Pub. Mat. UAB
Vol. 27 Nº 1 Març 1983

SOBRE L'ÍNDEX D'UN COS DE NOMBRES*

Enric Nart

ÍNDEX

*Memòria presentada a la Secció de Matemàtiques de la Universitat Autònoma de Barcelona per optar al titol de Doctor en Ciències Matemàtiques, realitzada sota la direcció del Doctor Pascual Llorente.

Pròleg.

L'índex d'un cos de nombres K d'anell d'enters A es defineix com:

$$i(K) = \text{m.c.d.}\{i(\theta)/\theta \in A \text{ primitiu}\},$$

on $i(\theta)=\text{card}\{A/\mathbb{Z}[\theta]\}$ és l'índex de l'enter θ i el terme "primitiu" té el sentit de generador del cos, és a dir, $K=\mathbb{Q}(\theta)$.

L'objectiu d'aquesta memòria és estudiar aquest nombre natural associat a tot cos de nombres, posant èmfasi en dues qüestions: la recerca d'invariants de K que el caracteritzin i la possibilitat de calcular el seu valor. Podem dividir l'estudi de i(K) en dos problemes: determinar quins primers $p\in\mathbb{Z}$ poden dividir-lo i després, si $p|i(K)$ determinar l'exponent $i_p(K)$ amb que el divideix. Un primer dividirà i(K) si i només si divideix tots els $i(\theta)$, per aquest motiu aquests primers foren anomenats "gemeinsamer ausserwesentlichen Diskriminantenteiler"; nosaltres els anomenarem *divisors comuns dels índexs*, abreviat d.c.i.. El problema de determinar els d.c.i. té una solució ben coneguda; la comentarem al Capítol 0. La segona qüestió és pròpiament el problema central que tractem en aquestes pàgines.

La memòria està subdividida en cinc capítols numerats del 0 al 4. El primer capítol està dedicat a fer un breu repàs històric dels problemes que estan connectats amb l'índex. En una primera part mostrem com el problema de determinar la possible existència de cossos de nombres amb $i(K)>1$ està lligat amb l'origen mateix de la teoria algebraica de nombres. Després fem una expo-

sició de l'estat actual dels resultats que concerneixen $i_p(K)$ per tal de centrar clarament el punt de partida de les nostres recerques. Per un breu resum del contingut dels altres capítols remitim al lector a les primeres línies de cadascun d'ells.

Tots els resultats etiquetats amb n.m, $n>0$, són originals excepte els Lemes 1.4, 2.2 i 3.1 i probablement les Proposicions 1.1 i 4.6. Les referències són donades de la forma [autor,data]; remarquem que la data és la de la publicació del treball concret citat a la llista final de referències i no correspon, a vegades, a la data original en que fou obtingut el resultat en qüestió. Adjuntem al final una llista dels símbols utilitzats, en ordre d'aparició. També incluim un índex terminològic dels termes menys usuals que emprearem. No obstant, donarem a continuació algunes de les notacions que seran fixes al llarg de tota la memòria.

Si L és un cos i $f(X),g(X)\in L[X]$, denotarem R(f,g) la seva resultant. Si M és una extensió finita de L i $\theta\in M$ denotarem per $Irr(\theta,L)$ el seu polinomi minimal sobre L.

Si θ és un enter algebraic sobre $\mathbb{Q}$ i $f(X)=Irr(\theta,\mathbb{Q})$ parlarem sempre que ens convingui de l'índex de f(X) en comptes de l'índex de θ, i ho denotarem i(f).

Siguin θ un enter algebraic sobre $\mathbb{Q}$, $f(X)=Irr(\theta,\mathbb{Q})$, $g(X)$, $h(X)\in\mathbb{Q}[X]$ i $m\in\mathbb{Z}$. Si $p\in\mathbb{Z}$ és un primer denotarem:

$$i_p(\theta),\ i_p(f),\ R_p(g,h),\ v_p(m),$$

per indicar la potència amb que p divideix $i(\theta)$, i(f), R(g,h) i m respectivament.

Sigui $p\in\mathbb{Z}$ un primer. Denotarem $\mathbb{Q}_p$, $\mathbb{Z}_p$ el cos dels nombres

p-àdics i el seu anell d'enters respectivament. $\mathbb{F}_q$ denotarà el cos finit de q elements, si $q=p^r$. Sempre suposarem sense fer-ne menció explícita que treballem en unes clàusures algebraiques Ω i $\bar{\Omega}$ de $\mathbb{Q}_p$ i $\mathbb{F}_p$ respectivament. Si L és una extensió finita de $\mathbb{Q}_p$, $\mathbb{Q}_p \subset L \subset \Omega$, denotarem A_L l'anell d'enters, P_L l'ideal primer de A_L i v_{P_L} la valoració associada. També denotarem $f(L/\mathbb{Q}_p)$ i $e(L/\mathbb{Q}_p)$ el grau residual i índex de ramificació de L. $\bar{L}$ denotarà el cos residual A_L/P_L que identificarem amb l'únic subcos de $\bar{\Omega}$ de $p^{f(L/\mathbb{Q}_p)}$ elements. Finalment, donat un enter algebraic sobre $\mathbb{Q}_p$, $\theta \in \Omega$, denotarem $v_p(\theta) = v_{P_L}(\theta)/e(L/\mathbb{Q}_p)$ essent L qualsevol extensió finita de $\mathbb{Q}_p$ que contingui θ. Denotarem també $\bar{\theta}$ l'element de $\bar{\Omega}$ obtingut prenent classe mòdul P_L. És clar que $v_p(\theta)$ i $\bar{\theta}$ no depenen de L.

He d'agrair moltes coses a en Pascual Llorente en relació amb aquesta memòria; no les enumeraré pas. Del que sí que m'agradaria deixar constància és de que el treball efectuat al seu costat en l'etapa immediatament anterior ha estat decisiu en la meva formació com a matemàtic.

Capítol 0. Breu història dels antecedents del problema

§1. El paper de l'índex en la construcció de la teoria dels ideals

Intentant provar el Teorema de Fermat, Kummer introdueix l'any 1846 el concepte de "nombre ideal" en un cos ciclotòmic per tal de tenir descomposició única en producte de primers en els anells d'enters d'aquests cossos. A mesura que la teoria dels nombres ideals es va donant a conèixer provoca una gran admiració en tots els medis científics de l'època i els seus resultats són tan espectaculars que l'extensió d'aquesta teoria a tots els cossos de nombres és considerat, sense discussió, l'objectiu prioritari dels teoristes de nombres d'aleshores. En els següents anys són nombrosíssims els matemàtics que ho intenten, de molt diverses maneres, i amb resultats parcials més o menys acceptables. Qui ho aconsegueix plenament és Dedekind.

El 1871, a la segona edició de les "Vorlesungen über Zahlentheorie" de Dirichlet, Dedekind ja desenvolupa la teoria abstracta dels ideals que coneixem avui en dia. La teoria de Dedekind introdueix a l'anell d'enters A de qualsevol cos de nombres K una estructura aritmètica (la que coneixem avui amb el nom de domini de Dedekind): tot ideal de A descomposa de manera única en producte d'ideals primers. El coneixement complet d'aquesta estructura per a un anell concret comporta resoldre dues qüestions fonamentals:

a) Determinar la descomposició:

$$pA = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r} \qquad (1)$$

de tots els primers $p \in \mathbb{Z}$.

b) Construir els P_i.

L'únic "defecte" que presentava la teoria de Dedekind és que no era efectiva, és a dir, no proporcionava la manera de resoldre a) i b) en un cos concret. Si es volia una estructura aritmètica era, naturalment, per fer-la servir; precisament la gran motivació era que al igual que la teoria de Kummer havia fet avançar extraordinàriament l'estudi de l'equació de Fermat, la teoria general permetria grans avenços en la resolució en general de les equacions diofàntiques. Veurem més endavant que fou el propi Dedekind qui va corregir en gran part aquest defecte.

El 1874, Zolotareff elabora una teoria en la qual els ideals primers que divideixen p són definits com les parelles $\{p, \varphi(\theta)\}$ essent θ un enter primitiu qualsevol de K i $\varphi(X)$ un dels factors irreductibles (mod.p) del polinomi minimal de θ. Aquesta teoria és efectiva per definició, però aquest punt de vista presenta un problema essencial: provar que els ideals són independents de l'equació definidora considerada. *Zolotareff ho aconsegueix si* p *no divideix l'índex de* θ, *de manera que si tots els cossos de nombres tenien* $i(K)=1$ *la teoria era completament satisfactòria*, doncs per a tot primer p existiria sempre un enter θ tal que $p \nmid i(\theta)$. Posteriorment, el 1880 Zolotareff crea, per un camí totalment diferent, una altra teoria dels ideals perfectament rigurosa i sense excepcions. Ho fa a partir de la

construcció d'un sistema de representants de A/pA. Aquesta teoria és a més a més efectiva, però el treballar-hi és enormement feixuc. Per altra banda, d'aquesta manera també es perd la possibilitat d'obtenir la solució de a) i b) directament a partir de l'equació definidora.

El 1878 Dedekind publica un treball fonamental: [Dedekind,1878], el contingut del qual no té desperdici. Ja a la introducció ens explica que feia molts anys que havia obtingut uns resultats anàlegs als de Zolotareff de 1874, però que no els havia publicat per la seva incompletitud. Al §2 prova el seu famós resultat:

Teorema 0.1. Sigui $f(X)\in\mathbb{Z}[X]$ mònic i irreduïble, θ una arrel de $f(X)$, $K=\mathbb{Q}(\theta)$ i A l'anell d'enters de K. Sigui p un primer tal que $p\nmid i(\theta)$ i sigui:

$$f(X) \equiv \varphi_1(X)^{e_1}\cdot\ldots\cdot\varphi_r(X)^{e_r} \pmod{p},$$

la factorització de f(X) en producte de factors irreduïbles a $\mathbb{F}_p[X]$. Aleshores,

$$pA = P_1^{e_1}\cdot\ldots\cdot P_r^{e_r},$$

essent $P_i=(p,\varphi_i(\theta))$ i $f(P_i/p)=gr(\varphi_i(X))$ per a tot i.#

Aquest important resultat converteix la seva teoria abstracta dels ideals en "molt" efectiva. Perquè ho fos del tot faltaria provar que $i(K)=1$ per a tot cos de nombres K. Entenem per tant que dediqui la resta del treball a aquest problema. Al §4 caracteritza els hipotètics d.c.i. de la següent manera:

Teorema 0.2.(*) Sigui K un cos de nombres. Un primer $p\in\mathbb{Z}$ divideix i(K) si i només si per algun $m\geqslant 1$ el nombre d'ideals primers de K que divideixen p amb grau residual m és més gran que $\rho(m)$, el nombre de polinomis irreduïbles de $\mathbb{F}_p[X]$ de grau m.#

Queda clar, per tant, quina cosa provocaria l'existència de d.c.i.'s: una excessiva acumulació d'ideals primers dividint un mateix $p\in\mathbb{Z}$ amb el mateix grau residual. Es pot donar aquest fenomen? Doncs si, al §5 Dedekind en dóna el primer exemple provant que $2=P_1P_2P_3$ al cos cúbic definit per X^3-X^2-2X-8. Pel Teorema 0.2, $2\mid i(K)$; concretament, $i(K)=2$.

En conseqüència, el Teorema 0.1, per desgràcia, no és una solució definitiva a a) i b). Però només queda pendent aquesta solució pels cossos amb $i(K)>1$ (ara que sabem que n'hi ha); o més precisament, només pels primers que siguin d.c.i.. La completa superació d'aquest obstacle ha d'esperar Hensel.

En efecte, la veritable revolució que significà a finals del segle passat la introducció dels mètodes p-àdics té el seu origen en la resolució d'aquests problemes. Els treballs de Hensel proporcionen la primera solució completa a a) de la següent manera:

Teorema 0.3. Sigui $f(X)\in\mathbb{Z}[X]$ mònic i irreduïble. Sigui θ una arrel de f(X), $K=\mathbb{Q}(\theta)$ i A l'anell d'enters de K. Sigui $p\in\mathbb{Z}$ un

(*) En realitat Dedekind dóna la condició següent: si $f_1,\ldots,f_r$ són els graus residuals dels r ideals primers que divideixen p, $p\nmid i(K)$ si i només si existeixen r polinomis $\varphi_1(X),\ldots,\varphi_r(X)$ irreduïbles de $\mathbb{F}_p[X]$ diferents dos a dos i tals que $gr(\varphi_i(X))=f_i$. A [Hensel,1894] es torna a provar aquest resultat reformulant l'enunciat (encertadament) com al Teorema 0.2. No sabem perquè, això ha fet que després tothom hagi atribuït aquest resultat a Hensel.

primer i:

$$f(X) = f_1(X)\cdot\ldots\cdot f_r(X), \qquad (2)$$

la factorització de f(X) en producte d'irreduïbles a $\mathbb{Q}_p[X]$. Per a cada i sigui $\theta^{(i)}$ una arrel de $f_i(X)$, $K_i=\mathbb{Q}_p(\theta^{(i)})$ i P_{K_i} l'ideal primer de K_i. Aleshores:

$$pA = P_1^{e_1}\cdot\ldots\cdot P_r^{e_r},$$

on $e_i=e(P_{K_i}/p)$ i $f(P_i/p)=f(P_{K_i}/p)$ per a tot i.#

De manera que ens podem reduir a saber descomposar els primers de $\mathbb{Z}$ en els cossos locals i aquest problema és soluble doncs, amb la definició natural de $i_p(\gamma)$ si γ és un enter algebraic sobre $\mathbb{Q}_p$, prova Hensel també que:

Teorema 0.4. Per a tota extensió finita L de $\mathbb{Q}_p$ existeix un enter $\gamma\in L$ tal que $i_p(\gamma)=0$.#

No obstant els d.c.i. continuàven preocupant els teoristes de nombres. Ara la incògnita era en quina mesura eren o no cassos realment excepcionals. La qüestió interessava vivament doncs hi havia algunes reticències a acceptar els mètodes de Hensel com a substitutoris dels de Dedekind. El propi Hensel a [Hensel,1894] se'n preocupa de donar més exemples de d.c.i.. Qui confirma la relativa "abundància" dels d.c.i. és Bauer.

El 1907 apareix un importantíssim treball, [Bauer,1907], on per primera vegada són aplicades les tècniques del polígon de Newton a l'aritmètica. La genial idea de Bauer permet factoritzar un polinomi a $\mathbb{Q}_p[X]$ observant només la potència de p que di-

videix els seus coeficients. El polígon proporciona també condicions suficients per assegurar que els factors obtinguts siguin ja irreduïbles. També dóna informació sobre els possibles valors dels índexs de ramificació, determinant-los completament en algunes ocasions. Tot això en llenguatge modern; Bauer no parlava per a res de $\mathbb{Q}_p$ i això que els treballs de Hensel ja tenien més de deu anys. Les reticències de que parlàvem?

El propi Bauer utilitza aquestes tècniques en una doble vessant. En primer lloc permeten "reconèixer" els d.c.i. ràpidament a partir de l'equació definidora; per exemple a Dedekind li costa tres pàgines provar que $2 = P_1 \cdot P_2 \cdot P_3$ en el cos cúbic definit per X^3-X^2-2X-8, i el polígon de Newton d'aquest polinomi ens ho prova a l'acte doncs té tres costats diferents (vegis fig.1). D'altra banda el polígon es revela molt eficaç per la construcció efectiva de cossos de nombres amb d.c.i. prefixats, doncs pel Teorema 0.2 només cal construir cossos de nombres amb determinades descomposicions (1) dels primers de $\mathbb{Z}$. A [Bauer,1907 b] es prova si $p<n$ l'existència de cossos de grau n en els quals p descomposa completament i si $p<n-1$ la de cossos en els quals $p = P_1^2 \cdot \ldots \cdot P_{n-1}$. L'exemple de Dedekind deixa de ser "una singularitat". Es prova uns anys més tard una mena de recíproc d'aquests últims resultats de Bauer:

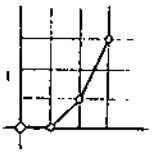


fig.1

Teorema 0.5.([Von Zylinsky,1913]) Si K és un cos de nombres de grau n i $p\in\mathbb{Z}$ divideix $i(K)$ aleshores $p<n$.#

Aquest resultat és molt important ja que restringeix les possibilitats de ser d.c.i. a una família ben concreta de pri-

mers. Doncs bé, encara que cronològicament correspon mencionar-lo aquí, es dedueix trivialment del Teorema 0.2. La gent va tardar 35 anys a adonar-se'n!

Destaquem finalment que aquestes idees de Bauer culminen en el treball [Ore,1923] on es refinen al màxim les tècniques del polígon i les seves aplicacions a aquests problemes. En particular es prova per primera vegada el resultat, comunment atribuït a Hasse, de l'existència de cossos de nombres amb descomposicions (1) arbitràries per un nombre finit de primers de $\mathbb{Z}$. Aquest resultat, després del Teorema 0.2, acaba de mostrar que no hi ha cap motiu per considerar els cossos amb $i(K) > 1$ com a cassos patològics.

§2. El paper de $i_p(K)$. La conjectura de Ore

Fins ara els d.c.i. s'han presentat com obstacles, la superació dels quals ha influït fortament en el desenvolupament de la teoria dels ideals i en la introducció dels mètodes p-àdics. Suposem que p és un d.c.i. de K. Veurem a continuació que *així com el fet de que* $i_p(K)=0$ *ó* >0 *decideix la possibilitat d'aplicar el mètode de Dedekind, el valor de* $i_p(K)$ *és una mesura de l'obstrucció que presenta* p *perquè li sigui trobada la descomposició en producte d'ideals primers mitjançant el mètode de Hensel.* En efecte, si es volen fer efectives l'obtenció de la factorització (2) del Teorema 0.3 i la recerca de l'enter γ del Teorema 0.4, s'han de truncar els desenvolupaments p-àdics en un lloc determinat, és a dir, s'ha de treballar $(\text{mod.}\, p^s)$ per a

s prou gran. El propi Hensel estableix quina és la cota mínima de s que permet assegurar que la factorització (2) (mod.p^s) és suficient pels nostres propòsits:

Teorema 0.6. Sigui $f(X)\in\mathbb{Z}[X]$ mònic i irreduïble, $p\in\mathbb{Z}$ un primer i $d_p(f)$ la màxima potència amb que p divideix el discriminant d(f) de f(X). Si $s>d_p(f)$ i:

$$f(X) \equiv F_1(X)\cdot\ldots\cdot F_r(X) \quad (\text{mod}.p^s), \qquad (3)$$

és la factorització de f(X) en producte de mònics i irreduïbles a $\mathbb{Z}/p^s\mathbb{Z}$, aleshores f(X) factoritza, $f(X)=f_1(X)\cdot\ldots\cdot f_r(X)$ en producte d'irreduïbles a $\mathbb{Q}_p[X]$. Cada factor satisfà $f_i(X)\equiv F_i(X)$ (mod.p^s) i a més a més $f_i(X)$ i $F_i(X)$ defineixen a menys de conjugació la mateixa extensió de $\mathbb{Q}_p$.#

Per tant, trobar la descomposició d'un primer racional en producte d'ideals primers en un cos de nombres K requereix treballar com a mínim (mod.p^s) amb:

$$s-1 = \min_{\substack{\theta\in A \\ \text{primitiu}}} \{ d_p(f)/f(X)=\text{Irr}(\theta,\mathbb{Q}) \}.$$

De la coneguda relació:

$$(-1)^{\frac{n(n-1)}{2}}\, d(f) = d(\theta) = i(\theta)^2 d(K),$$

on d(K) denota el discriminant absolut de K i $n=[K:\mathbb{Q}]$, tenim:

$$s-1 = \min_{\substack{\theta\in A \\ \text{primitiu}}} \{ 2i_p(\theta)+d_p(K) \} = d_p(K)+2i_p(K),$$

essent $d_p(K)$ la màxima potència de p que divideix d(K). De manera que $i_p(K)$, junt amb $d_p(K)$, proporcionen la cota mínima òptima mòdul la qual s'ha de treballar per obtenir (3).

Curiosament aquests dos invariants tenen una sèrie de propietats paral.leles que intentarem fer paleses. Anotem una llista de propietats de $d_p(K)$ ben conegudes:

1) El fet de que $d_p(K)$ s'anul.li o no ve determinat pel tipus de descomposició (1) de p (s'anul.la si i només si p no ramifica).

2) El tipus de descomposició de p no determina en canvi el valor de $d_p(K)$.

3) El càlcul de $d_p(K)$ és un problema local. En efecte, si $K_1,\ldots,K_r$ són els diferents cossos locals associats a p, $d_p(K)$ ve determinat pels discriminants locals: $d_p(K)=\sum_{i=1}^{r} d_p(K_i)$.

4) Si K és Galoisià hi ha invariants més febles dels cossos locals que ja determinen el valor de $d_p(K)$, són els nombres de ramificació.

El Teorema 0.2 assegura que $i_p(K)$ té la propietat 1). De la propietat 2) el primer que s'en preocupa és Ore, el qual conjectura que $i_p(K)$ la satisfà: "... man immer bei gegebener Form der Primidealzerlegung eine obere Grenze für die Potenz angeben kann, worin p in allen Diskriminanten aufgeht. Es wäre sogar denkbar, daß diese größte gemeinsame Potenz von p in den Indizen nur von der Form der Primidealzerlegung abhinge, ich halte diese Vermutung für unwahrscheinlich."([Ore,1928,pag.111]). La conjectura de Ore és confirmada per Engstrom donant exemples de cossos de nombres en els quals un determinat primer descomposa de la mateixa manera i en canvi $i_p(K)$ pren valors diferents [Engstrom, 1930]. Ja no sabem res més sobre propietats de $i_p(K)$; de fet,

posterior a aquest treball d'Engstrom totes les referències que es troben a la literatura sobre els d.c.i. i $i_p(K)$ són més aviat puntuals i no avançen gens en la línia d'idees exposada fins ara. Destaquem: [Bungers,1936], [Carlitz,1933,1952], [Tornheim,1955], [Nagell,1965] i [Llorente-Nart,1983]. Un resultat que destacaria seria [Sukallo,1955], on l'autor pretèn donar una fòrmula explícita per $i_p(K)$ en el cas en que tots els ideals primers de K que divideixen p tenen grau residual u, però els seus resultats són completament incorrectes com mostra, en particular, l'exemple d'Engstrom (vegis també la Remarca al Corol.lari 1.12).

El problema de trobar invariants de K que determinin $i_p(K)$ i el seu càlcul queda, per tant, sense resposta i així el podem trobar com un dels problemes oberts de la llista de l'excel.lent llibre: [Narkiewicz,1974] (*).

Clarament $i_p(K)$ no satisfà 3) ni 4). El càlcul de $i_p(K)$ no és un problema local doncs pel Teorema 0.3 els índexs locals són sempre trivials. No obstant, veurem al Capítol 1 que $i_p(K)$ satisfà una propietat paral.lela a 3). També suposem que satisfà una propietat paral.lela a 4) però no ho hem pogut provar (vègis la Conjectura 1.14).

§3. La contribució d'Engstrom

A continuació passem a exposar amb detall els resultats de [Engstrom,1930] ja que són el veritable punt de partida de la present memòria. A més a més estan escrits en un llenguatge molt clàssic que dificulta considerablement la seva lectura.

(*) En un treball recent [Śliwa,1982] es tracta el cas en que p no ramifica.

Separem aquests resultats en dos grups: els que es preocupen de la determinació de $i_p(K)$ en general i els que estan motivats per la confirmació de la conjectura de Ore. Pel que fa referència al càlcul de $i_p(K)$ en situacions més o menys generals Engstrom concentra els seus esforços en analitzar com influeix en el valor de $i_p(K)$ el nombre d'ideals primers de K dividint p amb grau residual 1. Obté una resposta completa que li permet fins i tot calcular explícitament $i_p(K)$ en el cas en que els ideals primers amb grau residual 1 tenen també índex de ramificació 1. Donem una idea de la demostració doncs ens inspirarem en ella més endavant.

En primer lloc és crucial per al càlcul en general de $i_p(K)$ el següent resultat:

Teorema 0.7. ([Ore,1926]) Sigui $f(X)\in\mathbb{Z}[X]$ mònic i irreduïble i $p\in\mathbb{Z}$ un primer. Si $f(X)=f_1(X)\cdot\ldots\cdot f_r(X)$ és la factorització de $f(X)$ en producte d'irreduïbles a $\mathbb{Q}_p[X]$ aleshores:

$$i_p(f) = \sum_{1\leq i<j\leq r} R_p(f_i,f_j) + \sum_{i=1}^{r} i_p(f_i).\#$$

Si un primer p descomposa completament en un cos de nombres K, el seu polinomi minimal descomposa en producte de factors lineals a $\mathbb{Q}_p[X]$. Doncs bé, Engstrom mostra que, per a s prou gran, aquests factors lineals els podem suposar arbitraris $(\mathrm{mod}.p^s)$. Concretament prova:

Teorema 0.8. Sigui K un cos de nombres de grau n i sigui $p\in\mathbb{Z}$ un primer que descomposa completament a K. Donats $a_1,\ldots,a_n\in\mathbb{Z}$

arbitraris i $s\in\mathbb{Z}$, $s>0$, existeix un enter $\theta\in K$ tal que el seu polinomi minimal satisfà:

$$f(X) \equiv (X-a_1)\cdot\ldots\cdot(X-a_n) \quad (\text{mod}.p^s).\#$$

Amb aquestes mateixes notacions, si $b_1,\ldots,b_n\in\mathbb{Z}_p$ són les veritables arrels de $f(X)$, $b_i\equiv a_i$ $(\text{mod}.p^s)$ implica que prenent s suficientment gran podrem aconseguir que $v_p(b_i-b_j)=v_p(a_i-a_j)$ per a tot i,j. Aplicant els Teoremes 0.7 i 0.8 tenim per tant que si p descomposa completament a K:

$$i_p(K) = \min_{\theta\in A \text{ primitiu}} \{i_p(\theta)\} = \min_{a_i\in\mathbb{Z}} \{\sum_{1\leqslant i<j\leqslant n} v_p(a_i-a_j)\}.$$

A [Hensel,1896] es prova que aquest últim mínim s'obté prenent els enters $1,2,\ldots,n$, de manera que queda provat que:

$$i_p(K) = \sum_{1\leqslant i<j\leqslant n} v_p(i-j) = \sum_{k=1}^{n-1} (n-k)v_p(k).$$

Remarca. Aquesta suma es pot comptar de diverses maneres; citem-ne dues, la de [Engstrom,1930,th.2] i una altra:

$$i_p(K) = \sum_{i\geqslant 1} [\frac{n}{p^i}](n - \frac{p^i}{2}([\frac{n}{p^i}]+1)) = \sum_{i\geqslant 1}\sum_{k=1}^{n-1} [\frac{k}{p^i}].$$

L'última igualtat essent certa sumand a sumand per a cada i.

El resultat més complet d'Engstrom en aquesta direcció consisteix en estendre aquest resultat, d'una banda deixant que apareguin ideals primers dividint p amb grau residual més gran que 1, però en nombre prou reduit (donat pel Teorema 0.2) perquè no contribueixin gens a l'augment de $i_p(K)$; i de l'altra permetent que hi hagi un sol ideal amb grau residual 1 i índex de ra-

mificació més gran que 1:

Teorema 0.9. Sigui K un cos de nombres i $p\in\mathbb{Z}$ un primer. Si per a tot $m>1$ el nombre d'ideals primers de K dividint p amb grau residual m és més petit o igual que $\rho(m)$ i tots els ideals primers de K dividint p amb grau residual 1 tenen també índex de ramificació 1 excepte potser un d'ells, tenim:

$$i_p(K) = t[\frac{n_0}{p}] + \sum_{i\geq 1} \sum_{k=1}^{n_0-1} [\frac{k}{p^i}],$$

on n_0 és el nombre d'ideals primers $P|p$ amb $e(P/p)=f(P/p)=1$ i $t=0$ ó 1 és el nombre dels que satisfan $f(P/p)=1$ i $e(P/p)>1$.#

És a dir que si p té una descomposició (1) com l'especificada en el Teorema 0.9 sí que el valor de $i_p(K)$ queda determinat per aquesta descomposició. Aquest resultat, junt amb algunes fórmules per $i_2(K)$ per algunes descomposicions particulars del primer 2 li permeten comprovar que pels cossos de nombres de grau més petit o igual que set, $i_p(K)$ està determinat sempre pel tipus de descomposició (1) de p i calcula explícitament el seu valor per a totes les descomposicions possibles. En canvi, prova finalment que pels cossos de grau vuit en els quals $3=(P_1P_2P_3P_4)^2$, $i_3(K)$ val 2 ó 3 depenent de propietats dels termes independents dels quatre factors quadràtics a $\mathbb{Q}_3[X]$ d'un polinomi definidor qualsevol del cos. També mostra que aquest fenomen es manté pels cossos de grau superior a vuit. D'aquesta manera queda provada la conjectura de Ore.

Capítol 1. Sobre l'índex d'un cos de nombres

Aquest primer capítol es pot considerar una continuació del treball d'Engstrom en les dues vertents següents: esbrinar quins invariants determinen l'índex, ja que la descomposició en producte d'ideals no ho fa, i estendre els cassos en que som capaços de calcular-lo. En el §1 es resol la primera qüestió; encara que el càlcul de $i_p(K)$ no és un problema local, el seu valor ve determinat pel conjunt de les extensions locals. Això permet, en el §4, confirmar amb més rotunditat la conjectura de Ore i esclarir el fenomen observat per Engstrom, mostrant que *es presenta sempre que hi ha una acumulació d'ideals primers de K dividint el mateix primer de $\mathbb{Z}$ amb el mateix grau residual i índex de ramificació*. En els §2 i 3 ens preocupem del càlcul de $i_p(K)$ en el cas en que les extensions locals són totes totalment ramificades; destaca el Teorema 1.10, o més pròpiament el Corol.lari 1.12, el qual estén força les fòrmules d'Engstrom.

Sigui $p\in\mathbb{Z}$ un primer que considerarem fix al llarg de tot el capítol i denotem per Ω una clausura algebraica de $\mathbb{Q}_p$. Sigui E el conjunt quocient obtingut al classificar les extensions finites de $\mathbb{Q}_p$, $\mathbb{Q}_p \subset L \subset \Omega$, per conjugació. Un polinomi irreduïble $f(X)\in\mathbb{Z}_p[X]$ determina un únic element de E, un representant del qual és $L=\mathbb{Q}_p(\theta)$, on $\theta\in\Omega$ és una arrel qualsevol de $f(X)$. Direm que $f(X)$ *genera* L. Si dos polinomis generen el mateix $L\in E$ escriurem $f(X)\sim g(X)$. Finalment, si $L\in E$ denotarem S_L el conjunt dels polinomis de $\mathbb{Z}_p[X]$ mònics i irreduïbles que generen L.

§1. Invariants que determinen $i_p(K)$

Sigui $\mathfrak{E}$ el subconjunt del $\mathbb{Z}$-mòdul lliure generat per E format pels elements:

$$n_1L_1+\ldots+n_tL_t, \quad L_i \in E,$$

tals que $n_i>0$ per a tot i. Tot cos de nombres K te intrínsecament associat un element de $\mathfrak{E}$ que denotarem $e_p(K)$. En efecte, si $P_1,..,P_r$ són els ideals primers de l'anell d'enters de K que divideixen p, les diferents completacions $K_{P_1},\ldots,K_{P_r}$ de K per la topologia P_i-àdica respectiva tenen una realització concreta dins Ω, única mòdul conjugació. Si continuem denotant K_{P_i} aquests cossos, $\mathbb{Q}_p \subset K_{P_i} \subset \Omega$, definim:

$$e_p(K) = K_{P_1}+\ldots+K_{P_r}.$$

Els K_{P_i} són tots diferents com a cossos topològics però les seves realitzacions com a subcossos de Ω poden coincidir. Concretament, si $K/\mathbb{Q}$ és Galoisiana i $f(X)\in\mathbb{Z}[X]$ és un polinomi les arrels del qual generen K, totes les imatges dels K_{P_i} dins Ω coincideixen amb $L=\mathbb{Q}_p(\theta_1,..,\theta_n)$, essent $\theta_1,..,\theta_n$ les arrels de f(X) a Ω. De manera que pels cossos de nombres Galoisians, $e_p(K)=rL$, essent $L/\mathbb{Q}_p$ Galoisiana. D'ara endavant pensarem sempre els K_{P_i} com elements de E, és a dir que prescindirem de la seva estructura topològica.

Donat qualsevol $\Gamma\in\mathfrak{E}$ és molt fàcil construir cossos de nombres K tals que $e_p(K)=\Gamma$. Si $\Gamma = L_1+\ldots+L_r$, prenem per a tot i polinomis $f_i(X)\in S_{L_i}$ i considerem,

$$f(X) = f_1(X)\cdot\ldots\cdot f_r(X) + p^s g(X),$$

amb $s > d_p(\prod_{i=1}^{r} f_i(X))$ i $g(X)$ adequat per tal que $f(X)$ sigui irreductible a $\mathbb{Q}$. Una arrel qualsevol de $f(X)$ genera un cos de nombres satisfent el que preteniem.

El nostre objectiu és mostrar que aquest element $e_p(K)$ de & determina el valor de $i_p(K)$. Per provar-ho ens inspirarem en el Teorema 0.8, el qual permet a Engstrom provar que $i_p(K)$ està determinat pels cossos en els quals p descomposa completament, és a dir pels cossos tals que $e_p(K)=n\mathbb{Q}_p$. El primer que farem, per tant, serà generalitzar el Teorema 0.8 del cas $e_p(K)=n\mathbb{Q}_p$ al cas general. La idea clau que permet la generalització és la seguent: si θ i ω són dos enters algebraics sobre $\mathbb{Q}_p$ que estan "aprop" per la distància ultramètrica usual de Ω, aleshores els seus polinomis minimals són congruents (mod.p^s) per s "elevat". Aquest fet l'imaginem conegut pero per manca de referències concretes l'enunciarem i provarem amb precisió.

Sigui $|\ |$ l'únic valor absolut definit sobre Ω que coincideix sobre $\mathbb{Q}_p$ amb el valor absolut p-àdic, $|x|=p^{-v_p(x)}$. Sigui S_n el conjunt dels polinomis de $\mathbb{Z}_p[X]$ mònics, irreductibles i de grau n. Considerem les seguents distàncies ultramètriques definides sobre S_n:

$$d(f,g) = \max_{1\leq i\leq n} \{|a_i-b_i|\}$$

$$\Delta(f,g) = \min_{1\leq i,j\leq n} \{|\theta_i-\omega_j|\}$$

$$d_n(f,g) = |R(f,g)|^{1/n} = |f(\omega_i)| = |g(\theta_j)|, \quad \text{([Krasner,1966])}$$

essent $f(X)=\sum_{i=0}^{n} a_i X^{n-i}$, $g(X)=\sum_{i=0}^{n} b_i X^{n-i} \in S_n$ d'arrels $\theta_1,\ldots,\theta_n$;

$\omega_1,\ldots,\omega_n \in \Omega$ respectivament. L'interès puntual que tenim en aquests moments és provar que Δ és més fina que d. No obstant, per tal de donar un resultat més complet provarem el seguent:

Proposició 1.1. Les tres distàncies d,Δ i d_n són equivalents.

Demostració. Siguin $f(X),g(X) \in S_n$ d'arrels respectives $\theta=\theta_1,\ldots,\theta_n$; $\omega=\omega_1,\ldots,\omega_n \in \Omega$. Si $s\in\mathbb{Z}$, $s>0$, les següents implicacions són clares:

$$f(X)\equiv g(X) \pmod{p^s} \Rightarrow f(\omega)\equiv 0 \pmod{p^s} \Rightarrow$$

$$v_p\Big(\prod_{i=1}^{n}(\omega-\theta_i)\Big) \geqslant s \Rightarrow \max_{1\leqslant i\leqslant n}\{v_p(\omega-\theta_i)\} \geqslant s/n.$$

Això prova que $d \geqslant d_n \geqslant \Delta$. La desigualtat que de veres necessitem és la menys immediata. Sigui A l'anell d'enters de $\mathbb{Q}_p(\theta)$ i considerem el morfisme d'anells $A \xrightarrow{\pi_s} A/p^sA$. Si $u=i_p(\theta)$ sabem que $p^uA\subset\mathbb{Z}_p[\theta]$, de manera que per a $s\geqslant u$ tenim:

$$\ker(\pi_{s|\mathbb{Z}_p[\theta]}) = \ker(\pi_s)\cap\mathbb{Z}_p[\theta] = p^sA\cap\mathbb{Z}_p[\theta] \subset p^{s-u}\mathbb{Z}_p[\theta].$$

Per tant, si ϕ_s denota la composició dels morfismes canònics,

$$\mathbb{Z}_p[X] \longrightarrow \mathbb{Z}_p[X]/f(X) \xrightarrow{\sim} \mathbb{Z}_p[\theta] \longrightarrow A \xrightarrow{\pi_s} A/p^sA,$$

tenim que $\ker(\phi_s) \subset (p^{s-u},f(X))$. En conseqüència, $\theta\equiv\omega \pmod{p^s}$ ens dóna $\phi_s(g(X))=0$ i per tant $g(X) \in (p^{s-u},f(X))$. Al ser els dos polinomis mònics i del mateix grau, a la força $f(X)\equiv g(X) \pmod{p^{s-u}}$. Per tant $\Delta\geqslant d$ i la proposició queda provada.#

Ja podem provar la generalització del Teorema 0.8:

Teorema 1.2. Sigui K un cos de nombres, A l'anell d'enters i

$$pA = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r},$$

la descomposició de p en producte d'ideals primers de A. Siguin $K_{P_1}, \ldots, K_{P_r} \in E$ les corresponents extensions locals i $g_1(X), \ldots, g_r(X)$ polinomis qualsevols tals que $g_i(X) \in S_{K_{P_i}}$ per a tot i. Aleshores, donat $s \in \mathbb{Z}$, $s > 0$, existeix $\theta \in A$ primitiu tal que si $f(X) = Irr(\theta, \mathbb{Q})$ i $f(X) = f_1(X) \cdot \ldots \cdot f_r(X)$ és la seva factorització en producte d'irreduibles a $\mathbb{Z}_p[X]$ es té:

$$f_i(X) \equiv g_i(X) \pmod{p^s}, \text{ per a tot i.}$$

Demostració. Per a cada j siguin $u_j = i_p(g_j)$ i $\theta_j \in \Omega$ una arrel de $g_j(X)$ tal que $K_{P_j} = \mathbb{Q}_p(\theta_j)$. Sigui $\theta \in A$ tal que:

$$\theta \equiv \theta_i \pmod{P_i^{m_i}}, \quad 1 \leq i \leq r, \tag{1}$$

amb $m_i \geq e_i(s+u_i)$. Podem suposar que θ és primitiu doncs si no ho fos considerem $\theta' = \theta + p^t\omega$ amb $\omega \in A$ primitiu. Per a qualsevol morfisme $K \xrightarrow{\sigma} \mathbb{C}$, $\theta' = \sigma(\theta')$ equival a,

$$\theta - \sigma(\theta) + p^t(\omega - \sigma(\omega)) = 0, \tag{2}$$

de manera que prenent t prou gran ens podem assegurar a la vegada de que θ' satisfà (1) i de que (2) no és possible.

Sigui $f(X) = Irr(\theta, \mathbb{Q})$ i sigui $f(X) = f_1(X) \cdot \ldots \cdot f_r(X)$ la seva factorització en producte d'irreduïbles a $\mathbb{Z}_p[X]$. Per a cada i el morfisme $K \longrightarrow K_{P_i}$ envia θ a una de les arrels de $f_i(X)$ a Ω, per tant, (1) i l'última part de la prova de la Proposició 1.1 mostren que $f_i(X) \equiv g_i(X) \pmod{p^s}$. #

Si K és un cos de nombres d'anell d'enters A i $K_{P_1}, \ldots, K_{P_r} \in E$ són les diferents extensions locals, pel Teorema 0.7 tenim:

$$i_p(K) = \min\{i_p(\theta)/\theta \in A \text{ primitiu}\} =$$

$$= \min\{\sum_{1\leqslant i<j\leqslant r} R_p(f_i,f_j) + \sum_{i=1}^{r} i_p(f_i)\},$$

aquest últim mínim considerat entre totes les famílies de polinomis $f_1(X),\ldots,f_r(X)\in\mathbb{Z}_p[X]$ que apareixen com a factors irreduïbles a $\mathbb{Z}_p[X]$ d'un $f(X)\in\mathbb{Z}[X]$ que sigui polinomi minimal d'un enter $\theta \in A$ primitiu.

Per altra banda, donat un element qualsevol $\Gamma = L_1+\ldots+L_r \in \mathfrak{E}$ podem anomenar a tota família de polinomis $g_1(X) \in S_{L_1}, \ldots, g_r(X) \in S_{L_r}$ una Γ-*família* i definir:

$$I_p(\Gamma) = \min_{\Gamma\text{-famílies}} \{\sum_{1\leqslant i<j\leqslant r} R_p(g_i,g_j) + \sum_{i=1}^{r} i_p(g_i)\}.$$

És clar que $i_p(K)\geqslant I_p(e_p(K))$. També és clar que les Γ-famílies tals que el producte $g(X)=g_1(X)\cdot\ldots\cdot g_r(X)$ és un polinomi irreduible de $\mathbb{Z}[X]$ una arrel del qual satisfà $K=\mathbb{Q}(\theta)$ no poden ser arbitràries ni molt menys. No obstant, pel Teorema 1.2 podem trobar Γ-famílies amb aquesta propietat "arbitràries $(\text{mod.}p^s)$" i per s arbitràriament gran. Ara, per a s prou gran, si dues famílies de polinomis tenen els seus membres congruents dos a dos $(\text{mod.}p^s)$ es tindrà $i_p(f_i)=i_p(g_i)$ i $R_p(f_i,f_j)=R_p(g_i,g_j)$ per a tot i,j. De manera que el Teorema 1.2 prova que:

$$i_p(K) = I_p(e_p(K)),$$

per a tot cos de nombres K. Queda provat per tant el següent:

Corol.lari 1.3. Si K i K' són dos cossos de nombres i $q \in \mathbb{Z}$ és un primer tal que $e_q(K)=e_q(K')$, aleshores $i_q(K)=i_q(K')$. En particular si K i K' tenen els mateixos d.c.i. i per a tots ells és $e_q(K)=e_q(K')$, aleshores $i(K)=i(K')$.#

Ja hem comentat al Capítol 0 que el càlcul de $i_p(K)$ no és un problema local perquè "mirant" cada K_{p_i} no veiem res doncs no hi ha índex local. Aquests resultats mostren que el que determina $i_p(K)$ és el conjunt de tots els K_{p_i}, precisant així en quin sentit $i_p(K)$ satisfà una propietat paral.lela a (3) del Capítol 0. Observis que també mostren que no es tracta d'un problema global doncs l'estructura global de K deixa d'importar.

A la llarga el nostre objectiu haurà de ser saber calcular $I_p(\Gamma)$ per a tot $\Gamma \in \&$. Centrem-nos de moment en el que resta de capítol en acabar d'esclarir perquè és que la sola descomposició de p en ideals primers de K no determina $i_p(K)$, quines descomposicions si que ho farien, explicar satisfactòriament el fenomen observat per Engstrom que confirma la conjectura de Ore i mostrar com un domini encara elemental del càlcul d'índexs i resultants ja permet, gràcies al Teorema 1.2, estendre àmpliament les fòrmules d'Engstrom.

Remarca. Tots els resultats d'aquest paràgraf s'estenen sense cap dificultat al cas relatiu i no ens hem situat d'entrada en aquest cas exclusivament per comoditat en l'exposició.

§2. Γ-configuracions. El cas totalment ramificat

Sigui $f(X)\in\mathbb{Z}_p[X]$ un polinomi mònic i irreduïble. Pel lema de Hensel:

$$f(X) \equiv \varphi(X)^m \quad (\text{mòd.}p),$$

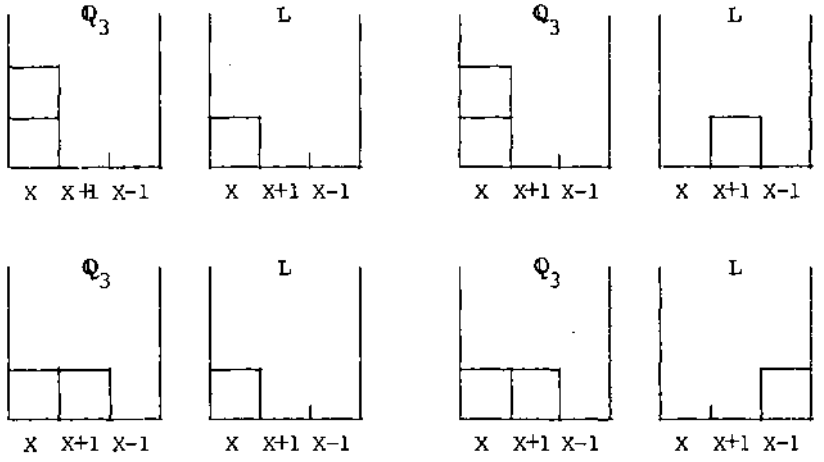
essent $\varphi(X)$ un polinomi mònic i irreduïble de $\mathbb{F}_p[X]$. Està clar que $\varphi(X)$ està unívocament associat a $f(X)$. Si $L=\mathbb{Q}_p(\theta)$ essent θ una arrel qualsevol de $f(X)$, el grau de $\varphi(X)$ és un divisor del grau residual de $L/\mathbb{Q}_p$ doncs tenim,

$$\mathbb{F}_p \subset \mathbb{F}_p(\bar{\theta}) \subset \bar{L},$$

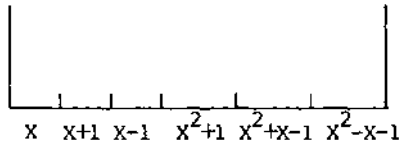
i clarament $\varphi(X)=\mathrm{Irr}(\bar{\theta}, \mathbb{F}_p)$.

Expressarem les diferents possibilitats que tenen les Γ-famílies de "repartirse" els polinomis irreduïbles de $\mathbb{F}_p[X]$ que han de tenir associats els seus membres mitjançant un esquema gràfic que ens serà molt útil. Considerem per a cada $L\in E$ una caixa amb tantes subdivisions com polinomis irreduïbles de $\mathbb{F}_p[X]$ de grau divisor del grau residual de $L/\mathbb{Q}_p$. Donat un $\Gamma\in\mathfrak{G}$ i una Γ-família, expressem el fet de que un polinomi $f_i(X)\in S_{L_i}$ tingui associat un determinat polinomi irreduïble $\varphi(X)$ de $\mathbb{F}_p[X]$ col.locant un quadradet a la subdivisió de la caixa L_i que correspon a $\varphi(X)$. Cada possible esquema gràfic així obtingut l'anomenarem una Γ-*configuració*. És fàcil comprovar que donats $\Gamma\in\mathfrak{G}$ i una Γ-configuració qualsevol que poguem imaginar, sempre es pot construir una Γ-família que tingui associats els polinomis irreduïbles de $\mathbb{F}_p[X]$ que la Γ-configuració indica.

Exemple 1. Si $L=\mathbb{Q}_3(\sqrt{3})$ i $\Gamma=2\mathbb{Q}_3+L$ les possibles Γ-configuracions són, a menys d'una permutació de X, X+1 i X-1:



Exemple 2. Si $L=\mathbb{Q}_3(\sqrt{-1})$ i $\Gamma=$ nL, com que $L/\mathbb{Q}_3$ és no-ramificada les Γ-configuracions són les possibles reparticions de n quadradets dins de la caixa:



El fet de que una Γ-família tingui una determinada Γ-configuració ja dóna una certa idea del valor:

$$\sum_{1\leqslant i<j\leqslant r} R_p(f_i,f_j) + \sum_{i=1}^{r} i_p(f_i), \qquad (3)$$

doncs és ben clar que si $f(X),g(X)\in\mathbb{Z}_p[X]$ són mònics i irreduibles, $R_p(f,g)>0$ *si i només si* $f(X)$ *i* $g(X)$ *tenen associat el mateix polinomi irreduible de* $\mathbb{F}_p[X]$. De manera que l'acumulació

de quadradets en una mateixa columna provoca en principi un augment de $\sum_{1\leqslant i<j\leqslant r} R_p(f_i,f_j)$ i sembla natural que si volem minimitzar aquest valor convindrà repartir el màxim possible els quadradets entre les diferents columnes. Naturalment que després hi ha una altra qüestió cabdal: quins valors pren $R_p(f,g)$ per polinomis de la mateixa columna?

Una resposta precisa a aquestes qüestions i que ens permetrà més endavant obtenir el valor de $I_p(\Gamma)$ per alguns $\Gamma\in\mathfrak{C}$ la donarem en aquest paràgraf però limitant-nos al cas en que totes les extensions que componen Γ són totalment ramificades. Sota aquesta condició totes les caixes de les Γ-configuracions tenen p subdivisions corresponents als polinomis X, X-1,...,X-(p-1). A més a més les columnes també són totes "iguals" ja que podem passar d'una a l'altra per un canvi lineal, el qual obviament deixa invariants els valors de $i_p(f)$ i $R_p(f,g)$. Per tant podem limitar-nos a estudiar la columna dels polinomis que satisfan $f(X)\equiv X^n$ (mòd.p), del quals interessen especialment els Eisensteinians; en efecte, és fàcil comprovar que:

Lema 1.4. Sigui $f(X)\in\mathbb{Z}_p[X]$ mònic, irreduïble, de grau n i tal que $f(X)\equiv X^n$ (mòd.p). Aleshores $i_p(f)=0$ si i només si n=1 ó f(X) és Eisenstenià.#

A continuació consignem alguns resultats sobre el càlcul de $R_p(f,g)$. Començem amb un resultat no gens difícil de provar i que, d'altra banda, està incluit en el tractament més general del càlcul de $R_p(f,g)$ que fem en el Capítol 2.

Lema 1.5. Siguin $f(X), g(X) \in \mathbb{Z}_p[X]$ mònics, de graus n,m respectivament i tals que $f(X) \equiv X^n$, $g(X) \equiv X^m$ (mòd.p). Aleshores $R_p(f,g) \geqslant \inf\{n,m\}$. Les següents condicions són suficients per assegurar la igualtat:

1) n=m i que un polinomi sigui Eisenstenià i l'altre no.

2) n<m i que g(X) sigui Eisenstenià.#

A [Krasner,1966] es dóna una fórmula per calcular $R_p(f,g)$ de dos polinomis Eisenstenians del mateix grau n:

$$R_p(f,g) = \min_{1\leqslant i\leqslant n} \{n\cdot v_p(pa_i - pb_i) + (n-i)\}, \qquad (4)$$

essent $f(X) = X^n + p\sum_{i=1}^{n} a_i X^{n-i}$, $g(X) = X^n + p\sum_{i=1}^{n} b_i X^{n-i}$. De la qual es desprèn que:

$$R_p(f,g) = n \quad \Leftrightarrow \quad a_n \not\equiv b_n \quad (\text{mòd.p}). \qquad (5)$$

Tornem amb les Γ-configuracions. Podem assignar a cada Γ-configuració el valor mínim que pren (3) considerant les Γ-famílies que tenen aquesta configuració. Per exemple, utilitzant el que acabem de veure sobre el càlcul de $R_p(f,g)$ es comprova fàcilment que aquest valor mínim és de 3,2,1 i 0 respectivament per les configuracions de l'Exemple 1. Així doncs, té sentit comparar les possibles Γ-configuracions d'un determinat $\Gamma \in \mathfrak{G}$, i n'hi haurà sempre una de mínima que és la que donarà el valor de $I_p(\Gamma)$. És natural preguntar-se si hi ha alguna mena de distribució standard dels quadradets que, independentment de Γ, permetès obtenir sempre la configuració mínima. Veurem a continuació que si prescindim de $\sum_i i_p(f_i)$ i suposem que $R_p(f,g)$ pren sempre el

mínim valor possible, donat pel Lema 1.5, si que hi ha una manera standard d'obtenir la configuració mínima.

Proposició 1.6. Suposem que tenim $n_1+\ldots+n_r$ objectes situats respectivament en r caixes, cadascuna de les quals consta de q subdivisions, $q \geqslant 2$. Assignem a cada caixa un valor $e_i \in \mathbb{Z}$, satisfent:

$$0 \leqslant e_1 \leqslant e_2 \leqslant \ldots \leqslant e_r. \tag{6}$$

Denotem una distribució qualsevol dels objectes de cada caixa entre les subdivisions per:

$$n_i = t_{i,1}+\ldots+t_{i,q}, \quad t_{i,k} \geqslant 0, \quad 1 \leqslant k \leqslant q, \tag{7}$$

per a tot $1 \leqslant i \leqslant r$. Si a cada parella no ordenada d'objectes situats en una mateixa subdivisió de les caixes i,j els hi assignem el pes $\min\{e_i,e_j\}$, la suma de tots aquests pesos és mínima si la distribució (7) satisfà les dues condicions:

$$\max_{1 \leqslant k<l \leqslant q} \{|t_{i,k}-t_{i,l}|\} \leqslant 1, \tag{8}$$

$$\max_{1 \leqslant k<l \leqslant q} \{\left|\sum_{j=1}^{i} t_{j,k} - \sum_{j=1}^{i} t_{j,l}\right|\} \leqslant 1, \tag{9}$$

per a tot $1 \leqslant i \leqslant r$.

Demostració. Per inducció sobre el nombre de caixes. Si tenim una sola caixa la suma total dels pesos és:

$$\left(\sum_{t_{1,k}>1} 1+2+\ldots+(t_{1,k}-1)\right)\cdot e_1. \tag{10}$$

Si la distribució no satisfà (8), existiran dues subdivisions k,l tals que $t_{1,k}-t_{1,l} \geqslant 2$, per tant, si treiem un objecte de la subdivisió k i el col.loquem a la subdivisió l obtenim una nova dis-

tribució per a la qual el valor (10) disminueix exactament en $(t_{1,k}-t_{1,1}-1)\cdot e_1 \geqslant 0$. Després d'un nombre finit de canvis com aquest obtenim una distribució que satisfà (8) i amb suma total de pesos menor o igual que la de la distribució de la qual havíem partit.

Suposem la proposició provada per a r-1 caixes, $r \geqslant 2$. Expressem la suma total dels pesos d'una distribució (7) qualsevol i la d'una distribució que satisfaci (8) i (9) respectivament per:

$$A = \sum_{i=1}^{r} a_i e_i + \sum_{i=1}^{r-1} x_i e_i; \quad B = \sum_{i=1}^{r} b_i e_i + \sum_{i=1}^{r-1} y_i e_i,$$

on a_i, b_i conten el nombre de parelles de la caixa i-èssima situades en una mateixa subdivisió i x_i, y_i el mateix, però amb parelles un membre de les quals sigui de la caixa i-èssima i l'altre d'una caixa de valor superior. Més precisament,

$$a_i = \frac{1}{2} \sum_{k=1}^{q} t_{i,k}(t_{i,k}-1) \quad \text{i} \quad x_i = \sum_{k=1}^{q} t_{i,k}\Big(\sum_{j>i} t_{j,k}\Big).$$

Prescindim en les dues distribucions de la primera caixa i imaginem que els valors associats a les r-1 caixes que ens queden són respectivament:

$$0 \leqslant e_2-e_1 \leqslant e_3-e_1 \leqslant \ldots \leqslant e_r-e_1.$$

Clarament la segona distribució continua satisfent (8) i (9). Per hipòtesi d'inducció tenim:

$$\sum_{i=2}^{r} a_i(e_i-e_1) + \sum_{i=2}^{r-1} x_i(e_i-e_1) \geqslant \sum_{i=2}^{r} b_i(e_i-e_1) + \sum_{i=2}^{r-1} y_i(e_i-e_1). \quad (11)$$

D'altra banda, si imaginem que tenim tots els objectes reunits en una sola caixa amb valor e_1 i distribuïts entre les subdivi-

sions tal com estan, la suma total dels pesos és:

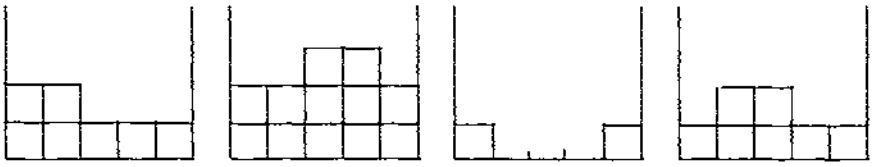
$$\left(\sum_{i=1}^{r} a_i + \sum_{i=1}^{r-1} x_i\right)\cdot e_1, \qquad \left(\sum_{i=1}^{r} b_i + \sum_{i=1}^{r-1} y_i\right)\cdot e_1, \qquad (12)$$

respectivament. Ara, la primera d'aquestes expressions és més gran o igual que la segona ja que l'única caixa que hem format amb la distribució que satisfeia (9) clarament satisfà (8). Aquesta desigualtat sumada a (11) ens dóna que A és més gran o igual que B, tal com desitjàvem.#

Aquest resultat suggereix quines Γ-configuracions són bones candidates a minimitzar sempre el valor de (3) independentment de Γ.

Definició. Considerem una configuració que consti només de caixes corresponents a extensions totalment ramificades. Ordenem les caixes de manera creixent segons l'índex de ramificació, ordenant les d'igual índex de ramificació de qualsevol manera entre elles. Denotem $t_{i,k}$ el nombre de quadradets de la k-èssima columna de la i-èssima caixa. Direm que la configuració és *normal* si satisfà les condicions (8) i (9) de l'enunciat de la Proposició 1.6. Parlarem sempre de "la" configuració normal doncs és única a menys d'una permutació de les columnes.

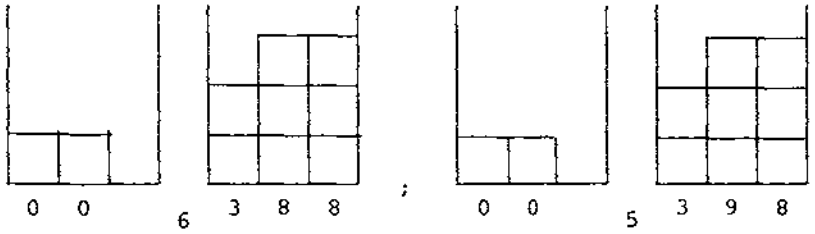
Notis que la condició (8) imposa la distribució equitativa a cadascuna de les caixes i la condició (9) la imposa a la reunió de les primeres i caixes, per a tot i. Un exemple de configuració normal pot ésser:



Ja sabem que aquesta situació ideal en la qual $R_p(f,g)$ pren sempre el mínim valor possible no es donarà en molts cassos, però tot i així sembla natural fer la:

Conjectura 1.7. Per a qualsevol $\Gamma\in\mathfrak{G}$ compost només d'extensions totalment ramificades la Γ-configuració normal és sempre mínima.

Doncs bé, si $L=\mathbb{Q}_3(\sqrt{3})$, $\Gamma=2\mathbb{Q}_3+8L$ n'és un contraexemple. En efecte, el mínim valor que pren (3) considerant Γ-famílies que tinguin la configuració normal és 25. Aquest valor es pot obtenir de dues maneres:

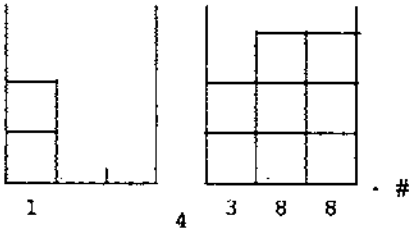


on els numerets sota de cada columna indiquen la contribució dels polinomis d'aquella columna i el numeret entre les caixes la que aporten tots els que estan a la mateixa columna però en caixes diferents. Justifiquem aquests valors:

Un polinomi Eisenstenià $f(X)=X^2+3aX+3b$ genera L si i només si $b\equiv -1 \pmod 3$; per tant, si $g(X)=X^2+3a'X+3b'\in S_L$ també és Eisenstenià, $R_3(f,g)\geqslant 3$ i $R_3(f,g)=3$ si i només si $a\not\equiv a' \pmod 3$

(vegis (4)). Per tant, per minimitzar tres polinomis de S_L sobre una mateixa columna (pensem en la columna X) és millor prendre'n dos d'Eisenstenians i un tercer amb terme independent divisible per 9, per exemple $h(X)=X^3+15X+9$. Es té $R_3(f,h)=R_3(g,h)=2$ pel Lema 1.5 i per tant $\sum_{i<j} R_3(f_i,f_j)=7$, $\sum_i i_3(f_i)=i_3(h)=1$; mentre que si els prenem tots tres Eisenstenians, encara que fem $a\equiv 0,1,-1$ (mòd.3) respectivament, tindrem $\sum_{i<j} R_3(f_i,f_j)=9$, $\sum_i i_3(f_i)=0$. Però per altra banda, un Eisenstenià fa $R_3(f,t)=1$ amb qualsevol $t(X)\in\mathbb{Z}_p[X]$ de grau 1 (Lema 1.5) mentre que $R_3(h,t)\geqslant 2$.

Ara bé, aquests mateixos raonaments mostren que $I_3(\Gamma)=24$ i que la configuració que minimitza és:



. #

Aquest exemple, que a més a més no és gens aïllat, ens fa veure que donar fòrmules per $I_p(\Gamma)$ pot ser tremendament complicat fins i tot restringits al cas en que les extensions són totalment ramificades. Fem observar que ni tan sols som capaços de calcular el valor mínim que pren (3) en una configuració normal en general doncs caldria saber, entre d'altres coses, què passa dins d'una sola caixa i això sol ja comporta una enorme complexitat (veure el Capítol 4). El que farem en el següent paràgraf és buscar elements $\Gamma\in\mathfrak{G}$ pels quals, ajudant-nos de la Proposició 1.6 poguem assegurar que la configuració normal és mínima i donar fòrmules de $I_p(\Gamma)$ només per aquests.

§3. Una fórmula

A la vista del contraexemple a la Conjectura 1.7 i de la Proposició 1.6 ens concentrarem en elements de $\mathfrak{E}$ amb un nombre prou limitat de repeticions de les extensions com perquè els valors $R_p(f,g)$ siguin tots mínims. El resultat clau que permet precisar amb detall aquesta limitació és el Teorema 1.8. En la seva prova utilitzarem un resultat del Capítol 4, on són estudiades amb més generalitat propietats dels polinomis que generen extensions totalment ramificades.

Sigui $S_n^E = \{f(X) \in S_n \text{ Eisenstenians}\}$. Considerem l'aplicació $S_n^E \xrightarrow{N} \mathbb{F}_p^*$ definida per $N(f(X))=\bar{a}_n$, si $f(X)=X^n+p\sum_{i=1}^{n} a_i X^{n-i}$. Si classifiquem els elements de S_n^E per conjugació el conjunt quocient és E_n^{ram}, el subconjunt de E format per les extensions totalment ramificades de $\mathbb{Q}_p$ de grau n.

Teorema 1.8. Sigui $n=p^s m$, $p\nmid m$.

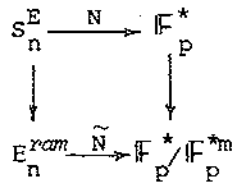
1) L'aplicació N "baixa" als respectius quocients i dóna lloc a una aplicació $E_n^{ram} \xrightarrow{\tilde{N}} \mathbb{F}_p^*/\mathbb{F}_p^{*m}$.

2) Si $p\nmid n$, $\tilde{N}$ coincideix amb la coneguda bijecció que hi ha entre aquests dos conjunts ([Hasse,1980,ch.16]).

3) Per a tot $L\in E_n^{ram}$, $\tilde{N}(L)=\tilde{N}(L_0)$, essent L_0 l'única subextensió moderadament ramificada de $L/\mathbb{Q}_p$ de grau m.

Demostració. Si $p\nmid n$ les afirmacions constitueixen el Corol.lari 4.4. En el cas general, si $L\in E_n^{ram}$ i $f(X),g(X)\in S_n^E \cap S_L$, prenem

$\pi,\pi' \in L$ arrels respectives. Tenim:



$$N_{L/\mathbb{Q}_p}(\pi)=N_{L_0/\mathbb{Q}_p}(N_{L/L_0}(\pi))=pa,$$

$$N_{L/\mathbb{Q}_p}(\pi')=N_{L_0/\mathbb{Q}_p}(N_{L/L_0}(\pi'))=pa',$$

amb $a,a' \in \mathbb{Z}_p$. Ara bé, $N_{L/L_0}(\pi)$ i $N_{L/L_0}(\pi')$ són uniformitzants de $L_0/\mathbb{Q}_p$, per tant els seus polinomis minimals sobre $\mathbb{Q}_p$ són Eisenstenians i pertanyen tots dos a S_{L_0}. Pel que sabem del cas moderadament ramificat les classes de $\bar{a}$ i $\bar{a}'$ mòdul $\mathbb{F}_p^{*m}$ coincideixen amb $\tilde{N}(L_0)$.#

En altres paraules, si $f(X),g(X) \in S_n^E$,

$$f(X) \sim g(X) \quad \Rightarrow \quad N(f(X)) = N(g(X)) \quad \text{mòdul } \mathbb{F}_p^{*m}, \qquad (13)$$

i en el cas moderadament ramificat val el recíproc. En general, si $f(X) \in S_L$, $g(X) \in S_L$, són Eisenstenians, $N(f(X))=N(g(X))$ mòdul $\mathbb{F}_p^{*m}$ implica que $L/\mathbb{Q}_p$ i $L'/\mathbb{Q}_p$ tenen la mateixa subextensió moderadament ramificada de grau m.

Ja tenim les cotes que anàvem buscant:

Corol.lari 1.9. Sigui $L/\mathbb{Q}_p$ totalment ramificada de grau $n=p^s m$, $p \nmid m$. El nombre màxim de polinomis Eisenstenians de S_L amb la propietat de que dos a dos tots tinguin $R_p(f,g)$ mínim (igual a n) és exactament de $(p-1)/(m,p-1)$.

Demostració. Per (13), si $f(X) \in S_L$ és Eisenstenià el seu terme independent és de la forma pa, on $\bar{a} \in \mathbb{F}_p^*$ pertany a una classe determinada de $\mathbb{F}_p^*/\mathbb{F}_p^{*m}$. És fàcil comprovar que els $\bar{a}$ poden prendre tots els valors d'aquesta classe; en total són $(p-1)/(m,p-1)$

$=\mathrm{card}(\mathbb{F}_p^{*m})$ valors diferents. Per (5) queda provat el Corol.lari.#

Ja estem en condicions d'enunciar la fórmula. Per 2) del Teorema 1.8, si $p\nmid n$, els polinomis de S_n^E que generen extensions distintes fan automàticament $R_p(f,g)=n$ ja que les classes (mòd.p) dels termes independents (dividits per p) pertanyen sempre a subconjunts disjunts de $\mathbb{F}_p^*$; pel Corol.lari 1.9, podem considerar elements de & en els quals les extensions de grau n estiguin repetides fins a $p(p-1)/(m,p-1)$ vegades cadascuna. En canvi, si $p|n$ poden haver extensions distintes amb la mateixa imatge per $\tilde{N}$ i per assegurar $R_p(f,g)$ mínim en tot cas hem d'exigir que per a cada $\vartheta\in \mathbb{F}_p^*/\mathbb{F}_p^{*m}$ la suma de totes les extensions de grau n amb $\tilde{N}(L)=\vartheta$ sigui menor o igual que $p(p-1)/(m,p-1)$. Per comoditat, en l'enunciat del Teorema 1.10 només donarem aquesta última condició ja que la primera hi queda englobada. Finalment destaquem que no limitem el nombre de vegades que es repeteix l'extensió trivial donat que el Teorema 0.9 ens dóna un control exacte del valor que pren $\min\{\sum_{i<j} R_p(f_i,f_j)\}$.

Teorema 1.10. Sigui $\Gamma = n_0\mathfrak{P}_p+n_1L_1+\ldots+n_rL_r\in$ & tal que les $L_i/\mathbb{Q}_p$ són totes distintes, totalment ramificades i ordenades per $[L:\mathbb{Q}_p]$ creixent sense importar l'ordre entre les del mateix grau. Suposem que per a tot $e\in\mathbb{Z}$, $e>1$, si $e=p^sm_e$, $p\nmid m_e$ se satisfà:

$$\sum_{\substack{[L_i:\mathbb{Q}_p]=e\\ \tilde{N}(L_i)=\vartheta}} n_i \leqslant p(p-1)/(m_e,p-1), \text{ per a tot } \vartheta\in \mathbb{F}_p^*/\mathbb{F}_p^{*m_e}. \quad (14)$$

Aleshores la Γ-configuració normal és mínima i:

$$I_p(\Gamma) = I_p(n_0\mathfrak{P}_p) + \sum_{i=1}^{r} [\frac{n_i}{p}](n_i - \frac{p}{2}([\frac{n_i}{p}]+1))e_i +$$

$$+ \sum_{i=0}^{r-1} \Big(n_i [\frac{u_i}{p}] + u_i [\frac{n_i}{p}] - p[\frac{u_i}{p}][\frac{n_i}{p}] + \\ + \max \{ n_i + u_i - p([\frac{n_i}{p}] + [\frac{u_i}{p}] + 1),\ 0 \} \Big) e_i, \qquad (15)$$

essent $u_i = \sum_{i<j} n_j$ i $e_i = [L_i : \Phi_p]$.

Demostració. Pels Lemes 1.4 i 1.5, el Teorema 1.8 i el Corol. lari 1.9, la condició (14) permet assegurar que la Γ-configuració normal pren el valor mínim de (3) considerant només polinomis amb $i_p(f)=0$ i tals que tots els valors de $R_p(f_i,f_j)$ són mínims excepte si tots dos polinomis estan a la primera caixa. Per altra banda no és difícil comprovar que aquest valor mínim ve donat per (15). La Proposició 1.6 ens ajudarà a provar que aquest valor és el mínim possible. No s'en desprèn de manera automàtica perquè els pesos interns de la primera caixa no són sempre mínims.

El resultat de [Hensel,1896] ja comentat al Capítol 0 de que $I_p(n_0\Phi_p)$ s'obté considerant els polinomis X-1,X-2,...,X-n_0 implica en particular que el $\min\{ \sum_{i<j} R_p(f_i,f_j) \}$ prenent t polinomis d'una mateixa columna l'obtindrem (si per exemple és la columna X) considerant els polinomis X-p,X-2p,...,X-tp. Per tant aquest mínim val:

$$\sum_{j\geq 0} [\frac{t}{p^j}] (t - p^j ([\frac{\frac{t}{p^j}]+1}{2})).$$

Això permet saber quin valor pren $\min\{ \sum_{i<j} R_p(f_i,f_j) \}$ considerant polinomis de S_{Φ_p} encara que no estiguin equitativament distribuits.

Considerem una Γ-configuració qualsevol,

$$n_i = t_{i,1} + \dots + t_{i,p}, \quad 0 \leq i \leq r.$$

Per a qualsevol Γ-família amb aquesta configuració, concedint-li que $\sum_i i_p(f_i)=0$ i que tots els $R_p(f_i,f_j)$ són mínims excepte quan tots dos polinomis són de la primera caixa tindriem:

$$\sum_{i<j} R_p(f_i,f_j) = \sum_{k=1}^{p} \Big(\sum_{j\geqslant 0} A_{j,k} \Big) + \sum_{i=1}^{r} a_i e_i + \sum_{i=0}^{r-1} x_i e_i,$$

on per a cada $0\leqslant i\leqslant r$, $1\leqslant k\leqslant p$, $j\geqslant 0$, hem denotat:

$$a_i = \frac{1}{2} \sum_{m=1}^{p} t_{i,m}(t_{i,m}-1), \quad x_i = \sum_{m=1}^{p} t_{i,m}\Big(\sum_{l>i} t_{l,m} \Big), \qquad (16)$$

$$A_{j,k} = \Big[\frac{t_{0,k}}{p^j} \Big] \Big(t_{0,k} - p^j \Big(\frac{\lfloor t_{0,k}/p^j \rfloor + 1}{2} \Big) \Big).$$

El valor (15) també el podem expressar de la mateixa manera:

$$\sum_{j\geqslant 1} B_j + \sum_{i=1}^{r} b_i e_i + \sum_{i=0}^{r-1} y_i e_i,$$

on els b_i, y_i tenen els corresponents valors de (16) però per la distribució normal i B_j denota per a tot $j\geqslant 0$:

$$B_j = \Big[\frac{n_0}{p^j} \Big] \Big(n_0 - p^j \Big(\frac{[n_0/p^j]+1}{2} \Big) \Big).$$

Per la Proposició 1.6 tenim:

$$\sum_{i=0}^{r} a_i e_i + \sum_{i=0}^{r-1} x_i e_i \geqslant \sum_{i=0}^{r} b_i e_i + \sum_{i=0}^{r-1} y_i e_i,$$

per tant només ens falta provar que:

$$\sum_{k=1}^{p} \Big(\sum_{j\geqslant 0} A_{j,k} \Big) - a_0 \geqslant \Big(\sum_{j\geqslant 1} B_j \Big) - b_0,$$

la qual cosa és equivalent a:

$$\sum_{k=1}^{p} \Big(\sum_{j\geqslant 1} A_{j,k} \Big) \geqslant \sum_{j\geqslant 2} B_j,$$

doncs clarament $a_0 = \sum_{k=1}^{p} A_{0,k}$ i $b_0 = B_1$. Provarem sumand a sumand que per a cada $j\geqslant 2$ és:

$$\sum_{k=1}^{p} A_{j-1,k} \geqslant B_j. \qquad (17)$$

Això també surt com a conseqüència de la Proposició 1.6 aplicada a una sola caixa amb valor assignat 1, p^j subdivisions i que contingui n_0 objectes distribuits:

$$n_0 = v_{1,1}+\ldots+v_{p^{j-1},1}+v_{1,2}+\ldots+v_{p^{j-1},2}+\ldots\ldots\ldots+v_{p^{j-1},p},$$

on els $v_{i,j}$ vindrien determinats al fer una distribució equitativa de cada $t_{0,k}$ en p^{j-1} subdivisions imaginàries, és a dir:

$$t_{0,k} = v_{1,k}+\ldots+v_{p^{j-1},k}, \quad 1 \leqslant k \leqslant p,$$

i imposant que $\max_{1\leqslant l<m\leqslant p^{j-1}} \{|v_{l,k}-v_{m,k}|\} \leqslant 1$. La suma de tots els pesos d'aquesta caixa dóna el membre de l'esquerra de (17) o el de la dreta segons si fem aquesta subdistribució imaginària a la primera caixa de la Γ-configuració considerada o a la de la normal. #

Al paràgraf següent tractarem el problema de determinar $i_p(K)$ només en funció de la descomposició de p en producte d'ideals de K; és a dir imaginant que no sabem quina és l'extensió local associada a cada P_i. Per aplicar el Teorema 1.10 ens hem d'assegurar que en tot cas se satisfà (14), per tant haurem d'exigir que per a tot $e>1$ el nombre d'ideals primers dividint p amb índex de ramificació e sigui $n_e \leqslant p(p-1)/(m_e,p-1)$, ja que hem de cobrir la possibilitat de que totes les extensions locals corresponents a aquests ideals tinguin la mateixa imatge per $\tilde{N}$. Fins i tot així estenem enormement el Teorema 0.9 d'Engstrom doncs aquesta restricció és força més generosa que la $\sum_{e>1} n_e \leqslant 1$ imposada per ell.

§4. Sobre la conjectura de Ore

Podem definir un *tipus de descomposició* (t.d.) com una família $\{n_{f,e}\}$, $e,f,n_{f,e}$ enters, $f,e>0$, $n_{f,e}\geq 0$, tal que $\sum_{f,e} n_{f,e}<\infty$. Donats un primer $p\in\mathbb{Z}$ i un cos de nombres K, els hi associem el t.d. que s'obté considerant que $n_{f,e}$ sigui el nombre d'ideals primers P de K tals que $e(P/p)=e$ i $f(P/p)=f$.

A [Ore,1923] es prova que donats un primer $p\in\mathbb{Z}$ i un t.d. qualsevol, sempre existeixen cossos de nombres K amb aquest t.d. associat a p i a [Ore,1928] es conjectura que per aquests cossos $i_p(K)$ pot prendre valors diferents. La conjectura és provada per Engstrom mitjançant un exemple.

El Teorema 1.2 permet assegurar que alguns t.d. si que determinen el valor de $i_p(K)$:

Corol.lari 1.11. Sigui $\{n_{f,e}\}$ un t.d. tal que per a tot e,f tals que $n_{f,e}>0$ sigui $p\nmid e$ i $(e,p^f-1)=1$. Aleshores $i_p(K)$ pren el mateix valor en tots els cossos de nombres K en els quals p té aquest t.d.

Demostració. Si $p\nmid e$ i $(e,p^f-1)=1$ hi ha, mòdul conjugació, una única extensió finita de $\mathbb{Q}_p$ amb grau residual f i índex de ramificació e. Per tant el t.d. determina $e_p(K)$.#

Remarca. En particular $i_p(K)$ queda determinat pel t.d. de p sempre que p no ramifica (*).

El fet de que en general no hi hagi una única extensió

(*) Veure [Śliwa,1982,Corollary 1].

finita de $\mathbb{Q}_p$ amb grau residual i índex de ramificació prefixats fa que una mateixa descomposició de p en producte d'ideals primers de K pugui donar lloc a diferents $e_p(K)$ i per tant a la possibilitat de $i_p(K)=I_p(e_p(K))$ diferents. No obstant, restringits al cas $f(P/p)=1$ per a tot $P|p$, el Teorema 1.10 també permet assegurar que si per a cada $e>1$ el nombre d'ideals primers amb $e(P/p)=e$ és prou reduit (vegis el comentari posterior al teorema), encara $i_p(K)$ queda determinat pel t.d.:

Corol.lari 1.12. Sigui $\{n_{f,e}\}$ un t.d. tal que:

$$\sum_e n_{f,e} \leqslant \rho(f) \quad \text{per a tot } f>1, \text{ i}$$

$$n_{1,e} \leqslant p(p-1)/(m_e,p-1) \quad \text{per a tot } e>1,$$

essent $e=p^s m_e$, $p\nmid m_e$. Aleshores $i_p(K)$ pren el mateix valor en tots els cossos de nombres K en els quals p té aquest t.d. i val:

$$i_p(K) = \sum_{i\geqslant 1} \left[\frac{n_1}{p^i}\right]\left(n_1-\frac{p^i}{2}\left(\left[\frac{n_1}{p^i}\right]+1\right)\right) + \sum_{e>1}\left[\frac{n_e}{p}\right]\left(n_e-\frac{p}{2}\left(\left[\frac{n_e}{p}\right]+1\right)\right)e +$$

$$+ \sum_{e\geqslant 1}\left(n_e\left[\frac{u_e}{p}\right]+u_e\left[\frac{n_e}{p}\right]-p\left[\frac{n_e}{p}\right]\left[\frac{u_e}{p}\right]+\max\left\{n_e+u_e-p\left(\left[\frac{n_e}{p}\right]\left[\frac{u_e}{p}\right]+1\right),0\right\}\right)e,$$

on hem denotat $n_e=n_{1,e}$ i $u_e=\sum_{k>e} n_k$ per a tot e.#

Remarca. Aquest resultat mostra que fins i tot en aquests cassos en que $i_p(K)$ ve determinat pel t.d. de p les fórmules de [Sukallo,1955] són incorrectes.

Finalment, si el t.d. de p permet la possibilitat de $e_p(K)$ diferents i el nombre de primers amb $e(P/p)$ i $f(P/p)$ determinats augmenta, $i_p(K)$ no queda determinat pel t.d.. Veiem-ho en detall

considerant, per exemple, una acumulació d'ideals primers tots satisfent $f(P/p)=1$, $e(P/p)=e$, amb e fix tal que $(m,p-1)>1$, si és $e=p^s m$, $p\nmid m$. Imaginem una caixa amb p subdivisions on col.loquem , segons el polinomi de $\mathbb{F}_p[X]$ de grau 1 associat, polinomis de $\mathbb{Z}_p[X]$ que generen extensions totalment ramificades de grau e, sense distingir-ne cap d'específica. Si considerem $t = (p(p-1)/(m,p-1))+1$ d'aquests polinomis i els repartim equitativament n'hi haurà $(p-1)/(m,p-1)$ a cada subdivisió excepte una (suposem que és la que correspon a X) on n'hi haurà un més. Ara, si tots els polinomis generen extensions amb la mateixa imatge per $\tilde{N}$, en aquesta subdivisió no serà possible que tots els $R_p(f,g)$ siguin mínims; en canvi, si no tots generen extensions amb el mateix $\tilde{N}(L)$, si que podrem aconseguir que a la columna conflictiva tots els polinomis siguin Eisenstenians i amb termes independents (dividits per p) no congruents dos a dos (mod.p).

Això confirma amb més rotunditat la conjectura de Ore. Podem enunciar un principi general que digui: *un mateix t.d. donarà lloc a un valor de* $i_p(K)$ *més alt quantes més repeticions d'elements de* E *presenti* $e_p(K)$.

Tornant a l'exemple anterior, si $p\nmid e$ i $L_1 \neq L_2$ són dues extensions totalment ramificades de grau e tenim:

$$I_p((t-1)L_1+L_2) = \frac{(p-1)e}{2(e,p-1)}\left(\frac{p(p-1)}{(e,p-1)} - (p-2)\right),$$

i en canvi:

$$I_p(tL_1) = I_p((t-1)L_1+L_2) + 1.$$

La primera igualtat surt de considerar que cada parella de polinomis en la mateixa subdivisió fa $R_p(f,g)=e$. La segona surt de

considerar que a la columna conflictiva hi ha una parella que fa $R_p(f,g)=e+1$, cosa que es pot aconseguir per (4) fent que la parella que obligatòriament té $\bar{a}_e \equiv \bar{b}_e \pmod{p}$ tingui $\bar{a}_{e-1} \not\equiv \bar{b}_{e-1} \pmod{p}$, si $f(X)=X^e+p\sum_{i=1}^{e} a_i X^{e-i}$ i $g(X)=X^e+p\sum_{i=1}^{e} b_i X^{e-i}$. En particular, per $p=3$ i $e=2$ (aleshores $t=4$) això esclareix completament el fenomen observat per Engstrom. Ara sabem que *si K és un cos de nombres de grau 8 en el qual* $3 = (P_1 \cdot P_2 \cdot P_3 \cdot P_4)^2$, $i_3(K)$ *val 3 ó 2 segons si les quatre extensions locals coincideixen o no.*

Clarament, els resultats d'aquest capítol mostren que aquest fenomen s'estén i amplia tant com es vulgui. Per exemple, continuant en el cas $p=3, e=2$, tenim que els cossos de nombres de grau 14 pels quals $3 = (P_1 \cdot \ldots \cdot P_7)^2$ tenen:

$$i_3(K) = 14,\ 13,\ 12 \text{ ó } 11,$$

respectivament, segons si:

$$e_3(K) = 7L_1,\ 6L_1+L_2,\ 5L_1+2L_2 \text{ ó } 4L_1+3L_2,$$

i els mateixos valors si intercanviem L_1 i L_2 els quals en aquest cas denoten les dues úniques extensions quadràtiques ramificades de $\mathbb{Q}_3$.

§5. Conclusió

Creiem haver fet palès que la tasca de calcular $I_p(\Gamma)$ per a tot $\Gamma \in \mathfrak{G}$ adquireix unes característiques realment infernals. Fins i tot restringits al cas en que totes les extensions són totalment ramificades, sortir-se de les cotes del Teorema 1.10 pot portar a situacions molt complicades (recordem el contraexem-

ple a la Conjectura 1.7).

Els resultats del Capítol 2, el qual està dedicat a profunditzar més en el càlcul de $R_p(f,g)$ podrien fer-nos millorar el Teorema 1.10 ampliant una mica més el nombre i/o tipus de les extensions, però més que continuar en aquesta línia hem preferit concentrar-nos en el problema que creiem que pot ser el millor "següent pas" que es pot donar després del que s'ha fet en aquest capítol: què passa dins d'una sola caixa?, és a dir, quin valor pren $I_p(nL)$ per a qualsevol $L\in E$?. En el Capítol 3 donem una resposta completa quan L és no-ramificada i en el Capítol 4 no tant completa si L ramifica totalment i moderada. Fem observar que d'aquesta manera queda englobat l'estudi de $i_p(K)$ pels cossos de nombres K Galoisians.

Un altre fet que volem destacar és que pels cossos de nombres Galoisians la conjectura de Ore no ha perdut vigència. En efecte, hem comprovat que el t.d. de p no determina $i_p(K)$ a causa de l'aparició, en major o menor quantitat, d'extensions locals repetides, però en el cas Galoisià no tenim elecció, les extensions locals són sempre totes iguals. Així, en l'exemple d'Engstrom veiem que els cossos de nombres Galoisians de grau vuit en els quals $3=(P_1P_2P_3P_4)^2$ tenen dues possibilitats: $e_3(K)=4L_1$ ó $4L_2$, però en tots dos cassos és $i_3(K)=I_3(4L_1)=I_3(4L_2)=3$. De manera que té sentit considerar encara la:

Conjectura 1.13. Si $L,L'\in E$ són Galoisianes i tenen el mateix grau residual i índex de ramificació aleshores $I_p(nL)=I_p(nL')$ per a tot n.#

Els resultats dels Capítols 3 i 4 semblen indicar que això serà cert si L i L' són moderadament ramificades. Pensem en canvi que la conjectura no és certa en el cas salvatgement ramificat, sino que s'ha de modificar en el següent sentit:

Conjectura 1.14. Si $L,L' \in E$ són Galoisianes i tenen els mateixos nombres de ramificació aleshores $I_p(nL)=I_p(nL')$ per a tot n.#

S'obtindria així una propietat en certa manera paral.lela a la 4) del Capítol 0. Indiquem finalment que una resposta a aquesta qüestió deu passar segurament per l'adopció del punt de vista topològic de Krasner i probablement per un estudi en profunditat dels seus treballs.

Capítol 2. El polígon de Newton en el càlcul de $i_p(f)$ i $R_p(f,g)$

El polígon de Newton fou aplicat per primera vegada a la teoria algebraica de nombres a [Bauer,1907] i es convertí aviat en una eina revolucionària. Ore, en els anys 1923-1928, la generalitza i perfecciona fins convertir-la en una amplíssima generalització del lema de Hensel amb nombroses aplicacions. Dediquem aquest capítol a mostrar una nova aplicació d'aquesta vella (i bella!) eina. En efecte, com veurem en els §1 i 3, les tècniques del polígon es revelen com les més adequades per fer un estudi amb profunditat sobre el càlcul de $R_p(f,g)$. La utilitat del polígon per calcular $i_p(f)$ ja havia estat destacada pel propi Ore a [Ore,1925,th.8]; al §2 retrobem, lleugerament millorat, aquest resultat. El §0 està dedicat a fer un repàs de la terminologia i principals resultats que necessitarem del polígon, els quals es poden trobar a [Ore,1928]. Naturalment, aquí adoptarem el punt de vista p-àdic, cosa a la qual Ore, per desgràcia, es mostrà reaci.

Al llarg de tot el capítol p denotarà un nombre primer fix i $\varphi(X)$ un polinomi mònic i irreduible de $\mathbb{F}_p[X]$ de grau $d \geqslant 1$. Identificarem sempre que ens convingui $\varphi(X)$ amb el polinomi de $\mathbb{Z}_p[X]$ obtingut escollint per a cada coeficient un representant d'entre $\{0,1,\ldots,p-1\}$. Denotarem per T l'única extensió no-ramificada de $\mathbb{Q}_p$ de grau d i p serà l'ideal primer de T. Denotarem també $q = p^d$.

§0. Preliminars

Sigui $f(X)\in \mathbb{Q}_p[X]$, mònic, de grau n i sigui $t=[\frac{n}{d}]$. Hi ha una única manera d'expressar f(X) com un polinomi en $\varphi(X)$:

$$f(X) = \sum_{i=0}^{t} Q_i(X)\varphi(X)^{t-i}, \qquad (1)$$

si exigim que $gr(Q_i(X)) < d$ per a tot i. Sigui u_i el màxim enter tal que p^{u_i} divideix tots els coeficients de $Q_i(X)$; al ser f(X) mònic sempre serà $u_0=0$. El $\varphi(X)$-*polígon* de f(X) és l'envoltura convexa inferior del conjunt $\{(i,u_i),\ 0\leqslant i\leqslant t\}$ de punts del pla Euclidià (vegis fig.1). Si $Q_i(X)=0$, considerem $u_i=\infty$ i el punt (i,u_i) no es dibuixa. El polígon de Newton clàssic s'obté considerant $\varphi(X)=X$.

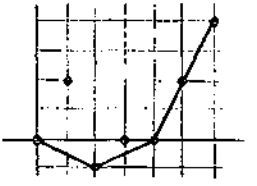


fig.1

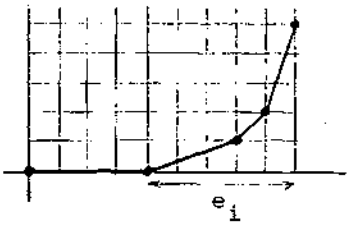
Si $f(X)\in\mathbb{Z}_p[X]$, el seu $\varphi(X)$-polígon no té cap costat amb pendent negativa i n'hi ha algun amb pendent no nul.la si i només si $\varphi(X)$ divideix f(X) (mod.p). Al conjunt de costats amb pendent estrictament positiva l'anomenem el $\varphi(X)$-*polígon principal* de f(X). Si tenim:

$$f(X) \equiv \varphi_1(X)^{e_1}\cdot\ldots\cdot\varphi_r(X)^{e_r} \pmod{p},$$

pel lema de Hensel f(X) factoritza a $\mathbb{Z}_p[X]$:

$$f(X) = g_1(X)\cdot\ldots\cdot g_r(X),$$

cadascun d'ells satisfent $g_i(X)\equiv\varphi_i(X)^{e_i} \pmod{p}$. Clarament el $\varphi_i(X)$-polígon de f(X) té la forma:



Doncs bé, el $\varphi_i(X)$-polígon de cada $g_i(X)$ coincideix amb el $\varphi_i(X)$-polígon principal de $f(X)$, per tant ens podem restringir en general a l'estudi del $\varphi(X)$-polígon de polinomis de grau múltiple de d. Això surt com a conseqüència d'un resultat més general que relaciona el polígon d'un producte de polinomis amb els polígons dels factors:

Teorema del producte. Siguin $g(X), h(X) \in \mathbb{Z}_p[X]$ mònics. El $\varphi(X)$-polígon principal de $g(X)h(X)$ s'obté empalmant els costats dels respectius $\varphi(X)$-polígons principals de $g(X)$ i $h(X)$ en ordre creixent de pendents.#

El veritable interès del polígon radica en que, recíprocament, l'existència de diversos costats en un polígon indica que el polinomi factoritza, si més no, en el mateix nombre de factors; en conseqüència cada $\varphi_i(X)$-polígon principal de $f(X)$ proporciona una ulterior factorització de cada $g_i(X)$. En efecte:

Teorema del polígon. Sigui $h(X) \in \mathbb{Z}_p[X]$ mònic i de grau múltiple de d. Siguin $S_1, \ldots, S_k$ els costats del seu $\varphi(X)$-polígon i $m_1, \ldots, m_k$ les seves respectives projeccions sobre l'eix d'abscisses. Aleshores $h(X)$ factoritza:

$$h(X) = h_1(X) \cdot \ldots \cdot h_r(X),$$

on cada $h_i(X)$ és un polinomi mònic de $\mathbb{Z}_p[X]$ de grau dm_i i el seu $\varphi(X)$-polígon té un sol costat igual a S_i. A més a més, per a qualsevol arrel θ de $h(X)$, $v_p(\varphi(\theta))$ coincideix amb la pendent del costat S_j corresponent a l'únic polinomi $h_j(X)$ del qual θ és arrel .#

Siguin $f(X)\in\mathbb{Z}_p[X]$ mònic, $Q_i(X)$, u_i com a (1) i $S_1,\ldots,S_k$ els costats del $\varphi(X)$-polígon principal de $f(X)$. Siguin m_i,h_i les projeccions de cada S_i sobre els eixos d'abscisses i ordenades respectivament i denotem $\epsilon_i=(m_i,h_i)$ i $\lambda_i=m_i/\epsilon_i$. Si S_i comença al punt (s,u_s) denotem per a tot $0\leqslant j\leqslant\epsilon_i$, $s_j=s+j\lambda_i$ i:

$$A_j(X) = \begin{cases} Q_{s_j}(X)/p^{u_{s_j}} & \text{si } (s_j,u_{s_j})\in S_i, \\ 0 & \text{en cas contrari.} \end{cases}$$

La imatge del polinomi:

$$F_i(X,Y) = A_0(X)Y^{\epsilon_i} + A_1(X)Y^{\epsilon_i-1} +\ldots+ A_{\epsilon_i}(X), \qquad (2)$$

a $\mathbb{Z}_p[X,Y]/(p,\varphi(X)) \cong \mathbb{F}_q[Y]$ l'anomenarem el *polinomi associat* a S_i. Aquests polinomis possibiliten una aplicació a un "segon nivell" del Teorema del producte i el Teorema del polígon. Concretament tenim, conservant les notacions:

Primer teorema dels polinomis associats. Siguin $g(X),h(X)\in\mathbb{Z}_p[X]$ mònics. Els costats del $\varphi(X)$-polígon principal de $g(X)h(X)$ que coincideixen amb un costat del polígon de només un dels dos polinomis tenen el mateix polinomi associat que aquest costat del qual provenen. Els costats constituits empalmant dos costats d'igual pendent, un de cada polígon, tenen per polinomi associat el producte dels polinomis associats d'aquests costats.#

Segon teorema dels polinomis associats. Sigui $f(X) \in \mathbb{Z}_p[X]$ mònic. Si el polinomi associat a un costat del $\varphi(X)$-polígon de $f(X)$ factoritza:

$$F(Y) = F_1(Y)^{e_1} \cdot \ldots \cdot F_r(Y)^{e_r},$$

a $\overline{\mathbb{F}}_q[Y]$, aleshores el factor $f_i(X)$ de $f(X)$ corresponent a aquest costat (donat pel Teorema del polígon) té una factorització:

$$f_i(X) = t_1(X) \cdot \ldots \cdot t_r(X),$$

on cada $t_j(X) \in \mathbb{Z}_p[X]$ és mònic, de grau $d\lambda_i e_j gr(F_j(Y))$ i té per $\varphi_i(X)$-polígon un costat de la mateixa pendent i polinomi associat $F_j(Y)^{e_j}$.#

Un polinomi $f(X) \in \mathbb{Z}_p[X]$ diem que és $\varphi(X)$-*regular* si cap dels polinomis associats als costats del seu $\varphi(X)$-polígon principal té arrels múltiples. Direm que $f(X)$ és *regular* si és $\varphi(X)$-regular per a tot factor irreduïble de $f(X)$ (mod.p). Un polinomi de $\mathbb{Z}[X]$ diem que és p-*regular* si és regular considerat com a polinomi de $\mathbb{Z}_p[X]$.

Pel Segon teorema dels polinomis associats podem obtenir la completa factorització en producte d'irreduïbles de qualsevol polinomi regular de $\mathbb{Z}_p[X]$. Després de provar (no constructivament) que tot cos de nombres admet una equació definidora p-regular Ore resol, però només teòricament, el problema d'obtenir la descomposició de p en producte d'ideals primers en un cos de nombres. Però l'interès que tenim nosaltres en el concepte de polinomi regular radica en el següent:

Teorema de Ore. Sigui $f(X) \in \mathbb{Z}[X]$ irreduible. Siguin $S_1,\ldots,S_k$ els costats del $\varphi(X)$-polígon principal de $f(X)$, m_i,h_i les projeccions de cada S_i sobre els eixos d'abscisses i ordenades respectivament i denotem $\epsilon_i=(m_i,h_i)$. L'expressió:

$$I_\varphi = d\left(\sum_{i=2}^{k} m_i \left(\sum_{j=1}^{i-1} h_j \right) + \frac{1}{2} \sum_{i=1}^{k} (m_i h_i - m_i - h_i + \epsilon_i) \right),$$

compta, treient el factor d, el nombre de punts de coordenades enteres que hi ha sota del $\varphi(X)$-polígon, sense comptar els de l'eix d'abscisses ni els de l'última ordenada. Doncs bé,

$$i_p(f) \geqslant \Sigma\, I_\varphi,$$

variant la suma entre tots els factors irreduïbles de $f(X)$ (mod.p). Si $f(X)$ és p-regular val la igualtat.#

Remarca. Conceptualment, i també a l'hora de les demostracions, aquesta generalització de Ore del concepte del polígon de Newton consisteix, en el fons, simplement en aplicar el polígon clàssic a la situació relativa en la qual T sigui el cos base; a menys d'un canvi lineal de la variable. No obstant, el llenguatge del $\varphi(X)$-polígon, a més a més de ser el més adequat per presentar els resultats, és imprescindible a l'hora de fer-los efectius en cassos concrets.

§1. El polígon de Newton en el càlcul de $R_p(f,g)$

Siguin $f(X),g(X)$ dos polinomis mònics de $\mathbb{Z}_p[X]$. Podem obtenir $R(f,g)$ calculant el conegut determinant d'ordre $gr(f(X))+gr(g(X))$ amb els coeficients, però aquest procediment, apart de

la considerable feixugesa que comporta, només és vàlid si tenim els dos polinomis donats explícitament. De cara al càlcul de $I_p(\Gamma)$ ens interessen mètodes que permetin calcular $R_p(f,g)$ (tampoc volem el valor precís de $R(f,g)$) a partir de propietats més generals dels polinomis i/o els seus coeficients.

Veurem en aquest paràgraf com els $\varphi(X)$-polígons respecte dels factors irreduïbles de $f(X)$ i $g(X)$ (mod.p) donen una primera aproximació al valor de $R_p(f,g)$ i també en quines condicions aquesta aproximació és exacta. Concretament el nostre objectiu és provar el següent:

Teorema 2.1. Siguin $f(X)$, $g(X) \in \mathbb{Z}_p[X]$ mònics. Siguin $S_1,\ldots,S_k$ (resp. $S'_1,\ldots,S'_{k'}$) els costats del $\varphi(X)$-polígon principal de $f(X)$ (resp. $g(X)$) i m_i,h_i (resp. m'_i,h'_i) les projeccions de cada costat als eixos d'abscisses i ordenades respectivament. Doncs bé, si denotem:

$$R_\varphi(f,g) = d \sum_{i,j} \inf\{m_i h'_j, m'_j h_i\}, \quad \text{tenim:}$$

$$R_p(f,g) \geqslant \Sigma\, R_\varphi(f,g),$$

variant la suma entre els factors irreduïbles comuns de $f(X)$ i $g(X)$ (mod.p). Val la igualtat si i només si no hi ha dos costats dels $\varphi(X)$-polígons principals de $f(X)$ i $g(X)$ amb la mateixa pendent i polinomis associats no primers entre si.#

Observis que el Lema 1.5 no és més que una aplicació d'aquest resultat a cassos molt particulars.

Per demostrar el Teorema 2.1 el primer que necessitem és esclarir el significat dels polinomis associats:

Lema 2.2. Sigui $f(X)\in\mathbb{Z}_p[X]$ mònic, irreduïble i tal que $f(X)\equiv\varphi(X)^m \pmod{p}$. Sigui h la projecció sobre l'eix d'ordenades de l'únic costat S del $\varphi(X)$-polígon de $f(X)$; siguin $\epsilon=(m,h)$, $\lambda=m/\epsilon$ i $\chi=h/\epsilon$. Sigui $\tau\in T$ una arrel qualsevol de $\varphi(X)$. Sigui $F(Y)\in\mathbb{F}_q[Y]$ la imatge del polinomi associat a S per l'isomorfisme $\mathbb{Z}_p[X,Y]/(p,\varphi(X))\cong\mathbb{F}_q[Y]$ donat per fer $X=\tau$ i prendre classe $(\mathrm{mod}.p)$. Aleshores el conjunt de les arrels de $F(Y)$ coincideix amb $\Sigma_\tau=\{\overline{\varphi(\theta)^\chi/p^\lambda},\ \theta$ arrel de $f(X)$ tal que $v_p(\theta-\tau)>0\}$.

Demostració. Sigui θ una arrel qualsevol de $f(X)$ tal que $v_p(\theta-\tau)>0$ i denotem $\omega=\varphi(\theta)^\chi/p^\lambda$. $v_p(\omega)=0$, per tant és un enter; sigui $g(Y)=\mathrm{Irr}(\omega,T)$ i $\bar{g}(Y)\in\mathbb{F}_q[Y]$ la imatge $(\mathrm{mod}.p)$ de $g(Y)$. Clarament $\bar{g}(Y)$ és una potència d'un polinomi irreduïble de $\mathbb{F}_q[Y]$ i el conjunt de les seves arrels coincideix amb Σ_τ. Sigui:

$$f(X)=\sum_{i=0}^{m}Q_i(X)\cdot\varphi(X)^{m-i},$$

i u_i l'exponent màxim amb el qual p divideix cada $Q_i(X)$. Clarament $u_m=h$. Si posem $Q_i(X)=p^{u_i}R_i(X)$, com que $\mathrm{gr}(R_i(X))=\mathrm{gr}(Q_i(X))<d$, $\varphi(X)=\mathrm{Irr}(\bar{\theta},\mathbb{F}_p)$ i $R_i(X)\not\equiv 0 \pmod{p}$, a la força $v_p(R_i(\theta))=0$ i per tant $v_p(Q_i(\theta))=u_i$. Per altra banda, $v_p(\varphi(\theta))=h/m$ pel Teorema del polígon, per tant tenim:

$$v_p(Q_i(\theta)\cdot\varphi(\theta)^{m-i})=u_i+(m-i)\frac{h}{m}\geqslant i\frac{u_m}{m}+(m-i)\frac{h}{m}=h,$$

per a tot $0\leqslant i\leqslant m$. I hi ha igualtat si i només si $u_i=i\frac{u_m}{m}$, és a dir si i només si el punt en qüestió pertany al costat del polígon. En conseqüència, la suma de tots els $Q_i(\theta)\varphi(\theta)^{m-i}$ amb v_p mínim igual a h coincideix amb:

$$T=p^h\,F(\theta,\varphi(\theta)^\chi/p^\lambda),$$

on $F(X,Y)$ denota el polinomi definit a (2). Com que:

$$0 = f(\theta) = \sum_{i=0}^{m} Q_i(\theta)\cdot\varphi(\theta)^{m-i},$$

a la força $v_p(T) > h$, o equivalentment:

$$v_p(F(\theta,\varphi(\theta)^{\chi}/p^{\lambda})) > 0.$$

Aquesta expressió indica exactament que ϖ és una arrel de $F(Y)$. Pel Segon teorema dels polinomis associats $F(Y)$ és una potència d'un polinomi irreduïble de $\mathbb{F}_q[Y]$, i com que $\bar{g}(Y)$ té la mateixa propietat, el fet de que tinguin una arrel comuna implica que les tenen totes (sense comptar la multiplicitat).#

Tenint en compte la bilinealitat de la resultant respecte del producte de polinomis, el Teorema del producte i el Primer teorema dels polinomis associats permeten reduir la prova del Teorema 2.1 al cas en que els dos polinomis són irreduïbles. Ens cal provar per tant:

Proposició 2.3. Siguin $f(X)$, $g(X)\in\mathbb{Z}_p[X]$ mònics, irreduïbles i de grau $n=md, n'=m'd$ respectivament. Siguin $\eta,\mu\in\mathbb{Q}$ les pendents respectives de l'únic costat S,S' que té cada $\varphi(X)$-polígon. Aleshores:

$$R_p(f,g) \geqslant \frac{nn'}{d}\inf\{\eta,\mu\}.$$

Si $\eta\neq\mu$ val sempre la igualtat i si $\eta=\mu>0$ hi ha igualtat si i només si els polinomis associats respectius són primers entre si.

Demostració. Si $\eta=\mu=0$ afirmem una trivialitat. Si una de les dues pendents és nul.la i l'altra no, afirmem que $R_p(f,g)=0$, i és cla-

rament cert doncs un polinomi té $\varphi(X)$ com a únic factor irreduïble (mod.p) i l'altre no és divisible per $\varphi(X)$ (mod.p). Suposem per tant que $\eta,\mu>0$.

Siguin $\beta_1,\ldots,\beta_m$ les arrels de $g(X)$. Ja sabem que,

$$R_p(f,g) = \sum_{i=1}^{n'} v_p(f(\beta_i)) = n' v_p(f(\beta)),$$

essent β una qualsevol d'aquestes arrels. Amb els usuals significats per $Q_i(X)$ i u_i, tal com hem vist a la prova del Lema 2.2 tindrem $v_p(Q_i(\beta))=u_i$, $v_p(\varphi(\beta))=\mu$ i:

$$v_p(Q_i(\beta)\varphi(\beta)^{m-i}) = u_i+(m-i)\mu \geqslant i\eta+(m-i)\mu \geqslant m\cdot\inf\{\eta,\mu\}, \quad (3)$$

per a tot $0\leqslant i\leqslant m$. Per tant:

$$v_p(f(\beta)) \geqslant m\cdot\inf\{\eta,\mu\} \quad \text{i} \quad R_p(f,g) \geqslant n'm\cdot\inf\{\eta,\mu\}. \qquad (4)$$

Si $\eta\neq\mu$ l'última desigualtat de (3) és estricta per a tots els sumands excepte per un, el primer si $\eta<\mu$ ó l'últim si $\eta>\mu$, pels quals l'altra desigualtat de (3) és sempre una igualtat. De manera que en aquest cas tenim igualtats a (4). Si $\eta=\mu$, (3) és una cadena d'igualtats si i només si $u_i=i\mu$, és a dir si i només si el corresponent punt pertany al costat del polígon. Per tant, la suma de tots els $Q_i(\beta)\varphi(\beta)^{m-i}$ amb v_p mínim i igual a $m\mu$ coincideix amb:

$$p^{u_m} F(\beta,\omega),$$

on $\omega=\varphi(\beta)^{\chi}/p^{\lambda}$, si $\lambda=m/\epsilon$, $\chi=u_m/\epsilon$, essent $\epsilon=(m,u_m)$; i $F(X,Y)$ denota el polinomi definit a (2). En conseqüència, $R_p(f,g)>n'm\mu$ si i només si $v_p(f(\beta))>m\mu$ per alguna arrel β de $g(X)$ i:

$$v_p(f(\beta))>m\mu \Leftrightarrow v_p(p^{u_m}F(\beta,\omega))>m\mu \Leftrightarrow v_p(F(\beta,\omega))>0. \quad (5)$$

Sigui $\tau \in T$ l'única arrel de $\varphi(X)$ tal que $v_p(\beta - \tau) > 0$. Siguin $F(Y)$, $G(Y) \in \mathbb{F}_q[Y]$ les imatges dels respectius polinomis associats a S i S' per l'isomorfisme $\mathbb{Z}_p[X,Y]/(p,\varphi(X)) \cong \mathbb{F}_q[Y]$ donat per fer $X=\tau$ i prendre classe (mod.p). L'última condició de (5) assegura que $\bar{\omega}$ és una arrel de $F(Y)$, però pel Lema 2.2 $\bar{\omega}$ és sempre una arrel de $G(Y)$, per tant (5) implica que tenen una arrel en comú. Recíprocament, pel Lema 2.2 totes les arrels de $G(Y)$ són de la forma $\overline{\varphi(\beta)^X/p^\lambda}$, essent β una arrel de $g(X)$ tal que $v_p(\beta-\tau) > 0$, per tant, l'existència d'una arrel en comú amb $F(Y)$ implica (5).#

Remarca. La Proposició 2.3 és vàlida a posteriori per polinomis amb $\varphi(X)$-polígon d'un sol costat encara que no siguin irreduïbles i així serà utilitzada algun cop més endavant.

Veiem a continuació un exemple que mostra la limitació del Teorema 2.1 per calcular en general $R_p(f,g)$ de dos polinomis qualsevols i confirma el qualificatiu de "primera aproximació" al valor de $R_p(f,g)$ que li donàvem.

Siguin $F(X), G(X) \in \mathbb{Z}_p[X]$ mònics, de grau n i tals que $F(X) \equiv G(X) \equiv X^n$ (mod.p). Apliquem a aquests polinomis les transformacions:

$$Y = p^s(X+a), \quad Y = p^{s'}(X+a'),$$

respectivament, on $s,s' > 0$ i $a,a' \in \{1,2,\ldots,p-1\}$. Siguin $f(Y), g(Y)$ els polinomis que s'obtenen. Que diu el Teorema 2.1 sobre el valor de $R_p(f,g)$? Doncs:

"$R_p(f,g) \geqslant n^2 \inf\{s,s'\}$,

si $s \neq s'$ hi ha igualtat i si $s = s'$ hi ha igualtat si i només si $a \neq a''$. Per tant, si $s = s'$ i $a = a'$ estem tan lluny com es vulgui de conèixer el veritable valor de $R_p(f,g)$ doncs clarament:

$$R_p(f,g) = n^2 s + R_p(F,G).$$

Pensem també que podriem empalmar una cadena arbitràriament llarga de transformacions com aquestes i el Teorema 2.1 sempre ens donaria només la contribució a $R_p(f,g)$ de l'últim esglaó.

No obstant, veurem en els Capítols 3 i 4 com en certa manera el Teorema 2.1 i un derivat seu, el Teorema 2.6, poden considerar-se com una eina perfectament suficient per calcular $R_p(f,g)$. Aquest exemple té estreta relació amb la manera com solventem en aqueixos capítols aquesta aparent limitació de les tècniques del polígon per calcular $R_p(f,g)$.

§2. El polígon de Newton en el càlcul de $i_p(f)$

Curiosament, els resultats del paràgraf anterior sobre el càlcul de $R_p(f,g)$ permeten donar una prova del Teorema de Ore radicalment més curta que l'original [Ore,1925]. Estendrem de passada el resultat a polinomis $f(X) \in \mathbb{Z}_p[X]$ qualsevols i veurem també que *la condició de regularitat és no només suficient sino també necessària perquè* $i_p(f)$ *coincideixi amb la cota inferior que dóna el Teorema de Ore.*

A la vista del Teorema 0.7 podem definir $i(f)$ per a un polinomi $f(X) \in \mathbb{Z}_p[X]$ qualsevol com:

$$i(f) = \prod_{1 \leq i < j \leq r} R(f_i, f_j) \cdot \prod_{j=1}^{r} i(f_j), \qquad (6)$$

on $f(X)=\prod_{i=1}^{r} f_i(X)$ és la seva factorització en producte d'irreduïbles. Fem notar que a posteriori (6) continua essent vàlida per a una factorització qualsevol.

D'entrada, el Teorema 2.1 (o més pròpiament la Proposició 2.3) ens permeten donar una "reinterpretació geomètrica" del Teorema de Ore. En efecte, els punts de coordenades enteres sota del $\varphi(X)$-polígon sense comptar els de l'eix d'abscisses ni els de l'última ordenada els podem subdividir en diversos grups: d'una banda els que estan sota dels triangles determinats per cada costat, i la resta, els podem agrupar en rectangles, un rectangle per cada parella de costats; seguint també el criteri de no comptar els punts de la linia horitzontal inferior ni els de la vertical de la dreta (vegis fig.2). Sigui:

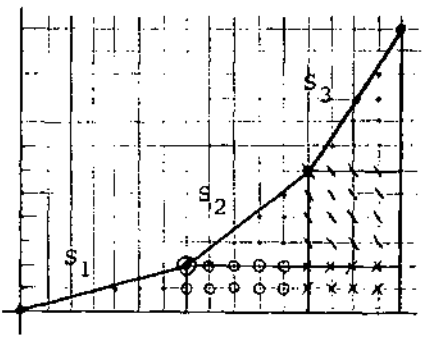


fig.2

$$f(X) = f_1(X)\cdot\ldots\cdot f_k(X),$$

la factorització de $f(X)$ que ens dóna el Teorema del polígon. D'acord amb la nostra definició tenim:

$$i_p(f) = \sum_{1\leq i<j\leq k} R_p(f_i,f_j) + \sum_{i=1}^{k} i_p(f_i).$$

Ara, el nombre de punts del triangle corresponent al costat S_i coincideix amb el nombre de punts sota del $\varphi(X)$-polígon de $f_i(X)$ i per tant, pel Teorema de Ore aquest nombre serà més gran o igual que $i_p(f_i)$. I d'altra banda, per la Proposició 2.3 el nombre de punts del rectangle determinat pels costats S_i i S_j coincideix exactament amb $R_p(f_i,f_j)$. Així, per exemple, un polinomi

que tinguès un $\varphi(X)$-polígon com el de la fig.2 descomposa en producte de tres factors satisfent:

$$i_p(f_1) \geq 3d, \quad i_p(f_2) \geq 6d \quad i_p(f_3) \geq 8d, \tag{7}$$

$$R_p(f_1,f_2) = 10d, \; R_p(f_1,f_3) = 8d, \; R_p(f_2,f_3) = 16d.$$

Si f(X) fos regular ho serien en particular tots els seus factors i a (7) tot serien igualtats.

Però de passada, aquesta reinterpretació mostra que podem reduir una prova del Teorema de Ore al cas en que f(X) té un $\varphi(X)$-polígon d'un sol costat. Suposem-ho així d'ara endavant. Encara més, ens podem reduir al cas en que f(X) és irreduïble. En efecte, qualsevol factorització, $f(X) = \prod_{i=1}^{r} f_i(X)$, permet una ulterior subdivisió dels punts sota de l'únic costat del polígon entre triangles, un per cada factor, i rectangles, un per a cada parella de factors. Així, si el polinomi $f_3(X)$ de l'exemple anterior factoritzés en producte de dos polinomis $f_3(X)=F(X)G(X)$, els $\varphi(X)$-polígons de F(X) i G(X) són troços del costat del polígon de $f_3(X)$ i els punts sota d'aquest costat queden subdividits com s'indica a la fig.3. Tindriem en aquesta ocasió:

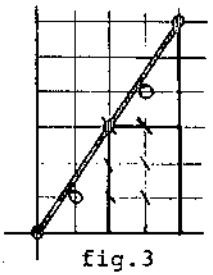


fig.3

$$i_p(F) \geq d, \; i_p(G) \geq d \quad i \quad R_p(F,G) \geq 6d.$$

Efectivament, en aquesta nova subdivisió el nombre de punts de cada rectangle no té perquè coincidir amb $R_p(f_i,f_j)$, però també sabem per la Proposició 2.3 que hi coincidirà per a tot i,j si i només si els polinomis associats als $f_i(X)$ són tots primers entre si. Si f(X) és regular clarament se satisfà aquesta condi-

ció i recíprocament, si aquesta condició és satisfeta la regularitat de $f(X)$ és equivalent a la regularitat de cada $f_i(X)$. Queda clar per tant que una prova del Teorema de Ore queda reduïda a provar:

Proposició 2.4. Sigui $f(X)\in\mathbb{Z}_p[X]$ mònic, irreduïble i tal que $f(X)\equiv\varphi(X)^m \pmod{p}$. Aleshores:

$$i_p(f) \geqslant \frac{d}{2}(mh-m-h+\epsilon),$$

on h és la projecció sobre l'eix d'ordenades de l'únic costat del $\varphi(X)$-polígon de $f(X)$ i $\epsilon=(m,h)$. Val la igualtat si i només si $f(X)$ és regular.

Demostració. Siguin θ arrel de $f(X)$, $L=\mathbb{Q}_p(\theta)$ i P l'ideal primer de L. Sabem que $\mathbb{Q}_p\subset T\subset L$. Siguin $\tau_1,\ldots,\tau_d\in T$ les arrels de $\varphi(X)$. La factorització de $f(X)$ en producte d'irreduibles a $T[X]$ és $f(X)=\prod_{i=1}^{d} f_i(X)$, on per cada $1\leqslant i\leqslant d$ és:

$$f_i(X) = \prod_{\theta'\in\Sigma_{\tau_i}} (X-\theta'),$$

essent Σ_{τ_i} el conjunt de les arrels de $f(X)$ que satisfan $v_p(\theta'-\tau_i)>0$. Com que les arrels de $\varphi(X)$ són totes distintes, tenim $R_p(f_i,f_j)=0$ per a tot $i\neq j$ i per tant:

$$i_p(f) = i_p(f) = \sum_{i=1}^{d} i_p(f_i).$$

Així doncs, quedem reduits a provar que $i_p(g)\geqslant\frac{1}{2}(mh-m-h+\epsilon)$, on $g(X)=\mathrm{Irr}(\theta,T)$. Sigui τ l'única arrel de $\varphi(X)$ tal que $v_p(\theta-\tau)>0$ i sigui $\beta=\theta-\tau$. Els canvis lineals no afecten l'índex, per tant:

$$i_p(g) = i_p(\theta) = i_p(\beta).$$

Com que per a totes les altres arrels de $\varphi(X)$ és $v_p(\theta-\tau_i)=0$,

$$v_p(\beta) = v_p(\theta-\tau) = v_p(\varphi(\theta)) = h/m.$$

En conseqüència, l'element:

$$\gamma_i = \beta^i/p^{[ih/m]}, \quad 0 \leqslant i < m,$$

és enter. Siguin A,B els anells d'enters respectius de T i L i

$$B_0 = \langle 1, \gamma_1, \ldots, \gamma_{m-1} \rangle_A.$$

Clarament $A[\beta] \subset B_0 \subset B$ i $(B_0 : A[\beta]) = \prod_{i=1}^{m-1} p^{[ih/m]}$. Per altra banda, $[ih/m]$ clarament coincideix amb el nombre de punts de coordenades enteres sota de la recta $Y=\frac{h}{m}X$ a l'ordenada i-èssima sense comptar el punt $(i,0)$, per tant:

$$(B_0 : A[\beta])_p = \sum_{i=1}^{m-1} \left[\frac{ih}{m}\right] = \frac{1}{2}(mh-m-h+e),$$

i queda provat que $i_p(\beta)$ és més gran o igual que aquest valor.

Finalment hem de provar que si $f(X)$ és regular aleshores $B_0=B$. Essent $f(X)$ irreduïble, que sigui regular equival a dir que el polinomi associat és un polinomi irreduïble de $\mathbb{F}_q[Y]$ de grau e. Pel Lema 2.2 aquest polinomi sempre té una arrel a $\bar{L}$, per tant en aquest cas $d \mid f(P/p)$. Siguin $\chi=h/e$ i $\lambda=m/e$; com que $(\chi,\lambda)=1$, $v_p(\varphi(\theta))=\chi e(P/p)/\lambda$ obliga a que $\lambda \mid e(P/p)$. Ara, de:

$$[L:\Phi_p] = dm = de\lambda = e(P/p)f(P/p),$$

concluim (com ja mostrà Ore) que en el cas regular $e(P/p)=\lambda$ i $f(P/p)=de$. En particular, qualsevol arrel $\overline{\varphi(\theta)^\lambda/p^\chi}$ del polinomi associat (Lema 2.2) és un generador de l'extensió residual $\bar{L}/\bar{T}$ i per tant $\bar{\gamma}_\lambda = \overline{\beta^\lambda/p^\chi}$ també doncs:

$$\varphi(\theta)^{\lambda}/p^{\chi} = \eta\beta^{\lambda}/p^{\chi}, \text{ essent } \quad \eta = \prod_{\tau_i \neq \tau} (\theta - \tau_i),$$

i clarament $\bar{\eta} \in \bar{T}$. Per tant, com que $\gamma_{\lambda}^{i} = \gamma_{i\lambda}$ per a tot $0 \leqslant i < \epsilon$, els enters $1, \gamma_{\lambda}, \gamma_{2\lambda}, \ldots, \gamma_{(\epsilon-1)\lambda}$ formen un sistema de representants d'una base de $\bar{L}$ sobre $\bar{T}$. Per altra banda, és fàcil comprovar que, al ser $(\lambda,\chi)=1$ es té:

$$\{ \frac{i\chi}{\lambda} - [\frac{i\chi}{\lambda}],\ 1 \leqslant i < \lambda \} = \{ \frac{1}{\lambda}, \ldots, \frac{\lambda-1}{\lambda} \},$$

encara que potser en diferent ordre, per tant els elements $\gamma_1, \ldots, \gamma_{\lambda-1}$ tenen v_p igual a $1,2,\ldots,\lambda-1$ encara que potser en diferent ordre. Finalment, com que:

$$\gamma_i = \gamma_b \cdot \gamma_{a\lambda}, \quad \text{per a tot } 0 \leqslant i \leqslant m,$$

si $i=a\lambda+b$, $0 \leqslant b < \lambda$, és ben conegut que sota aquestes condicions els $\{\gamma_i\}$ formen una base de B com A-mòdul.

Recíprocament, si $f(X)$ no és regular, $[\bar{T}(\bar{\gamma}_{\lambda}):\bar{T}] < \epsilon$ i per tant els $1, \gamma_{\lambda}, \ldots, \gamma_{(\epsilon-1)\lambda}$ no són linealment independents (mod.P). En particular els $\{\gamma_i\}$ no poden formar base.#

§3. Una aplicació del polígon de Newton clàssic.

En contra del que passa en el cas general, si $gr(\varphi(X))=1$ tots els resultats dels §0 i 1 són vàlids per polinomis de $\mathbb{Q}_p[X]$, és a dir, admetent polígons que tinguin costats amb pendents negatives. Això permet obtenir en aquest cas una fórmula més completa per calcular $R_p(f,g)$ de polinomis del mateix grau tals que el seu polígon té un sol costat. Fent un canvi lineal de la variable podem suposar sempre $\varphi(X)=X$.

Considerem dos polinomis de $\mathbb{Z}_p[X]$ de grau $n \geqslant 1$:

$$f(X) = X^n + a_1 X^{n-1} + \ldots + a_n, \quad g(X) = X^n + b_1 X^{n-1} + \ldots + b_n.$$

Suposem que $v_p(a_n) = v_p(b_n) = c \geqslant 0$ i que:

$$n\, v_p(a_i),\ n\, v_p(b_i) \geqslant ic, \quad \text{per a tot} \quad 1 \leqslant i \leqslant n,$$

de manera que el polígon de Newton de $f(X)$ i $g(X)$ té un sol costat de pendent $\mu = c/n$. Per obtenir la fórmula l'única cosa que fem és tenir en compte que $R(f,g) = R(f, g-f)$ i aplicar la Proposició 2.3 per calcular $R_p(f, g-f)$. Sigui:

$$h(X) = f(X) - g(X) = (a_r - b_r)X^{n-r} + \ldots + (a_n - b_n),$$

essent $a_r - b_r$ la primera no nul·la d'aquestes diferències. Denotem $e_i = v_p(a_i - b_i)$. El polígon de Newton de $h(X)$ acaba a l'abscissa $n-r$ i té tots els punts per damunt de la recta $Y = \mu(X+r)$ (vegis fig.4). Siguin:

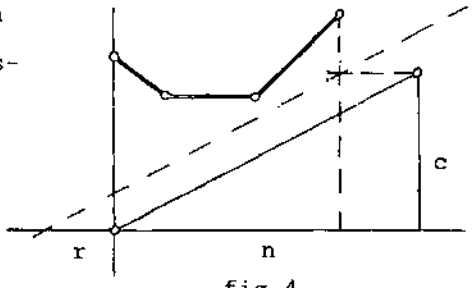


fig.4

$$r = r_0,\ r_1,\ \ldots,\ r_k = n,$$

els subíndexs tals que els vèrtexs d'aquest polígon són els punts $(r_i - r, e_i)$. Sigui r_s el subíndex que correspon al vèrtex que és l'origen del primer costat amb pendent estrictament més gran que μ; si tots els costats tenen pendent menor o igual que μ considerem $r_s = n$ (vegis fig.5).

Lema 2.5. Per a tot $1 \leqslant i \leqslant n$ es té:

$$ne_i - ic \geqslant ne_{r_s} - r_s c,$$

i hi ha algun altre punt que satisfà la igualtat si i només si el polígon de Newton de h(X) té algun costat de pendent μ.

Demostració. El punt (r_s-r,e_{r_s}) està caracteritzat per ser el d'abscissa més alta entre els primers punts que tocaria la recta $Y=\mu X$ si la desplaçem paral.lelament i vertical (vegis fig.5), la qual cosa és equivalent a dir que aquest punt està a distància mínima d'aquesta recta. Ara, la distància de cada punt $(i-r,e_i)$ a la recta $Y=\mu X$ ve donada per $(ne_i-c(i-r))/(1+c^2)^{1/2}$. Finalment, la recta $Y=\mu X$ desplaçada paral.lelament "toca" simultàniament tots els punts que estiguin a la distància mínima, per tant, l'existència de més d'un d'aquests punts equival a que hi hagi un costat del polígon de h(X) amb pendent μ.#

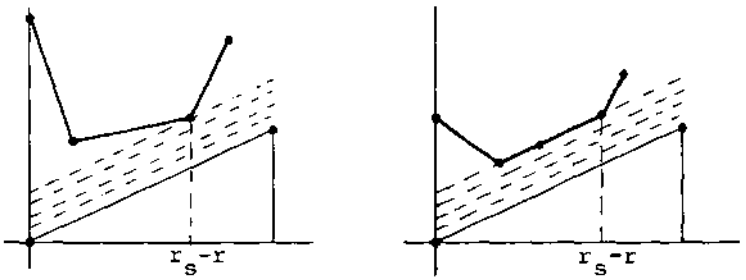


fig.5

Sigui $H(X) = \frac{1}{(a_r-b_r)}\, h(X)$. És un polinomi mònic de $\mathbb{Q}_p[X]$ i per tant li podem aplicar els resultats dels §0 i 1. En primer lloc observem que el polígon de Newton de H(X) s'obté desplaçant el de h(X) verticalment e_r unitats. Ara, sigui:

$$H(X) = h_1(X)\cdot\ldots\cdot h_k(X),$$

la factorització de H(X) a $\mathbb{Q}_p[X]$ donada pel Teorema del polígon. Per la Proposició 2.3 tindrem:

$$R_p(f,h_j) \geqslant n(r_j-r_{j-1})\cdot\inf\{\mu, \frac{e_{r_j}-e_{r_{j-1}}}{r_j-r_{j-1}}\}, \quad 1\leqslant j\leqslant k,$$

i si $\mu\neq(e_{r_j}-e_{r_{j-1}})/(r_j-r_{j-1})$ podem assegurar la igualtat. Per tant, la suma:

$$R_p(f,H) = \sum_{j=1}^{k} R_p(f,h_j),$$

descomposa en dos sumands:

$$\sum_{j=1}^{s} R_p(f,h_j) \geqslant n((e_{r_1}-e_{r_0})+(e_{r_2}-e_{r_1})+\ldots+(e_{r_s}-e_{r_{s-1}})) = n(e_{r_s}-e_{r_0}),$$

del qual només un eventual costat de pendent μ impediria assegurar la igualtat, i:

$$\sum_{j=s+1}^{k} R_p(f,h_j) = c((r_{s+1}-r_s)+(r_{s+2}-r_{s+1})+\ldots+(r_k-r_{k-1})) = c(n-r_s).$$

I com que $R(f,h)=(a_r-b_r)^n R(f,H)$ deduim que:

$$R_p(f,h) = R_p(f,H) + ne_1 \geqslant ne_{r_s} + c(n-r_s).$$

Tenint en compte el Lema 2.5 hem provat:

<u>Teorema 2.6</u>. Siguin $f(X)=X^n+\sum_{i=0}^{n} a_i X^{n-i}$, $g(X)=X^n+\sum_{i=0}^{n} b_i X^{n-i}\in\mathbb{Z}_p[X]$ tals que $v_p(a_n)=v_p(b_n)=c$ i:

$$n\,v_p(a_i),\ n\,v_p(b_i) \geqslant ic, \quad 1\leqslant i\leqslant n.$$

Aleshores:

$$R_p(f,g) \geqslant \min_{1\leqslant i\leqslant n}\{ n\,v_p(a_i-b_i) + c(n-i)\}, \qquad (8)$$

i si hi ha un únic $1\leqslant i\leqslant n$ per al qual es pren aquest mínim valor aleshores podem assegurar la igualtat.#

Remarca. 1) Si $c>0$ i aquest valor mínim es pren per diversos $1\leqslant i\leqslant n$, encara podrem assegurar que val la igualtat a (8) si el polinomi associat al costat de pendent μ que aquests punts determinen i el polinomi associat a $f(X)$ són primers entre si.
2) Si $(c,n)=1$ sempre (8) és una igualtat ja que és impossible que hi hagi dos $1\leqslant i\leqslant n$ que prenguin aquest valor. En efecte, denotant $e_i=v_p(a_i-b_i)$ tenim:

$$ne_i+c(n-i) = ne_j+c(n-j) \Leftrightarrow n(e_i-e_j)=c(i-j) \Rightarrow n|i-j \Rightarrow i=j.$$

Obtenim així una generalització de la fórmula de Krasner per polinomis Eisenstenians (i.e. el cas $c=1$) que hem enunciat a (4) del Capítol 1. Aquesta observació serà utilitzada sovint al Capítol 4.

Capítol 3. El cas no-ramificat

Sigui $p\in\mathbb{Z}$ un primer que suposarem fix al llarg de tot el capítol. Per a cada $m\geqslant 1$ denotem per T_m l'única extensió no-ramificada de $\mathbb{Q}_p$ de grau m, A_m l'anell d'enters de T_m i p_m l'ideal primer de A_m. L'objectiu principal d'aquest capítol és calcular $I_p(nT_m)$ per a qualsevols $n,m\geqslant 1$.

Sigui $m\geqslant 1$ un enter que suposarem fix d'ara endavant. Denotem $T=T_m$, $A=A_m$, $G=\mathrm{Gal}(T/\mathbb{Q}_p)$ i

$$\mathcal{R} = \{0\}\cup\{\text{arrels } p^m-1\text{-èssimes de la unitat de } T\}.$$

Recordem que $\mathcal{R}$ constitueix un sistema multiplicativament tancat de representants de $\bar{T}$ i que $\sigma(\mathcal{R})=\mathcal{R}$ per a tot $\sigma\in G$.

En el llenguatge del Capítol 1, si $\Gamma=nT\in\mathfrak{G}$, les Γ-configuracions consisteixen a repartir n quadradets dins d'una caixa amb $\sum_{d\mid m}\rho(d)$ subdivisions, però a diferència del cas totalment ramificat, si $m>1$ aquestes subdivisions no són totes iguals; segur que els polinomis de S_T que satisfan $f(X)\equiv X^m \pmod{p}$ tindran un comportament ben diferent al dels congruents (mod.p) a un determinat polinomi irreduïble de $\mathbb{F}_p[X]$ de grau m. Per tant, no té sentit, d'entrada, preguntar-se per la possible distribució que ha de tenir la Γ-configuració minimitzadora; si més no, aquest punt de vista no resulta de l'efectivitat demostrada al Capítol 1. ∎

Per calcular $I_p(nT)$ oblidarem, de moment, les Γ-configuracions i adoptarem un punt de vista radicalment diferent. Podem

dividir el procés que seguirem en tres fases:

1) Aconseguir una bona parametrització del conjunt S_T.

2) Calcular $i_p(f)$ i $R_p(f,g)$ dels elements de S_T en funció dels paràmetres que els caracteritzin.

3) Resolució del problema combinatori que representarà calcular $\min\{\sum_{i<j} R_p(f_i,f_j)+\sum_i i_p(f_i)\}$, prenent n polinomis de S_T.

Al terme "bona parametrització" li donem el sentit de parametrització que permeti resoldre 2) i 3). Al §1 resolem les tres qüestions restringits als polinomis amb $i_p(f)=0$. Entre els §2 i 3 es resolen 1) i 2). Finalment 3) és resolta al §4; malhauradament, la resposta no es dóna a través d'una fòrmula sino d'un algoritme.

Totes tres fases requereixen pasar a treballar a les extensions relatives T/T_d, $d|m$, d'aquí que ens convé introduir les següents notacions i definicions:

$G_d = \mathrm{Gal}(T/T_d)$.

$\mathcal{R}_d = \mathcal{R} \cap A_d$.

$A'_d = \{\theta \in A/\ T=T_d(\theta)\}$; $A' = A'_1$.

$S_{T/T_d} = \{f(X)=\mathrm{Irr}(\theta,T_d),\ \theta \in A'_d\}$.

$\rho_d(k)$ = nombre de polinomis irreduïbles de $\mathbb{F}_{p^d}[X]$ de grau k.

Com que estem en el cas no-ramificat, si $\theta \in A$ tenim:

$$i_p(\theta) = \frac{1}{2} d_p(\theta) = \frac{1}{2} \sum_{\sigma\neq\tau\in G} v_p(\sigma(\theta)-\tau(\theta)) = \frac{m}{2} \sum_{1\neq\sigma\in G} v_p(\theta-\sigma(\theta)).$$

D'altra banda, si $\theta,\omega\in$ A podem definir:

$$R_p(\theta,\omega) = \sum_{\sigma,\tau\in G} v_p(\sigma(\theta)-\tau(\omega)) = m\sum_{\sigma\in G} v_p(\theta-\sigma(\omega)).$$

Observis que si $f(X)=Irr(\theta,\mathbb{Q}_p)$, $g(X)=Irr(\omega,\mathbb{Q}_p)$, només tindrem $R_p(f,g)=R_p(\theta,\omega)$ si $\theta,\omega\in$ A'. Doncs bé, definim també per a tot divisor d de m i enters $\theta,\omega\in$A:

$$i_p^d(\theta) = v_p(i_{T/T_d}(\theta)) = \frac{m}{2d}\sum_{1\neq\sigma\in G_d} v_p(\theta-\sigma(\theta)),$$

$$R_p^d(\theta,\omega) = v_p(R_{T/T_d}(\theta,\omega)) = \frac{m}{d}\sum_{\sigma\in G_d} v_p(\theta-\sigma(\omega)).$$

Si $f(X),g(X)\in S_{T/T_d}$ definim $i_p^d(f)=i_p^d(\theta)$, $R_p^d(f,g)=R_p^d(\theta,\omega)$, essent θ i ω arrels respectives.

§1. Restricció als polinomis discriminantals

Sigui d un divisor de m que suposarem fix en tot aquest parägraf. Denotem $q=p^d$. Abans de resoldre 1),2) i 3) necessitem veure com es resolen les tres qüestions en la situació relativa T/T_d però restringint-nos al subconjunt de S_{T/T_d} dels polinomis que satisfan $i_p^d(f)=0$. Denotarem S^0_{T/T_d} aquest conjunt i anomenarem *discriminantals* aquests polinomis. Sabem perfectament quins polinomis de S_{T/T_d} són discriminantals:

Lema 3.1. Sigui $f(X)\in A_d[X]$ irreduïble. $i_p^d(f)=0$ si i només si f(X) és irreduïble (mod.p_d).

Demostració. Ambdues coses són equivalents a que p no divideixi el discriminant de f(X). #

Això permet considerar que aquests polinomis venen parametritzats directament pels seus coeficients; en efecte, si $t=\frac{m}{d}$, S^0_{T/T_d} queda dividit en $\rho_d(t)$ grups, un per cada polinomi irreduïble de $\mathbb{F}_q[X]$ de grau t. Si $\varphi(X)=X^t+\eta_1X^{t-1}+\ldots+\eta_t$ és un d'aquests polinomis, cada polinomi de S^0_{T/T_d} congruent amb ell (mod.p_d) el podem escriure de manera única com $f(X)=X^t+u_1X^{t-1}+\ldots+u_t$, amb:

$$u_i = a_i + u_{i,1}p + u_{i,2}p^2 + \ldots\ldots, \quad 1\leqslant i\leqslant t, \qquad (1)$$

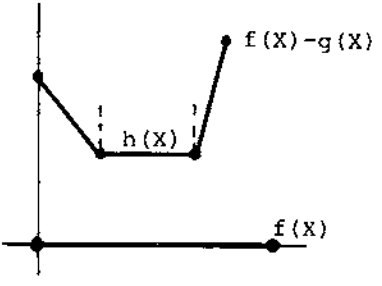
on a_i és l'únic element de $\mathcal{R}_d$ tal que $\bar{a}_i=\eta_i$ i els $u_{i,j}\in\mathcal{R}_d$ són totalment arbitraris. Té sentit considerar aquesta parametrització perquè donats $f(X),g(X)\in S^0_{T/T_d}$ sabem calcular $R^d_p(f,g)$ en funció dels coeficients:

Proposició 3.2. Siguin $f(X)=X^t+u_1X^{t-1}+\ldots+u_t$, $g(X)=X^t+v_1X^{t-1}+\ldots+v_t\in A_d[X]$, $t\geqslant 1$, irreduïbles (mod.p_d). Aleshores:

$$R^d_p(f,g) = t \min_{1\leqslant i\leqslant t}\{v_p(u_i-v_i)\}.$$

Demostració. És fàcil comprovar que el fet d'estar treballant amb T_d com a cos base no afecta la validesa de tots els resultats del Capítol 2. En particular, pel Teorema 2.6 tenim:

$$R^d_p(f,g) \geqslant t \min_{1\leqslant i\leqslant t}\{v_p(u_i-v_i)\}.$$



Però encara que aquest mínim es prengui per diversos coeficients, és a dir, encara que hi hagi en el polígon de Newton de f(X)-g(X) un costat amb pendent horitzontal, és segur que el factor h(X) de f(X)-g(X)

corresponent a aquest costat també fa $R_p^d(f,h)=0$, doncs f(X) i h(X) no poden tenir factors en comú (mod.p_d) perquè f(X) és irreduïble (mod.p_d) i h(X) té grau estrictament menor.#

Finalment, si definim:

$$I_p^{d,0}(n) = \min_{i<j} \{ R_p^d(f_i,f_j)\},$$

prenent n polinomis de S^0_{T/T_d}, tenim:

Proposició 3.3.(*) Sigui $t=\frac{m}{d}$. Per a tot $n\geqslant 1$ és:

$$I_p^{d,0}(n) = t \sum_{i\geqslant 0} \sum_{k=1}^{n-1} [\frac{k}{p^{im}\rho_d(t)}]. \qquad (2)$$

Demostració. Considerem n polinomis de S^0_{T/T_d} escollits equitativament entre els $\rho_d(t)$ grups en que estan classificats els elements d'aquest conjunt segons el polinomi irreduïble de $\mathbb{F}_{p^d}[X]$ de grau t amb el qual són congruents (mod.p_d). Dos polinomis de grups diferents fan $R_p^d(f,g)=0$ i els del mateix grup $R_p^d(f,g)\geqslant t$. Suposant que els coeficients dels polinomis estan expressats com a (1), dins de cada grup considerem que els polinomis estan equitativament escollits entre les p^m classes en que queda subdividit el grup segons la t-tupla $(u_{1,1},\ldots,u_{t,1})$. Per la Proposició 3.2 dos polinomis de classes diferents fan $R_p^d(f,g)=t$ i dos de la mateixa classe $R_p^d(f,g)\geqslant 2t$. Dins de cadascuna d'aquestes classes considerem que els polinomis estan equitativament escollits entre les p^m classes determinades per la t-tupla $(u_{1,2},\ldots,u_{t,2})$; per la Proposició 3.2 polinomis de classes diferents fan $R_p^d(f,g)=2t$ i els de la mateixa classe $R_p^d(f,g)\geqslant 3t$. Etc,etc.

El valor $\sum_{i<j} R_p^d(f_i,f_j)$ per n polinomis així escollits és

(*) Veure [Śliwa,1982,Theorem 2].

el donat per (2). En efecte, per la Proposició 3.2, podem pensar que $R_p^d(f_i,f_j)$ s'obté comptant t tantes vegades com $f_i(X)$ i $f_j(X)$ han anat coincidint en les successives classes en que hem anat subdividint S^0_{T/T_d}; per tant, podem pensar que $\sum_{i<j} R_p^d(f_i,f_j)$ s'obté comptant t per cada parella de polinomis que coincideixen en una classe determinada i això sumar-ho considerant totes les successives classificacions efectuades. Ara, l'haver escollit equitativament els polinomis de cada classe respecte de la classificació posterior fa que, per a tot i, els n polinomis estiguin equitativament repartits entre les $p^{im}\rho_d(t)$ classes que produeix la i-èssima classificació. Per tant, el nombre total de parelles de polinomis coincidents en una mateixa classe després de la i-èssima classificació és:

$$\frac{s_i(s_i-1)}{2}\, p^{im}\rho_d(t) + (n-s_i p^{im}\rho_d(t))s_i = s_i(n-p^{im}\rho_d(t)(\frac{s_i+1}{2})),$$

on hem denotat $s_i=[n/p^{im}\rho_d(t)]$. I és fàcil comprovar que aquesta expressió coincideix amb $\sum_{k=1}^{n-1}[k/p^{im}\rho_d(t)]$.

Faltaria veure que aquesta manera de seleccionar els polinomis minimitza el valor de $\sum_{i<j} R_p^d(f_i,f_j)$, però per qualsevol altra distribució de n polinomis de S^0_{T/T_d} entre les classes abans definides, sempre podem comptar aquest valor de la mateixa manera i es dedueix clarament de la Proposició 1.6 que per a cada classificació el nombre de parelles de polinomis en una mateixa classe és estrictament més gran en una distribució no equitativa.#

De cara a la resolució de la tercera fase en el cas general ens interessa destacar que en particular aquests raonaments proven que si definim:

$$I_p^{\varphi}(n) = \min_{i<j} \{ R_p^d(f_i, f_j) \},$$

prenent n polinomis de S^0_{T/T_d} tots congruents (mod.p_d) amb el mateix polinomi irreduïble $\varphi(X)$ de $\mathbb{F}_q[X]$ de grau t, tenim:

Corol.lari 3.4. $I_p^{\varphi}(n) = t \sum_{i\geq 0} \sum_{k=1}^{n-1} [\frac{k}{p^{im}}]$, i en conseqüència:

$$I_p^{\varphi}(n+1) - I_p^{\varphi}(n) = t \sum_{i\geq 0} [\frac{n}{p^{im}}] . \#$$

Remarca. Si m=1, és a dir, si $T=\mathbb{Q}_p$, els conjunts S^0_T i S_T coincideixen, per tant la Proposició 3.3 dóna el valor de $I_p(n\mathbb{Q}_p)$ trobat per Engstrom. Més generalment, si $T=T_d$, $S^0_{T/T}=S_{T/T}$ i la fórmula dóna el valor de $I_p(n(T/T))$ obtingut a [Llorente-Nart,1980].

D'ara endavant suposarem que $m>1$. Per calcular $I_p(nT)$ en el cas general "connectarem" cada element de S_T amb un polinomi discriminantal d'algun S_{T/T_d}. La parametrització de f(X) consistirà en aquest polinomi discriminantal associat, junt amb el propi procés que seguei f(X) per connectar-se amb ell.

§2. Càlcul de $i_p(\theta)$ i $R_p(\theta,\omega)$ en funció dels desenvolupaments p-àdics

Salvant la conjugació, el problema d'obtenir una bona parametrització de S_T és equivalent al de tenir una bona parametrització de A' i aquest últim és més fàcil de resoldre. Per començar ja sabem que tot element $\theta \in A$ s'escriu de manera única:

$$\theta = a_1 + a_2 p + a_3 p^2 + \ldots\ldots,$$

amb els $a_i \in \mathcal{R}$. Denotem $d_0=m_0=1$ i:

$$d_i = [\Phi_p(a_1,\ldots,a_i):\Phi_p(a_1,\ldots,a_{i-1})]\ ,\ m_i = \prod_{j>i} d_j,\ t_i=\frac{m}{m_i},$$

per a tot $i \geqslant 1$. $\Phi_p(a_1,\ldots,a_i)=T_{m_i} \subset T$; per tant els m_i divideixen tots m i com que $m_1 | m_2 | \ldots$, a la força aquesta successió esdevé constant. És a dir que existeix un s tal que:

$$\Phi_p(a_1,\ldots,a_{s+1}) = \Phi_p(a_1,\ldots,a_i,\ldots) = \Phi_p(\theta);$$

de manera que $\theta \in A'$ *si i només si per algun* s *és* $m=m_{s+1}$. Falta ara perquè aquesta descripció de A' sigui "bona" que donats θ, $\omega \in A'$ fóssim capaços de calcular $i_p(\theta)$ i $R_p(\theta,\omega)$ en funció dels seus desenvolupaments p-àdics.

Sigui, per a cada $i \geqslant 1$:

$$\theta_i = a_i + a_{i+1}p + a_{i+2}p^2 + \ldots;$$

de manera que $\theta=\theta_1$ i $\theta_i=a_i+p\theta_{i+1}$ per a tot i. Observis que encara que $\theta \in A'$ els θ_i's no tenen perquè ser primitius, tot el que podem assegurar és:

$$\theta \in A' \quad \Rightarrow \quad \theta_{i+1} \in A'_{m_i} \quad \text{per a tot } i \geqslant 1.$$

Reduïrem escalonadament el càlcul de $i_p(\theta)$ i $R_p(\theta,\omega)$ al dels $i_p^{m_k}(\theta)$ i $R_p^{m_k}(\theta,\omega)$.

<u>Lema 3.5</u>. Sigui $\theta = \sum_{i\geqslant 1} a_i p^{i-1}$, $a_i \in \mathcal{R}$. Per a tot $k \geqslant 1$ es té:

1) $i_p^{m_{k-1}}(\theta_k) = d_k i_p^{m_k}(\theta_k)$,

2) $i_p^{m_k}(\theta_k) = \frac{1}{2}t_k(t_k-1) + i_p^{m_k}(\theta_{k+1})$.

Sigui $\omega = \sum_{i\geqslant 1} b_i p^{i-1}$, $b_i \in \mathcal{R}$ i suposem que $a_k=b_k$. Aleshores:

3) $R_p^{m_{k-1}}(\theta_k,\omega_k) = d_k R_p^{m_k}(\theta_k,\omega_k)$,

4) $R_p^{m_k}(\theta_k,\omega_k) = t_k^2 + R_p^{m_k}(\theta_{k+1},\omega_{k+1})$.

Demostració. Recordem que $T_{m_{k-1}}(a_k)=T_{m_k}$ i que $d_k=[T_{m_k}:T_{m_{k-1}}]$. Si $d_k=1$ les afirmacions 1) i 3) són trivials. Si $d_k>1$, els $\sigma\in G_{m_{k-1}}$ que no pertanyen a G_{m_k} faran $\sigma(a_k)\neq a_k$, per tant $v_p(\theta_k-\sigma(\theta_k))=v_p(\theta_k-\sigma(\omega_k))=0$. En conseqüència:

$$i_p^{m_{k-1}}(\theta_k) = \frac{t_{k-1}}{2} \sum_{1\neq\sigma\in G_{m_{k-1}}} v_p(\theta_k-\sigma(\theta_k)) =$$

$$= \frac{t_{k-1}}{2} \sum_{1\neq\sigma\in G_{m_k}} v_p(\theta_k-\sigma(\theta_k)) = d_k i_p^{m_k}(\theta_k),$$

$$R_p^{m_{k-1}}(\theta_k,\omega_k) = t_{k-1} \sum_{\sigma\in G_{m_{k-1}}} v_p(\theta_k-\sigma(\omega_k)) =$$

$$= t_{k-1} \sum_{\sigma\in G_{m_k}} v_p(\theta_k-\sigma(\omega_k)) = d_k R_p^{m_k}(\theta_k,\omega_k).$$

Això prova 1) i 3). Per provar 2), com que $a_k\in T_{m_k}$ i els canvis lineals no afecten l'índex tenim:

$$i_p^{m_k}(\theta_k) = i_p^{m_k}(\theta_k-a_k) = i_p^{m_k}(p\theta_{k+1}) = \tfrac{1}{2}t_k(t_k-1) + i_p^{m_k}(\theta_{k+1}).$$

Finalment, 4) és obvia:

$$R_p^{m_k}(\theta_k,\omega_k) = R_p^{m_k}(p\theta_{k+1},p\omega_{k+1}) = t_k^2 + R_p^{m_k}(\theta_{k+1},\omega_{k+1}). \#$$

Definim l'*ordre de conjugació* entre dos enters $\theta,\omega\in A$ com:

$$k = \max_{\sigma\in G} \{ v_p(\theta-\sigma(\omega)) \}.$$

Clarament k està caracteritzat per ser el màxim natural tal que θ i algun conjugat de ω tenen els k primers coeficients del de-

senvolupament p-àdic iguals. Dos enters són conjugats si i només si tenen ordre de conjugació infinit.

Proposició 3.6.(*) Sigui $\theta = \sum_{i\geqslant 1} a_i p^{i-1}$, $a_i \in \mathcal{R}$. Aleshores,

$$i_p(\theta) = \frac{m}{2} \sum_{i\geqslant 1} (t_i - 1). \qquad (3)$$

Sigui $\omega = \sum_{i\geqslant 1} b_i p^{i-1}$, $b_i \in \mathcal{R}$. Sigui k l'ordre de conjugació entre θ i ω. Aleshores:

$$R_p(\theta,\omega) = m \sum_{i=1}^{k} t_i.$$

Demostració. Com ja hem vist abans, $\theta \in A'$ si i només si el membre de la dreta de (3) és finit; per tant, si $\theta \notin A'$ els dos membres de (3) valen ∞ i la fórmula és correcta. Suposem que $\theta \in A'$. L'aplicació recursiva del Lema 3.5 ens dóna:

$$i_p(\theta) = \frac{m}{2} \sum_{i=1}^{r} (t_i - 1) + m_r i_p^{m_r}(\theta_{r+1}),$$

per a qualsevol $r \geqslant 1$. Però a partir del moment en que $m_r = m$ ja es té que $t_r = 1$ i $i_p^{m_r}(\theta_{r+1}) = 0$.

Per provar la fórmula de la resultant podem suposar, substituïnt ω per un conjugat seu, que $a_i = b_i$ per a tot $i \leqslant k$. L'aplicació recursiva del Lema 3.5 dóna:

$$R_p(\theta,\omega) = m \sum_{i=1}^{k} t_i + m_k R_p^{m_k}(\theta_{k+1},\omega_{k+1}).$$

A la força a_{k+1} i b_{k+1} no són conjugats sobre T_{m_k} doncs si un $\sigma \in G_{m_k}$ fes $a_{k+1} = \sigma(b_{k+1})$, θ i ω tindrien ordre de conjugació més gran que k. En conseqüència, $v_p(\theta_{k+1} - \sigma(\omega_{k+1})) = 0$ per a tot $\sigma \in G_{m_k}$ i per tant $R_p^{m_k}(\theta_{k+1},\omega_{k+1}) = 0$. #

(*) Veure els Lemma 1 i Lemma 2 respectivament de [Śliwa,1982].

Per "baixar" aquests resultats mòdul conjugació i tenir-los a nivell de polinomis ens interessa considerar d'ara endavant que els enters de A' s'expressen de manera única com:

$$\theta = a_1 + a_2 p + a_3 p^2 + \ldots + a_s p^{s-1} + \xi p^s, \qquad (4)$$

amb $a_i \in \mathcal{R}$ tals que $m_s = [\varphi_p(a_1,\ldots,a_s):\varphi_p]$ és un divisor estricte de m i $\xi \in A'_{m_s}$ és discriminantal, és a dir, $i_p^{m_s}(\xi)=0$. Observis que s no és més que el primer subíndex que feia $m_{s+1}=m$ i que $\xi=\theta_{s+1}$. Com que $\bar{\theta}_{s+1}=\bar{a}_{s+1}$ genera l'extensió residual $\bar{T}/\bar{T}_{m_s}$, θ_{s+1} és discriminantal pel Lema 3.1. De la Proposició 3.6 deduïm:

Corol.lari 3.7. Sigui $\theta \in A$ expressat com a (4). Aleshores:

$$i_p(\theta) = \frac{m}{2} \sum_{i=1}^{s} (t_i - 1).$$

Sigui $\omega = \sum_{i=1}^{r} b_i p^{i-1} + \zeta p^r \in A$ en la seva expressió (4). Aleshores:

$$R_p(\theta,\omega) = m \sum_{i=1}^{k} t_i \quad \text{ó} \quad R_p(\theta,\omega) = m \sum_{i=1}^{s} t_i + m_s R_p^{m_s}(\zeta,\xi),$$

segons si l'ordre de conjugació k entre θ i ω és $<$ ó $\geqslant$ que $\inf\{r,s\}$.#

Destaquem finalment que absolutament tots els resultats d'aquest paràgraf són trivialment generalitzables al cas en que el cos base és T_d, $d|m$, i així seran utilitzats en el paràgraf següent. Més precisament, només cal substituir a totes les fórmules m per $\frac{m}{d}$. Els hem enunciat i provat sobre φ_p exclusivament per comoditat en l'exposició.

§3. Una bona parametrització de S_T

Com descriure els elements de S_T? Si assajem de buscar criteris en termes dels coeficients dels polinomis ara el fracàs és segur. El que farem és intentar caracteritzar un polinomi de S_T en termes del desenvolupament (4) de les seves arrels. Aquest desenvolupament i el Corol.lari 3.7 ens suggereixen les següents definicions: sigui d un divisor de m i denotem $d_0=m_0=d$. Definim Λ_d com el conjunt de les cadenes:

$$[\varphi_1(X),\varphi_2(X),\ldots,\varphi_s(X);F(X)], \qquad (5)$$

satisfent les següents propietats:

1) $\varphi_i(X)$, $1\leqslant i\leqslant s$, és un polinomi irreduïble de $\mathbb{F}_{p^{m_{i-1}}}[X]$, de grau d_i, essent $m_{i-1}=\prod_{j<i} d_j$.

2) $m_s=\prod_{i=0}^{s} d_i$ és un divisor estricte de m.

3) $F(X)\in A_{m_s}[X]$ és de grau $\frac{m}{m_s}$ i irreduïble (mod.p_{m_s}).

Definim per a cada $C\in\Lambda_d$ expressada com a (5):

$$i_p^d(C) = \frac{m}{2d}\sum_{i=1}^{s}(t_i-1),$$

on $t_i=m/m_i$ com fins ara. Si $C'\in\Lambda_d$ és una altra cadena,

$$C' = [\psi_1(X),\ldots,\psi_r(X);H(X)],$$

i k és el màxim natural tal que $\varphi_i(X)=\psi_i(X)$ per a tot $i\leqslant k$, definim:

$$R_p^d(C,C') = \frac{m}{d}\sum_{i=1}^{k} t_i \quad \text{ó} \quad R_p^d(C,C') = \frac{m}{d}\sum_{i=1}^{s} t_i + \frac{m_s}{d} R_p^{m_s}(F,H),$$

segons si k és $< \delta \geqslant \inf\{r,s\}$.

Sigui $\varphi(X) \in \mathbb{F}_{p^d}[X]$ irreduïble de grau d' divisor de $\frac{m}{d}$. Podem definir una aplicació:

$$\Lambda_{dd'} \xrightarrow{[\varphi, \ ]} \Lambda_d$$

que consisteix simplement en allargar les cadenes de $\Lambda_{dd'}$ posant $\varphi(X)$ com a primer polinomi. Les següents fòrmules són clares a partir de les definicions:

$$\begin{aligned} i_p^d([\varphi,C]) &= \frac{m}{2d}\left(\frac{m}{dd'}-1\right) + d' i_p^{dd'}(C), \\ R_p^d([\varphi,C],[\varphi,C']) &= \frac{m^2}{d^2 d'} + d' R_p^{dd'}(C,C'), \end{aligned} \tag{6}$$

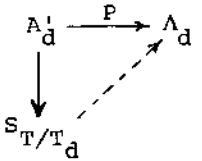
per a qualsevols $C,C' \in \Lambda_{dd'}$.

Tenim una aplicació natural $A_d' \xrightarrow{P} \Lambda_d$ consistent en assignar a cada $\theta \in A_d'$ expressat com a (4) la cadena constituïda pels $\mathrm{Irr}(\bar{a}_i, \mathbb{F}_{p^{m_{i-1}}})$ i $\mathrm{Irr}(\xi, T_{m_s})$. Seria desitjable que aquesta aplicació conservés índexs i resultants i que factoritzés a través de la conjugació. Concretament desitjem que:

a) $i_p^d(\theta) = i_p^d(P(\theta))$,

b) $R_p^d(\theta,\omega) = R_p^d(P(\theta),P(\omega))$,

c) θ i ω conjugats $\Rightarrow P(\theta) = P(\omega)$,



per a qualsevols $\theta,\omega \ A_d'$. Doncs bé, a) és obviament certa però b) i c) no ho són (veure Exemple 3.10). Cal adonar-se, però, que no volem una descripció "natural" de S_{T/T_d} sino que l'única cosa que ens interessa és construir una bijecció qualsevol entre S_{T/T_d} i Λ_d que conservi índexs i resultants ja que, clarament, el problema combinatori que comporta resoldre la tercera fase serà ales-

hores equivalent en tots dos conjunts. Per construir aquesta bijecció seleccionem per cada parella $(k,\varphi(X))$, $k\geqslant 1$, $\varphi(X)\in \mathbb{F}_{p^k}[X]$ irreduïble, una arrel de $\varphi(X)$ i la distingim de les demés. Aquesta elecció d'elements canònics dins dels $\mathbb{F}_{p^k}$ fa possible una elecció canònica de les arrels d'un polinomi de S_{T/T_d}:

Proposició 3.8. Per a tot $f(X)\in S_{T/T_d}$ hi ha una i només una de les seves arrels amb la propietat de que expressada com a (4) els $\bar{a}_1,\ldots,\bar{a}_s,\bar{\xi}$ són tots ells l'arrel canònica respectiva dels $\mathrm{Irr}(\bar{a}_i,\mathbb{F}_{p^{m_{i-1}}})$, $\mathrm{Irr}(\bar{\xi},\mathbb{F}_{p^{m_s}})$.

Demostració. Sigui $f(X)\equiv\varphi_1(X)^{t_1}\ (\mathrm{mod}.p_d)$, $\varphi_1(X)$ irreduïble de $\mathbb{F}_{p^d}[X]$ de grau d_1. Si $\eta_1,\ldots,\eta_{d_1}$ són les arrels de $\varphi_1(X)$ a $\mathbb{F}_{p^{dd_1}}$ sabem que la factorització de $f(X)$ en producte d'irreduïbles a $T_{dd_1}[X]$ és: $f(X)=g_1(X)\cdot\ldots\cdot g_{d_1}(X)$, cada $g_i(X)$ de grau t_1 i satisfent $g_i(X)\equiv(X-\eta_i)^{t_1}\ (\mathrm{mod}.p_d)$. Si η_j és l'arrel canònica de $\varphi_1(X)$ hi ha exactament t_1 arrels de $f(X)$ tals que en l'expressió (4) satisfan $\bar{a}_1=\eta_j$; són justament les arrels de $g_j(X)$ i per tant són totes elles conjugades sobre T_{dd_1}. Sigui θ una qualsevol d'aquestes arrels, considerem $\theta_1=(\theta-a_1)/p$ i $f_1(X)=\mathrm{Irr}(\theta_1,T_{dd_1})$ i tornem a començar. Al final tindrem que hi ha exactament t_s arrels de $f(X)$ $f(X)$ que en l'expressió (4) tenen $\bar{a}_1,\ldots,\bar{a}_s$ canònics; aquestes són exactament les arrels d'un dels factors irreduïbles, diguem-ne ne $F(X)$, de $f_{s-1}(X)$ a $T_{m_s}[X]$ i per tant conjugades sobre T_{m_s}. Aquest $F(X)$ ja és irreduïble $(\mathrm{mod}.p_{m_s})$ i per tant de les seves arrels només n'hi ha una que $(\mathrm{mod}.p_{m_s})$ sigui la canònica.#

En conseqüència tenim una aplicació $S_{T/T_d}\xrightarrow{\mathrm{can}}A'_d$ consistent en seleccionar de cada polinomi aquesta arrel canònica

de la qual acabem de provar l'existència. Doncs bé el sorprenent és que la composició:

$$S_{T/T_d} \xrightarrow{\text{can}} A_d' \xrightarrow{P} \Lambda_d$$

és bijectiva i conserva índexs i resultants. Clarament can és injectiva i conserva índexs i resultants, per tant només cal provar que P restringida a $A_d^{can} = \text{can}(S_{T/T_d})$ és bijectiva i conserva índexs i resultants. L'exhaustivitat és evident. Ara, si $P(\theta) = P(\omega)$, tenim que cada a_i és conjugat amb b_i sobre $T_{m_{i-1}}$ i ξ i ζ són conjugats sobre T_{m_s}. Aquesta propietat no és en general ni més dèbil ni més forta que el ser conjugats (vegis Exemple 3.10); això implica que $\bar{a}_i$ i $\bar{b}_i$ són arrels del mateix polinomi irreduïble de $\bar{\mathbb{F}}_{p^{m_{i-1}}}[X]$. però quan $\theta, \omega \in A_d^{can}$ a la força $\bar{a}_i = \bar{b}_i$ i en conseqüència $a_i = b_i$; junt amb el fet de que ξ i ζ siguin conjugats sobre T_{m_s} en aquest cas si que tenim que θ i ω són conjugats i per tant iguals. Finalment, entre enters de A_d^{can} també és cert que el fet de que tinguin ordre de conjugació k és equivalent a:

$$\text{Irr}(\bar{a}_i, \bar{\mathbb{F}}_{p^{m_{i-1}}}) = \text{Irr}(\bar{b}_i, \bar{\mathbb{F}}_{p^{m_{i-1}}}) \quad \text{per a tot } i \leqslant k, \text{ i}$$

$$\text{Irr}(\bar{a}_{k+1}, \bar{\mathbb{F}}_{p^{m_k}}) \neq \text{Irr}(\bar{b}_{k+1}, \bar{\mathbb{F}}_{p^{m_k}}).$$

Per tant $R_p^d(\theta, \omega) = R_p^d(P(\theta), P(\omega))$ per a qualsevols $\theta, \omega \in A_d^{can}$. Hem provat doncs:

Teorema 3.9. Existeix una aplicació bijectiva $S_{T/T_d} \xrightarrow{\tilde{P}} \Lambda_d$ tal que per a tot $f(X), g(X) \in S_{T/T_d}$:

$$i_p^d(f) = i_p^d(\tilde{P}(f)) \quad \text{i} \quad R_p^d(f,g) = R_p^d(\tilde{P}(f), \tilde{P}(g)). \#$$

Exemple 3.10. Donem a continuació un exemple amb p=2 que il.lustra tot el procés seguit. Siguin:

$$f(X) = X^4-7X^2+13, \quad g(X) = X^4-X^2+6X+43, \quad \varphi(X) = X^2+X+1.$$

Tenim $f(X)\equiv g(X)\equiv \varphi(X)^2$ (mod.2) i per les tècniques vistes al Capítol 2 es comprova que f(X) i g(X) són regulars, irreduïbles a $\mathbb{Q}_2[X]$ i generen T_4 l'única extensió no-ramificada de $\mathbb{Q}_2$ de grau quatre.

Siguin $\pm\theta, \pm\theta'$ les arrels de f(X); tenim $\theta^2+\theta'^2=7$ i $(\theta\theta')^2=13$. Observis que $3-\theta^2$ i $3-\theta'^2$ són arrels de $\varphi(X)$; posem:

$$a = 3-\theta^2, \quad b = 3-\theta'^2.$$

És clar que $\mathbb{R}\cap T_2=\{0,a,b\}$. És una simple comprovació que $g(\theta+\theta^2-\theta'^2)=0$, per tant les arrels de g(X) són:

$$\omega_1=\theta+\theta^2-\theta'^2, \quad \omega_2=-\theta+\theta^2-\theta'^2, \quad \omega_3=\theta'+\theta'^2-\theta^2, \quad \omega_4=-\theta'+\theta'^2-\theta^2.$$

Considerem els polinomis discriminantals de $T_2[X]$:

$$H(X) = X^2+aX-1, \quad F(X) = X^2+bX-1.$$

És fàcil comprovar que els enters de T_4:

$\frac{\theta-a}{2}=\frac{\omega_1-b}{2}$, $\frac{-\theta-a}{2}=\frac{\omega_2-b}{2}$ són les arrels de H(X), i

$\frac{\theta'-b}{2}=\frac{\omega_3-a}{2}$, $\frac{-\theta'-b}{2}=\frac{\omega_4-a}{2}$ són les arrels de F(X),

que podem denotar γ_1,γ_2 i β_1,β_2 respectivament. Per tant, l'expressió (4) de les arrels de f(X) i g(X) és:

$$\theta = a+2\gamma_1, \ -\theta = a+2\gamma_2, \ \theta' = b+2\beta_1, \ -\theta' = b+2\beta_2, \text{ i}$$

$$\omega_1 = b+2\gamma_1, \ \omega_2 = b+2\gamma_2, \ \omega_3 = a+2\beta_1, \ \omega_4 = a+2\beta_2,$$

i en conseqüència:

$$P(\theta) = P(-\theta) = P(\omega_1) = P(\omega_2) = [\varphi(X);H(X)], \text{ i}$$

$$P(\theta') = P(-\theta') = P(\omega_3) = P(\omega_4) = [\varphi(X);F(X)].$$

De manera que arrels del mateix polinomi tenen diferents cadenes associades i arrels de polinomis diferents la mateixa cadena. Quina podem assignar a f(X) i quina a g(X)? Per altra banda,

$$R_2(f,g) = R_2(\theta,\omega_1) = 8, \text{ i en canvi } R_2(P(\theta),P(\omega_1)) = \infty.$$

No obstant, si fem una elecció qualsevol d'arrels de $\varphi(X)$, $\bar{H}(X)$ i $\bar{F}(X)$, per exemple $\bar{\alpha},\bar{\gamma}_2,\bar{\beta}_1$ la situació queda solventada. L'arrel canònica de f(X) és $-\theta$ i la de g(X) és ω_3, per tant, a f(X) li associem la cadena $[\varphi(X);H(X)]$ i a g(X) la $[\varphi(X);F(X)]$. Tenim aleshores:

$$R_2(f,g) = R_2(-\theta,\omega_3) = R_2(P(-\theta),P(\omega_3)) = 8,$$

com cal. #

Per fí hem aconseguit una parametrització de S_T (i de S_{T/T_d}) més natural del que sembla. Cada $f(X) \in S_T$ l'hem caracteritzat pels $\varphi_i(X)$ irreduïbles de $\mathbb{F}_{p^{m_{i-1}}}[X]$ que es van obtenint al aplicar el procés descrit en la prova de la Proposició 3.8, fins arribar a un polinomi discriminantal. Què passa és que aquest procés no és únic i s'ha de fixar una manera canònica de fer-lo.

Remarca. Podem definir la *longitud* d'un polinomi $f(X) \in S_{T/T_d}$ com la longitud de la cadena de Λ_d unívocament associada a f(X) comptant com un sol esglaó cada grup de polinomis X contigus.

És clar que la longitud d'un f(X) pot ser arbitràriament gran (vegis l'exemple del final del §1 del Capítol 2). Un polinomi és discriminantal si i només si té longitud 0 i un polinomi és regular si i només si té longitud menor o igual que 1.

§4. Resolució del problema combinatori

Malhauradament només hem pogut trobar una solució algorítmica del problema combinatori que representa calcular:

$$J^d(n) = \min_{f}\{\sum_{i<j} R_p^d(C_i,C_j) + \sum_i i_p^d(C_i)\},$$

prenent n cadenes de Λ_d.

L'algoritme consisteix en elaborar una "llista" de cadenes de Λ_d:

$$C_1, C_2, \ldots, C_i, \ldots \qquad (7)$$

seguint el següent criteri: un cop escollides $C_1,\ldots,C_{i-1}$ seleccionem per al lloc i-èssim una qualsevol de les cadenes de Λ_d que tenen la propietat de que el valor:

$$c_d(i) = i_p^d(C_i) + \sum_{j<i} R_p^d(C_i,C_j),$$

sigui el mínim possible. El valor $c_d(i)$ l'anomenem la *contribució* de la cadena C_i (*). Aquesta llista la confeccionarem a partir de $\sum_{d'|\frac{m}{d}} \rho_d(d')$ subllistes, composta cadascuna per cadenes de Λ_d que comencen totes pel mateix polinomi irreduïble de $\mathbb{F}_p[X]$ de grau divisor de m/d i confeccionades seguint el mateix criteri

(*) Més que la llista en si el que ens interessa són aquestes contribucions, de manera que el que farà l'algoritme és elaborar la llista d'aquests valors.

de seleccionar en cada pas la cadena que aporta contribució mínima entre totes les d'aquest tipus. Cada cadena d'una determinada subllista fa $R_p^d(C,C')=0$ amb qualsevol cadena de les altres subllistes, per tant la llista (7) consisteix exactament en comparar les contribucions de les primeres cadenes de cada subllista encara no incorporades a la llista global i escollir la de contribució mínima. Observis que la contribució de la cadena a la llista global és la mateixa que tenia dins de la seva subllista.

Sigui $\varphi(X)\in \mathbb{F}_{p^d}[X]$ irreduïble de grau d' divisor de m/d. Les fórmules (6) mostren que si:

$$C_1',C_2',.....,C_i',..... \qquad (8)$$

és la llista global de les cadenes de $\Lambda_{dd'}$, aleshores:

$$[\varphi,C_1'],[\varphi,C_2'],.....,[\varphi,C_i'],..... \qquad (9)$$

és la subllista de les cadenes de Λ_d que comencen per $\varphi(X)$. També ens donen que si c és la contribució de la cadena i-èssima de la llista (8), aleshores,

$$d'c + \frac{m^2}{d^2d'}(i-1) + \frac{m}{2d}(\frac{m}{dd'}-1), \qquad (10)$$

és la contribució de la cadena i-èssima de la subllista (9). En particular comprovem que les contribucions de les cadenes d'una subllista només depenen del grau del primer polinomi; per tant, quan en un moment determinat convingui incorporar a la llista global la cadena k-èssima d'una determinada subllista a continuació haurem d'incorporar tots els elements k-èssims de les subllistes corresponents a polinomis irreduïbles de $\mathbb{F}_{p^d}[X]$ del mateix grau . En conseqüència ens preocuparem només de confeccionar una

sola sublista per a cada divisor de m/d.

Hem vist que la confecció de cada sublista requereix conèixer les llistes globals dels $\Lambda_{dd'}$, les quals també necessiten confeccionar les seves pròpies sublistes, elaborades altra vegada a partir de les llistes dels $\Lambda_{dd'd''}$,etc,etc. Observis que en particular cada llista global es necessita a si mateixa per confeccionar la sublista de les cadenes que comencen amb polinomis de grau 1 !

Naturalment, queda pendent la prova de que obrant així minimitzem, és a dir que per a qualsevol llista (7) obtinguda d'aquesta manera es tindrà:

$$J^d(n) = \sum_{1\leqslant i<j\leqslant n} R_p^d(C_i,C_j) + \sum_{i=1}^{n} i_p^d(C_i) = \sum_{i=1}^{n} c_d(i),$$

per a tot n. Aquesta propietat ja sabem que la gaudeixen les sublistes corresponents a polinomis irreduïbles (mod.p_d); en efecte, es dedueix de la prova de la Proposició 3.3 i del Corol.lari 3.4 que:

Proposició 3.11. Sigui:

$$[F_1(X)],[F_2(X)],.....,[F_i(X)],.....$$

una llista qualsevol de cadenes de Λ_d compostes d'un sol polinomi de $T_d[X]$ congruent (mod.p_d) al mateix polinomi irreduïble $\varphi(X)$ de grau t de $\overline{F}_{p^d}[X]$. Si la llista ha estat confeccionada minimitzant la contribució c_i de cada cadena amb les anteriors, es té:

$$I_p^{\varphi}(n) = \sum_{i=1}^{n} c_i,$$

per a tot n. En conseqüència, els c_i's estan obligats a valer:

$$c_{i+1} = t \sum_{k\geqslant 0} \left[\frac{i}{p^{km}}\right], \quad \text{per a tot } i \geqslant 0.\#$$

Passem ja a descriure l'algoritme en detall. Siguin:

$$m = d_{1,1} > d_{1,2} > \ldots\ldots > d_{1,r_1} = 1,$$

els divisors de m i per a cada $1 \leqslant i < r_1$ denotem:

$$d_{1,i} = d_{i,1} > d_{i,2} > \ldots\ldots > d_{i,r_i} = 1,$$

els divisors de $d_{1,i}$. Hem de confeccionar r_1-1 llistes; parlarem de la llista i-èssima per referir-nos a la formada per cadenes de $\Lambda_{m/d_{i,1}}$. Per cada llista hem d'elaborar r_i subllistes; parlarem de la subllista (i,j) per referir-nos a la formada per cadenes, el primer polinomi de les quals té grau $d_{i,j}$. Denotem:

$$q_{i,j} = \rho_{m/d_{i,1}}(d_{i,j}), \quad 1 \leqslant i < r_1, \ 1 \leqslant j \leqslant r_i.$$

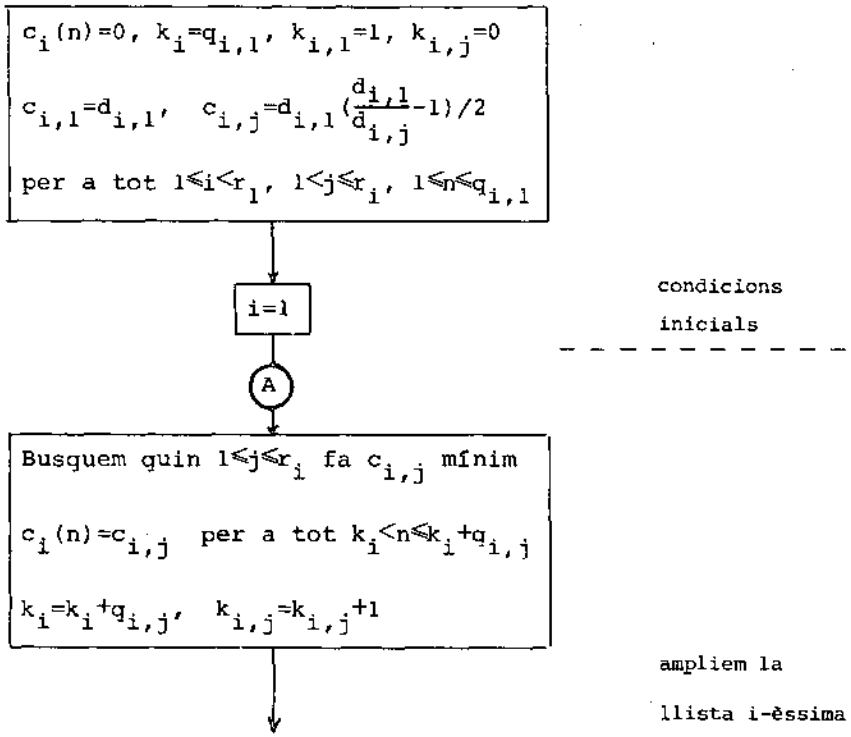
Denotarem en cada instant del procés per $c_{i,j}$ la contribució de la primera cadena de la subllista (i,j) encara no escollida per integrar-se a la llista i-èssima. Així doncs, cada nou element d'aquesta llista s'obtindrà buscant quin $c_{i,j}$, $1 \leqslant j \leqslant r_i$, és mínim. Un cop incorporat aquest element a la llista hem de canviar el valor de $c_{i,j}$ per la contribució que fa el següent element de la la mateixa subllista. L'única cosa que podria fer "encallar" aquest procés, i que per tant hem d'evitar, seria que per substituir el valor $c_{i,j}$ haguèssim de recòrrer al k-èssim terme d'una llista global que encara no hagués estat confeccionada fins a k termes. Perquè inicialment no hi hagi cap llista buïda suposem que ja tenen totes les $q_{i,1}$ cadenes a que dóna lloc el primer

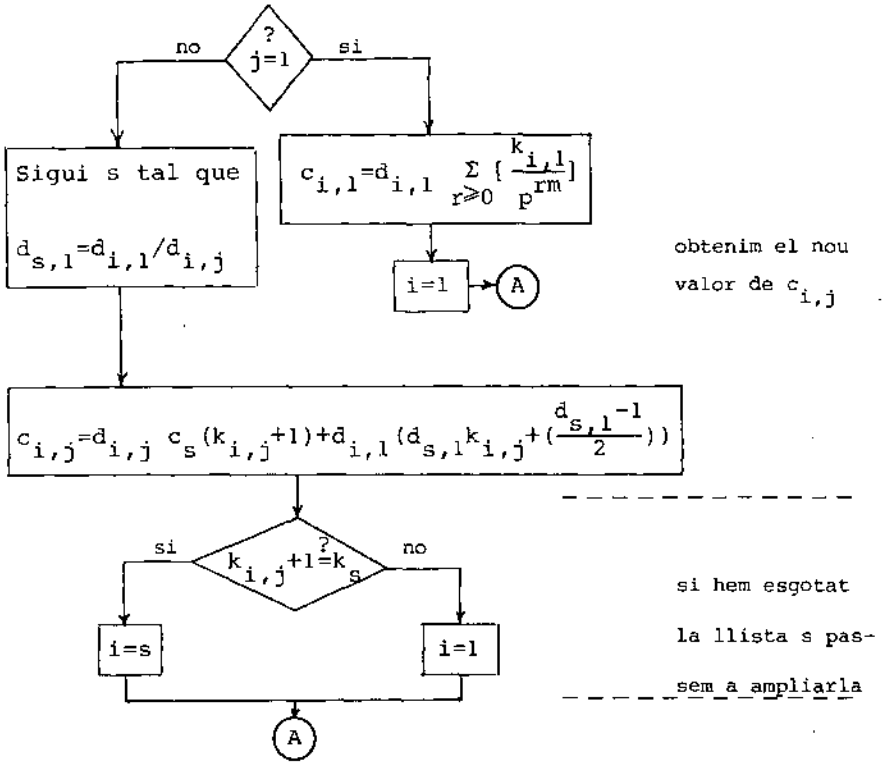
element de la subllista (i,1). Totes les subllistes (i,j) amb $j>1$ les suposem buïdes. En aquestes condicions tenim clarament:

$$c_{i,1} = d_{i,1}; \quad c_{i,j} = \frac{d_{i,j}}{2}\left(\frac{d_{i,1}}{d_{i,j}} - 1\right),$$

per a tot $1 \leqslant i < r_1$, i tot $j>1$. Les successives contribucions $c_{i,1}$ les treiem de la Proposició 3.11, mentre que les $c_{i,j}$, $j>1$ les obtenim recursivament utilitzant la fòrmula (10).

Teorema 3.12. Denotem k_i, $k_{i,j}$ les longituds respectives de la llista i-èssima i subllista (i,j), per a tot $1 \leqslant i < r_1$, $1 \leqslant j \leqslant r_i$. Denotem $c_i(n)=c_{m/d_{i,1}}(n)$ la contribució de l'element n-èssim de la llista i-èssima. Aleshores l'algoritme que descrivim a continuació permet anar obtenint els $c_i(n)$ sense interrupció.





Demostració. Les llistes de cadenes de Λ_d amb m/d primer són autosuficients; no necessiten recòrrer a d'altres llistes ja que només tenen dues subllistes, la (i,1) ben coneguda per la Proposició 3.11 i la (i,2) que es confecciona a partir de la pròpia llista global. És evident que per confeccionar aquestes llistes el procés no s'encalla; per tant, per recurrència no s'encalla tampoc a les altres.#

Provem finalment que aquest procés minimitza:

Proposició 3.13. Per a tot divisor d de m es té:

$$J^d(n) = \sum_{k=1}^{n} c_d(k) \quad \text{per a tot } n.$$

Demostració. Denotem $H^d(n)$ per indicar que l'afirmació de la Proposició és certa per a tot $r \leqslant n$. Ho provarem per doble inducció sobre n i sobre els divisors de m/d. Concretarem provarem:

$$H^d(n);\quad H^{dd'}(k), \forall k, \forall d' \mid \frac{m}{d},\ 1 < d' < \frac{m}{d} \quad \Rightarrow \quad H^d(n+1).$$

La primera de les hipòtesis implica que per a tot $r \leqslant n$ la suma de totes les contribucions dels r primers elements de la subllista de Λ_d corresponent a les cadenes que tenen el primer polinomi de grau 1 és la mínima possible. La segona hipòtesi implica que això és cert a les demés subllistes, per als primers k elements, i per a tot k.

Sigui $n+1=n_1+\ldots+n_r$ una distribució qualsevol de n+1 cadenes de Λ_d entre les respectives subllistes amb la propietat de que la suma de les contribucions és la mínima possible. Sigui $n+1=n'_1+\ldots+n'_r$ la distribució entre les subllistes de les n+1 primeres cadenes obtingudes minimitzant pas a pas. Clarament, el cas $n_1=\ldots=n_{r-1}=0$ no es pot donar doncs si treiéssim un dels n_r elements i n'afegíssim un de la primera subllista obtindriem una família de cadenes amb suma total de contribucions estrictament més petita. Per tant $n_r \leqslant n$. Com que la suma total de contribucions coincideix amb la suma de les r sumes de les contribucions dins de cada subllista, clarament podem suposar que les $n_1,\ldots,$ n_r cadenes són les primeres de cada subllista doncs en cas contrari, substituint-les per aquestes últimes minimitzariem o deixariem igual la suma de les contribucions. Finalment comprovem que aleshores no pot haver cap desigualtat $n_i < n'_i$, $n_j > n'_j$. En

efecte, si C' és la primera cadena de les n_i' que no hi és entre les n_i i C és la primera de les n_j que no hi és entre les n_j', la contribució de C' amb les n_i primeres cadenes és menor (o igual) que la de C amb les n_j' primeres, doncs en cas contrari en la minimització pas a pas haguèssim col.locat C abans de C'. Per tant si de la família $n_1,\ldots,n_r$ eliminem C i hi afegim C' obtenim una família amb suma total de contribucions més petita (absurd) o igual; en tot cas, o bé $n_i=n_i'$ per a tot i, o bé després d'una sèrie de canvis com aquest hi arribariem.

La prova acaba observant que si m/d és primer la segona hipòtesi és trivial i la primera se satisfà per $n\leqslant\rho_d(m/d)$. Si m/d és qualsevol, la segona hipòtesi és certa per hipòtesi d'inducció i la primera ho és per $n\leqslant\rho_d(m/d)$.#

L'algoritme del Teorema 3.12 encara que complicat en la seva elaboració és molt fàcilment programable i rapidíssim d'execució. Acabem aquest Capítol donant dues taules amb el valor de $I_p(nT_m)$ per p=2,3 i m=2,3,4,5 i 6. A les taules no repetim les contribucions sino que al costat de cada nova contribució c donem el nombre de vegades q que hi hauria de figurar repetida. De manera que $I_p(nT_m)$ ve donat per la suma dels productes c·q de totes les files fins arribar al lloc en que la suma de les q's és igual a n. En els cassos p=2,m=3 i p=3,m=2 les contribucions es repeteixen sempre el mateix nombre de vegades, 2 i 3 respectivament.

Taula 3.14. p=2.

m=2			m=3			m=4			m=5			m=6		
n	c	q	n	c	q	n	c	q	n	c	q	n	c	q
1	0	1	2	0	2	3	0	3	6	0	6	9	0	9
3	1	2	4	3		4	2	1	12	5	6	11	3	2
4	2	1	6	3		7	4	3	18	10	6	20	6	9
5	4	1	8	6		9	6	2	20	10	2	21	6	1
6	6	1	10	9		12	8	3	26	15	6	30	12	9
8	6	2	12	12		13	10	1	32	20	6	32	15	2
9	10	1	14	12		16	12	3	38	25	6	34	15	2
11	10	2	16	15		19	16	3	44	30	6	43	18	9
12	12	1	18	18		20	18	1	50	35	6	52	24	9
13	14	1	20	21		23	20	3	52	35	2	53	24	1
15	15	2	22	24		25	22	2	58	40	6	55	27	2
16	16	1	24	27		28	24	3	64	45	6	64	30	9
17	20	1	26	30		29	26	1	70	50	6	73	36	9
19	21	2	28	33		32	28	3	76	55	6	75	39	2
20	22	1	30	33		35	32	3	84	60	6	84	42	9
21	24	1	32	36		36	34	1	86	60	2	85	42	1
22	26	1	34	39		39	36	3	92	65	6	94	48	9
24	27	2	36	42		41	38	2	98	70	6	96	51	2
25	30	1	38	42		44	40	3	104	75	6	98	51	2
27	31	2	40	45		45	42	1	110	80	6	107	54	9
28	32	1	42	48		48	44	3	116	85	6	116	60	9
29	34	1	44	51		51	48	3	118	85	2	117	60	1
31	35	2	46	54		54	52	3	124	90	6	119	63	2
32	36	1	48	57		55	52	1	130	95	6	128	66	9
33	42	1	50	60		58	56	3	136	100	6	137	72	9
35	43	2	52	63		60	56	2	142	105	6	139	75	2
36	44	1	54	63		63	60	3	148	110	6	148	78	9
37	46	1	56	66		64	60	1	150	110	2	149	78	1
39	47	2	58	69		67	68	3	156	115	6	158	84	9
40	48	1	60	72		68	68	1	162	120	6	160	87	2
42	51	2	62	72		71	72	3	168	125	6	162	87	2
43	52	1	64	75		73	74	2	174	130	6	171	90	9
44	54	1	66	81		76	76	3	180	135	6	180	96	9
45	56	1	68	84		77	76	1	182	135	2	181	96	1
47	57	2	70	84		80	80	3	188	140	6	183	99	2
48	58	1	72	87		83	84	3	194	145	6	192	102	9
49	62	1	74	90		84	86	1	200	150	6	201	108	9
51	63	2	76	93		87	88	3	206	155	6	203	111	2
52	64	1	78	93		89	90	2	212	165	6	212	114	9
53	66	1	80	96		92	92	3	214	165	2	213	114	1
54	68	1	82	99		93	94	1	220	170	6	222	120	9
56	68	2	84	102		96	96	3	226	175	6	224	123	2
57	72	1	86	105		99	100	3	232	180	6	226	123	2
59	72	2	88	108		100	102	1	238	185	6	235	126	9
60	74	1	90	111		103	104	3	244	190	6	244	132	9
61	76	1	92	114		105	106	2	246	190	2	245	132	1
63	77	2	94	114		108	108	3	252	195	6	247	135	2
64	78	1	96	117		109	110	1	258	200	6	256	138	9
65	84	1	98	120		112	112	3	264	205	6	265	144	9
67	85	2	100	123		115	116	3	270	210	6	267	147	2

Taula 3.15. p=3

m=2			m=3			m=4			m=5			m=6		
n	c	q	n	c	q	n	c	q	n	c	q	n	c	q
3	0	3	8	0	8	18	0	18	48	0	48	116	0	116
6	1		16	3	8	21	2	3	96	5	48	124	3	8
9	2		19	3	3	39	4	18	144	10	48	240	6	116
12	4		27	6	8	42	6	3	147	10	3	243	6	3
15	5		35	9	8	60	8	18	195	15	48	359	12	116
18	6		43	12	8	63	10	3	243	20	48	367	15	8
21	8		46	12	3	81	12	18	291	25	48	370	15	3
24	9		54	15	8	99	16	18	339	30	48	486	18	116
27	10		62	18	8	102	18	3	387	35	48	602	24	116
30	12		70	21	8	120	20	18	390	35	3	605	24	3
33	14		73	21	3	123	22	3	438	40	48	613	27	8
36	14		81	24	8	141	24	18	486	45	48	729	30	116
39	16		89	27	8	144	26	3	534	50	48	845	36	116
42	18		97	30	8	162	28	18	582	55	48	853	39	8
45	20		100	30	3	180	32	18	630	60	48	969	42	116
48	22		108	33	8	183	34	3	633	60	3	972	42	3
51	22		116	36	8	201	36	18	681	65	48	1088	48	116
54	24		124	39	8	204	38	3	729	70	48	1096	51	8
57	26		127	39	3	222	40	18	777	75	48	1099	51	3
60	27		135	42	8	225	42	3	825	80	48	1215	54	116
63	28		143	45	8	243	44	18	873	85	48	1331	60	116
66	30		151	48	8	261	48	18	876	85	3	1334	60	3
69	31		154	48	3	264	50	3	924	90	48	1342	63	8
72	32		162	51	8	282	52	18	972	95	48	1458	66	116
75	34		170	54	8	285	54	3	1020	100	48	1574	72	116
78	35		178	57	8	303	56	18	1068	105	48	1582	75	8
81	36		181	57	3	306	58	3	1116	110	48	1698	78	116
84	40		189	60	8	324	60	18	1119	110	3	1701	78	3
87	41		197	63	8	342	64	18	1167	115	48	1817	84	116
90	42		205	66	8	345	66	3	1215	120	48	1825	87	8
93	44		208	66	3	363	68	18	1263	125	48	1828	87	3
96	45		216	69	8	366	70	3	1311	130	48	1944	90	116
99	46		224	72	8	384	72	18	1359	135	48	2060	96	116
102	48		232	75	8	387	74	3	1362	135	3	2063	96	3
105	49		240	78	8	405	76	18	1410	140	48	2071	99	8
108	50		243	78	3	423	80	18	1458	145	48	2187	102	116
111	52		251	84	8	426	82	3	1506	150	48	2303	108	116
114	54		259	87	8	444	84	18	1554	155	48	2311	111	8
117	54		262	87	3	447	86	3	1602	160	48	2427	114	116
120	56		270	90	8	465	88	18	1605	160	3	2430	114	3
123	58		278	93	8	468	90	3	1653	165	48	2546	120	116
126	60		286	96	8	486	92	18	1701	170	48	2554	123	8
129	62		289	96	3	504	96	18	1749	175	48	2557	123	3
132	62		297	99	8	507	98	3	1797	180	48	2673	126	116
135	64		305	102	8	525	100	18	1845	185	48	2789	132	116
138	66		313	105	8	528	102	3	1848	185	3	2792	132	3
141	67		316	105	3	546	104	18	1896	190	48	2800	135	8
144	68		324	108	8	549	106	3	1944	195	48	2916	138	116
147	70		332	111	8	567	108	18	1992	200	48	3032	144	116
150	71		340	114	8	585	112	18	2040	205	48	3040	147	8

Capítol 4. El cas totalment ramificat

Sigui $p \in \mathbb{Z}$ un primer que suposarem fix al llarg de tot el capítol. Volem calcular ara $I_p(nL)$ quan L és una extensió totalment ramificada de $\mathbb{Q}_p$ de grau e. Als §1 i §2 reduïm totalment el problema a l'estudi dels següents subconjunts de S_L:

$$S_L^r = \{ f(X) \in S_L \text{ les arrels del qual tenen } v_{P_L}(\theta)=r\}, \ 1 \leqslant r < e.$$

L'estudi detallat d'aquests conjunts només l'emprenem ja situats en el cas moderadament ramificat. Al §3 resolem completament el cas $(r,e)=1$ i això permet obtenir $I_p(nL)$ quan $e(L/\mathbb{Q}_p)$ és primer diferent de p. Al §5 estudiem el cas $(r,e)>1$, $(e,p-1)=1$ i obtenim una bona parametrització de S_L^r però deixem pendent la resolució del problema combinatori dins d'aquest conjunt.

§1. Classificació dels elements de S_L

En aquest paràgraf i el següent L denotarà una extensió totalment ramificada fixa de $\mathbb{Q}_p$ de grau e, A l'anell d'enters i P l'ideal primer de A.

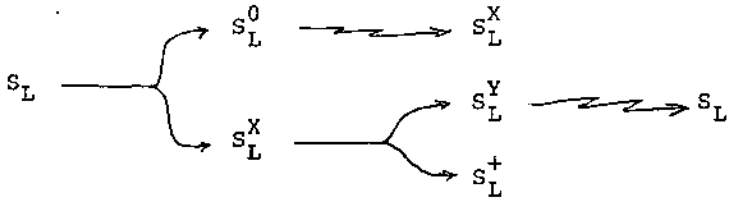
Els elements de S_L, pel fet de ser irreduïbles, tenen un polígon de Newton compost d'un sol costat amb pendent r/e, $r \geqslant 0$. Pel Teorema del polígon, les arrels d'un tal polinomi tenen totes $v_p(\theta)=r$. Classificarem els elements de S_L^r segons aquest valor. Definim per a tot $r \geqslant 0$:

$$S_L^r = \{ f(X) \in S_L \text{ les arrels del qual tenen } v_p(\theta) = r \}.$$

Sembla en principi una bona classificació de cara als nostres propòsits ja que per la Proposició 2.3:

$$f(X) \in S_L^r,\ g(X) \in S_L^{r'},\ r \neq r' \quad \Rightarrow \quad R_p(f,g) = e \cdot \inf\{r,r'\}.$$

Ara caldrà estudiar què passa dins de cada S_L^r. Encara podem filar més prim, si $r \geqslant e$ i $f(X) \in S_L^r$, per a cada arrel θ de $f(X)$, θ/p és un enter i $\mathrm{Irr}(\theta, \Phi_p) \in S_L^{r-e}$. Per tant el coneixement dels S_L^r amb $0 \leqslant r < e$ ja determina el coneixement de tots els altres. D'entre aquests, S_L^0 requereix un tractament especial; en efecte, si $f(X) \in S_L^0$, $f(X) \equiv (X-a)^e \pmod{p}$, $a \neq 0$, per tant un canvi lineal de la variable el transforma en un polinomi de $\bigcup_{r \geqslant 1} S_L^r$. Els $S_L^1, \ldots, S_L^{e-1}$ els considerem ja "irreduïbles", és a dir, no veiem manera de subdividir-los més i atacarem el seu estudi directament. Podem resumir la classificació que hem fet de S_L en el següent esquema:



on hem denotat:

$$S_L^X = \bigcup_{r \geqslant 1} S_L^r = \{ f(X) \in S_L / \ f(X) \equiv X^e \pmod{p} \},$$

$$S_L^Y = \bigcup_{r \geqslant e} S_L^r, \quad S_L^+ = \bigcup_{r=1}^{e-1} S_L^r.$$

La fletxa normal indica la descomposició d'un conjunt en la unió disjunta de dos subconjunts i la trencada indica que un conjunt

s'obté a partir de l'altre mitjançant transformacions que faran possible la resolució del seu problema combinatori a partir de la resolució del problema combinatori de l'altre. Es veu clarament que el conjunt S_L^+ precisa forçosament d'una descripció independent.

Abans de passar a concentrar-nos en l'estudi de S_L, dediquem el parägraf següent a analitzar en detall com s'han de fer totes aquestes connexions per tal de calcular $I_p(nL)$ suposant ja resolt el problema de calcular per a tot $1 \leqslant r < e$:

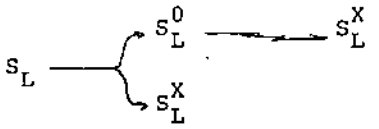
$$I^r(n) = \min\{\Sigma R_p(f_i,f_j) + \Sigma\, i_p(f_i)\},$$

prenent n elements de S_L^r.

§2. Resolució del problema combinatori

La resposta torna a ser, malhauradament, algorítmica. Adoptarem el mateix punt de vista que al Capítol 3. Confeccionarem dues llistes que anomenarem "llista de S_L" i "llista de S_L^X" formades respectivament per elements de S_L i S_L^X amb la propietat de que cada element està caracteritzat per minimitzar la contribució que fa amb tots els anteriors de la llista. En aquesta ocasió pensarem ja directament que elaborem les llistes d'aquestes contribucions més que la dels propis elements de S_L i S_L^X.

L'elaboració de la llista S_L a partir de la S_L^X és evident, cada element de la llista S_L^X l'anem col.locant a la llista S_L en el mateix ordre però repetit p vegades. Amb això resolem el troç d'esquema:



i tot queda pendent de la confecció de la llista S_L^X. Aquesta la elaborem a partir de e subllistes, una corresponent a cada S_L^r, $1 \leqslant r < e$ i l'última corresponent a S_L^Y. Aquesta darrera és molt fàcil d'obtenir, és qüestió simplement d'anar prenent els elements de la llista S_L i aplical's-hi la transformació $f(X) \longrightarrow$ $\longrightarrow p^e f(X/p)$. Si denotem $\tilde{f}(X)$ el polinomi així obtingut, tenim:

$$i_p(\tilde{f}) = i_p(f) + e(e-1)/2,$$

$$R_p(\tilde{f},\tilde{g}) = R_p(f,g) + e^2,$$

per a qualsevols $f(X), g(X) \in S_L$. Per tant l'i-èssim element d'aquesta subllista és:

$$c(i) + \frac{1}{2}\, e(e-1) + e^2(i-1),$$

si c(i) denota l'i-èssim element de la llista S_L.

Les e-1 primeres subllistes són les "dades" que permeten confeccionar totes les demés llistes i subllistes, dades que ara per ara ens són desconegudes. Denotem $x_{r,k}$ l'element k-èssim de la r-èssima subllista, per a tot $k \geqslant 1$, $1 \leqslant r < e$.

La llista S_L^X l'obtindrem escollint el "millor" element de cadascuna de les e subllistes, però fem observar que a diferència del que passava al Capítol 3, ara no tenim $R_p(f,g)=0$ sempre que f(X) i g(X) pertanyin a diferents subllistes $r \neq r'$ sino $R_p(f,g)=e \cdot \inf\{r,r'\}$. Per tant haurem de tenir en compte quants elements de cada subllista portem incorporats a la llista S_L^X per tal de saber la real contribució que aportaria cada nou ele-

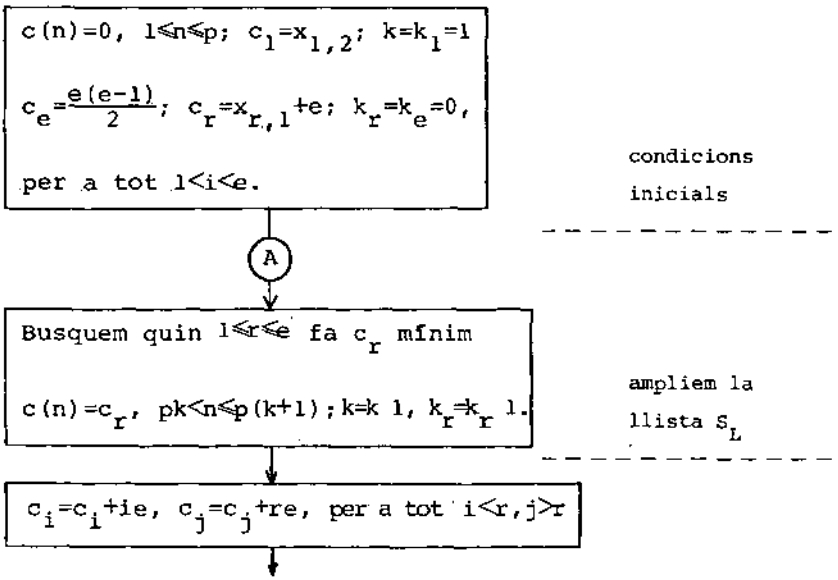
ment de cada subllista. Si en portem $k_1,\ldots,k_e$ ja incorporats, tocarà escollir per al següent lloc de la llista S_L^X el mínim d'entre els valors:

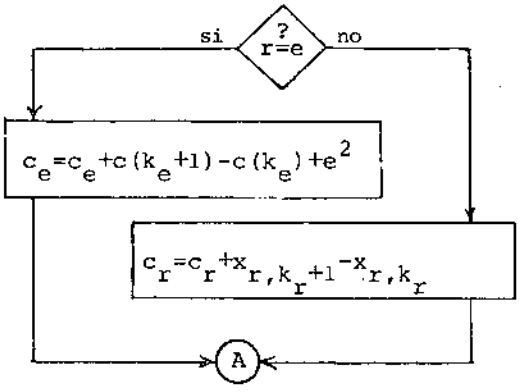
$$c_r = x_{r,k_r+1} + e\sum_{i=1}^{r-1} ik_i + er\sum_{i=r+1}^{e} k_i, \qquad 1\leqslant r<e,$$

$$c_e = c(k_e+1) + \frac{1}{2}e(e-1) + e^2k_e + e\sum_{i=1}^{e-1} ik_i.$$

Finalment, iniciarem la llista S_L amb el valor $x_{1,1}=0$ repetit p vegades. Correspon a escollir un polinomi Eisenstenià qualsevol i els derivats seus al fer el canvi de variable Y=X-a, a=1, ,...,p-1. Ja podem enunciar l'algoritme:

Teorema 4.1. Denotem k,k_r les longituds respectives de la llista S_L^X i la subllista r, $1\leqslant r<e$. Denotem $c(n),x_{r,n}$ l'n-èssim element de la llista S_L i subllista r, $1\leqslant r<e$, respectivament. L'algoritme que descrivim a continuació permet anar obtenint la llista S_L sense interrupció.





Demostració. L'única exigència perquè no s'encalli el procés és que $k_e+1 \leqslant pk$ en tot moment. És obvi que se satisfà.#

Falta provar que aquest procés permet obtenir $I_p(nL)$:

Proposició 4.2. Si per a tot $1 \leqslant r < e$ i $k \geqslant 1$ és $I^r(k) = \sum_{i=1}^{k} x_{r,i}$, aleshores $I_p(nL) = \sum_{i=1}^{n} c(i)$, per a tot n.

Demostració. La prova és anàloga a la de la Proposició 3.13 i no la detallem per no avorrir al lector. En comptes d'inducció múltiple podem pensar que funciona per recurrència. Si denotem $H(n)$ per indicar que la proposició és certa per a tot $k \leqslant n$ i $H^X(n)$ per indicar el mateix però restringits als elements de S_L^X, clarament $H(n)$ és certa per uns primers valors ($n \leqslant p$), per tant la subllista e-èssima té la mateixa propietat, per tant $H^X(m)$ és certa per a un m bastant més gran, per tant $H(pm)$ és certa, etc,etc.#

El Teorema 4.1 i la Proposició 4.2 mostren que ens hem reduït, tant en la faceta de la descripció dels conjunts com en la resolució del problema combimatori, a l'estudi dels S_L^r,

$1 \leqslant r < e$. Aquest estudi el limitarem al cas moderadament ramificat, cas en el qual ens situem d'ara endavant.

§3. Descripció de S_L^r, $(r,e)=1$, $p \nmid e$

Conservem les notacions dels parägrafs anteriors però suposarem d'ara endavant que $p \nmid e$. És ben conegut que en aquest cas L està biunívocament determinada, mòdul conjugació, per un element $\tilde{N}(L) \in \mathbb{F}_p^* / \mathbb{F}_p^{*e}$ de la següent manera: $L=\mathbb{Q}_p(\theta)$, essent θ l'arrel d'un binomi X^e+pa, amb $\bar{a} \in \tilde{N}(L)$ (veure [Hasse,1980,ch.16]). Si tenim un polinomi Eisensteniä qualsevol no binòmic també podem saber quina extensió genera només mirant-li el terme independent. I no només pels Eisenstenians, podem afirmar més generalment:

Proposició 4.3. Sigui $f(X)=X^e+\sum_{i=1}^{e} a_i X^{e-i} \in \mathbb{Z}_p[X]$, $p \nmid e$. Suposem que $v_p(a_e)=r$, $(r,e)=1$ i $v_p(a_i) \geqslant ir/e$ per a tot i. Aleshores $f(X)$ genera el mateix element de E que $g(X)=X^e+a_e$.

Demostració. En primer lloc tant $f(X)$ com $g(X)$ són irreductibles per tenir un polígon de Newton amb un sol costat de pendent r/e i ser $(r,e)=1$. Sigui β una arrel de $g(X)$ i ζ una arrel primitiva e-èssima de la unitat. Les altres arrels de $g(X)$ són $\beta_i=\zeta^i\beta$. Al ser $p \nmid e$, $\mathbb{Q}_p(\zeta)$ és no-ramificada i:

$$v_p(\zeta^i-\zeta^j)=0 \quad \text{si } i \not\equiv j \pmod{e}.$$

Per tant, si β_i, β_j són dues arrels diferents de $g(X)$ tenim:

$$v_p(\beta_i-\beta_j) = v_p(\beta) + v_p(\zeta^i-\zeta^j) = v_p(\beta) = r/e.$$

Per altra banda, per la Remarca posterior al Teorema 2.6:

$$R_p(f,g) = \min_{1\leqslant i<e} \{ e\, v_p(a_i) + r(e-i)\}.$$

Sigui k l'únic subíndex pel qual es pren aquest mínim. Si $\gamma=\gamma_1, \ldots,\gamma_e$ són les arrels de f(X) tenim:

$$R_p(f,g) = \sum_{i,j} v_p(\gamma_i-\beta_j) = e \sum_i v_p(\gamma-\beta_i),$$

i per tant existeix una arrel β de g(X) tal que:

$$v_p(\gamma-\beta) \geqslant \frac{v_p(a_k)}{e} + \frac{r(e-k)}{e^2}.$$

Però al ser (r,e)=1, a la força $v_p(a_k) > kr/e$, de manera que:

$$v_p(\gamma-\beta) > \frac{kr}{e^2} + \frac{r(e-k)}{e^2} = \frac{r}{e} = v_p(\beta-\beta_i),$$

per a qualsevol arrel β_i de g(X) diferent de β. Pel lema de Krasner, $f(X) \sim g(X)$.#

En conseqüència, si per a tot polinomi Eisenstenià definim $N(f(X)) = \overline{a_e/p}$, denotem $S_e^E \xrightarrow{\sim} E_e^{ram}$ el pas al quocient donat per conjugació i $\tilde{N}$ és la bijecció comentada al principi del paràgraf, ha quedat provat el:

Corol.lari 4.4. El següent diagrama és commutatiu:

$$\begin{array}{ccc} S_e^E & \xrightarrow{\ N\ } & \mathbb{F}_p^* \\ \sim\downarrow & & \downarrow \\ E_e^{ram} & \xrightarrow{\ \tilde{N}\ } & \mathbb{F}_p/\mathbb{F}_p^{*e} \end{array}.\#$$

El Teorema 1.8 del Capítol 1 utilitza aquest resultat i

l'esté al cas general no necessàriament moderadament ramificat. Com a conseqüència de la Proposició 4.3 un polinomi Eisenstenià genera l'únic element $M \in E$ tal que $\overline{a_e/p} \in \tilde{N}(M)$. De passada també mostra que per tenir un resultat similar en el cas $r>1$ només cal mirar-ho pels binomis:

Proposició 4.5. Suposem que $p \nmid e$ i $(r,e)=1$. Sigui $f(X)=X^e+p^r a$, $p \nmid a$ i sigui M l'element de E generat per $f(X)$. Aleshores $\bar{a} \in \tilde{N}(M)^r$.

Demostració. Si β és una arrel del binomi i n és un enter positiu tal que $nr \equiv 1 \pmod{e}$, clarament $\mathbb{Q}_p(\beta^n)=\mathbb{Q}_p(\beta)$ i el polinomi minimal de $\beta^n/p^{(rn-1)/e}$ serà Eisenstenià. Ara, el terme independent d'aquest polinomi és pa^n; per tant $\bar{a}^n \in N(M)$. Si denotem ϑ la classe de $\bar{a}$ dins $\mathbb{F}_p^*/\mathbb{F}_p^{*e}$, al ser $(r,e)=1$ existirà un $\vartheta' \in \mathbb{F}_p^*/\mathbb{F}_p^{*e}$ tal que $\vartheta'^r=\vartheta$. Per tant $\tilde{N}(M)=\vartheta^n=\vartheta'^{rn}=\vartheta'$.#

Remarca. Al ser $(r,e)=1$ elevar a r és una bijecció dins $\mathbb{F}_p^*/\mathbb{F}_p^{*e}$, per tant la Proposició 4.5 realment caracteritza l'element de E generat per un binomi a través del terme independent.

Aquesta observació junt amb les Proposicions 4.3 i 4.5 permeten obtenir una bona descripció de S_L^r:

Teorema 4.6. Sigui $f(X)=X^e+\sum_{i=1}^{e} a_i X^{e-i} \in \mathbb{Z}_p[X]$ i sigui $\vartheta=\tilde{N}(L)$. Si $(r,e)=1$ tenim:

$$f(X) \in S_L^r \quad \Leftrightarrow \quad v_p(a_e)=r,\ v_p(a_i) \geq ir/e \text{ i } \vartheta_0=\vartheta^r,$$

on ϑ_0 denota la classe de a_e/p^r dins $\mathbb{F}_p^*/\mathbb{F}_p^{*e}$.

Demostració. Si $f(X) \in S_L^r$ ja hem comentat que té per polígon de Newton un sol costat de pendent r/e. Per la Proposició 4.3, si $g(X)=X^e+a_e$ tenim també $g(X) \in S_L^r$ i per la Proposició 4.5 això implica que $\vartheta_0=\vartheta^r$. Recíprocament, per la Proposició 4.3 $f(X) \sim g(X)$ i per la Proposició 4.5 i la remarca posterior $g(X) \in S_L^r$.#

Hem fet servir tantes vegades i de manera tan decisiva que (r,e)=1 que no caldrà buscar exemples que mostrin que cap resultat d'aquest estil no es pot somniar en el cas (r,e) > 1. Fem observar que ni tan sols se sap quan un polinomi amb polígon de Newton d'un sol costat de pendent r/e és irreduïble.

Passem ja al càlcul de $I^r(n)$. En primer lloc observem que $i_p(f)$ és constant per a tots els elements de S_L^r ja que al ser (r,e)=1 el polinomi associat al costat del polígon de cada $f(X) \in S_L^r$ té sempre grau 1. Per tant els elements de S_L^r són tots regulars i pel Teorema de Ore:

$$i_p(f) = (r-1)(e-1)/2.$$

En conseqüència:

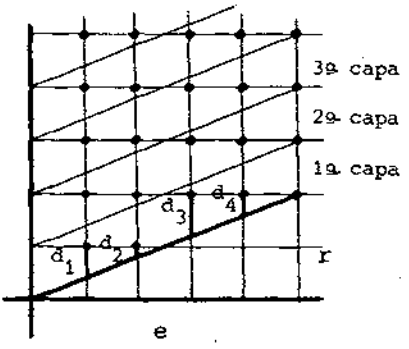
$$I^r(n) = \tfrac{1}{2}(r-1)(e-1)n + \min_{f_1(X),..,f_n(X) \in S_L^r} \{ \sum_{i<j} R_p(f_i,f_j) \}. \quad (1)$$

Pel Teorema 2.6, essent (r,e)=1 sabem que si $f(X),g(X) \in S_L^r$:

$$R_p(f,g) = e\, v_p(a_k-b_k)+r(e-k),$$

essent k l'abscissa del primer punt d'entre els $\{(i,v_p(a_i-b_i)),$ $1 \leqslant i \leqslant e\}$ que troba la recta $Y=\frac{r}{e}X$ enlairant-se. Pel Teorema 4.6, al variar f(X) i g(X), aquest conjunt de punts coincideix amb el dels punts de coordenades enteres amb abscissa $1 \leqslant i \leqslant e$ que hi ha

situats per damunt de la recta $Y=\frac{r}{e}X$, incluint el punt (e,r) (vegis dibuix). Per cada parella $f(X),g(X)\in S_L^r$ hi un d'aquests punts (x,y) tal que $R_p(f,g)=ey+r(e-x)$. Si (x',y') és un altre punt d'aquests, $ey+r(e-x)\leqslant ey'+r(e-x')$ és equivalent a que la recta $Y=\frac{r}{e}X$ trobi abans el primer punt al desplaçar-se. Per tant, de cara a minimitzar la suma dels $R_p(f_i,f_j)$ prenent elements de S_L^r ens interessen dues coses:



1) En quin ordre troba aquests punts la recta $Y=\frac{r}{e}X$ al desplaçar-se?

2) Quins valors va prenent $ey+r(e-x)$?

Si subdividim el conjunt d'aquests punts en capes delimitades per les rectes paral.leles a $Y=\frac{r}{e}X$ que tallen l'eix d'ordenades en punts de coordenades enteres, com s'indica en el dibuix, tots els punts d'una capa són trobats abans de qualsevol punt d'una capa superior. Dins d'una mateixa capa tenim e-1 punts sense comptar l'extrem, el qual és obviament el primer que sempre es troba. Si denotem $d_1,\ldots,d_{e-1}$ les distàncies de cada punt de la capa a la frontera inferior, és obvi que aquestes distàncies són les mateixes per a cada capa i valen:

$$d_i = 1-(\frac{ir}{e} - [\frac{ir}{e}]).$$

Com que (r,e)=1 és fàcil comprovar que:

$$\{\frac{ir}{e} - [\frac{ir}{e}],\ 1\leqslant i\leqslant e\} = \{\frac{1}{e},\frac{2}{e},\ldots,\frac{e-1}{e}\},$$

encara que potser en diferent ordre. Ara bé, a la m+1-èssima ca-

pa els valors ey+r(e-x) pels punts d'aquesta capa són e(r+m) per l'extrem i:

$$e(\frac{ir}{e} + m + d_i) + r(e-i) = e(r + m + d_i), \quad 1 \leqslant i < e,$$

pels demés. Per tant aquests valors són, en el mateix ordre en que la recta va trobant els respectius punts:

$$e(r+m),\ e(r+m)+1,\ldots,e(r+m)+e-1.$$

Això ja permet adonar-se de com hem de prendre els $f_i(X) \in S_L^r$ per minimitzar la suma de les resultants i quins valors prendrà aquest mínim:

Proposició 4.7. Si denotem $q_i = \frac{p^i(p-1)}{(e,p-1)}$ per a tot $i \geqslant 0$, tenim:

$$I^r(n) = \frac{1}{2}(r-1)(e-1)n + \frac{1}{2}ren(n-1) + \sum_{i\geqslant 0} \sum_{j=1}^{n-1} [\frac{j}{q_i}].$$

Demostració. Podem considerar pel Teorema 4.6 que els polinomis de S_L^r són de la forma:

$$f(X) = X^e + p^{k_1}a_1X^{e-1} + \ldots. + p^{k_{e-1}}a_{e-1}X + p^r a_e,$$

essent $k_i = 1+[\frac{ir}{e}]$, els $a_1,\ldots,a_{e-1} \in \mathbb{Z}_p$ totalment arbitraris i $a_e \in \mathbb{Z}_p$ no divisible per p i tal que $\bar{a}_e$ pertany a una classe determinada de $\mathbb{F}_p^*/\mathbb{F}_p^{*e}$. Considerem el desenvolupament p-àdic de $a_1,\ldots,a_e$:

$$a_i = a_{i,1} + a_{i,2}p + a_{i,3}p^2 + \ldots\ldots, \quad 1 \leqslant i \leqslant e.$$

Sigui $s_1,\ldots,s_{e-1}$ la permutació de 1,2,...,e-1 que fa que:

$$1 - (\frac{s_i r}{e} - [\frac{s_i r}{e}]) = \frac{i}{e}.$$

Classifiquem els polinomis de S_L^r segons $a_{e,1}$; polinomis de classes diferents fan $R_p(f,g)=re$ i els de la mateixa classe $R_p(f,g)>$ $>er$. Dins de cada classe classifiquem segons $a_{s_1,1}$; polinomis de diferent classe fan $R_p(f,g)=re+1$ i els de la mateixa classe $R_p(f,g)>re+1$, etc, etc. Dins de cada grup amb $a_{e,1}, a_{s_1,1}, \ldots,$ $, a_{s_{e-1},1}$ fixos classifiquem segons $a_{e,2}$; polinomis de classes diferents fan $R_p(f,g)=e(r+1)$ i els de la mateixa classe $R_p(f,g)>$ $>e(r+1)$, etc,etc,etc. El fet de que en cada nova classificació $R_p(f,g)$ augmenti sempre en una unitat exactament fa que si considerem n polinomis distribuits equitativament entre les classes per a totes les classificacions, igual com fèiem a la prova de la Proposició 3.3 poguem comptar:

$$\sum_{1\leqslant i<j\leqslant n} R_p(f_i,f_j) = \frac{n(n-1)}{2}re + m,$$

on m compta el nombre de parelles de polinomis en una mateixa classe, sumat considerant les successives classificacions efectuades. Com que els $a_{e,1}$ varien entre $(p-1)/(e,p-1)=\text{card}(\mathbb{F}_p^{*e})$ possibilitats i els $a_{i,j}$ per a $i\neq e$ ó $j\neq 1$ entre p possibilitats, aquest nombre és:

$$m = \sum_{i\geqslant 0} [\frac{n}{q_i}](n - \frac{q_i}{2}([\frac{n}{q_i}]+1)) = \sum_{i\geqslant 0} \sum_{j=1}^{n-1} [\frac{j}{q_i}].$$

De la mateixa manera com fèiem a la prova de la Proposició 3.3 es mostra que aquesta manera de considerar els polinomis minimitza aquest valor. (1) acaba la prova de la proposició.#

Corol.lari 4.8. Si fem una llista d'elements de S_L^r, $(r,e)=1$, minimitzant la contribució de cada element amb els anteriors, la contribució de l'element k-èssim és:

$$x_{r,k} = \tfrac{1}{2}(r-1)(e-1) + (k-1)er + \sum_{i\geqslant 0} \left[\frac{k-1}{q_i}\right]. \qquad (2)$$

A més a més, per a tot n, $I^r(n) = \sum_{k=1}^{n} x_{r,k}$. #

En conseqüència, el càlcul de $I_p(nL)$ queda totalment resolt si e és primer:

Corol.lari 4.9. Amb els valors de $x_{r,k}$, $1 \leqslant r < e$, $k \geqslant 1$, donats a (2) el Teorema 4.1 permet calcular $I_p(nL)$ si L és una extensió totalment ramificada de $\mathbb{Q}_p$ de grau primer diferent de p.#

Donem a continuació una taula amb el valor de $I_p(nL)$ per $p=2,3,5,7$ i $e(L/\mathbb{Q}_p)=2,3,5,7$, $e(L/\mathbb{Q}_p)\neq p$. La taula dóna en realitat la llista S_L^X, de manera que per calcular $I_p(nL)$ s'ha de sumar cada valor de la llista repetit p vegades fins arribar a sumar n valors.

Taula 4.10.

p=2			p=3			p=5			p=7		
e=3	e=5	e=7	e=2	e=5	e=7	e=2	e=3	e=7	e=2	e=3	e=5
0	0	0	0	0	0	0	0	0	0	0	0
4	6	8	3	5	7	2	3	7	2	3	5
7	12	17	5	11	15	5	6	14	4	7	10
12	18	24	8	16	22	7	9	21	7	10	15
16	24	32	11	22	30	9	13	29	9	13	20
20	32	42	14	27	37	12	16	36	11	17	25
25	38	50	17	32	45	14	19	43	13	20	31
29	43	59	19	39	53	17	22	50	16	24	36
33	50	67	22	44	60	19	25	58	18	27	41
37	56	74	26	50	68	21	29	65	20	31	46
41	64	85	29	55	75	24	32	72	23	34	51
46	70	93	32	61	83	26	35	79	25	37	56
51	76	102	34	66	90	29	38	87	27	41	62
55	83	110	38	72	99	32	42	94	29	44	67
59	89	118	41	78	106	34	45	101	32	48	72
63	95	127	44	83	114	37	48	108	34	51	77
67	102	135	46	89	121	39	51	115	36	56	82
72	108	144	49	94	129	41	55	123	39	59	87
76	115	152	53	100	136	44	58	130	41	62	92
80	121	160	56	105	143	46	61	137	43	66	98
85	126	171	58	113	153	49	64	144	45	69	103
89	136	179	61	118	160	51	67	153	48	73	108
92	142	188	64	123	168	53	72	160	50	76	113
99	149	196	67	129	175	56	75	167	52	80	118
103	154	203	70	134	183	58	78	174	55	83	123
107	160	213	72	140	190	62	81	182	58	86	129
112	168	221	75	145	199	64	85	189	60	90	134
116	174	230	80	152	206	67	88	196	62	93	139
119	180	238	83	157	214	69	91	203	65	97	144
125	186	248	85	163	221	71	94	211	67	100	149
129	192	256	88	168	228	74	97	218	69	104	154
132	200	264	91	173	236	76	101	225	71	107	160
137	206	273	94	179	243	79	104	232	74	111	165
141	212	281	97	184	252	81	107	240	76	115	170
145	219	291	99	191	259	83	110	247	78	118	175
151	225	298	102	196	267	86	114	254	81	122	180
155	232	306	106	202	274	88	117	261	83	125	185
160	238	315	109	207	282	91	120	269	85	129	191
163	244	323	112	213	289	94	123	276	87	132	196
167	251	335	114	218	298	96	127	283	90	135	201
172	257	343	118	224	306	99	130	290	92	139	206
176	263	351	122	231	313	101	133	297	94	142	211
180	273	360	124	236	321	103	136	306	97	146	216
185	279	368	127	242	328	106	139	313	99	149	222
188	286	378	130	247	336	108	144	320	101	153	228
192	291	385	134	253	343	111	147	327	103	156	233
199	297	393	137	258	352	113	150	335	106	159	238
204	305	402	139	264	359	115	153	342	108	163	243
208	311	410	142	270	367	118	157	349	110	166	248
212	317	420	145	275	374	120	160	356	114	171	253

§4. Un resultat de teoria de cossos

L'objectiu d'aquest paràgraf és provar el següent:

Teorema 4.11. Sigui K un cos commutatiu de característica zero. Sigui $L=K(\theta)$ una extensió finita de K de grau n i sigui $f(X)=X^n+a_1X^{n-1}+\ldots+a_n=\mathrm{Irr}(\theta,K)$. Si K conté les arrels m-èssimes de la unitat, $[K(\theta^m):K]=n/d$, on d és el màxim divisor de (n,m) tal que tots els coeficients de f(X) amb subíndex no múltiple de d són nuls. #

Sigui ζ una arrel primitiva m-èssima de la unitat. Considerem els polinomis:

$$f_i(Y) = \zeta^{in} f(Y/\zeta^i), \quad 0 \leqslant i < m.$$

Les arrels de $f_i(Y)$ són $\zeta^i\theta_1,\ldots,\zeta^i\theta_n$, essent $\theta=\theta_1,\ldots,\theta_n$ les arrels de f(X).

Lema 4.12. Sigui $\tilde{f}(X)=\mathrm{Irr}(\theta^m,K)$. Les següents condicions són equivalents:

1) $L=K(\theta^m)$
2) Els $\{\zeta^i\theta_j\}$, $0 \leqslant i < m$, $1 \leqslant j \leqslant n$ són tots diferents.
3) $f_0(Y)\cdot\ldots\cdot f_{m-1}(Y) = \tilde{f}(Y^m)$.

Demostració. ω és arrel de $\tilde{f}(Y^m)$ $\Leftrightarrow$ ω^m és arrel de $\tilde{f}(X)$ $\Leftrightarrow$ $\omega^m=\theta_j^m$ per algun $1 \leqslant j \leqslant n$ $\Leftrightarrow$ $\omega=\zeta^i\theta_j$ per alguns $0 \leqslant i < m$, $1 \leqslant j \leqslant n$. En conseqüència, $L = K(\theta^m)$ $\Leftrightarrow$ $\mathrm{gr}(\tilde{f}(X))=n$ $\Leftrightarrow$ $\mathrm{gr}(\tilde{f}(Y^m))=mn$ $\Leftrightarrow$

$\Leftrightarrow$ els $\{\zeta^i\theta_j\}$ són tots diferents $\Leftrightarrow$ $\tilde{f}(Y^m)=\prod_{i,j}(X-\zeta^i\theta_j)=\prod_{i=0}^{m-1}f_i(Y)$.#

Lema 4.13. Les següents condicions són equivalents:

1) Els $f_i(Y)$ són tots diferents.

2) Per a tot divisor $d>1$ de m existeix un coeficient a_k de $f(X)$ tal que $d\nmid k$ i $a_k\neq 0$.

3) Per a tot primer $p|m$ existeix un coeficient a_k de $f(X)$ tal que $p\nmid k$ i $a_k\neq 0$.

Demostració. $\zeta^{ki}=\zeta^{kj}$ és equivalent a $k(i-j)\equiv 0 \pmod m$, per tant: $f_i(Y)=f_j(Y)$ $\Leftrightarrow$ $a_k\zeta^{ki}=a_k\zeta^{kj}$ per a tot k $\Leftrightarrow$ $a_k=0$ sempre que $k(i-j)\not\equiv 0 \pmod m$ $\Leftrightarrow$ $a_k=0$ sempre que $k\not\equiv 0 \pmod{\frac{m}{(m,i-j)}}$.

Per tant 1) és equivalent a que aquesta última condició sigui falsa sempre que $i\neq j$. Ara bé, quan $i\neq j$ prenen els valors $0,1,\ldots,m-1$, $i-j$ val $1,2,\ldots,m-1$ i $\frac{m}{(m,i-j)}$ pren els valors de tots els divisors no trivials de m. Això prova que 1) és equivalent a 2). És obvi que 2) i 3) són equivalents. #

És clar que les condicions del Lema 4.12 impliquen les del Lema 4.13. El recíproc no és cert en general. En canvi:

Proposició 4.14. Si $\zeta\in K$ les condicions dels Lemes 4.12 i 4.13 són totes equivalents.

Demostració. Sota aquesta hipòtesi els $f_i(Y)$ són tots irreductibles a $K[Y]$ i divideixen $\tilde{f}(Y^m)$. Si són diferents el seu producte també el divideix i per tant coincideixen. #

Aquesta proposició caracteritza quan θ^m és primitiu, és

a dir, prova el cas d=1 del Teorema 4.11. El cas general s'en dedueix fàcilment:

Demostració del Teorema 4.11. $h(X)=f(X^{1/d})$ és un polinomi irreduïble de $K[X]$ de grau n/d i té $\omega=\theta^d$ com arrel. Per la Proposició 4.14 i 2) del Lema 4.13, $\omega^{m/d}$ genera la mateixa extensió que ω. #

§5. Descripció de S_L^r, $(r,e)>1$, $p\nmid e$, $(e,p-1)=1$

L'estudi de S_L^r quan $(r,e)>1$ només el fem en el cas $(e,p-1)=1$. En aquest cas L és, mòdul conjugació, l'única extensió totalment ramificada de $\mathbb{Q}_p$ de grau e.

Sigui $r=r_0m$, essent r_0 el màxim factor de r tal que $(r_0,e)=1$. Tots els factors primers de m divideixen e, per tant, en particular tenim $(m,p-1)=1$. Relacionarem els elements de S_L^r amb els de $S_L^{r_0}$ els quals són ben coneguts; pel Teorema 4.6:

$$S_L^{r_0} = \{X^e+p^{k_1}a_1X^{e-1}+\ldots+p^{r_0}a_e \;/\; a_1,\ldots,a_e\in\mathbb{Z}_p,\ p\nmid a_e\},$$

on $k_i=[\frac{ir_0}{e}]+1$, $1\leqslant i<e$; ja que ara $\mathbb{F}_p^{*e}=\mathbb{F}_p^*$.

En primer lloc observem que l'aplicació $H(\beta)=\beta^m$ defineix una bijecció entre $P^{r_0}-P^{r_0+1}$ i P^r-P^{r+1}, en efecte, els elements d'aquests conjunts s'escriuen de manera única com:

$$\pi^{r_0}a\,\xi\ ,\ \pi^r b\,\eta\ ,\quad a,b\in R,\ ab\neq 0,\ \xi,\eta\in U_1$$

respectivament, essent R el conjunt de les arrels p-1-èssimes de la unitat de $\mathbb{Q}_p$, U_1 el grup dels unitaris $\nu\in L$ tals que $v_p(\nu-1)>0$ i π un uniformitzant fix qualsevol. Com que $p\nmid m$ exis-

teix un únic $\xi \in U_1$ tal que $\xi^m=\eta$ [Hasse,1980,pag.217] i com que $(m,p-1)=1$ existeix un únic $a\in \mathcal{R}$ tal que $a^m=b$.

Si denotem per A' el subconjunt de l'anell d'enters de L format pels elements primitius, el conjunt de les arrels dels polinomis de S_L^r i $S_L^{r_0}$ és, respectivament:

$$A^r = (P^r-P^{r+1}) \cap A',$$

$$A^{r_0} = (P^{r_0}-P^{r_0+1}) \cap A' = P^{r_0}-P^{r_0+1},$$

ja que $P^{r_0}-P^{r_0+1} \subset A'$. Si definim $\phi = \{\beta \in A^{r_0} / \beta^m \notin A'\}$ ha quedat provat el:

Lema 4.15. L'aplicació $H(\beta)=\beta^m$ defineix una bijecció entre $A^{r_0}- \phi$ i A^r. #

Ara hem de baixar aquesta bijecció a nivell de polinomis. En primer lloc necessitem saber quins polinomis de $S_L^{r_0}$ tenen les seves arrels a ϕ. Això ens ho contesta la Proposició 4.14. En efecte, si ζ és una arrel primitiva m-èssima de la unitat, com que $p\nmid m$, $M=\mathbb{Q}_p(\zeta)$ és una extensió no-ramificada de $\mathbb{Q}_p$ i per tant linealment disjunta amb L. Per tant, si $f(X)\in S_L^{r_0}$ i β és una arrel seva, $f(X)=Irr(\beta,M)$ i per tant $\beta \in \phi$ si i només si per a tot divisor d de m existeix un coeficient no nul de f(X) en una posició no múltiple de d(*). Definim per tant:

$$\Phi = \{ f(X) \in S_L^{r_0} / \exists d|m \text{ tal que } a_k=0 \text{ per a tot } k\not\equiv 0 \pmod{d} \},$$

i considerem el diagrama:

(*) D'ara endavant ja no repetirem més aquest argument i aplicarem directament la Proposició 4.14 sense justificar-ho cada vegada.

$$\begin{array}{ccc} A^{r_0} - \phi & \xrightarrow{\quad H \quad} & A^r \\ \downarrow & & \downarrow \\ S_L^{r_0} - \Phi & \dashrightarrow & S_L^r, \end{array}$$

on les fletxes verticals assignen a cada enter el seu polinomi minimal sobre $\mathbb{Q}_p$. És una simple comprovació que:

Proposició 4.16. L'aplicació $S_L^{r_0}-\Phi \xrightarrow{\quad H \quad} S_L^r$ definida per $H(f(X)=\mathrm{Irr}(\beta^m,\mathbb{Q}_p)$, essent β una qualsevol de les arrels de $f(X)$, és bijectiva.#

Aquesta bijecció ens proporciona una parametrització de S_L^r. Perquè sigui útil hem d'aprendre a calcular i_p i R_p d'elements de S_L^r en funció de les seves antiimatges per H.

Càlcul de l'índex. Sigui $f(X)=X^e+a_1X^{e-1}+\ldots+a_e\in S_L^{r_0}$. Definim per a cada divisor d de m, $d>1$:

$$x_d(f) = \min_{k\not\equiv 0 \pmod{d}} \{e\, v_p(a_k)+r_0(e-k)\}.$$

De la Proposició 4.14 es dedueix que $f(X)\in S_L^{r_0}-\Phi$ si i només si $x_d(f)<\infty$ per a tot $d|m$, $d>1$; suposem que estem en aquest cas. Sigui $\tilde{f}(X)=H(f(X))$; sabem pel Lema 4.12 que:

$$\tilde{f}(Y^m) = f_0(Y)\cdot\ldots\cdot f_{m-1}(Y),$$

essent $f_i(Y)=\zeta^{ie}\, f(Y/\zeta^i)$. Relacionem el discriminant de $\tilde{f}(Y^m)$ d'una banda amb el de $\tilde{f}(X)$ i de l'altra amb el dels $f_i(Y)$'s:

$$d(\tilde{f}(Y^m)) = (-1)^e\, m^{me}\, a_e^{m(m-1)}\, d(\tilde{f}(X))^m,$$

$$d(\tilde{f}(Y^m)) = \prod_{i=1}^{m} d(f_i(Y)) \cdot \prod_{i<j} R(f_i(Y), f_j(Y))^2.$$

Si p denota l'ideal primer de $M=\mathbb{Q}_p(\zeta)$, com que és no-ramificada:

$$d_p(f_i(Y)) = d_p(f(X)) = d_p(f(X)) = 2i_p(f) + (e-1) =$$

$$= (e-1)(r_0-1) + (e-1) = r_0(e-1).$$

Per altra banda, pel Teorema 2.6:

$$R_p(f_i,f_j) = \min_{1\leq k\leq e} \{e\, v_p((\zeta^{ik}-\zeta^{jk})a_k) + r_0(e-k)\}.$$

Ara bé,

$$v_p((\zeta^{ik}-\zeta^{jk})a_k) = \begin{cases} v_p(a_k) & \text{si } k(i-j)\not\equiv 0 \pmod{m} \\ \infty & \text{si } k(i-j)\equiv 0 \pmod{m}. \end{cases}$$

La condició $k(i-j)\equiv 0 \pmod{m}$ és equivalent a $k\equiv 0 \pmod{\frac{m}{(m,i-j)}}$, per tant $R_p(f_i,f_j) = x_{m/(m,i-j)}(f)$. En particular $R_p(f_i,f_j)$ només depèn del valor de $i-j$, el qual, quan $i<j$ varien entre 0 i m-1, pren els valors $1,2,\ldots,m-1$ repetit $m-k$ vegades el valor k. Així:

$$\sum_{i<j} R_p(f_i,f_j) = \sum_{k=1}^{m-1} (m-k)x_{m/(m,k)}(f) =$$

$$= \sum_{\substack{d\mid m \\ d<m}} \Big(\sum_{\substack{0<k<m \\ (m,k)=d}} (m-k)x_{m/d}(f)\Big) = \sum_{\substack{d\mid m \\ d<m}} x_{\frac{m}{d}}(f) \Big(\sum_{\substack{0<k<m \\ (m,k)=d}} (m-k)\Big).$$

En aquesta última suma podem canviar $m-k$ per k. La suma val:

<u>Lema 4.17</u>. $$\sum_{\substack{0<k<m \\ (m,k)=d}} k = \frac{m}{2}\,\varphi(\tfrac{m}{d}).$$

<u>Demostració</u>. Si $d=1$ i $1, n_1, \ldots, n_t < m$ són els enters primers amb m, clarament $n_t = m-1$, $n_{t-1}=m-n_1$, etc. i l'afirmació del Lema

és clara. En el cas general:

$$\sum_{\substack{0<k<m\\(m,k)=d}} k = \sum_{\substack{0<s<\frac{m}{d}\\(\frac{m}{d},s)=1}} ds = d\cdot\frac{m}{2d}\cdot\varphi\left(\frac{m}{d}\right). \#$$

Per tant:

$$\sum_{i<j} R_p(f_i,f_j) = \sum_{\substack{d\mid m\\d<m}} x_{m/d}(f)\cdot\frac{m}{2}\cdot\varphi\left(\frac{m}{d}\right) = \frac{m}{2}\sum_{\substack{d\mid m\\d>1}}\varphi(d)x_d(f).$$

Ara, igualant els dos càlculs fets anteriorment de $\tilde{f}(Y^m)$ tenim:

$$(m-1)r+md_p(\tilde{f}(X)) = d_p(\tilde{f}(Y^m)) = r(e-1)+m\sum_{\substack{d\mid m\\d>1}}\varphi(d)x_d(f).$$

De $i_p(\tilde{f})=\frac{1}{2}\left(d_p(\tilde{f}(X))-(e-1)\right)$ treiem:

<u>Proposició 4.18</u>. Sigui $\tilde{f}(X)\in S_L^r$. Sigui $f(X)=H^{-1}(\tilde{f}(X))$. Aleshores:

$$i_p(\tilde{f}) = \frac{1}{2}\left(e(r_0-1) - (r-1) + \sum_{\substack{d\mid m\\d>1}}\varphi(d)x_d(f)\right). \#$$

<u>Càlcul de la resultant</u>. Siguin $f(X)=X^e+a_1X^{e-1}+\ldots+a_e$, $g(X)=X^e+b_1X^{e-1}+\ldots+b_e\in S_L^{r_0}-\Phi$. Per a tot divisor d de m definim:

$$y_d(f,g) = \min_{1\leq k\leq e}\{eR_k + r_0(e-k)\},$$

essent:

$$R_k = \begin{cases}\inf\{v_p(a_k),v_p(b_k)\} & \text{si } k\not\equiv 0 \pmod d\\ v_p(a_k)-v_p(b_k) & \text{si } k\equiv 0 \pmod d.\end{cases}$$

Observis que $y_1(f,g)=R_p(f,g)$ pel Teorema 2.6. Siguin $\tilde{f}(X)=H(f(X))$, $\tilde{g}(X)=H(g(X))$; per la Proposició 4.14 sabem que:

$$\tilde{f}(Y^m) = \prod_{i=0}^{m-1} f_i(Y),\quad \tilde{g}(Y^m) = \prod_{i=0}^{m-1} g_i(Y).$$

Per tant:

$$R(f(Y^m),g(Y^m)) = \prod_{i,j} R(f_i(Y),g_j(Y)) = (\prod_j R(f(Y),g_j(Y)))^m.$$

Per altra banda:

$$R(f(Y^m),g(Y^m)) = \prod_{i,j} g((\zeta^i\beta_j)^m) = \prod_{\substack{0\leqslant i<m\\ 1\leqslant j\leqslant e}} g(\beta_j^m) =$$

$$= (\prod_{1\leqslant j\leqslant e} g(\beta_j^m))^m = R(f(X),g(X))^m.$$

En conseqüència, $R_p(f,g) = \sum_{i=0}^{m-1} R_p(f,g_i)$. Ara, pel Teorema 2.6:

$$R_p(f,g_i) = \min_{1\leqslant k\leqslant e} \{ e\, v_p(a_k-\zeta^{ik}b_k) + r_0(e-k)\}.$$

I clarament:

$$v_p(a_k-\zeta^{ik}b_k) = \begin{cases} \inf\{v_p(a_k),v_p(b_k)\} & \text{si } ik\not\equiv 0 \pmod m \\ v_p(a_k-b_k) & \text{si } ik\equiv 0 \pmod m, \end{cases}$$

de manera que $R_p(f,g_i) = y_{m/(i,m)}(f,g)$. Per tant:

$$\sum_{i=0}^{m-1} R_p(f,g_i) = \sum_{d|m} \Big(\sum_{\substack{0\leqslant i<m\\ (i,m)=d}} y_{m/(i,m)}(f,g)\Big) =$$

$$= \sum_{d|m} \varphi(\tfrac{m}{d}) y_{m/d}(f,g) = \sum_{d|m} \varphi(d) y_d(f,g).$$

Queda provat per tant:

<u>Proposició 4.19</u>. Siguin $\tilde f(X),\tilde g(X)\in S_L^r$ i $f(X)=H^{-1}(\tilde f(X))$, $g(X)=H^{-1}(\tilde g(X))$. Aleshores:

$$R_p(\tilde f,\tilde g) = \sum_{d|m} \varphi(d) y_d(f,g).\#$$

<u>Remarca</u>. Les fòrmules de les Proposicions 4.18 i 4.19 engloben quan m=1 les que ja coneixiem del cas (r,e)=1. En els dos cassos si d/e, $x_d(f)=y_d(f,g)=er_0$. Apart d'aquesta petita simplificació

es dedueix del Teorema 4.6 que els valors de $x_d(f)$ i $y_d(f,g)$ són molt variables. En particular comprovem que $i_p(h)$ pels elements $h(X) \in S_L^r$ ara dista molt de ser constant.

Hem aconseguit finalment una bona parametrització de S_L^r. En efecte, el conjunt $S_L^{r_0}-\Phi$ el tenim perfectament parametritzat; si definim:

$$\hat{i}_p(f) = i_p(H(f)), \quad \hat{R}_p(f,g) = R_p(H(f),H(g)),$$

per a qualsevols $f(X),g(X) \in S_L^{r_0}-\Phi$, les fórmules de les Proposicions 4.18 i 4.19 permeten calcular $\hat{i}_p(f)$ i $\hat{R}_p(f,g)$ en funció dels paràmetres que caracteritzen $f(X)$ i $g(X)$ (els seus propis coeficients) i per la Proposició 4.16:

$$I^r(n) = \min \{ \sum_{i \leq j} \hat{R}_p(f_i,f_j) + \sum_i \hat{i}_p(f_i) \},$$

prenent n elements de $S_L^{r_0}-\Phi$. No obstant, ja es veu clarament que la resolució d'aquest problema combinatori serà ara particularment més complicada que en el cas $(r,e)=1$. Potser fins i tot ens veuriem abocats a considerar una solució algorítmica particular per obtenir els $x_{r,k}$ que necessitem per aplicar l'algoritme general del Teorema 4.1. Ho deixem estar.

SIMBOLS

Al costat de cada símbol indiquem la pàgina on es defineix per primera vegada.

Índex terminològic.

Referències.

M. Bauer, Zur allgemeine Theorie der algebraische Grössen, J. Reine Angew. Math. 132(1907), 21-32.

b) Über die ausserwesentlichen Diskriminantenteiler einer Gattung, Math. Ann. 64(1907), 572-576.

R. Bungers, Über Zahlkörper mit gemeinsamen ausserwesentlichen Diskriminantenteilern, Jber. Deutsch. Math.--Verein. 46(1936), 93-96.

L. Carlitz, On abelian fields, Trans. Amer. Math. Soc. 35 (1933), 122-136.

A note on common index divisors, Proc. Amer. Math. Soc. 3(1952), 688-692.

R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höhere Kongruenzen, Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen, vol.23(1878), 1-23.

H. T. Engstrom, On the common index divisors of an algebraic field, Trans. Amer. Math. Soc. 32(1930), 223-237.

H. Hasse, Number Theory, Springer, Berlin-Heidelberg-N.York, 1980.

K. Hensel, Aritmetische Untersuchungen über die gemeinsamer ausserwesentlichen Diskriminantenteiler einer Gattung, J. Reine Angew. Math. 113(1894), 128-160.

K. Hensel, Über den grössten gemeinsamen Teiler aller Zahlen, welche durch eine ganze Funktion von n Veränderlichen darstellbar sind, J. Reine Angew. Math. 116(1896), 350-356.

M. Krasner, Nombre des extensions d'un degreé donné d'un corps P-adique, Coll. Tend. Géom. en Algèbre, Paris 1966, 143-169.

J. Llorente-E. Nart, Sobre l'índex d'extensions relatives de cossos de nombres, Actes VII JMHL, Sant Feliu de Guíxols, 1980, Pub. Mat. UAB, 20(1980), 161-164.

Effective determination of the decomposition of the rational primes in a cubic field, apareixerà als Proc. Amer. Math. Soc.

T. Nagell, Quelques resultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algebrique, Arkiv Math. 6(1966), 269-289.

W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Monographie Matematyczne, 57, PWN-Polish scientific Publishers, Warsaw, 1974.

Ö. Ore Zur Theorie der algebraischen Körper, Acta Math. 44(1923), 219-314.

Bestimmung der Diskriminanten algebraischer Körper, Acta Math. 45(1925), 303-344.

Über den Zusammenhang zwischen den definierenden

Gleichungen und der Idealtheorie in algebraischen Körpern, Math. Ann. 96(1926), 313-352.

Newtonsche Polygone in der Theorie der algebraischen Körper, Math..Ann. 99(1928), 84-117.

A. A. Sukallo, К вопросу определения индекса поля алгебраических чисел, Уч. зап. ун-та Ростов н/Д.32(1955),4, 37-42.

L. Tornheim, Minimal basis and inessential discriminant divisors for a cubic field, Pacific J. Math. 5(1955), 623-631.

E. Von Zylinsky, Zur Theorie der ausserwesentlicher Diskriminantenteiler algebraischer Körper, Math. Ann. 73(1913), 273-274.

J. Śliwa, On the nonessential discriminant divisor of an algebraic number field, Acta Arith. 42(1982), 57-72.

Rebut el 27 de Setembre del 1982

Secció de Matemàtiques
Universitat Autònoma de Barcelona
Barcelona-Bellaterra