Nombres d'extensions abelianes i les seves funcions generatrius

Artur Travesa i Grau

NOMBRES D'EXTENSIONS ABELIANES

I LES SEVES FUNCIONS GENERATRIUS

Artur Travesa i Grau

Memòria presentada per a optar al grau de Doctor en Ciències Matemàtiques.

Facultat de Matemàtiques.
Universitat de Barcelona.

FAIG CONSTAR que aquesta memòria ha estat realitzada per Artur Travesa i Grau sota la meva direcció, a la Facultat de Matemàtiques de la Universitat de Barcelona.

P. Bayer

Barcelona, setembre del 1.987.

Dra. Pilar Bayer i Isant.

ÍNDEX.

INTRODUCCIÓ

El teorema d'Hermite-Minkowski assegura que, per a tot cos de nombres, el conjunt de les extensions de grau donat i no ramificades fora d'un conjunt finit de primers és finit. El coneixement de fites fines per a aquest número d'extensions jugaria un paper important a l'hora de fer efectius els resultats de G. Faltings sobre la conjectura de Mordell. El 1.962, I.R. Šafarevič proposà el problema de la determinació de si el grup de Galois de l'extensió maximal d'un cos de nombres no ramificada fora d'un conjunt finit de primers és o no topològicament finit generat i, en cas afirmatiu, de calcular una fita del número de generadors d'aquest grup.

En la línia de comptar extensions cal fer referència als resultats que, d'una manera o altra, incideixen en el present treball.

És ben conegut un teorema d'Artin-Schreier que caracteritza els cossos que tenen exactament una extensió finita no trivial com els cossos totalment ordenats maximals.

El coneixement del fet de l'existència d'una única extensió de grau donat per a cada cos finit es remunta a l'any 1.830, en què É. Galois escriu en [Ga 1] la frase, que cito textualment:

> *"Si maintenant on veut avoir les solutions imaginaires du second degré, on cherchera le plus grand facteur commun à* $Fx = 0$ *et à* $x^{p^2-1}=1$, *et en général, les solutions de l'ordre* ν *seront*

données par le plus grand commun diviseur à

$Fx = 0$ *et à* $x^{p^{\nu}-1}=1$."

Aquí, Fx és un polinomi separable en x, i Fx = 0 és la congruència mòdul un primer p.

La bijecció entre el conjunt de les extensions no ramificades d'un cos local i el conjunt de les extensions del seu cos residual dóna l'existència, per a cada cos local, d'una única extensió no ramificada de grau donat.

Més en general, el conjunt de totes les extensions de grau donat d'un cos p-àdic és també finit i el seu cardinal ha estat calculat per M. Krasner en [Kr 1] . En efecte, Krasner calcula el número d'extensions totalment ramificades de grau i discriminant donats d'un cos local; això li permet, en el cas p-àdic, obtenir el número d'extensions totalment ramificades de grau donat i, a partir d'aquí, el número total d'extensions de grau donat. Aquests números van ésser reobtinguts per J -P. Serre en [Se 1] on es dóna una fórmula de massa per a les extensions totalment ramificades de grau donat d'un cos local.

El cas de les extensions abelianes del cos dels números racionals ha estat tractat per S. Mäki en [Mä 1] , on calcula el número d'extensions abelianes de $\mathbb{Q}$ amb grup de Galois i discriminants donats.

En aquesta memòria ens situem en el problema de comptar extensions abelianes. En el capítol I tractem el problema en el cas local. Introduïm la funció generatriu de Dirichlet dels números d'extensions abelianes de grau donat d'un cos p-àdic, i ens plantegem com a principal objectiu l'estudi d'aquesta funció. Per a això, cal calcular exactament el número

d'extensions abelianes amb grau i índex de ramificació donats, cosa que s'aconsegueix a partir de la teoria de Lubin-Tate. El resultat principal d'aquest capítol és que, si $K|\mathbb{Q}_p$ és una extensió finita qualsevol de grau n_0, la funció generatriu de Dirichlet dels números d'extensions abelianes de grau fixat de K es prolonga a una funció meromorfa del pla complex amb pols simples únicament en els punts $t = 2,3,\ldots,n_0$, i un pol doble en $t = 1$. En $t = 0$ la funció presenta un pol simple si, i només si, K conté les arrels p-èsimes de la unitat.

Seguidament ens dedicquem al cas de les extensions abelianes de $\mathbb{Q}$. Fixat un conjunt finit P de primers, el conjunt de les extensions abelianes de $\mathbb{Q}$ de grau fixat i no ramificades fora de P és finit, i això ens permet introduir la funció generatriu de Dirichlet d'aquests números d'extensions. Abans, però, i imitant la línia de Krasner i Serre, calculem el número d'extensions abelianes de $\mathbb{Q}$ de grau donat i amb índexs de ramificació prefixats. Això és l'objectiu del capítol II. Aquesta manera de procedir dóna una partició del conjunt de les extensions abelianes de $\mathbb{Q}$ molt apta per a treure'n conseqüències: cossos de gèneres, divisors del número de classes, generadors de les extensions, construcció efectiva d'aquestes,.... En particular, obtenim un refinament del teorema de Kronecker-Weber per al cas de les extensions abelianes de $\mathbb{Q}$. Donada una extensió abeliana $K|\mathbb{Q}$, aquest teorema ens assegura l'existència d'una arrel de la unitat, ζ, tal que $K \subseteq \mathbb{Q}(\zeta)$ i que l'extensió $\mathbb{Q}(\zeta)|K$ és moderadament ramificada a tots els primers de K. Nosaltres obtenim l'existència d'una extensió abeliana $L|\mathbb{Q}$, que també es construeix de manera efectiva, tal que $K \subseteq L$ i que $L|K$ és no ramificada a tots els primers de K.

En el capítol III obtenim definitivament els números d'extensions abelianes de Q de grau donat i no ramificades fora d'un conjunt finit P de primers, i estudiem la funció generatriu d'aquests números.

Un estudi acurat dels discriminants i de la ramificació de les extensions abelianes de Q permetria obtenir, amb certa dificultat, i a partir dels números calculats per Mäki, els números d'extensions abelianes de Q de grau donat i no ramificades fora de P. També els podríem obtenir, sumant, a partir dels números calculats al capítol II. Per a tal fi, però, és més còmode procedir directament.

L'estudi de la funció generatriu de Dirichlet d'aquests números d'extensions queda facilitat utilitzant els resultats i les tècniques del capítol II, que permeten caracteritzar ràpidament els factors d'Euler que esdevenen trivials. El resultat final d'aquest capítol és que aquesta funció es prolonga a una funció meromorfa de tot el pla complex amb un únic pol en $t = 0$ d'ordre igual al número de primers del conjunt P.

Hem inclòs en un apèndix els resultats de grups que s'utilitzen a la resolució dels problemes de cossos. Alguns d'aquests resultats són coneguts; per exemple, l'ordre del grup d'automorfismes d'un grup abelià finit i el número de subgrups de tipus donat d'un p-grup abelià finit. D'altres són nous; per exemple, els teoremes 6.3 i 6.4, que donen els números de subgrups de tipus (resp. ordre) donat i subjectes a certes condicions suplementàries. Per últim, hem inclòs una interpretació dels factors difícils que ens apareixen a les fórmules en funció dels números de Betti de les Grassmannianes sobre els cossos finits.

Vull agrair molt sincerament a la Dra. Pilar Bayer Isant totes les hores que m'ha dedicat, moltes vegades traient-les del seu propi treball, així com els molts i valuosos consells que m'ha donat durant tot el temps de preparació d'aquest treball. Sense ells, aquest no hauria estat possible.

CAPÍTOL I.

EXTENSIONS ABELIANES DELS COSSOS LOCALS.

§1.- Introducció i notacions

En tot aquest capítol K designarà un cos local: és a dir, un cos complet respecte d'una valoració discreta no trivial i amb cos residual finit. Fixarem una clausura algebraica separable $\bar{K}$ de K i totes les extensions de K les considerarem incloses dins $\bar{K}$. Denotarem per $A = A_K$ l'anell dels enters de K, per $p = p_K$ l'ideal maximal de A i per $\tilde{K} = A/p$ el cos residual; sigui $p > 0$ la característica de $\tilde{K}$ i sigui q el número dels seus elements.

Donats enters positius n,e, definim els següents conjunts d'extensions de K:

$$\Sigma(n;K) = \{L: K \subseteq L \subseteq \bar{K} \text{ i amb grau } [L:K] = n\},$$

$$\Sigma(n,e;K) = \{L: K \subseteq L \subseteq \bar{K}, [L:K] = n \text{ i amb índex de ramificació } e(L|K) = e\},$$

$$\Sigma_{ab}(n;K) = \{L: L \in \Sigma(n;K) \text{ i } L|K \text{ és abeliana}\},$$

$$\Sigma_{ab}(n,e;K) = \{L: L \in \Sigma(n,e;K) \text{ i } L|K \text{ és abeliana}\}.$$

Posarem $s(n;K)$, $s(n,e;K)$, $a(n;K)$, $a(n,e;K)$ els cardinals respectius que, en algun cas, poden no ser finits.

Quan K és de característica zero, K és una extensió finita del cos Q_p dels números p-àdics; aleshores, el conjunt $\Sigma(n;K)$ és finit (cf. [La 1: cap. II, §5, prop. 14]) i, per tant, també ho són els conjunts $\Sigma(n,e;K)$, $\Sigma_{ab}(n;K)$ i $\Sigma_{ab}(n,e;K)$. M.

Krasner determinà, en [Kr 1] , el cardinal $s(n;K)$ de $\Sigma(n;K)$. Per a això, Krasner calculà en primer lloc el número d'extensions totalment ramificades de grau i discriminant donats d'un cos local qualsevol, no necessàriament de característica zero. A partir d'aquest número, i en el cas de característica zero, calculà $s(n,n;K)$; és a dir, el número d'extensions totalment ramificades de grau donat; i a partir d'aquest obtingué $s(n;K)$.

Posteriorment, J -P. Serre donà una fórmula de massa per a les extensions totalment ramificades de grau donat d'un cos local. Si $L|K$ és una extensió totalment ramificada de grau n de cossos locals, podem escriure la diferent $\mathcal{D}(L|K)$ de l'extensió en la forma

$$\mathcal{D}(L|K) = p_L^{n-1+c(L|K)}$$

(cf. [Se 2: cap. III, §6, prop. 13]). Serre, en [Se 1] , defineix la massa de l'extensió per la fórmula

$$\mu(L|K) = q^{-c(L|K)}.$$

És a dir, $\mu(L|K)$ és la norma de la component salvatge de la diferent de l'extensió $L|K$. Amb aquesta massa, Serre demostra la fórmula

$$\sum_{L \in \Sigma(n,n;K)} \mu(L|K) = n.$$

Tenint en compte les condicions d'Öre, Serre calcula també el número d'extensions totalment ramificades de grau i diferent donats. Això li permet reobtenir les fórmules de Krasner.

La fórmula de massa de Serre es pot estendre al cas de ramificació arbitrària. En efecte, si K és un cos local, $e|n$, i $L \in \Sigma(n,e;K)$, aleshores podem escriure la diferent en la forma

$$\mathcal{D}(L|K) = p_L^{e-1+c(L|K)}$$

(cf. [Se 2: loc. cit]), i podem definir la massa

$$\mu(L|K) = q^{-f.c(L|K)}$$

on $f = n/e$ és el grau residual de l'extensió $L|K$. Aleshores es verifica la fórmula

$$\sum_{L \in \Sigma(n,e;K)} \mu(L|K) = e$$

(cf. [Tr 1]).

Observem que $L|K$ és moderadament ramificada si, i només si, $c(L|K) = 0$ (cf. [Se 2: loc. cit]); és a dir si, i només si, $\mu(L|K) = 1$. En particular es té que, si $p \nmid e$, aleshores $s(n,e;K) = e$. Aquesta fórmula, que es pot demostrar independentment de masses, s'utilitzarà posteriorment.

En aquest capítol ens ocupem del cas abelià. Concretament, calculem $a(n;K)$ i $a(n,e;K)$ per a tota parella d'enters positius n,e, i tot cos local K de característica zero.

En primer lloc estudiem el cas $K = \mathbb{Q}_p$. El teorema de Kronecker-Weber permet calcular $a(n,e;\mathbb{Q}_p)$ i $a(n;\mathbb{Q}_p)$. El grup de Galois de les extensions ciclotòmiques de $\mathbb{Q}_p$ és el producte de dos grups cíclics, si $p \neq 2$, i el producte de dos grups cíclics i un factor $\mathbb{Z}/2\,\mathbb{Z}$, si $p = 2$. El fet que aquests grups siguin molt senzills permet resoldre fàcilment el problema de grups a què es redueix el càlcul dels $a(n,e;\mathbb{Q}_p)$ i $a(n;\mathbb{Q}_p)$. Però, a l'hora de generalitzar els resultats a una extensió finita de $\mathbb{Q}_p$, el problema no és tan directe. És per això que hem fet una demostració aparentment més complicada també en el cas $K = \mathbb{Q}_p$, però que és la gènesi de la demostració en el cas general. De fet, fixats el grau n, i l'índex de ramificació e, i si $p \neq 2$, es pot construir una extensió abeliana que només de-

pèn de n,e, tal que conté tots els cossos $K \in \Sigma_{ab}(n,e;\mathbb{Q}_p)$. Aquesta extensió té grup de Galois molt senzill i permet obtenir $a(n,e;\mathbb{Q}_p)$. Quan s'intenta el mateix en el cas $p = 2$, calen tres extensions en lloc d'una sola, i els seus grups de Galois no són gaire més complicats.

Aquesta manera de fer les coses, i el fet de conèixer els valors de $a(n,e;\mathbb{Q}_p)$ permet introduir i estudiar la funció generatriu dels números $a(n;\mathbb{Q}_p)$ (veure §4). Si considerem les funcions $a(n,1;\mathbb{Q}_p)$ i $a(n,n;\mathbb{Q}_p)$, obtenim que la funció generatriu dels $a(n;\mathbb{Q}_p)$ és el producte de les funcions generatrius dels $a(n,1;\mathbb{Q}_p)$ i dels $a(n,n;\mathbb{Q}_p)$.

Seguidament, passem a considerar el cas general d'un cos local de característica zero. El cas moderadament ramificat no té excessius problemes i és semblant al cas moderadament ramificat sobre $\mathbb{Q}_p$; l'única diferència important és la caracterització dels valors de n,e, tals que $a(n,e;K) \neq 0$, i els resultats són també vàlids en el cas d'un cos local de característica qualsevol. Pel cas general, però, el problema es complica; cal construir, a partir de la teoria de Lubin-Tate, una família finita d'extensions prou bones de K com per a què entre totes continguin tots els cossos $L \in \Sigma_{ab}(n,e;K)$. A partir d'aquí es pot calcular el valor de $a(n,e;K)$ i el de $a(n;K)$ en funció del número de cossos d'aquesta família, número que també donem explícitament.

Introduïm també la funció generatriu dels $a(n;K)$. Com en el cas de $\mathbb{Q}_p$, la funció $a(n;K)$ és la convolució de Dirichlet de les funcions $a(n,1;K)$, del cas no ramificat, i $a(n,n;K)$, del cas totalment ramificat. Això fa que puguem reduir-nos al cas totalment ramificat. La suma dels factors d'Euler de la

funció generatriu dels $a(n,n;K)$ ens permet estendre aquesta funció a una funció meromorfa del pla complex; i l'estudi dels seus pols, obtenir una caracterització dels cossos K que contenen les arrels p-èsimes de la unitat (veure el corol.lari 7.7).

§2.- El cas moderadament ramificat sobre $\mathbb{Q}_p$.

Sigui p un nûmero primer. En aquest § es fa el càlcul de $a(n,e;\mathbb{Q}_p)$ per a tota parella d'enters positius n,e, amb $p \nmid e$. Començarem, però, pel cas no ramificat; és a dir, pel cas e = 1.

De [La 1: cap. II, §4, prop. 7 i 9] i [Se 2: cap. III, §5, teor. 2] es dedueix que, per a tot enter $n \geqslant 1$, existeix una única extensió no ramificada $K|\mathbb{Q}_p$, de grau n; en efecte, les extensions no ramificades de $\mathbb{Q}_p$ són els cossos $\mathbb{Q}_p(\zeta_N)$ on ζ_N és una arrel primitiva N-èsima de la unitat, $p \nmid N$. El conjunt de les extensions no ramificades de $\mathbb{Q}_p$ està en correspondència bijectiva amb el conjunt de les extensions del cos residual, $\mathbb{F}_p$, de $\mathbb{Q}_p$. Les extensions $\mathbb{Q}_p(\zeta_N)|\mathbb{Q}_p$ són cícliques i el grau $[\mathbb{Q}_p(\zeta_N):\mathbb{Q}_p]$ és el menor enter $n \geqslant 1$ tal que $p^n \equiv 1 \pmod N$; de manera que si triem $N = p^n-1$ obtenim la següent

Proposició 2.1.- Donat un enter $n \geqslant 1$, sigui $N = p^n-1$ i sigui $\zeta = \zeta_N$ una arrel primitiva N-èsima de la unitat. Aleshores

$$\Sigma_{ab}(n,1;\mathbb{Q}_p) = \Sigma(n,1;\mathbb{Q}_p) = \{\mathbb{Q}_p(\zeta)\}.$$

En particular, $a(n,1;\mathbb{Q}_p) = s(n,1;\mathbb{Q}_p) = 1$. ∎

El següent resultat és vàlid en el cas general, no necessàriament moderadament ramificat, i dóna (les) condicions necessàries per a què el conjunt $\Sigma_{ab}(n,e;\mathbb{Q}_p)$ sigui no buit.

Lema 2.2.- Siguin n,e, enters positius, i posem $e = p^r e'$ amb $r \geqslant 0$ i $p \nmid e'$ Aleshores, si $\Sigma_{ab}(n,e;\mathbb{Q}_p)$ és no buit, es verifica que $e|n$ i que $p \equiv 1 \pmod{e'}$.

Demostració.- La condició e|n és clara. Suposem que $\Sigma_{ab}(n,e;\mathbb{Q}_p) \neq \phi$ i sigui $K \in \Sigma_{ab}(n,e;\mathbb{Q}_p)$. El teorema de Kronecker-Weber per a $\mathbb{Q}_p$ (cf. [Ne 1: cap. III, §3, cor. 3.7]) assegura que existeixen arrels de la unitat ζ_N, $\zeta_p t$, amb $p \nmid N$, tals que $K \subseteq \mathbb{Q}_p(\zeta_N, \zeta_p t)$. Com que l'índex de ramificació es comporta de manera multiplicativa per a cadenes d'extensions, i $e(\mathbb{Q}_p(\zeta_N,\zeta_p t)|\mathbb{Q}_p) = p^{t-1}(p-1)$, resulta que $e|p^{t-1}(p-1)$. Per tant, $t \geqslant r+1$ i $p \equiv 1$ (mòd e'), com volíem demostrar. ∎

Les condicions d'aquest lema són també suficients per a què $\Sigma_{ab}(n,e;\mathbb{Q}_p)$ sigui no buit. Seguidament ho veurem en el cas moderadament ramificat, $p \nmid e$. El cas salvatgement ramificat, el veurem en el § següent.

Suposem, doncs, que tenim enters positius n,e, tals que e|n i que $p \equiv 1$ (mòd e). Si $p = 2$, aquesta condició dóna $e = 1$; és a dir, el cas no ramificat. Per tant, també podem suposar que $p \neq 2$.

L'extensió $\mathbb{Q}_p(\zeta_p)|\mathbb{Q}_p$ és totalment ramificada de grau $p-1$ i, per ser $p \neq 2$, és cíclica; com que $e|p-1$, $\mathbb{Q}_p(\zeta_p)$ conté una única subextensió $E|\mathbb{Q}_p$ de grau e que, en conseqüència, és totalment ramificada i cíclica. Però $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p((-p)^{1/p-1})$ (cf. [Wa 1: cap. 14, lema 14.6]), de manera que $E = \mathbb{Q}_p(\theta)$ amb $\theta = (-p)^{1/e}$.

Posem $N = p^n - 1$ i sigui $L = \mathbb{Q}_p(\zeta_N, \theta)$; com que $\mathbb{Q}_p(\zeta_N)|\mathbb{Q}_p$ i $\mathbb{Q}_p(\theta)|\mathbb{Q}_p$ són extensions abelianes, $L|\mathbb{Q}_p$ és abeliana; i com que aquelles són linealment disjuntes (l'una no ramificada i l'altra totalment ramificada), és $\mathrm{Gal}(L|\mathbb{Q}_p) \simeq \mathrm{Gal}(\mathbb{Q}_p(\zeta_N)|\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\theta)|\mathbb{Q}_p) \simeq (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/e\mathbb{Z})$; a més a més, $e(L|\mathbb{Q}_p) = e(\mathbb{Q}_p(\theta)|\mathbb{Q}_p) = e$. Observem que l'extensió $L|\mathbb{Q}_p$ només depèn de

p,n,e, i no del fet que $\Sigma_{ab}(n,e;Q_p)$ sigui o no buit. Amb aques tes notacions es verifica el següent.

Teorema 2.3.- Siguin n,e, enters positius tals que e|n i $p \equiv 1$ (mòd e), i sigui L el cos que acabem de construir. Aleshores:

a) Per a tot cos $K \in \Sigma(n,e;Q_p)$ és $K \subseteq L$.

b) $\Sigma_{ab}(n,e;Q_p) = \Sigma(n,e;Q_p)$.

En particular, $a(n,e;Q_p) = s(n,e;Q_p) = e$.

Donarem dues demostracions d'aquest teorema. La primera utilitza el fet que en el cas moderadament ramificat, i com ja s'ha comentat en el §1, $s(n,e;Q_p) = e$; la segona és autocontinguda i donarà peu a un resultat que s'utilitzarà en el cas general sobre Q_p.

Primera demostració del teorema 2.3.- Posem f = n/e i sigui $K_0 = Q_p(\zeta_{p^f-1})$ l'únic cos extensió no ramificada de grau f de Q_p. Per a tot cos $K \in \Sigma(n,e;Q_p)$ resulta que $K_0|Q_p$ és la subextensió no ramificada maximal de $K|Q_p$ i en conseqüència $K \in \Sigma(e,e;K_0)$. A més a més, si $K|Q_p$ és abeliana també ho és $K|K_0$, de manera que tenim la cadena d'inclusions

$$(*) \qquad \Sigma_{ab}(n,e;Q_p) \subseteq \Sigma_{ab}(e,e;K_0) \subseteq \Sigma(e,e;K_0) = \Sigma(n,e;Q_p).$$

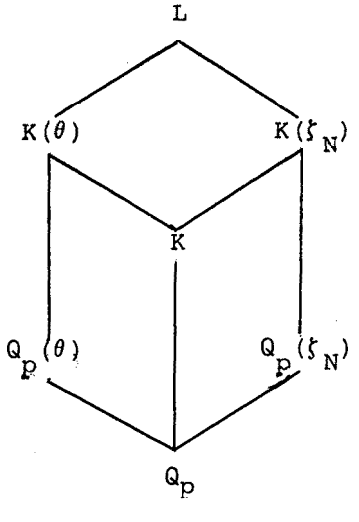
Si demostrem a) haurem demostrat la igualtat en (*) i, per tant, b). I com que p/e, és $s(n,e;Q_p) = e$ (cf. §1), de manera que $a(n,e;Q_p) = e$.

Suposem, doncs, que $K \in \Sigma(n,e;Q_p) = \Sigma(e,e;K_0)$. Com que l'extensió $K_0|Q_p$ és no ramificada, p és també un uniformitzant

de K_0, i per tant existeix una unitat u de K_0 tal que $K = K_0(\alpha)$ amb $\alpha^e = -up$ (cf. [La 1: cap. II, §5, prop. 12]). Sigui v tal que $v^e = u$; l'extensió $K_0(v)|K_0$ és no ramificada, ja que $p \nmid e$. Com que $e|p-1$, Q_p conté les arrels e-èsimes de la unitat i, per tant, l'extensió $K_0(v)|K_0$ és de grau divisor de e (cf. [La 2: cap. 8, §6, teor. 10,b]). En conseqüència, $K_0(v)|Q_p$ és una extensió no ramificada de grau divisor de $ef = n$, de manera que $K_0(v) \subseteq Q_p(\zeta_N)$. Aleshores, $K = K_0(\alpha) \subseteq K_0(v,(-p)^{1/e}) = K_0(v,\theta) \subseteq Q_p(\zeta_N,\theta) = L$, com volíem demostrar.■

Segona demostració del teorema 2.3.- Anàlogament a la primera demostració s'obté a) i b), així com les igualtats en (*). Només cal veure que $a(n,e;Q_p) = e$.

Sigui $K \subseteq L$ un subcòs qualsevol, no necessàriament en $\Sigma_{ab}(n,e;Q_p)$. Posem $X = Gal(L|K)$, $G_1 = Gal(L|Q_p(\theta)) \simeq Gal(Q_p(\zeta_N)|Q_p) \simeq \mathbb{Z}/n\mathbb{Z}$, $G_2 = Gal(L|Q_p(\zeta_N)) \simeq Gal(Q_p(\theta)|Q_p) \simeq \mathbb{Z}/e\mathbb{Z}$, i identifiquem cada G_i amb la seva imatge canònica dins $G = G_1 \oplus G_2 = Gal(L|Q_p)$. Tenim que $X \subseteq G$ i que podem calcular l'índex de ramificació $e(K|Q_p)$ de la manera següent:



com que $\mathbb{Q}_p(\zeta_N)|\mathbb{Q}_p$ és no ramificada, també ho és $K(\zeta_N)|K$ i, per tant, $e(K|\mathbb{Q}_p) = e(K(\zeta_N)|\mathbb{Q}_p) = e(K(\zeta_N)|\mathbb{Q}_p(\zeta_N))$. Però $L|\mathbb{Q}_p(\zeta_N)$ és totalment ramificada de grau e, de manera que $K(\zeta_N)|\mathbb{Q}_p(\zeta_N)$ és totalment ramificada; en conseqüència, $e(K|\mathbb{Q}_p) = [K(\zeta_N):\mathbb{Q}_p(\zeta_N)]$ és l'índex de $Gal(L|K(\zeta_N)) = Gal(L|\mathbb{Q}_p(\zeta_N)) \cap Gal(L|K) = G_2 \cap X$ en $Gal(L|\mathbb{Q}_p(\zeta_N)) = G_2$.

Això ens diu que $e(K|\mathbb{Q}_p) = e$ si, i només si, $G_2 \cap X = \{0\}$. Per tant, existeix una bijecció entre $\Sigma_{ab}(n,e;\mathbb{Q}_p)$ i el conjunt dels subgrups $X \subseteq G_1 \oplus G_2$ tals que $(G_1 \oplus G_2 : X) = n$ i $X \cap G_2 = \{0\}$, on $G_1 = \mathbb{Z}/n\mathbb{Z}$ i $G_2 = \mathbb{Z}/e\mathbb{Z}$. El resultat $a(n,e;\mathbb{Q}_p) = e$ s'obté del següent lema i acaba la demostració.■

Lema 2.4.- Siguin n,e, enters positius qualssevol tals que e|n. Posem $G_1 = \mathbb{Z}/n\mathbb{Z}$, $G_2 = \mathbb{Z}/e\mathbb{Z}$ i identifiquem G_i amb la seva imatge canònica dins $G = G_1 \oplus G_2$. Sigui $B = \{X \subseteq G: (G:X) = n \text{ i } X \cap G_2 = \{0\}\}$. Aleshores, $\#B = e$.

Demostració.- Per descomposició en subgrups de Sylow, podem suposar que n,e, són potències d'un mateix primer ℓ. Sigui $X \in B$ i suposem que X no és cíclic; aleshores X conté tots els elements de G d'ordre ℓ; en particular els de G_2 i $X \cap G_2 \neq \{0\}$. Per tant, tot $X \in B$ és un grup cíclic d'ordre $\#G_2 = e$. Sigui (a,b) un generador qualsevol de X; aleshores $a \in \frac{n}{e}(\mathbb{Z}/n\mathbb{Z})$, $b \in \mathbb{Z}/e\mathbb{Z}$ i a ó b és d'ordre $e = \#X$; però si a no és d'ordre e, ho és b i aleshores $0 \neq \frac{e}{\ell}(a,b) \in X \cap G_2$. Això diu que tots els generadors de X són de la forma (a,b) amb $a \in \mathbb{Z}/n\mathbb{Z}$ d'ordre e i $b \in \mathbb{Z}/e\mathbb{Z}$ qualsevol. Recíprocament, tot element (a,b) d'aquesta forma genera un subgrup $X \in B$. Com que X té $\varphi(e)$ gene

radors i en G hi ha $\varphi(e)e$ elements (a,b) com els anteriors, resulta que #B és el quocient, e.■

§3.- El cas general sobre Q_p.

Siguin n,e, enters positius; posem $n = p^s n'$, $e = p^r e'$ amb $r, s \geqslant 0$, $p \nmid n'$ i $p \nmid e'$. En el lema 2.2 hem vist que si $\Sigma_{ab}(n,e;Q_p) \neq \phi$ aleshores $e \mid n$ i $e' \mid p-1$; és a dir, que $r \leqslant s$, $e' \mid n'$ i $p \equiv 1 \pmod{e'}$. En aquest § es tracta de veure que aques tes condicions són també suficients per a què $\Sigma_{ab}(n,e;Q_p)$ sigui no buit, i de calcular $a(n,e;Q_p)$.

Com que totes les extensions que tractarem són abelianes, la descomposició dels grups de Galois en producte directe dels seus subgrups de Sylow i la correspondència de Galois entre subgrups i subcossos, permeten demostrar fàcilment que

$$a(n,e;Q_p) = a(n',e';Q_p) \cdot a(p^s,p^r;Q_p).$$

Com que $p \nmid e'$, $e' \mid n'$ i $p \equiv 1 \pmod{e'}$, resulta que $a(n',e';Q_p) = e'$, de manera que el càlcul de $a(n,e;Q_p)$ queda reduït al càlcul de $a(p^s,p^r;Q_p)$. Comencem pel cas $p \neq 2$.

Suposem, doncs, que $n = p^s$, $e = p^r$, $0 \leqslant r \leqslant s$, i que $p \neq 2$. Per a tot $t \geqslant r+1$, l'extensió $Q_p(\zeta_{p^t}) \mid Q_p$ és totalment ramificada de grau $p^{t-1}(p-1)$ i, per ser $p \neq 2$, és cíclica. Com que $e = p^r$ divideix el grau $[Q_p(\zeta_{p^t}):Q_p]$, $Q_p(\zeta_{p^t})$ conté una única subextensió de grau e sobre Q_p, que, en conseqüència, és també totalment ramificada i cíclica, i que denotarem per $Q_p(\theta) \mid Q_p$. Degut a la unicitat, resulta que $Q_p(\theta)$ no depèn del particular $t \geqslant r+1$ elegit.

Considerem, per altra banda, $N = p^{p^s}-1$ i sigui ζ_N una arrel primitiva N-èsima de la unitat. L'extensió $Q_p(\zeta_N) \mid Q_p$ és no ramificada de grau p^s. Posem $L = Q_p(\zeta_N,\theta)$; observem que L només depèn de p, r, s, que és una extensió abeliana de Q_p amb

grup de Galois $\mathrm{Gal}(L|\mathbb{Q}_p) \simeq \mathrm{Gal}(L|\mathbb{Q}_p(\theta)) \times \mathrm{Gal}(L|\mathbb{Q}_p(\zeta_N)) \simeq$ $\simeq \mathrm{Gal}(\mathbb{Q}_p(\zeta_N)|\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\theta)|\mathbb{Q}_p) \simeq (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/e\mathbb{Z})$, i que $e(L|\mathbb{Q}_p) = e$.

Teorema 3.1.- Siguin p un primer senar, $n = p^s$, $e = p^r$, $0 \leqslant r \leqslant s$, i sigui L el cos que acabem de definir. Aleshores, per a tot cos $K \in \Sigma_{ab}(n,e;\mathbb{Q}_p)$ és $K \subseteq L$. A més a més $a(n,e;\mathbb{Q}_p) = e$.

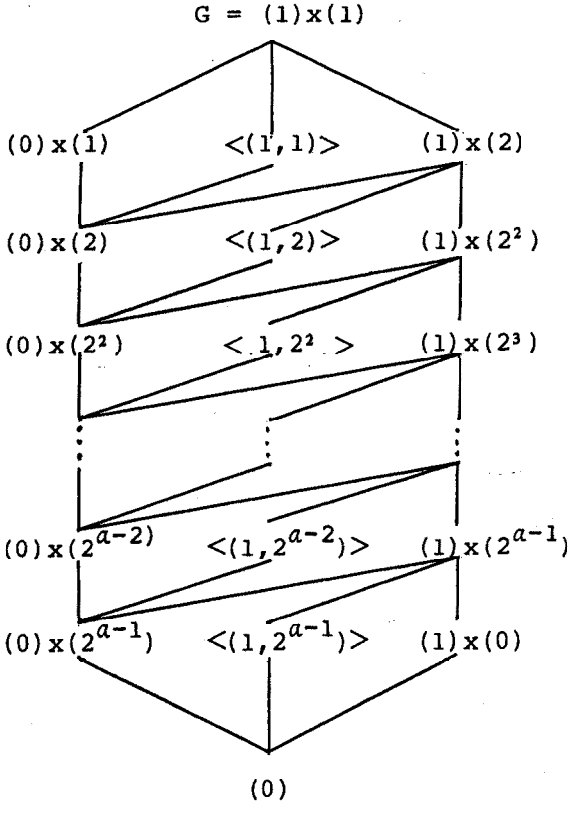
Demostració.- Suposem que $K \in \Sigma_{ab}(n,e;\mathbb{Q}_p)$; en virtut del teorema de Kronecker-Weber, existeixen arrels de la unitat ζ_M, $\zeta_p t$, tals que $K \subseteq \mathbb{Q}_p(\zeta_M, \zeta_p t)$; com que $[K:\mathbb{Q}_p]$ és una potència de p, podem suposar que M és de la forma $M = p^{p^u}-1$, i que $u \geqslant s$. L'extensió $\mathbb{Q}_p(\zeta_M, \zeta_p t)|\mathbb{Q}_p(\zeta_M)$ és totalment ramificada i cíclica, i les subextensions $K(\zeta_M)|\mathbb{Q}_p(\zeta_M)$ i $\mathbb{Q}_p(\zeta_M,\theta)|\mathbb{Q}_p(\zeta_M)$ tenen els mateixos índexs de ramificació; per tant coincideixen i $K \subseteq \mathbb{Q}_p(\zeta_M,\theta)$. Posem, ara, $X = \mathrm{Gal}(\mathbb{Q}_p(\zeta_M,\theta)|K)$, $G_1 = \mathrm{Gal}(\mathbb{Q}_p(\zeta_M,\theta)|\mathbb{Q}_p(\theta)) \simeq$ $\simeq \mathbb{Z}/p^u\mathbb{Z}$, $G_2 = \mathrm{Gal}(\mathbb{Q}_p(\zeta_M,\theta)|\mathbb{Q}_p(\zeta_M)) \simeq \mathbb{Z}/p^r\mathbb{Z}$, i $G = G_1 \oplus G_2 =$ $= \mathrm{Gal}(\mathbb{Q}_p(\zeta_M,\theta)|\mathbb{Q}_p)$; si raonem com a la segona demostració del teorema 2.3, obtenim que $e(K|\mathbb{Q}_p) = p^r$ si, i només si, $X \cap G_2 =$ $= \{0\}$. Ara bé, com que $s \geqslant r$, és $p^sG = p^sG_1 \oplus p^sG_2 = p^sG_1$ i, com que $(G:X) = p^s$, resulta que $p^sG \subseteq X$. Però

$$p^sG = \mathrm{Gal}(\mathbb{Q}_p(\zeta_M,\theta)|\mathbb{Q}_p(\zeta_N,\theta)) = \mathrm{Gal}(\mathbb{Q}_p(\zeta_M,\theta)|L),$$

de manera que $K \subseteq L$. Això és dir que podem suposar que $u = s$; és a dir, que $M = N$. Així, obtenim una bijecció entre $\Sigma_{ab}(p^s,p^r;\mathbb{Q}_p)$ i el conjunt de tots els subgrups X d'índex p^s de $G = G_1 \oplus G_2$ tals que $X \cap G_2 = \{0\}$, on $G_1 = \mathbb{Z}/p^s\mathbb{Z}$ i $G_2 = \mathbb{Z}/p^r\mathbb{Z}$. Podem, doncs, aplicar el lema 2.4, i obtenim que $a(p^s,p^r;\mathbb{Q}_p) = p^r$, com volíem demostrar. ∎

Només resta calcular $a(p^s, p^r; \mathbb{Q}_p)$ en el cas $p = 2$. Per a tot $t \geqslant r + 2$ l'extensió $\mathbb{Q}_2(\zeta_{2^t}) | \mathbb{Q}_2$ és totalment ramificada de grau 2^{t-1}; però, a diferència del cas $p \neq 2$, aquesta extensió no és, en general, cíclica; en efecte, $\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^t}) | \mathbb{Q}_2) \simeq$ $\simeq (\mathbb{Z} / 2\mathbb{Z}) \times (\mathbb{Z} / 2^{t-2}\mathbb{Z})$, i l'extensió només és cíclica en el cas $t = 2$. Tenim, però, el següent

Lema 3.2.- Sigui a un enter positiu. El reticle dels subgrups del grup $G = (\mathbb{Z} / 2\mathbb{Z}) \times (\mathbb{Z} / 2^a\mathbb{Z})$ és el següent:



Demostració.- Els subgrups $(0)x(1)$, $\langle(1,1)\rangle$ són cíclics d'índex 2 en G i contenen el subgrup $(0)x(2)$ com a subgrup d'índex 2. A més a més, $(1)x(2)$ és d'índex 2 en G, isomorf a $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{a-1}\mathbb{Z})$ i conté els subgrups $(0)x(2)$, $\langle(1,2)\rangle$ i $(1)x(4)$ com a subgrups d'índex 2. De manera que si demostrem que $(0)x(1)$, $\langle(1,1)\rangle$ i $(1)x(2)$ són els únics subgrups d'índex 2 en G, un argument inductiu acaba la demostració. Però això és un senzill exercici d'àlgebra elemental.■

D'aquest lema resulta que existeixen exactament tres subcossos de $Q_2(\zeta_{2^t})$ de grau 2^r sobre Q_2; els denotarem per $Q_2(\theta_j)$, $j = 1,2,3$. Són les tres úniques extensions totalment ramificades de grau 2^r de Q_2 incloses en $Q_2(\zeta_{2^t})$; en general, n'hi ha d'altres no incloses en $Q_2(\zeta_{2^t})$, com veurem més endavant. Dues d'elles són cícliques i l'altra és abeliana amb grup de Galois isomorf a $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{r-1}\mathbb{Z})$. Posarem $j = 3$ per a aquesta darrera i $j = 1,2$ per a les cícliques. Posem, també, $N = 2^{2^s}-1$ i $L_j = Q_2(\zeta_N, \theta_j)$, $1 \leqslant j \leqslant 3$. Amb aquestes notacions tenim que

Proposició 3.3.- Si $K \in \Sigma_{ab}(2^s, 2^r; Q_2)$ aleshores existeix $j \in \{1,2,3\}$, únic, tal que $K \subseteq L_j$.

Demostració.- Sigui $K \in \Sigma_{ab}(2^s, 2^r; Q_2)$; existeixen enters $M = 2^{2^u}-1$ i $t >> 0$ tals que $K \subseteq Q_2(\zeta_M, \zeta_{2^t})$ i podem suposar que $t \geqslant r+2$ i que $u \geqslant s$. Es té que $\mathrm{Gal}(Q_2(\zeta_M, \zeta_{2^t}) \mid Q_2(\zeta_M)) \simeq \mathrm{Gal}(Q_2(\zeta_{2^t})|Q_2) \simeq$ $\simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{t-2}\mathbb{Z})$, de manera que només hi ha tres subextensions, les $Q_2(\zeta_M, \theta_j) \mid Q_2(\zeta_M)$, totalment ramificades de grau 2^r; això diu que $K(\zeta_M) \mid Q_2(\zeta_M)$ és una d'elles i, per tant,

existeix j tal que $K \subseteq Q_2(\zeta_M, \theta_j)$. Aquest valor de l'índex j és únic, ja que si $K \subseteq Q_2(\zeta_M, \theta_j) \cap Q_2(\zeta_M, \theta_{j'})$ amb $j \neq j'$, es té que $e(K|Q_2) < 2^r$. El raonament que permet posar M = N és idèntic al del cas $p \neq 2$ (cf. teorema 3.1), i això acaba la demostració.■

Posem ara, $\Sigma_{ab}^{(j)}(2^s, 2^r; Q_2)$ el conjunt dels cossos $K \in \Sigma_{ab}(2^s, 2^r; Q_2)$ tals que $K \subseteq L_j$, i $a_j(2^s, 2^r; Q_2)$ el seu cardinal, $1 \leqslant j \leqslant 3$. Aleshores, si $r \geqslant 1$, es té que $a(2^s, 2^r; Q_2) = \sum_{j=1}^{3} a_j(2^s, 2^r; Q_2)$, ja que els tres conjunts són disjunts.

Per al càlcul dels $a_j(2^s, 2^r; Q_2)$ podem raonar de manera semblant a la del teorema 3.1: per a j = 1,2, $G_2 = \mathrm{Gal}(Q_2(\theta_j)|Q_2) \simeq \mathbb{Z} / 2^r \mathbb{Z}$ i per a j = 3, $G_2 = \mathrm{Gal}(Q_2(\theta_3)|Q_2) \simeq (\mathbb{Z} / 2\mathbb{Z}) \times (\mathbb{Z} / 2^{r-1}\mathbb{Z})$, mentre que $G_1 = \mathrm{Gal}(Q_2(\zeta_N)|Q_2) \simeq \mathbb{Z} / 2^s\mathbb{Z}$, en els tres casos. Existeix una bijecció entre $\Sigma_{ab}^{(j)}(2^s, 2^r; Q_2)$ i el conjunt dels subgrups $X \subseteq G = G_1 \oplus G_2$ d'índex 2^s i tals que $X \cap G_2 = \{0\}$. En virtut del lema 2.4, resulta que per a j = 1,2 és $a_j(2^s, 2^r; Q_2) = 2^r$. Pel cas j = 3 es té també que $a_3(2^s, 2^r; Q_2) = 2^r$. En efecte, es verifica el següent

Lema 3.4.- Siguin r,s, enters, $s \geqslant r \geqslant 2$; siguin $G_1 = \mathbb{Z} / 2^s \mathbb{Z}$, $G_2 = (\mathbb{Z} / 2\mathbb{Z}) \times (\mathbb{Z} / 2^{r-1}\mathbb{Z})$, i $G = G_1 \oplus G_2$. Aleshores, el número de subgrups $X \subseteq G$ tals que $(G:X) = 2^s$ i $X \cap G_2 = \{0\}$ és 2^r.

Demostració.- Si $X \subseteq G$ és un tal subgrup, aleshores X és cíclic. En efecte, si no ho fos, X contindria tres, o més, elements d'ordre 2 dels set que té G; d'aquests set elements, n'hi ha quatre amb primera component d'ordre 2 en G_1 i els altres tres amb pri-

mera component igual a zero; com que $X \cap G_2 = \{0\}$, els tres elements de X d'ordre 2 han de tenir primera component no nul.la; però això no és possible ja que la suma de dos d'ells és el tercer i té primera component nul.la. Per tant X és cíclic. Com que X és d'ordre 2^r, conté exactament 2^{r-1} generadors, i tots són de la forma (a,x,y) amb $a \in G_1$ d'ordre 2^r. Recíprocament, tot element de G d'aquesta forma genera un subgrup X com els de l'enunciat. Com que en G hi ha exactament $2^{r-1}(2.2^{r-1})$ elements d'aquesta forma, resulta que el número de subgrups X en les condicions de l'enunciat és el quocient, 2^r.■

Amb tot això ja podem establir el teorema final sobre Q_p:

Teorema 3.5.- Sigui p un primer i siguin n,e, enters positius. Aleshores:

$$\text{(i)}\quad a(n,e;Q_p) = \begin{cases} 1 & \text{si } e = 1, \\ e & \text{si } e = p^r e',\ p \equiv 1 \pmod{e'}, \\ & \quad e \mid n,\ p \neq 2, \\ 3e & \text{si } e = 2^r \mid n,\ r \geqslant 1,\ p = 2, \\ 0 & \text{altrament;} \end{cases}$$

$$\text{(ii)}\quad a(n;Q_p) = \begin{cases} \sigma_1((n,p-1))\ \sigma_1(p^{v_p(n)}) & \text{si } p \neq 2, \\ 3.2^{1+v_2(n)}-5 & \text{si } p = 2; \end{cases}$$

on $\sigma_1(m)$ és la suma de tots els divisors positius de m.

Demostració.- La part (i) no és res més que posar plegats els resultats següents: la proposició 2.1 en el cas e = 1; els teo

remes 2.3 i 3.1 en el cas $p \neq 2$; el teorema 2.3 i les observacions anteriors a aquest teorema en el cas $p = 2$, $r \geqslant 1$; i tenir en compte el lema 2.2 que caracteritza quan $a(n,e;Q_p) \neq 0$.

Per a demostrar (ii) només cal sumar: $a(n;Q_p) = \sum_{e|n} a(n,e;Q_p)$. En el cas $p \neq 2$, $a(n,e;Q_p) \neq 0$ només quan $e = p^r e'$ amb $e' | (n,p-1)$ i $0 \leqslant r \leqslant v_p(n)$, i aleshores $a(n,e;Q_p) = e = p^r e'$; per tant

$$a(n;Q_p) = \sum_{e' | (n,p-1)} \; \sum_{0 \leqslant r \leqslant v_p(n)} e'p^r = \sigma_1((n,p-1))\sigma_1(p^{v_p(n)}).$$

Anàlogament, si $p = 2$, $a(n,e;Q_2) \neq 0$ només quan $e = 2^r | n$, i aleshores $a(n,e;Q_2) = 3e$ si $e > 1$ i $a(n,1;Q_2) = 1$. Per tant

$$a(n;Q_2) = 3 \sum_{r=0}^{v_2(n)} 2^r - 2 = 3\,\frac{2^{1+v_2(n)}-1}{2-1} - 2 = 3.2^{1+v_2(n)} - 5. \blacksquare$$

§4.- La funció generatriu de $a(n;Q_p)$.

Sigui p un número primer. Definim les sèries de Dirichlet

$$G(Q_p;t) = \sum_{n \geqslant 1} a(n;Q_p)n^{-t},$$

$$G_{nr}(Q_p;t) = \sum_{n \geqslant 1} a(n,1;Q_p)n^{-t},$$

$$G_{tr}(Q_p;t) = \sum_{n \geqslant 1} a(n,n;Q_p)n^{-t},$$

i les anomenem les funcions generatrius de Dirichlet del número d'extensions abelianes de Q_p, del número d'extensions (abelianes) no ramificades de Q_p, i del número d'extensions abelianes totalment ramificades de Q_p, respectivament.

Fins aquí no tenim res més que una definició formal; cal veure on les sèries són convergents i quina funció defineixen. Començarem pel cas no ramificat; és a dir, el cas de la sèrie $G_{nr}(Q_p;t)$

Com que, per a tot enter $n \geqslant 1$, és $a(n,1;Q_p) = 1$, es té que $G_{nr}(Q_p;t) = \sum_{n \geqslant 1} n^{-t}$; és a dir:

Proposició 4.1.- La sèrie $G_{nr}(Q_p;t)$ és absolutament convergent en el semiplà $Re(t) > 1$ i coincideix amb la funció zeta de Riemann.■

Respecte de la convergència de les sèries $G(Q_p;t)$ i $G_{tr}(Q_p;t)$ tenim el següent

Lema 4.2.- Les sèries de Dirichlet $G(Q_p;t)$ i $G_{tr}(Q_p;t)$ són absolutament convergents en el semiplà $Re(t) > 2$.

Demostració.- El teorema 3.5 (ii) dóna el valor de $a(n;Q_p)$. Com que $0 \leqslant a(n,n;Q_p) \leqslant a(n;Q_p)$, és suficient provar el resultat per a la sèrie $G(Q_p;t)$. Però, si $p \neq 2$,

$$\begin{aligned} a(n;Q_p) &= (p^{1+v_p(n)} - 1)\ (p-1)^{-1}\ \sigma_1((n,p-1)) \leqslant \\ &\leqslant 2\ p^{v_p(n)}\ \sigma_1(p-1) \leqslant \\ &\leqslant 2\ n\ \sigma_1(p-1), \end{aligned}$$

i si $p = 2$,

$$\begin{aligned} a(n;Q_2) &= 3.2^{1+v_2(n)} - 5 \leqslant \\ &\leqslant 6\ n - 5 \leqslant \\ &\leqslant 6\ n. \end{aligned}$$

Així, existeix una constant M que només depèn de p, tal que $0 \leqslant a(n;Q_p) \leqslant Mn$, i, en conseqüència, la sèrie $G(Q_p;t)$ és absolutament convergent en el semiplà $\mathrm{Re}(t) > 2$.■

Corol.lari 4.3.- Les sèries $G(Q_p;t)$ i $G_{tr}(Q_p;t)$ defineixen funcions analítiques en el semiplà $\mathrm{Re}(t) > 2$.

Demostració.- Tota sèrie de Dirichlet defineix una funció analítica en el seu semiplà de convergència (cf.[Ap. 1: cap. 11, §7, teor. 11.12]). ■

Les funcions $G(Q_p;t)$ i $G_{tr}(Q_p;t)$ admeten descomposició en producte d'Euler. En efecte,

Lema 4.4.- Les funcions aritmètiques $a(n;Q_p)$ i $a(n,n;Q_p)$ són funcions multiplicatives de n.

Demostració.- Immediata a partir del fet que les extensions són abelianes, i per tant, $a(n;Q_p) = \prod_{\ell|n} a(\ell^{v_\ell(n)};Q_p)$ i $a(n,n;Q_p) = \prod_{\ell|n} a(\ell^{v_\ell(n)}, \ell^{v_\ell(n)};Q_p)$. ∎

D'aquest lema es dedueix que les funcions $G(Q_p;t)$ i $G_{tr}(Q_p;t)$ admeten la descomposició en producte d'Euler

$$G(Q_p;t) = \prod_{\ell} \sum_{r \geqslant 0} a(\ell^r;Q_p)\ell^{-rt}$$

$$G_{tr}(Q_p;t) = \prod_{\ell} \sum_{r \geqslant 0} a(\ell^r,\ell^r;Q_p)\ell^{-rt},$$

el producte estès a tots els números primers ℓ, i convergent en $Re(t) > 2$ (cf.[Ap 1: cap. 11, §5, teorema 11.6]).

Per a aquestes funcions podem calcular explícitament els factors d'Euler. Ho farem primerament per a la funció $G_{tr}(Q_p;t)$.

El cas més senzill és el cas $p = 2$. En efecte, de

$$a(\ell^r,\ell^r;Q_2) = \begin{cases} 1 & \text{si } r = 0, \\ 0 & \text{si } r \geqslant 1,\ \ell \neq 2, \\ 3\ell^r & \text{si } r \geqslant 1,\ \ell = 2, \end{cases}$$

resulta que els factors d'Euler de $G_{tr}(Q;t)$ són 1 si $\ell \neq 2$, i

$$1 + 3\sum_{r \geqslant 1} 2^{r(1-t)} = 1 + 3.2^{1-t}(1-2^{1-t})^{-1} = (1+2^{2-t})(1-2^{1-t})^{-1},$$

si $\ell = 2$. Per tant, tenim la següent:

Proposició 4.5.- En el semiplà $Re(t) > 2$, $G_{tr}(Q_2;t) = (1+2^{2-t})(1-2^{1-t})^{-1}$.■

Per a $p \neq 2$ el resultat és el següent:

Proposició 4.6.- En el semiplà $Re(t) > 2$, i si $p \neq 2$, aleshores

$$G_{tr}(Q_p;t) = (1-p^{1-t})^{-1} \sigma_{1-t}(p-1),$$

on $\sigma_{1-t}(p-1)$ és la suma de les potències $(1-t)$-èsimes dels divisors positius de $p-1$.

Demostració.- Si $\ell = p$ es té que $a(p^r,p^r;Q_p) = p^r$, de manera que el factor d'Euler de $G_{tr}(Q_p;t)$ que correspon al primer p és $\sum_{r \geq 0} p^{r(1-t)} = (1-p^{1-t})^{-1}$; per altra banda, si $\ell \neq p$ i $\ell^r \nmid p-1$, aleshores $a(\ell^r,\ell^r;Q_p) = 0$, mentre que si $\ell^r | p-1$ és $a(\ell^r,\ell^r;Q_p) = \ell^r$. Per tant, el factor d'Euler que correspon al primer $\ell \neq p$ val 1 si $\ell \nmid p-1$ i $\sum_{0 \leq r \leq v_\ell(p-1)} \ell^{r(1-t)} = \sigma_{1-t}(\ell^{v_\ell(p-1)})$, si $\ell | p-1$.

Com que σ_{1-t} és una funció multiplicativa, $\prod_{\ell | p-1} \sigma_{1-t}(\ell^{v_\ell(p-1)}) = \sigma_{1-t}(p-1)$, i això acaba la demostració.■

El següent resultat permet obtenir fàcilment $G(Q_p;t)$ a partir de $G_{nr}(Q_p;t)$ i $G_{tr}(Q_p;t)$.

Proposició 4.7.- La funció $a(n;Q_p)$ és la convolució de Dirichlet de les funcions $a(n,1;Q_p)$ i $a(n,n;Q_p)$.

Demostració.- Suposem que n,e, són enters positius tals que e|n. Aleshores, $a(n,e;Q_p) = a(e,e;Q_p)$ (cf. teorema 3.5 (i)), i $a(n/e,1;Q_p) = 1$. Per tant, $a(n;Q_p) = \sum_{e|n} a(n,e;Q_p) =$

$= \sum_{e|n} a(e,e;Q_p) \cdot a(n/e,1;Q_p)$, com volíem demostrar.■

Corol.lari 4.8.- En el semiplà $Re(t) > 2$ es verifica que

$$G(Q_p;t) = G_{nr}(Q_p;t)\ G_{tr}(Q_p;t);$$

és a dir:

$$G(Q_p;t) = \begin{cases} \zeta(t)\ (1-p^{1-t})^{-1}\ \sigma_{1-t}(p-1)\ , & \text{si } p \neq 2, \\ \\ \zeta(t)\ (1-2^{1-t})^{-1}\ \ (1+2^{2-t})\ , & \text{si } p = 2. \end{cases}$$

Demostració.- Cf. [Ap 1: cap. 11, §4, teor. 11.5].■

Observació 1.- Aquest resultat es pot demostrar directament calculant els factors d'Euler de $G(Q_p;t)$, i obtenir després, com a conseqüència, la proposició 4.7.

Els resultats anteriors permeten prolongar les funcions generatrius a funcions meromorfes de tot el pla complex. En efecte, les expressions de $G_{tr}(Q_p;t)$ donades a les proposicions 4.5 i 4.6 asseguren que aquesta funció es pot prolongar a una funció analítica de tot el pla complex llevat potser del punt $t = 1$ on els denominadors s'anul.len. Ara bé, $\sigma_0(p-1) \neq 0$, i $1+2^{2-1} = 3 \neq 0$, i com que $(1-p^{1-t})^{-1}$ té un únic pol en $t = 1$, d'ordre 1, i amb residu $(\log p)^{-1}$, obtenim el següent

Teorema 4.9.- La funció $G_{tr}(Q_p;t)$ admet prolongació meromorfa a tot el pla complex amb un únic pol simple en $t = 1$, i amb residu

$$\begin{cases} \sigma_0 (p-1)/\log p & , \text{ si } p \neq 2, \\ 3/\log 2 & , \text{ si } p = 2. \end{cases}$$ ■

Observació 2.- La funció $G_{tr}(Q_p;t)$ es pot expressar també com el producte de les funcions generatrius $G_{mr}(Q_p;t)$ i $G_{sr}(Q_p;t)$ dels números d'extensions abelianes totalment i moderadament ramificades, i dels números d'extensions abelianes totalment i salvatgement ramificades, de Q_p. En efecte, si $n = p^s n'$ amb $p \nmid n'$, $a(n,n;Q_p) = a(n',n';Q_p)\, a(p^s,p^s;Q_p)$ i això és, en aquest cas, la convolució de Dirichlet de les corresponents funcions.

Amb aquesta observació es té que $G_{mr}(Q_p;t)$ és una funció analítica de tot el pla complex. Notem que el pol de $G_{tr}(Q_p;t)$ prové exclusivament de la ramificació salvatge: $G_{sr}(Q_p;t) = (1-p^{1-t})^{-1}$ si $p \neq 2$, i $G_{sr}(Q_2;t) = (1+2^{2-t})(1-2^{1-t})^{-1}$, si $p = 2$.

§5.- El cas moderadament ramificat sobre un cos local.

A partir d'ara, i pel que resta de capítol, K designarà un cos local, $A = A_K$ el seu anell d'enters, $p = p_K$ l'ideal maximal, i $\tilde{K} = A/p$ el cos residual. Siguin p la característica de $\tilde{K}$, i $q = p^{f_0}$ el número d'elements de $\tilde{K}$.

El problema que resolem en aquest § és el del càlcul de $a(n,e;K)$ en el cas moderadament ramificat $p \nmid e$. Anàlogament al cas $K = Q_p$ començarem també pel cas no ramificat.

Proposició 5.1.- Sigui $N = q^n-1$, i sigui $\zeta = \zeta_N$ una arrel primitiva N-èsima de la unitat. Aleshores $\Sigma_{ab}(n,1;K) = \Sigma(n,1;K) = \{K(\zeta)\}$. En particular, $a(n,1;K) = 1$.

Demostració.- És completament anàloga a la del cas $K = Q_p$. Hi ha una bijecció entre $\Sigma(n,1;K)$ i el conjunt de les extensions de grau n de $\tilde{K}$, donada per reducció. Com que, si $L \in \Sigma(n,1;K)$, aleshores $\tilde{L} = \tilde{K}(\tilde{\zeta})$ amb $\tilde{\zeta}$ una arrel primitiva (q^n-1)-èsima de la unitat en característica p, i $\tilde{\zeta}$ és la reducció de ζ , el lema de Hensel ens diu que $L = K(\zeta)$.■

Suposem ara que $e \geq 1$ i que $p \nmid e$. Com que si $e \nmid n$ aleshores $\Sigma(n,e;K) = \phi$, podem suposar, també, que $e|n$. El teorema que es tracta de provar és el següent:

Teorema 5.2.- Siguin e,n, enters positius tals que e|n i p∤e.

Aleshores les propietats següents són equivalents:

(i) $\Sigma_{ab}(n,e;K) \neq \phi$,

(ii) K conté les arrels e-èsimes de la unitat,

(iii) e|q-1,

(iv) $a(n,e;K) = e$.

Si es verifiquen aquestes condicions,

$$\Sigma_{ab}(n,e;K) = \Sigma(n,e;K).$$

Demostració.- La implicació (iv) ⇒ (i) és immediata. Si ζ és una arrel primitiva M-èsima de la unitat en K amb p∤M, la seva reducció mòdul p és una arrel primitiva M-èsima de la unitat en $\tilde{K}$. Però $\tilde{K} = \mathbf{F}_q$ només conté les arrels (q-1)-èsimes de la unitat; per tant, si les arrels e-èsimes de la unitat estan en K, ha de ser e|q-1. Això és (ii) ⇒ (iii). Veiem, ara, que (iii) ⇒ (iv). Suposem que e|q-1. Aleshores $\tilde{K}$ conté les arrels e-èsimes de la unitat, i pel lema de Hensel, K conté les arrels e-èsimes de la unitat.

Sigui K_0 l'única extensió no ramificada de K de grau f = n/e. Aleshores K_0 conté les arrels e-èsimes de la unitat i, per tant, tota extensió de K_0 per una arrel d'un polinomi de la forma X^e-a, $a \in K_0$, és una extensió cíclica de grau divisor de e (cf.[La 2: cap. 8, §6, teor. 10]). Per altra banda (cf.[La 1: cap. II, §5, prop. 12]), tota extensió totalment i moderadament ramificada de grau e de K_0 ve generada per una arrel d'un polinomi de la forma X^e-a, amb a un uniformitzant de K_0 ; com que $K_0|K$ és no ramificada, si π és un uniformitzant de K, podem escriure a en la forma $a = u\pi$ amb $u \in U_{K_0}$, unitat de K_0..

Sigui, ara, $L \in \Sigma(n,e;K)$; aleshores L conté K_0 com a subextensió no ramificada maximal, de manera que $L \in \Sigma(e,e;K_0)$; per ser $p \nmid e$, tenim que $L = K_0(\alpha)$ amb $\alpha^e = u\pi$, i com que $K_0 = K(\zeta_{q^{f_1}})$, resulta que $L = K_0(\alpha) \subseteq K(\zeta_{q^{f_1}}, \alpha) \subseteq K(\zeta_{q^{f_1}}, u^{1/e}, \pi^{1/e})$. Degut al fet que les arrels e-èsimes de la unitat estan en K, l'extensió $K(\pi^{1/e})|K$ és cíclica, i per tant, abeliana. Per altra banda, l'extensió $K(\zeta_{q^{f_1}}, u^{1/e})|K$ és no ramificada, de manera que la composició $K(\zeta_{q^{f_1}}, u^{1/e}, \pi^{1/e})|K$ és una extensió abeliana. Per tant, l'extensió $L|K$ és abeliana, i obtenim les igualtats

$$\Sigma(n,e;K) = \Sigma(e,e;K_0) = \Sigma_{ab}(e,e;K_0) = \Sigma_{ab}(n,e;K).$$

Com que $p \nmid e$, és conegut que $s(n,e;K) = e$ (cf. §1) i, per tant, $a(n,e;K) = e$. Només resta demostrar la implicació (i) $\Rightarrow$ (ii).

Suposem que $\Sigma_{ab}(n,e;K) \neq \phi$ i sigui $L \in \Sigma_{ab}(n,e;K)$. Aleshores, $L \in \Sigma_{ab}(e,e;K_0)$ i, anàlogament al pas anterior, $L = K_0(\alpha)$. Com que $K(\alpha) \subseteq L$, l'extensió $K(\alpha)|K$ és abeliana i com que l'extensió $K_0(u^{1/e})|K$ és no ramificada, la composició $K(\alpha, u^{1/e})|K$ és abeliana. Però $K(\pi^{1/e}) \subseteq K(\alpha, u^{1/e})$, de manera que $K(\pi^{1/e})|K$ és abeliana. Per ser $\pi \in K$, això diu que K conté les arrels e-èsimes de la unitat, com volíem veure.■

§6.- El cas general sobre un cos p-àdic.

En aquest § es fa l'estudi de $\Sigma_{ab}(n,e;K)$ per a tot cos local K de característica zero. Mantinguem les notacions del §5 i siguin U_K el grup de les unitats de K, i $U_K^{(m)}$ el subgrup de les unitats congruents amb 1 mòdul p_K^m, per a tot enter $m \geqslant 1$.

Si K és de característica zero, aleshores K és una extensió finita de Q_p, i posarem $n_0 = [K:Q_p]$, $f_0 = f(K|Q_p) = [\tilde{K}:\mathbf{F}_p]$, $e_0 = e(K|Q_p)$ per designar el grau, el grau residual i l'índex de ramificació absoluts. Recordem que $q = \#\,\tilde{K} = p^{f_0}$.

Sigui π un uniformitzant de K i sigui F un A_K-mòdul de Lubin-Tate respecte de π (cf.[Ne 1: cap. III, §6, def. 6.5]). Per a tot enter $m \geqslant 1$, posem F[m] el grup dels punts de π^m-divisió, i $K_m = K(F[m])$. Siguin $K^{(\pi)} = \bigcup_{m \geqslant 1} K_m$, i $K^{nr}|K$ l'extensió no ramificada maximal de K. El cos $K^{(\pi)}$ depèn de l'elecció de l'uniformitzant π en K, encara que no del mòdul de Lubin-Tate, F, respecte de π ; malgrat tot, es verifica el següent

Teorema 6.1.- (i) Per a tot $m \geqslant 1$, $K_m|K$ és una extensió abeliana totalment ramificada de grau $q^{m-1}(q-1)$, amb grup de Galois $Gal(K_m|K) \simeq U_K/U_K^{(m)}$ ([Ne 1: cap III, §7, teor. 7.4]).

(ii) L'extensió abeliana maximal de K és la composició $K^{ab} = K^{nr}K^{(\pi)}$ ([Ne 1: cap. III, §7, cor. 7.7]).■

Siguin e,n, enters positius tals que e|n. Suposem que $\Sigma_{ab}(n,e;K) \neq \phi$ i sigui $L \in \Sigma_{ab}(n,e;K)$. Aleshores $L \subseteq K^{ab}$ i, per

tant, existeixen $m \geqslant 1$, $N \geqslant 1$, amb $p \nmid N$, i una arrel primitiva N-èsima de la unitat, ζ_N, tals que $L \subseteq K_m(\zeta_N)$. Però $e(K_m(\zeta_N)|K) = e(K_m|K) = q^{m-1}(q-1)$, de manera que $e = p^r.e'$ amb $e' | q-1$, $r \geqslant 0$. Així, s'obté el següent resultat, que generalitza el lema 2.2 del cas $K = \mathbb{Q}_p$:

Proposició 6.2.- Siguin n,e, enters positius. Posem $e = p^r e'$, amb $r \geqslant 0$ i $p \nmid e'$. Si $\Sigma_{ab}(n,e;K) \neq \phi$ aleshores $e | n$ i $e' | q-1$.■

Es tracta de veure que aquestes condicions també són suficients per a què $\Sigma_{ab}(n,e;K)$ sigui no buit. Anàlogament al cas $K = \mathbb{Q}_p$, si posem $n = p^s n'$, $e = p^r e'$, amb $p \nmid e', n'$, aleshores $a(n,e;K) = a(n',e';K)\, a(p^s,p^r;K)$, que és $e' a(p^s,p^r;K)$ si suposem que $e | n$ i que $e' | q-1$. De manera que el problema queda reduït a l'estudi de $\Sigma_{ab}(p^s,p^r;K)$ amb $0 \leqslant r \leqslant s$.

Suposem, doncs, que $0 \leqslant r \leqslant s$ i que $L \in \Sigma_{ab}(p^s,p^r;K)$. Siguin N, $m \geqslant 1$, amb $p \nmid N$, tals que $L \subseteq K_m(\zeta_N)$. Com que $[L:K] = p^s$, L està inclòs a la p-subextensió maximal de $K_m(\zeta_N)|K$, que és la composició de la p-subextensió maximal $K'_m|K$ de $K_m|K$ i la p-subextensió maximal de $K(\zeta_N)|K$. Per tant, podem suposar que N és de la forma $q^{p^u}-1$, amb $u \geqslant 0$, i que $L \subseteq K'_m(\zeta_N)$. El grup de Galois $Gal(K'_m|K)$ és isomorf al p-subgrup de Sylow de $Gal(K_m|K) \simeq U_K/U_K^{(m)}$, i el grup $Gal(K(\zeta_N)|K)$ és cíclic d'ordre p^u; com que les extensions $K'_m|K$ i $K(\zeta_N)|K$ són linealment disjuntes, resulta que $Gal(K'_m(\zeta_N)|K) \simeq Gal(K'_m(\zeta_N)|K'_m) \oplus$ $\oplus$ $Gal(K'_m(\zeta_N)|K(\zeta_N)) \simeq Gal(K(\zeta_N)|K) \oplus Gal(K'_m|K) \simeq (\mathbb{Z}/p^u\mathbb{Z}) \oplus$ $\oplus$ $(U_K^{(1)}/U_K^{(m)})$, ja que $U_K^{(1)}/U_K^{(m)}$ és (isomorf a) el p-subgrup de Sylow de $U_K/U_K^{(m)}$ (cf.[Ne 1: cap. III, §1, prop. 1.1]). Per

altra banda, el conjunt $\Sigma_{ab}(p^s,p^r;K)$ és finit, ja que K és de característica zero; per tant, podem elegir u, m, prou grans com per a què sigui $L \subseteq K'_m(\zeta_N)$ per a tot $L \in \Sigma_{ab}(p^s,p^r;K)$; en particular, podem suposar que $u \geqslant s$.

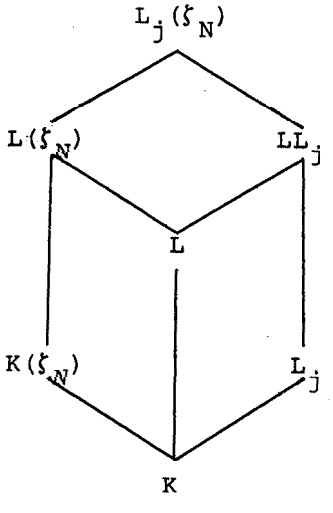
Un cop fixat m, K'_m té un número finit de subcossos de grau p^r sobre K. Siguin $L_1, L_2, \ldots, L_t$, aquests subcossos. Es verifica el següent

Lema 6.3.- Sigui $L \in \Sigma_{ab}(p^s,p^r;K)$. Aleshores existeix un únic $j \in \{1,2,\ldots,t\}$ tal que $L \subseteq L_j(\zeta_N)$.

Demostració.- Com que les extensions $K'_m|K$ i $K(\zeta_N)|K$ són linealment disjuntes, els cossos $L_j(\zeta_N)$, $1 \leqslant j \leqslant t$, són els únics subcossos de $K'_m(\zeta_N)$ de grau p^r sobre $K(\zeta_N)$. Ara bé, com que $K(\zeta_N)|K$ és no ramificada, també ho és $L(\zeta_N)|L$, de manera que $p^r = e(L|K) = e(L(\zeta_N)|K(\zeta_N))$; però l'extensió $K'_m(\zeta_N)|K(\zeta_N)$ és totalment ramificada i, per tant, $L(\zeta_N)|K(\zeta_N)$ és també totalment ramificada. Així, $L(\zeta_N)|K(\zeta_N)$ és una de les subextensions de $K'_m(\zeta_N)|K(\zeta_N)$ de grau p^r sobre $K(\zeta_N)$. Per tant, existeix $j \in \{1,2,\ldots,t\}$ i $L(\zeta_N) = L_j(\zeta_N)$. Per a la unicitat, si fos $L \subseteq L_j(\zeta_N) \cap L_{j'}(\zeta_N)$ amb $j \neq j'$, resultaria que $e(L|K) < p^r$, contradicció.■

Per a $1 \leqslant j \leqslant t$, posem $\Sigma_{ab}^{(j)}(p^s,p^r;K)$ el subconjunt de $\Sigma_{ab}(p^s,p^r;K)$ format pels cossos L tals que $L \subseteq L_j(\zeta_N)$. El lema anterior assegura que $\Sigma_{ab}(p^s,p^r;K)$ és la reunió disjunta dels conjunts $\Sigma_{ab}^{(j)}(p^s,p^r;K)$, $1 \leqslant j \leqslant t$; de manera que caracteritzar $\Sigma_{ab}(p^s,p^r;K)$ equival a caracteritzar els $\Sigma_{ab}^{(j)}(p^s,p^r;K)$, $1 \leqslant j \leqslant t$.

Considerem, doncs, un dels cossos L_j. Siguin $G_1 = \mathrm{Gal}(L_j(\zeta_N)|L_j) \simeq \mathrm{Gal}(K(\zeta_N)|K)$, $G_2 = \mathrm{Gal}(L_j(\zeta_N)|K(\zeta_N)) \simeq \mathrm{Gal}(L_j|K)$, i identifiquem G_1 i G_2 amb les seves imatges canòniques respectives en $G = G_1 \oplus G_2 = \mathrm{Gal}(L_j(\zeta_N)|K)$. Farem servir la notació additiva per a tots aquests grups. Si $L \subseteq L_j(\zeta_N)$ és un subcòs qualsevol i $X = \mathrm{Gal}(L_j(\zeta_N)|L)$, podem calcular l'índex de ramificació $e(L|K)$ de la manera següent:



L'extensió $L(\zeta_N)|L$ és no ramificada; per tant $e(L|K) = e(L(\zeta_N)|K(\zeta_N))$; com que $L_j(\zeta_N)|K(\zeta_N)$ és totalment ramificada, ho és $L(\zeta_N)|K(\zeta_N)$ i aleshores $e(L|K) = [L(\zeta_N):K(\zeta_N)]$. Això és l'índex de $\mathrm{Gal}(L_j(\zeta_N)|L(\zeta_N)) = G_2 \cap X$ en $\mathrm{Gal}(L_j(\zeta_N)|K(\zeta_N)) = G_2$; és a dir, $e(L|K) = (G_2 : G_2 \cap X)$. Podem enunciar, doncs, la següent:

Proposició 6.4.- Existeix una bijecció entre $\Sigma_{ab}^{(j)}(p^s, p^r; K)$ i el conjunt $B_j = \{X \subseteq G_1 \oplus G_2 : (G_1 \oplus G_2 : X) = p^s$ i $G_2 \cap X = \{0\}\}$.

Demostració.- La bijecció de Galois entre subcossos L de $L_j(\zeta_N)$ i subgrups de $G = G_1 \oplus G_2$, és tal que $[L:K] = (G_1 \oplus G_2 : X)$ i que $e(L|K) = (G_2 : G_2 \cap X)$, on $X = Gal(L_j(\zeta_N)|L)$. Però $e(L|K) = p^r$ si, i només si, $G_2 \cap X = \{0\}$, ja que G_2 és d'ordre p^r.■

Observem, també, que si $X \in B_j$, aleshores $X = Gal(L_j(\zeta_N)|L)$ és un grup cíclic; en efecte, l'extensió $L_j(\zeta_N)|L$ és no ramificada de cossos locals i, per tant, cíclica.

A més a més, podem suposar que u = s. En efecte, si $X \in B_j$, aleshores X és d'índex p^s en $G = G_1 \oplus G_2$, de manera que $p^s G \subseteq X$; però, per ser G_2 d'ordre p^r, amb $r \leqslant s$, és $p^s G_2 = \{0\}$, i aleshores $p^s G = p^s G_1$. Així, $p^s G_1 \subseteq X$, i com que $p^s G_1 = Gal(L_j(\zeta_N)|L_j(\zeta))$, on ζ és una arrel $(q^{p^s}-1)$-èsima primitiva de la unitat, resulta que $L \subseteq L_j(\zeta)$; això és dir que podem suposar que $\zeta_N = \zeta$, ò, el que és el mateix, que u = s.

Amb això es té que $\# B_j = p^r$, i no depèn de $s \geqslant r$, ni del p-grup abelià G_2, d'ordre p^r. En efecte: sigui $X \in B_j$ i sigui $(a,b) \in X$ un generador qualsevol de X amb $a \in G_1$, $b \in G_2$. Com que X és d'ordre p^r, a ò b és d'ordre p^r. Si a no fos d'ordre p^r, ho hauria de ser b i aleshores $0 \neq p^{r-1}(a,b) = (0, p^{r-1}b) \in X \cap G_2$. Així, tot generador de $X \in B_j$ és de la forma (a,b) amb $a \in G_1$ d'ordre p^r i b qualsevol element de G_2. Recíprocament, si (a,b) és un tal element en G, (a,b) genera un subgrup $X \in B_j$. Com que X té exactament $\varphi(p^r)$ generadors i G conté exactament $\varphi(p^r)p^r$ elements com els anteriors, el cardinal de B_j és el quocient, p^r.

Tot això es pot resumir en el següent:

Teorema 6.5.- El número d'extensions abelianes de K de grau p^s i amb índex de ramificació p^r, $0 \leqslant r \leqslant s$, és el producte de p^r pel número de subgrups d'índex p^r del grup U_k. En particular, no depèn de $s \geqslant r$.

Demostració.- El cardinal de $\Sigma_{ab}^{(j)}(p^s,p^r;K)$ és exactament p^r, com acabem de provar, i no depèn de $j \in \{1,2,\ldots,t\}$; de manera que $a(p^s,p^r;K) = t\,p^r$. Però t és el número de subcossos de K'_m de grau p^r sobre K; és a dir, el número de subcossos de K_m de grau p^r sobre K, ò equivalentment, el número de subgrups d'índex p^r de $Gal(K_m|K) \cong U_K/U_K^{(m)}$. Però hi ha bijecció entre el conjunt dels subgrups d'índex p^r de $U_K/U_K^{(m)}$ i el conjunt dels subgrups d'índex p^r de U_K que contenen $U_K^{(m)}$. Com que $U_K^{(m+h)} \subseteq U_K^{(m)}$ per a tot $h \geqslant 0$, aquest número no depèn de m suficientment gran, i com que U_K és el límit projectiu dels $U_K/U_K^{(m+h)}$, el resultat queda provat.■

Si ara sumem $a(n,e;K)$ per a tots els valors possibles de e obtenim el següent

Corol.lari 6.6.- Siguin n,e, enters positius. Aleshores:

(i) $$a(n,e;K) = \begin{cases} e\,t_r & \text{si } e = p^r e',\ e|n,\ e'|q-1, \\ 0 & \text{altrament.} \end{cases}$$

(ii) $$a(n;K) = \sigma_1((n,q-1)) \sum_{0 \leqslant r \leqslant v_p(n)} p^r t_r$$

on t_r és el número de subgrups d'índex p^r de U_K.■

Donarem tot seguit el valor de t_r. Per a això, donats enters no negatius N,M, posem

$$\begin{bmatrix} N+M \\ M \end{bmatrix}_p = \prod_{j=1}^{M} (p^{N+j}-1) \prod_{j=1}^{M} (p^j-1)^{-1}.$$

Es verifica que $\begin{bmatrix} N+M \\ M \end{bmatrix}_p$ és un enter positiu (cf. Apèndix, §5).

Proposició 6.7.- Sigui μ el màxim enter $\mu \geqslant 0$ tal que K conté les arrels p^μ -èsimes de la unitat. Posem $\underline{N} = (N_1,\ldots,N_r,0,\ldots)$ amb $N_i = n_0 + 1$ si $1 \leqslant i \leqslant \mu$ i $N_i = n_0$ si $\mu < i \leqslant r$. Aleshores:

$$t_r = \sum_{\underline{M}} p^{\gamma_{\underline{M}}} \prod_{i=1}^{r} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p$$

on $\gamma_{\underline{M}} = \sum_{i=1}^{r} M_{i+1}(N_i - M_i)$ i la suma s'estén a totes les successions $\underline{M} = (M_1,\ldots,M_r,\ldots)$ tals que $M_1 + \ldots + M_r = r$, $M_1 \geqslant M_2 \geqslant \ldots \geqslant M_r \geqslant 0$, i $M_i \leqslant N_i$ per a tot $i \geqslant 1$.

Demostració.- Si $X \subseteq U_K$ és un subgrup d'índex p^r, aleshores X conté el subgrup $U_K^{p^r}$ de les potències p^r-èsimes dels elements de U_K; de manera que hi ha bijecció entre el conjunt dels subgrups de U_K d'índex p^r i el conjunt dels subgrups de $U_K/U_K^{p^r}$ d'índex p^r. Ara bé, el teorema d'estructura de U_K (cf. [Ha 1: cap. 15, §5]) permet dir que $U_K/U_K^{p^r}$ és isomorf al grup abelià

$$G = \begin{cases} (\mathbb{Z}/p^r\mathbb{Z})^{n_0+1} & , \text{ si } 1 \leqslant r \leqslant \mu, \\ (\mathbb{Z}/p^\mu\mathbb{Z}) \times (\mathbb{Z}/p^r\mathbb{Z})^{n_0} & , \text{ si } \mu < r, \end{cases}$$

ja que $\mathbb{Z}_p/p^r\mathbb{Z}_p \simeq \mathbb{Z}/p^r\mathbb{Z}$. Però G és un p-grup abelià finit de tipus $\underline{N} = (N_1,\ldots,N_r,0,\ldots)$ (cf. Apèndix, §1, def.), on els N_i són n_0+1 per a $1 \leqslant i \leqslant \mu$, i n_0 per a $i > \mu$.

Com que G es abelià, el número de subgrups de G d'índex p^r és el mateix que el número de subgrups de $\hat{G} = \mathrm{Hom}(G,C^*) \simeq G$ d'ordre p^r, i en virtut del teorema 6.2 de l'apèndix, aquest número es pot escriure en la forma donada a l'enunciat.■

§7.- La funció generatriu de a(n;K).

Mantinguem les notacions dels §§ 5 i 6 i suposem que K és de característica zero. Anàlogament al cas $K = \mathbb{Q}_p$, podem definir les funcions generatrius de Dirichlet dels números d'extensions abelianes de K,

$$G(K;t) = \sum_{n \geqslant 1} a(n;K) n^{-t},$$

dels números d'extensions abelianes no ramificades de K,

$$G_{nr}(K;t) = \sum_{n \geqslant 1} a(n,1;K) n^{-t},$$

i dels números d'extensions abelianes totalment ramificades de K,

$$G_{tr}(K;t) = \sum_{n \geqslant 1} a(n,n;K) n^{-t}.$$

Igual que en el cas $K = \mathbb{Q}_p$, el coneixement de quina és la funció $G_{nr}(K;t)$ és immediat; com que, per a tot $n \geqslant 1$, és $a(n,1;K) = 1$, es verifica la següent

Proposició 7.1.- La sèrie $G_{nr}(K;t)$ és absolutament convergent en el semiplà $\mathrm{Re}(t) > 1$ i coincideix amb la funció zeta de Riemann.■

El següent pas consisteix a afitar a(n;K) a fi d'obtenir un semiplà de convergència per a les sèries G(K;t) i $G_{tr}(K;t)$. Es té el següent

Lema 7.2.- Sigui $n \geqslant 1$. Aleshores $a(n;K) \leqslant C_1 n^{C_2}$ on $C_2 = n_0 + 5$ i $C_1 = (2p)^{n_0+1} p^4 d_1 (q-1)$ són constants que només depenen del cos K.

Demostració.- Cal afitar $\sum_{0 \leqslant r \leqslant v_p(n)} p^r t_r$ i, per tant, cal afitar t_r. Per a tot tipus $\underline{M} \leqslant \underline{N}$ tal que $M_1 + \ldots + M_r = r$ i per a tot enter j, $1 \leqslant j \leqslant M_i - M_{i+1}$, es té que

$$\frac{p^{N_i - M_i + j} - 1}{p^j - 1} = p^{N_i - M_i} + \frac{p^{N_i - M_i} - 1}{p^j - 1} < 2p^{N_i - M_i} ;$$

de manera que

$$\prod_{i=1}^{r} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p \leqslant \prod_{i=1}^{r} \left(2^{M_i - M_{i+1}} \, p^{(M_i - M_{i+1})(N_i - M_i)}\right) =$$

$$= 2^{M_1} \, p^{\sum_{i=1}^{r} (M_i - M_{i+1})(N_i - M_i)} .$$

Així, cada un dels sumands de l'expressió de t_r està afitat per

$$2^{M_1} \, p^{\sum_{i=1}^{r} M_i (N_i - M_i)} .$$

Ara bé, $\sum_{i=1}^{r} M_i^2 \geqslant \sum_{i=1}^{r} M_i = r$, $\sum_{i=1}^{r} M_i N_i \leqslant N_1 \sum_{i=1}^{r} M_i = N_1 \, r$,

i $M_1 \leqslant N_1 \leqslant n_0 + 1$, i per tant, cada sumand de t_r està afitat per

$$2^{n_0 + 1} \, p^{n_0 r} .$$

Per altra banda, els índexs de sumació són particions de r que verifiquen certes condicions suplementàries, de manera que el número de sumands està afitat pel número total de particions de r. En virtut de [Ap 1: cap. 14, §7, teor. 14.5], el número de sumands de t_r està afitat per $\exp(\pi \sqrt{2/3} \sqrt{r}) \leqslant 2^{4\sqrt{r}} \leqslant p^{4\sqrt{r}}$ i, en conseqüència

$$t_r \leqslant 2^{n_0 + 1} \, p^{(n_0 + 4) r} .$$

Amb això, obtenim que

$$a(n;K) = \sigma_{1k}((n,q-1)) \sum_{0 \leqslant r \leqslant v_p(n)} p^r t_r \leqslant$$

$$\leqslant \sigma_1(q-1) \sum_{0 \leqslant r \leqslant v_p(n)} p^r t_r \leqslant$$

$$\leqslant \sigma_1(q-1)\, 2^{n_0+1} \sum_{0 \leqslant r \leqslant v_p(n)} p^{(n_0+5)r} \leqslant$$

$$\leqslant \sigma_1(q-1)\, 2^{n_0+1}\, p^{(n_0+5)(1+v_p(n))} \leqslant$$

$$\leqslant C_1\, n^{C_2},$$

ja que $p^{v_p(n)} \leqslant n$. ∎

Aquest resultat ens assegura que les sèries de Dirichlet $G_{tr}(K;t)$ i $G(K;t)$ són absolutament convergents en el semiplà $\mathrm{Re}(t) > n_0+6$, on defineixen funcions analítiques. Com que les funcions $a(n;K)$ i $a(n,n;K)$ són funcions multiplicatives de n, les funcions $G(K;t)$ i $G_{tr}(K;t)$ admeten els desenvolupaments en producte d'Euler:

$$G_{tr}(K;t) = \prod_{\ell} \sum_{r \geqslant 0} a(\ell^r,\ell^r;K)\, \ell^{-rt},$$

$$G(K;t) = \prod_{\ell} \sum_{r \geqslant 0} a(\ell^r;K)\, \ell^{-rt},$$

amb els productes estesos a tots els números primers ℓ, i convergents en el semiplà $\mathrm{Re}(t) > n_0+6$.

El resultat següent generalitza la proposició 4.7 i és bàsic a l'hora de calcular la funció $G(K;t)$.

Teorema 7.3.- La funció $a(n;K)$ és la convolució de Dirichlet de les funcions $a(n,1;K)$ i $a(n,n;K)$.

Demostració.- En virtut dels teoremes 5.2 i 6.5 i del fet que les funcions $a(n;K)$ i $a(n,n;K)$ són multiplicatives, resulta que sempre que n,e, siguin enters positius tals que $e|n$, es verifica la igualtat $a(n,e;K) = a(e,e;K)$. A més a més, com que, per a tot enter $m \geqslant 1$, és $a(m,1;K) = 1$, resulta que

$$a(n;K) = \sum_{e|n} a(n,e;K) =$$

$$= \sum_{e|n} a(e,e;K)\ a(n/e,1;K),$$

que es la convolució de Dirichlet de les funcions $a(n,n;K)$ i $a(n,1;K)$.■

Corol.lari 7.4.- En el semiplà $\mathrm{Re}(t) > n_0+6$ es té que

$$G(K;t) = G_{nr}(K;t)\ G_{tr}(K;t).■$$

Aquest corol.lari permet reduir el càlcul de $G(K;t)$ al càlcul de $G_{tr}(K;t)$. Per a tot primer ℓ, posem $B_\ell(K;t)$ el factor d'Euler de $G_{tr}(K;t)$ que correspon al primer ℓ. Es pot calcular fàcilment el producte

$$\prod_{\ell \neq p} B_\ell(K;t) .$$

En efecte, per a tot primer $\ell \neq p$, i per a tot enter $0 \leqslant r \leqslant v_\ell(q-1)$, resulta que $a(\ell^r,\ell^r;K) = \ell^r$, mentre que per a $r > v_\ell(q-1)$ és $a(\ell^r,\ell^r;K) = 0$; això diu que

$$B_\ell(K;t) = \sum_{0 \leqslant r \leqslant v_\ell(q-1)} \ell^{r(1-t)} =$$

$$= \sigma_{1-t}(\ell^{v_\ell(q-1)}).$$

En particular, si $\ell \nmid q-1$, $B_\ell(K;t) = 1$, i el producte $\prod_{\ell \neq p} B_\ell(K;t)$ és el producte finit

$$\prod_{\ell \mid q-1} B_\ell(K;t) = \prod_{\ell \mid q-1} \sigma_{1-t}(\ell^{v_\ell(q-1)}) =$$

$$= \sigma_{1-t}(q-1),$$

ja que la funció σ_{1-t} és multiplicativa. De manera que es té la següent:

Proposició 7.5.- Posem $B_p(K;t) = \sum_{r \geq 0} p^{r(1-t)} t_r$, on t_r és el número de subgrups d'índex p^r de U_K donat a la proposició 6.7. Aleshores, $B_p(K;t)$ és convergent en el semiplà $\mathrm{Re}(t) > n_0+6$ i es verifica, en aquest semiplà, que

$$G_{tr}(K;t) = \sigma_{1-t}(q-1)\ B_p(K;t),$$

$$G(K;t) = \zeta(t)\sigma_{1-t}(q-1)\ B_p(K;t),$$

on $\zeta(t)$ és la funció zeta de Riemann.■

Observem que la funció $\zeta(t)$ és el factor que mesura la quantitat d'extensions no ramificades. A més a més, el factor $\sigma_{1-t}(q-1)$ és el que mesura la quantitat d'extensions abelianes totalment i moderadament ramificades; no n'hi ha moltes, ja que $\sigma_{1-t}(q-1)$ defineix una funció analítica de tot el pla complex. Per últim, el factor $B_p(K;t)$, que és el difícil, és el que mesura la quantitat d'extensions totalment i salvatgement ramificades.

Es tracta, doncs, de calcular el factor d'Euler

$$B_p(K;t) = \sum_{r \geq 0} p^{r(1-t)} t_r \quad ,$$

on t_r és l'expressió donada a la proposició 6.7. Ara bé, observem que si $\underline{M} \leqslant \underline{N}$ és tal que $M_1+\ldots+M_r+\ldots = r$, aleshores per a tot $i > r$ és

$$\begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p = 1,$$

ja que $M_i - M_{i+1} = 0$; anàlogament, $\sum_{i \geqslant r} M_{i+1}(N_i - M_i) = 0$. Per tant, podem pensar que $\gamma_{\underline{M}} = \sum_{i \geqslant 1} M_{i+1}(N_i - M_i)$ i que el producte s'estén a tots els índexs $i \geqslant 1$. Per altra banda, el factor $p^{r(1-t)}$ de $B_p(K;t)$ pot entrar dins del sumatori de l'expressió de t_r en la forma $p^{(1-t)\sum_{i \geqslant 1} M_i}$; amb això es té que el factor d'Euler es pot escriure en la forma

$$B_p(K;t) = \sum_{\underline{M}} p^{\gamma_{\underline{M}}(t)} \prod_{i \geqslant 1} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p,$$

on $\gamma_{\underline{M}}(t) = \sum_{i \geqslant 1} M_{i+1}(N_i - M_i) + (1-t) \sum_{i \geqslant 1} M_i$, i la suma estesa a tots els $\underline{M} = (M_1, \ldots, M_r, 0, \ldots)$ tals que $M_1 \geqslant \ldots \geqslant M_r \geqslant \ldots \geqslant 0 \geqslant \ldots$, i que $M_i \leqslant N_i$ per a tot i, amb $N_i = n_0+1$ si $1 \leqslant i \leqslant \mu$ i $N_i = n_0$ si $i > \mu$.

Teorema 7.6.- El factor d'Euler $B_p(K;t)$ es prolonga a una funció meromorfa del pla complex amb pols simples en els punts $t = 1,2,\ldots,n_0$, si $\mu = 0$, i $t = 0,1,2,\ldots,n_0$, si $\mu \geqslant 1$.

Demostració.- Com que en el semiplà $\mathrm{Re}(t) > n_0+6$ la sèrie $B_p(K;t)$ és absolutament convergent, podem reordenar els termes de la suma com ens plagui. Comencem fent una partició del conjunt dels índex $\underline{M}$ en un número finit de classes.

Direm que $\underline{M}$ i $\underline{M}' = (M_1', \ldots, M_s', 0, \ldots)$ estan a la mateixa classe si, i només si, per a $1 \leqslant i \leqslant \mu$ es verifica la igualtat $M_i' = M_i$.

Com que els possibles valors de $(M_1, \ldots, M_\mu)$ són en número finit, ja que $M_i \leqslant N_i \leqslant n_0+1$, això fa que la sèrie $B_p(K;t)$ descompongui en la suma d'un número finit de sèries, només una si $\mu = 0$.

Fixem, i fixem-nos en, una d'aquestes classes. Els exponents

$$\sum_{i=1}^{\mu-1} M_{i+1}(N_i - M_i) = \sum_{i=1}^{\mu-1} M_{i+1}\,(n_0+1-M_i),$$

$$(1-t)\sum_{i=1}^{\mu} M_i \quad ,$$

i els factors

$$\prod_{i=1}^{\mu-1} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p = \prod_{i=1}^{\mu-1} \begin{bmatrix} n_0+1 - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p,$$

coincideixen per a tots els $\underline{M}$ de la mateixa classe, de manera que podem treure el factor comú

$$p^{\sum_{i=1}^{\mu-1} M_{i+1}(n_0+1-M_i) + (1-t)\sum_{i=1}^{\mu} M_i} \prod_{i=1}^{\mu-1} \begin{bmatrix} n_0+1-M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p,$$

factor que defineix una funció analítica de tot el pla complex i de la qual convé observar que no s'anul.la per a cap valor real de t. El que queda és la suma

$$(*) \qquad \sum_{\underline{M}'} p^{\gamma_{\underline{M}'}(t)} \prod_{i \geqslant \mu} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p$$

on $\gamma_{\underline{M}'}(t) = \sum_{i \geqslant \mu} M_{i+1}(N_i - M_i) + (1-t) \sum_{i \geqslant \mu+1} M_i$, i la suma estesa a tots els $\underline{M}' = (M_{\mu+1}, \ldots, M_r, 0, \ldots)$ tals que $M_{\mu+1} \geqslant \ldots \geqslant M_r$ i que $M_{\mu+1} \leqslant \min\{n_0, M_\mu\}$.

Dins de la classe, el valor $k = M_\mu$ és constant—ho són tots els $M_1, \ldots, M_\mu$—i pren un dels valors $0, 1, \ldots, n_0+1$, si $\mu \geqslant 1$, i $0, 1, \ldots, n_0$, si $\mu = 0$. Es tracta, ara, de calcular (*). Observem en primer lloc que si $k = 0$ no hi ha res a calcular, ja que (*) consta d'un únic sumand, que correspon a $\underline{M}' = (0, \ldots)$, i aquest sumand val 1. Per tant, podem suposar que $k \geqslant 1$.

Partim, de nou, els $\underline{M}'$ en un número finit de classes. Per a això, escrivim $\underline{M}'$ en la forma

$$\underline{M}' = (\underbrace{k, \ldots, k}_{h_k}, \ldots, \underbrace{2, \ldots, 2}_{h_2}, \underbrace{1, \ldots, 1}_{h_1}, 0, \ldots)$$

amb els $h_j \geqslant 0$, i $h_k = 0$ si $k = n_0+1$, i definim l'equivalència:

$\underline{M}' \sim \underline{M}''$ si, i només si, per a $1 \leqslant j \leqslant k$, $h_j(\underline{M}') = 0$ equival a $h_j(\underline{M}'') = 0$.

Això és dir que els salts de la successió $\underline{M}'$, és a dir, els valors $M_i - M_{i+1} > 0$, són iguals, encara que vénen en llocs diferents. Com que la suma dels salts és k, el número de classes en què es distribueixen els $\underline{M}'$ és finit.

Fixem, com abans, una d'aquestes classes, que ve caracteritzada pels valors de j, $1 \leqslant j \leqslant k$, tals que $h_j \neq 0$. Per a tots els $\underline{M}'$ d'aquesta classe, els factors no nuls

$$\prod_{i \geqslant \mu+1} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p = \prod_{i \geqslant \mu+1} \begin{bmatrix} n_0 - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p$$

són constants, ja que els factors amb $M_i - M_{i+1} > 0$ són iguals, encara que corresponguin a índexs diferents. Anàlogament, els factors

$$\begin{bmatrix} N_\mu & -M_{\mu+1} \\ M_\mu & -M_{\mu+1} \end{bmatrix}_p = \begin{bmatrix} n_0+1-M_{\mu+1} \\ k \quad -M_{\mu+1} \end{bmatrix}_p,$$

$$p^{M_{\mu+1}(N_\mu-M_\mu)} = p^{M_{\mu+1}\ (n_0+1-k)},$$

són constants dins la classe, i no nuls. Aquests factors comuns ho són de

$$(**) \qquad \sum_{\underline{M}'} p^{\sum_{i \geqslant \mu+1} M_{i+1}(n_0-M_i) + (1-t)\sum_{i \geqslant \mu+1} M_i},$$

la suma estesa a tots els $\underline{M}'$ de la mateixa classe. Calculem els exponents.

Observem que

$$\sum_{i \geqslant \mu+1} M_i = \sum_{j=1}^{k} j\, h_j,$$

i que

$$\sum_{i \geqslant \mu+1} M_i^2 = \sum_{j=1}^{k} j^2 h_j.$$

Per tant,

$$(1-t) \sum_{i \geqslant \mu+1} M_i = (1-t) \sum_{j=1}^{k} j\, h_j,$$

i també

$$\sum_{i \geqslant \mu+1} M_{i+1}(n_0-M_i) = n_0 \sum_{j=1}^{k} j h_j - n_0 M_{\mu+1} - \sum_{i \geqslant \mu+1} M_i(M_i-(M_i-M_{i+1})) =$$

$$= n_0 \sum_{j=1}^{k} j h_j - n_0 M_{\mu+1} - \sum_{j=1}^{k} j^2 h_j + \sum_{i \geqslant \mu+1} M_i(M_i-M_{i+1}).$$

Ara bé, $n_0 M_{\mu+1}$ i $\sum_{i \geqslant \mu+1} M_i(M_i-M_{i+1})$ són constants dins la mateixa classe: el terme $n_0 M_{\mu+1}$ és clar, i, per l'altre, només cal observar que els sumands no nuls són els que corresponen als salts

$M_i - M_{i+1} > 0, \ldots$. Així, (**) es pot escriure com el producte del factor comú

$$p^{\sum_{i \geqslant \mu+1} M_i(M_i - M_{i+1}) - n_0 M_{\mu+1}},$$

que és un número real i positiu, per la suma

$$\sum p^{\sum_{j=1}^{k} j\, h_j (1-t+n_0-j)}$$

estesa a totes les famílies $(h_1, \ldots, h_k)$ amb $h_j \geqslant 1$ per a tot j excepte per als valors de j que caracteritzen la classe, pels quals $h_j = 0$.

Però aquesta suma es pot escriure en la forma

$$\prod_j \sum_{h_j \geqslant 1} p^{j(1-t+n_0-j)h_j} = \prod_j p^{j(1-t+n_0-j)} \left(1 - p^{j(1-t+n_0-j)}\right)^{-1},$$

el producte estès a tots els j pels quals $h_j \neq 0$.

Aquest producte, finit i no buit ja que $k \geqslant 1$, defineix una funció meromorfa de tot el pla complex amb pols simples únicament en els punts $t = n_0 + 1 - j$ per als valors de j tals que $h_j \neq 0$.

Per a acabar, només cal observar que el factor $B_p(K;t)$ és una suma finita de funcions meromorfes amb pols simples en alguns dels punts $t = n_0 + 1 - j$, $1 \leqslant j \leqslant k$, i tots aquests punts són pol simple d'algun sumand. A més a més, $1 \leqslant k \leqslant n_0$ si $\mu = 0$ i $1 \leqslant k \leqslant n_0 + 1$ si $\mu \geqslant 1$. Això acaba la demostració.■

Com que la funció $\zeta(t)$ té un pol simple en $t = 1$, obtenim el

Corol.lari 7.7.- La funció $G_{tr}(K;t)$ es prolonga a una funció meromorfa de tot el pla complex amb pols simples en els punts $t = 1,2,\ldots,n_0$, si K no conté les arrels p-èsimes de la unitat, i en $t = 0,1,2,\ldots,n_0$, si K conté les arrels p-èsimes de la unitat.

El mateix passa a la funció G(K;t) excepte que el pol en t = 1 és un pol doble.■

CAPÍTOL II.

EXTENSIONS ABELIANES DE Q DE GRAU DONAT I RAMIFICACIÓ PREFIXADA.

§1. Introducció i notacions

En el capítol I hem vist que per a calcular el número d'extensions abelianes de grau donat d'un cos local és convenient comptar, en primer lloc, les extensions amb grau i índex de ramificació donats. En el cas de les extensions abelianes de Q passa quelcom semblant.

Sigui P un conjunt finit i no buit de números primers; posem $p_1, p_2, \ldots, p_k$, els primers senars de P, que considerarem ordenats en la forma $p_1 < p_2 < \ldots < p_k$, i posem $p_0 = 2$; d'aquesta manera, $P = \{p_1, p_2, \ldots, p_k\}$ si $2 \notin P$, i $P = \{p_0, p_1, \ldots, p_k\}$ si $2 \in P$.

Siguin $n, e_0, e_1, e_2, \ldots, e_k$, enters > 1 i posem $\underline{e} = (e_1, \ldots, e_k)$ si $2 \notin P$ i $\underline{e} = (e_0, e_1, \ldots, e_k)$ si $2 \in P$. Fixem una clausura algebraica $\bar{Q}$ de Q. A tot el que resta de memòria denotarem per $\Sigma_{ab}(n, \underline{e}; P)$ el conjunt de totes les extensions abelianes $K|Q$, $K \subseteq \bar{Q}$, de grau $[K:Q] = n$, amb índexs de ramificació $e_{p_i}(K|Q) = e_i$ en els primers $p_i \in P$, i no ramificades a cap primer finit $p \notin P$. Designarem per $a(n, \underline{e}; P)$ el cardinal de $\Sigma_{ab}(n, \underline{e}; P)$.

Com a conseqüència del teorema d'Hermite-Minkowski (cf. [Sam 1: cap. IV, §3]), el conjunt $\Sigma_{ab}(n, \underline{e}; P)$ és finit, possiblement buit. En aquest capítol es tracta el problema de donar (les) condicions necessàries per a què el conjunt $\Sigma_{ab}(n, \underline{e}; P)$

sigui no buit, i de calcular $a(n,\underline{e};P)$.

Comencem per fer una exposició dels resultats, per altra banda ben coneguts, del cas quadràtic i passem tot seguit a estudiar el cas en què el conjunt P està format per un únic primer. Igual que en el cas de $\mathbb{Q}_p$, el teorema de Kronecker-Weber (cf. [Ne 1: cap. III, §3, teor. 3.8]) permet resoldre immediatament aquest cas, ja que el grup de Galois de l'extensió abeliana maximal de $\mathbb{Q}$ no ramificada fora d'un primer és un grup molt senzill.

El pas següent consisteix a establir les condicions necessàries que ha de verificar la terna $(n,\underline{e};P)$ a fi que el conjunt $\Sigma_{ab}(n,\underline{e};P)$ sigui no buit. Per a això construïm unes extensions "universals" per a les parelles $(\underline{e};P)$ (cf. les definicions del §5). Aquestes extensions són tals que, entre totes, contenen tots els cossos $K \in \Sigma_{ab}(n,\underline{e};P)$, i que permeten obtenir un refinament del teorema de Kronecker-Weber (cf. les observacions 2 i 4 del §5). Aquestes extensions, que es poden interpretar en funció dels cossos de gèneres, permeten obtenir algunes conseqüències sobre el número de classes de les extensions abelianes de $\mathbb{Q}$ (cf. teor. 6.1).

Seguidament, i amb el fi de demostrar la suficiència de les condicions obtingudes, es fa la reducció del problema del càlcul de $a(n,\underline{e};P)$ a un problema combinatori de grups abelians finits. Aquesta reducció permet demostrar que les condicions obtingudes en el teorema 5.16 són suficients per a què el conjunt $\Sigma_{ab}(n,\underline{e};P)$ sigui no buit.

Per últim, i utilitzant els resultats de grups que s'inclouen a l'apèndix, es formulen els resultats concrets sobre els cardinals $a(n,\underline{e};P)$.

§2.- El cas n = 2.

En el cas de les extensions quadràtiques de $\mathbb{Q}$, els resultats dels problemes enunciats al §1 es poden establir en els termes següents (cf. [Sam 1: cap. V, §4]):

Proposició 2.1.- Sigui P un conjunt finit i no buit de números primers. Aleshores $\Sigma_{ab}(2,\underline{e};P) \neq \phi$ si, i només si, per a tot $p_i \in P$ és $e_i = 2$.■

Proposició 2.2.- Posem $d = \pm p_1 \cdot \ldots \cdot p_k$, el producte dels primers senars de P amb el signe elegit de manera que $d \equiv 1 \pmod 4$, i suposem que per a tot $p_i \in P$ és $e_i = 2$. Aleshores:

a) si $2 \notin P$, $\Sigma_{ab}(2,\underline{e};P) = \{\mathbb{Q}(\sqrt{d})\}$,

b) si $2 \in P$, $\Sigma_{ab}(2,\underline{e};P) = \{\mathbb{Q}(\sqrt{-d}), \mathbb{Q}(\sqrt{2d}), \mathbb{Q}(\sqrt{-2d})\}$.

En particular, obtenim el cardinal de $\Sigma_{ab}(2,\underline{e};P)$:

Corol.lari 2.3.- Amb les notacions anteriors:

$$a(2,\underline{e};P) = \begin{cases} 1 & \text{si } 2 \notin P \text{ i per a tot } p_i \in P \text{ és } e_i = 2, \\ 3 & \text{si } 2 \in P \text{ i per a tot } p_i \in P \text{ és } e_i = 2, \\ 0 & \text{si per a algun } p_i \in P \text{ és } e_i > 2. \blacksquare \end{cases}$$

Dels elements de $\Sigma_{ab}(2,\underline{e};P)$ es coneixen també generadors: $\sqrt{d}$, $\sqrt{-d}$, $\sqrt{2d}$, $\sqrt{-2d}$; els seus polinomis minimals X^2-d, X^2+d, X^2-2d, X^2+2d; i els anells d'enters, $\mathbb{Z}[\omega]$, per $\omega = \frac{1+\sqrt{d}}{2}$, $\sqrt{-d}$, $\sqrt{2d}$, $\sqrt{-2d}$, respectivament (cf.[Sam 1: cap. II, §5]).

§3.- El cas $P = \{p\}$, p primer senar.

En tot aquest § suposarem que $P = \{p\}$, p un número primer senar i, en conseqüència, el vector $\underline{e}$ introduït al §1 està format per un únic enter $e > 1$. El següent teorema caracteritza quan el conjunt $\Sigma_{ab}(n,e;\{p\})$ és no buit, i dóna una primera descripció dels seus elements.

Teorema 3.1.- Posem $e = p^r e'$ amb $p \nmid e'$. Es verifica que:

a) si $\Sigma_{ab}(n,e;\{p\}) \neq \phi$, aleshores $e = n$ i $p \equiv 1$ (mòd e'),

b) si $p \equiv 1$ (mòd e'), aleshores $\Sigma_{ab}(n,e;\{p\})$ està format per una única extensió de $\mathbb{Q}$, que és cíclica.

Observació 1.- La part a) d'aquest teorema, així com la demostració que es fa seguidament, també és vàlida en el cas $p = 2$ sense cap canvi. La condició $p \equiv 1$ (mòd e') es tradueix, en el cas $p = 2$, per $e' = 1$, ò equivalentment, per "e és una potència de 2". Aquest fet l'usarem al §4.

Demostració.- a) Si $K \in \Sigma_{ab}(n,e;\{p\})$, com que l'extensió $K|\mathbb{Q}$ és abeliana, el teorema de Kronecker-Weber ([Ne 1: cap. III, §3, teor. 3.8]) ens assegura que existeix una arrel primitiva m-èsima de la unitat, ζ, tal que $K \subseteq \mathbb{Q}(\zeta)$; a més a més, com que $K|\mathbb{Q}$ només ramifica en p, podem prendre m de la forma $m = p^t$, $t >> 0$. L'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}$ és totalment ramificada en p, de manera que $K|\mathbb{Q}$ també és totalment ramificada en p; això dó

na la igualtat e = n. A part, com que e divideix l'índex de ramificació $e_p(\mathbb{Q}(\zeta)|\mathbb{Q}) = p^{t-1}(p-1)$, resulta que $t \geqslant r + 1$ i que e' divideix p - 1.

b) Sigui ara $t \geqslant r + 1$ i sigui ζ una arrel primitiva p^t-èsima de la unitat; com que $p \neq 2$, l'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}$ és cíclica, i com que e divideix el grau d'aquesta extensió, resulta que $\mathbb{Q}(\zeta)$ conté un únic subcòs K tal que $[K:\mathbb{Q}] = e$. Aleshores, l'extensió $K|\mathbb{Q}$ és abeliana -encara més, és cíclica-, totalment ramificada en p i no ramificada fora de p, ja que ho és l'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}$; per tant $K \in \Sigma_{ab}(e,e;\{p\})$. Però K no depèn del particular $t \geqslant r + 1$ elegit, i com que tot cos de $\Sigma_{ab}(e,e;\{p\})$ està inclòs en $\mathbb{Q}(\zeta)$ per a algun $t >> 0$, es té la unicitat.■

Per a precisar millor quina és aquesta única extensió abeliana de $\mathbb{Q}$ en donarem un element primitiu. Recordem que n = e.

Posem $t \geqslant r + 1$ qualsevol i sigui ζ una arrel primitiva p^t-èsima de la unitat (cf. l'observació 4 més avall). El grup de Galois de l'extensió $\mathbb{Q}(\zeta)|\mathbb{Q}$ és cíclic, isomorf al grup multiplicatiu dels elements inversibles de $\mathbb{Z}/p^t\mathbb{Z}$; a més a més, si g és un generador de $(\mathbb{Z}/p^t\mathbb{Z})^*$, resulta que l'automorfisme σ de $\mathbb{Q}(\zeta)$ definit per $\sigma(\zeta) = \zeta^g$ és un generador de $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Com que $K \subseteq \mathbb{Q}(\zeta)$ i $[K:\mathbb{Q}] = n$, es té que $\mathrm{Gal}(\mathbb{Q}(\zeta)|K) = <\sigma^n>$, l'únic subgrup d'índex n de $<\sigma> = \mathrm{Gal}\,(\mathbb{Q}(\zeta)|\mathbb{Q})$.

Per comoditat d'escriptura, posarem $\zeta_i = \zeta^{g^i}$ per a tot enter, i. Es verifiquen sense cap dificultat les propietats:

(i) $\zeta_i = \zeta_j$ si, i només si, $i \equiv j \pmod{p^{t-1}(p-1)}$,

(ii) $\sigma^j(\zeta_i) = \zeta_{i+j}$,

per a tota parella d'enters i, j.

Definició.- Posem $d = p^{t-1}(p-1)/n$, i sigui, per a tot i, $0 \leqslant i \leqslant n-1$,

$$\eta_i = \sum_{j=0}^{d-1} \sigma^{jn}(\zeta_i) =$$

$$= \sum_{j=0}^{d-1} \zeta_{i+jn}.$$

Anomenarem a η_i el i-èsim n-període de ζ relatiu a l'arrel primitiva g (cf. l'observació 5 més avall).

En el cas $t = 1$, ζ és una arrel primitiva p-èsima de la unitat; Gauss calculà generadors de cada una de les subextensions de $Q(\zeta)$ (cf. l'observació 2 més avall). El teorema següent generalitza els resultats de Gauss per a totes les subextensions de $Q(\zeta)$ tals que $t = r + 1$, donant-ne un element primitiu. En efecte, amb les notacions anteriors:

Teorema 3.2.- Per a tot enter i, $0 \leqslant i \leqslant n-1$, si $t = r + 1$, aleshores $\Sigma_{ab}(n,n;\{p\}) = \{Q(\eta_i)\}$.

Per a demostrar aquest teorema farem servir el següent resultat.

Lema 3.3.- Siguin $x_0, x_1, \ldots, x_{d-1}$, elements algebraicament independents sobre un cos k de característica zero ò bé $> d$; siguin $\tau_1, \tau_2, \ldots, \tau_d$, els polinomis simètrics elementals en $x_0, x_1, \ldots, x_{d-1}$, i siguin

$\rho_k = x_0^k + x_1^k + \ldots + x_{d-1}^k$, $1 \leqslant k \leqslant d$, els polinomis de Newton dels $x_0, x_1, \ldots, x_{d-1}$. Aleshores $k(\tau_1, \ldots, \tau_d) = k(\rho_1, \ldots, \rho_d)$.

Demostració del lema 3.3.- En efecte, es verifiquen les identitats de Newton: $\rho_k - \tau_1\rho_{k-1} + \tau_2\rho_{k-2} - \ldots + (-1)^{k-1}\tau_{k-1}\rho_1 + (-1)^k k\tau_k = 0$, $1 \leqslant k \leqslant d$ (cf.[v d W 1: cap. V, §7, exercici 5.18]). Com que els ρ_k són polinomis simètrics en $x_0, x_1, \ldots, x_{d-1}$, resulta que $k(\rho_1, \ldots, \rho_d) \subseteq k(\tau_1, \ldots, \tau_d)$. Però, per a $1 \leqslant k \leqslant d$, és $(-1)^k k \neq 0$, de manera que τ_k s'expressa com una funció polinòmica de $\tau_1, \ldots, \tau_{k-1}, \rho_1, \ldots, \rho_k$; per inducció sobre k, i tenint en compte que $\tau_1 = \rho_1$, resulta que $\tau_k \in k(\rho_1, \ldots, \rho_k)$; en conseqüència, $\tau_1, \ldots, \tau_d \in k(\rho_1, \ldots, \rho_d)$, d'on l'altra inclusió.■

Demostració del teorema 3.2.- Sigui $f(X) = \mathrm{Irr}(\zeta, X, K) \in K[X]$ el polinomi minimal de ζ sobre K. Com que $K \subseteq \mathbb{Q}(\zeta)$, resulta que $\mathbb{Q}(\zeta) = K(\zeta)$ i, per tant, K s'obté de $\mathbb{Q}$ per l'adjunció dels coeficients de f(X); per ser $\mathrm{Gal}(\mathbb{Q}(\zeta)|K) = \langle\sigma^n\rangle$, és $f(X) = \prod_{j\neq 0}^{d-1} (X - \sigma^{jn}(\zeta))$, i els coeficients de f(X) són els polinomis simètrics elementals dels elements $x_j = \sigma^{jn}(\zeta) = \zeta_{nj}$, $0 \leqslant j \leqslant d-1$. En virtut del lema 3.3 es té que $K = \mathbb{Q}(\rho_1, \ldots, \rho_d)$, amb $\rho_k = \sum_{j=0}^{d-1} \zeta_{nj}^k$, $1 \leqslant k \leqslant d$. Però, per ser $t = r + 1$, és $d = p^r(p-1)/n \leqslant p-1 < p$, de manera que $1 \leqslant k < p$ i k és un element invers ible mòdul p^t; així, existeix $i = i(k)$ tal que $k = g^i$ i, aleshores, $\rho_k = \sum_{j=0}^{d-1} \zeta_{i+jn} = \eta_i$. Això demostra que $K \subseteq \mathbb{Q}(\eta_0, \eta_1, \ldots, \eta_{n-1})$. Per altra banda, per la definició dels η_i, és clar que $\sigma^n(\eta_i) = \eta_i$; és a dir, que η_i és fix per $\langle\sigma^n\rangle = \mathrm{Gal}(\mathbb{Q}(\zeta)|K)$ i, per tant, $\eta_i \in K$. D'aquí resulta que $K = \mathbb{Q}(\eta_0, \ldots, \eta_{n-1})$. Com que, per a i,j,qualssevol, $\sigma^j(\eta_i) = \eta_{i+j}$, els η_i són tots conjugats;

i per ser $\mathbb{Q}(\eta_i)$ de Galois sobre $\mathbb{Q}$, $\mathbb{Q}(\eta_i) = \mathbb{Q}(\eta_0,\ldots,\eta_{n-1}) = K$, com es volia demostrar.■

Observació 2.- En el cas moderadament ramificat, és a dir, si $p \nmid n$, ò equivalentment, si $r = 0$, la demostració d'aquest teorema 3.2 és més senzilla (cf.[v d W 1: cap. VIII, §4]): si $a_i \in \mathbb{Q}$ són tals que $\sum_{i=0}^{n-1} a_i\eta_i = 0$, aleshores els a_i, repetits d cops cada un, són els coeficients d'una combinació lineal de totes les arrels primitives p-èsimes de la unitat; és a dir, de $\zeta,\zeta^2,\ldots,\zeta^{p-1}$. Dividint per ζ , obtenim que ζ és arrel d'un polinomi a coeficients en $\mathbb{Q}$ i de grau $\leqslant p-2$; com que ζ és de grau p-1 sobre $\mathbb{Q}$, resulta que tots els a_i són zero, i els $\eta_0,\eta_1,\ldots,\eta_{n-1}$, són linealment independents; en conseqüència, els $\eta_0,\eta_1,\ldots,\eta_{n-1}$, són tots diferents. Com que són conjugats, es dedueix que $[\mathbb{Q}(\eta_0):\mathbb{Q}] \geqslant n$; però $[K:\mathbb{Q}] = n$ i $\eta_0 \in K$, ja que $\sigma^n(\eta_0) = \eta_0$, de manera que, per qüestió de graus, $K = \mathbb{Q}(\eta_0)$.

Observació 3.- En el cas salvatgement ramificat; és a dir, si $p|n$ ò equivalentment, si $r \geqslant 1$, la demostració de [v d W 1] no és possible, ja que $\sum_{i=0}^{n-1} \eta_i = 0$ i els η_i no són pas linealment independents; malgrat això, es dedueix de la demostració del teorema 3.2 que sí que són diferents. En efecte, $\sum_{i=0}^{n-1} \eta_i$ és la suma de totes les arrels primitives p^{r+1}-èsimes de la unitat; com que $r + 1 \geqslant 2$, afegint-hi la suma de totes les arrels p^r-èsimes de la unitat, primitives i no primitives, s'obté la suma de totes les arrels p^{r+1}-èsimes de la unitat. Però per a $t \geqslant 1$ la suma de les arrels p^t-èsimes de la unitat és zero i, per tant, $\sum_{i=0}^{n-1} \eta_i = 0$.

Observació 4.- Per a la validesa del teorema 3.2 cal prendre $t = r + 1$. Malgrat que per a tot $t \geqslant r + 1$ també és $K \subseteq Q(\zeta)$ i podem construir els n-períodes, no és cert que per a $t > r + 1$ sigui $K = Q(\eta_i)$ per a cap i. En efecte, es verifica la proposició 3.4 més avall, de manera que $K = Q(\eta_0)$ si, i només si, $t = r + 1$; és a dir si, i només si, t és la valoració p-àdica del conductor de l'extensió $K|Q$.

Observació 5.- Hem definit més amunt els n-períodes de ζ relatius a l'arrel primitiva g. El conjunt $\{\eta_0, \eta_1, \ldots, \eta_{n-1}\}$ no depèn, però, ni de l'elecció de g ni de l'elecció de l'arrel de la unitat ζ, de manera que es pot parlar dels n-períodes de l'extensió $Q(\zeta)|Q$. En efecte, com que n divideix l'ordre de $(\mathbb{Z}/p^t\mathbb{Z})^*$, resulta que els exponents g^{i+jn} de ζ en el n-període de η_i formen una classe lateral mòdul el subgrup $< g^n >$; com que $(\mathbb{Z}/p^t\mathbb{Z})^* = < g >$ és cíclic, el subgrup $< g^n >$ no depèn del generador g elegit i, en conseqüència, les classes laterals tampoc. Per altra banda, si canviem ζ per una altra arrel primitiva p^t-èsima de la unitat, ζ', resulta que $\zeta' = \zeta^{g^\alpha}$ per un cert α, i aleshores, per a tot i, $0 \leqslant i \leqslant n-1$, és $\eta'_i = \sum_{j=0}^{d-1} \zeta'_{i+jn} = \sum_{j=0}^{d-1} \zeta_{\alpha+i+jn} = \eta_{\alpha+i}$.

Observem, a més a més, que η_0 tampoc no depèn de g i que els η_i s'obtenen com els diferents η_0 associats a les diferents arrels primitives p^t-èsimes de la unitat, ζ.

Proposició 3.4.- Si $t > r + 1$, ζ és una arrel primitiva p^t-èsima de la unitat, i η_0 és un n-període qualsevol de ζ, aleshores $\eta_0 = 0$.

Demostració.- Com que n divideix $p^r(p-1)$, cada n-període és la suma d'exactament e' $p^r(p-1)$-períodes. Així, podem suposar que $n = p^r(p-1)$ i, per tant, que $e' = p-1$ i $d = p^{t-r-1}$. Considerem, doncs, $n = p^r(p-1)$, el n-període $\eta_0 = \zeta_n + \zeta_{2n} + \ldots + \zeta_{dn}$ i els exponents $g^n, g^{2n}, \ldots, g^{dn} = 1$, de ζ que apareixen en η_0. L'anell $\mathbb{Z}/p^t\mathbb{Z}$ és local, de manera que $1 + p^{r+1}(\mathbb{Z}/p^t\mathbb{Z})$ és un subgrup del grup de les unitats, $< g >$; com que l'ordre de $p^{r+1}(\mathbb{Z}/p^t\mathbb{Z})$ és $p^{t-r-1} = d$, que és l'ordre de $< g^n >$, resulta que $< g^n > = 1 + p^{r+1}(\mathbb{Z}/p^t\mathbb{Z})$. Aleshores, $\zeta^{-1}\eta_0$ és la suma de les potències $p^{r+1}, 2p^{r+1}, \ldots, d\,p^{r+1}$, de ζ ò, el que és el mateix, la suma de les potències $1, 2, \ldots, d$, de $\zeta^{p^{r+1}}$; però $\zeta^{p^{r+1}}$ és una arrel primitiva d-èsima de la unitat i, per tant, $\zeta^{-1}\eta_0 = 0$; en conseqüència, $\eta_0 = 0$.■

Observació 6.- La proposició 3.4 és equivalent al següent resultat que s'utilitza en [B-N 1; §2, lema 2.1]:

Lema 3.5.- Sigui $\psi : (\mathbb{Z}/p^{r+1}\mathbb{Z})^* \to C$, $r \geqslant 0$, una funció qualsevol, i sigui ζ una arrel primitiva p^t-èsima de la unitat, $t > r + 1$.
Aleshores, es verifica que

$$\sum_{u \in (\mathbb{Z}/p^t\mathbb{Z})^*} \psi(u)\zeta^u = 0.\blacksquare$$

En efecte, $\psi(u)$ és constant a cada classe lateral de $(\mathbb{Z}/p^t\mathbb{Z})^*$ mòdul p^{r+1}, de manera que només cal veure que $\Sigma\,\zeta^u = 0$ quan u recorre la dita classe lateral. Això és conseqüència de la proposició 3.4, ja que $\Sigma\,\zeta^u = \zeta^{u_0}\eta_0$ per a un cert u_0 que depèn de la classe lateral. Per altra banda, la proposició

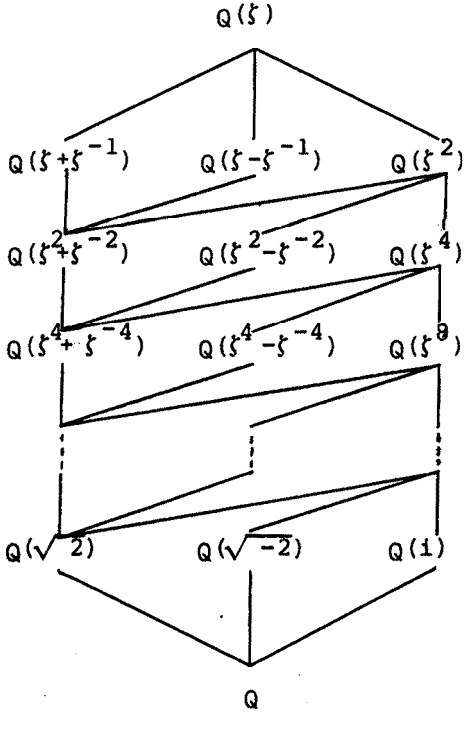
3.4 és el cas particular del lema 3.5 donat per la funció

$$\psi(u) = \begin{cases} 1 & , \text{ si } u \equiv 1 \pmod{p^{r+1}}, \\ 0 & , \text{ altrament.} \end{cases}$$

§4.- El cas $P = \{2\}$.

Suposem ara que $P = \{2\}$ i sigui e un enter > 1. En el teorema 3.1. a), hem vist que una condició necessària per a què $\Sigma_{ab}(n,e;\{2\}) \neq \phi$ és que e = n i que e sigui una potència de 2. Aquesta condició és també suficient. Per a demostrar-ho, calculem en primer lloc el reticle dels subcossos de $Q(\zeta)$ per a tota arrel primitiva 2^t-èsima de la unitat, ζ.

Proposició 4.1.- Sigui $t \geq 2$ i sigui ζ una arrel primitiva 2^t-èsima de la unitat. Aleshores, el reticle dels subcossos de $Q(\zeta)$ és el següent:



Demostració.- L'extensió $Q(\zeta)|Q$ és abeliana amb grup de Galois isomorf al grup $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{t-2}\mathbb{Z})$, i en el lema 3.2 del capítol I s'ha calculat el reticle dels subgrups d'aquest grup. Per tant, només cal veure quins cossos ocupen els vèrtexs del reticle. Com que ζ^2 és una arrel primitiva 2^{t-1}-èsima de la unitat, només cal comprovar que els cossos $Q(\zeta + \zeta^{-1})$, $Q(\zeta - \zeta^{-1})$ i $Q(\zeta^2 + \zeta^{-2})$ ocupen els vèrtexs corresponents, i un argument inductiu acaba la demostració. Com que $Q(\zeta + \zeta^{-1})|Q$ és la subextensió real maximal de $Q(\zeta)|Q$, queda clara la posició dels cossos $Q(\zeta + \zeta^{-1})$ i $Q(\zeta^2 + \zeta^{-2})$. Per tant, només cal veure que el tercer cos K tal que $[Q(\zeta):K] = 2$ és $K = Q(\zeta - \zeta^{-1})$. Però es té que ζ és arrel de $(X-\zeta)(X+\zeta^{-1}) = X^2 - (\zeta - \zeta^{-1})X - 1$, i que $(\zeta - \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} - 2 \in Q(\zeta^2 + \zeta^{-2})$. Per tant $[Q(\zeta) : Q(\zeta - \zeta^{-1})] = [Q(\zeta - \zeta^{-1}) : Q(\zeta^2 + \zeta^{-2})] = 2$. Com que $\zeta - \zeta^{-1} \notin \mathbb{R}$, és clar que $Q(\zeta - \zeta^{-1}) \neq Q(\zeta + \zeta^{-1})$. Només cal veure que $Q(\zeta - \zeta^{-1}) \neq Q(\zeta^2)$. Però $(\zeta - \zeta^{-1})(\zeta + \zeta^{-1}) = \zeta^2 - \zeta^{-2} \in Q(\zeta^2)$, de manera que $\zeta - \zeta^{-1} \notin Q(\zeta^2)$, ja que $\zeta + \zeta^{-1}$ no hi pertany.■

Ara ja estem en condicions de demostrar la suficiència de les condicions del teorema 3.1. a) en el cas $P = \{2\}$. Es té, efectivament, el següent

Teorema 4.2.- Siguin $e = n = 2^r$, $t = r + 2$, i ζ una arrel primitiva 2^t-èsima de la unitat. Aleshores, $\Sigma_{ab}(e,e;\{2\}) = \{Q(\zeta^2), Q(\zeta+\zeta^{-1}), Q(\zeta-\zeta^{-1})\}$. En particular, si $r \geq 1$, és $a(2^r,2^r;\{2\}) = 3$.

Demostració.- En virtut del teorema de Kronecker-Weber, si $K \in \Sigma_{ab}(e,e;\{2\})$, existeix $t >> 0$ i existeix una arrel primitiva 2^t-èsima de la unitat, ζ, tals que $K \subseteq \mathbb{Q}(\zeta)$; a més a més, podem prendre $t = r + 2$, per qüestió del grau (cf. la proposició anterior). Com que $\mathbb{Q}(\zeta)|\mathbb{Q}$ és totalment ramificada en 2 i no ramificada fora de $\{2\}$, també ho són totes les seves subextensions. Així, $\Sigma_{ab}(e,e;\{2\})$ està format per tots els subcossos $K \subseteq \mathbb{Q}(\zeta)$ de grau $[K:\mathbb{Q}] = 2^r$; és a dir, pels cossos $\mathbb{Q}(\zeta^2)$, $\mathbb{Q}(\zeta+\zeta^{-1})$, $\mathbb{Q}(\zeta-\zeta^{-1})$.■

Igual que en el cas n = 2, podem donar també els polinomis minimals per als elements primitius ζ^2, $\zeta+\zeta^{-1}$, $\zeta-\zeta^{-1}$. En efecte, es verifica que

Corol.lari 4.3.- Sigui $f(X) = X^2 - 2 \in \mathbb{Q}[X]$, i posem $f_j(X) = (\overset{j)}{f\circ\ldots\circ f})(X)$, per a tot natural j, la substitució consecutiva de X per f(X). Aleshores, es té que:

a) $\mathrm{Irr}(\zeta^2,X;\mathbb{Q}) = X^{2^r}+1$,

b) $\mathrm{Irr}(\zeta+\zeta^{-1},X,\mathbb{Q}) = f_r(X)$,

c) $\mathrm{Irr}(\zeta-\zeta^{-1},X,\mathbb{Q}) = f_{r-1}(X^2+2)$,

on $f_0(X) = X$. Els polinomis $f_r(X)$, i $f_{r-1}(X^2+2)$ són mònics, de grau 2^r, a coeficients enters i d'Eisenstein respecte del primer 2.

Demostració.- a) és clar, ja que ζ^2 és una arrel primitiva 2^{r+1}-èsima de la unitat i $X^{2^r}+1$ és el polinomi ciclotòmic 2^{r+1}-èsim. Per altra banda, i per inducció sobre r, $f_r(X)$ i

$f_{r-1}(X^2+2)$ són polinomis mònics i d'Eisenstein respecte del primer 2. Només cal veure que $f_r(\zeta+\zeta^{-1}) = f_{r-1}((\zeta-\zeta^{-1})^2+2) = 0$. Però $(\zeta-\zeta^{-1})^2+2 = \zeta^2+\zeta^{-2} = (\zeta+\zeta^{-1})^2-2$ i, per inducció sobre r, $f_r(\zeta+\zeta^{-1}) = 0$. Per tant, $f_r(X)$ anul.la $\zeta+\zeta^{-1}$ i $f_{r-1}(X^2+2)$ anul.la $\zeta-\zeta^{-1}$; com que tenen el grau adequat, fet.■

§5.- Condicions necessàries per a què $\Sigma_{ab}(n,\underline{e};P) \neq \phi$ en el cas general.

En aquest § es tracta el problema d'establir les condicions necessàries per a què, en el cas general, el conjunt $\Sigma_{ab}(n,\underline{e};P)$ sigui no buit. El següent resultat en dóna les primeres.

Proposició 5.1.- Si $\Sigma_{ab}(n,\underline{e};P) \neq \phi$, aleshores existeixen naturals $t_i \geqslant 1$ tals que per a $m = \prod_{p_i \in P} p_i^{t_i}$ es verifiquen les condicions:

a') $n \mid \varphi(m)$,

b) si $\mu = \text{m.c.m.}\ \{e_i : p_i \in P\}$, aleshores $\mu \mid n$,

c) per a tot $p_i \in P$, si posem $e_i = p_i^{r_i} e_i'$ amb $p_i \nmid e_i'$, aleshores $p_i \equiv 1 \pmod{e_i'}$.

Demostració.- Sigui $K \in \Sigma_{ab}(n,\underline{e};P)$; com que l'extensió $K|Q$ és abeliana, existeix una arrel primitiva m-èsima de la unitat, ζ , tal que $K \subseteq Q(\zeta)$; a més a més, com que $K|Q$ no ramifica fora de P , podem prendre m de la forma $m = \prod_{p_i \in P} p_i^{t_i}$, amb $t_i >> 0$. L'extensió $Q(\zeta)|Q$ és de grau $\varphi(m)$ i, per tant, el grau n de l'extensió $K|Q$ divideix $\varphi(m)$. Per altra banda, per a tot $p_i \in P$ és $e_{p_i}(Q(\zeta)|Q) = p_i^{t_i-1}(p_i-1)$, de manera que e_i divideix $p_i^{t_i-1}(p_i-1)$; en conseqüència, si $e_i = p_i^{r_i} e_i'$ amb $p_i \nmid e_i'$, ha de ser $t_i \geqslant r_i + 1$ i $e_i' \mid p_i-1$. Per últim, la condició b) és vàlida per a qualsevol extensió de Galois, ja que, per a tot primer p, l'índex de ramificació $e_p(K|Q)$ divideix el grau $[K:Q]$.∎

Aquestes condicions no són, però, suficients per a què el conjunt $\Sigma_{ab}(n,\underline{e};P)$ sigui no buit. Per exemple, en el cas $P = \{p\}$, un únic primer, es té que $\mu = e$; però en virtut del teorema 3.1, si $\Sigma_{ab}(n,e;\{p\})$ és no buit, aleshores $e = n$; és a dir, $\mu = n$. En conseqüència, cal buscar més condicions a fi de caracteritzar quan $\Sigma_{ab}(n,\underline{e};P) \neq \phi$.

A partir d'ara, i per simplicitat, convindrà distingir dos casos: $2 \notin P$ i $2 \in P$. Comencem pel cas $2 \notin P$ i suposem que es verifiquen les condicions a', b, c, de la proposició 5.1.

Per a tot $p_i \in P$, i com que p_i és senar, existeix una única extensió abeliana de Q de grau e_i, totalment ramificada en p_i i no ramificada fora de $\{p_i\}$ (cf. teorema 3.1. b). Sigui θ_i un element primitiu d'aquesta extensió, i posem $L = Q(\theta_1,\ldots,\theta_k)$, la composició de les extensions $Q(\theta_i)|Q$, per a $p_i \in P$. Convindrà considerar també els cossos $Q(\hat{\theta}_i) = Q(\theta_1,\ldots,\theta_{i-1},\theta_{i+1},\ldots,\theta_k)$ $1 \leqslant i \leqslant k$.

Lema 5.2.- L'extensió $L|Q$ és abeliana, de grau $\prod_{p_i \in P} e_i$, no ramificada fora de P , i amb índexs de ramificació $e_{p_i}(L|Q) = e_i$, per a tot $p_i \in P$.

Demostració.- Com que les extensions $Q(\theta_i)|Q$, $1 \leqslant i \leqslant k$, són abelianes i no ramificades fora de P , la composició $L|Q$ és abeliana i no ramificada fora de P . Per altra banda, les extensions $Q(\theta_i)|Q$, $1 \leqslant i \leqslant k$, són linealment disjuntes, ja que $Q(\theta_i)|Q$ és totalment ramificada en p_i i $Q(\hat{\theta}_i)|Q$ és no ramificada en p_i. Per tant $[L:Q] = \prod_{p_i \in P} e_i$. Calculem els ín-

dexs de ramificació $e_{p_i}(L|Q)$. Com que $Q(\tilde{\theta}_i)|Q$ és no ramificada en p_i, $e(L|Q) = e(L|Q(\tilde{\theta}_i)) = e(Q(\theta_i)|Q) = e_i$, com volíem demostrar.■

Per a tot $p_i \in P$, sigui ζ_i una arrel primitiva $p_i^{t_i}$-èsima de la unitat; aleshores, el producte $\zeta = \zeta_1 \cdot \ldots \cdot \zeta_k$ és una arrel primitiva m-èsima de la unitat. Posem $G_i = Gal(Q(\zeta_i)|Q)$, $1 \leqslant i \leqslant k$, i sigui $G = Gal(Q(\zeta)|Q)$. Com que els p_i són senars, les extensions $Q(\zeta_i)|Q$ són cícliques i podem escriure $G_i = <\sigma_i>$, amb σ_i un automorfisme de $Q(\zeta)$ d'ordre $p_i^{t_i-1}(p_i-1)$; a més a més, podem elegir els σ_i de manera que $G = <\sigma_1> \oplus \ldots \oplus <\sigma_k>$, ja que les extensions $Q(\zeta_i)|Q$ són linealment disjuntes. Com que, per a $1 \leqslant i \leqslant k$, és $Q(\theta_i) \subseteq Q(\zeta_i)$ (cf. teorema 3.1) i $Q(\zeta_i) \subseteq Q(\zeta)$, resulta que $L \subseteq Q(\zeta)$. Amb aquestes notacions es verifica el següent exercici:

Lema 5.3.- $Gal(Q(\zeta)|L) = <\sigma_1^{e_1}> \oplus \ldots \oplus <\sigma_k^{e_k}>$.

Demostració.- Com que $L = Q(\theta_1, \ldots, \theta_k)$, és $Gal(Q(\zeta)|L) = \bigcap_{i=1}^{k} Gal(Q(\zeta)|Q(\theta_i))$; però $Q(\theta_i)|Q$ és l'única subextensió de $Q(\zeta_i)|Q$ de grau e_i, de manera que $Gal(Q(\zeta_i)|Q(\theta_i)) = <\sigma_i^{e_i}>$, l'únic subgrup de G_i d'índex e_i. Per tant, $Gal(Q(\zeta)|Q(\theta_i)) = <\sigma_1> \oplus \ldots \oplus <\sigma_{i-1}> \oplus <\sigma_i^{e_i}> \oplus <\sigma_{i+1}> \oplus \ldots \oplus <\sigma_k>$ i, en conseqüència, $Gal(Q(\zeta)|L) = <\sigma_1^{e_1}> \oplus \ldots \oplus <\sigma_k^{e_k}>$.■

Aquest estudi dels grups de Galois ens permet calcular L en la forma següent:

Lema 5.4.- $L = \bigcap_{i=1}^{k} Q(\theta_i, \zeta\zeta_i^{-1})$.

Demostració.- La inclusió $L \subseteq \bigcap_{i=1}^{k} Q(\theta_i, \zeta\zeta_i^{-1})$ és clara. Per altra banda, (exercici), $Gal(Q(\zeta) | \bigcap_{i=1}^{k} Q(\theta_i, \zeta\zeta_i^{-1})) \supseteq$ $\supseteq (\bigsqcup_{i=1}^{k} Gal(Q(\zeta) | Q(\theta_i, \zeta\zeta_i^{-1}))) = Gal(Q(\zeta) | L)$, de manera que s'obté l'altra inclusió.■

La condició necessària que cal afegir a les de la proposició 5.1 per a què $\Sigma_{ab}(n,\underline{e};P)$ sigui no buit la deduirem del següent teorema (cf. corol.lari 5.8):

Teorema 5.5.- Suposem que $2 \notin P$ i que la terna $(n,\underline{e};P)$ verifica les condicions a'), b), i c), de la proposició 5.1. Sigui L el cos construït més amunt. Aleshores, per a tot cos $K \in \Sigma_{ab}(n,\underline{e};P)$ es té que $K \subseteq L$.

Observació 1.- El cos L no depèn ni de n, ni de l'elecció dels $t_i >> 0$. En efecte, per a tot primer $p_i \in P$ existeix el cos $Q(\theta_i)$ i està unívocament determinat per e_i, ja que $p_i \equiv 1$ (mòd e_i'). Per tant, el cos $L = Q(\theta_1,\ldots,\theta_k)$ està unívocament determinat per la parella $(\underline{e};P)$, en el cas en què $2 \notin P$ i que els e_i verifiquin la condició $e_i' | p_i - 1$, per a tot $p_i \in P$. De manera que podem donar la següent

Definició.- Anomenarem a $L|Q$ l'extensió $(\underline{e};P)$-universal.

Observació 2.- Un estudi acurat del conductor de les extensions $K|Q$ per a $K \in \Sigma_{ab}(n,\underline{e};P)$, juntament amb el teorema de Kronecker-Weber, donaria les inclusions $K \subseteq Q(\zeta)$ per a una arrel primitiva m-èsima de la unitat, ζ, amb $m = \prod_{p_i \in P} p_i^{r_i+1}$, i no per a valors més petits de m. Es té, però, que $L|Q$ és una subextensió, en general estricta, de $Q(\zeta)|Q$, de manera que el teorema 5.5 és un refinament del teorema de Kronecker-Weber en el cas $2 \notin P$. (Per al cas $2 \in P$, cf. el teorema 5.12 més avall).

Demostració del teorema 5.5.- En virtut del lema 5.4, només cal veure que, per a $1 \leqslant i \leqslant k$, és $K \subseteq Q(\theta_i, \zeta\zeta_i^{-1})$; però, com que $K \subseteq K(\zeta\zeta_i^{-1})$, és suficient provar que $K(\zeta\zeta_i^{-1}) \subseteq Q(\theta_i, \zeta\zeta_i^{-1})$. De fet, el següent resultat dóna la igualtat i acaba la demostració.■

Proposició 5.6.- Per a $1 \leqslant i \leqslant k$, i per a tot $K \in \Sigma_{ab}(n,\underline{e};P)$, es té que $K(\zeta\zeta_i^{-1}) = Q(\theta_i, \zeta\zeta_i^{-1})$.

Demostració.- Per a qualsevol elecció dels $t_i \geqslant r_i + 1$ es té que $Q(\zeta\zeta_i^{-1}) \subseteq Q(\theta_i,\zeta\zeta_i^{-1}) \subseteq Q(\zeta)$, mentre que per a $t_i >> 0$ es té que $Q(\zeta\zeta_i^{-1}) \subseteq K(\zeta\zeta_i^{-1}) \subseteq Q(\zeta)$; però l'extensió $Q(\zeta)|Q(\zeta\zeta_i^{-1})$ és cíclica, de manera que només cal veure que $Q(\theta_i,\zeta\zeta_i^{-1})$ i $K(\zeta\zeta_i^{-1})$ tenen el mateix grau relatiu sobre $Q(\zeta\zeta_i^{-1})$. Com que $Q(\zeta)|Q(\zeta\zeta_i^{-1})$ és totalment ramificada en p_i, també ho són les subextensions $Q(\theta_i,\zeta\zeta_i^{-1})|Q(\zeta\zeta_i^{-1})$ i $K(\zeta\zeta_i^{-1})|Q(\zeta\zeta_i^{-1})$ i, per tant, només cal veure que els índexs de ramificació en p_i de les dues extensions coincideixen. Però $Q(\zeta\zeta_i^{-1})|Q$ és no ramificada en p_i, de manera que $e_{p_i}(Q(\theta_i,\zeta\zeta_i^{-1})|Q(\zeta\zeta_i^{-1})) = e_{p_i}(Q(\theta_i)|Q) = e_i$, i també $e_{p_i}(K(\zeta\zeta_i^{-1})|Q(\zeta\zeta_i^{-1})) = e_{p_i}(K|Q) = e_i$.■

Corol.lari 5.7.- Per a tot cos $K \in \Sigma_{ab}(n,\underline{e};P)$, l'extensió $L|K$ és no ramificada a tot primer finit de K.

Demostració.- L'extensió $L|Q$ és no ramificada fora de P ; per tant, $L|K$ és no ramificada a tot primer finit de K que divideixi un número primer $p \notin P$. Per altra banda, per a tot $p_i \in P$ és $e_{p_i}(L|Q) = e_{p_i}(K|Q) = e_i$, de manera que $L|K$ és no ramificada a tot primer finit de K que divideixi un primer $p_i \in P$.■

Corol.lari 5.8.- Si $\Sigma_{ab}(n,\underline{e};P) \neq \phi$ aleshores n divideix $\prod_{p_i \in P} e_i$.

Demostració.- Si $K \in \Sigma_{ab}(n,\underline{e};P)$, aleshores $K \subseteq L$, de manera que el grau $n = [K:Q]$ divideix $[L:Q] = \prod_{p_i \in P} e_i$.■

Passem ara al cas $2 \in P$ i suposem que es verifiquen les condicions a'), b), c') del teorema 5.1. Estenguem les notacions del cas $2 \notin P$ al cas $2 \in P$: per a $1 \leqslant i \leqslant k$, sigui $Q(\theta_i)|Q$ l'única extensió abeliana de grau e_i, no ramificada fora de $\{p_i\}$ i totalment ramificada en p_i, com abans; per altra banda, siguin $k_1|Q$, $k_2|Q$, $k_3|Q$, les tres extensions abelianes de Q de grau $e_0 = 2^{r_0}$, no ramificades fora de $\{2\}$, i totalment ramificades en 2; posem $L = Q(\theta_1,\ldots,\theta_k)$, i siguin $L_j = k_j(\theta_1,\ldots,\theta_k) = k_jL$, $1 \leqslant j \leqslant 3$.

Observació 3.- L'extensió $L|Q$ és la mateixa que en el cas $2 \notin P$. Per altra banda, les extensions $k_j|Q$, $1 \leqslant j \leqslant 3$, només depenen de $e_0 = 2^{r_0}$; per tant, les extensions $L_j|Q$, $1 \leqslant j \leqslant 3$, només depenen de la parella $(\underline{e};P)$, i existeixen sempre que es

verifiquin les condicions $e_i' \mid p_i - 1$ per a tot primer $p_i \in P$ (cf. l'observació 1 més amunt). Anàlogament al cas $2 \notin P$ podem donar la següent

Definició.- Anomenarem a les $L_j|Q$, $1 \leqslant j \leqslant 3$, les extensions $(\underline{e};P)$-universals.

Lema 5.9.- Per a $1 \leqslant j \leqslant 3$, les extensions $L_j|Q$ són abelianes, no ramificades fora de P , de grau $\prod_{p_i \in P} e_i$, i amb índexs de ramificació $e_{p_i}(L_j|Q) = e_i$, per a tot $p_i \in P$.

Demostració.- És completament anàloga a la del lema 5.2.■

Sigui ara, per a $0 \leqslant i \leqslant k$, ζ_i una arrel primitiva $p_i^{t_i}$-èsima de la unitat, on prenem $t_i \geqslant r_i + 1$ si $1 \leqslant i \leqslant k$, i $t_0 \geqslant r_0 + 2$; posem $\zeta = \zeta_1 \cdot \ldots \cdot \zeta_k$, i $\tilde{\zeta} = \zeta\zeta_0$. Siguin $G_i = \mathrm{Gal}(Q(\zeta_i)|\, Q)$, $0 \leqslant i \leqslant k$. Es té que:

(i) per a $1 \leqslant i \leqslant k$, $G_i = \langle \sigma_i \rangle$,

(ii) per a $i = 0$, $G_0 = \langle \sigma \rangle \oplus \langle \sigma_0 \rangle$,

amb σ_i un automorfisme de $Q(\tilde{\zeta})$ d'ordre $p_i^{t_i - 1}(p_i - 1)$ i σ un automorfisme de $Q(\tilde{\zeta})$ d'ordre 2, que podem elegir, com el cas $2 \notin P$, de tal manera que $\mathrm{Gal}(Q(\tilde{\zeta})|\, Q) = \langle\sigma\rangle \oplus \langle\sigma_0\rangle \oplus \langle\sigma_1\rangle \oplus \ldots \oplus \langle\sigma_k\rangle = G_0 \oplus G_1 \oplus \ldots \oplus G_k$.

Posem, també, per a $1 \leqslant j \leqslant 3$, $H_j = \mathrm{Gal}(Q(\zeta_0)|\, k_j)$; els H_j són els tres subgrups de G_0 d'ordre $2^{t_0 - r_0 - 1}$. Les demostracions dels dos lemes següents són anàlogues a les dels lemes 5.3 i 5.4, respectivament, i no les repetirem.

Lema 5.10.- Per a $1 \leqslant j \leqslant 3$, $\mathrm{Gal}(\mathbb{Q}(\tilde{\zeta})|\ L_j) =$

$= H_j \oplus \langle \sigma_1^{e_1} \rangle \oplus \ldots \oplus \langle \sigma_k^{e_k} \rangle$. ■

Lema 5.11.- Per a $1 \leqslant j \leqslant 3$, $L_j = k_j(\zeta) \cap (\bigcap_{i=1}^{k} \mathbb{Q}(\theta_i, \tilde{\zeta}\zeta_i^{-1}))$. ■

Teorema 5.12.- Suposem que $2 \in P$ i que la terna $(n,\underline{e};P)$ verifica les condicions a'), b), c) de la proposició 5.1. Aleshores, per a tot cos $K \in \Sigma_{ab}(n,\underline{e};P)$, existeix un únic j, $1 \leqslant j \leqslant 3$, tal que $K \subseteq L_j$.

Demostració.- Veiem, primer, la unicitat. Si $j \neq j'$, $1 \leqslant j$, $j' \leqslant 3$, aleshores $L_j \cap L_{j'} = kL$ on $k = k_j \cap k_{j'}$. En efecte, $L_j \cap L_{j'} \supseteq kL$ és clara, i per altra banda, $\mathrm{Gal}(\mathbb{Q}(\tilde{\zeta})|L_j \cap L_{j'}) \supseteq$ $\supseteq \langle \mathrm{Gal}(\mathbb{Q}(\tilde{\zeta})|L_j), \mathrm{Gal}(\mathbb{Q}(\tilde{\zeta})|L_{j'}) \rangle = (H_j + H_{j'}) \oplus \langle \sigma_1^{e_1} \rangle \oplus \ldots \oplus \langle \sigma_k^{e_k} \rangle =$ $= \mathrm{Gal}(\mathbb{Q}(\tilde{\zeta})|kL)$ dóna l'altra inclusió. Però $e_{p_0}(kL|\mathbb{Q}) = e_{p_0}(k|\mathbb{Q}) =$ $= [k:\mathbb{Q}] = e_0/2 < e_0$, ja que $L|\mathbb{Q}$ és no ramificada en $p_0 = 2$; per tant, no pot ser $K \subseteq kL$, ja que $e_{p_0}(K|\mathbb{Q}) = e_0$, si $K \in$ $\in \Sigma_{ab}(n,\underline{e};P)$.

Per a l'existència, i en virtut del lema 5.11, és suficient veure que, donat $K \in \Sigma_{ab}(n,\underline{e};P)$, existeix j, $1 \leqslant j \leqslant 3$, tal que $K \subseteq k_j(\zeta)$ i $K \subseteq \mathbb{Q}(\theta_i, \tilde{\zeta}\zeta_i^{-1})$ per a $1 \leqslant i \leqslant k$. Anàlogament al cas $2 \notin P$, això és conseqüència de la següent proposició. ■

Proposició 5.13.- En les hipòtesis del teorema 5.12, existeix j, $1 \leqslant j \leqslant 3$, tal que $K(\zeta) = k_j(\zeta)$ i que, per a tot i, $1 \leqslant i \leqslant k$, és $K(\tilde{\zeta}\zeta_i^{-1}) = \mathbb{Q}(\theta_i, \tilde{\zeta}\zeta_i^{-1})$.

Demostració.- El cas $1 \leqslant i \leqslant k$ és anàleg al cas $2 \notin P$: $Q(\tilde{\zeta})|Q(\tilde{\zeta}\zeta_i^{-1})$ és totalment ramificada en p_i, no ramificada fora de $\{p_i\}$, i cíclica, i les extensions $K(\tilde{\zeta}\zeta_i^{-1})|Q(\tilde{\zeta}\zeta_i^{-1})$ i $Q(\theta_i,\tilde{\zeta}\zeta_i^{-1})|Q(\tilde{\zeta}\zeta_i^{-1})$ tenen el mateix índex de ramificació, e_i, en p_i; per tant, coincideixen. Pel cas que queda, l'extensió $Q(\tilde{\zeta})|Q(\zeta)$ és totalment ramificada en p_0 i amb grup de Galois isomorf a $Gal(Q(\zeta_0)|Q)$. Com que les extensions $K(\zeta)|Q(\zeta)$ i $k_j(\zeta)|Q(\zeta)$, $1 \leqslant j \leqslant 3$, tenen el mateix índex de ramificació e_0, en p_0, i els $k_j(\zeta)$ són les úniques subextensions de $Q(\tilde{\zeta})|Q(\zeta)$ de grau e_0 sobre $Q(\zeta)$, $K(\zeta)$ ha de ser una de les tres.■

Observació 4.- Anàlogament al cas $2 \notin P$, el teorema 5.12 és un refinament del teorema de Kronecker-Weber per al cas $2 \in P$. Ara, però, obtenim tres extensions de Q, en lloc d'una sola, que contenen entre totes tres tots els cossos K de $\Sigma_{ab}(n,\underline{e};P)$.

Corol.lari 5.14.- Per a $1 \leqslant j \leqslant 3$, si $K \in \Sigma_{ab}(n,\underline{e};P)$ i $K \subsetneq L_j$, aleshores $L_j|K$ és no ramificada a tot primer finit.■

Corol.lari 5.15.- Si $\Sigma_{ab}(n,\underline{e};P) \neq \phi$, aleshores n divideix

$$\prod_{p_i \in P} e_i .■$$

Pel que fa referència als problemes plàntejats al §1, els resultats d'aquest § es poden resumir en el següent

Teorema 5.16.- Sigui P un conjunt finit i no buit de números primers, i siguin $n,\underline{e}$, com al §1. Suposem que $\Sigma_{ab}(n,\underline{e};P)$ és no buit. Aleshores, es verifiquen les condicions

a) n divideix $\prod_{p_i \in P} e_i$,

b) si $\mu = \text{m.c.m.}\{e_i : p_i \in P\}$, aleshores μ divideix n,

c) si per a tot $p_i \in P$ posem $e_i = p_i^{r_i} e_i'$ amb $p_i \nmid e_i'$, aleshores $p_i \equiv 1 \pmod{e_i'}$. ∎

Observació 5.- Les condicions a) i c) impliquen l'existència de naturals $t_i >> 0$ tals que, per a $m = \prod_{p_i \in P} p_i^{t_i}$ és $n \mid \varphi(m)$; per tant, la condició a) d'aquest teorema és més forta que la condició a') de la proposició 5.1, sempre que es verifiqui la condició c). A més a més, es llegeix directament de les dades $n,\underline{e}$, P.

En particular, aquest teorema diu que les extensions abelianes de $\mathbb{Q}$ no són ni "poc" ramificades -el producte de tots els índexs de ramificació és múltiple del grau de l'extensió-, ni tampoc no són "molt" ramificades -el mínim múltiple comú dels índexs de ramificació divideix el grau. Això no és cert, en general, si l'extensió no és abeliana, ò si el cos base no és el cos dels números racionals. En efecte, es té el següent exemple en el cas no abelià sobre $\mathbb{Q}$ (cf.[Sam 1: cap. VI, problema 2.B.d]]).

Exemple 5.17.- Considerem el polinòmi $f(X) = X^3 - X + 1$; aquest polinomi és irreduïble a $\mathbb{Q}[X]$ i podem considerar una arrel α de $f(X)$ en $\bar{\mathbb{Q}}$; posem $K = \mathbb{Q}(\alpha)$ i sigui L la clausura normal de l'extensió $K|\mathbb{Q}$. El discriminant de $f(X)$ és -23, de manera que el discriminant de l'extensió $K|\mathbb{Q}$ és $\Delta(K|\mathbb{Q}) = -23$; en conseqüència, $K|\mathbb{Q}$ només ramifica en $p = 23$, i com que 23^2 no divideix $\Delta(K|\mathbb{Q})$, resulta que, per força, 23 ramifica en la forma $P^2 \cdot Q$ amb P , Q , primers diferents de K. Per altra banda, $K|\mathbb{Q}$ no és de Galois i, per tant, $[L:\mathbb{Q}] = 6$ i $L|\mathbb{Q}$ no és abeliana; a més a més, $L = K(\sqrt{-23})$ és la composició de les extensions $K|\mathbb{Q}$ i $\mathbb{Q}(\sqrt{-23})|\mathbb{Q}$; en particular, $L|\mathbb{Q}$ no ramifica fora de $\{23\}$. Veiem que $e_{23}(L|\mathbb{Q}) = 2$; amb això tindrem que $n = 6$ no divideix $\prod_{p_i \in P} e_i = 2$. Com que $e_{23}(\mathbb{Q}(\sqrt{-23})|\mathbb{Q}) = 2$, resulta que $e_{23}(L|\mathbb{Q}^{p_i})$ és parell; però com que en K hi ha més d'un primer que divideix 23, en L també; de la fórmula $n = efg$, com que $e_{23}(L|\mathbb{Q})$ és parell i $g_{23}(L|\mathbb{Q}) > 1$, resulta que $f_{23}(L|\mathbb{Q}) = 1$, $g_{23}(L|\mathbb{Q}) = 3$ i $e_{23}(L|\mathbb{Q}) = 2$, com volíem veure.

§6.- Conseqüències

En aquest § obtenim una conseqüència sobre el número de classes de les extensions abelianes de Q : concretament, n'obtenim un divisor. Per a això, suposem que la terna $(n,\underline{e};P)$ verifica les condicions del teorema 5.16.

Posem $e = \prod_{p_i \in P} e_i$ i sigui $L|Q$ una extensió $(\underline{e};P)$-universal. Per a tota extensió finita $K|Q$, posem $h(K)$ el número de classes del cos K. Amb aquestes notacions es verifica el següent

Teorema 6.1.- Si $K \in \Sigma_{ab}(n,\underline{e};P)$ i $K \subseteq L$, aleshores el quocient e/n divideix $2h(K)$. A més a més, si K és complex, ò bé si L és real, e/n divideix $h(K)$.

Demostració.- L'extensió $L|K$ és abeliana i no ramificada a tot primer finit de K (cf. corol.laris 5.7 i 5.14), de manera que si $L|K$ no ramifica en els primers de l'infinit de K, el grau $e/n = [L:K]$ divideix el grau, $h(K)$, del cos de classes de K. Ara bé, en el cas en què L (i per tant, K) és real, i en el cas en què K (i per tant, L) és complex, $L|K$ també és no ramificada en els primers de l'infinit de K. Per altra banda, en el cas en què L és complex i K és real, posem $L^+ \subseteq L$ la màxima subextensió real de L; aleshores $K \subseteq L^+$ i $L^+|K$ és abeliana i no ramificada a tot primer (finit o no) de K. En aquest cas, només cal veure que $[L^+:K] = e/2n$, ò equivalentment, que $[L:L^+] = 2$. Però això es verifica per a tota extensió de Galois complexa $L|Q$, ja que L^+ és el cos fix pel grup d'inèrcia en els primers

de l'infinit de L, i aquest grup és d'ordre 2.■

La següent proposició dóna una caracterització de quan el cos L és un cos real. Aquesta caracterització és una propietat que, si $2 \notin P$, només depèn de la parella $(\underline{e};P)$. Mantinguem les notacions del §5.

Proposició 6.2.- a) Si $2 \notin P$, L és real si, i només si, per a $1 \leqslant i \leqslant k$, es verifica que $p_i \equiv 1 \pmod{2e_i'}$.

b) Si $2 \in P$, L és real si, i només si, per a $1 \leqslant i \leqslant k$, es verifica que $p_i \equiv 1 \pmod{2e_i'}$ i a més a més l'extensió $(e_0;\{2\})$-universal inclosa en L és real.

Demostració.- El cos L és real si, i només si, totes les subextensions $(e_i;\{p_i\})$-universals de $L|Q$ són reals, ja que L és la composició d'aquestes. Ara bé, si $p_i \neq 2$, l'extensió $(e_i;\{p_i\})$-universal $Q(\theta_i)|Q$ és real si, i només si, $Q(\theta_i) \subseteq Q(\zeta_i+\zeta_i^{-1})$, on ζ_i és una arrel primitiva $p_i^{r_i+1}$-èsima de la unitat. Però $[Q(\zeta_i+\zeta_i^{-1}):Q] = p_i^{r_i}(p_i-1)/2$, i l'extensió $Q(\zeta_i)|Q$ és cíclica, de manera que $Q(\theta_i) \subseteq Q(\zeta_i+\zeta_i^{-1})$ si, i només si, $e_i = [Q(\theta_i):Q]$ divideix $p_i^{r_i}(p_i-1)/2$; equivalentment, si, i només si, e_i' divideix $(p_i-1)/2$.■

En el cas de les extensions quadràtiques de Q , el teorema 6.1 admet el següent enunciat, per altra banda ben conegut (cf.[B-S: cap. 3, §8, teor. 8]):

Corol.lari 6.3.- Sigui $K|Q$ una extensió quadràtica, i sigui k el número de primers finits que ramifiquen a K. Aleshores, 2^{k-2} divideix $h(K)$ i, si K és imaginari, 2^{k-1} divideix $h(K)$.■

Notem que si posem k' el número total de primers que ramifiquen a K, finits o no, aleshores $2^{k'-2}$ divideix $h(K)$ tant en el cas real com en el cas imaginari.

El cas de les extensions cícliques $K|Q$ de grau primer senar $n = p$, és també remarcable: com que L és real, si k és el número de primers de Q que ramifiquen a K, aleshores p^{k-1} divideix $h(K)$.

Observació 1.- En aquest cas $n = p$, primer senar, $k-1$ és una fita inferior del p-rang del grup de classes d'ideals de K. En efecte, $Gal(L|Q) \simeq (\mathbb{Z}/p\,\mathbb{Z})^k$ de manera que $Gal(L|K) \simeq (\mathbb{Z}/p\,\mathbb{Z})^{k-1}$; però $Gal(L|K)$ és un quocient de la p-component del grup de classes de K. Anàlogament pel cas quadràtic, $k-2$ és una fita inferior pel 2-rang del grup de classes, i $k-1$ quan K és imaginari.

El teorema 6.1 es pot interpretar en funció dels cossos de gèneres (genus fields) de les extensions abelianes de Q. En efecte, si $K|Q$ és una extensió abeliana, el cos de gèneres de $K|Q$ és el cos L_0, maximal entre els que verifiquen les condicions

(i) $L_0|Q$ és una extensió abeliana,

(ii) $L_0|K$ és no ramificada a tot primer, finit o no finit, de K

(cf.[Ja 1: cap. VI, §3, definició]).

Es té la caracterització següent:

Teorema 6.4.- Sigui $L_0|Q$ una extensió abeliana finita; sigui P el conjunt dels primers finits de Q que ramifiquen a L_0 , i sigui $e_{p_i}(L_0|Q) = e_i$, per a tot $p_i \in P$. Considerem les propietats següents:

a) L_0 és cos de gèneres d'alguna subextensió $K|Q$ de $L_0|Q$.

b) L_0 és cos de gèneres de $L_0|Q$.

c) L_0 és una de les extensions $(\underline{e};P)$-universals.

d) $[L_0:Q] = \prod_{p_i \in P} e_i$.

d') $[L_0:Q] = \frac{1}{2} \prod_{p_i \in P} e_i$.

Aleshores, es verifica que:

1) Si L_0 és complex, a),b),c),d) són equivalents.

2) Si L_0 és real, a),b) són equivalents, c),d) són equivalents, d) implica a), i a) implica d) ò d').

Demostració.- Les implicacions b) $\Rightarrow$ a) i c) $\Rightarrow$ d) són clares. A més a més, si $L|Q$ és l'extensió $(\underline{e};P)$-universal que conté L_0, $[L:Q] = \prod_{p_i \in P} e_i$, de manera que d) $\Rightarrow$ c). Suposem que es verifica a) i sigui $L|Q$ l'extensió $(\underline{e};P)$-universal que conté L_0; com que $L_0|K$ és no ramificada, $L|Q$ és l'extensió $(\underline{e};P)$-universal que conté K. Suposem que L_0 és complex; aleshores K és

complex i L és complex. Però $[L:Q] = \prod_{p_i \in P} e_i$, i com que $L|K$ és no ramificada a tot primer, finit o no, de K, és $L \subseteq L_0$; d'aquí es dedueix que $L = L_0$. En particular, d). Anàlogament, si L_0 és real, K és també real i si L és real es verifica d); però si L és complex i L^+ és la subextensió real maximal de $L|Q$, resulta que $L_0 = L^+$ i aleshores d').

Suposem que es verifica d) i sigui $L|Q$ el cos de gèneres de $L_0|Q$. Com que $L|Q$ és abeliana, $[L:Q]$ divideix $\prod_p e_p(L|Q) = \prod_{p_i \in P} e_i = [L_0:Q]$, i com que $L_0 \subseteq L$, resulta la igualtat $L = L_0$ i, per tant, b). Només resta veure que a) $\Rightarrow$ b), en el cas L_0 real, ja que pel cas L_0 complex hem vist que a) $\Rightarrow$ d) i que d) $\Rightarrow$ b). A més a més, si L_0 és real i l'extensió universal que conté L_0 és real, també hem vist que a) $\Rightarrow$ d) i d) $\Rightarrow$ b). Per tant, podem suposar que L_0 és real i L és complex, on L és l'extensió $(\underline{e};P)$-universal que conté L_0. Però aleshores, $L_0 = L^+$ i el cos de gèneres de $L_0|Q$ està inclòs en L^+, ja que és real i està inclòs en L. Per tant L_0 és el cos de gèneres de $L_0|Q$. ∎

Observació 2.- En el cas en què L_0 és real es té, en particular, que $L_0 = L^+$, de manera que $L_0 = L$ si, i només si, L és real. Hi ha casos en què $L^+ = L$ (per exemple, per a grau senar, sempre) i casos en què $L_0 = L^+ \subsetneq L$: per exemple, si $K = Q(\sqrt{3})$, aleshores $L_0 = L^+ = K$, mentre que $L = Q(i,\sqrt{3})$.

Corol.lari 6.5.- Sigui $K|Q$ una extensió abeliana finita; siguin P el conjunt dels primers finits de Q que ramifiquen a K, $e_i = e_{p_i}(K|Q)$ per a tot

$p_i \in P$, i sigui $L|\mathbb{Q}$ l'extensió $(\underline{e};P)$-universal que conté K. Aleshores:

a) Si K és complex, el cos de gèneres de K és L.

b) Si K és real, el cos de gèneres de K és L^+, i es té que $L = L^+$ si, i només si, L és real.■

§7.- Reducció del problema d'existència a un problema de grups.

En aquest §, l'objectiu és fer la reducció del càlcul del cardinal de $\Sigma_{ab}(n,\underline{e};P)$ a un problema combinatori de grups abelians finits. Per a això, suposem que la terna $(n,\underline{e};P)$ verifica les condicions a), b) i c) del teorema 5.16.

Sigui $L|Q$ una de les extensions $(\underline{e};P)$-universals; així, $L|Q$ és l'única extensió $(\underline{e};P)$-universal si $2 \notin P$, i una de les tres extensions $(\underline{e};P)$-universals si $2 \in P$. Posem $\Sigma_L(n,\underline{e};P)$ el subconjunt de $\Sigma_{ab}(n,\underline{e};P)$ format pels cossos K tals que $K \subseteq L$. En virtut del teorema 5.5 resulta que, si $2 \notin P$, aleshores $\Sigma_L(n,\underline{e};P) = \Sigma_{ab}(n,\underline{e};P)$, i en virtut del teorema 5.12 que, si $2 \in P$, aleshores $\Sigma_{ab}(n,\underline{e};P)$ és la reunió disjunta dels conjunts $\Sigma_L(n,\underline{e};P)$ per a les tres extensions $(\underline{e};P)$-universals, $L|Q$. Per tant, caracteritzar $\Sigma_{ab}(n,\underline{e};P)$ equival a caracteritzar cada un dels $\Sigma_L(n,\underline{e};P)$.

Si $2 \notin P$, L és la composició de la família d'extensions linealment disjuntes $\{Q(\theta_i)|Q\}_{p_i \in P}$, on $Q(\theta_i)|Q$ és l'única extensió $(e_i;\{p_i\})$-universal. Si $2 \in P$, cal afegir a la família anterior una de les extensions $(e_0;\{2\})$-universals, extensió que denotarem per $Q(\theta_0)|Q$. Per a unificar les notacions, posarem $Q(\theta_0) = Q$ si $2 \notin P$ i així, en tots els casos, serà $L = Q(\theta_0,\theta_1,\ldots,\theta_k)$, la composició de les extensions $Q(\theta_i)|Q$, $0 \leqslant i \leqslant k$.

Sigui $G = Gal(L|Q)$ i sigui $G_i = Gal(Q(\theta_i)|Q)$, $0 \leqslant i \leqslant k$; aleshores $G = \bigoplus_{i=0}^{k} G_i$, on identifiquem $Gal(Q(\theta_i)|Q)$ amb la seva imatge G_i dins G. Aleshores $G_i = Gal(Q(\theta_i)|Q) \simeq Gal(L|Q(\tilde{\theta}_i))$ on $Q(\tilde{\theta}_i) = Q(\theta_0,\ldots,\theta_{i-1},\theta_{i+1},\ldots,\theta_k)$, $0 \leqslant i \leqslant k$. Dels teoremes 3.1. b) i 4.2, es dedueix immediatament el següent

Corol.lari 7.1.- a) Per a $1 \leqslant i \leqslant k$, $G_i \simeq \mathbb{Z}/e_i\mathbb{Z}$.

b) Si $2 \notin P$ és $G_0 = \{0\}$.

c) Si $2 \in P$ G_0 és isomorf a un dels tres subgrups d'índex 2 de $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/e_0\mathbb{Z})$; és a dir, G_0 és isomorf a un dels tres subgrups $(0) \times (1)$, $\langle (1,1) \rangle$, $(1) \times (2)$. ■

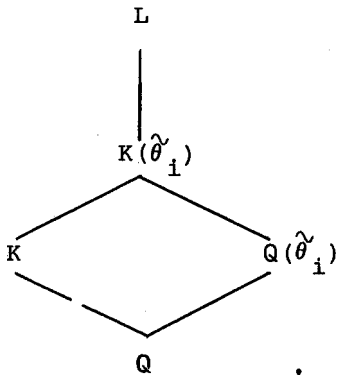
Amb aquestes notacions, la següent proposició caracteritza el conjunt $\Sigma_L(n,\underline{e};P)$, i transforma el problema del càlcul del seu cardinal, i del de $\Sigma_{ab}(n,\underline{e};P)$, en un problema combinatori de grups abelians finits.

Proposició 7.2.- Existeix una bijecció entre $\Sigma_L(n,\underline{e};P)$ i el conjunt dels subgrups $X \subseteq G$ tals que

a) $(G:X) = n$,

b) per a $0 \leqslant i \leqslant k$, $X \cap G_i = \{0\}$.

Demostració.- Podem considerar la restricció a $\Sigma_L(n,\underline{e};P)$ de l'aplicació bijectiva de la teoria de Galois entre el conjunt dels subcossos $K \subseteq L$ i el conjunt dels subgrups $X = \mathrm{Gal}(L|K) \subseteq G$; com que $(G:X) = [K:Q]$, resulta que la propietat a) caracteritza el grau n de les subextensions $K|Q$ de $L|Q$, i només cal veure que b) caracteritza els índexs de ramificació. Però, donat un subcòs qualsevol, $K \subseteq L$, i donat un primer $p_i \in P$, podem calcular efectivament l'índex de ramificació $e_{p_i}(K|Q)$. En efecte, considerem, per a tot i, $0 \leqslant i \leqslant k$, el diagrama de subcossos de L



Com que l'extensió $L|Q(\widetilde{\theta}_i)$ és totalment ramificada en p_i i l'extensió $K(\widetilde{\theta}_i)|K$ és no ramificada en p_i, $e_{p_i}(K|Q) = [K(\widetilde{\theta}_i):Q(\widetilde{\theta}_i)]$, és a dir, l'índex de $Gal(L|K(\widetilde{\theta}_i))$ en $Gal(L|Q(\widetilde{\theta}_i))$. Si $X = Gal(L|K)$, és $Gal(L|K(\widetilde{\theta}_i)) = X \cap G_i$, ja que $G_i = Gal(L|Q(\widetilde{\theta}_i))$.

Per tant, i com que G_i és d'ordre e_i, resulta que $e_{p_i}(K|Q) = e_i$ si, i només si, $X \cap G_i = \{0\}$, com volíem demostrar.■

Convé transformar el problema de grups en un altre problema equivalent. Per a això, siguin $G_0', G_1, \ldots, G_k$, grups abelians finits qualssevol, i sigui $G = \bigoplus_{i=0}^{k} G_i \simeq \prod_{i=0}^{k} G_i$. Posem $\Pi_i: G \to G_i$ les projeccions canòniques, i identifiquem G_i amb la seva imatge per la inclusió canònica $G_i \to G$. Per a tot divisor n de l'ordre de G, considerarem els següents conjunts de subgrups de G:

$$S(G_0,\ldots,G_k;n) = \{X \subseteq G: (G:X) = n \text{ i per a } 0 \leqslant i \leqslant k,\ X \cap G_i = \{0\}\}$$

$$P(G_0,\ldots,G_k;n) = \{X \subseteq G: \#X = n \text{ i per a } 0 \leqslant i \leqslant k,\ \Pi_i(X) = G_i\}$$

A més a més, posarem

$$S(G_0,\ldots,G_k) = \bigsqcup_{n \mid \# G} S(G_0,\ldots,G_k;n),$$

$$P(G_0,\ldots,G_k) = \bigsqcup_{n \mid \# G} P(G_0,\ldots,G_k;n).$$

Amb aquestes notacions es verifica la següent

Proposició 7.3.- Existeix una bijecció que inverteix l'ordre entre els conjunts $S(G_0,\ldots,G_k)$ i $P(G_0,\ldots,G_k)$ i que, per a tot divisor n de l'ordre de $G = G_0 \oplus \ldots \oplus G_k$, transforma $S(G_0,\ldots,G_k;n)$ en $P(G_0,\ldots,G_k;n)$.

Abans de procedir a la demostració d'aquest resultat convé recordar algunes notacions i resultats ben coneguts. Per a tot grup abelià finit, G, posarem $\hat{G} = \mathrm{Hom}(G,\mathbb{C}^*)$ el grup dels caràcters complexos de G. Si $X \subseteq G$ és un subgrup qualsevol, posarem $X^{\perp} = \{\rho \in \hat{G}: \rho(x) = 1 \text{ per a tot } x \in X\}$, l'ortogonal de X. Es verifica el resultat següent (cf.[Se 3: cap. VI, §1.1]).

Lema 7.4.- a) $\hat{G}$ és un grup abelià isomorf, no canònicament, a G; $\hat{\hat{G}}$ és canònicament isomorf a G.

b) Si $X \subseteq G$ és un subgrup, aleshores $X^{\perp}$ és un subgrup de $\hat{G}$, isomorf al grup $(G/X)^{\sim}$.

c) L'assignació $X \to X^{\perp}$ defineix una bijecció que inverteix l'ordre entre el conjunt dels subgrups de G i el conjunt dels subgrups de $\hat{G}$.■

Demostració de la proposició 7.3.- Com que $G = \bigoplus_{i=0}^{k} G_i$, resulta que $\hat{G} \simeq \prod_{i=0}^{k} \hat{G}_i$. Aquest isomorfisme dóna una bijecció que conserva l'ordre entre $S(\hat{G}_0,\ldots,\hat{G}_k)$ i $S(G_0,\ldots,G_k)$; en particular, respecta els índexs dels subgrups. Per altra banda, podem restringir al conjunt $P(G_0,\ldots,G_k)$ l'aplicació $X \to X^{\perp}$ del lema 7.4. c) i, com que $\#X = (\hat{G}:X^{\perp})$, la proposició quedarà provada si veiem que la imatge de $P(G_0,\ldots,G_k)$ és exactament $S(\hat{G}_0,\ldots,\hat{G}_k)$. Així, és suficient provar que per a tot i, $0 \leqslant i \leqslant k$, és $\Pi_i(X) = G_i$ si, i només si, $X^{\perp} \cap \hat{G}_i = \{1\}$.

Sigui, doncs, $i \in \{0,1,\ldots,k\}$, fix. Es té que $(\bigoplus_{j\neq i} G_j)^{\perp} = \hat{G}_i$, de manera que $X^{\perp} \cap \hat{G}_i = X^{\perp} \cap (\bigoplus_{j\neq i} G_j)^{\perp} = (X + \bigoplus_{j\neq i} G_j)^{\perp}$. Això diu que $X^{\perp} \cap \hat{G}_i = \{1\}$ si, i només si, $X + \bigoplus_{j\neq i} G_j = G$. Però això últim equival a dir que $\Pi_i(X + \bigoplus_{j\neq i} G_j) = G_i$ (exercici) i, com que $\Pi_i(X + \bigoplus_{j\neq i} G_j) = \Pi_i(X)$, resulta que $X^{\perp} \cap \hat{G}_i = \{1\}$ si, i només si, $\Pi_i(X) = G_i$, com volíem demostrar.■

Per a simplificar la resolució del problema de grups convé, encara, fer una nova reducció. Donats un grup abelià finit G qualsevol i un número primer p arbitrari, posem $S_p(G)$ l'únic p-subgrup de Sylow de G. És immediat que, si $G = \prod_{i=0}^{k} G_i$, aleshores $S_p(G) = \prod_{i=0}^{k} S_p(G_i)$.

Proposició 7.5.- Siguin $G_0,\ldots,G_k$, grups abelians finits d'ordre $e_0,e_1,\ldots,e_k$, i sigui $e = \prod_{i=0}^{k} e_i$. Aleshores, les aplicacions

$$P(G_0,\ldots,G_k) \to \prod_{p|e} P(S_p(G_0),\ldots,S_p(G_k)),$$

$$P(G_0,\ldots,G_k;n) \to \prod_{p|e} P(S_p(G_0),\ldots,S_p(G_k);p^{v_p(n)}),$$

definides per $X \to \{S_p(X)\}_{p|e}$, són bijectives per a tot $n|e$.

Demostració.- Posem $G = G_0 \times G_1 \times \ldots \times G_k$ i sigui X un subgrup de G. Aleshores $X = \bigoplus_{p|e} S_p(X)$, i, per a tot $p|e$, $S_p(X) \subseteq S_p(G) = \bigoplus_{i=0}^{k} S_p(G_i)$. A més a més, si X és d'ordre n, $S_p(X)$ és d'ordre $p^{v_p(n)}$. Per tant, l'assignació $X \to \{S_p(X)\}_{p|e}$ defineix una aplicació del conjunt dels subgrups de G en el producte cartesià dels conjunts dels subgrups de $S_p(G)$, i envia subgrups d'ordre n a subgrups d'ordre $p^{v_p(n)}$ a cada component. Com que X es recupera de $\{S_p(X)\}_{p|e}$, ja que $X = \bigoplus_{p|e} S_p(X)$, aquesta aplicació és injectiva (i exhaustiva).

Posem, ara, per a $0 \leqslant i \leqslant k$, i per a $p|e$,

$$\Pi_{p,i} : S_p(G_0) \times \ldots \times S_p(G_k) \to S_p(G_i)$$

la projecció canònica. Només cal veure que, per a $0 \leqslant i \leqslant k$, les dues condicions següents són equivalents:

(i) $\Pi_i(X) = G_i$.

(ii) Per a tot primer $p|e$, $\Pi_{p,i}(S_p(X)) = S_p(G_i)$.

En efecte, (ii) tradueix el fet que $S_p(X) \in P(S_p(G_0),\ldots,S_p(G_k))$ per a tot $p|e$.

Però, per a $p|e$ i per a $0 \leqslant i \leqslant k$, es té el diagrama commutatiu de morfismes de grups abelians:

$$\begin{array}{ccc} G_0 \times G_1 \times \ldots \times G_k & \xrightarrow{\psi_p} & S_p(G_0) \times S_p(G_1) \times \ldots \times S_p(G_k) \\ \Pi_i \downarrow & & \downarrow \Pi_{p,i} \\ G_i & \xrightarrow[\psi_{p,i}]{} & S_p(G_i) \end{array} ,$$

on $\psi_{p,i}$ és la projecció corresponent a la descomposició de G_i en suma directa dels seus p-subgrups de Sylow, i $\psi_p = (\psi_{p,0},\ldots,\psi_{p,k})$ ve donada per les $\psi_{p,i}$ component a component. Com que, si $X \subseteq G$, aleshores $\psi_p(X) = S_p(X)$, l'equivalència de (i) i (ii) és conseqüència de l'exhaustivitat de tots els morfismes del diagrama commutatiu. En efecte, (i) $\Rightarrow$ (ii) és clar. Recíprocament, per a $0 \leqslant i \leqslant k$, $\Pi_i(X)$ és un subgrup de G_i tal que $\psi_{p,i}(\Pi_i(X)) = S_p(G_i)$ per a tot p; per tant, l'ordre de $\Pi_i(X)$ és múltiple de l'ordre de $S_p(G_i)$ per a tot p; i, en conseqüència, $\Pi_i(X) = G_i$.■

Finalment, el corol.lari 7.1 i les proposicions 7.3 i 7.5 ens permeten escriure la proposició 7.2 en la forma equivalent següent, de manera que el càlcul de $a(n,\underline{e};P)$ queda reduït al càlcul, per a tot primer $p|n$, del cardinal

$$\#P(S_p(G_0),\ldots,S_p(G_k);\ p^{v_p(n)}).$$

Teorema 7.6.- Existeix una bijecció entre $\Sigma_L(n,\underline{e};P)$ i el conjunt

$$\prod_{p|n} P(S_p(G_0),\ldots,S_p(G_k);p^{v_p(n)}),$$

on

$$\begin{cases} G_i = \mathbb{Z}/e_i\,\mathbb{Z} & , \text{ si } 1 \leqslant i \leqslant k, \\ G_0 = \{0\} & , \text{ si } 2 \notin P, \\ G_0 = \mathbb{Z}/e_0\,\mathbb{Z} & , \text{ en dos dels tres casos en què } 2 \in P, \\ G_0 = (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/(e_0/2)\,\mathbb{Z}) & , \text{ en el tercer cas en què } 2 \in P. \blacksquare \end{cases}$$

Definició.- Direm que estem en el cas I quan G_0 sigui un grup cíclic; el cas II serà el cas en què G_0 no és cíclic.

En conseqüència, si $2 \notin P$, ò si $2 \in P$ i $e_0 = 2$, sempre estarem en el cas I, mentre que si $2 \in P$ i $e_0 = 2^{r_0} > 2$, estarem en el cas I per a dues extensions $(\underline{e};P)$-universals, $L|Q$, i en el cas II per a la tercera.

§8.- Demostració de l'existència.

En el §5 hem donat les condicions necessàries per a què el conjunt $\Sigma_{ab}(n,\underline{e};\mathcal{P})$ sigui no buit, i en el §7 hem reduït el càlcul del seu cardinal a un problema combinatori de grups abelians finits. En aquest § es tracta de demostrar que, si la terna $(n,\underline{e};\mathcal{P})$ verifica les condicions del teorema 5.16, aleshores el conjunt $\Sigma_{ab}(n,\underline{e};\mathcal{P})$ és, efectivament, no buit. Per a això, convé resoldre primer el cas particular $n = m.c.m.\{e_i : p_i \in \mathcal{P}\}$. Abans, però, donarem la solució dels casos particulars $n = p$, primer, i $n = \prod_{p_i \in \mathcal{P}} e_i$.

Comencem pel cas $n = p$, primer. En aquest cas, les condicions del teorema 5.16 es poden escriure en la forma: $e_i = p$, per a tot $p_i \in \mathcal{P}$ i, per a tot $p_i \in \mathcal{P}$, si $p_i \neq p$, aleshores $p_i \equiv 1 \pmod p$. En particular, si p és senar, $2 \notin \mathcal{P}$. En aquestes condicions es té que:

Teorema 8.1.- Suposem que p és primer i que la terna $(p,\underline{e};\mathcal{P})$ verifica les condicions del teorema 5.16.

a) Si $2 \notin \mathcal{P}$, aleshores $a(p,\underline{e};\mathcal{P}) = (p-1)^{k-1}$.

b) Si $2 \in \mathcal{P}$, aleshores $p = 2$ i $a(2,\underline{e};\mathcal{P}) = 3$.

Demostració.- En el cas $p = 2$, el resultat ha estat provat en el §2; en particular, s'obté b), i també a) en el cas $p = 2$. Suposem, doncs, que p és senar; en virtut de la proposició 7.2, $a(p,\underline{e};\mathcal{P}) = \#S(\mathbb{Z}/p\mathbb{Z},\overset{k)}{\ldots},\mathbb{Z}/p\mathbb{Z};p)$. Però $G = (\mathbb{Z}/p\mathbb{Z})^k$ és un $\mathbb{F}_p$-espai vectorial de dimensió k, i volem calcular el número de subespais de dimensió $k - 1$ que només tallen els eixos

coordenats a l'origen. Aquests hiperplans vénen donats per les equacions $a_1 x_1 + \ldots + a_k x_k = 0$, amb $a_i \in \mathbb{F}_p$, $a_i \neq 0$, i dues equacions defineixen el mateix hiperplà si, i només si, són proporcionals. Això dóna els $(p-1)^k/(p-1) = (p-1)^{k-1}$ subgrups buscats.■

Anem a resoldre, ara, els casos extrems de l'existència. El teorema 5.16 ens assegura que, si posem $\mu = \text{m.c.m.}\{e_i : p_i \in P\}$, $e = \prod_{p_i \in P} e_i$, i si $\Sigma_{ab}(n,\underline{e};P) \neq \phi$, aleshores $\mu | n$, i $n | e$; de manera que els valors extrems possibles per a n són els valors $n = \mu$ i $n = e$. Els teoremes 5.5 i 5.12 donen el resultat per a $n = e$:

Corol.lari 8.2.- Suposem que la parella $(\underline{e};P)$ verifica les condicions $p_i \equiv 1 \pmod{e_i'}$, per a tot $p_i \in P$. Aleshores:

$$a(e,\underline{e};P) = \begin{cases} 1 & \text{si } 2 \notin P, \\ 3 & \text{si } 2 \in P. \end{cases}$$ ■

El cas $n = \mu$ mereix atenció especial, ja que d'aquest cas es deduirà que $\Sigma_{ab}(n,\underline{e};P) \neq \phi$. Suposem, doncs, que per a tot $p_i \in P$ es verifiquen les condicions $p_i \equiv 1 \pmod{e_i'}$.

Proposició 8.3.- En les condicions anteriors, i si $2 \notin P$, aleshores

$$a(\mu,\underline{e};P) = \varphi(e_1) \ldots \varphi(e_k)/\varphi(\mu),$$

on φ és l'indicador d'Euler.

Demostració.- En el §7 hem reduït el càlcul de $a(\mu,\underline{e};P)$ al càlcul de $\#P(G_1,\ldots,G_k;\mu)$, amb $G_i = \mathbb{Z} / e_i\,\mathbb{Z}$, $1 \leqslant i \leqslant k$. Suposem, doncs, que $X \in P(G_1,\ldots,G_k;\mu)$ i sigui $\tilde{x}_i$ un element de G_i d'ordre e_i; com que $\Pi_i(X) = G_i$, X conté un element que es projecta en $\tilde{x}_i$ per Π_i, i que, per tant, té ordre múltiple de e_i. Així, per a $1 \leqslant i \leqslant k$, X conté un element d'ordre e_i i, en conseqüència, X conté un element d'ordre μ. Per tant, X és cíclic. Ara bé, si x és un generador qualsevol de X, i escrivim $x = (x_1,\ldots,x_k) \in G_1 \times\ldots\times G_k$, resulta que x_i genera $\Pi_i(X) = G_i$. Recíprocament, si per a $1 \leqslant i \leqslant k$, x_i és un generador qualsevol de G_i, el subgrup X de $G_1 \times\ldots\times G_k$ generat per $x = (x_1,\ldots,x_k)$ pertany a $P(G_1,\ldots,G_k;\mu)$. Això diu que el cardinal de $P(G_1,\ldots,G_k;\mu)$ és el quocient entre el número d'elements $x = (x_1,\ldots,x_k) \in G_1 \times\ldots\times G_k$ tals que x_i genera G_i, per a $1 \leqslant i \leqslant k$, i el número d'elements $x \in X$ tals que x genera X. El resultat és, doncs, conseqüència del fet que $\varphi(m)$ és el número d'elements que generen un grup cíclic d'ordre m, per a tot natural m.■

El cas $n = \mu$, $2 \in P$ és més complicat. Sigui $L|\mathbb{Q}$ una de les extensions $(\underline{e};P)$-universals amb grup de Galois isomorf al grup

$$(\mathbb{Z}/e_0\mathbb{Z}) \times (\mathbb{Z}/e_1\mathbb{Z}) \times\ldots\times (\mathbb{Z}/e_k\mathbb{Z}).$$

Això passa en el cas I; és a dir:

(i) si $e_0 = 2$, per a les tres extensions $(\underline{e};P)$-universals,

(ii) si $e_0 = 2^{r_0} > 2$, per a dues de les tres extensions $(\underline{e};P)$-universals.

En aquest cas es té, amb la mateixa demostració anterior, i afegint-hi el subíndex zero, el resultat següent:

Proposició 8.4.- El cardinal de $\Sigma_L(\mu,\underline{e};P)$ és $\varphi(e_0)\varphi(e_1)\ldots\varphi(e_k)/\varphi(\mu)$.■

El cas que queda és el cas II, en el qual $Gal(L|\mathbb{Q}) = G_0 \times\ldots\times G_k$ amb $G_0 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/(e_0/2)\mathbb{Z})$, $e_0 > 2$, i $G_i = \mathbb{Z}/e_i\mathbb{Z}$, $1 \leqslant i \leqslant k$. Posem α el número d'índexs, i, tals que $1 \leqslant i \leqslant k$, $4|e_i$, i β el número dels índexs, i, $1 \leqslant i \leqslant k$ tals que $2|e_i$, $4 \nmid e_i$. Aleshores:

Proposició 8.5.- El cardinal de $\Sigma_L(\mu,\underline{e};P)$ és no nul si, i només si, e_0 no divideix cap e_i, $1 \leqslant i \leqslant k$, i val $2^{\alpha}\,3^{\beta}\varphi(e_0)\ldots\varphi(e_k)/\varphi(\mu)$.

Demostració.- Cal calcular, en aquest cas, el cardinal de $P(G_0,\ldots,G_k;\mu)$. Posem $\mu' = m.c.m.\{2, e_0/2, e_1,\ldots,e_k\}$; aleshores $\mu' = \mu$ ò bé $\mu' = \mu/2$. Si $X \in P(G_0,\ldots,G_k;\mu)$ i si raonem de la mateixa manera que a la demostració de la proposició 8.3, resulta que X conté un element d'ordre μ'. Però X no pot ser cíclic, ja que $\Pi_0(X) = G_0$ no ho és. Això implica que $\mu' \neq \mu$, de manera que $\mu' = \mu/2$ i X és un grup abelià de tipus $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/\mu'\mathbb{Z})$; això passa si, i només si, $e_0 \nmid e_1,\ldots,e_0 \nmid e_k$. Aleshores, podem elegir elements $x,y \in X$ tals que x és d'ordre μ', y és d'ordre 2, i $X = \langle x \rangle \oplus \langle y \rangle$, ò equivalentment, $y \notin \langle x \rangle$. Posem $x = (x_{-1},x_0,x_1,\ldots,x_k)$, $y = (y_{-1},y_0,y_1,\ldots,y_k) \in G_0 \times G_1 \times\ldots\times G_k$, una parella qualsevol d'elements $x,y \in X$ en aquestes condicions.

Es tracta de veure que:

- en el cas $e_0 > 4$, G conté $4\varphi(e_0/2)\ 2^{\alpha}3^{\beta}\varphi(e_1)\ldots\varphi(e_k)$ parelles (x,y) en aquestes condicions, mentre que X en conté $4\varphi(\mu')$,

- en el cas $e_0 = 4$, G conté $6\varphi(e_0/2)\ 2^{\alpha}3^{\beta}\varphi(e_1)\ldots\varphi(e_k)$ parelles (x,y) en aquestes condicions, mentre que X en conté $6\ \varphi(\mu')$. Amb això, el cardinal buscat és el quocient i, com que $2\varphi(e_0/2) = \varphi(e_0)$ i $2\ \varphi(\mu') = \varphi(\mu)$, haurem acabat. El que queda de demostració és fer aquest exercici.

Fixem-nos en un índex i, $1 \leqslant i \leqslant k$. Com que $\Pi_i(X) = G_i$, resulta que G_i està generat per la parella x_i, y_i; i com que y és d'ordre 2, es té que

(i) si $2 \nmid e_i$, ha de ser $y_i = 0$ i aleshores x_i ha de ser d'ordre e_i,

(ii) si $4 \mid e_i$, ha de ser $y_i = 0$ ò $y_i = e_i/2$, i x_i ha de ser d'ordre e_i,

(iii) si $2 \mid e_i$, $4 \nmid e_i$, ha de ser x_i d'ordre e_i i $y_i = 0$ ò $e_i/2$; ò bé x_i d'ordre $e_i/2$ i $y_i = e_i/2$.

Nota: encara que $y_i = 0$ per a tot $1 \leqslant i \leqslant k$, veurem que y és d'ordre 2, ja que (y_{-1}, y_0) serà sempre d'ordre 2.

Això dóna, respectivament, $\varphi(e_i)$, $2\varphi(e_i)$, ò $2\varphi(e_i)+\varphi(e_i/2) = 3\varphi(e_i)$, parelles x_i, y_i; i, en conseqüència, $2^{\alpha}3^{\beta}\varphi(e_1)\ldots\varphi(e_k)$ parelles $(x_1,\ldots,x_k)$, $(y_1,\ldots,y_k)$, en G. Veiem, ara, quantes possibilitats hi ha per a les parelles $(x_{-1},x_0),(y_{-1},y_0)$. Per a això, distingirem els casos $e_0 > 4$, i $e_0 = 4$. Comencem pel cas $e_0 > 4$. Els elements de G_0 d'ordre $\leqslant 2$ són els elements $(0,0)$, $(0,e_0/4)$, $(1,0)$, $(1,e_0/4)$, de manera que (y_{-1},y_0) ha de ser un dels quatre. Per altra banda, (x_{-1},x_0) ha de ser d'ordre $e_0/2$ i, per tant, x_0 ha de ser d'ordre $e_0/2$ i $x_{-1} = 0$ ò 1. Això dóna $2\varphi(e_0/2)$ possibilitats per a (x_{-1},x_0). Però el subgrup generat per (x_{-1},x_0) en G_0 conté els elements $(0,0)$, $(0,e_0/4)$, de manera que per a (y_{-1},y_0) només queden les dues

possibilitats (1,0), $(1,e_0/4)$. Observem que (y_{-1},y_0) és d'ordre 2. En conseqüència, hi ha $4\varphi(e_0/2)$ parelles $(x_{-1},x_0),(y_{-1},y_0)$. Per tant, G conté $4\varphi(e_0/2)2^{\alpha}3^{\beta}\varphi(e_1)\ldots\varphi(e_k)$ parelles x,y, tals que x és d'ordre μ', y d'ordre 2, i $y \notin \langle x \rangle$. A més a més $(\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/\mu'\,\mathbb{Z})$ en conté $4\varphi(\mu')$, anàlogament, ò particularitzant $e_0 = \mu'$, $e_1 = \ldots = e_k = 1$.

En el cas $e_0 = 4$ és $G_0 = (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/2\,\mathbb{Z})$ i hi ha $6 = 6\varphi(e_0/2)$ parelles $(x_{-1},x_0),(y_{-1},y_0)$ adequades, i $6\varphi(\mu')$ maneres, en X, d'elegir la parella x,y: la parella (x_{-1},x_0) es pot elegir de $3\varphi(\mu')$ maneres i de 2 maneres la parella (y_{-1},y_0).■

Resumim els resultats anteriors en el següent:

Teorema 8.6.- Suposem que per a tot $p_i \in P$ es verifica que $p_i \equiv 1 \pmod{e_i'}$. Aleshores, el cardinal de $\Sigma_{ab}(\mu,\underline{e};P)$ és

$$a(\mu,\underline{e};P) = A \cdot \varphi(e_1)\ldots\varphi(e_k)/\varphi(\mu),$$

amb

$$A = \begin{cases} 1 & \text{si } 2 \notin P, \\ 3\varphi(e_0) & \text{si } 2 \in P,\ e_0 = 2, \\ 2\varphi(e_0) & \text{si } 2 \in P,\ e_0 > 2,\ \text{i } e_0 \mid e_i \text{ per a algun } 1 \leqslant i \leqslant k, \\ (2+2^{\alpha}3^{\beta})\varphi(e_0) & \text{si } 2 \in P,\ e_0 > 2,\ \text{i } e_0 \nmid e_i \text{ per a tot } 1 \leqslant i \leqslant k, \end{cases}$$

on α, β, són, respectivament, el número d'índexs i, $1 \leqslant i \leqslant k$, tals que $4 \mid e_i$ (per a α), i $2 \mid e_i$, $4 \nmid e_i$ (per a β).■

Podem demostrar ara que les condicions necessàries del teorema 5.16 són també suficients. En efecte, es té el resultat següent:

Teorema 8.7.- Suposem que la terna $(n,\underline{e};P)$ verifica les condicions

a) $n \mid e$,

b) $\mu \mid n$,

c) $p_i \equiv 1 \pmod{e_i'}$, per a tot $p_i \in P$,

on $e = \prod_{p_i \in P} e_i$, $\mu = \text{m.c.m.}\{e_i : p_i \in P\}$, i $e_i = p_i^{r_i} e_i'$, $p_i \nmid e_i'$. Aleshores, el conjunt $\Sigma_{ab}(n,\underline{e};P)$ és no buit.

Demostració.- N'hi ha prou amb demostrar que, per a alguna extensió $(\underline{e};P)$-universal, $L|Q$, el conjunt $\Sigma_L(n,\underline{e};P)$ és no buit. Prenguem $L|Q$ de manera que estiguem en el cas I; això és dir que $\text{Gal}(L|Q) \simeq G_0 \times \ldots \times G_k$, amb $G_i \simeq \mathbb{Z} / e_i \mathbb{Z}$, $0 \leqslant i \leqslant k$, i $e_0 = 1$ si $2 \notin P$. Cal veure que $P(G_0,\ldots,G_k;n)$ és no buit. Sigui H el subgrup de $G = G_0 \times \ldots \times G_k$ generat per $(1,\ldots,1) \in G$. Aleshores, $H \in P(G_0,\ldots,G_k;\mu)$, i si $X \in G$ és un subgrup qualsevol de G d'ordre n i tal que $H \subseteq X$, aleshores $\Pi_i(X) \supseteq \Pi_i(H) = G_i$, per a tot $p_i \in P$, de manera que $X \in P(G_0,\ldots,G_k;n)$. Però hi ha bijecció entre el conjunt dels subgrups de G d'ordre n i que contenen H i el conjunt dels subgrups de G/H d'ordre n/μ. Com que $\mu \mid n$ i G/H és un grup abelià, G/H conté com a mínim un subgrup d'ordre n/μ i, en conseqüència, $\Sigma_{ab}(n,\underline{e};P)$ és no buit.■

§9.- El càlcul de $a(n,\underline{e};P)$.

El problema de caracteritzar en quines condicions el conjunt $\Sigma_{ab}(n,\underline{e};P)$ és no buit ha estat resolt en el §8. En canvi, el problema de calcular el cardinal $a(n,\underline{e};P)$ de $\Sigma_{ab}(n,\underline{e};P)$ ha estat reduït, en el §7, a un problema combinatori de grups abelians finits. Recordem que, per a tot primer p i per a tota parella d'enters no negatius M,N, hem definit en el capítol I, §6, el símbol

$$\begin{bmatrix} N+M \\ M \end{bmatrix}_p = \prod_{j=1}^{M} (p^{N+j}-1) \prod_{j=1}^{M} (p^j-1)^{-1}.$$

Sigui ara $\underline{N} = (N_1,\ldots,N_s,0,\ldots)$ el tipus d'un p-grup abelià finit (cf. apèndix,§1, definició), i sigui v un enter no negatiu. Posem

$$f_p(\underline{N};v) = \sum_{\underline{M}=v} \prod_{i=1}^{s} \sum_{k_i=0}^{n_i} (-1)^{k_i} \binom{n_i}{k_i} p^{\beta_i(\underline{M})} \begin{bmatrix} N_i-k_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_p,$$

on $n_i = N_i - N_{i+1}$, $\beta_i(\underline{M}) = M_{i+1}(N_i-k_i-M_i)$, i la suma estesa a tots els tipus $\underline{M} \leqslant \underline{N}$ tals que $M_1+\ldots+M_s = v$.

El teorema 6.4 de l'apèndix assegura que, si G és un p-grup abelià finit de tipus $\underline{N}$, aleshores $f_p(\underline{N};v)$ és el cardinal del conjunt (cf.§7),

$$P(\mathbb{Z}/p^{n_1}\mathbb{Z},\ldots,\mathbb{Z}/p^{n_1}\mathbb{Z},\ldots,\mathbb{Z}/p^{s}\mathbb{Z},\ldots,\mathbb{Z}/p^{s}\mathbb{Z};p^v).$$

A la vista d'aquest resultat, anem a establir el resultat final sobre $a(n,\underline{e};P)$.

Suposem que la terna $(n,\underline{e};P)$ verifica les condicions del teorema 5.16. Aleshores, per a tot primer p es té que les condicions $p|e$, $p|\mu$, i $p|n$ són equivalents. Com que $a(n,\underline{e};P)$ és la suma dels cardinals de $\Sigma_L(n,\underline{e};P)$ per a les extensions $(\underline{e};P)$-universals $L|Q$ (cf. teorema 5.12), el problema és calcular aquests últims cardinals. Sigui $G = Gal(L|Q)$; aleshores $G \simeq G_0 \times \ldots \times G_k$ amb $G_i = \mathbb{Z}/e_i\mathbb{Z}$, $1 \leqslant i \leqslant k$, i $G_0 = \mathbb{Z}/e_0\mathbb{Z}$ (cas I) ò $G_0 = (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/(e_0/2)\mathbb{Z})$ (cas II). En virtut del teorema 7.6, el cardinal de $\Sigma_L(n,\underline{e};P)$ és el producte, quan p varia en el conjunt dels divisors primers de n, dels cardinals dels conjunts

$$P(S_p(G_0),\ldots,S_p(G_k);p^{v_p(n)}).$$

De manera que el primer que cal fer és calcular els grups $S_p(G_i)$.

Per a tot enter $j \geqslant 1$, els grups $p^{j-1}G/p^jG$ són $\mathbb{F}_p$-espais vectorials de dimensió finita; sigui $N_j = N_j(p) = \dim_{\mathbb{F}_p}(p^{j-1}G/p^jG)$, i posem $n_j = N_j - N_{j+1}$. Aleshores $n_j \geqslant 0$ per a tot $j \geqslant 1$ i existeix $s = s(p) \geqslant 1$ tal que $n_s \geqslant 1$ i que $n_t = 0$ per a tot $t > s$; en efecte, s ve determinat per l'exponent p^s del p-grup abelià $S_p(G)$, $p|n$. Amb aquestes notacions es té que

Lema 9.1.- $S_p(G) = (\mathbb{Z}/p\,\mathbb{Z})^{n_1} \times \ldots \times (\mathbb{Z}/p^s\mathbb{Z})^{n_s}$.

Demostració.- En el cas I per a tot primer p i en el cas II per a tot primer senar, p, resulta que $S_p(G) = \prod_{i=0}^{k} S_p(\mathbb{Z}/e_i\mathbb{Z}) = \prod_{i=0}^{k} (\mathbb{Z}/p^{v_p(e_i)}\mathbb{Z})$, de manera que només cal veure que $n_j =$

$= \#\{e_i : v_p(e_i) = j\}$. Però, per a $j \geqslant 1$, $p^{j-1}G/p^jG =$
$= p^{j-1}S_p(G)/p^jS_p(G)$, i el número N_j de factors $\mathbb{Z}/p\mathbb{Z}$ d'aquest quocient és exactament el número de factors cíclics no nuls de $p^{j-1}S_p(G) = \prod_{i=0}^{k} p^{j-1}(\mathbb{Z}/p^{v_p(e_i)}\mathbb{Z})$; és a dir, el cardinal de $\{e_i : v_p(e_i) > j-1\}$; per tant, $n_j = N_j - N_{j+1}$ és el cardinal de $\{e_i : v_p(e_i) = j\}$, com es volia veure. En el cas II, per a $p = 2$, és $2 = p \in P$, $e_0 > 2$ i $G_0 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/(e_0/2)\mathbb{Z})$; podem posar $\tilde{e}_{-1} = 2$, $\tilde{e}_0 = e_0/2$, $\tilde{e}_i = e_i$, $1 \leqslant i \leqslant k$, i repetir l'argument anterior pels $\tilde{e}_i$, $-1 \leqslant i \leqslant k$ en lloc dels e_i, ja que $S_2(G) = \prod_{i=-1}^{k} S_2(\mathbb{Z}/\tilde{e}_i\mathbb{Z}) = \prod_{i=-1}^{k} (\mathbb{Z}/2^{v_2(\tilde{e}_i)}\mathbb{Z})$.■

En el cas I tots els grups $S_p(G_i)$ són cíclics i podríem aplicar ja el teorema 6.4 de l'apèndix; en canvi, en el cas II, $S_2(G)$ no és cíclic. Es té, però, que si posem $G_0 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/e_0'\mathbb{Z})$, $G_{-1} = \mathbb{Z}/2\mathbb{Z}$, $G_0' = \mathbb{Z}/e_0'\mathbb{Z}$, $G_i = \mathbb{Z}/e_i\mathbb{Z}$, $1 \leqslant i \leqslant k$, i $e_0' = e_0/2$, aleshores:

Lema 9.2.- El conjunt $P(G_{-1}, G_0', G_1, \ldots, G_k)$ és la reunió disjunta de $P(G_0, \ldots, G_k)$ i de $P(H_0, G_1, \ldots, G_k)$, on H_0 és el subgrup de G_0 generat per l'element $(1,1)$.

Demostració.- Siguin $\Pi_i : G \to G_i$, $0 \leqslant i \leqslant k$, les projeccions usuals, i sigui $\Pi_0'' : H_0 \times G_1 \times \ldots \times G_k \to H_0$ la restricció de Π_0. És clar que $P(G_0, \ldots, G_k)$ i $P(H_0, G_1, \ldots, G_k)$ estan inclosos en $P(G_{-1}, G_0', G_1, \ldots, G_k)$; a més a més, els dos conjunts són disjunts, ja que si $X \in P(H_0, G_1, \ldots, G_k)$, aleshores $\Pi_0(X) \subsetneq H_0 \neq G_0$, de manera que $X \notin P(G_0, \ldots, G_k)$. Per altra banda, si $X \in P(G_{-1}, G_0', G_1, \ldots, G_k)$ i $X \notin P(G_0, \ldots, G_k)$, aleshores $\Pi_0(X) \neq G_0$, de manera que $\Pi_0(X)$

està inclòs en algun dels tres subgrups de G_0 d'índex 2: H_0, G_0', G_{-1} x 2 G_0'. Les dues darreres possibilitats s'exclouen considerant les projeccions sobre $G_{\mp 1}$ i sobre G_0', respectivament. Per tant, $\Pi_0(X) \subseteq H_0$. Considerant de nou les projeccions sobre G_{-1} i sobre G_0' s'obté la igualtat $\Pi_0(X) = H_0$, i aleshores $X \in P(H_0, G_1, \ldots, G_k)$. D'on resulta la descomposició de $P(G_{-1}, G_0', G_1, \ldots, G_k)$ com a reunió dels conjunts $P(G_0, \ldots, G_k)$ i $P(H_0, G_1, \ldots, G_k)$.■

Corol.lari 9.3.- En les hipòtesis del lema 9.2 es té que

$$\#P(G_0, \ldots, G_k; n) = \#P(G_{-1}, G_0', G_1, \ldots, G_k; n) -$$
$$- \#P(H_0, G_1, \ldots, G_k; n), \text{ per a tot enter positiu } n.■$$

Amb tot això podem establir, ja, el resultat final. Suposem que la terna $(n, \underline{e}; P)$ verifica les condicions del teorema 5.16. Per a tot primer $p|n$ i per a tot enter $j \geqslant 1$, posem $N_j(p) = \#\{e_i : v_p(e_i) \geqslant j\}$, i sigui $\underline{N}(p)$ el tipus $\underline{N}(p) = (N_1(p), \ldots, N_s(p), \ldots)$. En el cas $p = 2 \in P$, $e_0 = 2^{r_0} > 2$, considerem també els tipus

$$\underline{N}'(2) = (N_1(2)+1, N_2(2), \ldots, N_{r_0}(2)-1, \ldots, N_s(2), \ldots) \text{ i}$$
$$\underline{N}''(2) = (N_1(2), \ldots, N_{r_0}(2)-1, \ldots, N_s(2), \ldots).$$

Amb aquestes notacions es verifica el següent

Teorema 9.4.- Si es verifiquen les condicions $n \mid \prod_{p_i \in P} e_i, \mu \mid n$, i $p_i \equiv 1 \pmod{e_i'}$ per a tot $p_i \in P$, aleshores:

$$a(n,\underline{e};P) = \begin{cases} \prod_{p|n} f_p(\underline{N}(p);v_p(n)) \ , \text{ si } 2 \notin P, \\ 3 \prod_{p|n} f_p(\underline{N}(p);v_p(n)) \ , \text{ si } 2 \in P, e_0 = 2, \\ g(2) \prod_{\substack{p|n \\ p\neq 2}} f_p(\underline{N}(p);v_p(n)) \ , \text{ si } 2 \in P, e_0 = 2^{r_0} > 2, \end{cases}$$

on $g(2) = 2^{-}f_2(\underline{N}(2);v_2(n)) + f_2(\underline{N}'(2);v_2(n)) -$

$- f_2(\underline{N}''(2);\ v_2(n))$.

Demostració.- Sigui L una extensió $(\underline{e};P)$-universal, i sigui $G = Gal(L|Q)$. Aleshores, per a tot primer $p|\#G$ es té que $S_p(G)$ és un p-grup abelià de tipus $\underline{N}(p)$, excepte en el cas II en què $S_2(G)$ és un 2-grup abelià de tipus $\underline{N}'(2)$. Apliquem el teorema 7.6. En el cas $2 \notin P$ és $a(n,\underline{e};P) = a_L(n,\underline{e};P)$, ja que l'extensió $(\underline{e};P)$-universal és única. En el cas $2 \in P$, $e_0 = 2$, les tres extensions $(\underline{e};P)$-universals tenen grups de Galois isomorfs i estan en el cas I, de manera que $a(n,\underline{e};P) = 3\, a_L(n,\underline{e};P)$ per a qualsevol de les tres extensions $(\underline{e};P)$-universals $L|Q$. Per últim, en el cas $2 \in P$, $e_0 > 2$, dues de les tres extensions $(\underline{e};P)$-universals estan en el cas I i la tercera en el cas II. Però, aleshores, el corol.lari 9.3 permet dir que, per a aquesta extensió, és $a_L(n,\underline{e};P) = g'(2) \prod_{\substack{p|n \\ p\neq 2}} f_p(\underline{N}(p);v_p(n))$, on $g'(2) =$

$= f_2(\underline{N}'(2);v_2(n)) - f_2(\underline{N}''(2);v_2(n))$. Com que, en el cas I, $a_L(n,\underline{e};P) = f_2(\underline{N}\ (2);v_2(n)) \prod_{\substack{p|n \\ p\neq 2}} f_p(\underline{N}(p);v_p(n))$, el resultat queda provat.■

CAPÍTOL III.

EXTENSIONS ABELIANES DE Q AMB CONJUNT CRÍTIC AFITAT.

§1.- Introducció i notacions.

El teorema d'Hermite-Minkowski permet assegurar que, si fixem un conjunt finit i no buit de números primers P, i si fixem el grau n, aleshores el conjunt de les extensions de $\mathbb{Q}$ de grau n i no ramificades fora del conjunt P és finit. En aquest capítol estudiem aquest número en el cas abelià.

Sigui P un conjunt finit i no buit de números primers i sigui $\bar{\mathbb{Q}}$ una clausura algebraica de $\mathbb{Q}$. Donat un enter $n \geqslant 1$, posarem

$$\Sigma_{ab}(n;P) = \{K:\mathbb{Q} \subseteq K \subseteq \bar{\mathbb{Q}},\ K|\mathbb{Q} \text{ és abeliana i no ramificada a tot primer finit } p \notin P,\ \text{i } [K:\mathbb{Q}] = n\},$$

i indicarem per $a(n;P)$ el cardinal de $\Sigma_{ab}(n;P)$.

El cardinal $a(n;P)$ es podria obtenir dels resultats del capítol II a partir de sumar els cardinals $a(n,\underline{e}';P')$ per a tots els vectors $\underline{e}'$ possibles i tots els subconjunts $P' \subseteq P$; és més còmode, però, procedir directament. En efecte, per a tot grup abelià finit A, i si $n = \#\, A$, posarem

$$\Sigma(A;P) = \{K:\ K \in \Sigma_{ab}(n;P) \text{ amb } Gal(K|\mathbb{Q}) \simeq A\},$$

i denotarem per $a(A;P)$ el seu cardinal.

Clarament, el conjunt $\Sigma_{ab}(n;P)$ és la reunió disjunta dels conjunts $\Sigma(A;P)$ quan A recorre un sistema de representants de les classes d'isomorfia de grups abelians finits d'or

dre n. Això fa que $a(n;P)$ sigui la suma dels $a(A;P)$ i que, per tant, l'estudi de $\Sigma_{ab}(n;P)$ es redueixi a l'estudi dels conjunts $\Sigma(A;P)$.

Introduïm la funció generatriu de Dirichlet dels nú<u>me</u>ros $a(n;P)$; per a estudiar aquesta funció és còmode conèixer exactament quins són els valors de n pels quals $a(n;P) \neq 0$. Si bé això es pot conèixer directament a partir de la fórmula que els calcula, és més suggerent utilitzar els resultats del cap<u>í</u>tol II relatius a les extensions $(\underline{e};P)$-universals. Via aquests resultats s'obté una caracterització fàcil dels valors de n tals que $a(n;P) \neq 0$, i una extensió $L|\mathbb{Q}$ on hi ha inclosos tots els cossos $K \in \Sigma_{ab}(n;P)$.

Per a acabar, la suma dels factors d'Euler de la funció generatriu dels $a(n;P)$ permet estendre aquesta funció a una funció meromorfa de tot el pla complex amb un únic pol d'<u>or</u>dre $\#P$ en $t = 0$.

§2.- El càlcul de a(A;P).

Sigui P un conjunt finit i no buit de números primers, i sigui A un grup abelià qualsevol. En aquest § es fa el càlcul de $a(A;P)$.

Per a tot primer ℓ , posem $S_\ell(A)$ l'únic ℓ-subgrup de Sylow de A; el fet que $A \simeq \bigoplus_\ell S_\ell(A)$ fa que puguem establir una bijecció entre els conjunts $\Sigma(A;P)$ i $\prod_\ell \Sigma(S_\ell(A);P)$, prenent com a imatge de tot cos $K \in \Sigma(A;P)$ la família $\{K_\ell\}_\ell$ on K_ℓ és la ℓ-subextensió maximal de $K|Q$. En conseqüència, caracteritzar $\Sigma(A;P)$ equival a caracteritzar $\Sigma(S_\ell(A);P)$ per a tot primer ℓ. Això redueix el problema al cas dels ℓ-grups abelians finits.

Sigui $Q_{ab}^{P}|Q$ l'extensió abeliana maximal de Q no ramificada a tot primer finit $p \notin P$. En virtut del teorema de Kronecker-Weber (cf.[Ne 1: cap. III,§3, teor. 3.8]) es té que Q_{ab}^{P} s'obté de Q per l'adjunció de totes les arrels m-èsimes de la unitat amb m només divisible pels primers $p \in P$. Així, Q_{ab}^{P} és el cos composició de la família d'extensions linealment disjuntes $Q_{ab}^{\{p\}}|Q$ per a tots els primers $p \in P$. Com que $Q_{ab}^{\{p\}}$ és la reunió dels cossos $Q(\zeta)$ amb ζ una arrel primitiva p^r-èsima de la unitat, $r \geq 1$, i com que

$$\mathrm{Gal}(Q(\zeta)|Q) \simeq \begin{cases} \mathbb{Z}/p^{r-1}(p-1)\mathbb{Z} & \text{si } p \neq 2, \\ (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/2^{r-2}\,\mathbb{Z}) & \text{si } p = 2, \end{cases}$$

resulta que $\mathrm{Gal}(Q_{ab}^{\{p\}}|Q)$ és isomorf al grup abelià profinit $\mathbb{Z}_p \times (\mathbb{Z}/(p-1)\mathbb{Z})$ si $p \neq 2$, i a $\mathbb{Z}_2 \times (\mathbb{Z}/2\,\mathbb{Z})$ si $p = 2$. En conseqüència, es té que

$$\mathrm{Gal}(\mathbb{Q}_{ab}^{P}\,|\mathbb{Q}) = \begin{cases} \prod_{p\in P} \mathbb{Z}_p \times \prod_{p\in P} (\mathbb{Z}/(p-1)\mathbb{Z}) & \text{si } 2\notin P, \\ \prod_{p\in P} \mathbb{Z}_p \times \prod_{p\in P} (\mathbb{Z}/(p-1)\mathbb{Z}) \times (\mathbb{Z}/2\,\mathbb{Z}) & \text{si } 2\in P. \end{cases}$$

Si ℓ és un primer qualsevol, la ℓ-extensió abeliana maximal de $\mathbb{Q}$ no ramificada fora de P és la ℓ-subextensió maximal de $\mathbb{Q}_{ab}^{P}$ i, per tant, el seu grup de Galois, que denotarem per $G_\ell(P)$, és isomorf al ℓ-subgrup de Sylow del grup profinit $\mathrm{Gal}(\mathbb{Q}_{ab}^{P}\,|\mathbb{Q})$. Es verifica immediatament el següent

Lema 2.1.- Sigui ℓ un número primer. Aleshores:

$$G_\ell(P) \simeq \begin{cases} \mathbb{Z}_\ell \times \prod_{p\in P} \mathbb{Z}/\ell^{v_\ell(p-1)}\mathbb{Z} & \text{si } \ell\in P, \ell\neq 2, \\ \mathbb{Z}_2 \times \prod_{p\in P} \mathbb{Z}/2^{v_2(p-1)}\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z} & \text{si } \ell = 2\in P, \\ \prod_{p\in P} \mathbb{Z}/\ell^{v_\ell(p-1)}\mathbb{Z} & \text{si } \ell\notin P. \blacksquare \end{cases}$$

Siguin, doncs, ℓ un primer i A un ℓ-grup abèlià finit. Es tracta de caracteritzar el conjunt $\Sigma(A;P)$. Denotem per $X(G_\ell(P);A)$ el conjunt de tots els subgrups (oberts) $H \subsetneq G_\ell(P)$ tals que $G_\ell(P)/H \simeq A$. La teoria de Galois pel cas infinit (cf. [Ne 1; cap. 1, §1]) permet deduir de seguida la següent

Proposició 2.2.- Existeix una bijecció entre $\Sigma(A;P)$ i $X(G_\ell(P);A)$.$\blacksquare$

Observació 1.- Aquest resultat es pot establir, de manera equi valent, en els següents termes:

> Denotem per $\mathrm{Hom}_{exh}(G_\ell(P);A)$ el conjunt dels homomorfismes continus i exhaustius del grup profinit $G_\ell(P)$ en el grup finit A. Aleshores, $\mathrm{Hom}_{exh}(G_\ell(P);A) = a(A;P)\,\#\,\mathrm{Aut}(A)$.

Però comptar els morfismes es redueix al mateix problema de grups finits a què es redueix el càlcul de $X(G_\ell(P);A)$ (veure més avall).

De manera que el problema es redueix a caracteritzar el conjunt $X(G_\ell(P);A)$. Com que A és un ℓ-grup abelià finit, existeix $r \geqslant 1$ tal que $\ell^r A = 0$. Aleshores, si $H \in X(G_\ell(P);A)$, és $G_\ell(P)/H \simeq A$, de manera que $\ell^r G_\ell(P) \subseteq H$. Per tant, la bijecció entre el conjunt dels subgrups de $G_\ell(P)$ que contenen $\ell^r G_\ell(P)$ i el conjunt dels subgrups de $G_\ell(P)/\ell^r G_\ell(P)$ dóna una bijecció entre $\Sigma(A;P)$ i el conjunt dels subgrups de $G_\ell(P)/\ell^r G_\ell(P)$ que donen quocient isomorf a A, per a tot $r \geqslant 1$ tal que $\ell^r A = 0$. Com que P és finit, podem elegir r com el mínim enter $r \geqslant 1$ tal que $\ell^r A = 0$ i que $r \geqslant v_\ell(p-1)$ per a tot $p \in P$; per a aquest valor de r, posem

$$H_\ell(P;A) = G_\ell(P)/\ell^r G_\ell(P).$$

Lema 2.3.- Amb les notacions anteriors es verifica que

$$H_\ell(P;A) \simeq \begin{cases} \mathbb{Z}/\ell^r\mathbb{Z} \times \prod_{p \in P} \mathbb{Z}/\ell^{v_\ell(p-1)}\mathbb{Z} & \text{si } \ell \in P,\ \ell \neq 2 \\ \mathbb{Z}/2^r\mathbb{Z} \times \prod_{p \in P} \mathbb{Z}/2^{v_2(p-1)}\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z} & \text{si } \ell = 2 \in P \\ \prod_{p \in P} \mathbb{Z}/\ell^{v_\ell(p-1)}\mathbb{Z} & \text{si } \ell \notin P. \end{cases}$$

Demostració.- Només cal aplicar el lema 2.1 i tenir en compte que $\mathbb{Z}_\ell/\ell^r\mathbb{Z}_\ell \simeq \mathbb{Z}/\ell^r\mathbb{Z}$ i que, per ser $r \geqslant v_\ell(p-1)$, és $\ell^r(\mathbb{Z}/\ell^{v_\ell(p-1)}\mathbb{Z}) = 0$, per a tot $p \in P$.■

Així, el problema de calcular $a(A;P)$ ha quedat reduït al problema de calcular el número de subgrups del grup finit $H_\ell(P;A)$ que donen quocient isomorf a A. Sigui, doncs, G un ℓ-grup abelià finit qualsevol. Aleshores, podem escriure G en la forma

$$G \simeq (\mathbb{Z}/\ell\ \mathbb{Z})^{n_1} \times (\mathbb{Z}/\ell^2\mathbb{Z})^{n_2} \times \ldots \times (\mathbb{Z}/\ell^s\mathbb{Z})^{n_s},$$

amb els $n_1,\ldots,n_s \geqslant 0$. Posem $N_i = n_i + \ldots + n_s$ si $1 \leqslant i \leqslant s$, $N_i = 0$ si $i > s$, i sigui $\underline{N} = (N_1,\ldots,N_s,0,\ldots)$; direm que G és un ℓ-grup abelià finit de tipus $\underline{N}$. Si $\underline{M}$ és el tipus d'un altre ℓ-grup abelià finit, denotarem per $H(G;\underline{M})$ el conjunt dels subgrups de G de tipus $\underline{M}$ i per $h(G;\underline{M})$ el cardinal de $H(G;\underline{M})$ (cf. apèndix, §1). Si considerem el dual de G, $\hat{G} = \mathrm{Hom}(G,C^*)$, resulta que G és isomorf (no canònicament) a $\hat{G}$; aleshores, l'isomorfisme de $H_\ell(P;A)$ amb el seu dual permet demostrar fàcilment que hi ha una bijecció entre el conjunt dels subgrups de $H_\ell(P;A)$ que donen quocient isomorf a A i el conjunt $H(H_\ell(P;A);\underline{M})$, on $\underline{M}$ és el tipus del ℓ-grup abelià finit A (cf. cap II, §7, lema 7.4). De manera que a partir de la proposició 2.2 s'obté que $a(A;P) = h(H_\ell(P;A);\underline{M})$.

Si $\underline{M}$, $\underline{N}$, són tipus de ℓ-grups abelians finits, posarem $\underline{M} \leqslant \underline{N}$ si, i només si, $M_i \leqslant N_i$ per a tot $i \geqslant 1$. El teorema 6.1 de l'apèndix dóna el valor exacte de $h(G;\underline{M})$ per a tot ℓ-grup abelià finit G de tipus $\underline{N}$ i tot tipus $\underline{M} \leqslant \underline{N}$. Com a conseqüència, es té que:

Teorema 2.4.- Sigui A un ℓ-grup abelià finit de tipus $\underline{M}$, i sigui P un conjunt finit i no buit de números primers. Sigui $\underline{N} = (N_1,\ldots,N_s,0\ldots)$ el tipus del ℓ-grup abelià finit $H_\ell(P;A)$. Aleshores, si $\underline{M} \not\leqslant \underline{N}$ és $a(A;P) = 0$, i si $\underline{M} \leqslant \underline{N}$ és

$$a(A;P) = \ell^{\gamma(\underline{M})} \prod_{i=1}^{r} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_\ell$$

on $\gamma(\underline{M}) = \sum_{i=1}^{r} M_{i+1}\,(N_i - M_i)$. ■

§3.- El càlcul de $a(n;P)$.

En aquest § calculem $a(n;P)$ per a tot enter $n \geqslant 1$ i tot conjunt finit i no buit P de números primers. El primer problema consisteix a caracteritzar quan el conjunt $\Sigma_{ab}(n;P)$ és no buit. Es té el resultat següent:

Proposició 3.1.- El conjunt $\Sigma_{ab}(n;P)$ és no buit si, i només si, per a tot primer $\ell \mid n$ es verifiquen les condicions

(i) $\ell \in P$ ò bé existeix $p \in P$ tal que $p \equiv 1 \pmod{\ell}$,

(ii) si $\ell \notin P$ i per a tot $p \in P$ posem $s_p = v_\ell(p-1)$, aleshores $v_\ell(n) \leqslant \sum_{p \in P} s_p$.

Demostració.- Suposem que $\Sigma_{ab}(n;P)$ és no buit i sigui $K \in \Sigma_{ab}(n;P)$; sigui $\ell \mid n$ un primer. Per a tot primer $p \in P$ posem $e_p = e_p(K|Q)$ i escrivim $e_p = p^{r_p} e'_p$ amb $p \nmid e'_p$; siguin $\mu = \text{m.c.m.}\{e_p : p \in P\}$, $e = \prod_{p \in P} e_p$. Aleshores, en virtut del teorema 5.16 del capítol II, resulta que $\mu \mid n$, que $n \mid e$ i que $e'_p \mid p-1$ per a tot $p \in P$. De $\ell \mid n$, $n \mid e$, resulta que $\ell \mid e$ i, per tant, $\ell \mid e_p$ per a algun $p \in P$; així, ò bé $\ell \in P$ ò bé $\ell \mid p-1$ per a algun $p \in P$; per altra banda, si $\ell \notin P$ resulta que $v_\ell(n) \leqslant v_\ell(e) = \sum_{p \in P} v_\ell(e_p) \leqslant \sum_{p \in P} v_\ell(p-1) = \sum_{p \in P} s_p$, com volíem veure.

Recíprocament, com que les extensions són abelianes, és suficient veure que $\Sigma_{ab}(\ell^{v_\ell(n)}; P)$ és no buit per a tot primer $\ell \mid n$. Ara bé, per a tot ℓ i per a tot $r \geqslant 0$ resulta que

$\Sigma_{ab}(\ell^r,\ell^r;\{\ell\})$ és no buit, de manera que si $\ell \in P$, el conjunt $\Sigma_{ab}(\ell^{v_\ell(n)};P)$ és no buit. Suposem, doncs, que $\ell \notin P$. Per a tot $p \in P$ posem $\varepsilon_p = \min_{\varepsilon_p} \{v_\ell(n), s_p = v_\ell(p-1)\}$, i sigui $\underline{\varepsilon}$ el vector de components p^{ε_p}. De la condició $v_\ell(n) \leqslant \sum_{p \in P} s_p$, resulta que $\Sigma_{ab}(\ell^{v_\ell(n)}, \underline{\varepsilon};P)$ és no buit (cf. cap II, §8, teor. 8.7), de manera que $\Sigma_{ab}(\ell^{v_\ell(n)};P) \neq \phi$, com volíem veure.■

Podem reduir el problema del càlcul de $a(n;P)$ al cas de les ℓ-extensions, ja que $a(n;P) = \prod_{\ell|n} a(\ell^{v_\ell(n)};P)$. A partir d'ara, doncs, suposarem que $n = \ell^s$.

Per a tot enter $j \geqslant 1$ posem $T_j = \{p \in P: p = \ell$ ò $p \equiv 1(\text{mòd } \ell^j)\}$ $N_j = \# T_j$, i $n_j = N_j - N_{j+1}$. Aleshores, es té que els T_j formen una successió decreixent.

$$P \supseteq T_1 \supseteq T_2 \supseteq \dots \supseteq T_s \supseteq \dots ,$$

que $n_j = \#(T_j - T_{j+1})$, i que $n_j = 0$ per a $j >> 0$. Numerem els primers $p \in P$ de manera que per a tot $j \geqslant 1$ sigui $T_j = \{p_1,\dots,p_{N_j}\}$. En particular, si $\ell \in P$ serà $T_j = \{\ell\}$per a $j >> 0$ i, en conseqüència, tindrem que $p_1 = \ell$. Amb aquestes notacions es verifica que

Proposició.3.2.- $\Sigma_{ab}(\ell^s;P) = \Sigma_{ab}(\ell^s; T_1)$.

Demostració.- Immediata, ja que si $K \in \Sigma_{ab}(\ell^s;P)$ i $p \in P$, $p \notin T_1$, aleshores $p \neq \ell$, $\ell \nmid p-1$, de manera que $e_p(K|Q) = 1$ (cf. cap. II, §5, teor. 5.16).■

La proposició 3.1 dóna, en aquest cas, que $\Sigma_{ab}(\ell^s;P)$ és no buit si, i només si, $s \leqslant N_1 + \ldots + N_s + \ldots$. Amb tot això, podem demostrar, ja, el següent

Teorema 3.3.- a) Si $\ell \neq 2$, ò si $\ell = 2 \notin P$, hi ha una bijecció entre el conjunt $\Sigma_{ab}(\ell^s;P)$ i el conjunt de tots els subgrups d'ordre ℓ^s del ℓ-grup abelià finit $G = (\mathbb{Z}/\ell\,\mathbb{Z})^{n_1} \times \ldots \times (\mathbb{Z}/\ell^{s-1}\mathbb{Z})^{n_{s-1}} \times (\mathbb{Z}/\ell^s\mathbb{Z})^{N_s}$.

b) Si $\ell = 2 \in P$, hi ha una bijecció entre $\Sigma_{ab}(2^s;P)$ i el conjunt de tots els subgrups d'ordre 2^s del 2-grup abelià finit $G = (\mathbb{Z}/2\,\mathbb{Z})^{n_1+1} \times (\mathbb{Z}/4\,\mathbb{Z})^{n_2} \times \ldots \times (\mathbb{Z}/2^{s-1}\mathbb{Z})^{n_{s-1}} \times (\mathbb{Z}/2^s\,\mathbb{Z})^{N_s}$.

Demostració.- a) Podem suposar, en virtut de la proposició 3.2, que $P = T_1$. Per a tot $p_i \in P$ sigui $j = j(i)$ l'únic enter tal que $p_i \in T_j - T_{j+1}$, si $p \neq \ell$ i $v_\ell(p-1) \leqslant s$, i sigui $j = s$ si $p = \ell$ ò si $v_\ell(p-1) \geqslant s$. Sigui $Q(\theta_i)|Q$ l'única extensió abeliana de grau ℓ^j i no ramificada fora de $\{p_i\}$. És a dir, per a tot $p_i \in P$ considerem l'extensió $(\ell^j;\{p_i\})$-universal pel màxim $j \leqslant s$ possible (cf. cap II, §5). Com que $\ell \neq 2$, ò $\ell = 2 \notin P$, aquesta extensió és única per a tot $p_i \in P$. Posem també $L = Q(\theta_1;\ldots,\theta_{N_1})$. Sigui $K \in \Sigma_{ab}(\ell^s;T_1)$; si posem $\underline{e} = (\ldots,e_i,\ldots)$ on $e_i = e_{p_i}(K|Q)$, resulta que $Q(\theta_i)$ conté l'extensió $(e_i;\{p_i\})$-universal, de manera que L conté l'extensió $(\underline{e};T_1)$-universal i, per tant, $K \subseteq L$. Així, hi ha bijecció entre $\Sigma_{ab}(\ell^s;T_1)$ i el conjunt dels subcossos de grau ℓ^s de L. Però $L|Q$ és abeliana i $Gal(L|Q) \simeq G$. Només cal tenir en compte, ara, que el número de subgrups de G d'índex

ℓ^s és el mateix que el número de subgrups de G d'ordre ℓ^s.

b) En el cas $\ell = 2 \in P$ tot va de la mateixa manera excepte que cal canviar l'extensió $Q(\theta_1)|Q$, que correspon al primer $\ell = 2$, per la composició de les tres extensions $(2^s;\{2\})$-universals, que és $Q(\theta_1)|Q$ amb θ_1 una arrel primitiva 2^{s+2}-èsima de la unitat.■

Aquest teorema permet escriure ja el valor de $a(\ell^r;P) = a(\ell^r;T_1)$. En efecte, si apliquem el teorema 6.2 de l'apèndix als grups G del teorema 3.3 obtenim que

Teorema 3.4.- Posem, per a $1 \leqslant j \leqslant s$, $N_j = \# T_j$, excepte en el cas $\ell = 2 \in P$, $j = 1$, en què posem $N_1 = 1 + \# T_1$. Aleshores:

$$a(\ell^s;P) = \sum_{\underline{M}} \ell^{\gamma(\underline{M})} \prod_{i=1}^{s} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_\ell$$

on $\gamma(\underline{M}) = \sum_{i=1}^{s} M_{i+1}(N_i - M_i)$ i la suma s'estén a tots els tipus $\underline{M} = (M_1,\ldots,M_s,0,\ldots)$ tals que $M_1 + \ldots + M_s = s$, i que $M_i \leqslant N_i$ per a $1 \leqslant i \leqslant s$.■

§4.- La funció generatriu de $a(n;P)$.

Podem, ara, definir la funció generatriu de Dirichlet dels números d'extensions abelianes de $\mathbb{Q}$ de grau n i no ramificades fora de P:

$$G(P;t) = \sum_{n \geqslant 1} a(n;P)\ n^{-t}.$$

El primer problema consisteix a determinar algun semiplà on la sèrie sigui convergent. Es té la següent

Proposició 4.1.- Sigui P un conjunt finit i no buit de números primers, i sigui ℓ un primer qualsevol. Aleshores,

$$a(\ell^s;P) \leqslant \ell^{(5+\#P)s}.$$

Demostració.- Observem la fórmula del teorema 3.4. Els factors de $\begin{bmatrix} N_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_\ell$ admeten la següent afitació:

$$\frac{\ell^{N_i-M_i+j}-1}{\ell^j-1} = \ell^{N_i-M_i} + \frac{\ell^{N_i-M_i}-1}{\ell^j-1} \leqslant 2\,\ell^{N_i-M_i};$$

de manera que

$$\begin{bmatrix} N_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_\ell \leqslant 2^{M_i-M_{i+1}}\ \ell^{(M_i-M_{i+1})(N_i-M_i)}$$

i, per tant,

$$\prod_{i=1}^{s} \begin{bmatrix} N_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_\ell \leqslant 2^{M_1}\ \ell^{\sum_{i=1}^{s}(M_i-M_{i+1})(N_i-M_i)}.$$

Així, cada sumand de $a(\ell^s;P)$ admet la fita

$$2^{M_1} \quad \ell^{\sum_{i=1}^{s} M_i(N_i-M_i)} .$$

Com que $\sum_{i=1}^{s} M_i^2 \geqslant \sum_{i=1}^{s} M_i = s$, i $\sum_{i=1}^{s} M_iN_i \leqslant N_1 s$, resulta que

$$\sum_{i=1}^{s} M_i(N_i-M_i) \leqslant (N_1-1)s \leqslant s\ \#P$$

en tots els casos, ja que $N_1 \leqslant 1 + \#P$. Per tant, cada sumand de $a(\ell^s;P)$ és menor ò igual que

$$2^{M_1}\ \ell^{s\#P} \leqslant 2^s\ \ell^{s\#P} \leqslant \ell^{(1+\#P)s} .$$

Ara bé, la suma s'estén a una família de particions restringides de s, de manera que el número de sumands està afitat per

$$e^{\pi\sqrt{2/3}\ \sqrt{s}} \leqslant 2^{4\sqrt{s}} \leqslant \ell^{4s}$$

(cf.[Ap 1: cap. 14, §7, teor. 14.5]). Per tant,

$$a(\ell^s;P) \leqslant \ell^{(1+\#P)s}\ \ell^{4s} = \ell^{(5+\#P)s} ,$$

com volíem veure.■

Corol.lari 4.2.- Sigui P un conjunt finit i no buit de números primers, i sigui $n \geqslant 1$, un enter. Aleshores $a(n;P) \leqslant n^{5+\#P}$.

Demostració.- Immediata, ja que $a(n;P)$ és una funció multiplicativa.■

Aquest resultat implica que $G(P;t)$ defineix una funció analítica en el semiplà $\mathrm{Re}(t) > 6 + \#P$, i admet la descomposició en producte d'Euler

$$G(P;t) = \prod_{\ell} \sum_{r \geqslant 0} a(\ell^r;P)\, \ell^{-rt}$$

(cf. cap. I, §7).

El pas següent consisteix a calcular els factors d'Euler. Per a començar, observem que si $\ell \notin P$ i si $\ell \nmid p-1$ per a cap primer $p \in P$, aleshores $a(\ell^r;P) = 0$ per a tot $r \geqslant 1$ (cf. prop. 3.1), de manera que el factor d'Euler de $G(P;t)$ que correspon al primer ℓ és

$$C_\ell(P;t) = 1.$$

Amb això, es té que $G(P;t)$ és un producte finit de factors d'Euler.

Per altra banda, si $\ell \notin P$ però $\ell \mid p-1$ per a algun $p \in P$, posem $N_i = \#\{p \in P:\ p \equiv 1 \pmod{\ell^i}\}$, per a tot $i \geqslant 1$. Aleshores, existeix un s màxim tal que $N_s \neq 0$ i, en virtut dels resultats del §3, per a $r > s$ és $a(\ell^r;P) = 0$. De manera que el factor d'Euler que correspon al primer ℓ és la suma finita

$$C_\ell(P;t) = \sum_{r=0}^{s} a(\ell^r;P)\, \ell^{-rt}\ .$$

Aquesta suma defineix una funció analítica de tot el pla complex. Com que $a(\ell^r;P) \geqslant 0$ i $a(1;P) = 1$, resulta que $C_\ell(P;0) \geqslant 1$; en particular, $C_\ell(P;t)$ no s'anul.la en $t = 0$.

Estudiem ara el cas $\ell \in P$. Posem $N_i = 1 + \#\{p \in P: p \equiv 1 \pmod{\ell^i}\}$ per a tot $i \geqslant 1$, excepte en el cas $\ell = 2 \in P$, $i = 1$, en què posarem $N_1 = 1 + \#P = 2 + \#\{p \in P:\ p \equiv 1 \pmod 2\}$. Com abans, existeix un mínim valor de s tal que $N_{s+h} = 1$ per a tot $h \geqslant 0$. Si apliquem el teorema 3.4 obtenim que, per a tot $r \geqslant 1$, és

$$\ell^{-rt}\, a(\ell^r;P) = \sum_{\underline{M}} \ell^{\gamma_{\underline{M}}(t)} \prod_{i=1}^{r} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_\ell$$

on $\gamma_{\underline{M}}(t) = \sum_{i=1}^{r} M_{i+1}(N_i-M_i) - t \sum_{i=1}^{r} M_i$, i el sumatori estès a tots els tipus $\underline{M} = (M_1,\dots,M_r,0,\dots) \leqslant \underline{N} = (N_1,\dots,N_s,1,\dots,1,\dots)$ tals que $M_1 +\dots+ M_r = r$.

Observem que el número de sumands creix quan creix r. Però, si $i \geqslant s$, aleshores $N_i = 1$; això fa que $M_i \leqslant 1$, de manera que si $M_{i+1} = 1$, aleshores $M_i = 1$ i $M_{i+1}(N_i-M_i) = 0$. A més a més, per a $i \geqslant s$, és

$$\begin{bmatrix} N_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_{\ell} = 1 ,$$

ja que, si $M_i = M_{i+1}$, és un producte buit, i si $M_{i+1} = 0$, $M_i = 1$, és $N_i = M_i$. En qualsevol cas, doncs, el límit superior del producte, r, es pot substituir per s - 1, i $\gamma_{\underline{M}}(t)$ es pot substituir per l'expressió

$$\gamma_{\underline{M}}(t) = \sum_{i=1}^{s-1} M_{i+1}(N_i-M_i) - t \sum_{i \geqslant 1} M_i .$$

Per tant, el factor d'Euler de $G(P;t)$ que correspon al primer $\ell \in P$ és

$$\sum_{r \geqslant 0} \ell^{-rt}\, a(\ell^r;P) = \sum_{\underline{M}} \ell^{\gamma_{\underline{M}}(t)} \prod_{i=1}^{s-1} \begin{bmatrix} N_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_{\ell} ,$$

on $\gamma_{\underline{M}}(t) = \sum_{i=1}^{s-1} M_{i+1}(N_i-M_i) - t \sum_{i \geqslant 1} M_i$, i la suma estesa a totes les successions decreixents $M_1 \geqslant M_2 \geqslant\dots\geqslant M_r \geqslant\dots$, nulles d'un lloc endavant, i tals que $M_i \leqslant N_i$ per a tot $i \geqslant 1$.

Degut a la convergència absoluta en $\mathrm{Re}(t) > 6 + \#P$, podem reordenar els termes de la sèrie com ens plagui (de fet, ja ho hem fet). Així, podem partir les successions $\underline{M}$ en dues classes: per una banda, aquelles que tenen $M_s = 0$, i per l'altra, les que tenen $M_s = 1$. De successions $\underline{M}$ amb $M_s = 0$, n'hi

ha un número finit, i podem considerar la suma

$$A_\ell(P;t) = \sum_{\underline{M}''} \ell^{\gamma_{\underline{M}''}(t)} \prod_{i=1}^{s-1} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_\ell ,$$

on $\gamma_{\underline{M}''}(t) = \sum_{i=1}^{s-1} M_{i+1}(N_i - M_i) - t \sum_{i=1}^{s-1} M_i$, i la suma estesa a tots els $\underline{M}'' = (M_1, \ldots, M_s)$ amb $M_1 \geqslant \ldots \geqslant M_s = 0$, i $M_i \leqslant N_i$ per a tot i. Aleshores, $A_\ell(P;t)$ defineix una funció analítica de tot el pla complex.

Per altra banda, les successions $\underline{M}$ tals que $M_s = 1$ es poden partir, encara, en un número finit de classes: dues, $\underline{M}$, $\underline{M}'$, estan a la mateixa classe si, i només si, $M_i = M'_i$ per a $1 \leqslant i \leqslant s$. Aleshores, cada classe està formada per les successions $\underline{M}' = (M_1, \ldots, M_{s-1}, M_s=1, M_{s+1}, \ldots, M_{s+h}=1, 0, \ldots)$ quan $h \geqslant 0$, i els $M_1, \ldots, M_{s-1}, M_s=1$, són constants a cada classe. Així, a cada classe, els factors

$$\prod_{i=1}^{s-1} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_\ell ,$$

$$\ell^{\sum_{i=1}^{s-1} M_{i+1}(N_i - M_i) - t \sum_{i=1}^{s} M_i} ,$$

són constants, i la suma dels termes de la classe és el producte d'aquests dos factors per la sèrie

$$\sum_{h \geqslant 0} \ell^{-ht} = (1-\ell^{-t})^{-1} ;$$

de manera que, si posem

$$B_\ell(P;t) = \sum_{\underline{M}'} \ell^{\gamma_{\underline{M}'}(t)} \prod_{i=1}^{s-1} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_\ell ,$$

amb $\gamma_{\underline{M}'}(t) = \sum_{i=1}^{s-1} M_{i+1}(N_i - M_i) - t \sum_{i=1}^{s} M_i$, i la suma estesa a totes les famílies finites $\underline{M}' = (M_1, \ldots, M_s)$ amb $M_1 \geqslant M_2 \geqslant \ldots \geqslant M_s = 1$, $M_i \leqslant N_i$ per a $1 \leqslant i \leqslant s$, el factor d'Euler de $G(P;t)$ que correspon al primer $\ell \in P$ és el producte del factor $(1-\ell^{-t})^{-1}$ pel factor

$$C_\ell(P;t) = B_\ell(P;t) + (1-\ell^{-t})\, A_\ell(P;t).$$

Observem que $B_\ell(P;t)$ és una suma finita i que defineix una funció analítica de tot el pla complex que no s'anul.la en $t = 0$. En conseqüència, com que $(1-\ell^{-t})^{-1}$ defineix una funció meromorfa del pla complex amb un únic pol simple en $t = 0$, obtenim els següents

Teorema 4.3.- La funció generatriu de Dirichlet dels números $a(n;P)$ es pot escriure, en el semiplà $\mathrm{Re}(t) > 6 + \#P$, en la forma

$$G(P;t) = \prod_{\ell \in P} (1-\ell^{-t})^{-1} \prod_{\ell} C_\ell(P;t).$$

Les funcions $C_\ell(P;t)$ són funcions analítiques de tot el pla complex, i $C_\ell(P;t) = 1$ quan $\ell \notin P$ i $\ell \nmid p-1$ per a cap primer $p \in P$. ■

Teorema 4.4.- La funció $G(P;t)$ es pot estendre a una funció meromorfa de tot el pla complex amb un únic pol en $t = 0$, d'ordre $\#P$. ■

APÈNDIX.

SUBGRUPS D'UN p-GRUP ABELIÀ FINIT.

§1.- Introducció i notacions.

L'objectiu d'aquest apèndix és, essencialment, el càlcul del número de subgrups d'un grup abelià finit que satisfan certes condicions.

Sigui p un número primer i sigui G un p-grup abelià finit. Aleshores, existeix $s \geqslant 0$ i existeixen enters no negatius $n_1, n_2, \ldots, n_s$, tals que, tret d'isomorfisme, podem escriure G en la forma

$$G = (\mathbb{Z}/p\,\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times \ldots \times (\mathbb{Z}/p^s\mathbb{Z})^{n_s}.$$

Els successius quocients $p^{i-1}G/p^iG$, $i \geqslant 1$, són els p-quocients elementals de G; són $\mathbf{F}_p$-espais vectorials de dimensió finita, N_i. No és gens difícil comprovar que $N_i = n_i + \ldots + n_s$, $1 \leqslant i \leqslant s$, i que $N_i = 0$ per a tot $i > s$ (cf. cap II, §9, lema 9.1); de manera que el coneixement dels N_i equival al dels n_i i, per tant, al coneixement de G.

Clàssicament (cf.[Bu 1: cap. VII, §81]) es definia el tipus de G com el vector $(s,\overset{n_s)}{\ldots},s,s-1,\overset{n_{s-1})}{\ldots},s-1,\ldots,2,\overset{n_2)}{\ldots},2,1,\overset{n_1)}{\ldots},1)$. La possibilitat que algun n_i sigui zero fa que treballar amb aquesta definició sigui bastant enutjós, sobre tot a l'hora de comparar diferents p-grups abelians finits.

Sigui s el màxim natural $s \geqslant 0$ tal que $n_s > 0$; aleshores, podríem definir el tipus de G en la forma $(n_1, \ldots, n_s)$ ò

en la forma equivalent $(N_1,\ldots,N_s)$ (cf.[Dy 1]); això té la mateixa dificultat que la definició clàssica: el valor de s que correspon a dos p-grups abelians finits pot ésser diferent, de manera que els vectors són de longituds diferents. Si, per a poder-los comparar, igualem les longituds tot afegint zeros a un en la forma $(n_1,\ldots,n_s,0,\ldots 0)$, resulta que el vector no queda unívocament determinat. Però aquesta dificultat desapareix si posem $n_i = N_i = 0$ per a tot $i > s$, amb la següent

Definició.- Posarem $\underline{N} = (N_1,\ldots,N_s,N_{s+1},\ldots)$ i direm que G és un p-grup abelià de tipus $\underline{N}$.

D'aquesta manera, el tipus d'un p-grup abelià finit és una successió decreixent de números naturals, nul.la d'un lloc endavant, i que el determina a menys d'isomorfismes. Observem que el valor de s queda determinat per l'exponent, p^s, de G, que $\sum_{i \geqslant 1} N_i = N_1 +\ldots+ N_s = n_1 + 2n_2 +\ldots+ sn_s$, i que G és d'ordre $p^{N_1+\ldots+N_s}$.

Sigui X_0 un p-grup abelià finit de tipus $\underline{M}$. Veurem a la proposició 2.1 que G conté un subgrup de tipus $\underline{M}$ si, i només si, per a tot natural $i \geqslant 1$ es verifica $M_i \leqslant N_i$, fet que indicarem per $\underline{M} \leqslant \underline{N}$. Si posem $\underline{M} + \underline{N}$ el vector de components $N_i + M_i$, $i \geqslant 1$, és immediat comprovar que $G \times X_0$ és de tipus $\underline{N} + \underline{M}$.

Sigui $H(G;\underline{M})$ el conjunt format per tots els subgrups $X \subseteq G$ de tipus $\underline{M}$, i posem $h(G;\underline{M})$ el seu cardinal. En aquest apèndix es tracta de resoldre els problemes següents:

Problema 1.- Calcular $h(G;\underline{M})$.

Problema 2.- Donat $0 \leqslant v \leqslant N_1 + \ldots + N_s$, calcular el número de subgrups de G d'ordre p^v.

El grup G és el producte de n_r factors $\mathbb{Z}/p^r\mathbb{Z}$, $1 \leqslant r \leqslant s$; indicarem per $\Pi_{r,u}: G \to \mathbb{Z}/p^r\mathbb{Z}$, $1 \leqslant u \leqslant n_r$, $1 \leqslant r \leqslant s$, la projecció usual de G en el u-èsim dels factors $\mathbb{Z}/p^r\mathbb{Z}$, i per $\underline{n}$ el conjunt de les parelles (r,u), $1 \leqslant u \leqslant n_r$, $1 \leqslant r \leqslant s$.

Problema 3.- Calcular el número de subgrups $X \subseteq G$ de tipus $\underline{M}$ tals que per a tot $(r,u) \in \underline{n}$ es verifica que $\Pi_{r,u}(X) = \mathbb{Z}/p^r\mathbb{Z}$.

Problema 4.- Calcular el número de subgrups $X \subseteq G$ d'ordre donat p^v, amb $0 \leqslant v \leqslant N_1 + \ldots + N_s$, i tals que per a tot $(r,u) \in \underline{n}$ es verifica que $\Pi_{r,u}(X) = \mathbb{Z}/p^r\mathbb{Z}$.

Amb les notacions del capítol II, això és calcular el cardinal del conjunt

$$P(\mathbb{Z}/p\mathbb{Z}, \overset{n_1)}{\ldots}, \mathbb{Z}/p\mathbb{Z}, \ldots, \mathbb{Z}/p^s\mathbb{Z}, \overset{n_s)}{\ldots}, \mathbb{Z}/p^s\mathbb{Z}; p^v).$$

Els dos problemes següents s'inclouen per a completar, ja que la seva solució s'obté de manera senzilla a partir de la solució dels problemes anteriors.

Problema 5.- Calcular el número de subgrups X de G tals que per a tot $(r,u) \in \underline{n}$ és $\Pi_{r,u}(X) = \mathbb{Z}/p^r\mathbb{Z}$, sense restriccions ni a l'ordre ni al tipus de X.

Problema 6.- Calcular el número total de subgrups de G, sense restriccions.

Tots aquests problemes es poden enunciar en el cas d'un grup abelià finit qualsevol, $\tilde{G}$, no necessàriament p-grup. Però la descomposició de $\tilde{G}$ en producte dels seus subgrups de Sylow, $\tilde{G} = \prod_p S_p(G) \simeq \bigoplus_p S_p(G)$, permet reduir els problemes al cas de p-grups. Això és clar en el cas dels problemes 1,2,6, en els quals no intervenen les propietats relatives a les projeccions. Per als altres problemes, si $\tilde{G} = \mathbb{Z}/e_1\mathbb{Z} \times \ldots \times \mathbb{Z}/e_k\mathbb{Z}$ i $\Pi_i : G \to \mathbb{Z}/e_i\mathbb{Z}$ és una projecció qualsevol, és fàcil veure que per a tot subgrup $X \subseteq \tilde{G}$ és $\Pi_i(X) = \mathbb{Z}/e_i\mathbb{Z}$ si, i només si, per a tot primer p, és $\Pi_i(S_p(X)) = S_p(\mathbb{Z}/e_i\mathbb{Z})$ (cf. cap. II, §7, prop. 7.5); de manera que els problemes 3,4 i 5, també es redueixen al cas de p-grups abelians finits.

La solució del problema 1 està enunciada en [Dy 1: teor. A]. De tota manera, i per fer aquesta memòria més autocontinguda, en donarem una demostració. Això, a més a més, ens servirà per a establir les notacions i alguns resultats necessaris per als altres problemes.

§2.- Inici de la resolució del problema 1.

Sigui p un número primer i sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\ldots,N_s,0,\ldots)$. Mantindrem les notacions del §1, de manera que $n_i = N_i - N_{i+1}$, per a tot $i \geqslant 1$. Tot element de G és una família $x = (\ldots,x_{r,u},\ldots)$, $(r,u) \in \underline{n}$, d'elements $x_{r,u} \in \mathbb{Z}/p^r\mathbb{Z}$, pels quals sovint prendrem representants enters amb $0 \leqslant x_{r,u} < p^r$.

Sigui X_0 un p-grup abelià finit de tipus $\underline{M}$. El problema 1 consisteix a calcular $h(G;\underline{M})$. Comencem per caracteritzar quan $h(G;\underline{M}) \geqslant 1$.

Proposició 2.1.- Sigui G un p-grup abelià finit de tipus $\underline{N}$. Aleshores G conté algun subgrup de tipus $\underline{M}$ si, i només si, $\underline{M} \leqslant \underline{N}$.

Demostració.- Per pas al dual $\hat{G} = \mathrm{Hom}(G;C^*)$ G conté un subgrup de tipus $\underline{M}$ si, i només si, G té un quocient de tipus $\underline{M}$. Però si $G \xrightarrow{\Pi} X_0$ és un morfisme de grups exhaustiu, resulta que, per a tot natural $i \geqslant 1$ es verifica que $\Pi(p^iG) = p^iX_0$, de manera que obtenim, per pas al quocient, morfismes exhaustius Π_i: $p^{i-1}G/p^iG \to p^{i-1}X_0/p^iX_0$, que ho són de $\mathbb{F}_p$-espais vectorials. Per tant, $M_i = \dim_{\mathbb{F}_p}(p^{i-1}X_0/p^iX_0) \leqslant \dim_{\mathbb{F}_p}(p^{i-1}/p^iG) = N_i$, per a tot $i \geqslant 1$. En conseqüència, $\underline{M} \leqslant \underline{N}$.

Recíprocament, suposem que $\underline{M} \leqslant \underline{N}$; podem passar de $\underline{M}$ a $\underline{N}$ per una successió finita de vectors tals que només diferei-xin en una component, i d'una unitat en aquesta component. Així, podem suposar que $N_j = M_j + 1$ en el lloc j-èsim i que $M_i = N_i$ per a $i \neq j$. Això significa que els grups G i X_0 són, respec

tivament,

$$G = (\mathbb{Z}/p\,\mathbb{Z})^{n_1} x \ldots x\, (\mathbb{Z}/p^j\mathbb{Z})^{n_j} x \ldots x\, (\mathbb{Z}/p^s\mathbb{Z})^{n_s},$$

$$X_0 = (\mathbb{Z}/p\,\mathbb{Z})^{n_1} x \ldots x\, (\mathbb{Z}/p^{j-1}\mathbb{Z})^{n_{j-1}+1} x\, (\mathbb{Z}/p^j\mathbb{Z})^{n_j-1} x \ldots x (\mathbb{Z}/p^s\mathbb{Z})^{n_s}.$$

Però el factor diferent, $\mathbb{Z}/p^{j-1}\mathbb{Z}$, de X_0 és isomorf al subgrup $p(\mathbb{Z}/p^j\mathbb{Z})$ del corresponent factor $\mathbb{Z}/p^j\mathbb{Z}$ de G; de manera que podem incloure X_0 en G component a component.■

Aquesta proposició fa que, a partir d'ara, puguem suposar que $\underline{M} \leqslant \underline{N}$. Per a fixar les notacions, posem p^s l'exponent de G, de manera que $\underline{N} = (N_1, \ldots, N_s, 0, \ldots)$ amb $N_s > 0$; escriurem també $\underline{M} = (M_1, \ldots, M_s, 0, \ldots)$ amb $M_s \geqslant 0$, i posarem $m_i = M_i - M_{i+1}$ per a tot $i \geqslant 1$. Denotarem, anàlogament a com hem fet amb $\underline{n}$, per $\underline{m}$ el conjunt de les parelles (i,j) tals que $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant m_i$.

Considerem el conjunt $B(G;\underline{M})$ format per totes les famílies $\{e_{i,j}\}_{(i,j)\in \underline{m}}$ (abreujarem $\{e_{i,j}\}_{\underline{m}}$) d'elements $e_{i,j} \in G$ tals que per a tota família d'enters $\{\lambda_{i,j}\}_{\underline{m}}$ es verifica l'equivalència

(1) $$\sum_{(i,j)\in \underline{m}} \lambda_{ij}\, e_{ij} = 0 \text{ en } G \Leftrightarrow \text{per a tot } (i,j) \in \underline{m} \text{ és } \lambda_{i,j} \equiv 0 \pmod{p^i}.$$

Definició.- Anomenarem $\underline{M}$-base en G tota família $\{e_{i,j}\}_{\underline{m}}$ com l'anterior. Així, $B(G;\underline{M})$ és el conjunt de totes les $\underline{M}$-bases en G.

El significat d'aquesta definició queda aclarit pel següent resultat:

Lema 2.2.- a) Sigui $\{e_{i,j}\}_{\underline{m}}$ una $\underline{M}$-base en G. Aleshores, el subgrup de G generat pels $e_{i,j}$ és de tipus $\underline{M}$ i no admet un sistema de generadors amb menys elements.

b) Sigui $X \subseteq G$ un subgrup de G de tipus $\underline{M}$. Aleshores, existeix una $\underline{M}$-base en G, $\{e_{i,j}\}_{\underline{m}}$, tal que X és el subgrup de G generat pels $e_{i,j}$.

Demostració.- Sigui $\{e_{i,j}\}_{\underline{m}}$ una $\underline{M}$-base en G, i sigui X el subgrup de G generat pels $e_{i,j}$. L'equivalència (1) permet demostrar, si triem famílies $\lambda_{i,j}$ adequades, que cada $e_{i,j}$ és un element de G d'ordre p^i. Considerem, en X_0, la $\underline{M}$-base canònica en X_0; $\tilde{E}_{i,j} = (0,\ldots,0,1,0,\ldots,0)$ amb 1 a la component (i,j). Aleshores $X_0 = \bigoplus_{\underline{m}} \langle \tilde{E}_{i,j} \rangle$ i, efectivament, $\{\tilde{E}_{i,j}\}_{\underline{m}}$ és una $\underline{M}$-base en X_0. Com que $\tilde{E}_{i,j}$, $e_{i,j}$, són d'ordre p^i, podem definir un únic morfisme de grups $\psi_X: X_0 \to X$ tal que $\psi_X(\tilde{E}_{i,j}) = e_{i,j}$. Com que els $e_{i,j}$ generen X, ψ_X és exhaustiu. Per altra banda, un petit càlcul tenint en compte la condició (1) demostra que ψ_X és injectiu. Per tant, ψ_X és un isomorfisme. És clar, a més a més, que X_0 no admet un sistema de menys generadors que el sistema $\{E_{i,j}\}_{\underline{m}}$; per tant, el mateix passa a X amb el sistema $\{e_{i,j}\}_{\underline{m}}$.

Recíprocament, si X és un subgrup de G de tipus $\underline{M}$, i si $\psi : X_0 \to X$ és un isomorfisme qualsevol, la família $\{e_{i,j}\}_{\underline{m}}$, definida per $e_{i,j} = \psi(\tilde{E}_{i,j})$, és una $\underline{M}$-base en G, ja que la condició (1) es manté per isomorfisme.■

Aquest lema ens permet fer una primera reducció del problema 1. En efecte, per a tot $X \in H(G;\underline{M})$ podem triar un iso

morfisme fix φ_X: $X_0 \to X$. Donada, ara, una $\underline{M}$-base en G, $\{e_{i,j}\}_{\underline{m}}$, denotem per X el subgrup de G generat pels $e_{i,j}$, i sigui ψ_X: $X_0 \to X$ l'isomorfisme definit per $\psi_X(\tilde{E}_{i,j}) = e_{i,j}$ a la demostració del lema anterior. Aleshores, $\varphi_X^{-1} \circ \psi_X \in \mathrm{Aut}(X_0)$ i podem definir una aplicació

$$f: B(G;\underline{M}) \longrightarrow H(G;\underline{M}) \times \mathrm{Aut}(X_0)$$

$$\{e_{i,j}\}_{\underline{m}} \longmapsto (X, \varphi_X^{-1} \circ \psi_X) \quad .$$

Es verifica el següent:

Corol.lari 2.3.- L'aplicació f és bijectiva. En particular,

$$h(G;\underline{M})\ \#\mathrm{Aut}(X_0) = \#B(G;\underline{M}).$$

Demostració.- Com que els φ_X no depenen de $\{e_{i,j}\}_{\underline{m}}$, disposar d'un automorfisme φ de X_0 equival a disposar de l'isomorfisme $\varphi_X \circ \varphi$ de X_0 en X, per a un $X \in H(G;\underline{M})$, ð per a tot $X \in H(G;\underline{M})$. Així, una parella qualsevol $(X,\varphi) \in H(G;\underline{M}) \times \mathrm{Aut}(X_0)$ es pot escriure en la forma $(X, \varphi_X^{-1} \circ \psi_X)$ on $\psi_X = \varphi_X \circ \varphi$, i per a tota parella $(i,j) \in \underline{m}$ podem definir $e_{i,j} = \psi_X(\tilde{E}_{i,j})$. Com que ψ_X és isomorfisme, els $e_{i,j}$ formen una $\underline{M}$-base en G i és clar que $f(\{e_{i,j}\}_{\underline{m}}) = (X,\varphi)$. Per tant, f és exhaustiva; però com que $\{e_{i,j}\}_{\underline{m}}$ es recupera de $f(\{e_{i,j}\}_{\underline{m}})$ per $e_{i,j} = \psi_X(\tilde{E}_{i,j})$, f també és injectiva.■

Amb aquest corol.lari, el càlcul de $h(G;\underline{M})$ queda reduït al càlcul de $\#\mathrm{Aut}(X_0)$ i al càlcul de $\#B(G;\underline{M})$. Comencem a fer el càlcul d'aquest últim.

Per a tot $r \geqslant 0$ posem $U_r(G)$ el conjunt dels elements de G d'ordre exactament p^r. Aleshores G és la reunió disjunta

dels $U_r(G)$ per a $0 \leqslant r \leqslant s$. Com que l'exponent de G és p^s, es té que $U_s(G) \neq \phi$ i que $U_r(G) = \phi$ per a tot $r > s$.

A la demostració del lema 2.2. hem vist que si $\{e_{i,j}\}_{\underline{m}}$ és una $\underline{M}$-base en G, i si $M_s \geqslant 1$, aleshores existeix e_{s,m_s} i és un element d'ordre p^s. Per tant, si $M_s > 0$, podem definir una aplicació $g : B(G;\underline{M}) \to U_s(G)$ per $g(\{e_{i,j}\}_{\underline{m}}) = e_{s,m_s}$.

Proposició 2.4.- L'aplicació g és exhaustiva i totes les fibres tenen el mateix cardinal.

Per a demostrar aquesta proposició serà útil el següent resultat, que farem servir també al §4.

Lema 2.5.- L'acció de Aut(G) en $U_s(G)$ donada per $(\varphi,x) \to \varphi(x)$ és una acció transitiva.

Demostració del lema 2.5.- Sigui $E = E_{s,n_s} = (0,\ldots,0,1) \in G$. Aleshores $E \in U_s(G)$ i és suficient provar que donat $a \in U_s(G)$ existeix un automorfisme φ de G que transforma E en a. Considerem la $\underline{N}$-base canònica en G, $\{E_{r,u}\}_{\underline{n}}$, i sigui G' el grup G excepte l'últim factor $\mathbb{Z}/p^s\mathbb{Z}$; és a dir,

$$G' = \bigoplus_{(r,u)\neq(s,n_s)} \langle E_{r,u} \rangle .$$

Aleshores $G = G' \oplus \langle E \rangle$, i com que $\langle E \rangle \simeq \langle a \rangle$, és suficient veure que $G = G' \oplus \langle a \rangle$. Podem suposar, ja que permutar les darreres n_s components de G és un automorfisme, que la darrera component, a_{s,n_s}, de a és un generador de $\mathbb{Z}/p^s\mathbb{Z}$, i via un automorfisme de G que només mogui l'última component, que $a_{s,n_s} = 1$.

Però, aleshores, $a - E \in G'$, i d'aquí s'obté fàcilment que $G = G' \oplus \langle a \rangle$.■

Demostració de la proposició 2.4.- Siguin a, $a' \in U_s(G)$. En virtut del lema 2.5, existeix un automorfisme φ de G tal que $\varphi(a) = a'$. Com que la condició (1) es manté per isomorfismes, φ transforma bijectivament $g^{-1}(a)$ en $g^{-1}(a')$ i, per tant, tots els conjunts $g^{-1}(a)$, $a \in U_s(G)$, tenen el mateix cardinal. A més a més, com que $\underline{M} \leqslant \underline{N}$ i $M_s \geqslant 1$, $B(G;\underline{M}) \neq \phi$. Això implica que g és exhaustiva, ja que algun $g^{-1}(a)$ és no buit.■

Aquesta proposició permet reduir el càlcul de $\#B(G;\underline{M})$ al càlcul de $\#U_s(G)$ i de $g^{-1}(E)$, amb $E = E_{s,n_s} = (0,\ldots,0,1) \in G$. Per a això, continuarem suposant que $\underline{M} \leqslant \underline{N}$ i que $M_s \geqslant 1$. Sigui G' com abans i sigui $X_0' = \bigoplus_{(i,j)\neq(s,m_s)} \langle \tilde{E}_{i,j} \rangle$. Aleshores, si $\underline{M}'$, $\underline{N}'$, són els tipus respectius de X_0' i de G', resulta que $M_i' = M_i - 1$, $N_i' = N_i - 1$, $1 \leqslant i \leqslant s$, i podem considerar el conjunt $B(G';\underline{M}')$. Es verifica la següent

Proposició 2.6.- $g^{-1}(E)$ és equipotent al producte cartesià

$$B(G';\underline{M}') \times X_0' \ .$$

Demostració.- Sigui $\{e_{i,j}\}_{\underline{m}} \in g^{-1}(E)$. Aleshores $\{e_{i,j}\}_{\underline{m}}$ és una $\underline{M}$-base en G tal que $e_{s,m_s} = E$; posem $e_{i,j} = (\ldots, a_{r,u}^{(i,j)}, \ldots) \in G$, i definim, per a tot $(i,j) \neq (s,m_s)$, $e_{i,j}' = e_{i,j} - a_{s,n_s}^{(i,j)} E$; és a dir, $e_{i,j}'$ és $e_{i,j}$ excepte la darrera component, que és zero. Com que $e_{i,j}$ és d'ordre p^i, resulta que $a_{s,m_s}^{(i,j)} \equiv 0 \ (\text{mòd } p^{s-i})$ i podem escriure $a_{s,m_s}^{(i,j)} = p^{s-i} b_{i,j}$ amb $b_{i,j}$ únic tal que

$0 \leqslant b_{i,j} < p^i$. Sigui $b = (\ldots,b_{i,j},\ldots) \in X'_\delta$. Aleshores $\{e'_{i,j}\}_{\underline{m}}$, és una $\underline{M}'$-base en G'. En efecte, si tenim enters $\lambda_{i,j}$, $(i,j) \in \underline{m}'$, resulta que

$$\Sigma' \lambda_{i,j} e'_{i,j} = 0 \text{ en } G' \Leftrightarrow \Sigma' \lambda_{i,j} e'_{i,j} = 0 \text{ en } G \Leftrightarrow$$

$$\Leftrightarrow \Sigma' \lambda_{i,j} e_{i,j} - (\Sigma' \lambda_{i,j} a_{s,n_s}^{(i,j)})E =$$

$$= 0 \text{ en } G \Leftrightarrow$$

$$\Leftrightarrow \lambda_{i,j} \equiv 0 \ (\text{mòd } p^i) \text{ i } \Sigma' \lambda_{i,j} a_{s,n_s}^{(i,j)} \equiv$$

$$\equiv 0 \ (\text{mòd } p^s),$$

on Σ' és la suma estesa a les parelles $(i,j) \in \underline{m}'$. Però, com que $a_{s,n_s}^{(i,j)} \equiv 0 \ (\text{mòd } p^{s-i})$, això últim equival a dir que $\lambda_{i,j} \equiv 0 \ (\text{mòd } p^i)$ per a tot $(i,j) \in \underline{m}'$. De manera que $\{e'_{i,j}\}_{\underline{m}'}$ verifica la condició (1') i és una $\underline{M}'$-base en G'. Per tant, podem definir una aplicació $h: g^{-1}(E) \to B(G';\underline{M}') \times X'_\delta$ per la fórmula

$$h(\{e_{i,j}\}_{\underline{m}}) = (\{e'_{i,j}\}_{\underline{m}'}, b).$$

Es suficient veure que h és bijectiva. Com que podem recuperar els $a_{s,n_s}^{(i,j)} = p^{s-i} b_{i,j}$ a partir de b, podem recuperar $e_{i,j} = e'_{i,j} + a_{s,n_s}^{(i,j)} E$, $(i,j) \in \underline{m}', e_{s,m_s} = E$, i h és injectiva. Per altra banda, si definim $e_{i,j}$ com ara mateix, només cal veure que $\{e_{i,j}\}_{\underline{m}} \in g^{-1}(E)$. Però això és jugar amb la condició (1) anàlogament a com ho hem fet per a definir h.■

Podem resumir les proposicions 2.4 i 2.6 en el següent

Corol.lari 2.7.- Si $M_s \geqslant 1$, aleshores $\#B(G;\underline{M}) = \#U_s(G) \#X'_\delta \#B(G';\underline{M}')$.■

§3.- El pas inductiu.

El corol.lari 2.7 permet establir un pas inductiu per al càlcul de $\#B(G;\underline{M})$. Comencem per calcular $\#U_s(G)$.

Proposició 3.1.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\dots,N_s,0,\dots)$. Aleshores

$$\#U_s(G) = p^{N_1+\dots+N_{s-1}}(p^{N_s}-1).$$

Demostració.- Un element $x \in G$ és d'ordre p^s si, i només si, alguna de les seves darreres n_s components és d'ordre p^s. Però això és dir que $U_s(G)$ és el complementari en G del subgrup

$$(\mathbb{Z}/p\mathbb{Z})^{n_1} x \dots x (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}} x (p\mathbb{Z}/p^s\mathbb{Z})^{n_s},$$

de manera que $\#U_s(G) = p^{N_1+\dots+N_s} - p^{N_1+\dots+N_{s-1}} = p^{N_1+\dots+N_{s-1}}(p^{N_s}-1)$. Observem que la fórmula és vàlida encara que $N_s = 0$.■

Corol.lari 3.2.- Amb les notacions del corol.lari 2.7 , si G és de tipus $\underline{N} = (N_1,\dots,N_s,0,\dots)$, i $\underline{M} = (M_1,\dots,M_s,0,\dots)$ amb $M_s \geqslant 1$, aleshores

$$\#B(G;\underline{M}) = \#B(G';\underline{M}').(p^{N_s}-1).p^{N_1+\dots+N_{s-1}+M_1+\dots+M_{s-1}+M_s-s}.$$■

Si $M_s > 1$, podem aplicar M_s vegades consecutives el corol.lari 3.2, cada una a un grup diferent i a un tipus diferent. En efecte, els tipus $\underline{N}$, $\underline{M}$, es redueixen, a cada pas, a $\underline{N}'$, $\underline{M}'$, amb $N_i' = N_i-1$, $M_i' = M_i-1$. De manera que, després dels M_s passos, els tipus s'hauran reduït a $(N_1-M_s,\dots,N_s-M_s,0,\dots)$,

$(M_1-M_s,\ldots,M_{s-1}-M_s,0,\ldots)$ i tindrem $M'_s = 0$. Sigui $\tilde{G}$ un p-grup abelià finit de tipus $(N_1-M_s,\ldots,N_s-M_s,0,\ldots)$ i posem $\underline{M}'=$ $= (M_1-M_s,\ldots,M_{s-1}-M_s,0,\ldots)$. Amb aquestes notacions es té que:

Lema 3.3.- Suposem que $N_s > 0$ i que $M_s \geqslant 0$. Aleshores:

$$\#B(G;\underline{M}) = \#B(\tilde{G};\underline{M}')\ p^{\beta_s} \prod_{j_s=1}^{M_s} (p^{N_s-M_s+j_s}-1),$$

$$\text{on } \beta_s = M_s(N_1+\ldots+N_{s-1}+(M_1-M_s)+\ldots+(M_{s-1}-M_s))+$$

$$+ M_s(M_s-1)/2.$$

Demostració.- El factor $p^{N_s}-1$ del corol.lari 3.2 s'ha de multiplicar consecutivament per $p^{N_s-j}-1$, $0 \leqslant j \leqslant M_s - 1$; si posem $j_s = M_s - j$, obtenim el producte de l'enunciat. Per altra banda, cal sumar els exponents de p:

$$(N_1-j)+\ldots+(N_{s-1}-j)+(M_1-j)+\ldots+(M_{s-1}-j)+(M_s-j)-s\ ,$$

per a $0 \leqslant j \leqslant M_s-1$. Això dóna l'exponent

$$\beta_s = M_s(N_1+\ldots+N_{s-1})+M_s(M_1+\ldots+M_{s-1})+M_sM_s-(2s-1)\sum_{j=0}^{M_s-1} j -sM_s =$$

$$= M_s(N_1+\ldots+N_{s-1}+(M_1-M_s)+\ldots+(M_{s-1}-M_s))+sM_s^2-sM_s -$$

$$- (2s-1)\sum_{j=0}^{M_s-1} j.$$

Però:

$$sM_s^2 - sM_s - (2s-1)\sum_{j=0}^{M_s-1} j = sM_s^2 - sM_s - (2s-1)(M_s-1)M_s/2 =$$

$$= M_s(sM_s - s - s(M_s-1)+(M_s-1)/2) =$$

$$= M_s(M_s-1)/2,$$

com volíem demostrar. Observem que, si $M_s = 0$, aleshores $\tilde{G} = G$ i $\underline{M}' = \underline{M}$; i com que $\beta_s = 0$ i el producte és buit, la fórmula és trivial.■

Sigui $G^{(s-1)}$ el grup que s'obté de $\tilde{G}$ canviant les components $\mathbb{Z}/p^s\mathbb{Z}$ per components $\mathbb{Z}/p^{s-1}\mathbb{Z}$. Això fa que $G^{(s-1)}$ sigui de tipus $(N_1-M_s,\ldots,N_{s-1}-M_s,0,\ldots)$. Però tota $\underline{M}'$-base en $\tilde{G}$ està inclosa en $G^{(s-1)}$, ja que no conté elements d'ordre p^s. Per tant, podem canviar $B(\tilde{G};\underline{M}')$ per $B(G^{(s-1)};\underline{M}')$. Això ens permet establir el següent pas inductiu.

Per a $0 \leqslant i \leqslant s$, sigui $G^{(i)}$ un p-grup abelià finit de tipus $\underline{N}^{(i)} = (N_1-M_{i+1},\ldots,N_i-M_{i+1},0,\ldots)$, i sigui $\underline{M}^{(i)} = (M_1-M_{i+1},\ldots,M_i-M_{i+1},0,\ldots)$. Aleshores, $G = G^{(s)}$, $\underline{M} = \underline{M}^{(s)}$, i el lema 3.3 i aquesta observació demostren que, per a $1 \leqslant i \leqslant s$ es verifica que

$$\#B(G^{(i)};\underline{M}^{(i)}) = \#B(G^{(i-1)};\underline{M}^{(i-1)})\,p^{\beta_i} \prod_{j_i=1}^{M_i-M_{i+1}} (p^{N_i-M_i+j_i}-1)$$

on $\beta_i = (M_i-M_{i+1})((N_1-M_{i+1})+\ldots+(N_{i-1}-M_{i+1})+(M_1-M_i)+\ldots+(M_{i-1}-M_i))+$

$+ (M_i-M_{i+1})(M_i-M_{i+1}-1)/2.$

Si ara substituïm successivament els $\#B(G^{(i)};\underline{M}^{(i)})$ obtenim que:

Proposició 3.4.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\ldots,N_s,0,\ldots)$ i sigui $\underline{M} = (M_1,\ldots,M_s,0,\ldots) \leqslant \underline{N}$ un tipus. Aleshores:

$$\#B(G;\underline{M}) = p^{\beta} \prod_{i=1}^{s} \prod_{j_i=1}^{M_i-M_{i+1}} (p^{N_i-M_i+j_i}-1),$$

on

$$\beta = \sum_{i=1}^{s} (M_i - M_{i+1}) \sum_{\ell=1}^{i-1} ((N_\ell - M_{i+1}) + (M_\ell - M_i)) + \frac{1}{2} \sum_{i=1}^{s} (M_i - M_{i+1})(M_i - M_{i+1} - 1).$$

Demostració.- El producte de la fórmula és clar, i $\beta = \sum_{i=1}^{s} \beta_i$. A més a més, $\#B(G^{(0)};\underline{M}^{(0)}) = 1$, ja que $\underline{M}^{(0)} = (0,\ldots)$ correspon al grup trivial. Només cal observar que si $N_s = 0$, aleshores $M_s = 0$ i $\underline{N}^{(s)} = \underline{N}^{(s-1)}$, $\underline{M}^{(s)} = \underline{M}^{(s-1)}$, i $\beta_s = 0$ i el producte $\prod_{j_s=1}^{M_s - M_{s-1}} (p^{N_s - M_s + j_s - 1}) = 1$.■

Per a poder escriure una fórmula per a $h(G;\underline{M})$, i en virtut del corol.lari 2.3, només cal conèixer $\#Aut(X_0)$.

§4.- Automorfismes d'un grup abelià finit.

L'ordre del grup d'automorfismes d'un grup abelià finit és ben conegut (cf.[Sp 1: cap. 9, §43, teor. 114]). En aquest § en donem una demostració utilitzant el llenguatge d'accions d'un grup en un conjunt i que, essencialment, depèn del lema 2.5. Aprofitem per a enunciar el teorema en forma directament aplicable al càlcul de $h(G;\underline{M})$.

Si $\tilde{G}$ és un grup abelià finit qualsevol, $\mathrm{Aut}(\tilde{G}) \simeq \prod_p \mathrm{Aut}(S_p(\tilde{G}))$, de manera que podem reduir-nos al cas dels p-grups abelians finits.

Suposem, doncs, que G és un p-grup abelià finit de tipus $\underline{N} = (N_1,\ldots,N_s,0,\ldots)$ amb $N_s > 0$. En el lema 2.5 s'ha demostrat que Aut(G) opera transitivament en $U_s(G)$ i a la proposició 3.1 s'ha calculat explícitament el cardinal de $U_s(G)$. Per tant, el càlcul de #Aut(G) es redueix al càlcul de l'ordre del grup d'isotropia d'un element qualsevol de $U_s(G)$; per exemple, de $E = (0,\ldots,0,1) \in G$. Posem $H = \{\varphi \in \mathrm{Aut}(G) : \varphi(E) = E\}$ aquest grup d'isotropia. Sigui S(G;E) el conjunt de tots els suplementaris de $\langle E\rangle$ en G; amb les notacions dels §§2 i 3, $G' \in S(G;E)$. Es verifica que:

Lema 4.1.- H opera transitivament en S(G;E).

Demostració.- Immediata, ja que dos suplementaris de $\langle E\rangle$ en G són sempre isomorfs i podem estendre un isomorfisme a G via la identitat en $\langle E\rangle$.■

Lema 4.2.- El grup d'isotropia de G' és isomorf a Aut(G').

Demostració.- Els automorfismes de G que deixen fix E i que deixen fix G' són automorfismes de G' (per restricció), i cada automorfisme de G' s'estén de manera única a un automorfisme de G que deixi fix E.■

En conseqüència, $\#Aut(G) = \#U_s(G)\ \#S(G;E)\ \#Aut(G')$ permet fer el càlcul de #Aut(G) per un procés inductiu. Només cal calcular #S(G;E). Es té, però, que:

Lema 4.3.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\ldots,N_s,0,\ldots)$ amb $N_s > 0$, i sigui $E = (0,\ldots,0,1) \in G$. Aleshores

$$\#S(G;E) = p^{(N_1-1)+\ldots+(N_s-1)}.$$

Demostració.- Donar un suplementari de $\langle E\rangle$ en G, posem A, equival a donar la projecció de G en $\langle E\rangle$ relativa al suplementari A; és a dir, a donar un morfisme de grups $\Pi: G \to \langle E\rangle$ tal que $\Pi(E) = E$. Però, com que $G = G' \oplus \langle E\rangle$, això equival a donar un morfisme qualsevol $\varphi: G' \to \langle E\rangle$. Per tant, $\#S(G;E) = \#Hom(G', \langle E\rangle)$.

Com que $G' = \bigoplus_{r=1}^{s-1} (\mathbb{Z}/p^r\mathbb{Z})^{n_r} \oplus (\mathbb{Z}/p^s\mathbb{Z})^{n_s-1}$, resulta que

$$\text{Hom}(G';\langle E\rangle) \simeq \prod_{r=1}^{s-1} (\text{Hom}(\mathbb{Z}/p^r\mathbb{Z};\langle E\rangle))^{n_r} \times (\text{Hom}(\mathbb{Z}/p^s\mathbb{Z};\langle E\rangle))^{n_s-1} \simeq$$

$$\simeq \prod_{r=1}^{s-1} (\mathbb{Z}/p^r\mathbb{Z})^{n_r} \times (\mathbb{Z}/p^s\mathbb{Z})^{n_s-1} \simeq$$

$$\simeq G',$$

ja que $\text{Hom}(\mathbb{Z}/p^r\mathbb{Z},\langle E\rangle) \simeq \text{Hom}(\mathbb{Z}/p^r\mathbb{Z}, \mathbb{Z}/p^s\mathbb{Z}) = \text{Hom}(\mathbb{Z}/p^r\mathbb{Z}, \mathbb{Z}/p^r\mathbb{Z}) \simeq$ $\simeq \mathbb{Z}/p^r\mathbb{Z}$, per què E és d'ordre $p^s > p^r$.

Per tant, $\#S(G;E) = \#G' = p^{(N_1-1)+\ldots+(N_s-1)}$, com volíem veure.■

Corol.lari 4.4.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\ldots,N_s,0,\ldots)$, $N_s > 0$, i sigui G' un p-grup abelià finit de tipus $(N_1-1,\ldots,N_s-1,0,\ldots)$. Aleshores:

$$\#\text{Aut}(G) = \#\text{Aut}(G')\ (p^{N_s}-1)p^{\alpha_s},$$

amb $\alpha_s = (N_1+\ldots+N_{s-1}) + (N_1-1)+\ldots+(N_s-1)$.■

Sigui, ara, $G_0 = G$ i, per a $0 \leqslant j \leqslant N_s$, sigui G_j un p-grup abelià finit de tipus $\underline{N}^{(j)} = (N_1-j,\ldots,N_s-j,0,\ldots)$. Posem $\bar{G} = G_{N_s}$. L'aplicació reiterada del corol.lari 4.4 dóna el següent

Lema 4.5.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\ldots,N_s,0,\ldots)$ amb $N_s > 0$. Aleshores,

$$\#\text{Aut}(G) = \#\text{Aut}(\bar{G})p^{\gamma_s} \prod_{j_s=1}^{N_s} (p^{j_s}-1),$$

on $\gamma_s = 2\,N_s(N_1+\ldots+N_s) - sN_s^2 - \dfrac{N_s(N_s+1)}{2}$.

Demostració.- Si $N_s = 0$, aleshores la fórmula és una identitat. Si $N_s > 0$ podem aplicar el corol.lari 4.4 successivament als grups G_j, $0 \leqslant j \leqslant N_s-1$. Com que $\alpha_{s-j} = (N_1-j)+\ldots+(N_{s-1}-j)+$ $+ (N_1-j-1)+\ldots+(N_s-j-1)$, si sumem $\alpha_{N_s}+\ldots+\alpha_1$, obtenim que

$$\gamma_s = \sum_{j=0}^{N_s-1} [(N_1-j)+\ldots+(N_{s-1}-j)+(N_1-j-1)+\ldots+(N_s-j-1)] =$$

$$= 2N_s(N_1+\ldots+N_{s-1}) + N_s^2 - sN_s - (2s-1)\sum_{j=0}^{N_s-1} j =$$

$$= 2N_s(N_1+\ldots+N_s) - N_s^2 - sN_s - (2s-1)(N_s-1)\,N_s/2 =$$

$$= 2N_s(N_1+\ldots+N_s) - sN_s^2 - \frac{N_s(N_s+1)}{2},$$

ja que $N_s^2 + sN_s + sN_s(N_s-1) - N_s(N_s-1)/2 = sN_s^2 + \frac{N_s(N_s+1)}{2}$.■

Per a acabar el càlcul, i per a $0 \leqslant i \leqslant s$, posem $\bar{G}_i$ un p-grup abelià finit de tipus $(N_1-N_{i+1},\ldots,N_i-N_{i+1},0,\ldots)$. Aleshores, $\bar{G}_s = G$, $\bar{G}_{s-1} = \bar{G}$, i $\bar{G}_0 = \{0\}$. El lema 4.5, aplicat a $\bar{G}_i$ dóna

$$\#\mathrm{Aut}(G_i) = \#\mathrm{Aut}(\bar{G}_{i-1}) \cdot p^{\gamma_i} \prod_{j_i=1}^{N_i-N_{i+1}} (p^{j_i}-1),$$

amb $\gamma_i = 2(N_i-N_{i+1}) \sum_{\ell=1}^{i} (N_\ell-N_{i+1}) - i(N_i-N_{i+1})^2 - \frac{1}{2}(N_i-N_{i+1})(N_i-N_{i+1}+$

per a $1 \leqslant i \leqslant s$.

Substituint successivament, i tenint en compte que $\#\mathrm{Aut}(\bar{G}_0) = 1$, s'obté el teorema final:

Teorema 4.6.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\ldots,N_s,0,\ldots)$, amb $N_s \geqslant 0$. Aleshores:

$$\#\mathrm{Aut}(G) = p^{\gamma} \prod_{i=1}^{s} \prod_{j_i=1}^{N_i-N_{i+1}} (p^{j_i}-1),$$

$$\text{on } \gamma = \sum_{i=1}^{s} (N_i-N_{i+1}) \sum_{\ell=1}^{i-1} ((N_\ell-N_i)+(N_\ell-N_{i+1})) +$$

$$+ \frac{1}{2} \sum_{i=1}^{s} (N_i-N_{i+1})(N_i-N_{i+1}-1).$$

Demostració.- Només cal comprovar que $\gamma = \sum_{i=1}^{s} \gamma_i$. Cada γ_i és el producte de (N_i-N_{i+1}) per la suma

$$2 \sum_{\ell=1}^{i} (N_\ell-N_{i+1}) - i\,(N_i-N_{i+1}) - \frac{1}{2}(N_i-N_{i+1}+1) =$$

$$= \sum_{\ell=1}^{i} [(N_\ell-N_{i+1})-(N_i-N_{i+1})] + \sum_{\ell=1}^{i} (N_\ell-N_{i+1}) - \frac{1}{2}(N_i-N_{i+1}+1) =$$

$$= \sum_{\ell=1}^{i-1} (N_\ell-N_i) + \sum_{\ell=1}^{i-1} (N_\ell-N_{i+1}) + (N_i-N_{i+1}) - \frac{1}{2}(N_i-N_{i+1}+1) =$$

$$= \sum_{\ell=1}^{i-1} [(N_\ell-N_i)+(N_\ell-N_{i+1})] + \frac{1}{2}(N_i-N_{i+1}-1).$$

El resultat és, doncs, clar. ∎

§5.- El símbol $\begin{bmatrix} N+M \\ M \end{bmatrix}_p$.

Per a tota parella d'enters no negatius, N,M, considerem la funció racional de $\mathbb{Q}(X)$ definida pel símbol

$$\begin{bmatrix} N+M \\ M \end{bmatrix}_X = \prod_{j=1}^{M} (X^{N+j}-1) \prod_{j=1}^{M} (X^j-1)^{-1}.$$

Les propietats elementals d'aquest símbol es resumeixen en el següent

Lema 5.1.- a) $\begin{bmatrix} N+M \\ M \end{bmatrix}_X = \prod_{j=1}^{N+M} (X^j-1) \prod_{j=1}^{N} (X^j-1)^{-1} \prod_{j=1}^{M} (X^j-1)^{-1}.$

b) $\begin{bmatrix} N+M \\ M \end{bmatrix}_X = \begin{bmatrix} N+M \\ N \end{bmatrix}_X .$

c) $\begin{bmatrix} N \\ 0 \end{bmatrix}_X = \begin{bmatrix} N \\ N \end{bmatrix}_X = 1.$

d) Equació funcional: $\begin{bmatrix} N+M \\ M \end{bmatrix}_X = X^{NM} \begin{bmatrix} N+M \\ M \end{bmatrix}_{X^{-1}} .$

e) Si $M \geqslant 1$, aleshores $\begin{bmatrix} N+M \\ M \end{bmatrix}_X = X^N \begin{bmatrix} N+M-1 \\ M-1 \end{bmatrix}_X + \begin{bmatrix} N-1+M \\ M \end{bmatrix}_X .$

f) $\begin{bmatrix} N+M \\ M \end{bmatrix}_X = \prod_{d=1}^{N+M} \phi_d(X)^{\left[\frac{N+M}{d}\right] - \left[\frac{N}{d}\right] - \left[\frac{M}{d}\right]},$

on $\phi_d(X)$ és el d-èsim polinomi ciclotòmic i $\left[\frac{N}{d}\right]$ és la part entera de $\frac{N}{d}$.

Demostració.- a), b), i c), són immediats a partir de la definició, d) Calculem $X^{NM} \begin{bmatrix} N+M \\ M \end{bmatrix}_{X^{-1}}$. Com que $X^{-j}-1 = -X^{-j}(X^j-1)$, es té que

$$\prod_{j=1}^{T} (X^{-j}-1) = (-1)^T X^{-\frac{1}{2}T(T+1)} \prod_{j=1}^{T} (X^j-1) ;$$

si fem T = M, N, N+M , i multipliquem, el resultat és conseqüèn cia de la igualtat:

$$\frac{(N+M)(N+M+1)}{2} - \frac{N(N+1)}{2} - \frac{M(M+1)}{2} = NM.$$

e). De l'expressió de $\begin{bmatrix} N+M \\ M \end{bmatrix}_X$ separem el factor $X^{N+M}-1$ del numerador i el factor X^M-1 del denominador; el que queda és l'expressió de $\begin{bmatrix} N+M-1 \\ M-1 \end{bmatrix}_X$. Però $(X^{N+M}-1)(X^M-1)^{-1} = X^N+(X^N-1)(X^M-1)^{-1}$, i el producte del factor $(X^N-1)(X^M-1)^{-1}$ pel símbol $\begin{bmatrix} N+M-1 \\ M-1 \end{bmatrix}_X$ és exactament el símbol $\begin{bmatrix} N-1+M \\ M \end{bmatrix}_X$.

f) Del fet que $X^j-1 = \prod_{d|j} \phi_d(X)$, resulta que

$$\prod_{j=1}^{T} (X^j-1) = \prod_{d=1}^{T} \phi_d(X)^{e(T,d)} \quad ,$$

on $e(T,d) = \left[\frac{T}{d}\right]$ és el número d'enters j, $1 \leqslant j \leqslant T$, tals que $d|j$. El resultat és, doncs, conseqüència del fet que, per a $d > T$ és $\left[\frac{T}{d}\right] = 0$, quan particularitzem T = N,M,N+M, i multipliquem.■

Corol.lari 5.2.- Siguin N,M, enters no negatius. Aleshores, $\begin{bmatrix} N+M \\ M \end{bmatrix}_X$ és un polinomi de grau NM amb coeficients enters estrictament positius.

Demostració.- $\begin{bmatrix} N+M \\ M \end{bmatrix}_X$ és un quocient de polinomis; el numerador, de grau $\sum_{j=1}^{M} (N+j)$ i, el denominador, de grau $\sum_{j=1}^{M} j$; de manera que la qüestió del grau serà immediata un cop vist que el símbol és un polinomi. Però, per inducció sobre N+M, la pro

pietat e) del lema 5.1 permet demostrar que $\begin{bmatrix} N+M \\ M \end{bmatrix}_X$ és un polinomi i que els coeficients són enters no negatius. Però, si els coeficients de $\begin{bmatrix} N+M-1 \\ M-1 \end{bmatrix}_X$ i els de $\begin{bmatrix} N-1+M \\ M \end{bmatrix}_X$ són positius, com que el grau del segon és $(N-1)M \geqslant N-1$, els coeficients de $X^N \begin{bmatrix} N+M-1 \\ M-1 \end{bmatrix}_X + \begin{bmatrix} N-1+M \\ M \end{bmatrix}_X = \begin{bmatrix} N+M \\ M \end{bmatrix}_X$ són positius, si $M \geqslant 1$. El cas $M = 0$ és clar, així com el cas $N+M = 1$, que ens permeten començar la inducció.■

Seguidament donarem una caracterització del polinomi $\begin{bmatrix} N+M \\ M \end{bmatrix}_X$ en funció de les varietats Grassmannianes sobre els cossos finits.

Sigui p un primer i sigui $G_p(N,M)$ la varietat Grassmanniana formada per tots els subespais vectorials de dimensió M d'un espai vectorial de dimensió N+M sobre una clausura algebraica $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$. Sigui $g_p r(N,M)$ el número de punts $\mathbb{F}_p r$-definits de $G_p(N,M)$. Un exercici senzill d'àlgebra lineal elemental permet demostrar que $g_p r(N,M) = \begin{bmatrix} N+M \\ M \end{bmatrix}_{p^r}$.

És un fet ben conegut que la funció zeta de $G = G_p(N,M)$, definida per

$$Z(G;t) = \exp \sum_{r \geqslant 1} g_p r\ (N,M)\ \frac{t^r}{r}$$

és una funció racional de la forma $Z(G;t) = \prod_{i=0}^{d} P_{2i}(t)^{-1}$ on $d = NM$ és la dimensió de G i els $P_{2i}(t)$ són polinomis amb coeficients enters de la forma

$$P_{2i}(t) = \prod_{j=1}^{\beta_{2i}} (1-\alpha_{i,j}t),$$

amb els $\alpha_{i,j}$ enters algebraics de valor absolut p^i. El grau, β_{2i}, de $P_{2i}(t)$ és el (2i)-èsim número de Betti de G.

Utilitzarem el següent

Lema 5.3.- Sigui k un cos de característica zero; siguin $a_1,\dots,a_n,b_1,\dots,b_m \in k^*$ i suposem que per a tot natural $r \geqslant 1$ és $\sum_{i=1}^{n} a_i^r = \sum_{j=1}^{m} b_j^r$. Aleshores $n = m$ i existeix una permutació σ del conjunt $\{1,2,\dots,n\}$ tal que per a tot índex $1 \leqslant i \leqslant n$ és $b_i = a_{\sigma(i)}$.

Demostració.- Si $n < m$, completem els a_i amb zeros a fi de tenir $n = m$; la hipòtesi sobre les sumes de potències es manté i assegura que els polinomis de Newton dels a_i i dels b_j coincideixen per a tot $r \geqslant 1$. Per tant, també coincideixen les seves funcions simètriques elementals (cf. cap. II, §3, lema 3.3). En conseqüència, els polinomis $\prod_{i=1}^{m}(X-a_i)$ i $\prod_{j=1}^{m}(X-b_j)$ coincideixen i, per tant, les seves arrels també.■

Amb aquest resultat podem ja establir el següent

Teorema 5.4.- Es verifica la identitat:

$$\begin{bmatrix} N+M \\ M \end{bmatrix}_X = \sum_{i=0}^{NM} \beta_{2i} X^i,$$

on β_i és el i-èsim número de Betti de $G_p(N,M)$.

Demostració.- És ben conegut que el coneixement dels $\alpha_{i,j}$ permet calcular els coeficients $g_p r(N,M)$ en la forma $g_p r(N,M) = \sum_{i,j} \alpha_{i,j}^r$; per altra banda, com ja hem comentat, $g_p r(N,M) = \begin{bmatrix} N+M \\ M \end{bmatrix}_{p^r}$. Per tant, obtenim que, per a tot $r \geqslant 1$, si $\begin{bmatrix} N+M \\ M \end{bmatrix}_X =$

$= \sum_{i=0}^{NM} a_i X^i$, aleshores

$$\sum_{i=0}^{NM} \sum_{j=1}^{\beta_{2i}} \alpha_{i,j}^{r} = \sum_{i=0}^{NM} a_i p^{ir} = \sum_{i=0}^{NM} \sum_{j=1}^{a_i} p^{ir},$$

ja que els a_i són enters positius. De les relacions $|\alpha_{i,j}| = p^i$, i aplicant el lema anterior, obtenim que $\alpha_{i,j} = p^i$ i que $a_i = \beta_{2i}$ per a $0 \leqslant i \leqslant NM$.■

Per a acabar, una observació sobre els β_{2i}. És conegut que β_{2i} és el número de particions de i en $\leqslant M$ parts, cada part $\leqslant N$ (cf.[Eh 1]). Per tant, obtenim el següent resultat:

Corol.lari 5.5.- $\begin{bmatrix} N+M \\ M \end{bmatrix}_X$ és la funció (polinòmica) generatriu del número de particions en $\leqslant M$ parts, cada part $\leqslant N$.■

§6.- La solució dels problemes.

En aquest § establirem les fórmules que donen les solucions dels problemes plantejats al §1. Per a obtenir la solució del problema 1 només cal dividir $\#B(G;\underline{M})$ per $\#Aut(X_0)$. De manera que obtenim el resultat (cf.[Dy 1: teor. A]):

Teorema 6.1.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\dots,N_s,0,\dots)$. Aleshores, per a tot tipus $\underline{M} \leqslant \underline{N}$:

$$h(G;\underline{M}) = p^{\gamma_{\underline{M}}} \prod_{i=1}^{s} \begin{bmatrix} N_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_p ,$$

$$\text{on } \gamma_{\underline{M}} = \sum_{i=1}^{s} M_{i+1}(N_i-M_i).$$

Demostració- Sigui X_0 un p-grup abelià finit de tipus $\underline{M} \leqslant \underline{N}$. Si apliquem la proposició 3.4 al grup G i al tipus $\underline{M}$, i el teorema 4.6 al p-grup X_0 , només cal dividir. El producte

$$\prod_{i=1}^{s} \begin{bmatrix} N_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_p$$

s'obté de manera directa de la divisió dels corresponents productes en $\#B(G;\underline{M})$ i en $\#Aut(X_0)$; per altra banda, la potència de p, $\gamma_{\underline{M}}$, és la diferència de les expressions β de 3.4 i γ de 4.6 per al tipus $\underline{M}$:

$$\gamma_{\underline{M}} = \sum_{i=1}^{s} (M_i - M_{i+1}) \sum_{\ell=1}^{i-1} [(N_\ell - M_{i+1}) + (M_\ell - M_i) - (M_\ell - M_i) - (M_\ell - M_{i+1})] =$$

$$= \sum_{i=1}^{s} (M_i - M_{i+1}) \sum_{\ell=1}^{i-1} (N_\ell - M_\ell) =$$

$$= \sum_{1 \leqslant \ell < i \leqslant s} (M_i - M_{i+1})(N_\ell - M_\ell) =$$

$$= \sum_{\ell=1}^{s-1} \sum_{i=\ell+1}^{s} (M_i - M_{i+1})(N_\ell - M_\ell) =$$

$$= \sum_{\ell=1}^{s-1} M_{\ell+1} (N_\ell - M_\ell),$$

com volíem demostrar.■

Aquest teorema ens permet obtenir la solució dels altres problemes en la forma següent:

Teorema 6.2.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1, \ldots, N_s, 0, \ldots)$. El número de subgrups de G d'ordre p^v, $0 \leqslant v \leqslant N_1 + \ldots + N_s$, ve donat per l'expressió $\sum_{\underline{M}} h(G;\underline{M})$, el sumatori estès a tots els tipus $\underline{M} \leqslant \underline{N}$ tals que $M_1 + \ldots + M_s = v$.

Demostració.- A la proposició 2.1 hem vist que G té algun subgrup de tipus $\underline{M}$ si, i només si, $\underline{M} \leqslant \underline{N}$. A més a més, l'ordre d'un p-grup abelià de tipus $\underline{M} \leqslant \underline{N}$ és $p^{M_1 + \ldots + M_s}$. De manera que l'enunciat és clar.■

Teorema 6.3.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\dots,N_s,0,\dots)$. El número de subgrups $X \leqslant G$ de tipus $\underline{M} \leqslant \underline{N}$ i tals que per a tota parella $(r,u) \in \underline{n}$ és $\Pi_{r,u}(X) = \mathbb{Z}/p^r\mathbb{Z}$ ve donat per l'expressió

$$\prod_{i=1}^{s} \sum_{k_i=0}^{n_i} (-1)^{k_i} \binom{n_i}{k_i} p^{M_{i+1}(N_i-k_i-M_i)} \begin{bmatrix} N_i-k_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_p$$

on escrivim $n_i = N_i - N_{i+1}$.

Demostració.- Siguin $A_1,\dots,A_N$, conjunts finits; sigui $A = \bigcup_{j=1}^{N} A_j$, i sigui B un conjunt finit que conté A. Aleshores, si entenem, com és habitual, que $\bigcap_{\nu=1}^{0} A_{j_\nu} = B$, es té que:

$$\#(B-A) = \#B - \sum_{k=1}^{N} (-1)^{k+1} \sum_{1 \leqslant j_1 <\dots< j_k \leqslant N} \#(A_{j_1} \cap \dots \cap A_{j_k}) =$$

$$= \sum_{k=0}^{N} (-1)^k \sum_{1 \leqslant j_1 <\dots< j_k \leqslant N} \#(A_{j_1} \cap \dots \cap A_{j_k}).$$

Reordenem el conjunt $\underline{n}$ de les parelles (r,u), $1 \leqslant r \leqslant s$, $1 \leqslant u \leqslant n_r$, de la manera següent: per a $1 \leqslant j \leqslant N_1$, existeix un únic r, $1 \leqslant r \leqslant s$, tal que $n_1+\dots+n_{r-1} < j \leqslant n_1+\dots+n_r$; posarem $G_j = \mathbb{Z}/p^r\mathbb{Z}$, de manera que $G = G_1 \times \dots \times G_{N_1}$ i, per a tot j, podem escriure $\Pi_j = \Pi_{(r,u)} : G \to G_j$ la projecció canònica. Volem comptar quants subgrups X de G són de tipus $\underline{M}$ i tals que $\Pi_j(X) = G_j$, per a tot j. Amb aquesta ordenació, sigui A_j el conjunt dels subgrups $X \subseteq G$ de tipus $\underline{M}$ i tals que $\Pi_j(X) \subseteq pG_j$;

és a dir, els que els falla la projecció j-èsima. Posem $A = A_1 \cup \ldots \cup A_{N_1}$ i $B = H(G;\underline{M})$. Es tracta, doncs, de calcular $\#(B-A)$, i en virtut de la fórmula anterior, cal calcular $\#(A_{j_1} \cap \ldots \cap A_{j_k})$ per a tota successió $1 \leqslant j_1 < \ldots < j_k \leqslant N_1$. Però aquesta intersecció és el conjunt dels subgrups de tipus $\underline{M}$ del grup

$$G' = G_1 \times \ldots \times p\,G_{j_1} \times \ldots \times p\,G_{j_2} \times \ldots \times p\,G_{j_k} \times \ldots \times G_{N_1}.$$

Sigui, per a $1 \leqslant r \leqslant s$, k_r el número d'índexs j_ν, $1 \leqslant \nu \leqslant k$, tals que $G_{j_\nu} = \mathbb{Z}/p^r\mathbb{Z}$. Aleshores, $k = k_1 + \ldots + k_s$ i G' és un p-grup abelià finit de tipus

$$(N_1-k_1, \ldots, N_s-k_s, 0, \ldots),$$

de manera que $\#(A_{j_1} \cap \ldots \cap A_{j_k}) = h(G';\underline{M})$ ve donat per la fórmula (cf. teor. 6.1):

$$h(G';M) = p^{\sum_{i=1}^{s} M_{i+1}(N_i-k_i-M_i)} \prod_{i=1}^{s} \begin{bmatrix} N_i-k_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_p .$$

De totes les possibles famílies $1 \leqslant j_1 < \ldots < j_k \leqslant N_1$ amb $k_1, \ldots, k_s$, fixats, n'hi ha exactament $\prod_{i=1}^{s} \binom{n_i}{k_i}$, de manera que podem escriure $\#(B-A) =$

$$= \sum_{k_1=0}^{n_1} \ldots \sum_{k_s=0}^{n_s} (-1)^{k_1+\ldots+k_s} \prod_{i=1}^{s} \binom{n_i}{k_i} p^{\sum_{i=1}^{s} M_{i+1}(N_i-k_i-M_i)} \prod_{i=1}^{s} \begin{bmatrix} N_i-k_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_p =$$

$$= \prod_{i=1}^{s} \sum_{k_i=0}^{n_i} (-1)^{k_i} \binom{n_i}{k_i} p^{M_{i+1}(N_i-k_i-M_i)} \begin{bmatrix} N_i-k_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_p ,$$

com volíem demostrar.■

Si ara sumem igual que en el teorema 6.2 obtenim el següent

Teorema 6.4.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\dots,N_s,0,\dots)$, i sigui $0 \leqslant v \leqslant N_1+\dots+N_s$. El número de subgrups $X \subseteq G$ d'ordre p^v i tals que $\Pi_{(r,u)}(X) = \mathbb{Z}/p^r\mathbb{Z}$, per a tot $(r,u) \in \underline{n}$, ve donat per

$$\sum_{\underline{M}} \prod_{i=1}^{s} \sum_{k_i=0}^{n_i} (-1)^{k_i} \binom{n_i}{k_i} p^{M_{i+1}(N_i-k_i-M_i)} \begin{bmatrix} N_i-k_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_p ,$$

la suma estesa a tots els tipus $\underline{M} \leqslant \underline{N}$ tals que $M_1+\dots+M_s = v$. ■

A partir del teorema 6.3 i si sumem per a tots els tipus $\underline{M} \leqslant \underline{N}$, obtenim que:

Teorema 6.5.- Sigui G un p-grup abelià finit de tipus $\underline{N} = (N_1,\dots,N_s,0,\dots)$. El número de subgrups $X \subseteq G$ tals que per a tota parella $(r,u) \in \underline{n}$ és $\Pi_{r,u}(X) = \mathbb{Z}/p^r\mathbb{Z}$ ve donat per

$$\sum_{\underline{M} \leqslant \underline{N}} \prod_{i=1}^{s} \sum_{k_i=0}^{n_i} (-1)^{k_i} \binom{n_i}{k_i} p^{M_{i+1}(N_i-k_i-M_i)} \begin{bmatrix} N_i-k_i-M_{i+1} \\ M_i-M_{i+1} \end{bmatrix}_p . \blacksquare$$

Anàlogament, a partir del teorema 6.1 s'obté que

Teorema 6.6.- El número total de subgrups d'un p-grup abelià finit de tipus N és

$$\sum_{\underline{M} \leqslant \underline{N}} p^{\sum_{i=1}^{s} M_{i+1}(N_i - M_i)} \prod_{i=1}^{s} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_p .\blacksquare$$

REFERÈNCIES.

[Ap 1] T.M. Apostol: *Introduction to Analytic Number Theory.* UTM. Springer-Verlag: New York, 1.976.

[B-N 1] P. Bayer, E. Nart: Zeta Functions and Genus of Quadratic Forms. Per aparèixer.

[B-S 1] Z.I. Borevich, I.R. Shafarevich: *Number Theory.* Academic Press: New York-London, 1.966. Edició original: *Teoriya Čisel*: Moscow, 1.964.

[Bu 1] W. Burnside: *Theory of groups of finite order.* Dover: New York, 1.955. De la segona edició; Cambridge Univ. Press, 1.911.

[Dy 1] P.E. Dyubyuk: On the number of subgroups of a finite abelian group. *Soviet Math. Dokl.* 2 (1.961), pp. 298-300.

[Eh 1] C. Ehresmann: Sur la topologie de certains espaces homogènes. *Ann. of Math.* 35 (1.934), pp. 396-443.

[F-W 1] G. Faltings, G. Wüstholz, et al.: *Rational Points.* Seminar Bonn-Wuppertal 1.983/84. Friedr. Vieweg & Sohn, 1.984.

[Ga 1] É. Galois: Sur la Théorie des Nombres. *Bull. Sc. Math. Férussac*, XIII, §218 (1.830). Reproduit en R. Bourgne, J-P. Azra: *Écrits et Mémoires Mathématiques d'Évariste Galois.* Gauthier Villars: Paris, 1.962.

[Ha 1] H. Hasse: *Number Theory*. G M W 229. Springer-Verlag: Berlin-Heidelberg, 1.970. Traducció corregida i ampliada de *Zahlentheorie*, tercera edició. Akademie-Verlag: Berlin , 1.969.

[Ja 1] G.J. Janusz: *Algebraic Number Fields*. Academic Press: London and New York, 1.973.

[Kr 1] M. Krasner: Nombre des extensions d'un degré donné d'un corps p-adique. *C.R. Acad. Sc. Paris* 254 (1.962), pp. 3.470-3.472; 255 (1.962), pp. 224-226, 1.682-1.684, 2.342-2.344, 3.095-3.097. Veure també Les Tendances Géométriques en Algèbre et Théorie des Nombres. *Colloques Internationaux du C.N.R.S.* 143 (1.966), pp. 143-169.

[La 1] S. Lang: *Algebraic Number Theory*. Addison-Wesley: Reading, MA, 1.970.

[La 2] S. Lang: *Algebra*. Aguilar: Madrid, 1.971. Traducció de l'edició original de Addison-Wesley, 1.965.

[Mä 1] S. Mäki: On the density of abelian number fields. *Ann. Acad. Sc. Fennicae* 54 (1.985).

[Ne 1] J. Neukirch: *Class Field Theory*. GMW 280. Springer-Verlag: Berlin-Heidelberg, 1.986.

[Ri 1] P. Ribemboim: *L'Arithmétique des Corps*. Hermann: Paris, 1.972.

[Sa 1] I.R. Šafarevič: Algebraic Number Fields. *Amer. Math. Soc. Transl.* 31 (1.963), pp. 25-39.

[Sam 1] P. Samuel: *Teoría Algebraica de Números*. Omega: Barcelona, 1.972. Traducció de l'original francès. Hermann: Paris, 1.967.

[Se 1] J-P. Serre: Une formule de masse pour les extensions totallement ramifiées de degré donné d'un corps local. *C.R. Acad. Sc. Paris* 286 (1.978), pp. 1.031-1.036.

[Se 2] J-P. Serre: *Local Fields*. GTM 67. Springer-Verlag: New York, 1.979. Traducció de l'original francès. Hermann: Paris, 1.962.

[Se 3] J-P. Serre: *Cours d'Arithmétique*. Presses Universitaires de France. Seconde édition. Paris, 1.977.

[Sp 1] A. Speiser: *Die Theorie der Gruppen von Endlicher Ordnung*. Birkhäuser. 4 Auflage. Bassel, 1.956.

[Tr 1] A. Travesa: Sobre el número de extensiones de grado dado de un cuerpo local. *Actas de las X Jornadas Hispano-Lusas de Matemáticas. Sección 1: Algebra y Fundamentos*. Murcia, 1.985, pp. 235-243.

[vdW 1] B.L. van der Waerden: *Algebra*, vol. 1. Frederick Ungar Pub. Comp: New York, 1.970. Traducció de la setena edició en alemany de *Algebra*. Springer-Verlag: Berlin, 1.967.

[Wa 1] L.C. Washington: *Introduction to Cyclotomic Fields*. GTM 83. Springer-Verlag: New York, 1.982.

ÍNDEX DE SÍMBOLS.