valor absolut **no arquimedià**, és a dir,

$$|x+y|_\mathfrak{p} \leq \max\{|x|_\mathfrak{p}, |y|_\mathfrak{p}\}, \quad \forall x, y \in K. \tag{2.4}$$

Definició 2.6.2. *Diem que dos valors absoluts $|\cdot|_1$, $|\cdot|_2$ definits en un cos K són* **equivalents** *si defineixen la mateixa topologia en K.*

Proposició 2.6.3. *Els valors absoluts $|\quad|_c$ definits per $|x|_c = c^{-v_\mathfrak{p}(x)}$, $\forall x \in K$, amb $c \in \mathbb{R}_{>1}$, defineixen valors absoluts equivalents al valor absolut $|\quad|_\mathfrak{p}$.*

Algunes de les propietats que utilitzarem són les següents.

Proposició 2.6.4. *Sigui $v_\mathfrak{p}$ una valoració discreta definida en un cos K. Aleshores:*

(1) El parell $(K, |\quad|_\mathfrak{p})$ és un espai ultramètric.

(2) L'anell de valoració discreta $A = \{x \in K : v_\mathfrak{p}(x) \geq 0\} = \{x \in K : |x|_\mathfrak{p} \leq 1\}$ és tancat.

(3) Si $|x|_\mathfrak{p} > |y|_\mathfrak{p}$, aleshores $|x+y|_\mathfrak{p} = |x|_\mathfrak{p}$.

(4) Siguin $x_i \in K$ tals que $v_\mathfrak{p}(x_i) > v_\mathfrak{p}(x_1)$, per a $i \geq 2$. Aleshores $x_1 + x_2 + \cdots + x_n \neq 0$.

Definició 2.6.5. *Es diu que un espai mètric és* **complet** *si tota successió de Cauchy convergeix.*

Hem vist que la clausura entera de l'anell d'enters d'un cos de nombres és un anell de Dedekind, però la clausura entera d'un anell de valoració discreta no és, en general, un anell de valoració discreta. Ara bé, per a espais mètrics $(K, |\quad|_\mathfrak{p})$ complets, aquesta propietat sí que se satisfà.

3 Teoria de valoracions

Estudiem les valoracions $\mathfrak{p}$-àdiques. Comencem introduint els nombres racionals p-àdics i continuem amb l'estudi de les valoracions $\mathfrak{p}$-àdiques i complecions d'un cos de nombres. També estudiem les extensions de cossos $\mathfrak{p}$-àdics per tal de demostrar el lema de Krasner i, a continuació, introduïm el lema de Hensel. Per últim, estudiem en detall les extensions no ramificades i les totalment i moderadament ramificades. Els resultats, amb les seves demostracions, es poden trobar en [11], [17], [18] o [25].

3.1 Els nombres p-àdics

El matemàtic alemany K. Hensel (1861-1941) va introduir els nombres p-àdics a principis del segle XX per introduir en teoria de nombres eines de desenvolupament de funcions en seriès de potències. Hensel va veure una analogia entre l'anell $\mathbb{Z}$ dels enters racionals i l'anell $\mathbb{C}[X]$ dels polinomis de coeficients complexos. Tot enter descompon de manera única com ± 1 vegades un producte de primers (positius), i tot polinomi descompon de manera única com $a \in \mathbb{C}$ vegades un producte de polinomis lineals $X - \alpha \in \mathbb{C}[X]$.

En el cas d'un polinomi $f(X) \in \mathbb{C}[X]$, el seu comportament local en un punt $\alpha \in \mathbb{C}$ es pot conèixer pel seu desenvolupament en sèrie de Taylor al voltant del punt α. I més generalment, per a funcions racionals $f(X) \in \mathbb{C}(X)$, el seu comportament local en α ve donat pel desenvolupament en sèrie de Laurent. Amb els nombres enters passa una cosa similar. Primer, tot enter positiu $n \in \mathbb{Z}$ admet una **expansió p-àdica**

$$n = a_0 + a_1 p + \cdots + a_n p^n, \quad \text{amb } a_i \in \{0, 1, \ldots, p-1\};$$

i aquests coeficients a_i són únics. Quan volem escriure aquestes expansions p-àdiques per a nombres negatius o racionals, ja hem d'incloure sumes infinites.

Definició 3.1.1. *Fixat un nombre primer p, un* **enter p-àdic** *és una sèrie formal*

$$a_0 + a_1 p + a_2 p^2 + \ldots, \quad \textit{amb } a_i \in \{0, 1, \ldots, p-1\}.$$

El conjunt de tots els enters p-àdics el denotem per $\mathbb{Z}_p$.

Tot nombre racional $x \in \mathbb{Z}_{(p)}$ amb denominador no divisible per p defineix una successió de classes de residus $x \equiv \overline{s}_n \pmod{p^n}$ amb $n \geq 1$ i $\overline{s}_n \in \{0, 1, \ldots, p^n - 1\}$, de manera que podem trobar una única successió $(a_n)_{n \geq 0}$, amb $a_n \in \{0, 1, \ldots, p-1\}$, tal que

$$\overline{s}_n \equiv a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \pmod{p^n}, \quad \forall n \geq 1.$$

La successió de sumes $\sum_{i=0}^{n} a_i p^i$ defineix el nombre p-àdic $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$, que s'anomena **l'expansió p-àdica** de x. Amb analogia amb les sèries de Laurent, podem estendre els nombres p-àdics acceptant també les sèries formals de la forma $\sum_{i=-m}^{\infty} a_i p^i$, amb $m \in \mathbb{Z}$. El conjunt d'aquestes sèries s'anomena el conjunt dels **nombres p-àdics**.

Ara, per a qualsevol $y \in \mathbb{Q}$, podem posar $y = p^{-m} x$, amb $x \in \mathbb{Z}_{(p)}$, i obtenir l'expansió p-àdica de y. D'aquesta manera, tenim una injecció $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ que envia $\mathbb{Z}$ a $\mathbb{Z}_p$. Per tal de definir una suma i una multiplicació que converteixi $\mathbb{Z}_p$ en un anell i $\mathbb{Q}_p$ en el seu cos de fraccions, és convenient veure els nombres p-àdics $\mathbb{Z}_p$ com el **límit projectiu** dels anells $\mathbb{Z}/p^n\mathbb{Z}$:

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \{(x_n)_{n \geq 1} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : \lambda_n(x_{n+1}) = x_n, \, \forall n \},$$

on les aplicacions λ_n són les projeccions $\lambda_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, i podem definir la suma i la multiplicació component a component. Es pot comprovar que les classes de residus $\overline{s}_n \equiv \sum_{i=0}^{n-1} a_i p^i \pmod{p^n}$ definieixen una bijecció entre $\mathbb{Z}_p$ i $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

Donat un nombre primer $p \in \mathbb{Z}$, l'anell $\mathbb{Z}_{(p)}$ és un anell de valoració discreta i ja hem vist en 2.6 que a tot element $x \in \mathbb{Q}$ li podem associar una valoració $v_p(x)$, que s'anomena la **valoració p-àdica** de x.

Definició 3.1.2. *Per a tot $x \in \mathbb{Q}$, es defineix el* **valor absolut p-àdic** *de x com $|x|_p = p^{-v_p(x)}$, si $x \neq 0$, i definim $|0|_p = 0$.*

Així, en $\mathbb{Q}$ coneixem el valor absolut trivial, que ve donat per $|x| = 1$, $\forall x \in \mathbb{Q}$; el valor absolut usual, que denotem per $|\cdot|_\infty$; i els valors absoluts p-àdics que acabem de definir. Es pot demostrar que tots aquests valors absoluts defineixen topologies diferents en $\mathbb{Q}$ i, per tant, no són equivalents. Un resultat fonamental pel que fa als valors absoluts de $\mathbb{Q}$ és el teorema d'Ostrowski, que determina quins són els valors absoluts que hi ha.

Teorema 3.1.3 (Ostrowski)**.** *Qualsevol valor absolut not trivial de $\mathbb{Q}$ és equivalent a un dels valors absoluts $|\cdot|_p$, on p és un nombre primer o bé $p = \infty$.*

Els nombres racionals no són un cos complet respecte de cap valor absolut no trivial, i el cos $\mathbb{Q}_p$ dels nombres p-àdics és el que s'anomena **la compleció** de $\mathbb{Q}$ respecte d'aquest valor absolut. A continuació entendrem millor el concepte de compleció.

3.2 Valoracions $\mathfrak{p}$-àdiques i complecions d'un cos de nombres

Siguin K un cos de nombres, A el seu anell d'enters i $\mathfrak{p} \subset A$ un ideal primer no nul. En 2.6 hem vist que tenim definida una valoració $v_\mathfrak{p} : K \longrightarrow \mathbb{Z} \cup \{+\infty\}$ associada a l'ideal $\mathfrak{p}$ i que aquesta valoració indueix un valor absolut no arquimedià $|\cdot|_\mathfrak{p} : K \longrightarrow \mathbb{R}$, definit per $|x|_\mathfrak{p} = e^{-v_\mathfrak{p}(x)}$, i que anomenem **valor absolut $\mathfrak{p}$-àdic**.

Si K és un cos dotat d'un valor absolut $|\quad|$, podem completar K de la mateixa manera que es construeixen els nombres reals a partir dels racionals. Considerem el conjunt $\mathcal{C}(K)$ format les successions de Cauchy de K. Aquest conjunt és un anell i el subconjunt $\mathcal{I}_0(K)$ de les successions de Cauchy de K que tenen límit zero és un ideal maximal de l'anell. Aleshores, el quocient $\hat{K} = \mathcal{C}(K)/\mathcal{I}_0(K)$ és un cos. Si identifiquem cada element $x \in K$ amb la successió constant de valor x, aquest cos $\hat{K}$ conté K com a subcòs, el valor absolut de K s'estén a $\hat{K}$ per continuïtat, K és dens en $\hat{K}$ i $\hat{K}$ és complet. A més a més, un cos amb aquestes propietats és únic llevat d'isomorfismes que respecten els valors absoluts i s'anomena la **compleció** de K respecte del valor absolut $|\quad|$.

Definició 3.2.1. *Un cos $\mathfrak{p}$-àdic és la compleció $K_\mathfrak{p}$ d'un cos de nombres K respecte d'un valor absolut $\mathfrak{p}$-àdic.*

Siguin A un anell de valoració discreta, $\mathfrak{p}$ el seu ideal maximal i K el seu cos de fraccions. La valoració $v_\mathfrak{p}$ s'estén a una valoració $\hat{v}_\mathfrak{p}$ de $\hat{K}$ per continuïtat: si $a = \lim_{n\to\infty} a_n \in \hat{K}$, amb $(a_n)_{n\geq 1} \subset K$, es defineix

$$\hat{v}_\mathfrak{p}(a) = \lim_{n\to\infty} v_\mathfrak{p}(a_n).$$

Si $a \neq 0$, la successió $(v_\mathfrak{p}(a_n))_{n\geq 1}$ és estacionària , ja que, per a n prou gran, $\hat{v}_\mathfrak{p}(a - a_n) > \hat{v}_\mathfrak{p}(a)$ i, per la propietat (3) de 2.6.4,

$$v_\mathfrak{p}(a_n) = \hat{v}_\mathfrak{p}(a_n - a + a) = \min\{\hat{v}_\mathfrak{p}(a_n - a), \hat{v}_\mathfrak{p}(a)\} = \hat{v}_\mathfrak{p}(a),$$

de manera que $v_{\mathfrak{p}}(K^*) = \hat{v}_{\mathfrak{p}}(\hat{K}^*)$. Aquesta valoració $\hat{v}_{\mathfrak{p}}$ de $\hat{K}$ és l'única que estén la valoració $v_{\mathfrak{p}}$ i tal que el valor absolut de $\hat{K}$ ve definit per aquesta valoració.

Proposició 3.2.2. *Siguin A un anell de valoració discreta, $\mathfrak{p} = \pi A$ el seu ideal maximal, K el seu cos de fraccions i $\hat{K}$ la compleció de K respecte del valor absolut $\mathfrak{p}$-àdic. Definim $\hat{A} := \{x \in \hat{K} : |x|_{\mathfrak{p}} \leq 1\}$ i $\hat{\mathfrak{p}} := \{x \in \hat{K} : |x|_{\mathfrak{p}} < 1\}$. Aleshores, $\hat{A}$ és un anell de valoració discreta amb ideal maximal $\hat{\mathfrak{p}}$ i cos de fraccions $\hat{K}$, i*

(i) $\hat{\mathfrak{p}}^n = \pi^n \hat{A} \quad i \quad A/\mathfrak{p}^n \simeq \hat{A}/\hat{\mathfrak{p}}^n, \quad \forall n \in \mathbb{Z}_{\geq 0}$; *i*

(ii) $\hat{A}$ és la compleció de A respecte del valor absolut $\mathfrak{p}$-àdic.

Observació 3.2.3. L'anell $\hat{A}$ és el límit projectiu dels anells $A/\mathfrak{p}^n$. Si K és un cos de nombres, el cos residual $\kappa_{\mathfrak{p}}$ de A és un cos finit i els anells $A/\mathfrak{p}^n$ també són finits. És a dir, són anells topològics discrets, compactes i Hausdorff. En la pàgina 91 de [22] es demostra de manera senzilla que, en aquest cas, $\hat{A}$ també és compacte.

Proposició 3.2.4. *Siguin A un anell de valoració discreta, $\mathfrak{p} = \pi A$ el seu ideal maximal, K el seu cos de fraccions i $\hat{K}$ la compleció de K respecte del valor absolut $\mathfrak{p}$-àdic. Sigui $R \subseteq A$ un sistema de representants per al cos residual $\kappa_{\mathfrak{p}}$, amb $0 \in R$. Tot element no nul $x \in \hat{K}^*$ es pot escriure de manera única com*

$$x = \sum_{n=n_0}^{\infty} a_n \pi^n, \quad amb \ a_n \in R, \, a_{n_0} \neq 0, \, n_0 \in \mathbb{Z}.$$

Sigui K un cos de nombres dotat d'un valor absolut $|\quad|$. La restricció de $|\quad|$ a $\mathbb{Q}$ ha de ser un dels valors absoluts de $\mathbb{Q}$, de manera que, en virtut del teorema d'Ostrowski (3.1.3), o bé és el trivial, o bé és l'usual, o bé és un valor absolut p-àdic per a un cert nombre primer p. Es pot demostrar que si $K'|k$ és una extensió algebraica de cossos, aleshores l'únic valor absolut de K' que estén el valor absolut trivial de k és el trivial. A més a més, un valor absolut arquimedià de K' es restringeix a un valor absolut arquimedià de k.

Així doncs, si $|\quad|$ és un valor absolut no trivial i no arquimedià de K, aleshores $|\quad|$ és l'extensió d'un dels valors absoluts p-àdics de $\mathbb{Q}$. Veiem com es poden estendre aquests valors absoluts p-àdics a un cos de nombres.

Siguin K un cos de nombres, $\mathcal{O}_K$ el seu anell d'enters, $\mathfrak{p}$ un ideal primer de $\mathcal{O}_K$, A el localitzat de $\mathcal{O}_K$ en $\mathfrak{p}$ i $L|K$ una extensió finita. Sabem que A és un anell de valoració discreta i, de 2.2.11, deduïm que l'anell B localitzat de $\mathfrak{p}\mathcal{O}_L$ en $\mathcal{O}_L$ és un anell de Dedekind que, a més, és la clausura entera de A en L.

Llavors, tenim que $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$, on $e_i \geq 1$, i $\mathfrak{P}_i$ són els únics ideals primers de B. Els anells localitzats de B en els ideals $\mathfrak{P}_i$ són anells de valoració discreta que contenen A, i podem considerar la valoració $\mathfrak{P}_i$-àdica de L. Normalitzant aquesta valoració de manera que el seu grup de valors sigui $e_i^{-1}\mathbb{Z}$, obtenim una valoració que estén la valoració $\mathfrak{p}$-àdica de K. És a dir, per a cada ideal primer $\mathfrak{P}$ de B que divideix $\mathfrak{p}$ obtenim un valor absolut en L que estén el valor absolut $\mathfrak{p}$-àdic de K. El resultat que enunciem a continuació ens assegura que, mòdul valors absoluts equivalents, aquests són els únics valors absoluts de L que estenen el valor absolut $\mathfrak{p}$-àdic de K.

Proposició 3.2.5. *Tot valor absolut de L que estén el valor absolut $\mathfrak{p}$-àdic de K és un dels valors absoluts $\mathfrak{P}_i$-àdics. A més a més, els valors absoluts $\mathfrak{P}_i$-àdic i $\mathfrak{P}_j$-àdic de L no són equivalents, si $i \neq j$.*

3.3 Extensió de cossos $\mathfrak{p}$-àdics

Siguin K un cos de nombres, A el seu anell d'enters, $L|K$ una extensió finita i B la clausura entera de A en L. Siguin també $\mathfrak{P}$ un ideal primer no nul de B, $\mathfrak{p} = \mathfrak{P} \cap A$ la seva contracció a A, i e i f l'índex de ramificació i el grau residual de l'extensió, respectivament. Considerem $L_{\mathfrak{P}}$, la compleció de L respecte del valor absolut $\mathfrak{P}$-àdic, i $K_{\mathfrak{p}}$, la compleció de K respecte del valor absolut $\mathfrak{p}$-àdic. Per 3.2.2, aquests cossos són els cossos de fraccions de les complecions dels anells de valoració discreta localitzats de B en $\mathfrak{P}$ i de A en $\mathfrak{p}$. Denotem per $\hat{\mathfrak{P}}$ i $\hat{\mathfrak{p}}$ els seus ideals maximals, respectivament. Tal i com hem fet en l'apartat 2.3, podem considerar l'índex de ramificació $\hat{e}$ i el grau residual $\hat{f}$ de l'extensió completada.

Proposició 3.3.1. *$L_{\mathfrak{P}}$ conté $K_{\mathfrak{p}}$ i l'extensió $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ és finita de grau ef. La valoració $\hat{\mathfrak{P}}$-àdica és l'única valoració de $L_{\mathfrak{P}}$ que estén la valoració $\hat{\mathfrak{p}}$-àdica i, a més, $e = \hat{e}$ i $f = \hat{f}$.*

Aquest resultat és, en part, conseqüència del lema que enunciem a continuació.

Lema 3.3.2. *Siguin K un cos $\mathfrak{p}$-àdic i A el seu anell de valoració discreta. Si $L|K$ és una extensió finita, aleshores la clausura entera B de A en L és un anell de valoració discreta, i L és complet per la topologia definida per B.*

Vist això, podem estudiar com es relacionen els grups de Galois d'extensions de Galois $L|K$ amb els de les seves completades $L_{\mathfrak{P}}|K_{\mathfrak{p}}$.

Proposició 3.3.3. *Si $L|K$ és una extensió de Galois, aleshores l'extensió $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ també ho és i el seu grup de Galois és $D_{\mathfrak{P}|\mathfrak{p}}$, el grup de descomposició de $\mathfrak{P}$ en $L|K$.*

Demostració. Sigui $\sigma \in D_{\mathfrak{P}|\mathfrak{p}}$. En ser $L_{\mathfrak{P}}$ la compleció de L en $\mathfrak{P}$, i $\sigma(\mathfrak{P}) = \mathfrak{P}$, aleshores σ s'estén per continuïtat a un automorfisme de $L_{\mathfrak{P}}$. A més a més, com que σ és la identitat en K, també ho és en $K_{\mathfrak{p}}$, de manera que σ defineix un element de $\mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}})$. D'altra banda, dos elements diferents de $D_{\mathfrak{P}|\mathfrak{p}}$ defineixen elements diferents de $\mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}})$, ja que actuen diferent en L. Per 3.3.1, $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef = \#D_{\mathfrak{P}|\mathfrak{p}}$, amb el que concloem que $D_{\mathfrak{P}|\mathfrak{p}} \simeq \mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}})$. □

Observació 3.3.4. Més endavant definirem els grups de ramificació superior d'una extensió de Galois. D'aquest resultat es dedueix que els grups de ramificació superior de l'extensió $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ coincideixen amb els de l'extensió $L|K$.

Com que $K_{\mathfrak{p}}$ és un cos complet respecte d'un valor absolut no trivial i no arquimedià, llavors en tot $K_{\mathfrak{p}}$-espai vectorial de dimensió finita dues normes qualssevol són equivalents. Això permet deduir que si $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ és una extensió finita de cossos, dues extensions del valor absolut de $K_{\mathfrak{p}}$ en $L_{\mathfrak{P}}$ són equivalents, fet que és clau en la demostració del 3.3.2. Fixada una clausura algebraica $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}$, aquest argument també permet provar el resultat següent.

Proposició 3.3.5. *Existeix una única extensió del valor absolut de $K_{\mathfrak{p}}$ a un de $\overline{\mathbb{Q}}_p$.*

Corol·lari 3.3.6. *Sigui $\alpha \in \overline{\mathbb{Q}}_p$. Per a tota $K_{\mathfrak{p}}$-immersió σ de $K_{\mathfrak{p}}(\alpha)$ en $\overline{\mathbb{Q}}_p$, se satisfà que $|\sigma(\alpha)| = |\alpha|$. Conseqüentment, si $n = [K_{\mathfrak{p}}(\alpha) : K_{\mathfrak{p}}]$, aleshores $|\alpha| = |\mathrm{N}(\alpha)|^{1/n}$.*

El lema de Krasner dóna un criteri per establir quan dues extensions finites i del mateix grau coincideixen.

Teorema 3.3.7 (Lema de Krasner)**.** *Siguin $\alpha, \beta \in \overline{\mathbb{Q}}_p$ i suposem que per a tots els conjugats, $\sigma(\alpha) \neq \alpha$, de α sobre $K_{\mathfrak{p}}$ tenim que $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$. Aleshores, $K_{\mathfrak{p}}(\alpha) \subseteq K_{\mathfrak{p}}(\beta)$.*

Demostració. Només cal provar que si τ és una $K_{\mathfrak{p}}(\beta)$-immersió de $K_{\mathfrak{p}}(\beta, \alpha)$ en $\overline{\mathbb{Q}}_p$, ales-

hores $\tau(\alpha) = \alpha$. Per la unicitat de l'extensió de valors absoluts sobre cossos complets, se satisfà que $|\beta - \tau(\alpha)| = |\tau(\beta - \alpha)| = |\beta - \alpha|$ i, si σ és una $K_\mathfrak{p}$-immersió de $K_\mathfrak{p}(\alpha)$ en $\overline{\mathbb{Q}}_p$ diferent de la identitat, aleshores $|\beta - \tau(\alpha)| < |\sigma(\alpha) - \alpha|$. Per hipòtesi,

$$|\tau(\alpha) - \alpha| = |\tau(\alpha) - \beta + \beta - \alpha| \leq \max\{|\tau(\alpha) - \beta|, |\beta - \alpha|\} < |\sigma(\alpha) - \alpha|,$$

i ha de ser $\tau(\alpha) = \alpha$. □

Sigui $f(X) \in K_\mathfrak{p}[X]$ un polinomi mònic i siguin $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}_p$ les seves arrels, totes diferents. Sigui $g(X) \in K_\mathfrak{p}[X]$ un altre polinomi mònic de grau n. Denotem per $|g|$ el màxim dels valors absoluts dels coeficients de g. Tenim el resultat següent.

Lema 3.3.8. *Posem $g = X^n + b_{n-1}X^{n-1} \ldots b_1 X + b_0 \in K_\mathfrak{p}[X]$ i sigui $\beta \in \overline{\mathbb{Q}}_p$ una arrel de g. Aleshores, $|\beta| \leq |g|$.*

Suposem que f i g són propers, és a dir, que $|f - g| < \varepsilon < 1$, amb ε petit. En ser f mònic, aleshores $|f| \geq 1$ i $|g| = |f + (g - f)| < \max\{|f|, \varepsilon\} = |f|$. En virtut del lema, si β és una arrel de g, les potències $1, \beta, \ldots, \beta^{n-1}$ estan fitades per $|f|^{n-1}$, de manera que $|f(\beta)| = |f(\beta) - g(\beta)| < |f|^{n-1}\varepsilon$. És a dir, si f i g són propers, $|f(\beta)|$ és petit i, per la continuïtat de les arrels dels polinomis, β està a prop d'una arrel de f. Com que totes les arrels de f són diferents, la distància de β a les altres arrels de f està fitada inferiorment.

Ara, d'entre els polinomis g tals que $|f - g| < \varepsilon$, sempre n'hi ha de separables. En efecte, un polinomi g no és separable si, i només si, el polinomi resultant de g i el seu derivat g' és nul, i aquest resultant – que és un polinomi en els coeficients de g – no pot ser idènticament nul en un entorn obert de f perquè $K_\mathfrak{p}$ no és finit.

Això ens assegura que si f i g són dos polinomis prou propers i r és la multiplicitat de α com a arrel de f, aleshores hi ha exactament r arrels de g que s'apropen a α i mantenen distància afitada inferiorment amb les altres arrels de f. Si no fos així, podríem construir una successió de polinomis separables g_n de límit f i amb tantes arrels que s'apropen a α com les de g. Per pas al límit, arribaríem a una contradicció. Per tant, se satisfà el resultat següent.

Proposició 3.3.9. *Si f és un polinomi mònic i irreductible, aleshores qualsevol polinomi g mònic i del mateix grau prou proper a f també és irreductible. A més a més, per a tota arrel α de f, existeix una arrel β de g tal que $K_\mathfrak{p}(\alpha) = K_\mathfrak{p}(\beta)$.*

Corol·lari 3.3.10. *Sigui $K_\mathfrak{p}$ un cos extensió finita de $\mathbb{Q}_p$. Aleshores, existeix un cos de nombres K contingut en $K_\mathfrak{p}$, de grau $[K : \mathbb{Q}] = [K_\mathfrak{p} : \mathbb{Q}_p]$ i dens en $K_\mathfrak{p}$. De fet, $K_\mathfrak{p} = K\mathbb{Q}_p$.*

Demostració. Posem $K_\mathfrak{p} = \mathbb{Q}_p(\alpha)$, sigui f el polinomi irreductible de α sobre $\mathbb{Q}_p$ i sigui g un polinomi prou proper a f de coeficients racionals que satisfaci les condicions de la proposició anterior. Prenent $K = \mathbb{Q}(\beta)$, hem acabat. □

Observació 3.3.11. De fet, el cos $K_\mathfrak{p}$ és la compleció de K respecte d'un valor absolut $\mathfrak{p}$-àdic, amb $\mathfrak{p}$ un ideal primer no nul de l'anell dels enters de K que divideix l'ideal $p\mathbb{Z}$.

Del lema de Krasner i del fet que els anells de valoració de cossos $\mathfrak{p}$-àdics són compactes (observació 3.2.3), s'obté un resultat molt important.

Proposició 3.3.12. *Siguin $K_\mathfrak{p} \subset \overline{\mathbb{Q}}_p$ un cos $\mathfrak{p}$-àdic i $n > 1$ un enter. El conjunt de les extensions de $K_\mathfrak{p}$ de grau n incloses en $\overline{\mathbb{Q}}_p$ és finit.*

3.4 Lema de Hensel

Pel que fa a l'estudi de polinomis de coeficients en un cos $\mathfrak{p}$-àdic, el lema de Hensel és un resultat fonamental. Primer, donem una versió del lema de Hensel que ens permet trobar les arrels d'un polinomi en un cos $\mathfrak{p}$-àdic per mitjà d'un mètode iteratiu; de fet, és un anàleg del mètode de Newton. Acabem amb l'enunciat de la versió del lema de Hensel que ens permet factoritzar un polinomi en l'anell de valoració discreta a partir d'una factorització en el cos residual.

Lema 3.4.1 (Hensel)**.** *Siguin A un anell de valoració discreta, $\mathfrak{p}$ el seu ideal maximal, i suposem que el cos de fraccions K de A és complet respecte del valor absolut $\mathfrak{p}$-àdic. Sigui $f(X) \in A[X]$ i suposem que existeix un element $a_0 \in A$ tal que*

$$|f(a_0)| < |f'(a_0)^2|,$$

on f' és el polinomi derivat de f. Aleshores, existeix un element $a \in A$ tal que $f(a) = 0$.

La demostració d'aquest resultat es pot trobar en [3], i no és res més que l'anàleg del mètode de Newton per a valors absoluts $\mathfrak{p}$-àdics.

Corol·lari 3.4.2. *(i) Sigui $p \neq 2$ un nombre primer. Una unitat $a \in \mathbb{Z}_p^\times$ és un quadrat de $\mathbb{Z}_p^\times$ si, i només si, existeix un element $\alpha \in \mathbb{Z}_p^\times$ tal que $\alpha^2 \equiv a \pmod{p\mathbb{Z}_p}$.*

(ii) Una unitat $a \in \mathbb{Z}_2^\times$ és un quadrat de $\mathbb{Z}_2^\times$ si, i només si, $a \equiv 1 \pmod{8\mathbb{Z}_2}$.

Una altra versió del lema de Hensel, que podem trobar en [27], és la següent.

Teorema 3.4.3 (Lema de Hensel)**.** *Siguin A un anell de valoració discreta, $\mathfrak{p}$ el seu ideal maximal, i suposem que el cos de fraccions K de A és complet respecte del valor absolut $\mathfrak{p}$-àdic. Sigui $f(X) \in A[X]$ un polinomi primitiu i suposem que $\mathcal{G}(x)$ i $\mathcal{H}(x)$ són polinomis de $\kappa_\mathfrak{p}[X]$ primers entre si tals que la reducció mòdul $\mathfrak{p}$ de $f(X)$ és*

$$\overline{f}(X) = \mathcal{G}(X)\mathcal{H}(X).$$

Aleshores, existeixen polinomis $g(X), h(X) \in A[X]$ tals que

$$f(x) = g(x)h(x).$$

A més a més, $\overline{g}(X) = \mathcal{G}(x)$, $\overline{h}(X) = \mathcal{H}(X)$, i $\deg g(X) = \deg \mathcal{G}(X)$.

En aquest cas, els polinomis g i h s'obtenen com els límits de dues successions de polinomis que es construeixen inductivament a partir dels polinomis $\mathcal{G}$ i $\mathcal{H}$.

Corol·lari 3.4.4. *El cos $\mathbb{Q}_p$ només conté les arrels $(p-1)$-èsimes de la unitat, si $p \neq 2$; i les arrels quadrades de la unitat, 1, -1, si $p = 2$.*

3.5 Extensions no ramificades

Siguin $\overline{\mathbb{Q}}_p$ una clausura algebraica fixada de $\mathbb{Q}_p$, $K \subset \overline{\mathbb{Q}}_p$ un cos $\mathfrak{p}$-àdic i A el seu anell de valoració discreta. Ens disposem a estudiar les extensions de K que són no ramificades.

Recordem que si $L|K$ és una extensió finita i B és la clausura entera de A en L, aleshores B és un anell de valoració discreta, amb ideal maximal $\mathfrak{P}$ tal que $\mathfrak{P} \cap A = \mathfrak{p}$. Denotem per $\kappa_\mathfrak{p}$ i $\kappa_\mathfrak{P}$ els cossos residuals (finits) de K i L, respectivament, i siguin e i f l'índex de ramificació i el grau residual de l'extensió $L|K$, respectivament. La definició 2.3.5 també

serveix aquí, per tant, l'extensió és **no ramificada** si, i només si, $e = 1$. Per la igualtat (2.1), $[L : K] = ef$ i l'extensió és no ramificada si, i només si, $[L : K] = [\kappa_{\mathfrak{P}} : \kappa_{\mathfrak{p}}]$. Denotem amb una barra a sobre les reduccions dels elements dels anells en els cossos residuals.

Proposició 3.5.1. *L'extensió $L|K$ és no ramificada si, i només si, $L = K(\alpha)$, on α és una arrel d'un polinomi mònic $f(X) \in A[X]$ i $\overline{\alpha}$ és una arrel simple de $\overline{f}(X) \in \kappa_{\mathfrak{p}}[X]$. A més a més, $\kappa_{\mathfrak{P}} = \kappa_{\mathfrak{p}}(\overline{\alpha})$.*

Demostració. Suposem que l'extensió $L|K$ és no ramificada. Com que l'extensió residual és separable – és de cossos finits –, existeix un element $\alpha \in B$ tal que $\kappa_{\mathfrak{P}} = \kappa_{\mathfrak{p}}(\overline{\alpha})$. Sigui $f(X)$ el polinomi minimal de α sobre K, que és de coeficients en A per 2.1.5. Com que l'extensió és no ramificada,

$$\deg \operatorname{Irr}(\overline{\alpha}, \kappa_{\mathfrak{p}}) = [\kappa_{\mathfrak{P}} : \kappa_{\mathfrak{p}}] = [L : K] \geq \deg f = \deg \overline{f},$$

de manera que $\overline{f} = \operatorname{Irr}(\overline{\alpha}, \kappa_{\mathfrak{p}})$, i la desigualtat anterior es converteix en una igualtat, amb el que aconseguim la primera part.

Recíprocament, si α satisfà les condicions de l'enunciat, podem suposar sense pèrdua de generalitat que $f = \operatorname{Irr}(\alpha, K)$ i, llavors, $\overline{\alpha}$ és una arrel simple de $\overline{f}$. Ara, pel lema de Hensel (teorema 3.4.3), $\overline{f}$ és una potència d'un polinomi irreductible, però en ser $\overline{\alpha}$ una arrel simple de $\overline{f}$, aleshores $\overline{f}$ és irreductible. Per tant,

$$[L : K] = [K(\alpha) : K] = \deg f = \deg \overline{f} = [\kappa_{\mathfrak{p}}(\overline{\alpha}) : \kappa_{\mathfrak{p}}] \leq [\kappa_{\mathfrak{P}} : \kappa_{\mathfrak{p}}] \leq [L : K].$$

Així doncs, les desigualtats anteriors es converteixen en igualtats i $\kappa_{\mathfrak{p}}(\overline{\alpha}) = \kappa_{\mathfrak{P}}$. □

Proposició 3.5.2. *Sigui $K \subseteq K' \subseteq L$ una cadena d'extensions finites de cossos $\mathfrak{p}$-àdics.*

(i) $L|K$ és no ramificada si, i només si, $K'|K$ i $L|K'$ són no ramificades.

(ii) Si $L|K$ és no ramificada, aleshores $LK'|K'$ és no ramificada.

(iii) Si $L|K$ i $K'|K$ són no ramificades, aleshores $LK'|K$ també ho és.

Demostració. La primera propietat és conseqüència de la multiplicativitat dels índexs de ramificació per a cadenes d'extensions. De la proposició anterior es dedueix (ii), i (iii) és conseqüència de (i) i (ii). □

Teorema 3.5.3. *Siguin $L|K$ una extensió finita i $\kappa_{\mathfrak{P}}$ el cos residual de L. L'aplicació $L \longmapsto \kappa_{\mathfrak{P}}$ indueix una bijecció entre les extensions finites no ramificades de K i les extensions finites de $\kappa_{\mathfrak{p}}$.*

Demostració. La proposició 3.5.1 ens assegura que tota extensió finita de $\kappa_{\mathfrak{p}}$ s'obté com el cos residual $\kappa_{\mathfrak{P}}$ d'una extensió finita i no ramificada $L|K$. Provem-ne la unicitat. Siguin $L_1|K, L_2|K$ extensions no ramificades. Podem posar $L_i = K(\alpha_i)$, amb $i = 1, 2$, on α_i és tal que $f_i(X) = \operatorname{Irr}(\alpha_i, K)(X) \in A[X]$ i $\overline{\alpha}_i$ és una arrel simple de $\overline{f}_i$. Aleshores, $L = L_1L_2 = L_2(\alpha_1)$ i α_1 satisfà condicions similars respecte de L_2. Per 3.5.1, tenim que $\kappa_{\mathfrak{P}} = \kappa_{\mathfrak{P}_2}(\overline{\alpha}_1) = \kappa_{\mathfrak{p}}(\overline{\alpha}_1, \overline{\alpha}_2) = \kappa_{\mathfrak{P}_1}\kappa_{\mathfrak{P}_2}$. Si $\kappa_{\mathfrak{P}_1} = \kappa_{\mathfrak{P}_2}$, aleshores $\kappa_{\mathfrak{P}} = \kappa_{\mathfrak{P}_2}$ i, com que $L|L_2$ és no ramificada, ha de ser $[L : L_2] = [\kappa_{\mathfrak{P}} : \kappa_{\mathfrak{P}}] = 1$. Per tant, $L_2 = L$ i $\alpha_1 \in L_2$, de manera que $L_1 \subseteq L_2$. Anàlogament s'obté $L_2 \subseteq L_1$, i hem acabat. □

En ser $\kappa_{\mathfrak{p}}$ un cos finit, qualsevol extensió és cíclica. Si $\#\kappa_{\mathfrak{p}} = q$, el grup de Galois de l'extensió residual està generat per l'automorfisme de Frobenius $\sigma : x \mapsto x^q$. Tota extensió no ramificada $L|K$ és de Galois, ja que si α, α' són conjugats, aleshores $\kappa_{\mathfrak{p}}(\overline{\alpha}) = \kappa_p(\overline{\alpha}')$ i $K(\alpha) = K(\alpha')$; i també és cíclica ja que, en ser no ramificada, el grup d'inèrcia $I_{\mathfrak{P}|\mathfrak{p}}$ és el trivial (això es dedueix de 2.5.5) i, per 3.3.3 i 2.5.4, $\operatorname{Gal}(L|K) \simeq \operatorname{Gal}(\kappa_{\mathfrak{P}}|\kappa_{\mathfrak{p}}) = \langle\sigma\rangle$.

Corol·lari 3.5.4. *Sigui $q = \#\kappa_{\mathfrak{p}}$. Per a cada enter $f > 0$, existeix una única extensió $L|K$ no ramificada de grau f. Aquesta extensió és de la forma $L = K(\zeta)$, on ζ és una arrel $(q^f - 1)$-èsima primitiva de la unitat.*

Demostració. Per a cossos finits, existeix una única extensió de grau f i aquesta ve donada per una arrel $(q^f - 1)$-èsima primitiva de la unitat. Com que ζ satisfà les condicions de 3.5.1, hem acabat. □

3.6 Extensions totalment i moderadament ramificades

Seguint amb les notacions de l'apartat anterior, diem que l'extensió $L|K$ és **moderadament ramificada** si la característica residual p de $\kappa_{\mathfrak{p}}$ no divideix e. En cas contrari, diem que l'extensió és **salvatgement ramificada**. També diem que l'extensió $L|K$ és **totalment ramificada** si $[L : K] = e$.

Proposició 3.6.1. *Suposem que l'extensió $L|K$ és totalment ramificada de grau e i sigui Π un uniformitzant de B. Aleshores, $L = K(\Pi)$ i Π és una arrel d'un polinomi d'Eisenstein de grau e, és a dir, d'un polinomi de la forma*

$$X^e + a_{e-1}X^{e-1} + \cdots + a_1X + a_0,$$

on $a_i \equiv 0 \pmod{\mathfrak{p}}$, $\forall i \geq 1$ i $a_0 \not\equiv 0 \pmod{\mathfrak{p}^2}$. Recíprocament, tot polinomi d'Eisenstein és irreductible i qualsevol arrel seva genera una extensió totalment ramificada.

Demostració. Per 3.3.6, tots els conjugats de Π sobre K tenen el mateix valor absolut, de manera que, si $\mathrm{Irr}(\Pi, K)(X) = \sum_{i=0}^{m} a_iX^i \in A[X]$, aleshores $a_0 \in \mathfrak{p}$. Siguin $\Pi_1 = \Pi, \ldots, \Pi_m$, amb $m \leq e$ els conjugats de Π. Sabem que $\Pi_1 \ldots \Pi_m = (-1)^m a_0$ i $|\Pi|^m = |a_0|$. Si posem $\mathfrak{p} = \pi A$, existeix una unitat $u \in A^\times$ tal que $a_0 = u\pi^r$, amb $r > 0$. Atès que l'extensió $L|K$ és totalment ramificada de grau e, podem posar $\Pi^e = v\pi$, amb $v \in B^\times$. Així doncs, $|\Pi|^{er} = |a_0| = |\Pi|^m$ i $er = m$. Però, en ser $m \leq e$, aleshores $r = 1$ i $m = e$; amb el que tenim la primera part.

Recíprocament, pel criteri d'irreductibilitat d'Eisenstein, qualsevol polinomi d'Eisenstein és irreductible, i si β és arrel d'un polinomi d'Eisenstein de grau e i $\mathfrak{p} = \pi A$, llavors $|\beta|^e = |\pi|$. □

Proposició 3.6.2. *Si $L|K$ és una extensió totalment i moderadament ramificada de grau e, aleshores existeix un uniformitzant de B amb polinomi minimal $X^e - \pi$, on $\pi \in \mathfrak{p} - \mathfrak{p}^2$.*

Demostració. Sigui Π un uniformitzant de B, de manera que $L = K(\Pi)$. Si π_0 és un uniformitzant de A, aleshores $|\Pi|^e = |\pi_0|$; és a dir, existeix una unitat $u \in B^\times$ tal que $\Pi^e = u\pi_0$. Com que l'extensió és totalment ramificada, l'extensió de cossos residuals és de grau 1, de manera que podem trobar una unitat $u_0 \in A^\times$ tal que $u \equiv u_0 \pmod{\mathfrak{P}}$. Posem $\pi = \pi_0 u_0$. Aleshores, $\Pi^e = \pi + \pi x$, per a algun element $x \in \mathfrak{P}$. Així doncs, $|\Pi^e - \pi| < |\pi|$. Siguin $f(X) = X^e - \pi$, i $\alpha_1, \ldots, \alpha_e$ les seves arrels. Aleshores,

$$|f(\Pi)| = |\Pi - \alpha_1| \ldots |\Pi - \alpha_e|, \quad \text{i} \quad |\alpha_i| = |\Pi|, \ \forall i.$$

Si fos $|\Pi - \alpha_i| = |\Pi|$, $\forall i$, seria $|\Pi^e - \pi| = |\Pi|^e = |\pi|$, i tindríem una contradicció. Així doncs, podem suposar que $|\Pi - \alpha_1| < |\alpha_1|$. Ara bé,

$$|f'(\alpha_1)| = |\alpha_1|^{e-1} = |\alpha_1 - \alpha_2| \ldots |\alpha_1 - \alpha_e| \leq |\alpha_1|^{e-1}.$$

Per tant, ha de ser $|\alpha_1 - \alpha_i| = |\alpha_1|$, $\forall i > 1$, i en virtut del lema de Krasner, $K(\alpha_1) \subseteq K(\Pi)$. Com que el polinomi $f(X)$ és irreductible i de grau e, $K(\alpha_1) = K(\Pi) = L$. □

4 Ramificació superior

Aprofundim en la ramificació d'ideals primers en extensions de cossos de nombres. Comencem per l'estudi de l'ideal diferent, i introduïm els cossos de descomposició i d'inèrcia. A més a més, obtenim una resolució del grup de descomposició d'extensions de Galois de cossos de nombres. Per últim, donem una relació entre el diferent i els grups de ramificació superior per a cossos $\mathfrak{p}$-àdics. Els resultats, amb les seves demostracions, es poden trobar en [18], [23] o [25].

4.1 El diferent i el discriminant

Siguin $L|K$ una extensió finita de cossos de nombres (resp. de cossos $\mathfrak{p}$-àdics), A un localitzat de l'anell d'enters de K (resp. l'anell de valoració discreta de K), i B la clausura entera de A en L. Hem vist que el discriminant de l'extensió $B|A$ determina els ideals primers de A que ramifiquen. En aquest apartat introduïm un altre invariant que determina els ideals primers de B que ramifiquen sobre A.

Observació 4.1.1. Notem que en 2.4 estudiem el discriminant quan l'extensió $L|K$ és de cossos de nombres. Per a extensions de cossos $\mathfrak{p}$-àdics, la mateixa definició serveix i totes les propietats esmentades en 2.4 també se satisfan.

Definició 4.1.2. *El conjunt* $\mathcal{C}_{B|A} = \{b \in L : \mathrm{Tr}_{L|K}(bc) \in A, \quad \forall c \in B\}$ *s'anomena el* **codiferent** *de l'extensió* $B|A$.

És fàcil comprovar la inclusió $B \subseteq \mathcal{C}_{B|A}$, i la linealitat de la traça ens assegura que el codiferent és el més gran dels B-submòduls M de L tals que $\mathrm{Tr}_{L|K}(M) \subseteq A$.

Proposició 4.1.3. *El codiferent* $\mathcal{C}_{B|A}$ *és un ideal fraccionari de* B.

Definició 4.1.4. *El* **diferent** $\mathcal{D}_{B|A}$ *de l'extensió* $B|A$ *és l'ideal fraccionari invers del codiferent, és a dir,* $\mathcal{D}_{B|A} = \{b \in L : b\mathcal{C}_{B|A} \subseteq B\}$. *Quan no hi ha confusió de l'extensió d'anells que considerem, el denotem per* $\mathcal{D}_{L|K}$.

Notem que, com que $B \subseteq \mathcal{C}_{B|A}$, el diferent és un ideal enter no nul de B. També tenim que $\mathcal{C}_{B|A}\mathcal{D}_{B|A} = B$ i $\mathcal{D}_{B|A} = \prod_{i=1}^{r} \mathfrak{P}_i^{d_i}$, per a certs ideals primers $\mathfrak{P}_i$ de B, amb d_i, l'exponent diferencial de $\mathfrak{P}_i$, un enter no negatiu. A més a més, el diferent es comporta bé per localització i per cadendes d'extensions. Donem també una manera de calcular l'ideal diferent que ens serà útil quan l'extensió $L|K$ és de cossos $\mathfrak{p}$-àdics.

Proposició 4.1.5. *Sigui* $\alpha \in B$ *tal que* $L = K(\alpha)$ *i* $B = A[\alpha]$ *i sigui* $f(X) = \mathrm{Irr}(\alpha, K)(X)$. *Aleshores,* $\mathcal{D}_{B|A} = f'(\alpha)B$, *on* f' *és el polinomi derivat de* f.

Establim ara les relacions del diferent amb la ramificació i el discriminant. Siguin $\mathfrak{P} \subset B$ un ideal primer no nul de B, $\mathfrak{p} = \mathfrak{P} \cap A$ la seva contracció a A, i siguin $d_{\mathfrak{P}}$ l'exponent diferencial de $\mathfrak{P}$ i $e_{\mathfrak{P}|\mathfrak{p}}$ l'índex de ramificació de $\mathfrak{P}$ sobre $\mathfrak{p}$. Denotem també per $\kappa_{\mathfrak{p}}$ el cos residual $A/\mathfrak{p}$, i per $\kappa_{\mathfrak{P}}$ el cos residual $B/\mathfrak{P}$.

Proposició 4.1.6. *Un ideal primer* $\mathfrak{P}$ *de* B *ramifica en l'extensió* $B|A$ *si, i només si,* $\mathfrak{P}$ *divideix* $\mathcal{D}_{B|A}$. *A més, se satisfà que* $d_{\mathfrak{P}} \geq e_{\mathfrak{P}|\mathfrak{p}} - 1$ *i es té la igualtat si, i només si,* $e_{\mathfrak{P}|\mathfrak{p}}$ *no és divisible per la característica residual de* $\kappa_{\mathfrak{p}}$.

Proposició 4.1.7. $\Delta_{B|A} = \mathrm{N}_{L|K}(\mathcal{D}_{B|A})$.

En aquests dos últims resultats, la forma bilineal traça és clau a l'hora de fer la demos-

tració. Aquesta última proposició també ens condueix cap al resultat següent.

Corol·lari 4.1.8. *Siguin $K \subseteq K' \subseteq L$ una cadena d'extensions finites de cossos de nombres o cossos $\mathfrak{p}$-àdics, i A' i B les clausures enteres de A en K' i L, respectivament. Aleshores,*

$$\Delta_{B|A} = \Delta_{A'|A}^{[L:K']} \mathrm{N}_{K'|K}(\Delta_{B|A'}).$$

4.2 Cossos de descomposició i d'inèrcia

Deixant de banda el diferent, aprofundim en la ramificació d'ideals primers per mitjà dels grups de descomposició i d'inèrcia.

Seguint amb la notació de 4.1, suposem que l'extensió $L|K$ és de Galois, i sigui $G = \mathrm{Gal}(L|K)$ el seu grup de Galois. Siguin també $\mathfrak{P} \subset B$ un ideal primer no nul de B i $\mathfrak{p} = \mathfrak{P} \cap A$ la seva contracció a A. Hem definit el grup de descomposició de $\mathfrak{P}$ sobre $\mathfrak{p}$:

$$G_{-1}(\mathfrak{P}|\mathfrak{p}) = D_{\mathfrak{P}|\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

i també el seu grup d'inèrcia $G_0(\mathfrak{P}|\mathfrak{p}) = I_{\mathfrak{P}|\mathfrak{p}}$, de manera que la successió de grups següent és exacta:

$$1 \longrightarrow G_0(\mathfrak{P}|\mathfrak{p}) \longrightarrow G_{-1}(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(\kappa_{\mathfrak{P}}|\kappa_{\mathfrak{p}}) \longrightarrow 1.$$

Si $K' \subseteq L$ és un cos que conté K, A' és la clausura entera de A en K', i posem $\mathfrak{P}' = \mathfrak{P} \cap A'$; llavors, $G_i(\mathfrak{P}|\mathfrak{P}') = G_i(\mathfrak{P}|\mathfrak{p}) \cap \mathrm{Gal}(L|K')$, per a $i = 0, 1$.

Continuem estudiant l'extensió de Galois $L|K$ i sigui n el seu grau. Per alleugerir la notació, escrivim $D = D_{\mathfrak{P}|\mathfrak{p}}$ i $I = I_{\mathfrak{P}|\mathfrak{p}}$, i siguin e, f i g l'índex de ramificació de $\mathfrak{P}$ sobre $\mathfrak{p}$, el grau residual de $L|K$ en $\mathfrak{P}$ i el nombre d'ideals primers diferents de L que divideixen $\mathfrak{p}$, respectivament.

Com que D i I són subgrups del grup de Galois de $L|K$, podem considerar els respectius cossos fixos L^D i L^I. El cos L^D s'anomena el **cos de descomposició** en $\mathfrak{P}$ i el cos L^I, el **cos d'inèrcia** en $\mathfrak{P}$. Passem a estudiar les diferents subextensions de la cadena de cossos $K \subseteq L^D \subseteq L^I \subseteq L$.

En ser $L|K$ una extensió de Galois, les extensions $L|L^I$ i $L|L^D$ també ho són. A més, l'extensió $L^I|L^D$ també es de Galois ja que I és un subgrup normal D. Quant als graus de les extensions, en ser $efg = n$ i en virtut de 2.5.5, aleshores

$$[L^D : K] = |G : D| = g, \quad [L^I : L^D] = |D : I| = f, \quad [L : L^I] = e.$$

Siguin $\mathfrak{P}_I$ i $\mathfrak{P}_D$ les contraccions de $\mathfrak{P}$ en els cossos L^I i L^D, respectivament. Siguin també B_I i B_D les clausures enteres de A en aquests cossos, respectivament.

Proposició 4.2.1. *L'ideal $\mathfrak{P}$ és l'únic ideal primer de B que divideix $\mathfrak{P}_I$ i també és l'únic ideal primer de B que divideix $\mathfrak{P}_D$. A més a més,*

(i) $\mathfrak{P}_I B = \mathfrak{P}^e$ *i* $f_{\mathfrak{P}|\mathfrak{P}_I} = 1$, *i*

(ii) $\mathfrak{P}_D \mathfrak{P}_I = \mathfrak{P}_I$, $f_{\mathfrak{P}_I|\mathfrak{P}_D} = f$ *i* $\mathfrak{P}_D$ *no ramifica en* $B_I|B_D$.

D'aquesta proposició, on s'han de tenir en compte els grups de descomposició i d'inèrcia de les extensions $L|L^D$, $L|L^I$ i $L^I|L^D$, així com els grups de Galois de les respectives extensions residuals, es dedueix el corol·lari següent.

Corol·lari 4.2.2. *Sigui K un cos $\mathfrak{p}$-àdic. Per a tota extensió finita i de Galois $L|K$, el cos d'inèrcia és el subcòs maximal no ramificat.*

4.3 Grups de ramificació superior

L'objectiu d'aquest apartat és trobar una resolució del grup de descomposició d'extensions de Galois de cossos de nombres. Per fer-ho, introduïrem els grups de ramificació superior i n'enunciarem algunes propietats, que ens portaran al resultat desitjat. Seguim amb les notacions de l'apartat anterior.

Definició 4.3.1. *Per a $k \in \mathbb{Z}$, amb $k \geq -1$, es defineix el k-èsim grup de ramificació de $\mathfrak{P}$ sobre $\mathfrak{p}$ com el conjunt*

$$G_k(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G_{-1}(\mathfrak{P}|\mathfrak{p}) \mid \sigma(b) \equiv b \pmod{\mathfrak{P}^{k+1}}, \quad \forall b \in B\}.$$

Per tal d'alleugerir la notació, posem $G_k = G_k(\mathfrak{P}|\mathfrak{p})$. Els grups de descomposició i d'inèrcia es corresponen, tal i com els havíem definit, amb G_{-1} i G_0, respectivament.

El grup G_k, amb $k \geq 0$, és el nucli del morfisme de grups $G_{-1} \to \mathrm{Aut}_{\kappa_\mathfrak{p}}(B|\mathfrak{P}^{k+1})$, de manera que és un subgrup normal de G_{-1}. Com que, per a tot $k \geq -1$, G_{k+1} és un subgrup de G_k, llavors G_{k+1} és un subgrup normal de G_k i tenim la cadena

$$G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_k \supseteq G_{k+1} \supseteq \ldots$$

És un resultat conegut d'àlgebra commutativa que si B és un domini noetherià, aleshores $\bigcap_{k\geq 0} \mathfrak{P}^k = \{0\}$. Com que G_{-1} és un grup finit, la successió de subgrups ha de ser estacionària, és a dir, per a algun n_0 se satisfà que $G_{n_0} = G_k$, $\forall k \geq n_0$. Ara, $G_{n_0} = \bigcap_{k\geq -1} G_k$ i, per tant, $\sigma \in G_{n_0}$ si, i només si, $\sigma(b) - b \in \bigcap_{k\geq 0} \mathfrak{P}^k = \{0\}$, $\forall b \in B$. D'aquesta manera, $G_{n_0} = \{1\}$. Hem vist, doncs, que existeix una cadena finita de subgrups

$$G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_{n_0} = \{1\}$$

tal que, per a $-1 \leq k \leq n_0 - 1$, G_{k+1} és un subgrup normal de G_k. Per veure si aquesta cadena de subgrups conformen una resolució del grup de descomposició G_{-1}, s'ha de comprovar si els quocients G_k/G_{k+1} són abelians per a tot $-1 \leq k \leq n_0$.

Proposició 4.3.2. *(i) G_0/G_1 és isomorf a un subgrup del grup multiplicatiu $\kappa_\mathfrak{P}^*$.*

(ii) Si $k \geq 1$, el grup G_k/G_{k+1} és isomorf a un subgrup del grup additiu de $\kappa_\mathfrak{P}$.

En la demostració del resultat s'utilitza el bon comportament dels grups de ramificació i dels cossos residuals per localització en $\mathfrak{p}$ per tal de poder suposar que A és un anell local principal i que B és principal. Donat un generador $\pi \in B$ de l'ideal $\mathfrak{P}$ i $\sigma \in G_{-1}$, és fàcil adonar-se que $\sigma(\pi) = u_\sigma \pi$, per a un cert $u_\sigma \in B - \mathfrak{P}$. Llavors, es demostra que l'aplicació $G_0 \longrightarrow \kappa_\mathfrak{P}^*$ definida per $\sigma \mapsto \overline{u}_\sigma$ és un morfisme de grups que té G_1 per nucli. De manera similar, per a $k \geq 1$ i $\sigma \in G_k$, es pot posar $\sigma(\pi) - \pi = u_\sigma \pi^{k+1}$ per a un cert $u_\sigma \in B$. Llavors, es demostra que l'aplicació $G_k \longrightarrow (\kappa_\mathfrak{P}, +)$ definida per $\sigma \mapsto \overline{u}_\sigma$ és un morfisme de grups que té G_{k+1} per nucli.

Corol·lari 4.3.3. *El grup G_0/G_1 és cíclic i, si la característica de $\kappa_\mathfrak{P}$ és $p > 0$, aleshores:*

(i) El grup G_0/G_1 és d'ordre primer amb p.

(ii) Per a $k \geq 1$, els grups G_k/G_{k+1} són sumes directes de grups cíclics d'ordre p i el grup G_1 és un p-grup.

(iii) El grup G_1 és el trivial si, i només si, l'extensió és moderadament ramificada.

Corol·lari 4.3.4. *El grup d'inèrcia és resoluble. Si els cossos residuals són finits, aleshores el grup de descomposició és resoluble.*

D'aquest resultat i de 3.3.3 s'obté el corol·lari que enunciem a continuació.

Corol·lari 4.3.5. *Les extensions de Galois finites de cossos* $\mathfrak{p}$*-àdics són resolubles.*

4.4 Grups de ramificació superior i diferent

Siguin K un cos $\mathfrak{p}$-àdic, A el seu anell de valoració discreta, $\mathfrak{p}$ el seu ideal primer i $\kappa_{\mathfrak{p}}$ el seu cos residual. Si $L|K$ és una extensió finita, siguin B la clausura entera de A en L – que és un anell de valoració discreta complet per 3.3.2 –, $\mathfrak{P}$ l'ideal primer de B i $\kappa_{\mathfrak{P}}$ el seu cos residual.

Lema 4.4.1. *Existeix un element* $x \in B$ *tal que* $B = A[x]$*. Si l'extensió* $B|A$ *és totalment ramificada, qualsevol uniformitzant de* B *satisfà aquesta propietat.*

Aquest lema permet demostrar la proposició següent.

Proposició 4.4.2. *Si l'extensió* $L|K$ *és de Galois,* $\mathcal{D}_{L|K}$ *denota el diferent de l'extensió i* $v_{\mathfrak{P}}$ *denota la valoració* $\mathfrak{P}$*-àdica del cos* L*, se satisfà que*

$$v_{\mathfrak{P}}(\mathcal{D}_{L|K}) = \sum_{i=0}^{\infty}(\#G_i - 1). \tag{4.1}$$

Com a conseqüència de 3.6.1, 4.1.5, 4.1.7 i 4.4.1, obtenim com és el discriminant en un cas particular.

Proposició 4.4.3. *Si l'extensió* $L|K$ *està generada per una arrel d'un polinomi d'Eisenstein, aleshores el discriminant de l'extensió* $B|A$ *és justament l'ideal generat pel discriminant del polinomi.*

Part II : Resolució per radicals de quíntiques resolubles

5 Resolució per radicals de les quíntiques resolubles

Estudiem la resolubilitat per radicals dels polinomis irreductibles de grau 5. Comencem amb un resultat de Galois que ens permet caracteritzar els polinomis resolubles, i introduïm les bases de Gröbner, que són un element clau per trobar les fórmules de la resolució. Exposem la resolució (la primera resolució explícita publicada) que fa Dummit en [7] l'any 1991, i comentem breument les fórmules publicades per Faggal i Lazard en [9] l'any 2014.

5.1 Subgrups transitius resolubles del grup simètric S_5

Sigui p un nombre primer i considerem el grup simètric S_p, és a dir, el grup format per totes les permutacions del conjunt $C_p = \{0, 1, \dots, p-1\}$. Siguin $\sigma, \tau_i \in S_p$, amb $1 \leq i \leq p-1$, les permutacions definides per

$$\begin{aligned} \tau_i : \quad x &\mapsto ix \qquad (\mathrm{mod}\ p), \quad \forall x \in C_p, \\ \sigma : \quad x &\mapsto x+1 \qquad (\mathrm{mod}\ p), \quad \forall x \in C_p. \end{aligned}$$

Sigui $\mathrm{GA}(p) := \langle \sigma, \{\tau_i : 1 \leq i \leq p-1\} \rangle \subset S_p$ el subgrup generat per aquestes permutacions. És fàcil comprovar que, de fet,

$$\mathrm{GA}(p) = \{\sigma^j \circ \tau_i : 1 \leq i \leq p-1,\ 0 \leq j \leq p-1\}$$

i $\#\mathrm{GA}(p) = p(p-1)$. Així, el grup $\mathrm{GA}(p)$ està format per les permutacions de la forma $x \mapsto ax + b \pmod p$, amb $a \in \{1, \dots, p-1\}$, $b \in \{0, 1, \dots, p-1\}$.

Galois, en les seves memòries, demostra que aquest grup $\mathrm{GA}(p)$ és, essencialment, l'únic subgrup transitiu resoluble de S_p.

Teorema 5.1.1 (Galois)**.** *Tot subgrup transitiu de S_p és el conjugat d'un subgrup de $\mathrm{GA}(p)$. Recíprocament, tot subgrup de S_p que és el conjugat d'un subgrup de $\mathrm{GA}(p)$ és resoluble.*

Per tal de demostrar aquest resultat, necessitem dos lemes previs.

Lema 5.1.2. *Siguin G un subgrup transitiu de S_p i $N \neq \{\mathrm{Id}\}$ un subgrup normal de G. Aleshores, N també és transitiu.*

Demostració. Per la fórmula de les òrbites, tenim que

$$p = \#C_p = \sum_{x \in R} |N : N_x|,$$

on R designa un conjunt de representants de les òrbites i $|N : N_x|$ és l'índex del grup d'isotropia de x en N. Com que G és transitiu, donats $x, y \in C_p$, existeix una permutació $\sigma \in G$ tal que $\sigma(x) = y$. Ara, per la normalitat de N, $N(y) = \sigma \circ N \circ \sigma^{-1}(y) = \sigma \circ N(x)$ i σ indueix una bijecció entre $N(x)$ i $N(y)$. En particular, $\#N(x) = \#N(y)$ i $|N : N_x| = c$ per a tot $x \in R$. Així doncs, $p = c(\#R)$ i en ser p un nombre primer i $N \neq \{\mathrm{Id}\}$, ha de ser $\#R = 1$. És a dir, hi ha una única òrbita i el grup N és transitiu. □

Lema 5.1.3. *Sigui $\rho \in S_p$ tal que $\theta_\rho := \rho \circ \sigma \circ \rho^{-1} \in \mathrm{GA}(p)$. Aleshores, $\rho \in \mathrm{GA}(p)$.*

Demostració. Demostrem primer que θ_ρ és una potència de σ. Si no fos així, θ_ρ seria de la forma $\theta_\rho : x \mapsto ax + b \pmod p$, amb $a \not\equiv 0, 1 \pmod p$. Llavors,

$$\theta_\rho^{p-1} : x \mapsto a^{p-1}x + (a^{p-2} + \cdots + a + 1)b \pmod p$$

i, com que $a \not\equiv 0 \pmod p$, aleshores $a^{p-1} \equiv 1 \pmod p$. Ara,

$$(a-1)(a^{p-2} + \cdots + a + 1) = a^{p-1} - 1 \equiv 0 \pmod p$$

i, atès que $a \not\equiv 1 \pmod p$, ha de ser $a^{p-2} + \cdots + a + 1 \equiv 0 \pmod p$. Així doncs, $\theta_\rho^{p-1} = \mathrm{Id}$. Ara bé, $\theta_\rho^{p-1} = \rho \circ \sigma^{p-1} \circ \rho^{-1}$, de manera que $\sigma^{p-1} = \mathrm{Id}$, però $\#\langle\sigma\rangle = p$, amb el que obtenim una contradicció.

Per tant, $\theta_\rho = \sigma^i$ per a alguna $1 \leq i \leq p-1$. Això implica que $\rho \circ \sigma = \sigma^i \circ \rho$, o el que és el mateix, $\rho(x+1) = \rho(x) + i \pmod p$, $\forall x \in C_p$. D'aquí es dedueix que $\rho(x) = \rho(p+x) = ix + \rho(0) \pmod p$, $\forall x \in C_p$ i, per tant, $\rho = \sigma^{\rho(0)} \circ \tau_i \in \mathrm{GA}(p)$. □

Demostració (del teorema 5.1.1). Sigui G un subgrup transitiu resoluble de S_p. Sabem que existeix una cadena de subgrups

$$G = G_0 \supset G_1 \supset \cdots \supset G_t = \{1\}$$

tal que G_{i+1} és un subgrup normal de G_i i el grup quocient G_i/G_{i+1} és cíclic d'ordre primer. Com que G és transitiu, pel lema 5.1.2, els grups $G_1, \ldots, G_{t-1}$ també ho són. Per la fórmula de les òrbites, $p \mid \#G_{t-1}$, però $\#G_{t-1}$ és un nombre primer, de manera que $\#G_{t-1} = p$. Així doncs, G_{t-1} està generat per un p-cicle. Llevat de conjugacions, podem suposar que $G_{t-1} = \langle\sigma\rangle \subset \mathrm{GA}(p)$. Ara, G_{t-1} és un subgrup normal de G_{t-2}, és a dir, $\forall \rho \in G_{t-2}$, $\rho \circ \sigma \circ \rho^{-1} \in G_{t-1} \subset \mathrm{GA}(p)$ i, pel lema 5.1.3, $G_{t-2} \subset \mathrm{GA}(p)$. Recursivament, s'obté $G = G_0 \subseteq \mathrm{GA}(p)$, com volíem veure.

Recíprocament, n'hi ha prou amb demostrar que $\mathrm{GA}(p)$ és resoluble. Sigui g una arrel primitiva mòdul p. Per a $d \mid p-1$, definim

$$H_d := \{x \mapsto g^{di}x + c \pmod p : 0 \leq c \leq p-1,\ 0 \leq i \leq (p-1)/d - 1\} \subseteq \mathrm{GA}(p).$$

És fàcil comprovar que H_d és un subgrup normal de $\mathrm{GA}(p)$ i que $\#H_d = p(p-1)/d$. Si $d \mid d' \mid p-1$, aleshores $H_{d'} \subseteq H_d$ i $|H_d : H_{d'}| = d'/d$. Posem $p - 1 = q_1 \ldots q_r$, amb q_i nombres primers (que, potser, no són diferents) i sigui $d_0 := 1, d_1 := q_1, \ldots, d_{r-1} = q_1 \ldots q_{r-1}, d_r = p-1$. Aleshores la cadena

$$\mathrm{GA}(p) = H_{d_0} \supset H_{d_1} \supset \cdots \supset H_{d_r} \supset \{\mathrm{Id}\}$$

conforma una resolució del grup $\mathrm{GA}(p)$. □

Corol·lari 5.1.4. *Els subgrups transitius resolubles de S_5 són els conjugats a un d'aquests grups:*

(i) $\langle\sigma\rangle$*, que és un grup cíclic C_5 d'ordre 5.*

(ii) $\langle\sigma, \tau_2^2\rangle$*, isomorf al grup diedral $D_{2\cdot 5}$ d'ordre 10.*

(iii) $F_{20} := \mathrm{GA}(5) = \langle\sigma, \tau_2\rangle$*, que es diu que és un grup de Frobenius d'ordre 20.*

Demostració. Com que $\#F_{20} = 5 \cdot 4$, els seus subgrups transitius propis són d'ordre 5 o 10. L'únic grup d'ordre 5 és el cíclic i, per Sylow, els únics grups d'ordre 10 són el cíclic C_{10} i el diedral $D_{2\cdot 5}$. Com que S_5 no té 10-cicles, hem acabat. □

5.2 Bases de Gröbner

Una eina molt important per a la resolució de les quíntiques són les bases de Gröbner. Els resultats que esmentem, amb les seves demostracions, es poden trobar en [4]. A més a més, exposem també els resultats que utilitza Lazard en [16] per tal de donar una resolució de les quíntiques resolubles.

Sigui k un cos i sigui $k[x_1, \ldots, x_n]$ l'anell de polinomis de coeficients en k i n indeterminades. Podem identificar el conjunt format pels monomis de $k[x_1, \ldots, x_n]$ amb $\mathbb{Z}^n_{\geq 0}$ de la manera següent: a cada monomi $x^\alpha = x_1^{m_1} \ldots x_n^{m_n}$ li fem correspondre la n-tupla $\alpha = (m_1, \ldots, m_n) \in \mathbb{Z}^n_{\geq 0}$.

Definició 5.2.1. *Un* **ordre monomial** *en l'anell $k[x_1, \ldots, x_n]$ és una relació $>$ en $\mathbb{Z}^n_{\geq 0}$ tal que:*

(i) $>$ és un ordre total.

(ii) Si $\alpha > \beta$ i $\gamma \in \mathbb{Z}^n_{\geq 0}$, aleshores $\alpha + \gamma > \beta + \gamma$.

(iii) Tot subconjunt no buit de $\mathbb{Z}^n_{\geq 0}$ té un element mínim sota l'ordre $>$.

Estenem aquest ordre a $k[x_1, \ldots, x_n]$: donats dos polinomis no nuls $f = \sum_i a_i x^{\alpha_i}$, $g = \sum_j a_j x^{\beta_j} \in k[x_1, \ldots, x_n]$, ordenem els seus termes de manera que $x^{\alpha_1} > x^{\alpha_2} > \ldots$ i $x^{\beta_1} > x^{\beta_2} > \ldots$ Diem que $f > g$ quan $x^{\alpha_r} > x^{\beta_r}$, on r és el primer índex tal que els monomis x^{α_r} i x^{β_r} són d'ordre diferent.

Definició 5.2.2. *Siguin $f = \sum_\alpha a_\alpha x^\alpha$ un polinomi no nul de $k[x_1, \ldots, x_n]$ i $>$ un ordre monomial. Definim el multigrau i el terme líder de f, respectivament, per*

$$\text{multideg}(f) := \max\{\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0\}, \quad \text{LT}(f) := a_{\text{multideg}(f)} x^{\text{multideg}(f)}.$$

Teorema 5.2.3 (Algoritme de Divisió)**.** *Fixat un ordre monomial $>$ en $\mathbb{Z}^n_{\geq 0}$ i donada $F = (f_1, \ldots, f_s)$ una s-tupla de polinomis de $k[x_1, \ldots, x_n]$, aleshores tot polinomi $f \in k[x_1, \ldots, x_n]$ es pot escriure com*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

on $a_i, r \in k[x_1, \ldots, x_n]$ i, o bé $r = 0$, o bé r és una k-combinació lineal de monomis, cap dels quals és divisible per $\text{LT}(f_1), \ldots, \text{LT}(f_s)$. Anomenem r el **residu** *de la divisió de f per F. A més a més, si $a_i f_i \neq 0$, aleshores $\text{multideg}(f) \geq \text{multideg}(a_i f_i)$.*

Observació 5.2.4. La demostració és constructiva. A més, el residu depèn de l'ordre dels polinomis $f_1, \ldots, f_s$ en què fem la divisió.

Definició 5.2.5. *Un conjunt finit $G = \{g_1, \ldots, g_t\}$ generador d'un ideal I de $k[x_1, \ldots, x_n]$ és una* **base de Gröbner** *si $\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle = \langle \text{LT}(I) \rangle$.*

Proposició 5.2.6. *Sigui $G = \{g_1, \ldots, g_t\}$ una base de Gröbner de $I \subset k[x_1, \ldots, x_n]$ i sigui $f \in k[x_1, \ldots, x_n]$. Aleshores existeix un únic polinomi $r \in k[x_1, \ldots, x_n]$ tal que*

(i) cap terme de r és divisible per cap dels monomis $\text{LT}(g_1), \ldots, \text{LT}(g_t)$; i

(ii) existeix un polinomi $g \in I$ tal que $f = g + r$.

En particular, r és el residu de la divisió de f per G, sense importar l'ordre dels elements de G en l'algoritme de divisió. Aquest residu r s'anomena la **forma normal** *de f per G i el denotem per $\overline{f}^G$.*

Corol·lari 5.2.7. *Si G és una base de Gröbner de I, llavors $f \in I$ si, i només si, $\overline{f}^G = 0$.*

Definició 5.2.8. *Una base de Gröbner G d'un ideal I es diu que és* **reduïda** *si el coeficient del terme líder de tot polinomi de G és 1 i, si per a qualsevol $f \in G$, cap monomi de f és de l'ideal generat pels termes líders de $G - \{f\}$.*

Donat un subgrup G del grup simètric S_n, el podem fer actuar en el conjunt de les indeterminades $\{x_1, \ldots, x_n\}$. Es diu que un polinomi $f \in k[x_1, \ldots, x_n]$ és invariant per G si $\sigma(f) = f$, per a qualsevol permutació $\sigma \in G$.

Teorema 5.2.9. *Per a tot subgrup G de S_n, l'anell $k[x_1, \ldots, x_n]^G$ dels polinomis invariants per G és un $k[x_1, \ldots, x_n]^{S_n}$-mòdul lliure que té per base polinomis homogenis invariants de grau com a molt $n(n-1)/2$.*

Reproduïm la demostració que en dóna Lazard en [16], ja que ens serà útil per a resoldre les quíntiques resolubles. Considerem els polinomis simètrics elementals s_i, i siguin $e_1, \ldots, e_d$ noves indeterminades, que faran el paper de 'noms' per a les s_i. Sigui I l'ideal de $k[x_1, \ldots, x_n, e_1, \ldots, e_n]$ generat per $s_i - e_i$. Primer, en calculem una base de Gröbner per a qualsevol ordre monomial de les indeterminades x_i tal que

(i) $x_1 < x_2 < \cdots < x_n$,

(ii) $m_1 < m_2$ per a qualsevol parella de monomis tals que els seus graus totals en les x_i satisfan la mateixa desigualtat.

Lema 5.2.10. *Per a un ordre monomial satisfent aquestes propietats,*

$$\begin{aligned} J = \; & \{x_1^n - e_1 x_1^{n-1} + \cdots + (-1)^{n-1} e_{n-1} x_1 + (-1)^d e_n, \\ & C_{n-1}^{(2)} - e_1 C_{n-2}^{(2)} + \cdots + (-1)^{n-2} e_{n-2} C_1^{(2)} + (-1)^{n-1} e_{n-1}, \\ & \ldots, \\ & C_2^{(n-1)} - e_1 C_1^{(n-1)} + e_2, \\ & C_1^{(n)} - e_1 = s_1 - e_1\}, \end{aligned}$$

on $C_k^{(i)}$ és la suma de tots els monomis de grau k en $x_1, \ldots, x_i$, és una base de Gröbner reduïda de l'ideal I.

La demostració d'aquest lema utilitza conceptes bàsics de bases de Gröbner i de geometria algebraica que podem trobar en [4].

Lema 5.2.11 (Lazard)**.** *Sigui $G \subseteq S_n$ un subgrup del grup simètric S_n. Aleshores, el $k[e_1, \ldots, e_n]$-mòdul dels polinomis en les x_i invariants per G està generat pels seus elements tals que el monomi líder de la seva forma normal per J és independent de les e_i.*

Demostració. Per tal de demostrar això, demanem que l'ordre ordeni primer els monomis del mateix grau total en les x_i d'acord amb les e_i.

Sigui $f \in k[x_1, \ldots, x_n, e_1, \ldots, e_n]$ un polinomi invariant per G i sigui $g = \overline{f}^J$ la seva forma normal després de reduir-lo per J. Sigui E el monomi en les e_i que apareix en el terme líder $\mathrm{LT}(g)$ de g, i sigui h el polinomi homogeni en les x_i tal que hE és la part de g que consisteix en tots els monomis que són el producte de E per un monomi en les x_i, del mateix grau que $\mathrm{LT}(g)$. L'elecció que hem fet de l'ordenació fa que els monomis de g que no es troben en hE són més petits que qualsevol monomi de hE, és a dir, hE és la part líder de g.

Veiem que la forma normal per J de $\sum_{\sigma \in G} \sigma(g)$ és $(\#G)g$. En efecte, si J_i són els polinomis de J, podem posar $f = \sum_i h_i J_i + g$, per a certs polinomis h_i. En ser $\sigma(f) = f$,

aleshores $g - \sigma(g) = \sum_i h_i J_i - \sum_i \sigma(h_i)\sigma(J_i)$. Quan substituïm les e_i per s_i, és fàcil veure que $J_i = \sigma(J_i) = 0$ i, per tant, $g - \sigma(g) = 0$. Com que el lloc de zeros de I és $V(I) = \{(x_1, \ldots, x_n, e_1, \ldots, e_n) \in k^{2n} : e_i = s_i\}$, aleshores $V(I) \subset V(g - \sigma(g))$ de manera que $g - \sigma(g) \in IV(I) = I$, ja que I és un ideal primer de $k[x_1, \ldots, x_n, e_1, \ldots, e_n]$. Així doncs, $\overline{g - \sigma(g)}^J = 0$ i $\overline{\sum_{\sigma\in G} \sigma(g)}^J = (\#G)g$.

El polinomi $H := \sum_{\sigma\in G} \sigma(h)$ és invariant per G. Atès que $g = hE + g'$, on tot monomi de g' és estrictament estrictament més petit que qualsevol monomi de hE, podem posar

$$\sum_{\sigma\in G} \sigma(g) = EH + \sum_{\sigma\in G} \sigma(g')$$

i, reduint per J, obtenim que la part líder de H és $(\#G)h$.

Així doncs, $f - EH/(\#G)$ (que també és invariant per G) redueix per J a un polinomi amb un terme líder més petit que g. Iterant aquest procés, anem obtenim polinomis $H = H_0, H_1, \ldots, H_{r-1}$ invariants per G i satisfent la condició de l'enunciat, de manera que

$$f = \frac{E}{\#G}H + \frac{E_1}{\#G}H_1 + \cdots + \frac{E_{r-1}}{\#G}H_{r-1} + f_r,$$

on f_r és un polinomi tal que el monomi líder de la seva forma normal per J és independent de les e_i. □

Demostració (del teorema 5.2.9). Com que els termes líders de J són $\{x_1^n, x_2^{n-1}, \ldots, x_n\}$, qualsevol polinomi irreductible per J – és a dir, tal que la seva forma normal per J és ell mateix – és de grau, com a molt, $n(n-1)/2$ en les x_i, de manera que els polinomis H del lema anterior també, perquè els polinomis h són irreductibles per J. Així doncs, per provar el resultat només cal extreure una $k[e_1, \ldots, e_d]$-base del conjunt dels polinomis H i substituir les e_i per les s_i.

Per a cada monomi m de grau com a molt $n(n-1)/2$ en les x_i, sigui $M := \sum_{\sigma\in G} \sigma(m)$ i R el resultat de reduir M per J. Si el terme líder de R és independent de les e_i i és diferent dels termes líders d'un R anterior, afegim M a la base.

És fàcil comprovar que el conjunt format per aquests polinomis M genera i, mirant els termes líders, es comprova immediatament que són linealment independents. □

Aquesta demostració indueix un algoritme per calcular una base d'invariants de G i per expressar qualsevol invariant en aquesta base. Per trobar la base, es calculen els polinomis $M := \sum_{\sigma\in G} \sigma(m)$ per a cada monomi $m \in k[x_1, \ldots, x_n]$ de grau com a molt $n(n-1)/2$ en les x_i. En la prova del teorema hem vist com saber si el polinomi M apareix en una base. Quan s'han considerat prou d'aquests polinomis amb terme líder linealment independents, s'obté una base.

Per expressar qualsevol invariant $f \in k[x_1, \ldots, x_n]^G$, es calcula la seva forma normal per J. Aleshores, el seu terme líder serà un múltiple d'un terme líder d'un invariant F_1 de la base. Definim una nova indeterminada f_1. Podem posar $\overline{f}^J = c_1\overline{F_1}^J + g$, amb $c_1 \in k$, per a algun polinomi g de grau estrictament més petit que $\overline{f}^J$, o el que és el mateix, $\overline{f}^J = c_1(\overline{F_1}^J - f_1) + c_1 f_1 + g$. Per a una base d'invariants $F_1, \ldots, F_r$, si apliquem aquest procés reiteradament i substituïm les indeterminades f_i per F_i, i les e_i per s_i, obtenim

$$f = c_1F_1 + \ldots c_rF_r.$$

Tot i que no hi entrarem, per tal de calcular la base, no cal considerar molts monomis. Existeix el que s'anomena la sèrie de Molien d'un anell d'invariants que dóna immedi-

atament el nombre d'invariants d'un grau donat en una base. Aquesta sèrie és de la forma $P(t)/\prod_{i=1}^{n}(1-t^i)$, on $P(t)$ és un polinomi en t. El coeficient t^i de P és el nombre d'elements de la base de grau i, i hi ha mètodes que permeten calcular aquest polinomi.

En [16], Lazard veu que el $k[s_1,\ldots,s_5]$-mòdul $k[x_1,\ldots,x_5]^{F_{20}}$ té una base formada per 1 i les sumes, per a ρ recorrent F_{20}, dels monomis $\rho(x_1^2x_2x_5)$, $\rho(x_1^3x_2x_5)$, $\rho(x_1^4x_2x_5)$, $\rho(x_1^3x_2^2x_5^2)$, $\rho(x_1^4x_2^2x_5^2)$. Aleshores, tot polinomi invariant per F_{20} es pot expressar com a $k[s_1,\ldots,s_5]$-combinació lineal d'aquests.

5.3 Dummit (1991)

L'any 1991 Dummit publica en [7] un criteri per a la resolubilitat d'una quíntica d'acord amb si existeix una arrel racional d'un resolvent de grau 6 associat a la quíntica i, quan això és així, dóna una fórmula per a les arrels i en determina el grup de Galois. Dummit treballa sobre el cos $\mathbb{Q}$ dels nombres racionals dins de $\mathbb{C}$, però els resultats que obté són vàlids sobre qualsevol cos de característica diferent de 2 i 5.

Siguin x_1,x_2,x_3,x_4,x_5 les arrels del polinomi general de grau 5, $X^5-s_1X^4+s_2X^3-s_3X^2+s_4X-s_5$, on les s_i són els polinomis simètrics elementals en les x_i. Veiem S_5 com el grup de les permutacions de $\{x_1,x_2,x_3,x_4,x_5\}$, de manera que ens serà útil pensar en les permutacions de $\{1,2,3,4,5\}$. Sigui F_{20} el grup de Frobenius d'ordre 20 generat per $\sigma=(1\,2\,3\,4\,5)$ i $\tau=(2\,3\,5\,4)$. Aleshores, F_{20} és l'estabilitzador en S_5 de l'element

$$\begin{aligned}\theta=\theta_1=\ & x_1^2x_2x_5+x_1^2x_3x_4+x_2^2x_1x_3+x_2^2x_4x_5+x_3^2x_1x_5+x_3^2x_2x_4+x_4^2x_1x_2\\ & +x_4^2x_3x_5+x_5^2x_1x_4+x_5^2x_2x_3.\end{aligned}$$

D'aquesta manera, θ_1 satisfà un polinomi de grau 6 sobre $\mathbb{Q}(s_1,s_2,s_3,s_4,s_5)$, amb conjugats $\theta_2=(1\,2\,3\,)\theta_1$, $\theta_3=(1\,3\,2)\theta_1$, $\theta_4=(1\,2)\theta_1$, $\theta_5=(2\,3)\theta_1$ i $\theta_6=(1\,3)\theta_1$.

Mitjançant el mètode de Waring, podem expressar els polinomis simètrics elementals en les θ_i, que són polinomis simètrics en x_1,x_2,x_3,x_4,x_5, en funció de s_1,s_2,s_3,s_4,s_5, per obtenir el polinomi resolvent f_{20} de grau 6 que té θ per arrel. A més a més, per mitjà d'una translació, sempre podem suposar que $s_1=0$, és a dir, que el polinomi quíntic que estudiem és $f(X)=X^5+pX^3+qX^2+rX+s$, cosa que simplifica molt els càlculs. Aquest polinomi f_{20} es pot trobar en [7] i ocupa un espai considerable, però es pot programar fàcilment per obtenir-lo en tots els casos particulars que calcularem.

Teorema 5.3.1 (Dummit)**.** *Un polinomi irreductible $f(X)=X^5+pX^3+qX^2+rX+s\in\mathbb{Q}[X]$ és resoluble per radicals si, i només si, $f_{20}(X)$ té una arrel racional. Si això és així, $f_{20}(X)$ factoritza en el producte d'un polinomi lineal i d'un irreductible de grau 5.*

Demostració. En virtut del corol·lari 5.1.4, el polinomi $f(X)$ és resoluble per radicals si, i només si, el seu grup de Galois G està contingut en F_{20} o en un dels seus conjugats, és a dir, en els estabilitzadors de $\theta_1,\ldots,\theta_6$. Ara, $\theta_1\in\mathbb{Q}$ si, inomés si, $\mathbb{Q}=L^{F_{20}\cap G}$ i això passa només quan $G\subseteq F_{20}$. Demostrem ara la segona part de l'enunciat.

Sense pèrdua de generalitat, podem suposar que $\theta=\theta_1$ és racional, de manera que $G\subseteq F_{20}$. Com que $f(X)$ és irreductible, G ha de ser un subgrup transitiu del grup simètric S_5 i $5\mid \#G$. En ser $\langle\sigma\rangle$ un subgrup normal de F_{20}, $\langle\sigma\rangle$ és l'únic subgrup d'ordre 5 de F_{20} i, per tant, $\langle\sigma\rangle\subseteq G$. Com que aquest σ és transitiu en $\theta_2,\ldots,\theta_6$, o bé aquests θ_i són les arrels d'un polinomi de grau 5 irreductible sobre $\mathbb{Q}$, o bé $\theta_2=\cdots=\theta_6$. És senzill demostrar que això últim només pot passar quan una de les arrels x_i és racional. □

Ara ens disposem a resoldre per radicals les arrels de f quan és resoluble, és a dir, resoldre les arrels $x_1, \ldots, x_5$ per radicals sobre el cos $\mathbb{Q}(s_1, \ldots, s_5, \theta)$. Suposem que l'arrel racional de f_{20} és $\theta = \theta_1$, de manera que el grup de Galois G de f està contingut en $F_{20} = \langle \sigma, \tau \rangle$. Així, tenim determinades les arrels x_i llevat de permutacions de F_{20}.

Tornem a suposar que f és el polinomi general de grau 5. Fixem ζ una arrel cinquena primitiva de la unitat, i definim $k := \mathbb{Q}(s_1, \ldots, s_5)$, $K := k(\theta)$, $F := \mathbb{Q}(x_1, \ldots, x_5)$, de manera que $F(\zeta)|K$ és una extensió de Galois amb grup de Galois $F_{20} \times (\mathbb{Z}/5\mathbb{Z})^*$. Estenem σ, τ a automorfismes de F (deixen $K(\zeta)$ fix) i definim $\omega : \zeta \mapsto \zeta^3$ (deixa F fix). Sigui $\Delta = \prod_{i<j}(x_i - x_j)$ una arrel quadrada fixada del discriminat D de f.

Lema 5.3.2. *Si $f(X) \in \mathbb{Q}[X]$ és un polinomi irreductible i resoluble de grau 5, aleshores $D > 0$.*

Demostració. Si el grup de Galois G de f és el diedral o el cíclic, D és un quadrat. Si el grup de Galois és el grup de Frobenius F_{20}, tenint en compte que tots els seus elements són de la forma $x \mapsto ax + b$, amb $a \in \mathbb{F}_p^*$ i $b \in \mathbb{F}_p$ és fàcil comprovar que $\langle \sigma, \tau^2 \rangle$ és el seu únic subgrup d'índex 2. Si F és el cos de descomposició del polinomi, tenim la cadena de cossos $\mathbb{Q} \subset \mathbb{Q}(\sqrt{D}) = F^{\langle \sigma, \tau^2 \rangle} \subset F^{\langle \sigma \rangle}$, i $\langle \sigma \rangle$ és un subgrup normal de F_{20}, de manera $\mathbb{Q}(\sqrt{D})$ és un subcòs d'una extensió cíclica de grau 4. Sabem que $F^{\langle \sigma \rangle} = \mathbb{Q}(\sqrt{D}, \sqrt{a + b\sqrt{D}}) = \mathbb{Q}(\sqrt{a + b\sqrt{D}})$, per a certs $a, b \in \mathbb{Q}$. Com que l'extensió $F^{\langle \sigma \rangle}|\mathbb{Q}$ és de Galois, aleshores $\sqrt{a - b\sqrt{D}} \in \mathbb{Q}(\sqrt{a + b\sqrt{D}})$ i, en ser cíclica de grau 4, és senzill comprovar que $\sqrt{D}\sqrt{a + b\sqrt{D}}\sqrt{a - b\sqrt{D}} \in \mathbb{Q}$, és a dir, $D(a^2 - b^2 D) = x^2$ per a algun $x \in \mathbb{Q}$. Així doncs, $D = (x/a)^2 + (bD/a)^2 > 0$. □

Recordem que estem suposant que les arrels del polinomi general satisfan la igualtat $x_1 + x_2 + x_3 + x_4 + x_5 = 0$. Definim els resolvents de Langrange:

$$\begin{aligned} r_1 &= x_1 + x_2\zeta + x_3\zeta^2 + x_4\zeta^3 + x_5\zeta^4, \\ r_2 &= x_1 + x_2\zeta^2 + x_3\zeta^4 + x_4\zeta + x_5\zeta^3, \\ r_3 &= x_1 + x_2\zeta^3 + x_3\zeta + x_4\zeta^4 + x_5\zeta^2, \\ r_4 &= x_1 + x_2\zeta^4 + x_3\zeta^3 + x_4\zeta^2 + x_5\zeta; \end{aligned}$$

de manera que

$$\begin{aligned} x_1 &= (r_1 + r_2 + r_3 + r_4)/5, \\ x_2 &= (\zeta^4 r_1 + \zeta^3 r_2 + \zeta^2 r_3 + \zeta r_4)/5, \\ x_3 &= (\zeta^3 r_1 + \zeta r_2 + \zeta^4 r_3 + \zeta^2 r_4)/5, \\ x_4 &= (\zeta^2 r_1 + \zeta^4 r_2 + \zeta r_3 + \zeta^3 r_4)/5, \\ x_5 &= (\zeta r_1 + \zeta^2 r_2 + \zeta^3 r_3 + \zeta^4 r_4)/5. \end{aligned} \tag{5.1}$$

Escrivim

$$(x_1, z) = x_1 + x_2 z + x_3 z^2 + x_4 z^3 + z_5 x^4,$$

on z és una indeterminada. Desenvolupant $(x_1, z)^5$, obtenim que

$$R_1 = r_1^5 = l_0 + l_1\zeta + l_2\zeta^2 + l_3\zeta^3 + l_4\zeta^4,$$

on $l_i \in F$ és, per definició, la suma dels termes de $(x_1, z)^5$ que contenen potències z^k de z amb $k \equiv i \pmod 5$. Les expressions explícites d'aquests l_i es poden trobar en [7]. En ser

$l_0 + l_1 + l_2 + l_3 + l_4 = s_1^5$, tenim que $l_0 = -(l_1 + l_2 + l_3 + l_4)$. De la mateixa manera,

$$\begin{aligned} R_2 &= r_2^5 = l_0 + l_3\zeta + l_1\zeta^2 + l_4\zeta^3 + l_2\zeta^4, \\ R_3 &= r_3^5 = l_0 + l_2\zeta + l_4\zeta^2 + l_1\zeta^3 + l_3\zeta^4, \\ R_4 &= r_4^5 = l_0 + l_4\zeta + l_3\zeta^2 + l_2\zeta^3 + l_1\zeta^4. \end{aligned}$$

Veiem com actua el grup de Galois G sobre tots aquests elements. Notem que, si definim els índexs mòdul 5, aleshores $\sigma(r_i) = \zeta^{-i} r_i$, i $\tau(r_i) = \omega(r_i) = r_{3i}$. D'aquí es dedueix que l_0, l_1, l_2, l_3, l_4 són fixos per σ i, a més,

$$\tau(l_0) = l_0, \quad \tau(l_1) = l_2, \quad \tau(l_2) = l_4, \quad \tau(l_3) = l_1, \quad \tau(l_4) = l_3.$$

Així doncs, $l_0 \in K$ i, en ser $l_i \neq l_j$, si $i \neq j$, llavors l_1, l_2, l_3, l_4 són les arrels d'un polinomi de grau 4 sobre K i el cos $L = K(l_1)$ és una extensió cíclica de grau 4 sobre K, amb grup de Galois generat per la restricció de τ. En efecte, tenim $K \subseteq L \subseteq K(l_1, l_2, l_3, l_4) \subseteq F^{\langle\sigma\rangle}$ i $[F^{\langle\sigma\rangle} : K] = [L : K] = 4$. L'únic subcòs quadràtic de L sobre K (corresponent a l'únic subgrup d'índex 2 de F_{20}) és $K(\Delta)$, de manera que tenim la cadena de cossos

$$\begin{array}{ccccccccc} k & \subset & K = F^{\langle\sigma,\tau\rangle} & \subset & K(\Delta) = F^{\langle\sigma,\tau^2\rangle} & \subset & L = F^{\langle\sigma\rangle} & \subset & F. \\ & 6 & & 2 & & 2 & & 5 & \end{array}$$

Atès que el grup de Galois de $L|K$ és cíclic d'ordre 4, l_1, l_2, l_3, l_4 són les arrels d'un polinomi de grau 4 sobre K, que factoritza sobre $K(\Delta)$ com el producte de dos polinomis quadràtics conjugats:

$$\left(X^2 + (T_1 + T_2\Delta)X + (T_3 + T_4\Delta)\right)\left(X^2 + (T_1 - T_2\Delta)X + (T_3 - T_4\Delta)\right), \tag{5.2}$$

amb $T_i \in K$. Les arrels d'aquests polinomis quadràtics són $\{l_1, l_4 = \tau^2(l_1)\}$ i $\{l_2 = \tau(l_1), l_3 = \tau^3(l_1)\}$. Fixem ara l'ordre d'aquests polinomis quadràtics per determinar els coeficients T_i explícitament. Suposem, doncs, que les arrels del primer factor de (5.2) són $\{l_1, l_4\}$. Aleshores,

$$l_1 + l_4 = -T_1 - T_2\Delta, \quad l_2 + l_3 = -T_1 + T_2\Delta, \quad l_1 l_4 = T_3 + T_4\Delta, \quad l_2 l_3 = T_3 - T_4\Delta.$$

Per tal de trobar les expressions dels T_i en funció de θ, Dummit utilitza mètodes d'aproximació numèrica p-àdica. Seguint la idea de Lazard, però, es poden calcular aquests T_i utilitzant bases de Gröbner i sense haver de fer cap aproximació. En efecte, ja hem vist que Lazard dóna una base d'invariants de $\langle\sigma, \tau\rangle$ i, a més, també expressa $\theta, \ldots, \theta^5$ en funció d'aquesta base. Com que $L^{F_{20}} = K$, resolent el sistema que obté, pot expressar els elements de la base en funció de θ. Tenim que

$$T_1 = l_0/2, \quad T_2 = (l_2 + l_3 - l_1 - l_4)\Delta/(2D), \quad T_3 = l_1 l_4 + l_2 l_3, \quad T_4 = (l_1 l_4 - l_2 l_3)\Delta/(2D)$$

i el mètode de Lazard permet obtenir els numeradors d'aquestes expressions com polinomis de coeficients en el cos $\mathbb{Q}(s_1, s_2, s_3, s_4)$ i amb indeterminada θ. En [8], es poden trobar totes aquestes expressions.

Una vegada calculats els T_i en funció de θ, el fet d'haver fixat Δ, una arrel quadrada del discriminant D de f, ens permet assegurar que les arrels del primer factor de (5.2) són $\{l_1, l_4\}$ i les del segon, $\{l_2, l_3\}$. Per poder resoldre els resolvents R_1, R_2, R_3, R_4, hem d'imposar més restriccions (si canviéssim l_2 per l_3 i no canviéssim l_1 per l_4, aleshores no obtindríem una permutació dels R_i). Notem que $(l_1 - l_4)(l_2 - l_3) = \mathcal{O}\Delta$ per a algun

$\mathcal{O} \in K$, ja que $K((l_1 - l_4)(l_2 - l_3)) = L^{\langle \sigma, \tau^2 \rangle}$. Com que $\mathcal{O} = (l_1 - l_4)(l_2 - l_3)\Delta/D$, podem calcular $\mathcal{O}$ en funció de θ pel mètode de Lazard.

Per a un polinomi específic, sigui Δ' una arrel quadrada del seu discriminant D. Definim l'_1 i l'_4 les arrels del primer polinomi quadràtic de (5.2), i l'_2 i l'_3, les del segon, de manera que $(l'_1 - l'_4)(l'_2 - l'_3) = \mathcal{O}\Delta'$. Si $\Delta' = \Delta$, aleshores (l'_1, l'_2, l'_3, l'_4) és o bé (l_1, l_2, l_3, l_4), o bé (l_4, l_3, l_2, l_1). Si $\Delta' = -\Delta$, aleshores (l'_1, l'_2, l'_3, l'_4) és o bé (l_2, l_4, l_1, l_3), o bé (l_3, l_1, l_4, l_2). Els resolvents R_i que s'obtenen són, en cada cas, (R_1, R_2, R_3, R_4), (R_4, R_3, R_2, R_1), (R_3, R_1, R_4, R_2), (R_2, R_4, R_1, R_3), respectivament. Veurem més endavant que això només comporta una permutació de les arrels x_i que s'obtenen amb (5.1).

Només cal considerar l'elecció de les arrels cinquenes de R_i per tal d'obtenir els resolvents r_i. Veurem que fixada una arrel cinquena de R_1, les altres queden completament determinades. Els productes r_1r_4 i r_2r_3 queden fixos per $\sigma, \tau\omega^{-1}$ i τ^2, de manera que $r_1r_4, r_2r_3 \in F(\zeta)^{\langle \sigma, \tau\omega^{-1}, \tau^2 \rangle} = K(\Delta(\zeta + \zeta^{-1})) = K(\Delta\sqrt{5})$. Pel lema 5.3.2, el discriminant D de qualsevol polinomi quíntic resoluble és un nombre racional positiu, de manera que, per a qualsevol polinomi específic, $r_1r_4, r_2r_3 \in \mathbb{Q}(\sqrt{5D}) \subset \mathbb{R}$. Com que els resolvents r_i estan completament determinats llevat de multplicació per una arrel cinquena de la unitat, aleshores r_1 determina r_4 i r_2 determina r_3. Només queda per veure que r_1 determina r_2.

Ara, els productes $r_1r_2^2, r_3r_1^2, r_4r_3^2, r_2r_4^2$ són invariants per σ i es permuten cíclicament per τ i ω, de manera que són les arrels d'un polinomi cíclic de grau 4 sobre K i existeixen elements $u, v \in K$ tals que

$$\begin{aligned} r_1r_2^2 + r_4r_3^2 &= u + v\Delta\sqrt{5}, \\ r_3r_1^2 + r_2r_4^2 &= u - v\Delta\sqrt{5}, \end{aligned} \tag{5.3}$$

on ζ es pren de manera que $\zeta + \zeta^{-1} = (-1 + \sqrt{5})/2$.

Lema 5.3.3. *Donat r_1 només existeix una única elecció de r_2, r_3, r_4 tal que $r_1r_4, r_2r_3 \in K(\Delta\sqrt{5})$ i tal que se satisfan les equacions de (5.3).*

Demostració. Només hem de provar que r_1 determina r_2. Si substituíssim r_2 per εr_2, on ε és una arrel cinquena primitiva de la unitat, aleshores r_3 se substituiria per $\varepsilon^{-1}r_3$ ja que $r_2r_3 \in \mathbb{R}$. Si aquesta nova elecció per a r_2 i r_3 també satisfés les equacions de (5.3), aleshores,

$$\begin{aligned} r_1r_2^2 + r_4r_3^2 = u + v\Delta\sqrt{5}, &\quad r_1(\varepsilon r_2)^2 + r_4(\varepsilon^{-1}r_3)^2 = u + v\Delta\sqrt{5}, \\ r_3r_1^2 + r_2r_4^2 = u - v\Delta\sqrt{5}, &\quad (\varepsilon^{-1}r_3)r_1^2 + (\varepsilon r_2)r_4^2 = u - v\Delta\sqrt{5}; \end{aligned}$$

i igualant les expressions per a $u + v\Delta\sqrt{5}$ i per a $u - v\Delta\sqrt{5}$, obtindríem que

$$\frac{r_1r_2^2}{r_4r_3^2} = -\frac{1 - \varepsilon^{-2}}{1 - \varepsilon^2} = \varepsilon^{-2}, \quad \frac{r_1^2r_3}{r_4^2r_2} = -\frac{1 - \varepsilon}{1 - \varepsilon^{-1}} = \varepsilon \quad \Rightarrow \quad \left(\frac{r_1}{r_4}\right)^5 = 1,$$

i r_1/r_4 seria una arrel cinquena de la unitat. Ara bé, del fet que $\sigma(r_1/r_4) = \zeta^3 r_1/r_4$ es dedueix que r_1/r_4 genera una extensió de grau 5 sobre $L(\zeta)$. Com que l'ordre del grup de Galois de f és divisible per 5, aquesta extensió no col·lapsa per a cap polinomi específic, amb el que arribem a una contradicció i provem el resultat. □

Aquests elements u, v es calculen amb el mateix mètode de Lazard.

Observació 5.3.4. En cas que volguéssim resoldre la quíntica sobre un cos Q diferent dels racionals, l'argument de $r_1r_4, r_2r_3 \in \mathbb{R}$ podria no servir. El que sí que es pot utilitzar

és que existeixen $a, b \in K$ tals que $r_1 r_4 = a + b\Delta\sqrt{5}$ i $r_2 r_3 = a - b\Delta\sqrt{5}$ i a, b es poden calcular pel mètode de Lazard. Amb aquesta modificació, el lema se segueix complint. A més a més, podria ser que $\mathrm{Gal}(Q(\zeta)|Q) \subsetneq (\mathbb{Z}/4\mathbb{Z})^*$, però això no influiria en la fórmula final.

Teorema 5.3.5 (Dummit)**.** *Suposem que el polinomi irreductible $f(X) = X^5 + pX^3 + qX^2 + rX + s \in \mathbb{Q}[X]$ és resoluble per radicals, i sigui θ l'única arrel racional del resolvent $f_{20}(X)$. Fixem una arrel quadrada Δ del discriminant D de f i sigui ζ una arrel cinquena primitiva de la unitat. Denotem per l_1, l_4 i l_2, l_3 les arrels dels factors quadràtics de (5.2) satisfent les condicions $(l_1 - l_4)(l_2 - l_3) = \mathcal{O}\Delta$. Aleshores, el grup de Galois de f és:*

(i) El grup de Frobenius F_{20} d'ordre 20 si, i només si, D no és un quadrat, o el que és el mateix, els factors quadràtics de (5.2) són irreductibles sobre $\mathbb{Q}(\sqrt{D})$.

(ii) El diedral $D_{2\cdot 5}$ d'ordre 10 si, i només si, D és un quadrat i els factors quadràtics són irreductibles sobre $\mathbb{Q}$.

(iii) El cíclic C_5 d'ordre 5 si, i només si, D és un quadrat i els factors quadràtics descomponen sobre $\mathbb{Q}$.

Sigui r_1 una arrel cinquena qualsevol de R_1 i siguin r_2, r_3, r_4 les arrels cinquenes corresponents de R_2, R_3, R_4, com en el lema anterior. Aleshores, les fórmules de (5.1) expressen per radicals les arrels de f i x_1, x_2, x_3, x_4, x_5 es permuten cíclicament per algun 5-cicle del grup de Galois.

Demostració. Les propietats (i), (ii) i (iii) són immediates.

Ja hem vist que l'elecció de Δ i dels l_i determina els R_i llevat de les permutacions (R_1, R_2, R_3, R_4) o (R_4, R_3, R_2, R_1), si l'elecció de Δ és la mateixa que en els càlculs que hem fet, i (R_3, R_1, R_4, R_2) o (R_2, R_4, R_1, R_3) si hem canviat el signe de Δ respecte dels càlculs anteriors. És fàcil comprovar que els corresponents resolvents r_i són (r_1, r_2, r_3, r_4), (r_4, r_3, r_2, r_1), (r_3, r_1, r_4, r_2), (r_2, r_4, r_1, r_3), respectivament. Les fórmules de (5.1) expressen les arrels x_i en els ordres $(x_1, x_2, x_3, x_4, x_5)$, $(x_1, x_5, x_4, x_3, x_2)$, $(x_1, x_3, x_5, x_2, x_4)$, $(x_1, x_4, x_2, x_5, x_3)$. En termes del 5-cicle σ, aquestes permutacions corresponen a les permutacions donades per $\sigma, \sigma^{-1}, \sigma^2, \sigma^3$, respectivament. Per últim, qualsevol elecció de ζ produeix les mateixes permutacions en les x_i, de manera que les arrels de $f(X)$ que s'obtenen estan permutades cíclicament per algun 5-cicle, independentment de totes les eleccions. □

5.4 Faggal, Lazard (2014)

Hem estudiat la manera com Dummit resol la quíntica: utilitzant una arrel d'un polinomi resolvent de grau 6. Ara bé, els diferents invariants involucrats en la fórmula de Dummit tenen expressions gairebé monstruoses en funció de l'arrel. A més a més, el mètode de Dummit requeriria considerar un polinomi resolvent de grau 120 per resoldre les equacions de grau 7. Lazard, l'any 2004, també publica en [16] una fórmula una mica més senzilla però que només refina la idea de Dummit.

L'any 2014, però, Faggal i Lazard en [9] donen una fórmula extremadament més simple per tal d'expressar per radicals les arrels d'un polinomi quíntic (i, de fet, també d'un polinomi de grau 7). En el cas del polinomi de grau 5, el que fan és utilitzar la següent caracterització dels polinomis resolubles.

Proposició 5.4.1. *Sigui $f(X)$ un polinomi quíntic de coeficients en un cos K tal que el seu discriminant és un quadrat i sigui f_{10} el polinomi de grau 10 que té per arrels les*

sumes de dues arrels diferents de f. Aleshores, f és resoluble per radicals si, i només si, f_{10} descompon en dos polinomis irreductibles de grau 5.

Demostració. Siguin x_1, x_2, x_3, x_4, x_5 les arrels de f, G el seu grup de Galois, D el seu discriminant i L el seu cos de descomposició. Siguin $\sigma = (1\,2\,3\,4\,5)$, $\tau = (2\,3\,5\,4) \in S_5$, i podem suposar que $\sigma \in G$. El polinomi $f_{2,5}(X) = \prod_{i=1}^{5}(X - (x_i + x_{i+2}))$ té $x_2 + x_5$ per arrel i queda fix per $G \cap \langle \sigma, \tau^2 \rangle$, de manera que podem considerar la cadena de cossos següent:

$$K = L^G = K(\sqrt{D}) \subseteq L^{G\cap\langle\sigma,\tau^2\rangle} \subseteq K(x_2 + x_5) \subseteq L^{G\cap\langle\tau^2\rangle} \subseteq L.$$

A més a més, $f_{2,5}(X)$ és irreductible sobre $K^{G\cap\langle\sigma,\tau^2\rangle}$, ja que σ actua transitivament en les seves arrels i, si fossin totes iguals, aleshores f no seria irreductible. Així doncs, $[K(x_2 + x_5) : L^{G\cap\langle\sigma,\tau^2\rangle}] = 5$. Per últim, podem suposar que G és resoluble si, i només si $G \subseteq \langle \sigma, \tau \rangle$. Ara, en ser $G \subseteq A_5$, la inclusió $G \subseteq \langle \sigma, \tau \rangle$, és equivalent a $G \subseteq \langle \sigma, \tau^2 \rangle$, i això només se satisfà quan $f_{2,5}$ és irreductible i de grau 5 sobre K. Per al polinomi $f_{3,4}(X) = \prod_{i=1}^{5}(X - (x_i + x_{i+1}))$ tenim exactament el mateix, de manera que f és resoluble per radicals si, i només si, el polinomi $f_{10} = f_{2,5}f_{3,4}$ descompon en dos polinomis irreductibles de grau 5. □

D'aquí deduïm fàcilment que un polinomi f de grau 5 és resoluble per radicals si, i només si, f_{10} descompon en dos polinomis irreductibles de grau 5 sobre el cos generat per una arrel quadrada del discriminant de f.

En [9], es torna a utilitzar el mètode de Lazard per tal d'expressar un invariant, que serà útil a l'hora de resoldre les arrels del polinomi, en funció d'un conjunt d'invariants que són fàcils de calcular. Ja hem vist que els lemes 5.2.10 i 5.2.11 permeten obtenir un procediment per calcular invariants.

Sigui F_1 un invariant i calculem la seva forma normal $\overline{F_1}^J$ per la base de Gröbner J, definida en el lema 5.2.10. Si el seu terme líder només depèn de les x_i, afegim F_1 a la base i considerem una nova indeterminada f_1 i el polinomi $P_1 := \overline{F_1}^J - f_1$. Suposem que tenim calculats $F_1, \ldots, F_r$ invariants linealment independents. Donat un altre invariant F_{r+1}, considerem $\overline{F}^J_{r+1}$ i mirem si el seu terme líder és el producte del terme líder d'un dels P_i per un monomi independent de les x_i. Si això no és així, afegim F_{r+1} a la base d'invariants.

Una vegada calculada una base, podem expressar un invariant f qualsevol en aquesta base: en calculem la forma normal per J i sabem que el seu terme líder és el producte del terme líder d'un dels P_i per un monomi independent de les x_i. Llavors anem aplicant el procediment que hem explicat al final de l'apartat 5.2.

Sigui $f(X) = X^5 - s_1X^4 + s_2X^3 - s_3X^2 + s_2X - s_1$ el polinomi general de grau 5 i siguin x_1, x_2, x_3, x_4, x_5 les seves arrels. Considerem també els polinomis

$$F_1(X) = \prod_{i=1}^{5}(X - (x_i + x_{i+1})), \quad F_2(X) = \prod_{i=1}^{5}(X - (x_i + x_{i+2})).$$

És fàcil comprovar que $\sigma(F_i) = \tau^2(F_i) = F_i$ i $\tau(F_i) = F_j$, amb $\{i, j\} = \{1, 2\}$. Denotem per B_i i C_i els coeficients de X^{5-i} en F_1 i F_2, respectivament; i definim $D_i := B_i - C_i$.

El mètode descrit anteriorment, amb l'ajuda de la sèrie de Molien de l'anell dels polinomis en les x_i invariants per $\langle \sigma, \tau^2 \rangle$, que té per polinomi $P(t) = t^{10} + t^8 + t^7 + 2t^6 + 2t^5 + 2t^4 + t^3 + t^2 + 1$, ens permet provar el resultat següent.

Proposició 5.4.2. *El conjunt* $\{1,\ D_2,\ D_3,\ D_4,\ D_5,\ B_4+C_4,\ B_5+C_5,\ D_2^3,\ D_3^2,\ D_2D_5,\ D_2^4,\ D_2D_3D_5\}$ *és una base del mòdul lliure dels invariants del grup* $\langle\sigma,\tau^2\rangle$.

Sigui $f(X)=X^5+pX^3+qX^2+rX+s$ un polinomi irreductible i resoluble de grau 5, de coeficients en un cos K que conté les arrels cinquenes de la unitat. Sabem que el seu grup de Galois està contingut en F_{20}. Considerem l'extensió $K(\sqrt{D})|K$, on D és el discriminant de f. Sobre aquest cos, el grup de Galois de f és C_5 o $D_{2\cdot5}$. Per tant, les especialitzacions f_1 i f_2 dels polinomis F_1 i F_2 són de coeficients en aquest cos i, com que el grup de Galois és transitiu en les seves arrels, són irreductibles. A més a més, si el discriminant no és un quadrat de K, el seu grup de Galois és transitiu en les sumes de dues arrels diferents de f, i f_1 i f_2 són conjugats.

Proposició 5.4.3. *El polinomi minimal* f_{10} *de la suma de dos arrels diferents de* f *factoritza sobre* $K(\sqrt{D})$ *com el producte de dos polinomis irreductibles de grau 5. A més a més, si el discriminant de* f *no és un quadrat de* K*, els polinomis* f_1 *i* f_2 *són conjugats. En qualsevol cas, els coeficients de* f_1+f_2 *i de* $(f_1-f_2)\sqrt{D}$ *són de* K.

A més a més, es pot comprovar que

$$\begin{aligned} f_{10}(X) &= X^{10}+3pX^8+qX^7+3(p^2-r)X^6+(2pq-11s)X^5+(-2rp+p^3-q^2)X^4\\ &+ (-4qr+p^2q-4sp)X^3+(7sq+rp^2-4r^2-pq^2)X^2+(4rs-p^2s-q^3)X\\ &- s^2+pqs-rq^2. \end{aligned}$$

Denotem per e_i i d_i els coeficients de X^{5-i} dels polinomis f_1+f_2 i f_1-f_2, respectivament. Aleshores, $\tau(e_i)=e_i$ i $\tau(d_i)=-d_i$. La proposició 5.4.2 ens assegura que qualsevol invariant de $\langle\sigma,\tau^2\rangle$ s'expressa com un polinomi de coeficients en $K[p,q,r,s]$ i indeterminades d_i,e_i. Com en l'apartat anterior, considerem els resolvents $r_i=\sum_{i=0}^4\zeta^{ij}x_{i+1}\in K(x_1,x_2,x_3,x_4,x_5)$. És fàcil veure que r_1r_4, $r_1^5+r_4^5$, $r_4^2r_2+r_1^2r_3$ i $r_1^3r_2+r_4^3r_3$ són fixos per $\langle\sigma,\tau^2\rangle$ i, amb el mètode descrit anteriorment, trobem:

$$r_1r_4=-\frac{\sqrt{5}}{2}d_2-\frac{5}{2}p, \tag{5.4}$$

$$r_1^5+r_4^5=\frac{125}{2}\sqrt{5}d_5+125e_5-\frac{25}{4}\sqrt{5}d_3p-\frac{75}{4}\sqrt{5}d_2q-\frac{125}{2}pq-\frac{375}{2}s, \tag{5.5}$$

$$r_4^2r_2+r_1^2r_3=-\frac{5}{2}\sqrt{5}d_5-\frac{25}{2}q, \tag{5.6}$$

$$r_1^3r_2+r_4^3r_3=\frac{25}{2}\sqrt{5}d_4+\frac{15}{2}e_4-\frac{15}{2}\sqrt{5}d_2p-40r-\frac{5}{2}p^2, \tag{5.7}$$

on $\zeta^2+\zeta^{-2}=(-1-\sqrt{5})/2$. Denotem per h_{i-3} la part dreta de la igualtat de l'equació $(5.i)$. Les equacions (5.4) i (5.5) mostren que r_1^5 i r_4^5 són les solucions d'una equació quadràtica. Per tant, la podem resoldre i extreure'n l'arrel cinquena per obtenir r_1. Si $r_1\neq0$, l'equació (5.5) ens permet obtenir r_4. Llavors, s'obtenen r_2 i r_3 com les solucions del sistema lineal de les equacions (5.6) i (5.7).

Si les dues solucions de l'equació quadràtica són zero, aleshores podem intercanviar f_1 i f_2 per tal de canviar els signes de tots els d_i en les equacions (5.4)-(5.7). Si la nova quadràtica també tingués dues solucions nul·les, aleshores tots els r_i serien zero i les cinc arrels de f serien iguals, cosa que no pot passar ja que f és irreductible.

Si una arrel de l'equació quadràtica és zero, aleshores escollim $r_4=0$, de manera que r_1 és una arrel cinquena de la part dreta de la igualtat de (5.5).

Ara, el determinant del sistema lineal en r_2, r_3 és $r_1^5 - r_4^5$. Si fos $r_1^5 = r_4^5 \neq 0$, tindríem $r_4 = \zeta^i r_1$ per a alguna i. Aleshores, $r_1^2 = h_1/\zeta^i$ i $r_2\zeta^i + r_3 = h_3$. Com que $r_2 r_3 = \tau(r_1 r_4) = d_2\sqrt{5}/2 - 5p/2$, aleshores $r_2^2 \in K$, $r_3 \in K(r_2)$ i, per 5.7, $r_1^3 \in K(r_2)$, de manera que tots els resolvents r_i viurien en una extensió de K de grau coprimer amb 5 i, per tant, les arrels x_i de f, també i f no seria irreductible.

Com hem fet amb el Dummit, no és complicat demostrar que, independentment de com elegim l'arrel ζ de la unitat, els polinomis f_1 i f_2, i els resolvents r_i a partir de resoldre les equacions (5.4)-(5.7), les arrels x_1, x_2, x_3, x_4, x_5 de f s'obtenen amb les equacions (5.1). Així doncs, els passos per resoldre les arrels són:

- Llegim f, un polinomi irreductible de grau 5 de coeficients a_i.
- Definim $t := a_4/(5a_5)$, $g(X) := f(X - t)$, $D := \mathrm{disc}(g)$.
- Factoritzem f_{10} en l'extensió generada per $\sqrt{D}$ i anomenem f_1, f_2 els polinomis mònics de grau 5 que en resulten.
- Definim e_i com els coeficients de $(f_1 + f_2)(X) = 2X^5 + e_1X^4 + e_2X^3 + e_3X^2 + e_4X + e_5$.
- Definim d_i com els coeficients de $(f_1 - f_2)(X) = d_1X^4 + d_2X^3 + d_3X^2 + d_4X + d_5$.
- Si $h_1 = h_3 = 0$, canviem d_i per $-d_i$.
- Si $h_1 = 0$, definim $r_1 := h_2^{1/5}$, $r_4 := 0$ i $d := h_2$.
- Si $h_1 \neq 0$, definim $d := \sqrt{h_2^2 - 4h_1^5}$, $r_1 := ((h_2 + d)/2)^{1/5}$, $r_4 := h_1/r_1$.
- Definim $w := (\sqrt{-10 - 2\sqrt{5}} + \sqrt{5} - 1)/4$, $r_2 := (h_4r_1^2 - h_3r_4^3)/d$, $r_3 := (h_3r_1^3 - h_4r_4^2)/d$.
- Les arrels de f són:

$$\begin{aligned}
x_1 &= -t + (r_1 + r_2 + r_3 + r_4)/5,\\
x_2 &= -t + (wr_1 + w^2r_2 + w^3r_3 + w^4r_4)/5,\\
x_3 &= -t + (w^2r_1 + w^4r_2 + wr_3 + w^3r_4)/5,\\
x_4 &= -t + (w^3r_1 + wr_2 + w^4r_3 + w^2r_4)/5,\\
x_5 &= -t + (w^4r_1 + w^3r_2 + w^3r_3 + wr_4)/5.
\end{aligned}$$

Com que la fórmula obtinguda per Faggal i Lazard és molt més senzilla que la de Dummit, és la que hem utilitzat a l'hora de calcular els exemples que donem al final del treball.

Malgrat que, teòricament, amb les fórmules de Dummit ja podríem resoldre per radicals qualsevol polinomi $f(X) \in \mathbb{Q}[X]$ de grau 5 i irreductibble sobre un cos p-àdic, les comprovacions que s'han de fer per tal d'elegir adequadament cada invariant de la fórmula semblen inviables de dur a terme. És cert que amb les fórmules de Lazard en [16] això és més senzill de fer, però no resoldrem les quíntiques d'aquesta manera. Notem que, amb les fórmules donades per Faggal i Lazard el 2014, a més, necessitaríem descompondre un polinomi sobre una extensió p-àdica, cosa que ja s'ha fet en [2], però no ens n'ocuparem.

El que farem nosaltres és demostrar que tot polinomi de grau 5 irreductible sobre $\mathbb{Q}_p$ es pot expressar com una $\mathbb{Q}_p$-combinació lineal d'expressions radicals sobre els racionals i, gràcies a l'algoritme de Panayi, podrem trobar aproximacions tan bones com vulguem d'aquests coeficients p-àdics. Per tal de fer això, necessitem estudiar amb detall les extensions de grau 5 sobre $\mathbb{Q}_p$.

Part III : Estudi de les quíntiques en $\mathbb{Q}_p$

6 Extensions moderadament ramificades sobre $\mathbb{Q}_p$ de grau 5

Per a les extensions de grau 5 sobre $\mathbb{Q}_p$ només podem tenir 3 tipus diferents de ramificació. En efecte, l'índex de ramificació de l'extensió ha de dividir-ne el grau i, conseqüentment, o bé és 1 i l'extensió és no ramificada; o bé és 5 i l'extensió és totalment ramificada. En aquest segon cas, l'extensió és moderadament ramificada si $p \neq 5$, i és salvatgement ramificada si $p = 5$. En aquesta secció estudiem els dos primers casos.

6.1 Extensions no ramificades sobre $\mathbb{Q}_p$

Siguin $f(X) \in \mathbb{Q}_p[X]$ un polinomi de grau 5 irreductible sobre $\mathbb{Q}_p$, α una arrel d'aquest polinomi i suposem que l'extensió $\mathbb{Q}_p(\alpha)|\mathbb{Q}_p$ és no ramificada, és a dir, que el grup d'inèrcia és el trivial. Per 3.5.4 sabem que, en aquest cas, $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\zeta)$, on ζ és una arrel (p^5-1)-èsima primitiva de la unitat i, a més a més, l'extensió $\mathbb{Q}_p(\alpha)|\mathbb{Q}_p$ és cíclica.

Observació 6.1.1. Notem que no sempre cal considerar una arrel (p^5-1)-èsima primitiva de la unitat com a element primitiu de l'extensió. L'extensió de cossos residuals $\mathbb{F}_p(\overline{\zeta})|\mathbb{F}_p$ és cíclica de grau 5, de manera que $\mathbb{F}_p(\overline{\zeta}) = \mathbb{F}_{p^5}$. Si $\overline{\xi} \in \mathbb{F}_{p^5}^*$ és un element d'ordre d, amb $d \mid p^5 - 1$ i $d \nmid p - 1$, aleshores $\mathbb{F}_{p^5} = \mathbb{F}_p(\overline{\xi})$ i $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\xi)$, on ξ és una arrel d-èsima primitiva de la unitat.

6.2 Extensions ramificades sobre $\mathbb{Q}_p$, amb $p \neq 5$

Siguin $p \neq 5$ un nombre primer, $f(X) \in \mathbb{Q}_p[X]$ un polinomi de grau 5 irreductible sobre $\mathbb{Q}_p$, α una arrel d'aquest polinomi i suposem que l'extensió $\mathbb{Q}_p(\alpha)|\mathbb{Q}_p$ és ramificada. Sabem que, aleshores, l'extensió és totalment i moderadament ramificada i que el grup d'inèrcia G_0 coincideix amb el grup de Galois de l'extensió.

Lema 6.2.1. *Tota extensió totalment i moderadament ramificada de grau n sobre $\mathbb{Q}_p$ està generada per una arrel d'algun dels polinomis*

$$X^n - \zeta^r p, \quad 0 \leq r \leq p-1,$$

on $\zeta \in \mathbb{Q}_p$ és una arrel $(p-1)$-èsima primitiva de la unitat.

Demostració. Sigui $K|\mathbb{Q}_p$ una extensió d'aquesta forma. Per 3.6.2, sabem que $K = \mathbb{Q}_p(\tilde{\beta})$, on $\tilde{\beta}$ és una arrel d'un polinomi $\tilde{g}(X)$ de la forma $X^n - up$, amb $u \in \mathbb{Z}_p^\times$, una unitat de $\mathbb{Z}_p$. Si ζ és una arrel $(p-1)$-èsima primitiva de la unitat, podem posar $u = \zeta^r + \sum_{j=1}^{\infty} a_j p^j$, amb $a_j \in \{0, 1, \zeta, \ldots, \zeta^{p-2}\}$. Seguint la demostració de 3.6.2, es veu que, per a alguna arrel β del polinomi $g(X) = X^n - \zeta^r p$, se satisfà que $\mathbb{Q}_p(\tilde{\beta}) = \mathbb{Q}_p(\beta)$. □

En [21], es demostra un resultat encara més fort.

Proposició 6.2.2. *Sigui $g = \mathrm{mcd}(p-1, n)$. Hi ha exactament n extensions totalment i moderadament ramificades de grau n sobre $\mathbb{Q}_p$. A més a més, aquestes n extensions es classifiquen en g classes de n/g extensions conjugades, i totes les extensions de la mateixa classe estan generades per una de les arrels del polinomi*

$$X^n - \zeta^r p, \quad 0 \leq r \leq g-1.$$

Demostració. Si β és una arrel del polinomi $X^n-\zeta^i p$, aleshores β i $\zeta^h\beta$ generen la mateixa extensió, ja que $\zeta\in\mathbb{Q}_p$. A més, el polinomi minimal de $\zeta^h\beta$ sobre $\mathbb{Q}_p$ és $X^n-\zeta^{nh+i}p$.

Sigui $0\leq r<g$ tal que $r\equiv i \pmod g$. Podem escollir h tal que $nh+i\equiv r \pmod{p-1}$. Per tant, en termes de l'extensió, considerar el polinomi $X^n-\zeta^i p$ és el mateix que considerar el polinomi $X^n-\zeta^{nh+i}p$, per a qualsevol h, i aquest h el podem prendre de manera que $nh+i\equiv r \pmod{p-1}$, per a algun $0\leq r<g$. Així doncs, només cal considerar els polinomis

$$X^n-\zeta^r p,\quad 0\leq r<g.$$

Ara, siguin α i α' arrels dels polinomis $X^n-\zeta^r p$ i $X^n-\zeta^{r'}p$, respectivament, amb $0\leq r<r'<g$. Suposem que α i α' generen el mateix cos. Aleshores, $(\alpha/\alpha')^n=\zeta^{r-r'}$ i $\alpha/\alpha'\in\mathbb{Q}_p(\alpha)$ és una arrel n-èsima de $\zeta^{r-r'}$. Però això no pot ser, ja que $\mathbb{Q}_p(\alpha)$ només conté les arrels $(p-1)$-èsimes primitives de la unitat (l'extensió és totalment ramificada) i, com que $r\not\equiv r' \pmod g$, aleshores $r-r'$ no és un múltiple de n mòdul $p-1$ i α/α' no pot ser una arrel $(p-1)$-èsima de la unitat.

Per tant, α i α' generen extensions diferents de $\mathbb{Q}_p$. Si w és una arrel n-èsima primitiva de la unitat tal que $w^{n/g}=\zeta^{\frac{p-1}{g}}$, aleshores els conjugats de α sobre $\mathbb{Q}_p$ són $\alpha, w\alpha,\dots,w^{n-1}\alpha$, i $\alpha, w^{n/g}\alpha=\zeta^{\frac{p-1}{g}}\alpha,\dots,w^{(g-1)\frac{n}{g}}\alpha=\zeta^{(g-1)\frac{p-1}{g}}\alpha$ generen el mateix cos i, en canvi, $\alpha, w\alpha,\dots,w^{n/g-1}\alpha$ generen extensions diferents. Tenint en compte la proposició anterior s'acaba la demostració. □

Observació 6.2.3. De fet, el resultat que apareix en [21] és més general: amb una demostració molt similar s'aconsegueix un resultat anàleg per a extensions $K|k$ totalment i moderadament ramificades de grau n, on $k|\mathbb{Q}_p$ és una extensió finita.

Així doncs, si L denota el cos de descomposició d'una extensió totalment i moderadament ramificada de grau n sobre $\mathbb{Q}_p$, se satisfà que $L=\mathbb{Q}_p(\beta,w)$, on β és una arrel d'un dels polinomis $X^n-\zeta^r p$ i w és una arrel n-èsima primitiva de la unitat. Ara, en virtut de 3.5.1, l'extensió $\mathbb{Q}_p(w)|\mathbb{Q}_p$ és no ramificada i, pel teorema 3.5.3 i la teoria de cossos finits, el grau de l'extensió $\mathbb{Q}_p(w)|\mathbb{Q}_p$ és l'enter positiu més petit f tal que $p^f\equiv 1 \pmod n$. En resum, per a les extensions de grau 5, tenim el resultat següent.

Corol·lari 6.2.4. *Siguin $p\neq 5$ un nombre primer, $f(X)\in\mathbb{Q}[X]$ un polinomi de grau 5 irreductible sobre $\mathbb{Q}_p$, L el cos de descomposició del polinomi sobre $\mathbb{Q}_p$, $\alpha\in L$ una arrel d'aquest polinomi i suposem que l'extensió $\mathbb{Q}_p(\alpha)|\mathbb{Q}_p$ és (totalment) ramificada. Aleshores:*

(i) $\mathbb{Q}_p(\alpha)=\mathbb{Q}_p(\beta)$ per a una determinada arrel β d'algun dels polinomis

$$X^5-\zeta^r p,\quad 0\leq r\leq g-1,$$

on $g=\mathrm{mcd}(5,p-1)$ i $\zeta\in\mathbb{Q}_p$ és una arrel $(p-1)$-èsima primitiva de la unitat.

(ii) $L=\mathbb{Q}_p(\beta,w)$, on w és una arrel cinquena primitiva de la unitat.

(iii) Si definim $\sigma(\beta)=\beta w$ i $\tau(w)=w^2$, aleshores

$$\begin{aligned}
&\mathrm{Gal}(L|\mathbb{Q}_p)=\langle\sigma\rangle\simeq C_5 && \Leftrightarrow\quad p\equiv 1 \pmod 5,\\
&\mathrm{Gal}(L|\mathbb{Q}_p)=\langle\sigma,\tau^2\rangle\simeq D_{2\cdot 5} && \Leftrightarrow\quad p\equiv -1 \pmod 5,\\
&\mathrm{Gal}(L|\mathbb{Q}_p)=\langle\sigma,\tau\rangle\simeq F_{20} && \Leftrightarrow\quad p\equiv \pm 2 \pmod 5.
\end{aligned}$$

Corol·lari 6.2.5. *En les condicions de la proposició anterior, el discriminant de f és un quadrat de $\mathbb{Q}_p$ si, i només si, $p\equiv\pm 1 \pmod 5$.*

7 Extensions ramificades sobre $\mathbb{Q}_5$ de grau 5

Ja hem estudiat les extensions de grau 5 moderadament ramificades sobre $\mathbb{Q}_p$: tenim un element primitiu per a cada extensió i en coneixem el grup de Galois. Es tracta de fer el mateix per a les extensions que són (totalment i salvatgement) ramificades sobre $\mathbb{Q}_5$.

En [15], Krasner és capaç d'obtenir una fórmula per calcular el nombre d'extensions p-àdiques d'un grau donat i, en [20] i [21], Pauli i Roblot adapten els mètodes de Krasner per construir un conjunt de polinomis generadors d'aquestes extensions. Reproduïm aquesta construcció per tal d'obtenir aquest conjunt per a les extensions de grau 5 ramificades sobre $\mathbb{Q}_5$.

Siguin $\overline{\mathbb{Q}}_p$ una clausura algebraica fixada de $\mathbb{Q}_p$, $K \subset \overline{\mathbb{Q}}_p$ una extensió totalment ramificada de grau n sobre un cos $\mathfrak{p}$-àdic k amb anell de valoració discreta A. Sigui $\mathfrak{p} = \pi A$ l'ideal primer de k, i e l'índex de ramificació de l'extensió $k|\mathbb{Q}_p$. Denotem per $v_\mathfrak{p}$ l'única extensió de la valoració p-àdica v_p en k tal que $v_\mathfrak{p}(\pi) = 1$. Sigui q el cardinal del cos residual de k.

7.1 Mètrica en els polinomis d'Eisenstein

Tal i com fa Krasner, Pauli i Roblot comencen introduint una mètrica en el conjunt dels polinomis d'Eisenstein de grau i discriminant donat.

Proposició 7.1.1 (Condicions d'Ore)**.** *Sigui k una extensió finita de $\mathbb{Q}_p$ amb ideal maximal $\mathfrak{p}$. Donat $j \in \mathbb{Z}$, siguin $a, b \in \mathbb{Z}$ tals que $j = an + b$ i $0 \leq b < n$. Existeixen extensions $K|k$ totalment ramificades de grau n i discriminant $\mathfrak{p}^{n+j-1}$ si, i només si,*

$$\min\{v_\mathfrak{p}(b)n, v_\mathfrak{p}(n)n\} \leq j \leq v_\mathfrak{p}(n)n.$$

Demostració. Per 3.6.1, tota extensió totalment ramificada K de k està generada per una arrel Π d'un polinomi d'Eistenstein $f(X) = X^n + f_{n-1}X^{n-1} + \cdots + f_1X + f_0$, i per 4.4.3, $\Delta_{K|k} = \mathrm{disc}(f)A$. A més, de 2.4.3 deduïm que $v_\mathfrak{p}(\mathrm{disc}(f)) = v_\mathfrak{p}(f'(\Pi))n$, ja que $|f'(\Pi)| = |\mathrm{N}_{K|k}(f'(\Pi))|^{1/n}$. Com que $v_\mathfrak{p}(\Pi) = 1/n$, les valoracions de $if_i\Pi^{i-1}$ per a $1 \leq i < n$ i $n\Pi^{n-1}$ són totes diferents i, per la propietat (3) de 2.6.4,

$$\begin{aligned} v_\mathfrak{p}(f'(\Pi)) &= v_\mathfrak{p}(n\Pi^{n-1} + (n-1)f_{n-1}\Pi^{n-2} + \cdots + f_1) \\ &= \min_{1\leq i\leq n-1}\left\{v_\mathfrak{p}(n) + \frac{n-1}{n}, v_\mathfrak{p}(i) + v_\mathfrak{p}(f_i) + \frac{i-1}{n}\right\} \\ &= \min_{1\leq i\leq n-1}\left\{\frac{nv_\mathfrak{p}(n)}{n}, \frac{n(v_\mathfrak{p}(i) + v_\mathfrak{p}(f_i) - 1) + i}{n}\right\} + \frac{n-1}{n}. \end{aligned}$$

Si definim $j := v_\mathfrak{p}(\mathrm{disc}(f)) - n + 1 = nv_\mathfrak{p}(f'(\Pi)) - n + 1$, aleshores

$$j = \min_{1\leq i\leq n-1}\{nv_\mathfrak{p}(n), n(v_\mathfrak{p}(i) + v_\mathfrak{p}(f_i) - 1) + i\}.$$

D'aquesta manera, o bé $j = nv_\mathfrak{p}(n)$, o bé $j = n(v_\mathfrak{p}(b) + v_\mathfrak{p}(f_b) - 1) + b$, per a algun $1 \leq b \leq n-1$. Fixem $b \in \mathbb{Z}$, $1 \leq b \leq n-1$ i definim $a := v_\mathfrak{p}(b) + v_\mathfrak{p}(f_b) - 1$. Com que $v_\mathfrak{p}(f_b) - 1 \geq 0$ perquè $f(X)$ és un polinomi d'Eisenstein, aleshores $nv_\mathfrak{p}(b) + b \leq j = an + b$ i $nv_\mathfrak{p}(b) \leq j = an + b$. Així doncs, $\min\{nv_\mathfrak{p}(b), nv_\mathfrak{p}(n)\} \leq j \leq nv_\mathfrak{p}(n)$.

Recíprocament, per a qualsevol $j = an + b$, amb $\min\{nv_\mathfrak{p}(b), nv_\mathfrak{p}(n)\} \leq j \leq nv_\mathfrak{p}(n)$ podem construir un polinomi d'Eisenstein $f(X)$ amb discriminant $\mathfrak{p}^{n+j-1}$. En fecte, si $b =$

0, aleshores $j = nv_{\mathfrak{p}}(n)$ i només cal prendre els f_i de manera que $v_{\mathfrak{p}}(f_i) \geq \max\{1, v_{\mathfrak{p}}(n) - v_{\mathfrak{p}}(i) + 1\}$, per a $1 \leq i \leq n-1$. En cas que $b \neq 0$, només cal prendre f_b amb $v_{\mathfrak{p}}(f_b) = a - v_{\mathfrak{p}}(b) + 1$ i $v_{\mathfrak{p}}(f_i) \geq \max\{1, v_{\mathfrak{p}}(n) - v_{\mathfrak{p}}(i) + 1 - i/n\}$, per a $1 \leq i \leq n-1$, $i \neq b$. □

Sigui j un enter satisfent les condicions d'Ore respecte de n, de manera que $0 \leq j \leq v_{\mathfrak{p}}(n)n$ i sigui $j = an + b$ la divisió euclidiana de j entre n. Aleshores, n divideix j si, i només si, $b = 0$, que equival a tenir $a = v_{\mathfrak{p}}(n)$.

Fixat un enter $j \in \mathbb{Z}$, denotem per $K_{n,j}$ el conjunt de les extensions $K|k$ totalment ramificades de grau n i de discriminant $\mathfrak{p}^{n+j-1}$, que ja sabem que no és buit. Sigui $E_{n,j}$ el conjunt dels polinomis d'Eisenstein de grau n sobre k, i de discriminant $\mathfrak{p}^{n+j-1}$. Per 3.6.1, les arrels dels polinomis de $E_{n,j}$ generen tots els cossos $K \in K_{n,j}$.

Siguin $f, g \in E_{n,j}$ dos polinomis d'Eisenstein de grau n i discriminant $\mathfrak{p}^{n+j-1}$. Siguin $\alpha_1, \ldots, \alpha_n$ les arrels de f i $\beta_1, \ldots, \beta_n$ les arrels de g. Definim $d(f,g) := |f(\beta_1)|$ i veiem que no depèn de l'elecció de l'arrel de g: si σ és una k-immersió de $k(\beta)$ tal que $\sigma(\beta_1) = \beta_i$, aleshores $|f(\beta_1)| = |\sigma(f(\beta_1))| = |f(\sigma(\beta_1))| = |f(\beta_i)|$. A més a més,

$$|f(\beta_1)|^n = \prod_{i=1}^{n} |f(\beta_i)| = \prod_{1 \leq i,j \leq n} |\beta_i - \alpha_j| = |g(\alpha_1)|^n,$$

de manera que $d(f,g) = d(g,f)$. Fixem ara una arrel α de f i suposem que β és una arrel de g tal que la distància $|\beta - \alpha|$ és mínima. Aquestà distància no depèn de l'elecció de α. En efecte, sigui σ una k-immersió de $k(\alpha, \beta)$ tal que $\sigma(\alpha) = \alpha_i$. Aleshores $|\beta - \alpha| = |\sigma(\beta) - \sigma(\alpha)| = |\sigma(\beta) - \alpha_i|$ i, atès que $|\beta - \alpha| \leq |\beta_j - \alpha|$ per a tot j, llavors $|\sigma(\beta) - \alpha_i| \leq |\beta_j - \alpha_i|$ per a tot j. Així doncs,

$$d(f,g) = |f(\beta)| = \prod_{i=1}^{n} |\beta - \alpha_i|.$$

Si $|\beta - \alpha_i| \neq |\beta - \alpha|$, aleshores $|\beta - \alpha_i| > |\beta - \alpha|$ i $|\alpha - \alpha_i| = |\alpha - \beta + \beta - \alpha_i| = |\beta - \alpha_i|$, per la propietat (3) de 2.6.4. D'aquesta manera, queda demostrat que

$$d(f,g) = \prod_{i=1}^{n} \max\{|\beta - \alpha|, |\alpha - \alpha_i|\}. \tag{7.1}$$

Si ara prenem $h \in E_{n,j}$ i considerem γ (resp. γ') una arrel de h tal que la distància $|\beta - \gamma|$ (resp. $|\alpha - \gamma'|$) és mínima, aleshores

$$\begin{aligned}
d(f,h) &= \prod_{i=1}^{n} \max\{|\alpha - \gamma'|, |\alpha - \alpha_i|\} \leq \prod_{i=1}^{n} \max\{|\alpha - \gamma|, |\alpha - \alpha_i|\} \\
&\leq \prod_{i=1}^{n} \max\{\max\{|\alpha - \beta|, |\beta - \gamma|\}, |\alpha - \alpha_i|\} \\
&\leq \max\left\{ \prod_{i=1}^{n} \max\{|\alpha - \beta|, |\alpha - \alpha_i|\}, \prod_{i=1}^{n} \max\{|\beta - \gamma|, |\alpha - \alpha_i|\} \right\} \\
&\leq \max\{d(f,g), d(g,h)\}.
\end{aligned}$$

Clarament, $d(f,g) = 0$ si, i només si, $f = g$, amb el que s'obté el resultat següent.

Proposició 7.1.2. *Siguin $f, g \in E_{n,j}$, α una arrel de f i β una arrel de g. L'aplicació $d(f,g) := |f(\beta)| = |g(\alpha)|$ defineix una distància ultramètrica en $E_{n,j}$.*

Lema 7.1.3. *Si posem* $f(X) = \sum_{i=0}^{n} f_i X^i$ *i* $g(X) = \sum_{i=0}^{n} g_i X^i$, *amb* $f_n = g_n = 1$, *i definim*

$$w := \min_{0 \le i \le n-1} \{v_{\mathfrak{p}}(g_i - f_i) + i/n\},$$

aleshores $d(f,g) = |\pi|^w$.

Demostració. Notem que $g(\alpha) = g(\alpha) - f(\alpha) = \sum_{i=1}^{n-1}(g_i - f_i)\alpha^i$. En ser $v_{\mathfrak{p}}(\alpha) = 1/n$, tots els sumands tenen valoracions diferents i, per la propietat (3) de 2.6.4, hem acabat. □

7.2 Polinomis generadors de les extensions

Presentem ara els polinomis que construeixen Pauli i Roblot que generen tots els cossos de $K_{n,j}$, amb $j = an + b$ satisfent les condicions d'Ore.

Siguin $m \ge l \ge 1$ dos enters, i $R_{l,m}$ un sistema de representants del quocient $\mathfrak{p}^l/\mathfrak{p}^m$. Denotem per $R^*_{l,m}$ el subconjunt dels elements de $R_{l,m}$ tals que la seva valoració $v_{\mathfrak{p}}$ és l. Per a $1 \le i \le n-1$, definim

$$l(i) := \begin{cases} \max\{2 + a - v_{\mathfrak{p}}(i), 1\} & \text{si} \quad i < b, \\ \max\{1 + a - v_{\mathfrak{p}}(i), 1\} & \text{si} \quad i \ge b. \end{cases}$$

Sigui c un enter tal que $c > 1 + 2a + 2b/n = (n + 2j)/n$.

Definim Ω com el conjunt de n-tuples $(w_0, \ldots, w_{n-1}) \in k^n$ que satisfan:

$$w_i \in \begin{cases} R^*_{1,c} & \text{si} \quad i = 0, \\ R_{l(i),c} & \text{si} \quad 1 \le i \le n-1 \ \text{ i } \ i \ne b, \\ R^*_{l(b),c} & \text{si} \quad i = b \ne 0. \end{cases} \tag{7.2}$$

A cada element $w = (w_0, \ldots, w_{n-1}) \in \Omega$, li associem el polinomi $A_w(X) \in A[X]$ definit per $A_w(X) := X^n + w_{n-1}X^{n-1} + \cdots + w_1 X + w_0$.

Lema 7.2.1. *Els polinomis* $A_w(X)$ *són polinomis d'Eisenstein de discriminant* $\mathfrak{p}^{n+j-1}$.

Demostració. En ser $l(i) \ge 1$, aleshores $v_{\mathfrak{p}}(w_i) \ge 1$ i, per (7.2), $v_{\mathfrak{p}}(w_0) = 1$, de manera que A_w és un polinomi d'Eisenstein. Sigui α una arrel de A_w. Per 2.4.3 i 4.4.3, el discriminant de A_w és $\mathfrak{p}^{n+j-1}$ si, i només si,

$$v_{\mathfrak{p}}(A'_w(\alpha)) = (n + j - 1)/n = 1 + a + (b-1)/n.$$

Ara bé, $A'w(\alpha) = n\alpha^{n-1} + (n-1)w_{n-1}\alpha^{n-2} + \cdots + w_1$ i, com que les valoracions de tots aquests sumands són diferents, aleshores $v_{\mathfrak{p}}(A'_w(\alpha))$ és el mínim d'aquestes.

Per la definició de $l(i)$ i per (7.2), és fàcil comprovar que

$$\begin{aligned} v_{\mathfrak{p}}(iw_i\alpha^{i-1}) &> 1 + a + (b-1)/n, \quad \text{si} \quad i \ne b, \\ v_{\mathfrak{p}}(bw_b\alpha^{b-1}) &= 1 + a + (b-1)/n, \quad \text{si} \quad i = b \ne 0. \end{aligned} \tag{7.3}$$

Si $b \ne 0$, les condicions d'Ore ens asseguren que $v_{\mathfrak{p}}(n\alpha^{n-1}) > v_{\mathfrak{p}}(bw_b\alpha^{b-1})$ i, per tant, $v_{\mathfrak{p}}(A'_w(\alpha)) = 1 + a + (b-1)/n$.

Si $b = 0$, aleshores les condicions d'Ore ens asseguren que $a = v_{\mathfrak{p}}(n)$ i, per (7.3),

$$v_{\mathfrak{p}}(n\alpha^{n-1}) = v_{\mathfrak{p}}(n) + (n-1)/n < v_{\mathfrak{p}}(iw_i\alpha^{i-1}),$$

amb el que aconseguim que $v_{\mathfrak{p}}(A'_w(\alpha)) = 1 + a + (b-1)/n$. □

Teorema 7.2.2 (Krasner). *Sigui c un enter tal que $c > 1 + 2a + 2b/n$. El conjunt $E_{n,j}$ és la unió disjunta dels discs tancats $D_w := D_{E_{n,j}}(A_w, r)$ de centre A_w i radi $r := |\pi^c|$, per a tot $w \in \Omega$.*

Demostració. Ja sabem que $A_w \in E_{n,j}$ per a tot $w \in \Omega$. Siguin $w, w' \in \Omega$ dos elements diferents i sigui i un índex tal que $w_i \neq w'_i$. Per com hem definit el elements de Ω, $w_i - w'_i \notin \mathfrak{p}^c$, de manera que $v_\mathfrak{p}(w_i - w'_i) + i/n \leq c - 1 + i/n < c$. Ara, pel lema 7.1.3, ha de ser $d(A_w, A_{w'}) > r$ i, en ser d una distància ultramètrica, aleshores $D_w \cap D'_w = \emptyset$.

Sigui ara $f \in E_{n,j}$ i posem $f(X) = X^n + f_{n-1}X^{n-1} + \cdots + f_1 X + f_0$. Llavors, $v_\mathfrak{p}(f_0) = 1$ i existeix un element $w_0 \in R^*_{1,c}$ tal que $f_0 \equiv w_0 \pmod{\mathfrak{p}^c}$.

Amb un raonament anàleg al del lema anterior, es pot demostrar que $v_\mathfrak{p}(f_i) \geq l(i)$, per a tot $i > 0$. Així doncs, existeixen w_i complint (7.2) i tal que $f_i \equiv w_i \pmod{\mathfrak{p}^c}$. Sigui $w := (w_0, \ldots, w_{n-1})$. Aleshores, $v_\mathfrak{p}(f_i - w_i) \geq c$ per a tot i i, per tant, $v_\mathfrak{p}(f_i - w_i) + i/n \geq c$, de manera que, per 7.1.3, $f \in D_w$. □

Corol·lari 7.2.3. *Un cos K és de $K_{n,j}$ si, i només si, existeixen un element $w \in \Omega$ i una arrel α de $A_w(X)$ tals que $K = k(\alpha)$.*

Demostració. Siguin α un uniformitzant de K, f el seu polinomi irreductible sobre k, $\alpha = \alpha_1, \ldots, \alpha_n$ les arrels de f i δf la distància mínima entre α i les altres arrels de f. Aleshores,

$$|f'(\alpha)| = \prod_{i=2}^{n} |\alpha - \alpha_i| \leq \delta f \cdot |\pi^{(n-2)/n}|,$$

ja que els α_i també són uniformitzants de K. Ara bé, per 2.4.3, $|f'(\alpha)| = |\pi^{(n+j-1)/n}|$, de manera que $\delta f \geq |\pi^{(j+1)/n}|$. Sigui ara $w \in \Omega$ tal que $d(f, A_w) \leq r := |\pi^c|$ i sigui β una arrel de A_w tal que la distància $|\alpha - \beta|$ és mínima. Si fos $|\alpha - \beta| \geq \delta f$, per (7.1), seria

$$d(f, A_w) = \prod_{i=1}^{n} \max\{|\alpha - \beta|, |\beta - \beta_i|\} \geq \prod_{i=1}^{n} \max\{\delta f, |\beta - \beta_i|\} \geq \delta f |f'(\beta)| \geq |\pi^{(n+2j)/n}|,$$

però $|\pi^{(n+2j)/n}| > r$. Així doncs, $|\alpha - \beta| < \delta f$ i, pel lema de Krasner, $K = k(\alpha)$. □

7.3 Nombre d'extensions

Lema 7.3.1. *Sigui $t > j + 1$ un enter i $s := |\pi^{(n+j-1+t)/n}|$. Sigui $\#D_{E_{n,j}}(s)$ el nombre de discs tancats disjunts de radi s en $E_{n,j}$. Aleshores, el nombre d'elements de $K_{n,j}$ és*

$$\#K_{n,j} = \#D_{E_{n,j}}(s) \frac{n}{(q-1)q^{t-2}}.$$

Demostració. Sigui $\Pi_{n,j}$ la unió dels conjunts $\mathfrak{P} - \mathfrak{P}^2$, on $\mathfrak{P}$ recorre els ideals primers dels cossos de $K_{n,j}$. Definim una aplicació exhaustiva $\chi : \Pi_{n,j} \to E_{n,j}$ per $\chi(\alpha) := \mathrm{Irr}(\alpha, k)(X)$.

Sigui $u := |\pi^{t/n}|$, i siguin $\alpha, \beta \in \Pi_{n,j}$ tals que $|\alpha - \beta| \leq u$. Aleshores

$$|\alpha - \beta| \leq u = |\pi^{t/n}| < |\pi^{(j+1)/n}| \leq \delta\chi(\alpha),$$

com hem vist en la demostració de 7.2.3. Pel lema de Krasner, $k(\alpha) = k(\beta) \in K_{n,j}$. Ara,

$$d(\chi(\alpha), \chi(\beta)) = \prod_{i=1}^{n} \max\{|\alpha - \beta|, |\alpha - \alpha_i|\} \leq u|\chi'(\alpha)| = u|\pi^{(n+j-1)/n}| = s,$$

de manera que $\chi(D_\Pi(\alpha,u)) \subseteq D_{E_{n,j}}(\chi(\alpha),s)$, on $D_\Pi(\alpha,u)$ és el disc tancat de centre α i radi u en $\Pi_{n,j}$. Recíprocament, siguin $f \in E_{n,j}$, i α una arrel de f. Aleshores $f = \chi(\alpha)$ i $D_{E_{n,j}}(\chi(\alpha),s) \subseteq \chi(D_\Pi(\alpha,u))$. En efecte, siguin $g \in D_{E_{n,j}}(\chi(\alpha),s)$ i $\beta \in \Pi_{n,j}$ tals que $\chi(\beta) = g$. Llavors,

$$s \geq d(f,g) = \prod_{i=1}^{n} \max\{|\alpha-\beta|, |\alpha-\alpha_i|\} \geq |\alpha-\beta||f'(\alpha)| = |\alpha-\beta||\pi^{(n+j-1)/n}|$$

i $|\alpha-\beta| \leq u$. Així doncs, $D_{E_{n,j}}(\chi(\alpha),s) = \chi(D_\Pi(\alpha,u))$, per a tot $\alpha \in \Pi_{n,j}$.

L'aplicació χ és exhaustiva. A més, l'antiïmatge de $\chi(\alpha)$ són els conjugats de α sobre k i, en ser $t > j+1$, els discs tancats de radi u centrats en els conjugats de α són tots disjunts. Per tant,

$$\chi^{-1}(D_{E_{n,j}}(\chi(\alpha),s)) = \chi^{-1}(\chi(D_\Pi(\alpha,u))) = \bigcup_{i=1}^{n} D_\Pi(\alpha_i,u). \tag{7.4}$$

Atès que tots els elements del disc $D_\Pi(\alpha_i,u)$ generen la mateixa extensió, aleshores $D_\Pi(\alpha_i,u) \subseteq \mathfrak{P} - \mathfrak{P}^2$ per a algun $K \in K_{n,j}$, i el nombre de discs tancats disjunts de radi u en $\Pi_{n,j}$ ha de ser $\#K_{n,j}$ vegades el nombre de discs tancats disjunts en $\mathfrak{P} - \mathfrak{P}^2$. Calculem aquest nombre. Siguin $\alpha \in \mathfrak{P} - \mathfrak{P}^2$ i R un sistema de representants del cos residual de K, format per q elements. Per a tot $\beta \in \mathfrak{P} - \mathfrak{P}^2$, podem posar

$$\beta = a_1\alpha + a_2\alpha^2 + \cdots + a_{t-1}\alpha^{t-1} + A_t\alpha^t, \quad \text{amb } a_i \in R,\ a_1 \neq 0,\ v_{\mathfrak{P}}(A_t) \geq 0.$$

Si $\beta - \beta' = (A_t - A_t')\alpha^t$, aleshores $|\beta-\beta'| \leq |\pi^{t/n}| = u$. Per tant, només hem de considerar $q^{t-2}(q-1)$ elements. Siguin $\beta \neq \beta'$ i sigui j el primer índex tal que $a_j \neq a_j'$. Aleshores, $|\beta-\beta'| = |\pi^{j/n}||(a_j - a_j') + \pi(*)| = |\pi^{j/n}| > u$, si $j < t$. La igualtat (7.4) ens permet concloure que $\#K_{n,j}q^{t-2}(q-1) = n\#D_{E_{n,j}}(s)$. □

Lema 7.3.2. *El nombre de discs tancats disjunts de radi $r := |\pi^c|$ en $E_{n,j}$ ve donat per*

$$\#D_{E_{n,j}}(r) = \begin{cases} (q-1)q^{nc-n-j-1+\sum_{i=1}^{\lfloor a/e\rfloor} en/p^i} & si \quad b=0, \\ (q-1)^2 q^{nc-n-j-1+\sum_{i=1}^{\lfloor a/e\rfloor} en/p^i + \lfloor (j-\lfloor a/e\rfloor en-1)/p^{\lfloor a/e\rfloor+1}\rfloor} & si \quad b>0. \end{cases}$$

Demostració. És fàcil adonar-se que $\#R_{1,c}^* = (q-1)q^{c-2}$, $\#R_{l(i),c} = q^{c-l(i)}$, si $i \neq b$, i $\#R_{l(b),c}^* = (q-1)q^{c-l(b)-1}$. Per tant,

$$\#D_{E_{n,j}}(r) = \begin{cases} (q-1)^{c-2+(n-1)c-\sum_{i=1}^{n-1} l(i)} & \text{si} \quad b=0, \\ (q-1)^2 q^{c-2+(n-1)c-\sum_{i=1}^{n-1}(l(i)-1)} & \text{si} \quad b>0. \end{cases}$$

Només cal calcular la suma $\sum_{i=1}^{n-1} l(i)$. Tal i com es demostra en [21], els termes $l(i)$ es poden manipular per tal d'obtenir el resultat de l'enunciat. □

Amb aquests dos lemes obtenim directament el resultat següent.

Teorema 7.3.3 (Krasner)**.** *Sigui k una extensió finita de $\mathbb{Q}_p$, $\mathfrak{p}$ l'ideal primer de k, e l'índex de ramificació de l'extensió, i q el nombre d'elements del cos residual de k. Sigui $j = an+b$, amb $0 \leq b < n$, un enter que satisfà les condicions d'Ore. Aleshores, el nombre d'extensions totalment ramificades de k de grau n i discriminant $\mathfrak{p}^{n+j-1}$ és*

$$\#K_{n,j} = \begin{cases} nq^{\sum_{i=1}^{\lfloor a/e\rfloor} en/p^i} & si \quad b=0, \\ n(q-1)q^{\sum_{i=1}^{\lfloor a/e\rfloor} en/p^i + \lfloor (j-\lfloor a/e\rfloor en-1)/p^{\lfloor a/e\rfloor+1}\rfloor} & si \quad b>0. \end{cases}$$

7.4 Algoritme de Panayi per determinar les extensions

En [20], Pauli continua treballant sobre un cos $\mathfrak{p}$-àdic k per tal de trobar un conjunt minimal de polinomis generadors d'extensions totalment ramificades de grau p sobre k. Nosaltres ens reduïrem al cas en què $[k : \mathbb{Q}_p] = 1$. A l'hora de trobar aquest conjunt minimal, Pauli utilitza com a eina principal l'algoritme de Panayi, que se sosté sobre el resultat següent.

Lema 7.4.1. *Sigui K un cos $\mathfrak{p}$-àdic, A el seu anell de valoració discreta i π un uniformitzant. Sigui $f(X) = f_nX^n + \dots f_1X + f_0 \in A[X]$ i definim $v_\mathfrak{p}(f) := \min_{0\le i\le n}\{v_\mathfrak{p}(f_i)\}$, i $f^\# := f/\pi^{v_\mathfrak{p}(f)}$. Denotem amb una barra a sobre les reduccions dels elements de l'anell en el cos residual.*

(i) Sigui $\beta \in A$ tal que $\overline{\beta}$ és una arrel de $\overline{f}$, i sigui $g(X) := f(\pi X + \beta)$. Aleshores, $\deg(\overline{g^\#}) \le \deg(\overline{f^\#})$.

(ii) Si $\deg(\overline{f^\#}) = 0$, aleshores f no té cap arrel en A.

(iii) Si $\deg(\overline{f^\#}) = 1$, aleshores f té una arrel en A.

(iv) Si $\overline{f^\#}(X) = (X - \overline{\beta})^m h(X)$, on $\mathrm{mcd}(X - \overline{\beta}, h(X)) = 1$, i si $g(X) := f(\pi X + \beta)$, aleshores $\deg(\overline{g^\#}) \le m$.

Demostració. (i) Sigui $d = \deg(\overline{f^\#})$. Aleshores, $v_\mathfrak{p}(f_d) \le v_\mathfrak{p}(f_\nu)$, $\forall \nu \le d$, i $v_\mathfrak{p}(f_d) < v_\mathfrak{p}(f_\nu)$, $\forall \nu > d$. Ara,

$$g_i = \sum_{i=1}^{n} \binom{j}{i} f_j \pi^i \beta^{j-i}$$

i $v_\mathfrak{p}(g_d) = v_\mathfrak{p}(f_d) + d$ i $v_\mathfrak{p}(g_\nu) \ge v_\mathfrak{p}(f_d) + \nu$, $\forall \nu > d$. Així doncs, $\deg(\overline{g^\#}) \le \deg(\overline{f^\#})$.

(ii) És evident.

(iii) En ser $\deg(\overline{f^\#}) = 1$, aleshores $v_\mathfrak{p}(f_1^\#) = 0$ i $v_\mathfrak{p}(f_\nu^\#) \ge 1$, $\forall \nu > 1$. Així doncs, $f^{\#'}(\beta) \not\equiv 0 \pmod{\mathfrak{p}}$ i $f^\#(\beta) \equiv 0 \pmod{\mathfrak{p}}$. Per 3.4.1, $f^\#$ i f tenen una arrel en A.

(iv) Podem suposar que $f = f^\#$. Considerem el desenvolupament de Taylor

$$f(\pi X + \beta) = \sum_{i=0}^{n} \frac{f^{(i)}(\beta)}{i!} \pi^i X^i.$$

Com que $\overline{f}(X) = (X - \overline{\beta})^m h(X)$, ha de ser $v_\mathfrak{p}(f^{(m)}(\beta)/m!) = 0$, i $v_\mathfrak{p}(f^{(i)}(\beta)\pi^i/i!) \ge i > v_\mathfrak{p}((f^{(m)}(\beta)/m!)\pi^m) = m$ per a $i > m$, ja que $f^{(i)}(\beta)/i! \in A$. Per tant, $\deg(\overline{g^\#}) \le m$. □

Suposem que f té una arrel $\alpha \in A$, amb $\alpha \equiv \beta \pmod{\mathfrak{p}}$. Sigui $f_1(X) := f^\#(\pi X + \beta)$. En ser $\alpha \equiv \beta \pmod{\mathfrak{p}}$, podem posar $\alpha \equiv \beta + \beta_1\pi \pmod{\mathfrak{p}^2}$. A més, $\overline{f_1}(\beta_1) = \overline{f^\#}(\beta_1\pi + \beta) = \overline{f^\#}(\overline{\alpha}) = 0$. De la mateixa manera, el polinomi $f_2(X) := f_1^\#(\pi X + \beta_1)$, reduït mòdul $\mathfrak{p}$ té β_2 per arrel, on β_2 és tal que $\alpha \equiv \beta + \beta_1\ \pi + \beta_2\pi^2 \pmod{\mathfrak{p}^3}$. En efecte, $\overline{f_2}(\beta_2) = \overline{f_1^\#}(\beta_2\pi + \beta_1) = \overline{f^\#}(\beta_2\pi^2 + \beta_1\pi + \beta) = \overline{f^\#}(\overline{\alpha}) = 0$. Vist això, definim les successions $(f_\nu)_\nu$ i $(b_\nu)_\nu$ de la següent manera:

$$f_0 := f^\#, \quad b_0 := \beta, \quad f_{\nu+1}(X) := f_\nu^\#(\pi X + \beta_\nu), \quad b_{\nu+1} := \beta_{\nu+1}\pi^{\nu+1} + b_\nu;$$

on $\beta_\nu \in A$ és tal que $\overline{\beta}_\nu$ és una arrel de $\overline{f_\nu}$, si existeix. A cada pas de la successió, podem trobar una arrel de f – si, de fet, f té una arrel en A congruent amb β mòdul $\mathfrak{p}$ –, i b_ν és congruent amb aquesta arrel mòdul potències creixents de $\mathfrak{p}$. El lema següent ens assegura que, amb un nombre finit de passos, o bé $\overline{f}$ no té arrels en $A/\mathfrak{p}$, o bé $\deg(\overline{f_\nu}) \le 1$, de manera que les propietats (ii) i (iii) de 7.4.1 permeten concloure si f té o no arrels en A.

Lema 7.4.2. *Si* $\nu \geq v_{\mathfrak{p}}(\mathrm{disc}(f))$, *aleshores* $\deg(\overline{f_{\nu+1}}) \leq 1$.

Demostració. Tenim que

$$f_{\nu+1}(X) = f_{\nu}^{\#}(\pi X + \beta_\nu) = f^{\#}(\pi^{\nu+1}X + \pi^{\nu}\beta_\nu + \cdots + \pi\beta_1 + \beta) = f^{\#}(\pi^{\nu+1}X + b_\nu).$$

Considerem el desenvolupament de Taylor del polinomi

$$f(\pi^{\nu+1}X + b_\nu) = \sum_{i=0}^{n} \frac{f^{(i)}(b_\nu)}{i!}\pi^{(\nu+1)i}X^i.$$

Si fos $\deg(\overline{f_{\nu+1}}) \geq 2$, aleshores $v_{\mathfrak{p}}(f(b_\nu)) \geq 2(\nu+1)$ i $v_{\mathfrak{p}}(f'(b_\nu)) \geq \nu+1$. En particular, f tindria com a mínim una arrel doble mòdul $\mathfrak{p}^{\nu+1}$; però això no pot passar ja que el discriminant de f no és zero mòdul $\mathfrak{p}^{\nu+1}$. □

Algoritme 7.4.3 (Panayi)**.**

- *Llegim* K *i* f.
- *Definim el conjunt* $C := \{f^{\#}\}$.
- *Inicialitzem* $m = 0$.
- *Mentre* C *no és buit:*
  - *Per a tot polinomi* c *de* C*:*
    - *Traiem* c *del conjunt* C.
    - *Definim* $R := \{$ *arrels de* $\overline{c}$ *en* $\kappa_{\mathfrak{p}}\}$.
    - *Per a tot* β *de* R*:*
      - *Definim* $h(X) := c(\pi X + \beta)$.
      - *Substituïm* h *pel polinomi* $h^{\#}$.
      - *Si* $\deg \overline{h} = 1$, *aleshores* m *passa a ser* $m+1$.
      - *Si* $\deg \overline{h} > 1$, *aleshores afegim el polinomi* h *al conjunt* C.
- *Retornem el nombre* m *d'arrels de* f *en l'anell de valoració discreta* A *de* K.

Observació 7.4.4. Fent una petita modificació d'aquest algoritme, també podem trobar aproximacions per a les arrels de f. Enlloc d'aturar l'algoritme quan $\deg \overline{h} = 1$, el fem continuar i anem calculant les diferents arrels β de $\overline{h}$. D'aquesta manera, obtenim la successió de $(b_\nu)_\nu$ definida anteriorment que té per límit una arrel de f.

Ara ja podem utilitzar aquest algoritme de Panayi per trobar un conjunt minimal de polinomis generadors. Sigui $j = ap + b$ un nombre que satisfà les condicions d'Ore per a extensions ramificades de grau p sobre $\mathbb{Q}_p$. Aleshores, del teorema 7.3.3 es dedueix que

$$\#K_{p,j} = \begin{cases} p^2 & \text{si} \quad b = 0, \\ p(p-1) & \text{si} \quad b \neq 0. \end{cases} \tag{7.5}$$

Teorema 7.4.5. *Tota extensió de grau* p *sobre* $\mathbb{Q}_p$ *de discriminant* $p^{2p-1}\mathbb{Z}_p$ *està generada per una arrel d'exactament un dels polinomis*

$$\varphi_a(X) = X^p + p + ap^2, \quad amb \quad 0 \leq a \leq p-1.$$

Demostració. Siguin $\varphi_{a_1}, \varphi_{a_2}$ dos d'aquests polinomis, amb $a_1 \neq a_2$. Siguin α_1 una arrel de φ_{a_1}, α_2 una arrel de φ_{a_2} i A l'anell de valoració discreta de $\mathbb{Q}_p(\alpha_1)$. Mitjançant l'algoritme de Panayi veurem que $\mathbb{Q}_p(\alpha_1) \neq \mathbb{Q}_p(\alpha_2)$. En ser $\varphi_{a_2}(X) \equiv X^p \pmod{p\mathbb{Z}_p[X]}$, definim $f_1(X) := \varphi_{a_2}^{\#}(\alpha_1 X)$. Llavors,

$$\begin{aligned} \varphi_{a_2}(\alpha_1 X) &= \alpha_1^p X^p + p + a_2 p^2 = (-p - a_1 p^2) X^p + p + a_2 p^2, \\ f_1(X) &= (-1 - a_1 p) X^p + 1 + a_2 p \quad \equiv \quad -X^p + 1 \pmod{\alpha_1 A[X]}. \end{aligned}$$

Notem que, d'acord amb com hem definit $f^{\#}$, $f_1(X)$ hauria de ser $\varphi_{a_2}(\alpha_1 X)/\alpha_1^p$ enlloc de $\varphi_{a_2}(\alpha_1 X)/p$, però a l'hora d'aplicar l'algoritme de Panayi això no té cap influència. Així doncs, si definim $f_2(X) := f_1^{\#}(\alpha_1 X + 1)$, obtenim

$$\begin{aligned} f_1(\alpha_1 X + 1) &= (-1 - a_1 p)(\alpha_1 X + 1)^p + 1 + a_2 p \equiv p(X^p + a_2 - a_1) \pmod{p\alpha_1 A[X]}, \\ f_2(X) &= \frac{f_1(\alpha_1 X + 1)}{p} \quad \equiv \quad X^p + a_2 - a_1 \pmod{\alpha_1 A[X]}. \end{aligned}$$

Com que $A/\alpha_1 A \simeq \mathbb{F}_p$, definim $f_3(X) := f_2^{\#}(\alpha_1 X + a_1 - a_2)$. Llavors,

$$\begin{aligned} f_2(\alpha_1 X + a_1 - a_2) &\equiv p(a_2 - a_1)\alpha_1 \pmod{p\alpha_1^2 A[X]}, \\ f_3(X) = \frac{f_2(\alpha_1 X + a_1 - a_2)}{\alpha_1 p} &\equiv a_2 - a_1 \pmod{\alpha_1 A[X]}. \end{aligned}$$

En ser $a_1 \not\equiv a_2 \pmod{p}$, aleshores $\mathbb{Q}_p(\alpha_1) \neq \mathbb{Q}_p(\alpha_2)$. Atès que $\mathbb{Q}_p$ no conté les arrels p-èsimes de la unitat, amb la família de polinomis de l'enunciat obtenim $p \cdot p$ extensions diferents (tenim p polinomis i hem de considerar els p conjugats d'una arrel d'aquests polinomis), que, per (7.5), són totes les extensions de discriminant $p^{2p+1}\mathbb{Z}_p$ que hi ha. □

Teorema 7.4.6. *Tota extensió de grau p sobre $\mathbb{Q}_p$ de discriminant $p^{p+b-1}\mathbb{Z}_p$ està generada per una arrel d'exactament un dels polinomis*

$$\begin{cases} \varphi_{a,b}(X) = X^p + apX^b + p, & amb \quad 1 \leq a, b \leq p-1, \quad i \quad ab \neq (p-1)^2; \\ \varphi_a(X) = X^p - pX^{p-1} + ap^2 + p, & amb \quad 0 \leq a \leq p-1, \quad i \quad b = p-1. \end{cases}$$

Només les extensions generades per un polinomi de la segona família són de Galois.

Demostració. Per a $i = 1, 2$, considerem el polinomi $\varphi_i(X) := X^p + a_i p X^b + p + c_i p^2$, amb $a_i, b, c_i \in \mathbb{Z}$ tals que el polinomi és un dels de l'enunciat. Sigui α_i una arrel del polinomi φ_i, i sigui A l'anell de valoració discreta de $\mathbb{Q}_p(\alpha_1)$. Veurem que $\mathbb{Q}_p(\alpha_1) \neq \mathbb{Q}_p(\alpha_2)$. En ser $\varphi_2(X) \equiv X^p \pmod{\alpha_1 A[X]}$, definim $f_1(X) := \varphi_2^{\#}(\alpha_1 X)$. Llavors,

$$\begin{aligned} \varphi_2(\alpha_1 X) &= (-a_1 p\alpha_1^b - p - c_1 p^2) X^p + a_2 p \alpha_1^b X^b + p + c_2 p^2, \\ f_1(X) &= (-a_1 \alpha_1^b - 1 - c_1 p) X^p + a_2 \alpha_1^b X^b + 1 + c_2 p \;\equiv\; -X^p + 1 \pmod{\alpha_1 A[X]}. \end{aligned}$$

Ara,

$$f_1(\alpha_1 X + 1) \equiv \alpha_1^b (a_2 - a_1) + p(c_2 - c_1 + X^p) + a_2 b \alpha_1^{b+1} X \pmod{\alpha_1^{b+2} A[X]}.$$

L'algoritme de Panayi ens assegura que, per tal que φ_2 tingui una arrel en A, ha de ser $a_2 \equiv a_1 \pmod{p}$. Si $a_1 \not\equiv -1 \pmod{p}$ o $a_1 = a_2 = p - 1$, per tal que φ_1 i φ_2 siguin polinomis de l'enunciat ha de ser $c_1 = c_2 = 0$ i, conseqüentment, $\varphi_1 = \varphi_2$. Si

$a_1 = a_2 = -1$, ha de ser $b = p-1$ i, per tal que φ_2 tingui una arrel en A, ha d'existir un element $x \in \mathbb{F}_p$ tal que

$$c_2 - c_1 + x^p - (-1)(p-1)x \equiv 0 \pmod{p} \Leftrightarrow c_2 \equiv c_1 \pmod{p}$$

i hauria de ser $c_1 = c_2$. Notem que si $a_i = -1$, $a_j = p-1$ per a $\{i,j\} = \{1,2\}$, aleshores $b = p-1$ i un dels polinomis φ_1, φ_2 ja no seria de l'enunciat. D'aquesta manera, hem vist que arrels de polinomis de l'enunciat diferents generen extensions diferents.

Siguin ara α una arrel del polinomi φ_a i A l'anell d'enters de $\mathbb{Q}_p(\alpha)$. Hem de veure que $\mathbb{Q}_p(\alpha)$ conté totes les arrels de φ_a. Definim $f_1(X) := \varphi_a^{\#}(\alpha X)$ i $f_2^{\#}(\alpha X + 1)$. Aleshores,

$$\begin{aligned} f_1(\alpha X + 1) &= (\alpha^{p-1} - ap - 1)(\alpha X + 1)^p - \alpha^{p-1}(\alpha X + 1)^{p-1} + ap + 1 \\ &\equiv pX(X^{p-1} - 1) \pmod{\alpha p A[X]}, \end{aligned}$$

de manera que $f_2(X) \equiv X^p - X \pmod{\alpha A[X]}$, que té p arrels diferents en $A/\alpha A$. Si definim $f_3(X) := f_2^{\#}(\alpha X + \beta)$, per a cadascuna d'aquestes arrels β, es pot comprovar que $\overline{f}_3$ és de grau 1; per tant, φ_a té p arrels en A i l'extensió $\mathbb{Q}_p(\alpha)|\mathbb{Q}_p$ és de Galois.

En canvi, per als polinomis $\varphi_{a,b}$ el mateix algoritme de Panayi permet comprovar que cada arrel genera un cos diferent. Amb les famílies de polinomis de l'enunciat obtenim $p(p-1)$ extensions diferents que, per (7.5), són totes les que hi ha. □

Observacions 7.4.1. (1) Els polinomis dels teoremes 7.4.5 i 7.4.6 ja van ser trobats per Amano [1] l'any 1971. A més a més, descriu explícitament el cos de descomposició dels polinomis i dóna elements generadors del cos d'inèrcia i del cos fix per G_1.

(2) L'any 2003, Jones i Roberts en [13] descriuen una base de dades en línia creada per ells mateixos que, donat un primer p i un grau n (petits), dóna totes les extensions de grau n sobre $\mathbb{Q}_p$. A més a més, donat un polinomi mònic i separable de coeficients enters, identifica l'extensió que genera. Aquesta base de dades es troba en [14].

Amb tot això, estudiem ara les extensions ramificades de grau 5 sobre $\mathbb{Q}_5$, que sabem que vénen definides exactament pels polinomis

$$\begin{aligned} &X^5 + 5^2 a + 5, && \text{amb} \quad 0 \le a \le 4, \\ &X^5 - 5X^4 + 5^2 a + 5, && \text{amb} \quad 0 \le a \le 4, \\ &X^5 + 5aX^b + 5, && \text{amb} \quad 1 \le a, b \le 4, \quad ab \neq 16. \end{aligned}$$

7.5 Extensions d'ideal discriminant $5^9\mathbb{Z}_5$

Proposició 7.5.1. *Siguin π una arrel del polinomi $\varphi_a(X) = X^5 + 5^2 a + 5$, amb $0 \le a \le 4$, L el seu cos de descomposició, $G = \mathrm{Gal}(L|\mathbb{Q}_5)$ i G_i els grups de ramificació. Aleshores, $L = \mathbb{Q}_5(\pi, w)$, on w és una arrel cinquena primitiva de la unitat i*

$$G = G_{-1} = G_0 \simeq F_{20}, \quad G_1 \simeq C_5, \quad L^{G_1} = \mathbb{Q}_5(w).$$

Demostració. Sabem que $L = \mathbb{Q}_p(\pi, w)$, on w és una arrel cinquena primitiva de la unitat. Sigui $\Phi_5(X)$ el cinquè polinomi ciclotòmic. Com que $\Phi_5(X+1)$ és 5-Eisenstein, l'extensió $\mathbb{Q}_5(w)|\mathbb{Q}_5$ és totalment ramificada de grau 4 i, conseqüentment, l'extensió $L|\mathbb{Q}_5$ també és totalment ramificada, i de grau 20. D'aquesta manera, tenim que $G = G_{-1} = G_0 \simeq F_{20}$. Per 4.3.3, $5 \nmid \#G_0/G_1$ i G_1 és l'únic 5-subgrup de Sylow de G (perquè G_1 és normal en G). Així doncs, $G_1 \simeq C_5$. En ser $[L : \mathbb{Q}_5(w)] = 5$, també ha de ser $L^{G_1} = \mathbb{Q}_5(w)$. □

7.6 Extensions d'ideal discriminant $5^{4+b}\mathbb{Z}_5$, amb $b \neq 0$

Proposició 7.6.1. *Siguin π una arrel del polinomi $\varphi_a(X) = X^5 - 5X^4 + 5^2a + 5$, amb $0 \leq a \leq 4$, L el seu cos de descomposició, $G = \mathrm{Gal}(L|\mathbb{Q}_5)$ i G_i els grups de ramificació. Aleshores $L = \mathbb{Q}_5(\pi)$ i l'extensió $\mathbb{Q}_5(\pi)|\mathbb{Q}_5$ és cíclica de grau 5. A més a més,*

$$G = G_{-1} = G_0 = G_1 \simeq C_5.$$

Demostració. Només queda per veure que $G_1 \simeq C_5$, que és conseqüència de 4.3.3. □

A continuació, estudiem els cossos de descomposició dels polinomis $\varphi_{a,b}(X) = X^5 + 5aX^b + 5$, amb $1 \leq a, b \leq 4$, $ab \neq 16$.

Proposició 7.6.2. *Siguin π una arrel del polinomi $\varphi_{a,b}(X)$, $K = \mathbb{Q}_5(\pi)$ i L el seu cos de descomposició. Siguin G el grup de Galois del polinomi i G_i els grups de ramificació. Aleshores, existeix un element $\alpha \in L$ tal que $L = \mathbb{Q}_5(\pi, \alpha)$, $\alpha^4 \in \mathbb{Q}_5$ i $L^{G_1} = \mathbb{Q}_5(\alpha)$. A més, $G_1 \simeq C_5$ i*

$$\mathrm{Gal}(L|\mathbb{Q}_5) = \begin{cases} D_{2\cdot 5}, & si \quad (a,b) \in \{(1,4),(2,2),(3,2)\}, \\ F_{20}, & altrament. \end{cases}$$

Demostració. Com que l'extensió $L|\mathbb{Q}_5$ és salvatgement ramificada, G_1 no és el grup trivial i, com que és un 5-grup, ha de ser $\#G_1 = 5$; de manera que $G_1 \simeq C_5$ i l'extensió $L|L^{G_1}$ és cíclica de grau 5. A més a més, l'extensió $L^{G_1}|\mathbb{Q}_5$ és de Galois, perquè G_1 és un subgrup normal de G_{-1} i podem posar $L^{G_1} = \mathbb{Q}_5(\alpha)$ per a algun $\alpha \in L$ tal que $\alpha^4 \in \mathbb{Q}_5$, ja que $\mathrm{Gal}(L^{G_1}|\mathbb{Q}_5)$ és isomorf a un subgrup de C_4 i $\mathbb{Q}_5$ conté les arrels quartes de la unitat. En ser $[L : \mathbb{Q}_5(\alpha)] = 5$ i $\mathbb{Q}_5(\alpha) \subsetneq \mathbb{Q}_5(\pi, \alpha) \subseteq L$, aleshores $L = \mathbb{Q}_5(\pi, \alpha)$.

Calculem-ne ara el grup de Galois. Ja sabem que $G = G_{-1} \not\simeq C_5$ ja que l'extensió $\mathbb{Q}_5(\pi)|\mathbb{Q}_5$ no és de Galois. Per tant, només pot ser $G \simeq D_{2\cdot 5}$, si el discriminant de $\varphi_{a,b}$ és un quadrat de $\mathbb{Q}_5$; o $G \simeq F_{20}$, si no ho és. Tenint en compte el corol·lari 3.4.2 i que

$$\begin{aligned} &\mathrm{disc}(\varphi_{a,1}(X)) = 5^5(5^4 + 2^8a^5), \quad &&\mathrm{disc}(\varphi_{a,2}(X)) = 5^6(5^3 + 2^2 3^3 a^5), \\ &\mathrm{disc}(\varphi_{a,3}(X)) = 5^7(5^2 + 2^2 3^3 a^5), \quad &&\mathrm{disc}(\varphi_{a,4}(X)) = 5^8(5 + 2^8 a^5); \end{aligned}$$

s'obté el resultat de l'enunciat. □

El lema següent, que podem trobar demostrat en [5], permet determinar el grup d'inèrcia – i, de fet, tots els grups de ramificació – de la clausura galoisiana de $K|\mathbb{Q}_5$.

Lema 7.6.3. *Siguin p un nombre primer, $K|\mathbb{Q}_p$ una extensió totalment ramificada de grau p i L la clausura galoisiana de K. Denotem per $\Delta_{K|\mathbb{Q}_p}$ el discriminant de l'extensió $K|\mathbb{Q}_p$ i definim $t := \#(G_0/G_1)$. Aleshores, existeix un enter $d > 0$, amb $\mathrm{mcd}(d,t) = 1$ tal que*

$$v_p(\Delta_{K|\mathbb{Q}_p}) = (p-1)\left(1 + \frac{d}{t}\right).$$

Demostrar que existeix un enter $d > 0$ que satisfà la igualtat és prou senzill. És suficient considerar alguns resultats de 4.1 i el teorema 5.1.1. Per demostrar que d i t són coprimers, s'utilitzen resultats que es poden trobar en la secció 2 del capítol IV de [23], aprofundint una mica més en l'estudi dels grups de ramificació. D'aquest últim lema obtenim immediatament com són els grups d'inèrcia per a cada extensió.

Proposició 7.6.4. *Seguint amb les notacions de l'última proposició,*

$$G_0 = \begin{cases} C_5, & si \quad b = 4, \\ D_{2\cdot 5}, & si \quad b = 2, \\ F_{20}, & altrament. \end{cases}$$

8 Resolució per radicals de quíntiques en $\mathbb{Q}_p$

Utilitzem l'algoritme de Panayi per poder expressar les arrels de qualsevol polinomi de grau 5 irreductible sobre $\mathbb{Q}_p$ en funció d'expressions radicals sobre $\mathbb{Q}$.

8.1 Polinomis generadors resolubles per radicals sobre $\mathbb{Q}$

Fixem $\overline{\mathbb{Q}}_p$ una clausura algebraica de $\mathbb{Q}_p$. Hem vist que les extensions no ramificades de grau 5 sobre $\mathbb{Q}_p$ estan generades per una arrel (p^5-1)-èsima primitiva de la unitat i que les moderadament ramificades estan generades per una arrel d'un dels polinomis de la forma $X^5-\zeta^r p$, amb $0 \leq r \leq \mathrm{mcd}(p-1,5)-1$, i ζ una arrel $(p-1)$-èsima primitiva de la unitat. És a dir, que en tots dos casos, les extensions estan generades per elements algebraics que es poden resoldre per radicals sobre $\mathbb{Q}$. De fet, això és cert per a qualsevol extensió.

Proposició 8.1.1. *Sigui $K \subset \overline{\mathbb{Q}}_p$ una extensió de grau 5 sobre $\mathbb{Q}_p$ i sigui $\alpha \in K$ un element primitiu de l'extensió. Aleshores, existeix un polinomi $g(X) \in \mathbb{Q}[X]$ resoluble per radicals tal que, per a alguna de les seves arrels β, se satisfà que*

$$\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta), \quad i \quad |\alpha| = |\beta|.$$

Demostració. Pel lema de Krasner, podem suposar que α és arrel d'un polinomi $f(X)$ de grau 5 i de coeficients en $\mathbb{Q}$, irreductible sobre $\mathbb{Q}_p$. Sigui $f_{20}(X)$ el polinomi resolvent sèxtic de $f(X)$ que defineix Dummit. Si $f(X)$ és resoluble per radicals en $\mathbb{Q}$, prenem $g = f$. En cas contrari, $f_{20}(X)$ té una arrel p-àdica no racional, que anomenem θ.

Sabem que α es pot escriure com $\alpha = R(\theta)$, on R és una funció radical. Si $\tilde{\theta} \in \mathbb{Q}$ és una aproximació p-àdica prou acurada de θ, aleshores, en virtut del lema de Krasner, tenim que $\tilde{\alpha} = R(\tilde{\theta}) \in \mathbb{Q}_p(\alpha)$. A més a més, podem prendre $\tilde{\theta}$ de manera que $\mathbb{Q}_p(\tilde{\alpha}) = \mathbb{Q}_p(\alpha)$. En efecte, com que l'extensió $\mathbb{Q}_p(\alpha)|\mathbb{Q}_p$ és de grau primer, o bé $\tilde{\alpha} \in \mathbb{Q}_p$, o bé $\mathbb{Q}_p(\tilde{\alpha}) = \mathbb{Q}_p(\alpha)$. Suposem que, per a un nombre infinit de $\tilde{\theta}$, $\tilde{\alpha} \in \mathbb{Q}_p$. Aleshores, podem construir una successió $(\alpha_n)_{n\geq 1} \subset \mathbb{Q}_p$ tal que $\alpha_n \underset{n}{\longrightarrow} \alpha$. Com que $\mathbb{Q}_p$ és un cos complet, hauria de ser $\alpha \in \mathbb{Q}_p$ i arribem a una contradicció.

Per últim, només cal comprovar que podem prendre $\tilde{\theta}$ de manera que $|\alpha| = |\tilde{\alpha}|$, que és conseqüència del fet que, per a tota successió $(\alpha_n)_{n\geq 1} \subset \mathbb{Q}_p(\alpha)$ tal que $\alpha_n \underset{n}{\longrightarrow} \alpha$, se satisfà que $|\alpha_n| = |\alpha|$, per a tot n prou gran. □

Ara bé, aquest resultat no és eficient a l'hora de trobar un generador que sigui resoluble per radicals sobre $\mathbb{Q}$. Per a les extensions no ramificades ja n'hem trobat i, de fet, en [10], Gauss explica com resoldre per radicals les arrels de la unitat. Per a les moderadament ramificades, de la demostració del lema 6.2.1 deduïm que podem substituir els polinomis $X^5-\zeta^r p$ pels polinomis $X^5-a^r p$, on $a \in \{1,\ldots,p-1\}$ és una arrel primitiva mòdul p. Així doncs, només falta trobar polinomis de coeficients racionals i resolubles que generin totes les extensions de grau 5 ramificades sobre $\mathbb{Q}_5$. Els de la forma X^5+5^2a+5, amb $0 \leq a \leq 4$ són resolubles per radicals sobre $\mathbb{Q}$. Per tal de trobar-ne la resta, demostrem el resultat següent.

Proposició 8.1.2. *Sigui p un nombre primer i siguin $f(X), g(X) \in \mathbb{Z}_p[X]$ dos polinomis d'Eisenstein de grau p que generen extensions isomorfes sobre $\mathbb{Q}_p$. Si definim $v := v_p(\mathrm{disc}(f(X)) = v_p(\mathrm{disc}(g(X)))$, aleshores*

$$\frac{\mathrm{disc}(f(X))}{p^v} \equiv \frac{\mathrm{disc}(g(X))}{p^v} \pmod{p\mathbb{Z}_p}.$$

Demostració. Siguin π una arrel de f i α una arrel de g tals que $\mathbb{Q}_p(\pi) = \mathbb{Q}_p(\alpha)$. En virtut del corol·lari 2.1.8 i del lema 4.4.1, sabem que $\{1, \pi, \ldots, \pi^{p-1}\}$ i $\{1, \alpha, \ldots, \alpha^{p-1}\}$ són bases de l'anell d'enters $\mathbb{Z}_p[\pi]$ de $\mathbb{Q}_p(\pi)$, de manera que existeixen enters p-àdics $a_{i,j} \in \mathbb{Z}_p$ tals que

$$\begin{pmatrix} 1 \\ \pi \\ \vdots \\ \pi^{p-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ a_{0,1} & a_{1,1} & \ldots & a_{p-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0,p-1} & a_{1,p-1} & \ldots & a_{p-1,p-1} \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{p-1} \end{pmatrix}.$$

Sigui A aquesta matriu del canvi de base. Com que π i α són uniformitzants de $\mathbb{Z}_p[\pi]$, les igualtats $\pi^r = a_{0,r} + a_{1,r}\alpha + \cdots + a_{p-1,r}\alpha^{p-1}$, amb $1 \leq r \leq p-1$, comporten les congruències

$$a_{i,r} \equiv 0 \pmod{p\mathbb{Z}_p} \quad \forall i: \ 0 \leq i \leq r-1, \quad \pi^r \equiv a_{r,r}\alpha^r \pmod{\mathfrak{p}^{r+1}},$$

on $\mathfrak{p}$ és l'ideal primer generat per α. Ara bé, com que π també genera aquest ideal, existeix una unitat $u \in \mathbb{Z}_p[\pi]^\times$ tal que $\pi = u\alpha$, i l'última congruència equival a

$$u^r\alpha^r \equiv a_{r,r}\alpha^r \pmod{\mathfrak{p}^{r+1}} \quad \Leftrightarrow \quad u^r \equiv a_{r,r} \pmod{\mathfrak{p}}.$$

A més a més, podem escriure $u = u_0 + u_1\alpha + \ldots u_{p-1}\alpha^{p-1}$, amb $u_j \in \mathbb{Z}_p$, i $u^r \equiv a_{r,r} \pmod{\mathfrak{p}}$ si, i només si, $u_0^r \equiv a_{r,r} \pmod{p\mathbb{Z}_p}$. Desenvolupant el determinant de la matriu A per la primera columna, obtenim que

$$\begin{aligned} \det A &= \begin{vmatrix} a_{1,1} & \ldots & a_{p-1,1} \\ \vdots & \ddots & \vdots \\ a_{1,p-1} & \ldots & a_{p-1,p-1} \end{vmatrix} \equiv a_{1,1} \begin{vmatrix} a_{2,2} & \ldots & a_{p-1,2} \\ \vdots & \ddots & \vdots \\ a_{2,p-1} & \ldots & a_{p-1,p-1} \end{vmatrix} \pmod{p\mathbb{Z}_p} \\ &\equiv a_{1,1}a_{2,2} \begin{vmatrix} a_{3,3} & \ldots & a_{p-1,3} \\ \vdots & \ddots & \vdots \\ a_{3,p-1} & \ldots & a_{p-1,p-1} \end{vmatrix} \equiv a_{1,1}a_{2,2}\ldots a_{p-1,p-1} \pmod{p\mathbb{Z}_p}. \end{aligned}$$

Així doncs,

$$\det A \equiv u_0u_0^2 \ldots u_0^{p-1} \equiv u_0^{\sum_{n=1}^{p-1} n} \equiv u_0^{\frac{p(p-1)}{2}} \equiv (u_0^p)^{\frac{p-1}{2}} \equiv u_0^{\frac{p-1}{2}} \pmod{p\mathbb{Z}_p}$$

i $(\det A)^2 \equiv u_0^{p-1} \equiv 1 \pmod{p\mathbb{Z}_p}$. En ser

$$\operatorname{disc}(f(X)) = d(1, \pi, \ldots, \pi^{p-1}) = (\det A)^2 d(1, \alpha, \ldots, \alpha^{p-1}) = (\det A)^2 \operatorname{disc}(g(X)),$$

hem acabat. □

A l'hora de trobar els polinomis resolubles per radicals sobre $\mathbb{Q}$, ens interessa que siguin polinomis 5-Eisenstein per poder aplicar després l'algoritme de Panayi. Considerem el polinomi

$$f(X) = a_5X^5 + 5a_4X^4 + 5a_3X^3 + 5a_2X^2 + 5a_1X + 5a_0 \in \mathbb{Z}[X], \quad \text{amb} \quad 5 \nmid a_5, \quad 5 \nmid a_0.$$

Es pot comprovar que

$$v_5(\operatorname{disc}(f)) = \begin{cases} 5, & \text{si} \quad a_1 \not\equiv 0 \pmod 5, \\ 6, & \text{si} \quad a_1 \equiv 0 \pmod 5 \quad \text{i} \quad a_2 \not\equiv 0 \pmod 5, \\ 7, & \text{si} \quad a_1, a_2 \equiv 0 \pmod 5 \quad \text{i} \quad a_3 \not\equiv 0 \pmod 5, \\ 8, & \text{si} \quad a_1, a_2, a_3 \equiv 0 \pmod 5 \quad \text{i} \quad a_4 \not\equiv 0 \pmod 5. \end{cases}$$

A més a més, si definim $v := v_5(\mathrm{disc}(f))$, aleshores

$$\frac{\mathrm{disc}(f)}{5^v} \equiv \begin{cases} a_1 a_5^3 \pmod 5, & \text{si} \quad v = 5 \\ 3a_0 a_2 a_5^2 \pmod 5, & \text{si} \quad v = 6, \\ 3a_0^2 a_3 a_5 \pmod 5, & \text{si} \quad v = 7, \\ a_0^3 a_4 \pmod 5, & \text{si} \quad v = 8. \end{cases}$$

Fent el mateix per als polinomis generadors de les extensions, obtenim:

$$\frac{1}{5^5}\mathrm{disc}(X^5 + 5aX + 5) \equiv a \pmod 5, \qquad \frac{1}{5^6}\mathrm{disc}(X^5 + 5aX^2 + 5) \equiv 3a \pmod 5,$$
$$\frac{1}{5^7}\mathrm{disc}(X^5 + 5aX^3 + 5) \equiv 3a \pmod 5, \qquad \frac{1}{5^8}\mathrm{disc}(X^5 + 5aX^4 + 5) \equiv a \pmod 5,$$
$$\frac{1}{5^8}\mathrm{disc}(X^5 - 5X^4 + 5^2a + 5) \equiv 4 \pmod 5.$$

En virtut de la proposició 8.1.2, per tal que el polinomi f generi l'extensió que volem, hem d'imposar que

$$a_1 a_5^3 \equiv a, \quad a_0 a_2 a_5^2 \equiv a, \quad a_0^2 a_3 a_5 \equiv a, \quad a_0^3 a_4 \equiv a \quad \text{o} \quad a_0^3 a_4 \equiv 4 \pmod 5.$$

Per trobar aquests polinomis $f(X) \in \mathbb{Z}[X]$ resolubles per radicals sobre $\mathbb{Q}$, fem córrer els coeficients a_i de f de -10 a 10, imposant totes les condicions necessàries que hem vist. Quan el polinomi resolvent $f_{20}(X)$, a més, té una arrel racional, el polinomi f és un dels polinomis que busquem.

Per a les extensions generades per arrels de polinomis diferents de $X^5 - 5X^4 + 5^2a + 5$, la proposició 8.1.2 ens assegura que n'hi ha prou amb aquest càlcul del discriminant per trobar un polinomi per a cada classe de conjugació de les extensions. En cas que l'extensió estigui generada per una arrel d'un dels polinomis $X^5 - 5X^4 + 5^2a + 5$, haurem de trobar polinomis diferents (per a $0 \leq a \leq 4$) i aplicar l'algoritme de Panayi per saber quina de les classes de conjugació de les extensions generen.

D'aquesta manera, obtenim la següent llista de polinomis resolubles per radicals sobre $\mathbb{Q}$, que generen totes les extensions que ens falten:

$$\begin{aligned}
X^5 + 5X + 5 &\sim X^5 + 5X^3 + 5X + 5, \\
X^5 + 10X + 5 &\sim 2X^5 + 15X^4 + 40X^3 + 40X^2 + 20X + 10, \\
X^5 + 15X + 5 &\sim 2X^5 - 10X^4 - 45X - 35, \\
X^5 + 20X + 5 &\sim X^5 + 10X^3 + 20X + 5, \\
X^5 + 5X^2 + 5 &\sim X^5 - 10X^3 + 20X^2 - 25X + 20, \\
X^5 + 10X^2 + 5 &\sim X^5 + 5X^3 + 10X^2 + 5, \\
X^5 + 15X^2 + 5 &\sim X^5 + 5X^4 + 30X^2 + 40, \\
X^5 + 20X^2 + 5 &\sim X^5 - 5X^3 + 30X^2 - 25X + 20, \\
X^5 + 5X^3 + 5 &\sim X^5 + 20X^3 + 25X^2 + 25X - 10, \\
X^5 + 10X^3 + 5 &\sim X^5 + 10X^3 + 5, \\
X^5 + 15X^3 + 5 &\sim X^5 + 5X^4 + 15X^3 + 25X^2 + 25X + 5, \\
X^5 + 20X^3 + 5 &\sim X^5 + 5X^4 - 45X^3 - 250X^2 + 25X - 15,
\end{aligned}$$

$$
\begin{aligned}
X^5+5X^4+5 &\sim X^5-10X^4+25X^2-35,\\
X^5+10X^4+5 &\sim X^5+10X^4-50X^3-175X^2+200X-20,\\
X^5+15X^4+5 &\sim X^5-10X^4+50X^3-75X^2-75X-20,\\
X^5-5X^4+5 &\sim X^5-5X^4+25X^2-25X+5,\\
X^5-5X^4+30 &\sim X^5-10X^4-75X^3+200X-40,\\
X^5-5X^4+55 &\sim X^5-15X^4-175X^3+175X^2-10,\\
X^5-5X^4+80 &\sim X^5-20X^4-75X^3-50X^2+50X+45,\\
X^5-5X^4+105 &\sim X^5-5X^4+100X-20.
\end{aligned}
$$

8.2 Exemples

Exemple 8.2.1 (*Cas moderadament ramificat).* Considerem el polinomi

$$f(X)=X^5-121X+11 \quad \text{sobre} \quad \mathbb{Q}_{11}.$$

Veiem primer que aquest polinomi no és resoluble per radicals sobre $\mathbb{Q}$. És fàcil comprovar que té exactament dues arrels complexes no reals, de manera que el seu grup de Galois G conté una transposició. En ser un polinomi 11-Eisenstein, és irreductible sobre $\mathbb{Q}$ i, per tant, el seu grup de Galois també conté un 5-cicle. També és senzill demostrar que el grup simètric S_5 està generat per una transposició i un 5-cicle qualssevol, de manera que $G=S_5$ i f no és resoluble per radicals sobre $\mathbb{Q}$.

Sigui $\alpha\in\overline{\mathbb{Q}}_{11}$ una arrel de f. Com que f és un polinomi 11-Eisenstein, l'extensió $\mathbb{Q}_{11}(\alpha)|\mathbb{Q}_{11}$ és totalment ramificada i, per tant, està generada per alguna arrel d'un dels polinomis X^5-2^r11, amb $0\leq r\leq 4$. L'algoritme de Panayi ens permet identificar que el polinomi és X^5-11. Per a una arrel π d'aquest polinomi el mateix algoritme de Panayi ens permet trobar la següent aproximació de α:

$$
\begin{aligned}
\alpha \;\equiv\;& 2\pi+10\pi^6+8\pi^7+4\pi^{11}+\pi^{13}+9\pi^{16}+9\pi^{17}+3\pi^{18}+7\pi^{19}+\pi^{21}+9\pi^{22}+9\pi^{23}\\
+\;& 7\pi^{24}+2\pi^{26}+3\pi^{27}+\pi^{28}+10\pi^{29}+10\pi^{31}+7\pi^{33}+5\pi^{34}+6\pi^{36}+2\pi^{37}+4\pi^{38}\\
+\;& 6\pi^{39}+\pi^{42}+4\pi^{44}+5\pi^{46}+2\pi^{47}+9\pi^{48}+2\pi^{49} \pmod{\pi^{50}\mathbb{Z}_{11}[\pi]},
\end{aligned}
$$

i tenint en compte que $\pi^5=11$, aleshores, mòdul $11^{10}\mathbb{Z}_{11}[\pi]$,

$$
\begin{aligned}
\alpha \;\equiv\;& (2+10\cdot 11+4\cdot 11^2+9\cdot 11^3+11^4+2\cdot 11^5+10\cdot 11^6+6\cdot 11^7+5\cdot 11^9)\pi\\
+\;& (8\cdot 11+9\cdot 11^3+9\cdot 11^4+3\cdot 11^5+2\cdot 11^7+11^8+2\cdot 11^9)\pi^2\\
+\;& (11^2+3\cdot 11^3+9\cdot 11^4+11^5+7\cdot 11^6+4\cdot 11^7+9\cdot 11^9)\pi^3\\
+\;& (7\cdot 11^3+7\cdot 11^4+10\cdot 11^5+5\cdot 11^6+6\cdot 11^7+4\cdot 11^8+2\cdot 11^9)\pi^4.
\end{aligned}
$$

Així, si $w=(\sqrt{-10-2\sqrt{5}}+\sqrt{5}-1)/4$ és una arrel cinquena primitiva de la unitat, per a cada $\pi=\sqrt[5]{11}w^i$, amb $i=0,1,2,3,4$, podem obtenir aproximacions de cadascuna de les 5 arrels de f expressada com una $\mathbb{Q}_p$-combinació lineal d'expressions radicals sobre $\mathbb{Q}$.

Exemple 8.2.2 (*Cas salvatgement ramificat).* Considerem el polinomi

$$f(X)=X^5+5X^3+5 \quad \text{sobre} \quad \mathbb{Q}_5.$$

El polinomi resolvent de grau 6 que defineix Dummit és $f_{20}(X)=X^6+15\,625X^3-10\,390\,625X-3\,906\,250$, que no té arrels racionals. Per tant, el polinomi no és resoluble

per radicals sobre $\mathbb{Q}$. Ja hem vist que l'extensió generada per una arrel α de f coincideix amb l'extensió generada per alguna arrel π del polinomi $X^5+20X^3+25X^2+25X-10$. Com abans, l'algoritme de Panayi ens permet trobar la següent aproximació de α:

$$\begin{aligned}\alpha &\equiv 2\pi+3\pi^3+3\pi^4+2\pi^5+4\pi^6+4\pi^7+2\pi^8+\pi^9+3\pi^{11}+4\pi^{12}+3\pi^{14}+2\pi^{15}\\ &+ \pi^{16}+4\pi^{19}+4\pi^{22}+4\pi^{24}+2\pi^{25}+\pi^{26}+2\pi^{27}+3\pi^{28}+\pi^{29}+3\pi^{30}+2\pi^{31}\\ &+ 4\pi^{33}+4\pi^{34}+2\pi^{35}+2\pi^{36}+2\pi^{37}+3\pi^{39}+\pi^{40}+2\pi^{43}+2\pi^{44}+3\pi^{45}+2\pi^{46}\\ &+ \pi^{47}+\pi^{48}+4\pi^{49} \pmod{\pi^{50}\mathbb{Z}_{11}[\pi]},\end{aligned}$$

i, tenint en compte que $\pi^5+20\pi^3+25\pi^2+25\pi-10=0$, aleshores, mòdul $5^{10}\mathbb{Z}_5[\pi]$,

$$\begin{aligned}\alpha &\equiv (4\cdot 5+3\cdot 5^2+2\cdot 5^3+2\cdot 5^4+2\cdot 5^5+5^6+2\cdot 5^7+3\cdot 5^8+3\cdot 5^9)\\ &+ (2+3\cdot 5+5^3+5^4+4\cdot 5^5+4\cdot 5^6+2\cdot 5^8+3\cdot 5^9)\pi\\ &+ (3\cdot 5+3\cdot 5^2+2\cdot 5^3+4\cdot 5^4+3\cdot 5^9)\pi^2\\ &+ (3+5+5^3+3\cdot 5^5+2\cdot 5^6+5^7+5^9)\pi^3\\ &+ (3+5+2\cdot 5^2+3\cdot 5^3+2\cdot 5^4+3\cdot 5^5+2\cdot 5^6+2\cdot 5^7+4\cdot 5^8+4\cdot 5^9)\pi^4.\end{aligned}$$

Ara, amb les fórmules de Faggal i Lazard, obtenim que les arrels del polinomi $X^5+20X^3+25X^2+25X-10$ són

$$\frac{w^i r_1+w^{2i}r_2+w^{3i}r_3+w^{4i}r_4}{5}, \quad \text{amb} \quad 0\le i\le 4,$$

on $w=(\sqrt{-10-2\sqrt{5}}+\sqrt{5}-1)/4$ és una arrel cinquena primitiva de la unitat, i

$$\begin{aligned}r_1 &= \sqrt[5]{\frac{5+4\sqrt{17}+\sqrt{5(85+8\sqrt{17})}}{2}},\ r_4=\frac{-50}{r_1},\\ r_2 &= \frac{5(-1+5\sqrt{17})r_1^2+(5+\sqrt{17})r_4^3}{2\cdot 5^2\sqrt{5(85+8\sqrt{17})}},\ r_3=\frac{-(5+\sqrt{17})r_1^3-5(-1+5\sqrt{17})r_4^2}{2\cdot 5^2\sqrt{5(85+8\sqrt{17})}}.\end{aligned}$$

Si substituïm aquestes expressions per π en l'aproximació de α, obtenim aproximacions per a les cinc arrels de f expressades com $\mathbb{Q}_p$-combinacions lineals d'expressions radicals sobre $\mathbb{Q}$.

Exemple 8.2.3 (*Cas no ramificat)*. Considerem el polinomi

$$f(X)=X^5+2X+1 \quad \text{sobre} \quad \mathbb{Q}_3.$$

Aquest polinomi és irreductible sobre $\mathbb{Q}$, i el seu polinomi resolvent f_{20} és $X^6+16X^5+160X^4+1\,280X^3+6\,400X^2+13\,259X-2\,366$, que no té arrels racionals. Per tant, el polinomi no és resoluble per radicals sobre $\mathbb{Q}$. Sigui α una arrel de f. Com que $\operatorname{disc}(f)\in\Delta_{\mathbb{Q}_3(\alpha)|\mathbb{Q}_3}$ i $3\nmid\operatorname{disc}(f)=11\,317$, aleshores l'ideal generat per 3 no divideix $\Delta_{\mathbb{Q}_3(\alpha)|\mathbb{Q}_3}$ i l'extensió $\mathbb{Q}_3(\alpha)|\mathbb{Q}_3$ és no ramificada.

Com hem destacat en l'observació 6.1.1, atès que $11\mid 3^5-1$ i $11\nmid 2$, si ζ és una arrel onzena primitiva de la unitat, aleshores l'extensió $\mathbb{Q}_3(\zeta)|\mathbb{Q}_3$ és l'extensió no ramificada de grau 5 sobre $\mathbb{Q}_p$. Amb l'algoritme de Panayi es comprova que f no té arrels en $\mathbb{Q}_3$ i que $\alpha\in\mathbb{Q}_3(\zeta)$, de manera que $[\mathbb{Q}_3(\alpha):\mathbb{Q}_3]=5$ i el polinomi f és irreductible sobre $\mathbb{Q}_3$.

Per trobar l'expressió de α, hem de considerar el polinomi irreductible de ζ sobre $\mathbb{Q}_3$. Notem que

$$\phi_{11}(X) \equiv (X^5 + 2X^3 + X^2 + 2X + 2)(X^5 + X^4 + 2X^3 + X^2 + 2) \pmod 3,$$

i podem suposar que la reducció de ζ a $\mathbb{F}_{3^5}$ és arrel del primer polinomi. La demostració del lema de Hensel, que podem trobar en [27], ens permet construir el polinomi de grau 5 irreductible sobre $\mathbb{Q}_3$ que té ζ per arrel. De fet, el programa PARI [19] té un algoritme implementat que permet obtenir una aproximació tan bona com vulguem d'aquest irreductible:

$$\begin{aligned} g(X) &:= \operatorname{Irr}(\zeta, \mathbb{Q}_3)(X) \equiv X^5 + (3 + 3^2 + 2\cdot 3^2 + 2\cdot 3^4 + 2\cdot 3^6 + 3^8 + 2\cdot 3^9)X^4 - X^3 \\ &\quad + X^2 + (2 + 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 2\cdot 3^6 + 3^8 + 2\cdot 3^9)X - 1 \pmod{3^{10}\mathbb{Z}_3}. \end{aligned}$$

Si denotem per A l'anell de valoració discreta de $\mathbb{Q}_3(\zeta)$, implementant l'algoritme de Panayi amb aquesta aproximació de g, trobem:

$$\begin{aligned} \alpha &\equiv (2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^5 + 2\cdot 3^6 + 3^7 + 3^8 + 3^9) + (3^3 + 2\cdot 3^4 + 3^5 + 3^6 + 2\cdot 3^9)\zeta \\ &+ (2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 2\cdot 3^5 + 2\cdot 3^7 + 3^9)\zeta^2 + (1 + 2\cdot 3^2 + 3^4 + 3^5 + 3^7 + 3^8)\zeta^3 \\ &+ (2 + 3 + 2\cdot 3^2 + 3^3 + 3^5 + 2\cdot 3^6 + 3^7 + 2\cdot 3^8)\zeta^4 \pmod{3^{10}A}. \end{aligned}$$

Ara, ens proposem expressar ζ per radicals. Per fer-ho, descomponem el polinomi $\Phi_{11}(X)$ sobre $\mathbb{Q}(\sqrt{\operatorname{disc}(\Phi_{11})})$ i obtenim:

$$\begin{aligned} \Phi_{11}(X) &= \left(X^5 + \frac{1+\sqrt{-11}}{2}X^4 - X^3 + X^2 - \frac{1-\sqrt{-11}}{2}X - 1\right) \\ &\quad \left(X^5 + \frac{1-\sqrt{-11}}{2}X^4 - X^3 + X^2 - \frac{1+\sqrt{-11}}{2}X - 1\right) \end{aligned}$$

i, com que $\sqrt{-11} \in \mathbb{Q}_3$, prenent una determinació de l'arrel quadrada adequada, aleshores el primer factor, que anomenem $h(X)$, es correspon amb $g(X)$. Les fórmules de Faggal i Lazard ens permeten resoldre per radicals el polinomi $h(X - (1+\sqrt{-11})/10)$ per obtenir $\zeta = (r_1 + r_2 + r_3 + r_4)/5 - (1+\sqrt{-11})/10$, amb

$$\begin{aligned} r_1 &= \sqrt[5]{\frac{363 + 55\sqrt{5} + 98\sqrt{-11} + 30\sqrt{5}\sqrt{-11}}{4} + \frac{d}{2}}, \quad r_4 = -\frac{\sqrt{-11}(-1+\sqrt{5})}{2r_1}, \\ r_2 &= \frac{h_4 r_1^2 - h_3 r_4^3}{d}, \quad r_3 = \frac{h_3 r_1^3 - h_4 r_4^2}{d}, \quad h_3 = \frac{-33 - 11\sqrt{5} - 7\sqrt{-11} - 9\sqrt{5}\sqrt{-11}}{4}, \\ h_4 &= \frac{33 - 33\sqrt{5} - 75\sqrt{-11} - 5\sqrt{5}\sqrt{-11}}{4}, \\ d &= 5\sqrt{\frac{11(-15 - 45\sqrt{5} + 140\sqrt{-11} + 68\sqrt{5}\sqrt{-11})}{2}}. \end{aligned}$$

Com que $\operatorname{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) = \langle \omega : \zeta \mapsto \zeta^2 \rangle$, aleshores $\mathbb{Q}(\zeta)^{\langle \omega^2 \rangle}$ és l'únic subcòs quadràtic de $\mathbb{Q}(\zeta)$ i les altres arrels de f s'obtenen substituint ζ per ζ^i, amb $i = 3, 4, 5, 9$ en l'expressió de α.

Referències

[1] Amano, S.: *Eisenstein equations of degree p in a* $\mathfrak{p}$*-adic field*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 18, 1-21.

[2] Cantor, D. G.; Gordon, D.: *Factoring polynomials over p-adic fields*, *Proceedings of ANTS IV*, LNCS **1838**, pàg. 185-208, Springer-Verlag, Berlin, 2000.

[3] Cassels, J. W. S.: *Local Fields*, Student Texts, Vol. 3, London Math. Soc., Cambridge Univ. Press, Cambridge, 1986.

[4] Cox, D.; Little, J.; O'Shea, D.: *Ideals, Varieties, and Algorithms: An introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, 4th edition, Springer, Cham, 2015.

[5] Doud, Darrin.: *Wild ramification in number field extensions of prime degree*, Archiv der Mathematik 81, pàg. 646-649, 2003.

[6] Dummit, D.S.; Foote, R. M.: *Abstract Algebra*, Prentice-Hall, New York, 1990.

[7] Dummit, D. S.: *Solving solvable quintics*, *Math. Comp.*, **57**, 387-401, 1991.

[8] Dummit, D. S.: `http://www.emba.uvm.edu/~ddummit/quintics/quintics.html`. Última consulta: gener de 2016.

[9] Faggal, A.; Lazard, D.: *Solving Quintics and Septics by Radicals*, *IJSRP*, Vol. 4, Issue 12, desembre de 2014.

[10] Gauss, C. F.: *Disquisicions Aritmètiques*, traducció i pròleg de G. Pascual, IEC, Barcelona, 1996.

[11] Gouvea, F.: *p-adic Numbers: An Introduction*, Universitext, Springer-Verlag, Berlin, 1993.

[12] Hasse, H.: *Number Theory*, Springer-Verlag, Berlin, 1980.

[13] Jones, J.; Roberts, D.: *A database of local fields*, `arXiv:math/0309309v1[math.NT]`, setembre de 2003.

[14] Jones, J.; Roberts, D.: `http://math.la.asu.edu/~jj/localfields/`.
Última consulta: desembre de 2015.

[15] Krasner, M.: *Nombre des extensions d'un degré donné d'un corps p-adique*, C. R. Acad. Sc. Paris **254**, **255**, 1962.

[16] Lazard, D.: *Solving Quintics by Radicals*, *The Legacy of Niels Hendrik Abel*, pàg. 207-225, Springer, Berlin, 2004.

[17] Lang, S.: *Algebraic Number Theory*, Addison-Wesley, Reading, 1970.

[18] Neukirch, J.: *Algebraic Number Theory*, translated by N. Schappacher, Grundlehren der Mathematischen Wissenschaften 322, Springer-Verlag, Berlin, 1999.

[19] PARI/GP, version `2.7.5`, Bordeaux, 2015.
`http://pari.math.u-bordeaux.fr/`. Última consulta: gener de 2016.

[20] Pauli, S.: *Efficient Enumeration of Extensions of Local Fields with Bounded Discriminant*, tesi doctoral, Montreal, 2001.

[21] Pauli, S.; Roblot, X-F.: *On the computation of all extensions of a p-adic field of a given degree*, *Math. Comp.*, **70** (236), pàg. 1641-1659, 2001.

[22] Ribenboim, P.: *L'arithmétique des corps*, Hermann, Paris, 1972.

[23] Serre, J-P.: *Corps Locaux*, Hermann, Paris, 1962.

[24] Tignol, J-P.:*Galois' Theory of Algebraic Equations*, World Scientific, Singapore, 2001.

[25] Travesa, A.: *Teoria de Nombres*, `https://atlas.mat.ub.edu/personals/travesa/`. Última consulta: gener de 2016.

[26] Travesa, A.: *Curs d'Àlgebra*, `https://atlas.mat.ub.edu/personals/travesa/`. Última consulta: gener de 2016.

[27] Weiss, E.: *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

[28] Wolfram Research, Inc.: *Mathematica*, version `10.3`, Champaign, 2015.