Polígonos de Newton de orden superior y aplicaciones aritméticas

Jesús Montes Peral

Polígonos de Newton de orden superior y aplicaciones aritméticas

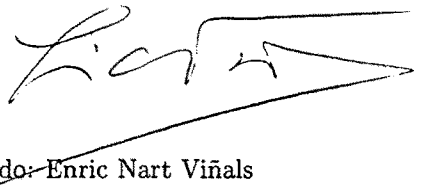
Memoria presentada
para optar al grado de
Doctor en Matemáticas
por

Jesús Montes Peral

Universitat de Barcelona, 1999

Departament d'Àlgebra i Geometria
Programa de Doctorado comenzado el año 1983
Doctorando: Jesús Montes Peral
Tutora: Dra. Pilar Bayer Isant
Director de Tesis: Dr. Enric Nart Viñals

Enric Nart Viñals, Catedrático de Álgebra del Departament
de Matemàtiques de la Universitat Autònoma de Barcelona,
HAGO CONSTAR
que el Sr. Jesús Montes Peral ha realizado esta memoria, para
optar al grado de Doctor en Matemáticas, bajo mi dirección.



Firmado: Enric Nart Viñals
Barcelona, septiembre de 1999

Ratificación del Tutor:

Firmado: Pilar Bayer Isant, Catedrática de Álgebra del Departament
d'Àlgebra i Geometria de la Universitat de Barcelona
Barcelona, septiembre de 1999

A Lola

Contenido

Introducción 1

CAPÍTULO 1

Polígonos de Newton (de orden uno) 9

§1. Notaciones y definiciones 9

§2. Desarrollos admisibles. Teorema del producto 16

§3. Teoremas del polígono y del polinomio asociado 21

§4. Teoremas de la resultante y del índice 27

CAPÍTULO 2

Polígonos de Newton de orden superior 33

§1. Notaciones, hipótesis de inducción y tipos 33

§2. El par de valoración (v_r, ω_r) 38

§3. Construcción de $\phi_r(X)$ 51

§4. Definición del polígono y del polinomio asociado 56

§5. Desarrollos admisibles 64

§6. Teorema del producto 66

§7. Cálculo del valor $v(R(\theta))$ con el polígono 70

§8. Teorema del polígono 77

§9. Teorema del polinomio asociado 82

§10. Teorema de la resultante 89

§11. Teorema del índice 96

CAPÍTULO 3
Descomposición de números primos 111
§1. Introducción 111
§2. Determinación de buenos representantes 112
§3. Determinación del tipo de descomposición 120
§4. Profundidad de un polinomio 124
§5. Generadores de los ideales primos 126
§6. Ejemplos 134

CAPÍTULO 4
Ramificación en cuerpos cuárticos 141
§1. Introducción 141
§2. Resultados previos 143
§3. Ramificación diádica (primera parte) 147
§4. Ramificación diádica (segunda parte) 157
§5. Ramificación triádica 177
§6. Ramificación de los primos mayores que tres 186

Bibliografía 195

Introducción

La teoría algebraica de números tiene sus inicios en los trabajos de Kummer sobre la ecuación de Fermat. En los anillos ciclotómicos deja de ser cierto el teorema fundamental de la aritmética: los elementos descomponen en producto de elementos "primos", pero no de manera única. Kummer, en una intuición genial, apuntó que esta dificultad podía salvarse considerando la existencia de *números ideales* que permitirían recuperar la unicidad en la descomposición en producto de *números ideales primos*. Estas ideas las culminó Dedekind en 1878 fundando la teoría de ideales tal como la conocemos hoy en día. Los anillos de enteros de los cuerpos de números son *dominios de Dedekind*, es decir, todo ideal descompone de manera única en producto de ideales primos.

No obstante, la teoría de Dedekind no es efectiva. Cuando nos enfrentamos a un problema concreto, como por ejemplo resolver una ecuación diofántica, que exige considerar un cuerpo de números K, de anillo de enteros $\mathcal{O}$, necesitamos resolver en general dos cuestiones fundamentales:

(a) Determinar el *tipo de descomposición*:

$$p\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

de los primos racionales en K. Es decir, para cada primo $p \in \mathbb{Z}$ determinar el número de ideales primos distintos $\mathfrak{p}_i$ de $\mathcal{O}$ que dividen al ideal generado por p, y calcular los *índices de ramificación* $e(\mathfrak{p}_i/p) := e_i$ y los *grados residuales* $f(\mathfrak{p}_i/p) := [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_p]$.

(b) Determinar generadores de los ideales $\mathfrak{p}_i$.

Usualmente querremos computar estos datos a partir de una ecuación definidora del cuerpo K, es decir de un polinomio mónico irreducible $F(X) \in \mathbb{Z}[X]$ tal que $K \simeq \mathbb{Q}[X]/(F(X))$.

Este aspecto efectivo lo cubre parcialmente Dedekind, usando ideas de Kummer, con el siguiente resultado:

0.1. Teorema. (Teorema de Kummer-Dedekind) *Sea* $\overline{F}(X) \in \mathbb{F}_p[X]$ *el polinomio obtenido reduciendo módulo* p *los coeficientes de* $F(X)$*; sea*

$$\overline{F}(X) = \psi_1(X)^{a_1} \cdots \psi_r(X)^{a_r} ,$$

la factorización de $\overline{F}(X)$ *en* $\mathbb{F}_p[X]$ *en producto de polinomios irreducibles distintos. Sean* $\phi_i(X) \in \mathbb{Z}[X]$ *polinomios mónicos arbitrarios que reduzcan a los* $\psi_i(X)$ *y consideremos el polinomio*

$$G(X) := \frac{1}{p}\left(F(X) - \phi_1(X)^{a_1} \cdots \phi_r(X)^{a_r}\right) \in \mathbb{Z}[X] .$$

Supongamos que para cada $1 \leq i \leq r$ *se tiene:*

$$a_i = 1 \quad \acute{o} \quad \psi_i(X) \nmid \overline{G}(X) \text{ en } \mathbb{F}_p[X] . \tag{1}$$

Entonces,

$$p\mathcal{O} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r},$$

con:

$$f(\mathfrak{p}_i/p) = \mathrm{gr}(\psi_i) \quad y \quad \mathfrak{p}_i = p\mathcal{O} + \phi_i(\theta)\,\mathcal{O} ,$$

donde θ *es una raíz cualquiera de* $F(X)$.

En la práctica este resultado permite resolver las dos cuestiones para todos los primos p excepto un número finito, los que dividen al índice $\mathrm{ind}(F) := (\mathcal{O} : \mathbb{Z}[\theta])$, que son exactamente los primos para los cuales falla la condición (1).

El siguiente paso, extraordinariamente importante tanto desde un punto de vista conceptual como de la efectividad, lo da Hensel, con la introducción de los cuerpos p-ádicos. Esta idea revolucionaria permite "descomponer" los problemas aritméticos globales en una suma de problemas locales, donde se focaliza la atención en los fenómenos que afectan a un primo concreto p. Esta filosofía, en el problema que nos atañe, se traduce en el siguiente resultado:

0.2. Teorema. (Hensel) *Sea*

$$F(X) = F_1(X) \cdots F_g(X)\,,$$

la factorización de $F(X)$ en producto de polinomios irreducibles de $\mathbb{Q}_p[X]$. Para cada $1 \leq i \leq g$ sea K_i el cuerpo local $\mathbb{Q}_p[X]/(F_i(X))$ y denotemos por $e(K_i/\mathbb{Q}_p)$, $f(K_i/\mathbb{Q}_p)$ el índice de ramificación y el grado residual locales. Entonces, hay exactamente g ideales primos $\mathfrak{p}_i$ en $\mathcal{O}$ dividiendo a $p\mathcal{O}$ y para cada uno de ellos se tiene:

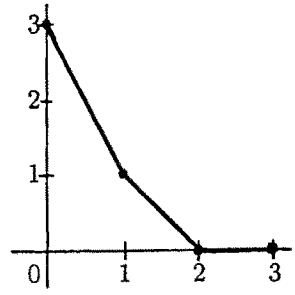
$$e(\mathfrak{p}_i/p) = e(K_i/\mathbb{Q}_p) \quad y \quad f(\mathfrak{p}_i/p) = f(K_i/\mathbb{Q}_p)\,.$$

Después de este resultado, el problema de la efectividad puede resolverse mediante técnicas locales que comportan esencialmente la factorización de polinomios en cuerpos p-ádicos (que se traduce en la práctica en factorizar módulo una potencia suficientemente alta de p) y la determinación de bases de enteros de órdenes locales. Utilizando distintas variantes de estas ideas se han obtenido diversos algoritmos para hallar la descomposición en producto de ideales primos. Destaquemos los de Pohst-Zassenhaus, Böffgen-Reichert y Buchmann-Lenstra.

El objetivo principal de la memoria es el de desarrollar un nuevo algoritmo, basado en la técnica del polígono de Newton. El polígono de Newton se utilizó en el siglo pasado para estudiar las singularidades de curvas planas. En 1907 Bauer reconvirtió la técnica para su aplicación a cuestiones aritméticas. Si dibujamos en el plano los puntos de coordenadas $(i, v_p(a_i))$, donde los a_i son los coeficientes del polinomio $F(X)$, la envoltura convexa inferior de esta nube de puntos es un polígono abierto, cuyos lados marcan una factorización de $F(X)$ en $\mathbb{Q}_p[X]$ en producto de polinomios coprimos dos a dos (no necesariamente irreducibles) y las pendientes de los lados determinan el valor p-ádico de las distintas raíces de $F(X)$ en la clausura algebraica de $\mathbb{Q}_p$. Si esos lados no contienen puntos de coordenadas enteras (aparte de los vértices) se obtiene una solución completa a la cuestión (a) mencionada anteriormente.

Por ejemplo, $F(X) = X^3 + X^2 - 2X + 8$ factoriza como $X^2(X+1)$ módulo $p = 2$ y el lema de Hensel no basta para determinar su factorización

en $\mathbb{Q}_2[X]$; habría que factorizar módulo 4 para detectar que ese polinomio descompone completamente en $\mathbb{Q}_2$. En cambio, una simple ojeada a su polígono de Newton:



nos hace ver que $F(X)$ tiene tres raíces en $\mathbb{Q}_2$ (con valor 2-ádico 0, 1 y 2 respectivamente) y que por tanto el primo 2 descompone completamente en el cuerpo cúbico determinado por $F(X)$. Este cuerpo cúbico lo introdujo el propio Dedekind para ilustrar las limitaciones de su método. Se puede probar fácilmente que para cualquier polinomio $F(X)$ generador de este cuerpo se tiene $2 \mid \mathrm{ind}(F)$, con lo que el teorema de Kummer-Dedekind no puede nunca proporcionar la información que nos interesa.

Las ideas de Bauer fueron extensamente ampliadas por Ore, quien en una serie de artículos en los años 20, introduce un concepto más general de polígono, el $\phi(X)$-polígono, que permite tratar el caso en que los factores irreducibles de $\overline{F}(X)$ no son necesariamente lineales. Este punto de vista permite incluir el teorema de Kummer-Dedekind como un caso particular; más precisamente, la condición (1) se traduce en que el $\phi_i(X)$-polígono de $F(X)$ tenga un solo lado de pendiente negativa, con alguna de las dos proyecciones sobre los ejes de longitud 1. También, Ore asocia a cada lado del polígono un polinomio sobre un cuerpo finito, cuya factorización en producto de irreducibles permite acabar de determinar la descomposición de los primos en numerosos casos no cubiertos por la técnica anterior.

En la terminología clásica (cf. [**Be 27**]) la aplicación estricta del polígono (Bauer-Ore) es conocida como la "segunda aproximación", mientras que la información extra que obtiene Ore de cada lado se bautizó como la "tercera aproximación" (el teorema de Kummer-Dedekind era la " primera aproximación"). Esas aproximaciones han sido mejoradas y generalizadas por distintos autores; por ejemplo, Ore puso en un contexto más general

la segunda aproximación inicial de Bauer, ó Montes-Nart en [**Mo-Na 92**] refinan la tercera aproximación. Ahora bien, los autores clásicos ya eran conscientes de que por mucho que se refinaran esas aproximaciones, siempre quedarían polinomios para los cuales todavía no se obtiene la respuesta definitiva (cf. [**Be 27**], [**Or 28**]). También intuían que debería ser posible introducir aproximaciones de más alto nivel que permitieran resolver la cuestión para cualquier polinomio en un proceso iterativo finito. Ésa es precisamente la cuestión que resolvemos en la memoria con nuestros *polígonos de orden superior.*

Está muy claro que la técnica del polígono aventaja en simplicidad y rapidez a cualquier otro método iterativo conocido. La segunda aproximación, por ejemplo, es un cómputo directo que no requiere ningún proceso algorítmico y el número de casos que cubre es espectacularmente grande; la sensación que se tiene es que se obtiene la mayor cantidad posible de información con el mínimo de trabajo. Para la tercera aproximación ya se requiere un proceso de búsqueda: factorizar polinomios sobre un cuerpo finito; aún así, hay que tener en cuenta que se dispone de algoritmos muy eficientes (mucho más eficientes que los que se precisan para factorizar módulo una potencia de p, donde no hay factorización única). Intuitivamente, la posibilidad de aplicar la técnica del polígono a distintos niveles con un control de la finitud del proceso tiene que dar forzosamente un algoritmo mucho más eficiente que los algoritmos no basados en el polígono. En el algoritmo que presentamos, además, se mantiene el hecho de que en cada nivel el único proceso de búsqueda necesario sigue siendo la factorización de polinomios en cuerpos finitos. Sin haber hecho un estudio teórico de la complejidad de nuestro algoritmo, la experimentación con casos prácticos muestra con creces la eficiencia del algoritmo (véase capítulo 3).

Pasamos a describir brevemente el contenido de los distintos capítulos de la memoria. En el capítulo 1 se exponen los principales resultados de Ore sobre el polígono de Newton trasladados al contexto de cuerpos locales. Se distinguen cuatro fases distintas, cada una culminando con un resultado clave que denominamos respectivamente teorema del producto (de carácter instrumental), del polígono (segunda aproximación), del polinomio asociado (tercera aproximación) y del índice. El conjunto de estas fases constituye lo que llamamos el nivel 1 o orden 1. Cada fase marca los distintos obstáculos

que será necesario superar en cada nivel con los polígonos de orden superior. Este es el objetivo del segundo capítulo, que constituye el núcleo principal de la memoria.

Dentro del segundo capítulo merecen mención especial las definiciones del polígono y del polinomio asociado en orden r. La definición correcta de "polígono a otro nivel" requiere considerar extensiones adecuadas de la valoración p-ádica al anillo de polinomios, marcadas por datos proporcionados por el polígono de orden anterior. Valoraciones de este tipo fueron introducidas por MacLane ([**Ma 36**a], [**Ma 36**b]) también con el propósito de obtener un algoritmo para determinar la descomposición de los primos en cuerpos de números; no obstante, sus métodos no son efectivos. La definición del polinomio asociado en orden r es el obstáculo cuya superación presentó mayores dificultades. En el fondo su construcción se reduce a encontrar "buenos" representantes de ciertas clases residuales módulo las valoraciones que acabamos de mencionar; ahora bien, la elección correcta (es decir, que funcione) de esos representantes pasa por un delicado trabajo con fracciones racionales. Finalmente, el teorema del índice es el resultado clave en el control de la finitud del proceso iterativo. Mencionemos también que cada vez que el proceso permite aislar un factor irreducible en $\mathbb{Q}_p[X]$ del polinomio inicial $F(X)$, el método permite explicitar una base de enteros del correspondiente anillo local (cf. 11.12).

En el tercer capítulo se desarrolla el algoritmo para resolver las cuestiones (a) y (b) del principio de esta introducción, basado en la sucesiva consideración de polígonos de Newton. Las técnicas expuestas en el capítulo anterior ya proporcionan, sin más, un algoritmo para resolver la cuestión (a). En este capítulo se describe un proceso de obtención de "representantes optimales", que permiten recoger toda la información posible que se puede obtener a un nivel determinado antes de verse obligado a pasar al nivel superior. Con esta técnica se obtiene una implementación mucho más ágil del algoritmo que la que se obtendría con una aplicación ciega de los resultados del capítulo 2. En el capítulo se resuelve también la cuestión (b) explicitando generadores de los ideales primos que dividen a $p\mathcal{O}$ en término de los datos (las pendientes de los lados y los polinomios asociados) del polígono de orden $r+1$, si ha sido necesario llegar hasta orden r para resolver (a). En este capítulo presentamos varios ejemplos con una doble finalidad; por

un lado, ilustrar la estructura general del algoritmo (en particular como intervienen las aproximaciones de nivel superior), y por otro, mostrar su eficiencia en general con polinomios de grado muy alto. Los cálculos con estos polinomios se han llevado a término usando el paquete *Newton*, la implementación que ha hecho J. Guàrdia del algoritmo.

En el cuarto capítulo se usan las técnicas del capítulo 2 para determinar de manera no algorítmica el discriminante absoluto y el tipo de descomposición de los primos en un cuerpo cuártico arbitrario. Evidentemente, no se puede obtener este resultado mediante una simple aplicación del algoritmo al polinomio genérico $X^4 + aX^2 + bX + c$, con a, b, c indeterminados, pues nos podría pasar que estuviéramos distinguiendo casos indefinidamente. Destaquemos que los resultados para el primo 2 son excepcionalmente enrevesados debido a los numerosos casos de ramificación salvaje que presenta.

Al acabar la presente introducción, quiero expresar mi agradecimiento a todos los que han contribuido a que este trabajo vea la luz: a mi familía; al Seminari de Teoria de Nombres de Barcelona, en especial a la Profesora Pilar Bayer por su continuo estímulo; al Departament d'Àlgebra i Geometria. Y quiero dar las gracias al Profesor Enric Nart por su eterna paciencia conmigo, y por haberme enseñado a conocer la regularidad del polígono aritmético.

CAPÍTULO 1

Polígonos de Newton (de orden uno)

En este capítulo se agrupan los principales resultados de Ore relativos a las aplicaciones aritméticas del polígono de Newton (cf. [**Or 23**] y [**Or 28**]) en cuatro teoremas: del producto, del polígono, del polinomio asociado y del índice; los cuales se enuncian ya en el contexto más general de los cuerpos $\mathfrak{p}$-ádicos que permite su aplicación al caso relativo (cf. [**Mo-Na 92**]).

La exposición de estos resultados sigue un patrón que facilita su extensión y completación en el contexto de polígonos de orden superior en el próximo capítulo. Por ello introducimos también en este capítulo el concepto de desarrollo admisible de un polinomio que, además de reducir la demostración de los teoremas anteriores al caso del polígono de Newton clásico, nos permitirá demostrar el teorema del producto de orden superior.

Así mismo, se expone el teorema de la resultante (cf. §1 y §2 del capítulo 2 de [**Na 83**]), que permite dar una prueba del teorema del índice radicalmente más corta que la original de Ore; ya que esta vía también la utilizaremos para probar el teorema del índice en orden superior.

§1. Notaciones y definiciones

A lo largo de todo este capítulo p denotará un primo racional fijado, y $\mathbb{Q}_p^{al}$ y $\mathbb{F}_p^{al}$ denotarán clausuras algebraicas fijadas de $\mathbb{Q}_p$ y $\mathbb{F}_p$, respectivamente. Para cualquier extensión finita L de $\mathbb{Q}_p$, $L \subset \mathbb{Q}_p^{al}$, denotamos por v_L la valoración standard de $\mathbb{Q}_p^{al}$ normalizada de forma que $v_L(L^*) = \mathbb{Z}$, por $\mathcal{O}_L := \{x \in L : v_L(x) \geq 0\}$ su anillo de valoración en L, por $\mathfrak{p}_L$ su ideal maximal, y por $\mathbb{F}_L := \mathcal{O}_L/\mathfrak{p}_L$ su cuerpo residual, el cual lo supondremos

inmerso en $\mathbb{F}_p^{al}$ de manera que todas las aplicaciones de reducción $\mathcal{O}_L \to \mathbb{F}_L$, denotadas por $a \mapsto \overline{a}$, sean compatibles.

Tomamos una extensión finita K de $\mathbb{Q}_p$, $K \subset \mathbb{Q}_p^{al}$, como cuerpo base y ponemos $v := v_K$, $\mathcal{O} := \mathcal{O}_K$ y $\mathfrak{p} := \mathfrak{p}_K$. Además, fijamos un uniformizante $\pi \in \mathcal{O}$ de v, y denotamos por $q := p^{f(K/\mathbb{Q}_p)}$ al número de elementos del cuerpo finito $\mathbb{F}_K$; así, es $\mathbb{F}_K = \mathbb{F}_q$. Nótese que si $L \subset \mathbb{Q}_p^{al}$ es una extensión finita de K, entonces para cada $\theta \in \mathbb{Q}_p^{al}$ es $v_L(\theta) = e(L/K)v(\theta)$.

A continuación, extendemos la valoración discreta $v_{|K}$ de K a una valoración de $K(X)$, denotada también por v, de forma que $v(X) = 0$. Para un polinomio $P(X) = \sum A_i X^i \in \mathcal{O}[X]$, definimos

$$v(P) := \min v(A_i) \in \mathbb{N} \cup \{+\infty\}\,.$$

Así, el valor $v(P) = 0$ si y sólo si el polinomio $\overline{P}(Y) \in \mathbb{F}_q[Y]$ es no nulo. Además, para cada par de polinomios $P(X), Q(X) \in \mathcal{O}[X]$ tenemos

$$v(P\,Q) = v(P) + v(Q)\,, \quad v(P+Q) \geq \min\{v(P), v(Q)\}\,.$$

Para una fracción racional $R(X) \in K(X)^*$, definimos ahora

$$v(R) := v(P) - v(Q) \in \mathbb{Z}\,;$$

donde $P(X), Q(X) \in \mathcal{O}[X]$ son polinomios no nulos cuyo cociente es $R(X)$. La aplicación $v : K(X)^* \to \mathbb{Z}$ determina también una valoración discreta de $K(X)$, cuyo anillo de valoración, denotado por $\mathcal{O}_v$, es el localizado del anillo $\mathcal{O}[X]$ en el ideal primo $\mathfrak{p}[X]$, y cuyo cuerpo residual, denotado por k_v, es isomorfo al cuerpo $\mathbb{F}_q(Y)$.* Más concretamente, puesto que la intersección del ideal maximal de $\mathcal{O}_v$ con $\mathcal{O}$ es igual a $\mathfrak{p}$, podemos pensar el cuerpo $\mathbb{F}_q$ como un subcuerpo de k_v; además, si la aplicación de reducción $\mathcal{O}_v \to k_v$ la denotamos por $R(X) \mapsto \overline{R(X)}$, tenemos que el cuerpo $k_v = \mathbb{F}_q\left(\overline{X}\right)$ y que el elemento $\overline{X}$ es trascendente sobre $\mathbb{F}_q$, ya que $\overline{P(X)} = \overline{P}\left(\overline{X}\right)$ para cada polinomio $P(X) \in \mathcal{O}[X]$.

Fijamos un polinomio mónico e irreducible $\psi(Y) \in \mathbb{F}_q[Y]$, y ponemos $m := \mathrm{gr}(\psi)$ y $q_1 := q^m$. Fijamos también una raíz $\zeta \in \mathbb{F}_p^{al}$ de $\psi(Y)$, y un

* La utilización de la indeterminada Y cuando se pasa a trabajar con polinomios con coeficientes en $\mathbb{F}_q$ se debe a Ore. Hemos mantenido esa tradición para distinguir en cada momento el lugar donde se trabaja.

polinomio mónico arbitrario $\phi(X) \in \mathcal{O}[X]$ tal que $\overline{\phi}(Y) = \psi(Y)$ en $\mathbb{F}_q[Y]$. Así, es $\mathbb{F}_q(\zeta) = \mathbb{F}_{q_1}$. Denotaremos por v_ϕ (resp. v_ψ) la valoración de $K(X)$ (resp. $\mathbb{F}_q(Y)$) asociada al polinomio irreducible $\phi(X)$ (resp. $\psi(Y)$).

Para un polinomio no nulo $P(X) \in \mathcal{O}[X]$, definimos ahora

$$P_0(X) := P(X)/\pi^{v(P)} \in \mathcal{O}[X], \quad \omega(P) := v_\psi\left(\overline{P_0}\right) \in \mathbb{N}.$$

De esta forma, $\omega(P) = 0$ si y sólo si el elemento $\overline{P_0}(\zeta) \in \mathbb{F}_{q_1}$ es no nulo. Además, para cada par de polinomios no nulos $P(X), Q(X) \in \mathcal{O}[X]$ se tiene

$$\omega(PQ) = \omega(P) + \omega(Q),$$

lo cual nos permite extender ω a $K(X)^*$ definiendo

$$\omega(P/Q) := \omega(P) - \omega(Q) \in \mathbb{Z}.$$

Desgraciadamente, la aplicación $\omega : K(X)^* \to \mathbb{Z}$ así definida no es una valoración de $K(X)$; por ejemplo, para $\psi(Y) = Y$ tenemos $\omega(X + \pi) = \omega(X) = 1$ y en cambio $\omega(X + \pi - X) = 0$. Sin embargo, satisface las siguientes propiedades

(i) ω es un homomorfismo de grupos.

(ii) Si $P(X), Q(X) \in \mathcal{O}[X]$ son dos polinomios no nulos tales que el valor $v(P) = v(Q) =: u$ y $\omega(P) \neq \omega(Q)$, entonces el valor $v(P + Q) = u$ y $\omega(P + Q) = \min\{\omega(P), \omega(Q)\}$.

Diremos entonces que la aplicación ω es una *pseudo-valoración* de $K(X)$ respecto de la valoración v (o que el par (v, ω) es un *par de valoración*).

Sea $P(X) \in \mathcal{O}[X]$ un polinomio no nulo. Vamos a definir ahora el polígono de Newton y el polinomio asociado del polinomio $P(X)$. Por sucesivas divisiones por el polinomio $\phi(X)$, podemos escribir, y en forma única,

$$P(X) = \sum_{i=0}^{[\mathrm{gr}(P)/m]} A_i(X)\,\phi(X)^i \qquad (1.\,1.\,1)$$

con los $A_i(X) \in \mathcal{O}[X]$ de grado menor que m. A esta expresión la llamaremos el desarrollo ϕ-ádico del polinomio $P(X)$.

1.1. Definición. *Llamaremos polígono de Newton del polinomio $P(X)$ respecto de la valoración v y del polinomio $\phi(X)$, y lo denotaremos por*

$\mathbf{N}_{(v,\phi)}(P)$ *o abreviadamente por* $\mathbf{N}(P)$, *a la envolvente convexa inferior del conjunto de puntos del plano euclideo*

$$\mathbf{D}(P) = \mathbf{D}_{(v,\phi)}(P) := \{(i, u_i) : 0 \leq i \leq [\mathrm{gr}(P)/m], A_i(X) \neq 0\},$$

donde $u_i := v(A_i)$. *Al conjunto* $\mathbf{D}(P)$ *le llamaremos el diagrama de Newton del polinomio* $P(X)$ *respecto de la valoración* v *y del polinomio* $\phi(X)$.

Llamaremos parte principal del polígono $\mathbf{N}(P)$, *y lo denotaremos por* $\mathbf{N}^0(P)$, *al polígono obtenido al considerar sólo los lados con pendiente negativa de* $\mathbf{N}(P)$. *Cuando el polígono* $\mathbf{N}(P)$ *no tenga lados con pendiente negativa, entenderemos que su parte principal se reduce al primer vértice (vértice con menor abscisa) del polígono.*

El siguiente lema nos indica cómo es la forma típica del polígono $\mathbf{N}(P)$, la cual es mostrada en la figura 1.1. En este polígono se pueden leer los valores $v_\phi(P)$, $v(P)$ y $\omega(P)$ de la siguiente manera.

1.2. Lema. *Con las notaciones anteriores, tenemos*

(a) $v_\phi(P) = \min\{i : A_i(X) \neq 0\}$.

(b) $v(P) = \min\{u_i : i\}$.

(c) $\omega(P) = \min\{i : u_i = v(P)\}$. □

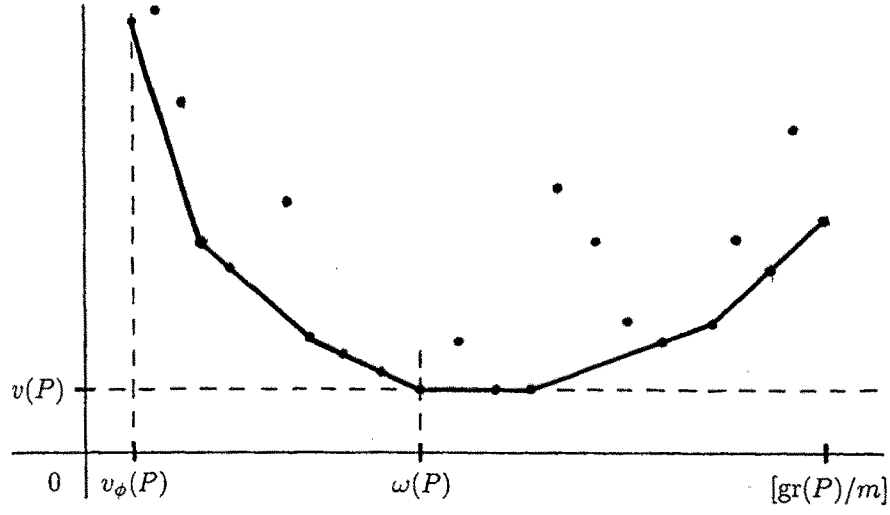


Figura 1.1. $\mathbf{D}(P)$, $\mathbf{N}(P)$ y $\mathbf{N}^0(P)$.

1.3. Observaciones. (1). En este capítulo veremos que la parte principal contiene la información que nos interesa del polinomio $P(X)$ con respecto a $\psi(Y)$ (cf. teoremas de 3.1, 3.5, 4.5 y 4.8). En la práctica esto significará que solamente habremos de trabajar con los polinomios $A_i(X)$ para $i \leq \omega(P)$, el resto ni siquiera necesitaremos calcularlos.

(2). El polígono $\mathbf{N}_{(v,\phi)}(P)$ depende del polinomio mónico $\phi(X) \in \mathcal{O}[X]$ que reduce a $\psi(Y)$ fijado. Por ejemplo, consideremos el polinomio

$$P(X) := \phi(X)^2 + \pi(\pi+2)\,\phi(X) + \pi^2(\pi^3+\pi+1) \in \mathcal{O}[X]\,.$$

Entonces el polígono $\mathbf{N}_{(v,\phi)}(P)$ consta de un solo lado de pendiente -1; mientras que para el polinomio mónico $\phi'(X) := \phi(X) + \pi \in \mathcal{O}[X]$, que también reduce a $\psi(Y)$, el polígono $\mathbf{N}_{(v,\phi')}(P)$ consta de dos lados, como muestra la igualdad

$$P(X) = \phi'(X)^2 + \pi^2\phi'(X) + \pi^5.$$

Con el teorema del polígono (cf. 3.1) veremos que el polinomio $\phi'(X)$ nos proporciona más información sobre el polinomio $P(X)$ que $\phi(X)$. En el §2 del capítulo 3 se verá un método general para hallar con el polígono un "buen representante".

Sean $h, e \geq 1$ enteros primos entre si y S cualquier segmento del plano euclideo con pendiente $-h/e$, de origen (α, β) y final $(\alpha + de, \beta - dh)$ con $\alpha, \beta, d \geq 0$ enteros. Así, los puntos con coordenadas enteras del segmento S son exactamente los $d+1$ puntos

$$(\alpha + je, \beta - jh)\,, \quad j = 0, \ldots, d\,.$$

Para poder definir el *polinomio asociado al polinomio* $P(X)$ *y al segmento* S necesitaremos que se satisfaga la siguiente condición:

Para todo entero j, $0 \leq j \leq d$, el punto $(\alpha + je, u_{\alpha+je})$ está por encima del segmento S o tocando a este segmento (es decir, cada $u_{\alpha+je} \geq \beta - jh$).

La condición anterior se satisface para los segmentos con pendiente $-h/e$ que contienen al segmento con pendiente $-h/e$ del polígono $\mathbf{N}^0(P)$. Cuando este polígono no tenga lados con pendiente igual a $-h/e$, entenderemos que su segmento con pendiente $-h/e$ está formado por el vértice que se obtiene

al levantar paralelamente la recta con pendiente $-h/e$ que pasa por el origen hasta que toca a este polígono.

El polinomio asociado tendrá sus coeficientes en el cuerpo finito $\mathbb{F}_{q_1}$. Asociamos a cada término $A_i(X)\,\phi(X)^i$ con $\alpha \le i \le \alpha + de$, $i \equiv \alpha \pmod{e}$, un elemento de $\mathbb{F}_{q_1}$, definiendo el polinomio

$$B_i(X) := A_i(X)/\pi^{\beta-(i-\alpha)h/e} \in \mathcal{O}[X]$$

y considerando el elemento $\overline{B_i}(\zeta) \in \mathbb{F}_{q_1}$; el cual es no nulo si y sólo si el punto $(i, u_i) \in S$.

1.4. Definición. *Definimos el polinomio asociado al polinomio $P(X)$ y al segmento S como*

$$P_S(Y) := \sum_{i:(i,u_i)\in S} \overline{B_i}(\zeta)\, Y^{(i-\alpha)/e} \in \mathbb{F}_{q_1}[Y].$$

1.5. Observaciones. (1). El polinomio asociado es independiente, a menos de un cambio lineal de la indeterminada Y, del uniformizante $\pi \in \mathcal{O}$ de v fijado. En efecto, el polinomio asociado construido con un nuevo uniformizante $\pi' \in \mathcal{O}$ de v es igual a $c^{-\beta}\, P_S(c^h Y)$, donde $c := \overline{\pi'/\pi} \in \mathbb{F}_q^*$.

(2). El polinomio asociado también es independiente, salvo conjugación, de la raíz $\zeta \in \mathbb{F}_p^{al}$ de $\psi(Y)$ fijada. En efecto, el polinomio asociado construido con otra raíz $\zeta' \in \mathbb{F}_p^{al}$ de $\psi(Y)$ es igual a $P_S^{\sigma}(Y)$ donde $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_1}/\mathbb{F}_q)$ es el único automorfismo tal que $\sigma(\zeta) = \zeta'$.

(3). El coeficiente en $Y^{(i-\alpha)/e}$ del polinomio asociado es no nulo si y sólo si el punto $(i, u_i) \in S$. Por tanto, si S es el segmento con pendiente $-h/e$ del polígono $\mathrm{N}^0(P)$, $P_S(Y)$ es un polinomio de grado d y con término constante no nulo; pero, si S está por debajo de la recta que contiene al segmento con pendiente $-h/e$ del polígono $\mathrm{N}^0(P)$, el polinomio $P_S(Y) = 0$.

(4). Supongamos que el segmento S contiene al segmento con pendiente $-h/e$ del polígono $\mathrm{N}^0(P)$. Si S' es un segmento con pendiente $-h/e$ conteniendo a S de origen (α', β'), entonces $P_{S'}(Y) = Y^{(\alpha-\alpha')/e} P_S(Y)$, ya que la parte $S' \setminus S$ no contiene ningún punto (i, u_i).

(5). Si $Q(X) \in \mathcal{O}[X]$ es un polinomio no nulo distinto de $-P(X)$ para el cual podemos definir el polinomio asociado $Q_S(Y)$, entonces para $P(X) + Q(X)$

también podemos definir el polinomio asociado $(P+Q)_S(Y)$ y se tiene $(P+Q)_S(Y) = P_S(Y) + Q_S(Y)$.

(6). Si $A \in \mathcal{O}^*$, entonces $\mathrm{N}(AP) = \mathrm{N}(P)$ y $(AP)_S(Y) = \overline{A}P_S(Y)$.

A continuación, introducimos un polinomio de $K[X]$, también asociado al polinomio $P(X)$ y al segmento S, y que de hecho motiva la definición del polinomio $P_S(Y) \in \mathbb{F}_{q_1}[Y]$.

1.6. Definición. *Definimos el polinomio* $P^S(X) := \dfrac{P^o(X)}{\phi(X)^\alpha \pi^\beta} \in K[X]$, *donde* $P^o(X) := \displaystyle\sum_{i:(i,u_i)\in S} A_i(X)\,\phi(X)^i \in \mathcal{O}[X]$.

1.7. Observaciones. (1). Por definición, los polinomios $P(X)$ y $P^o(X)$ tienen el mismo polinomio asociado; es decir, $P_S(Y) = (P^o)_S(Y)$ en $\mathbb{F}_{q_1}[Y]$.

(2). Si ponemos $\gamma(X) := \phi(X)^e/\pi^h \in K[X]$, entonces tenemos la igualdad

$$P^S(X) = \sum_{i:(i,u_i)\in S} B_i(X)\,\gamma(X)^{(i-\alpha)/e}.$$

(3). Sea $\theta \in \mathbb{Q}_p^{al}$ un entero algebraico tal que el valor $v(\phi(\theta)) = h/e$, y ponemos $L := K(\theta)$. Entonces el elemento $\overline{\theta} \in \mathbb{F}_L$ es también una raíz de $\psi(Y)$, $v(\gamma(\theta)) = 0$, $v(P^S(\theta)) \geq 0$ y

$$\overline{P^S(\theta)} = P_S^\sigma\left(\overline{\gamma(\theta)}\right) \text{ en } \mathbb{F}_L\,,$$

donde $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_1}/\mathbb{F}_q)$ es el único automorfismo tal que $\sigma(\zeta) = \overline{\theta}$.

Terminamos esta primera sección, definiendo de forma análoga el polígono de Newton y el polinomio asociado para un ϕ-desarrollo arbitrario de nuestro polinomio $P(X)$,

$$P(X) = \sum_{i\geq 0} A_i'(X)\,\phi(X)^i \qquad (1.\,1.\,2)$$

con los polinomios $A_i'(X) \in \mathcal{O}[X]$ casi todos nulos (no necesariamente de grado menor que m).

1.8. Definición. *Llamaremos polígono de Newton del ϕ-desarrollo* (1.1.2) *del polinomio $P(X)$ respecto de la valoración v y del polinomio $\phi(X)$, y*

lo denotaremos por $\mathbf{N}_{(v,\phi)}(P,\{A_i'\})$ *o abreviadamente por* $\mathbf{N}(P,\{A_i'\})$, *a la envolvente convexa inferior del conjunto finito de puntos del plano euclideo*

$$\mathbf{D}(P,\{A_i'\}) = \mathbf{D}_{(v,\phi)}(P,\{A_i'\}) := \{(i,u_i') : i \geq 0, A_i'(X) \neq 0\},$$

donde $u_i' := v(A_i')$. *Al conjunto* $\mathbf{D}(P,\{A_i'\})$ *le llamaremos el diagrama de Newton del* ϕ*-desarrollo* (1.1.2) *del polinomio* $P(X)$ *respecto de la valoración* v *y del polinomio* $\phi(X)$.

Llamaremos parte principal del polígono $\mathbf{N}(P,\{A_i'\})$, *y lo denotaremos por* $\mathbf{N}^0(P,\{A_i'\})$, *al polígono obtenido al considerar sólo los lados con pendiente negativa de* $\mathbf{N}(P,\{A_i'\})$.

Sea S un segmento con datos $(\alpha,\beta), d, e, h$ con el mismo significado que antes. Suponemos ahora que el punto $(\alpha + j\,e, u'_{\alpha+j\,e})$ está por encima de o tocando a S para $0 \leq j \leq d$.

1.9. Definición. *Definimos el polinomio asociado al* ϕ*-desarrollo* (1.1.2) *del polinomio* $P(X)$ *y al segmento* S *como*

$$(P,\{A_i'\})_S(Y) := \sum_{i:(i,u_i')\in S} \overline{B_i'}(\zeta)\, Y^{(i-\alpha)/e} \in \mathbb{F}_{q_1}[Y],$$

donde cada $B_i'(X) := A_i'(X)/\pi^{\beta-(i-\alpha)h/e} \in \mathcal{O}[X]$.

1.10. Observación. Ahora, el coeficiente en $Y^{(i-\alpha)/e}$ del polinomio asociado $(P,\{A_i'\})_S(Y)$ es no nulo si y sólo si $(i,u_i') \in S$ y $\omega(A_i') = 0$.

§2. Desarrollos admisibles. Teorema del producto

Para los propositos que perseguimos, será básico y crucial saber obtener, para un producto de un número finito de polinomios, la parte principal de su polígono de Newton y el polinomio asociado a cada uno de sus lados a partir de los de cada uno de los factores. El problema principal que nos encontramos entonces es que cuando tenemos desarrollos ϕ-ádicos de cada factor y hacemos su producto el ϕ-desarrollo que nos sale no es necesariamente el ϕ-ádico. Por consiguiente, para un polinomio de $\mathcal{O}[X]$, estamos

interesados en conocer con qué desarrollos ya obtenemos la parte principal de su polígono de Newton y el polinomio asociado a cada uno de sus lados.

2.1. Proposición. *Sea $P(X) \in \mathcal{O}[X]$ un polinomio no nulo. Consideramos los enteros (eventualmente $+\infty$) $u_i := v(A_i)$ y $u'_i := v(A'_i)$ correspondientes a los ϕ-desarrollos* (1.1.1) *y* (1.1.2), *respectivamente, del polinomio $P(X)$. Sean $i_0 \leq i_g$ las abscisas del primer y último vértice, respectivamente, del polígono $\mathbf{N}^0(P, \{A'_i\})$. Sean $h, e \geq 1$ enteros primos entre si, S el segmento con pendiente $-h/e$ de $\mathbf{N}^0(P, \{A'_i\})$, y (α, β), $(\alpha + de, \beta - dh)$ los extremos de S. Entonces*

(a) *El polígono $\mathbf{N}(P)$ está "por encima" del polígono $\mathbf{N}^0(P, \{A'_i\})$; es decir,*

(i) *$A_i(X) = 0$, para $0 \leq i < i_0$,*

(ii) *(i, u_i) está por encima de o tocando a S, para $\alpha \leq i \leq \alpha + de$, y*

(iii) *$u_i \geq u'_{i_g}$, para todo $i \geq 0$.*

(b) *Para todo i, $\alpha \leq i \leq \alpha + de$, se tiene la equivalencia*

$$(i, u_i) \in S \iff (i, u'_i) \in S \text{ y } \omega(A'_i) = 0;$$

además, en tal caso, se tiene la igualdad $\overline{B_i}(\zeta) = \overline{B'_i}(\zeta)$ en $\mathbb{F}_{q_1}$, donde $B_i(X) := A_i(X)/\pi^{\beta-(i-\alpha)h/e}$ y $B'_i(X) := A'_i(X)/\pi^{\beta-(i-\alpha)h/e}$.

DEMOSTRACIÓN. Sea $A'_j(X) = \sum_{k \geq 0} A'_{j,k}(X)\, \phi(X)^k$ el desarrollo ϕ-ádico del polinomio $A'_j(X)$, $j \geq 0$. Así, por la unicidad del desarrollo ϕ-ádico, obtenemos que

$$A_i(X) = \sum_{j \leq i} A'_{j,i-j}(X), \quad i \geq 0; \tag{$*$}$$

por tanto, teniendo en cuenta que $A'_j(X) = 0$ para $j < i_0$, tenemos (i) de la parte (a). Además, por la parte (b) del lema de 1.2 aplicado al polinomio $A'_j(X)$, se tiene que

$$u'_j \leq v(A'_{j,i-j}), \quad 0 \leq j \leq i; \tag{$**$}$$

de donde se deduce (iii) de la parte (a), teniendo presente la igualdad de $(*)$ y que $u'_j \geq u'_{i_g}$ para todo $j \geq 0$.

Ahora, consideremos un entero i tal que $\alpha \leq i \leq \alpha + de$, y ponemos $\mu_i := \beta - (i-\alpha)h/e \in \mathbb{Q}$. Entonces, por la igualdad de $(*)$, podemos escribir $A_i(X) = A'_{i,0}(X) + R_i(X)$ con $R_i(X) \in \mathcal{O}[X]$ y $v(R_i) > \mu_i$, por la desigualdad de $(**)$ y puesto que $u'_j > \mu_i$ para $j < i$. Por consiguiente, como $v(A'_{i,0}) \geq u'_i \geq \mu_i$, obtenemos que $u_i \geq \mu_i$ y las equivalencias

$$u_i = \mu_i \iff v(A'_{i,0}) = u'_i = \mu_i \iff u'_i = \mu_i \text{ y } \omega(A'_i) = 0,$$

la última equivalencia por la parte (c) del lema de 1.2. Además, si $u_i = \mu_i$, tenemos $\overline{B_i}(Y) = \overline{B'_{i,0}}(Y)$ en $\mathbb{F}_q[Y]$, donde $B'_{i,0}(X) := A'_{i,0}(X)/\pi^{\mu_i} \in \mathcal{O}[X]$; pero, como el polinomio $\phi(X)$ divide a $B'_i(X) - B'_{i,0}(X)$ en $\mathcal{O}[X]$, entonces $\overline{B'_i}(\zeta) = \overline{B'_{i,0}}(\zeta) = \overline{B_i}(\zeta)$ en $\mathbb{F}_{q_1}$. Con esto hemos visto (ii) de la parte (a) y la parte (b), que era lo que nos faltaba para probar la proposición. □

La proposición anterior nos lleva a la siguiente

2.2. Definición. *El ϕ-desarrollo* (1.1.2) *de un polinomio no nulo $P(X) \in \mathcal{O}[X]$ diremos que es admisible cuando $\omega(A'_i) = 0$ para todo entero i tal que el punto (i, u'_i) pertenece al conjunto de vértices del polígono $\mathrm{N}^0(P, \{A'_i\})$.*

Desde luego, el desarrollo ϕ-ádico de un polinomio siempre es admisible. Pues bien, de la proposición anterior y la observación de 1.10 se deduce el siguiente corolario, que responde a la pregunta que nos formulábamos al comienzo de la sección.

2.3. Corolario. *Sea $P(X) = \sum_{i \geq 0} A'_i(X)\,\phi(X)^i$ un ϕ-desarrollo admisible de un polinomio no nulo $P(X) \in \mathcal{O}[X]$. Entonces*

(a) $\mathrm{N}^0(P, \{A'_i\}) = \mathrm{N}^0(P)$.

(b) $(P, \{A'_i\})_S(Y) = P_S(Y)$ *para cada segmento S del polígono* $\mathrm{N}^0(P)$. □

2.4. Observación. Cambiando de cuerpo base y, en ocasiones, de polinomio con los que estamos trabajando, siempre podemos suponer, tanto conceptualmente como a la hora de hacer demostraciones, que el grado m de nuestro polinomio $\psi(Y)$ es igual a uno. En efecto, sea $K' \subset \mathbb{Q}_p^{al}$ la extensión no ramificada de K de grado m. Entonces la valoración $v_{K'} = v$ y el cuerpo residual $\mathbb{F}_{K'} = \mathbb{F}_{q_1}$; luego, la valoración v' de $K'(X)$ que extiende

a $v_{|K'}$ de forma que $v'(X) = 0$ (cf. §1) restringida a $K(X)$ coincide con v. Descomponemos el polinomio $\psi(Y)$ en $\mathbb{F}_{q_1}[Y]$ en la forma

$$\psi(Y) = \psi'(Y)\,\varphi(Y), \quad \psi'(Y) := Y - \zeta \in \mathbb{F}_{q_1}[Y], \quad \varphi(Y) \in \mathbb{F}_{q_1}[Y];$$

así, $c := \varphi(\zeta) \in \mathbb{F}_{q_1}^*$ y la pseudo-valoración ω' de $K'(X)$ respecto de v' asociada al polinomio $\psi'(Y)$ (cf. §1) restringida a $K(X)$ coincide con ω. Podemos escribir entonces (por el lema de Hensel)

$$\phi(X) = \phi'(X)\,\rho(X)$$

con $\phi'(X), \rho(X) \in \mathcal{O}_{K'}[X]$ mónicos, $\overline{\phi'}(Y) = \psi'(Y)$ y $\overline{\rho}(Y) = \varphi(Y)$; por tanto, $v'(\rho) = 0$ y $\omega'(\rho) = 0$.

Sea $P(X) \in \mathcal{O}[X]$ un polinomio no nulo. Si $P(X) = \sum A_i(X)\,\phi(X)^i$ es el desarrollo ϕ-ádico de $P(X)$, y substituimos en él $\phi(X)$ por $\phi'(X)\,\rho(X)$, entonces se tiene que

$$P(X) = \sum A_i'(X)\,\phi'(X)^i, \quad A_i'(X) := A_i(X)\,\rho(X)^i \in \mathcal{O}_{K'}[X],$$

y que este ϕ'-desarrollo de $P(X)$ es admisible, puesto que cada $\omega'(A_i') = 0$. Además, cada $v'(A_i') = v(A_i)$. Aplicando el corolario de 2.3 (en K'), vemos entonces que se satisfacen las propiedades

(a) $\mathbf{N}^0_{(v',\phi')}(P) = \mathbf{N}^0_{(v,\phi)}(P)$.

(b) Para cada segmento S del polígono $\mathbf{N}^0_{(v',\phi')}(P)$, de origen (α,β) y pendiente $-h/e$, su polinomio asociado en K', denotado por $P_S'(Y)$, es igual a $P_S'(Y) = c^\alpha P_S(c^e Y)$.

En algunas ocasiones se habrá de demostrar cierta propiedad para un polinomio irreducible de $\mathcal{O}[X]$. Entonces al cambiar de cuerpo base de K a K' se perderá la irreducibilidad del polinomio, pero podremos reducirnos a demostrar la propiedad para uno de sus factores irreducibles en $K'[X]$. En efecto, sea ahora $P(X) \in \mathcal{O}[X]$ un polinomio mónico. Ponemos $a := \omega(P) = \omega'(P)$, entonces podemos escribir

$$P(X) = Q(X)\,R(X)$$

con $Q(X), R(X) \in \mathcal{O}_{K'}[X]$ mónicos, $\overline{Q}(Y) = \psi'(Y)^a$ y $\lambda := \overline{R}(\zeta) \in \mathbb{F}_{q_1}^*$; así, $v'(R) = 0$ y $\omega'(R) = 0$. Trabajando con el ϕ'-desarrollo admisible de

$P(X)$ obtenido al introducir $R(X)$ dentro del desarrollo ϕ'-adico de $Q(X)$, y aplicando de nuevo el corolario de 2.3 (en K'), vemos ahora que se satisfacen las propiedades

(c) $\mathrm{N}^0_{(v',\phi')}(P) = \mathrm{N}_{(v',\phi')}(Q)$.

(d) $P'_S(Y) = \lambda Q'_S(Y)$ para cada segmento S del polígono anterior.

Queda justificada pues la afirmación del principio de esta observación; y que podemos suponer incluso que nuestro polinomio $\phi(X)$ es igual a X (cambiando el anterior $Q(X)$ por $Q(X+A)$, donde $\phi'(X) =: X - A$). Sin embargo, es importante hacer notar que la idea de Ore de considerar el polígono de Newton respecto de (v,ϕ) es indispensable en la práctica para obtener algorítmicamente los resultados que nos interesan (descomposición de primos en cuerpos de números) trabajando a partir del polinomio original de partida.

A continuación, pasaremos a enunciar el teorema del producto, para lo cual nos será conveniente definir antes la "suma" de las partes principales de los polígonos de Newton de dos polinomios. Sean $h, e \geq 1$ enteros primos entre si. En el conjunto Γ de los segmentos (orientados) del plano euclideo con pendiente $-h/e$, al cual entenderemos que pertenecen todos los segmentos formados por un solo punto, definimos la suma $S_1 + S_2$ de dos segmentos $S_1, S_2 \in \Gamma$ de la manera usual. Si (α_ν, β_ν) y $(\alpha'_\nu, \beta'_\nu)$ son el origen (extremo con menor abscisa) y final (extremo con mayor abscisa), respectivamente, de S_ν $(\nu = 1,2)$, definimos $S_1 + S_2$ como el segmento de Γ de origen $(\alpha_1 + \alpha_2, \beta_1 + \beta_2)$ y final $(\alpha'_1 + \alpha'_2, \beta'_1 + \beta'_2)$. Con esta operación $+$ el conjunto Γ tiene estructura de monoide conmutativo, cuyo elemento neutro es el segmento $\{(0,0)\}$.

Si $\mathrm{N}^0(P_1)$ y $\mathrm{N}^0(P_2)$ son las partes principales de los polígonos de Newton de dos polinomios no nulos $P_1(X), P_2(X) \in \mathcal{O}[X]$, definimos ahora su suma, y la denotaremos por $\mathrm{N}^0(P_1) + \mathrm{N}^0(P_2)$, como el polígono que se obtiene al sumar los segmentos con pendiente $-h/e$ de cada parte, al recorrer $-h/e$ el conjunto de las pendientes de los lados de las dos partes. (Recordar que si un polígono $\mathrm{N}^0(P_\nu)$ no tiene lados con pendiente igual a $-h/e$, entendemos que su segmento con pendiente $-h/e$ está formado por el vértice que se obtiene al levantar paralelamente la recta con pendiente

$-h/e$ que pasa por el origen hasta que toca a este polígono.) Si las dos partes principales están formadas por un solo punto, $\mathrm{N}^0(P_\nu) = \{(\alpha_\nu, \beta_\nu)\}$ $(\nu = 1, 2)$, entenderemos que $\mathrm{N}^0(P_1) + \mathrm{N}^0(P_2) := \{(\alpha_1 + \alpha_2, \beta_1 + \beta_2)\}$.

Resumiendo, la suma $\mathrm{N}^0(P_1) + \mathrm{N}^0(P_2)$ es el polígono obtenido al pintar el punto $(\omega(P_1) + \omega(P_2), v(P_1) + v(P_2))$ y a continuación los lados trasladados de cada polígono $\mathrm{N}^0(P_\nu)$ en orden decreciente de pendientes (cf. lema de 1.2).

2.5. Teorema. (Teorema del producto) *Sean $P_1(X), \ldots, P_g(X) \in \mathcal{O}[X]$ polinomios no nulos y $P(X) := P_1(X) \cdots P_g(X)$ su producto. Sean $h, e \geq 1$ enteros primos entre si, S_ν el segmento con pendiente $-h/e$ del polígono $\mathrm{N}^0(P_\nu)$, $1 \leq \nu \leq g$, y $S := S_1 + \cdots + S_g$. Entonces*

(a) *S es el segmento con pendiente $-h/e$ del polígono $\mathrm{N}^0(P)$.*

Por tanto, $\mathrm{N}^0(P) = \mathrm{N}^0(P_1) + \cdots + \mathrm{N}^0(P_g)$.

(b) *$P_S(Y) = (P_1)_{S_1}(Y) \cdots (P_g)_{S_g}(Y)$ en $\mathbb{F}_{q_1}[Y]$.* □

Teniendo en cuenta la observación (4) de 1.5, se deduce ahora el siguiente resultado, que será utilizado en el próximo capítulo.

2.6. Corolario. *Sean $h, e \geq 1$ enteros primos entre si. Sea S (resp. T) el segmento con pendiente $-h/e$ del polígono $\mathrm{N}^0(P)$ (resp. $\mathrm{N}^0(Q)$) de un polinomio no nulo $P(X)$ (resp. $Q(X)$) de $\mathcal{O}[X]$, y sea S' un segmento con pendiente $-h/e$ conteniendo a S. Si $Q(X)$ divide a $P(X)$ en $\mathcal{O}[X]$, entonces $Q_T(Y)$ divide a $P_{S'}(Y)$ en $\mathbb{F}_{q_1}[Y]$.* □

§3. Teoremas del polígono y del polinomio asociado

El teorema del producto de la sección anterior muestra que si se tiene un polinomio que es producto de g polinomios de $\mathcal{O}[X]$, cuyas partes principales de sus polígonos de Newton tienen un solo lado y cuyas pendientes son distintas, entonces su parte principal consta de g lados; mientras que si todas las pendientes coinciden y sus polinomios asociados son primos entre

si dos a dos, entonces su parte principal consta de un solo lado y su polinomio asociado descompone en producto de g polinomios primos entre si dos a dos. Más útiles para nuestros propositos son los recíprocos de Ore de estos dos hechos, que se expondrán en esta sección.

Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico tal que $a := \omega(P) \geq 1$, entonces, por el lema de Hensel, $P(X)$ descompone en $\mathcal{O}[X]$ de la forma

$$P(X) = Q(X)\,R(X)$$

con $Q(X), R(X) \in \mathcal{O}[X]$ mónicos, $\overline{Q}(Y) = \psi(Y)^a$ y $\omega(R) = 0$. Por el teorema del producto, $\mathbf{N}^0(P) = \mathbf{N}^0(Q) = \mathbf{N}(Q)$ y para cada segmento S de este polígono es $P_S(Y) = c\,Q_S(Y)$ en $\mathbb{F}_{q_1}[Y]$, para algún $c \in \mathbb{F}_{q_1}^*$.

Si $\theta \in \mathbb{Q}_p^{al}$ es una raíz de $Q(X)$ y ponemos $L := K(\theta)$, entonces el entero m divide al grado residual $f(L/K)$; además, si $a = 1$, entonces el polinomio $Q(X)$ es irreducible en $K[X]$, la extensión L/K es no ramificada de grado m, el ideal $\mathfrak{p}_L = \pi\mathcal{O}_L$ y el anillo $\mathcal{O}_L = \mathcal{O}[\theta]$. Por tanto, estamos interesados en saber descomponer $Q(X)$ en $\mathcal{O}[X]$ cuando $a \geq 2$.

El próximo teorema nos proporciona una ulterior descomposición de este factor $Q(X)$ de $P(X)$ correspondiente al polinomio $\psi(Y)$, a partir de la descomposición en lados de su polígono de Newton $\mathbf{N}(Q) = \mathbf{N}^0(P)$.

3.1. Teorema. (Teorema del polígono) *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico tal que el polígono $\mathbf{N}^0(P)$ no se reduce a un solo punto; es decir, tal que el valor $v_\phi(P) < \omega(P)$. Sean $S_1, \ldots, S_g$ los lados de $\mathbf{N}^0(P)$ y sean d_i, e_i, h_i los datos asociados a S_i $(1 \leq i \leq g)$. Entonces el factor $Q(X)$ de $P(X)$ correspondiente al polinomio $\psi(Y)$ admite una factorización de la forma*

$$Q(X) = \phi(X)^{v_\phi(P)} \cdot P_1(X) \cdots P_g(X)\,,$$

donde cada $P_i(X) \in \mathcal{O}[X]$ es un polinomio mónico, no divisible por $\phi(X)$, de grado $m\,e_i d_i$, cuyo polígono $\mathbf{N}(P_i)$ consta de un solo lado S_i', con datos d_i, e_i, h_i, y cuyo polinomio asociado a este lado es $(P_i)_{S_i'}(Y) = c_i P_{S_i}(Y)$, para algún elemento $c_i \in \mathbb{F}_{q_1}^*$. Además, para todo i, $1 \leq i \leq g$, si $\theta \in \mathbb{Q}_p^{al}$ es una raíz de $P_i(X)$, tenemos

$$v(\phi(\theta)) = \frac{h_i}{e_i}\,. \quad \square$$

3.2. Definición. *Al polinomio $P_i(X)$ le llamaremos el factor de $P(X)$ correspondiente al polinomio $\psi(Y)$ y a la pendiente $-h_i/e_i$.*

De la definición de la valoración v y del teorema del producto se sigue ahora el siguiente corolario, que nos proporciona la información que más nos interesa sobre el polinomio $P_i(X)$.

3.3. Corolario. *Con las mismas hipótesis y notaciones que en el teorema anterior. Para cada i, $1 \leq i \leq g$, se tiene*

(a) *El número de factores mónicos e irreducibles del polinomio $P_i(X)$ en $K[X]$ es menor o igual que d_i. Cada uno de estos factores tiene grado múltiplo de $m\,e_i$ y su polígono de Newton consta de un solo lado, cuya pendiente es igual a $-h_i/e_i$.*

(b) *Sea $\theta \in \mathbb{Q}_p^{al}$ una raíz de $P_i(X)$ y ponemos $L := K(\theta)$. Entonces el entero e_i divide al índice de ramificación $e(L/K)$ de la extensión L/K. Además, si $d_i = 1$, entonces el polinomio $P_i(X)$ es irreducible en $K[X]$, $e(L/K) = e_i$, $f(L/K) = m$ y $\mathfrak{p}_L = (\phi(\theta)^j/\pi^k)\mathcal{O}_L$, donde j, k son enteros cualesquiera tales que $j\,h_i - k\,e_i = 1$.* □

3.4. Observación. En el caso $d_i = 1$, Ore ve, cuando prueba el teorema del índice, que el conjunto

$$\{\theta^{j_0}\phi(\theta)^{j_1}/\pi^{[j_1 h_i/e_i]} : 0 \leq j_0 < m,\ 0 \leq j_1 < e_i\} \subset \mathcal{O}_L$$

es una base del $\mathcal{O}$-módulo libre $\mathcal{O}_L$.

Después del teorema del polígono y del corolario de 3.3, nuestro interés está en saber descomponer el factor $P_i(X)$ en $\mathcal{O}[X]$ cuando el entero $d_i \geq 2$. El próximo teorema nos proporciona una ulterior descomposición de este factor, a partir de la descomposición en $\mathbb{F}_{q_1}[Y]$ de su polinomio asociado $(P_i)_{S_i'}(Y) = c_i P_{S_i}(Y)$.

3.5. Teorema. (Teorema del polinomio asociado) *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico tal que el polígono $\mathrm{N}^0(P)$ no se reduce a un solo punto; es decir, tal que $v_\phi(P) < \omega(P)$. Sean S un lado de $\mathrm{N}^0(P)$ y d, e, h sus datos. Sea*

$$P_S(Y) = c\,\psi_1(Y)^{a_1} \cdots \psi_g(Y)^{a_g}\,, \quad c \in \mathbb{F}_{q_1}^*\,,$$

la factorización del polinomio asociado $P_S(Y)$ en producto de potencias de distintos polinomios mónicos irreducibles de $\mathbb{F}_{q_1}[Y]$ con grado $f_i := \mathrm{gr}(\psi_i)$. Entonces el factor de $P(X)$ correspondiente al polinomio $\psi(Y)$ y a la pendiente $-h/e$, dado por el teorema del polígono (cf. 3.1 y 3.2), admite una factorización de la forma

$$Q_1(X)\cdots Q_g(X),$$

donde cada $Q_i(X) \in \mathcal{O}[X]$ es un polinomio mónico, de grado $m\,e\,f_i a_i$, cuyo polígono $\mathbf{N}(Q_i)$ consta de un solo lado T_i, con datos $f_i a_i$, e, h, y cuyo polinomio asociado a este lado es igual a $(Q_i)_{T_i}(Y) = c_i\psi_i(Y)^{a_i}$, para algún elemento $c_i \in \mathbb{F}_{q_1}^*$. Además, para todo i, $1 \le i \le g$, si $\theta \in \mathbb{Q}_p^{al}$ es una raíz de $Q_i(X)$ y ponemos $\gamma(X) := \phi(X)^e/\pi^h \in K[X]$, tenemos que el valor $v(\gamma(\theta)) = 0$ y que $\psi_i^\sigma(Y) = \mathrm{Irr}\left(\overline{\gamma(\theta)}, \mathbb{F}_{q_1}, Y\right)$, donde $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_1}/\mathbb{F}_q)$ es el único automorfismo tal que $\sigma(\zeta) = \overline{\theta}$. □

3.6. Definición. *Al polinomio $Q_i(X)$ le llamaremos el factor de $P(X)$ correspondiente al polinomio $\psi(Y)$, a la pendiente $-h/e$ y al polinomio $\psi_i(Y)$ (o, pensando en el próximo capítulo, correspondiente al tipo $(\psi; h/e, \psi_i)$).*

De nuevo con la ayuda del teorema del producto se obtiene la información que nos preocupa de este factor $Q_i(X)$.

3.7. Corolario. *Con las mismas hipótesis y notaciones que en el teorema anterior. Para cada i, $1 \le i \le g$, se tiene*

(a) *El número de factores mónicos e irreducibles del polinomio $Q_i(X)$ en $K[X]$ es menor o igual que a_i. Cada uno de estos factores tiene grado múltiplo de $m\,e\,f_i$, su polígono de Newton consta de un solo lado, con pendiente $-h/e$, y su polinomio asociado a este lado es, salvo constante de $\mathbb{F}_{q_1}^*$, igual a una potencia de $\psi_i(Y)$.*

(b) *Sea $\theta \in \mathbb{Q}_p^{al}$ una raíz de $Q_i(X)$ y ponemos $L := K(\theta)$. Entonces el entero $m\,f_i$ divide al grado residual $f(L/K)$ de la extensión L/K. Además, si $a_i = 1$, entonces el polinomio $Q_i(X)$ es irreducible en $K[X]$, $e(L/K) = e$, $f(L/K) = m\,f_i$ y $\mathfrak{p}_L = (\phi(\theta)^j/\pi^k)\mathcal{O}_L$, donde j, k son enteros cualesquiera tales que $j\,h - k\,e = 1$.* □

3.8. Observaciones. (1). En el caso $a_i = 1$, Ore también ve, al probar el teorema del índice, que el conjunto

$$\{\theta^{j_0}\phi(\theta)^{j_1}/\pi^{[j_1 h/e]} : 0 \le j_0 < m,\ 0 \le j_1 < e\, f_i\} \subset \mathcal{O}_L$$

es una base del $\mathcal{O}$-módulo libre $\mathcal{O}_L$.

(2). El teorema del polinomio asociado y el corolario de 3.7 no son suficientes para nuestros fines, ya que no siempre tenemos que el exponente a_i es igual a uno. En efecto, consideremos el polinomio

$$P(X) := \phi(X)^4 + 2\pi\,\phi(X)^2 + \pi^\nu A(X)\,\phi(X) + \pi^2 \in \mathcal{O}[X]\,,$$

con $\nu \ge 2$ entero, y $A(X) \in \mathcal{O}[X]$ de grado menor que m y $v(A) = 0$. Entonces el polígono de Newton $\mathbf{N}(P)$ consta de un solo lado S, cuya pendiente es $-1/2$, y su polinomio asociado es $P_S(Y) = \left(Y + \overline{1}\right)^2$.

A la vista del ejemplo dado en la observación (2) de 1.3, uno podría pensar que cambiando $\phi(X)$ por un adecuado "representante" de $\psi(Y)$

$$\phi'(X) := \phi(X) + \pi\, M(X)\,, \quad M(X) \in \mathcal{O}[X]\,, \quad \mathrm{gr}(M) < m\,,$$

se nos podría arreglar la situación para poder aplicar el teorema del polinomio asociado y el corolario de 3.7. Pero, es fácil comprobar en este mismo ejemplo que, para cualquier representante $\phi'(X)$ que elijamos, el nuevo polígono $\mathbf{N}_{(v,\phi')}(P)$ sigue siendo el mismo que antes y que su polinomio asociado también es $\left(Y + \overline{1}\right)^2$. Nos quedamos pues sin poder aplicar los teoremas de Ore.

En cambio, los resultados del próximo capítulo nos permitirán deducir en el acto de la igualdad

$$P(X) = \phi_2(X)^2 + \pi^\nu A(X)\,\phi(X)\,, \quad \phi_2(X) := \phi(X)^2 + \pi\,,$$

que el polinomio $P(X)$ es siempre irreducible en $K[X]$; además, si $\theta \in \mathbb{Q}_p^{al}$ es una raíz cualquiera de $P(X)$ y $L := K(\theta)$, con ellos se obtendrá que el valor $v(\phi_2(\theta)) = (2\nu + 1)/4$, $e(L/K) = 4$, $f(L/K) = m$, el ideal

$$\mathfrak{p}_L = \begin{cases} \left(\phi_2(\theta)/\pi^{\nu/2}\right)\mathcal{O}_L & \text{si } \nu \text{ es par,} \\ \left(\phi(\theta)\phi_2(\theta)/\pi^{(\nu+1)/2}\right)\mathcal{O}_L & \text{si } \nu \text{ es impar,} \end{cases}$$

y que el conjunto

$$\{\theta^{j_0}\phi(\theta)^{j_1}\phi_2(\theta)^{j_2}/\pi^{[(2j_1+(2\nu+1)j_2)/4]} : 0 \le j_0 < m,\, j_1, j_2 \in \{0,1\}\} \subset \mathcal{O}_L$$

es una $\mathcal{O}$-base de $\mathcal{O}_L$.

(3). Fijado el primo p, Ore también demuestra que todo cuerpo de números tiene un elemento entero, primitivo sobre $\mathbb{Q}$, tal que para su polinomio irreducible sobre $\mathbb{Q}$ (trabajando en $K := \mathbb{Q}_p$) siempre se obtiene que todas las a_i son uno (cf. [**Or 24**]). Por tanto, después de los trabajos de Hensel, con este polinomio podríamos encontrar la descomposición del primo p en este cuerpo. Desgraciadamente, esta demostración no es constructiva cuando uno parte de un polinomio arbitrario definidor de dicho cuerpo.

(4). En [**Mo-Na 92**] se obtiene una condición computable, más débil que la condición anterior $a_i = 1$, bajo la cual todavía es posible obtener la información que nos interesa sobre el polinomio $Q_i(X)$.

(5). Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico, irreducible, con $a := \omega(P) \ge 1$ y distinto de $\phi(X)$. Entonces $\overline{P}(Y) = \psi(Y)^a$, y el teorema del polígono nos dice que el polígono $\mathbf{N}(P)$ consta de un solo lado S, cuya pendiente $-h/e$ es negativa, y que $v(\phi(\theta)) = h/e$ para cada raíz θ de $P(X)$. Además, el teorema del polinomio asociado nos dice que el polinomio asociado $P_S(Y)$ es (salvo constante) una potencia, $\psi_1(Y)^{a_1}$, de un polinomio mónico e irreducible $\psi_1(Y) \in \mathbb{F}_{q_1}[Y]$, y que $\psi_1(Y) = \mathrm{Irr}\left(\overline{\gamma(\theta)}, \mathbb{F}_{q_1}, Y\right)$ para cada raíz θ de $P(X)$ tal que $\overline{\theta} = \zeta$, donde $\gamma(X) := \phi(X)^e/\pi^h$. De hecho, podemos dar una descripción explícita de todas las raíces del polinomio asociado a partir de las de $P(X)$. Concretamente, se tiene la igualdad

$$P_S(Y)^e = c \prod_{\theta \in Z_1(P)} \left(Y - \overline{\gamma(\theta)}\right),$$

para algún elemento $c \in \mathbb{F}_{q_1}^*$, donde el conjunto

$$Z_1(P) := \{\theta \in \mathbb{Q}_p^{al} : P(\theta) = 0, \overline{\theta} = \zeta\}.$$

En efecto, observemos que el cardinal $\#Z_1(P) = a = \mathrm{gr}(P)/m$ y que, por el lema de 1.2, también $a = e\, f_1\, a_1$, donde $f_1 := \mathrm{gr}(\psi_1)$. Fijemos un elemento $\theta \in Z_1(P)$, y pongamos $L := K(\theta)$. Sea K_1 la extensión no ramificada de K de grado m; así, el cuerpo $K_1 \subseteq L$, el grado $[L : K_1] = a$ y el cuerpo

residual $\mathbb{F}_{K_1} = \mathbb{F}_{q_1}$. Ponemos ahora $F(X) := \mathrm{Irr}(\gamma(\theta), K_1, X) \in \mathcal{O}_{K_1}[X]$ y $n := \mathrm{gr}(F)$. Entonces se tiene que el grado $[L : K_1(\gamma(\theta))] = a/n$, y que $\overline{F}(Y) = \psi_1(Y)^{n/f_1}$ y $\overline{F}(Y)^{a/n} = \psi_1(Y)^{e\,a_1}$. Por consiguiente, para ver la igualdad que antes hemos afirmado se ha de probar que

$$\overline{F}(Y)^{a/n} = \prod_{\theta' \in Z_1(P)} \left(Y - \overline{\gamma(\theta')}\right).$$

Para ello, consideremos las a K_1-inmersiones, $\sigma_1, ..., \sigma_a$, de $L = K_1(\theta)$ en $\mathbb{Q}_p^{al}$. Cada $\sigma_i(\theta)$ es una raíz de $P(X)$ y además $\overline{\sigma_i(\theta)} = \zeta$, ya que el polinomio irreducible $\mathrm{Irr}(\theta, K_1, X) \in \mathcal{O}_{K_1}[X]$ reduce a $(Y - \zeta)^a$ en $\mathbb{F}_{q_1}[Y]$. Por tanto, el conjunto $\{\sigma_1(\theta), ..., \sigma_a(\theta)\} = Z_1(P)$ y obtenemos que

$$F(Y)^{a/n} = \prod_{i=1}^{a}(Y - \sigma_i(\gamma(\theta))) = \prod_{i=1}^{a}(Y - \gamma(\sigma_i(\theta))) = \prod_{\theta' \in Z_1(P)} (Y - \gamma(\theta'))\,;$$

con lo cual se prueba lo que se quería.

Después de la segunda observación anterior, en el próximo capítulo nuestro interés se centrará en descomponer por completo en $\mathcal{O}[X]$ el factor $Q_i(X)$ del teorema de 3.5, cuando $a_i \geq 2$, a partir de información contenida en nuestro polinomio original $P(X)$.

§4. Teoremas de la resultante y del índice

Estamos interesados también en determinar con el polígono la valoración p-ádica del discriminante absoluto de un cuerpo de números, a partir de cualquier ecuación definidora de dicho cuerpo. Para ello es útil introducir la noción de "índice local" de un polinomio mónico y sin raíces múltiples de $\mathcal{O}[X]$ (cf. [**Na 83**]).

Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico e irreducible. Sean $\theta \in \mathbb{Q}_p^{al}$ una raíz de $P(X)$ y $L := K(\theta)$. Trabajando con los factores invariantes de $\mathcal{O}[\theta]$ en $\mathcal{O}_L$ (ambos considerados como $\mathcal{O}$-módulos), y teniendo en cuenta que para todo elemento $A \in \mathcal{O}$, $A \neq 0$, el anillo cociente $\mathcal{O}/A\mathcal{O}$ es finito con $q^{v(A)}$ elementos, obtenemos la igualdad

$$(\mathcal{O}_L : \mathcal{O}[\theta]) = q^{\mathrm{i}(P)},$$

para algún entero $\mathrm{i}(P) = \mathrm{i}_K(P) \geq 0$. Además, tenemos también la relación

$$v(\Delta(P)) = 2\,\mathrm{i}(P) + v(\Delta(L/K))\,,$$

donde $\Delta(P)$ (resp. $\Delta(L/K)$) denota el discriminante del polinomio $P(X)$ (resp. el discriminante de la extensión L/K).

Ahora, sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico y sin raíces múltiples, y sea $P(X) = \prod_{i=1}^{g} P_i(X)$ su factorización como producto de polinomios mónicos e irreducibles de $\mathcal{O}[X]$.

4.1. Definición. *Definimos el entero no negativo*

$$\mathrm{i}(P) = \mathrm{i}_K(P) := \sum_{i=1}^{g} \mathrm{i}(P_i) + \sum_{1 \leq i < j \leq g} v(\mathrm{Res}(P_i, P_j)) \in \mathbb{N}, \qquad (1.\,4.\,1)$$

donde $\mathrm{Res}(P_i, P_j)$ *denota la resultante de los polinomios* $P_i(X)$ *y* $P_j(X)$.

4.2. Observaciones. (1). Teniendo en cuenta la bilinealidad de la resultante respecto del producto, la igualdad de (1.4.1) es válida a posteriori para cualquier descomposición de $P(X)$ como producto de polinomios mónicos de $\mathcal{O}[X]$ (no necesariamente irreducibles).

(2). Si $P(X) \in \mathbb{Z}[X]$ es un polinomio mónico e irreducible, entonces el entero $\mathrm{i}_{\mathbb{Q}_p}(P)$ (pensando $P(X) \in \mathbb{Z}_p[X]$) coincide con la valoración p-ádica del índice usual, $\mathrm{ind}(P)$, del polinomio $P(X)$ (cf. **[Or 26]**, **[Se 79]**). Recordar que el entero $\mathrm{ind}(P) := (R : \mathbb{Z}[\theta]) \geq 1$, donde θ es una raíz cualquiera de $P(X)$ y R es el anillo de enteros del cuerpo de números $\mathbb{Q}(\theta)$, y que se tiene la relación

$$\Delta(P) = \mathrm{ind}(P)^2 \Delta(\mathbb{Q}(\theta))\,,$$

donde $\Delta(\mathbb{Q}(\theta))$ denota el discriminate absoluto de $\mathbb{Q}(\theta)$.

(3). $\mathrm{i}(\phi) = 0$, ya que $\overline{\phi}(Y) = \psi(Y)$ es irreducible en $\mathbb{F}_q[Y]$.

Después de la segunda observación anterior, estamos interesados en calcular con el polígono el entero $\mathrm{i}(P)$. Por la definición de 4.1 para hallar este entero necesitamos calcular los enteros $\mathrm{i}(P_i)$ y los valores $v(\mathrm{Res}(P_i, P_j))$. Aunque en la práctica no conoceremos explícitamente una factorización de

$P(X)$ en $\mathcal{O}[X]$, podemos obtener información de $\mathrm{i}(P)$ a partir del polígono de $P(X)$. En esta línea se encuentran dos resultados fundamentales que exponemos seguidamente; uno de Nart, sobre el cálculo de la valoración de la resultante de dos polinomios, y otro de Ore, sobre el cálculo del entero $\mathrm{i}(P)$. Para cada polinomio mónico e irreducible $\psi(Y) \in \mathbb{F}_q[Y]$, fijamos un polinomio mónico $\phi(X) \in \mathcal{O}[X]$ que reduzca a $\psi(Y)$.

Sean $P(X), Q(X) \in \mathcal{O}[X]$ dos polinomios mónicos y sin raíces comunes. Nos interesa calcular con el polígono el entero $v(\mathrm{Res}(P,Q))$. Recordemos que dados explícitamente los dos polinomios, sabemos calcular directamente la resultante $\mathrm{Res}(P,Q)$ (por ejemplo, usando la idea del algoritmo de Euclides); pero, en general, éste no será nuestro caso, ya que tan solo tendremos información de sus polígonos y de sus polinomios asociados. Recordemos también que se tiene la equivalencia

$$v(\mathrm{Res}(P,Q))=0 \iff \overline{P}(Y) \text{ y } \overline{Q}(Y) \text{ no tienen factores comunes (en } \mathbb{F}_q[Y]).$$

Consideremos ahora un polinomio mónico e irreducible $\psi(Y) \in \mathbb{F}_q[Y]$. Sean $S_1, \ldots, S_g$ (resp. $S'_1, \ldots, S'_{g'}$) los lados del polígono $\mathrm{N}^0_{(v,\phi)}(P)$ (resp. $\mathrm{N}^0_{(v,\phi)}(Q)$), y sean E_i, H_i (resp. E'_j, H'_j) las longitudes de las proyecciones sobre los ejes de abscisas y ordenadas, respectivamente, de cada lado S_i (resp. S'_j).

4.3. Definición. *Definimos el entero no negativo*

$$\mathrm{R}_\psi(P,Q) := m\left(\sum_{i,j} \min\{E_i H'_j, E'_j H_i\} + \varepsilon_\psi(P,Q)\right) \in \mathbb{N},$$

donde el entero

$$\varepsilon_\psi(P,Q) := v_\phi(Q)\cdot\sum_{i=1}^{g} H_i + v_\phi(P)\cdot\sum_{j=1}^{g'} H'_j \in \mathbb{N}.$$

4.4. Observaciones. (1). Si alguna de las dos partes principales $\mathrm{N}^0_{(v,\phi)}(P)$ y $\mathrm{N}^0_{(v,\phi)}(Q)$ se reduce a un solo punto (lo cual pasa cuando alguno de los dos polinomios es de la forma $\phi(X)^\alpha R(X)$, con $\alpha \geq 0$ entero y $R(X) \in \mathcal{O}[X]$ tal que $\overline{R}(Y)$ no es divisible por $\psi(Y)$), entonces entenderemos que el entero $\mathrm{R}_\psi(P,Q) := m \cdot \varepsilon_\psi(P,Q)$.

(2). En nuestras aplicaciones, el entero $\varepsilon_\psi(P,Q)$ será siempre nulo, ya que tendremos $v_\phi(P) = v_\phi(Q) = 0$.

4.5. Teorema. (Teorema de la resultante) *Sean $P(X), Q(X) \in \mathcal{O}[X]$ dos polinomios mónicos y sin raíces comunes.*

(a) *Tenemos*

$$v(\mathrm{Res}(P,Q)) \geq \sum_{\psi(Y)} \mathrm{R}_\psi(P,Q)\,,$$

donde la suma anterior está extendida sobre todos los factores mónicos e irreducibles $\psi(Y) \in \mathbb{F}_q[Y]$ comunes a $\overline{P}(Y)$ y a $\overline{Q}(Y)$.

(b) *La igualdad vale en* (a) *si y sólo si para cada factor mónico e irreducible común a $\overline{P}(Y)$ y a $\overline{Q}(Y)$ no hay dos lados, S y S', de los polígonos $\mathrm{N}^0_{(v,\phi)}(P)$ y $\mathrm{N}^0_{(v,\phi)}(Q)$ con la misma pendiente y polinomios asociados, $P_S(Y)$ y $Q_{S'}(Y)$, con factores comunes (en $\mathbb{F}_{q_1}[Y]$).* □

Pasemos ahora a interesarnos de nuevo por el índice local, $\mathrm{i}(P)$, de un polinomio $P(X) \in \mathcal{O}[X]$ mónico y sin raíces múltiples. Consideremos otra vez un polinomio mónico e irreducible $\psi(Y) \in \mathbb{F}_q[Y]$. Sean $S_1, \ldots, S_g$ los lados del polígono $\mathrm{N}^0_{(v,\phi)}(P)$, y sean $d_i, e_i, h_i, E_i := d_i e_i, H_i := d_i h_i$ los datos asociados a cada lado S_i. Suponemos ordenadas las pendientes de forma que $-h_1/e_1 < \cdots < -h_g/e_g$.

4.6. Definición. *Definimos el entero no negativo*

$$\mathrm{i}_\psi(P) := m(\mathrm{i}^0_\psi(P) + \epsilon_\psi(P)) \in \mathbb{N},$$

donde los enteros

$$\mathrm{i}^0_\psi(P) := \frac{1}{2}\sum_{i=1}^{g}(E_iH_i - E_i - H_i + d_i) + \sum_{1\leq i<j\leq g} E_iH_j \in \mathbb{N},$$

$$\epsilon_\psi(P) := v_\phi(P)\cdot\sum_{i=1}^{g} H_i \in \mathbb{N}.$$

4.7. Observaciones. (1). Si el polígono $\mathrm{N}^0_{(v,\phi)}(P)$ se reduce a un solo punto (es decir, $v_\phi(P) = \omega(P)$), entonces entenderemos que el entero $\mathrm{i}_\psi(P) := 0$; así, $\mathrm{i}_\psi(\phi) = 0$.

(2). El entero $\mathrm{i}^0_\psi(P)$ es igual al número de puntos de coordenadas enteras del recinto acotado delimitado por el polígono $\mathrm{N}^0_{(v,\phi)}(P)$, el eje de abscisas y la recta vertical de ecuación $x = v_\phi(P)$, incluyendo los puntos que están sobre los lados del polígono $\mathrm{N}^0_{(v,\phi)}(P)$, excepto el origen del primer lado y el final del último lado, y excluyendo los puntos que están sobre estas rectas (ver figura 1.2).

(3). En nuestras aplicaciones, el entero $\epsilon_\psi(P)$ será siempre nulo, ya que tendremos que nuestro polinomio $P(X)$ no será divisible por $\phi(X)$.

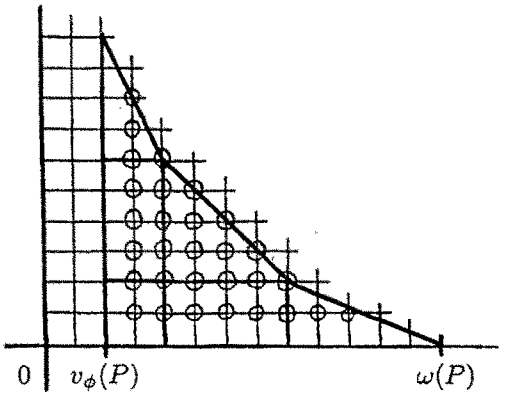


Figura 1.2. $\mathrm{i}^0_\psi(P)$

El siguiente teorema de Ore, por una parte, nos muestra lo que nos "comemos" del entero $\mathrm{i}(P)$ con el polígono de primer orden y, por otra, nos proporciona una condición suficiente para asegurar que ya hemos terminado de calcularlo con él.

4.8. Teorema. (Teorema del índice) *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico y sin raíces múltiples.*

(a) *Tenemos*

$$\mathrm{i}(P) \geq \sum_{\psi(Y)} \mathrm{i}_\psi(P)\,,$$

donde la suma anterior está extendida sobre todos los factores mónicos e irreducibles $\psi(Y) \in \mathbb{F}_q[Y]$ de $\overline{P}(Y)$.

(b) *Si para cada factor mónico e irreducible de $\overline{P}(Y)$ todos los polinomios asociados al polinomio $P(X)$ y a los lados del polígono $\mathrm{N}^0_{(v,\phi)}(P)$ no tienen raíces múltiples, entonces vale la igualdad en* (a). □

4.9. Observaciones. (1). En general, el teorema del índice no es suficiente para calcular el valor exacto del entero $\mathrm{i}(P)$ para cualquier polinomio $P(X)$. En el ejemplo dado en la observacion (2) de 3.8, el teorema nos dice sólo que $\mathrm{i}(P) \geq 2m$, puesto que la condición de la parte (b) no se satisface.

(2) En el teorema 2 de [**Mo-Na 92**] se da una condición necesaria y suficiente para que valga la igualdad en la parte (a) del teorema de 4.8. Esta condición también es computable en términos del polinomio $P(X)$. Así, en el ejemplo citado anteriormente nos dice que $\mathrm{i}(P) = 2m$ si y sólo si $\nu = 2$. De hecho, de los resultados del próximo capítulo se deducirá que en ese ejemplo el entero $\mathrm{i}(P) = \nu\, m$.

CAPÍTULO 2

Polígonos de Newton de orden superior

En este capítulo, desarrollamos inductivamente la teoría de los polígonos de Newton de orden superior. Esta teoría imita, generaliza y completa la teoría del polígono de Newton (de orden uno) de Ore expuesta en el capítulo anterior. Además, esta teoría nos permitirá extraer un algoritmo eficiente para obtener la descomposición de los primos racionales en cualquier cuerpo de números, dado por una ecuación definidora arbitraria, y el valor del discriminante absoluto de dicho cuerpo (cf. capítulo 3).

§1. Notaciones, hipótesis de inducción y tipos

A lo largo de todo este capítulo p denotará un primo racional fijado, y $\mathbb{Q}_p^{al}$ y $\mathbb{F}_p^{al}$ denotarán clausuras algebraicas fijadas de $\mathbb{Q}_p$ y $\mathbb{F}_p$, respectivamente. Para cualquier extensión finita L de $\mathbb{Q}_p$, $L \subset \mathbb{Q}_p^{al}$, denotamos por v_L la valoración standard de $\mathbb{Q}_p^{al}$ normalizada de forma que $v_L(L^*) = \mathbb{Z}$, por $\mathcal{O}_L$ su anillo de valoración en L, por $\mathfrak{p}_L$ su ideal maximal, y por $\mathbb{F}_L$ su cuerpo residual, el cual lo supondremos inmerso en $\mathbb{F}_p^{al}$ de manera que todas las aplicaciones de reducción $\mathcal{O}_L \to \mathbb{F}_L$, denotadas por $a \mapsto \overline{a}$, sean compatibles. Para un polinomio irreducible $\phi(X) \in \mathcal{O}_L[X]$ (resp. $\psi(Y) \in \mathbb{F}_L[Y]$) denotaremos por v_ϕ (resp. v_ψ) la valoración del cuerpo $L(X)$ (resp. $\mathbb{F}_L(Y)$) asociada a este polinomio.

Tomamos una extensión finita K de $\mathbb{Q}_p$, $K \subset \mathbb{Q}_p^{al}$, como cuerpo base

y ponemos $v := v_K$, $\mathcal{O} := \mathcal{O}_K$ y $\mathfrak{p} := \mathfrak{p}_K$. Además, fijamos un uniformizante $\pi \in \mathcal{O}$ de v, y denotamos por q_0 al número de elementos del cuerpo finito $\mathbb{F}_K = \mathbb{F}_{q_0}$.

Fijamos un entero $r \geq 2$ y un *tipo* de orden $r-1$

$$\mathbf{t}_{r-1} := (\psi_0; h_1/e_1, \psi_1; \ldots; h_{r-1}/e_{r-1}, \psi_{r-1}),$$

donde $\psi_0(Y) \in \mathbb{F}_{q_0}[Y]$ es un polinomio mónico irreducible de grado f_0 y para cada i, $1 \leq i \leq r-1$, $h_i, e_i \geq 1$ son enteros primos entre si y $\psi_i(Y) \in \mathbb{F}_{q_i}[Y]$ es un polinomio mónico irreducible de grado f_i con término constante no nulo, donde $q_i := (q_{i-1})^{f_{i-1}} = (q_0)^{f_0 \cdots f_{i-1}}$.* Además, ponemos $e_0 := 1$ y $q_r := (q_{r-1})^{f_{r-1}} = (q_0)^{f_0 \cdots f_{r-1}}$. Así mismo, fijamos una raíz $\zeta_0 \in \mathbb{F}_p^{al}$ de $\psi_0(Y)$ y para cada i, $1 \leq i \leq r-1$, fijamos una raíz $\zeta_i \in \mathbb{F}_p^{al}$ de $\psi_i(Y)$ y un entero l_i tal que $h_i l_i \equiv 1 \pmod{e_i}$. Nótese que cada cuerpo $\mathbb{F}_{q_i}(\zeta_i) = \mathbb{F}_{q_{i+1}}$.

Al tipo $\mathbf{t}^{\circ}_{r-1} := (\psi_0; h_1/e_1, \psi_1; \ldots; h_{r-2}/e_{r-2}, \psi_{r-2}; h_{r-1}/e_{r-1})$ (quitamos el polinomio $\psi_{r-1}(Y)$ del tipo $\mathbf{t}_{r-1}$) le llamaremos tipo *reducido* de orden $r-1$.

Denotaremos por v_1 a la valoración discreta $v_{|K}$ de K extendida a $K(X)$ de manera que $v_1(X) = 0$, y por ω_1 a la pseudo-valoración de $K(X)$ respecto de la valoración v_1 que proviene del polinomio $\psi_0(Y)$ (cf. §1 del capítulo 1). Ponemos $\phi_0(X) := X$, $m_0 := 1$, y fijamos un polinomio mónico arbitrario $\phi_1(X) \in \mathcal{O}[X]$ con grado igual a $m_1 := m_0 e_0 f_0 = f_0$ y tal que $\overline{\phi_1}(Y) = \psi_0(Y)$ en $\mathbb{F}_{q_0}[Y]$. Nótese que el valor $v_1(\phi_1) = 0$ y que $\omega_1(\phi_1) = 1$.

En el capítulo anterior se ha expuesto la teoría de Ore del polígono de Newton (de orden uno) a partir del tipo (ψ_0) de orden 0, del par de valoración (v_1, ω_1) y del polinomio $\phi_1(X)$. La teoría del polígono de Newton de orden r se desarrollará inductivamente a partir del tipo $\mathbf{t}_{r-1}$, de un par de valoración (v_r, ω_r) asociado a $\mathbf{t}_{r-1}$, que será construido en la §2, y de un polinomio $\phi_r(X)$ "representante" de grado mínimo de $\mathbf{t}_{r-1}$, que será construido en la §3.

Algunos de los resultados (resp. las definiciones) de este capítulo serán probados por inducción sobre r (resp. serán dadas inductivamente). En

* Cuando se trabaja en orden r con un tipo $\mathbf{t}_{r-1}$ de orden $r-1$ que tiene s eslabones $(h_i/e_i, \psi_i)$ que satisfacen $e_i f_i > 1$, de hecho se está trabajando en nivel $s+1$ (cf. §2 del capítulo 3).

orden uno estos resultados (resp. estas definiciones) son debidos a Ore y han sido expuestos en el capítulo anterior. Por tanto, hacemos la siguiente hipótesis de inducción:

Suponemos que todos los resultados (resp. las definiciones) de este capítulo son válidos (resp. han sido dadas) en orden i, para $1 \leq i \leq r-1$.

Si $r > 2$, para cada i, $1 \leq i \leq r-2$, denotamos por v_{i+1} a la valoración de $K(X)$ asociada inductivamente a la terna $(v_i, \phi_i, h_i/e_i)$ y por ω_{i+1} a la pseudo-valoración asociada inductivamente a la cuaterna $(v_i, \phi_i, h_i/e_i, \psi_i)$ (cf. §2), y fijamos un polinomio mónico arbitrario $\phi_{i+1}(X) \in \mathcal{O}[X]$ de grado $m_{i+1} := m_i e_i f_i = e_0 f_0 \cdots e_i f_i$ que satisfaga las propiedades siguientes (cf. §3 y §4):

(a) El polígono $\mathbf{N}_i(\phi_{i+1}) := \mathbf{N}_{(v_i,\phi_i)}(\phi_{i+1})$ consta de un solo lado, cuya pendiente es igual a $-h_i/e_i$.

(b) El polinomio asociado (en orden i) al polinomio $\phi_{i+1}(X)$ y a este lado es $c_i\psi_i(Y)$, para algún elemento $c_i \in \mathbb{F}_{q_i}^*$.

Además, ponemos $m_r := m_{r-1}e_{r-1}f_{r-1} = e_0 f_0 \cdots e_{r-1}f_{r-1}$.

A partir de ahora, pensaremos el tipo $\mathbf{t}_{r-1}$ junto con una elección de los polinomios $\phi_i(X)$, $1 \leq i \leq r-1$.

Para cada i, $1 \leq i \leq r-1$, definimos recurrentemente las siguientes fracciones racionales de $K(X)$ asociadas al tipo $\mathbf{t}_{r-1}$

$$\begin{aligned} \Phi_0(X) &:= X, & \gamma_0(X) &:= X, \\ \Pi_1(X) &:= 1, & \pi_1(X) &:= \pi, \\ \Phi_i(X) &:= \frac{\phi_i(X)}{\Pi_i(X)}, & \gamma_i(X) &:= \frac{\Phi_i(X)^{e_i}}{\pi_i(X)^{h_i}}, \\ \Pi_{i+1}(X) &:= \Pi_i(X)^{e_i f_i}\pi_i(X)^{h_i f_i}, & \pi_{i+1}(X) &:= \frac{\Phi_i(X)^{l_i}}{\pi_i(X)^{l_i'}}, \end{aligned}$$

donde $l_i' := (h_i l_i - 1)/e_i \in \mathbb{Z}$. Observemos que cada una de estas fracciones racionales puede ser escrita en la forma

$$\Phi(\mathbf{n})(X) := \pi^{n_0}\phi_1(X)^{n_1} \cdots \phi_{r-1}(X)^{n_{r-1}},$$

para cierto $\mathbf{n} := (n_0, n_1, \ldots, n_{r-1}) \in \mathbb{Z}^r$. Además, tenemos que cada

$$\Pi_{i+1}(X) = \prod_{j=1}^{i} \pi_j(X)^{e_j f_j \cdots e_i f_i h_j/e_j},$$

y también que cada

$$\Phi_i(X) = \cdots \phi_i(X), \qquad \gamma_i(X) = \cdots \phi_i(X)^{e_i},$$
$$\Pi_{i+1}(X) = \cdots, \qquad \pi_{i+1}(X) = \cdots \phi_i(X)^{l_i},$$

donde los puntos suspensivos a continuación de una igualdad indican un producto de potencias enteras de π y de los $\phi_j(X)^{l_j}$ con $1 \leq j < i$.

A continuación, introducimos una definición que usaremos con frecuencia en el resto de este capítulo.

1.1. Definición. *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico. Diremos que $P(X)$ tiene tipo de orden $r-1$ igual a $\{\mathrm{t}_{r-1}\}$ cuando $P(X)$ no sea divisible por ningún polinomio $\phi_i(X)$ $(1 \leq i \leq r-1)$, satisfaga la propiedad*

(0.b) $\overline{P}(Y) = \psi_0(Y)^{a_0}$ *en* $\mathbb{F}_{q_0}[Y]$, *para algún entero* $a_0 \geq 1$.

y para cada i, $1 \leq i \leq r-1$, satisfaga las propiedades siguientes

(i.a) *El polígono $\mathrm{N}_i(P)$ consta de un solo lado, cuya pendiente es igual a $-h_i/e_i$.*

(i.b) *El polinomio asociado (en orden i) al polinomio $P(X)$ y a este lado es $c_i\,\psi_i(Y)^{a_i}$ en $\mathbb{F}_{q_i}[Y]$, para algún elemento $c_i \in \mathbb{F}_{q_i}^*$ y para algún entero $a_i \geq 1$.*

Diremos que un entero algebraico $\theta \in \mathbb{Q}_p^{al}$ tiene tipo de orden $r-1$ igual a $\{\mathrm{t}_{r-1}\}$ cuando lo tenga su polinomio irreducible sobre K.

Acabamos esta sección viendo una caracterización de los polinomios que tienen tipo de orden $r-1$ igual a $\{\mathrm{t}_{r-1}\}$.

1.2. Proposición. *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico. Entonces las condiciones siguientes son equivalentes:*

(1) *$P(X)$ tiene tipo de orden $r-1$ igual a $\{\mathrm{t}_{r-1}\}$.*

(2) *$P(X)$ no es divisible por ningún polinomio $\phi_i(X)$ $(1 \leq i \leq r-1)$, tiene grado múltiplo de m_{r-1} y satisface las propiedades $(r-1.\mathrm{a})$ y $(r-1.\mathrm{b})$ de la definición de* 1.1.

Además, cuando alguna de las dos condiciones anteriores se satisface, te-

nemos las relaciones

$$a_0 = e_1 f_1 \cdots e_{r-1} f_{r-1} a_{r-1}\,,$$
$$\mathrm{gr}(P) = m_{r-1} a_{r-2} = m_r a_{r-1}\,,$$
$$v_{r-1}(P - (\phi_{r-1})^{a_{r-2}}) > v_{r-1}(P)\,.$$

DEMOSTRACIÓN. Comenzamos suponiendo que se satisface la condición (1). Veamos entonces que el entero $a_0 = e_1 f_1 \cdots e_{r-1} f_{r-1} a_{r-1}$ y que el grado $\mathrm{gr}(P) = m_{r-1} a_{r-2} = m_r a_{r-1}$, con lo cual quedará probada la condición (2). Puesto que $\mathrm{gr}(P) = \mathrm{gr}\,(\overline{P}) = f_0 a_0$, por la propiedad (0.b), entonces nos bastará con probar que $a_{i-1} = e_i f_i a_i$ para cada entero i, $1 \leq i \leq r-1$. Pero, por la propiedad $(i-1.\mathrm{b})$ es $\omega_i(P) = a_{i-1}$, y por el lema de 4.2 en orden i y las propiedades $(i.\mathrm{a})$ y $(i.\mathrm{b})$ tenemos

$$\omega_i(P) = v_{\phi_i}(P) + e_i f_i a_i = e_i f_i a_i\,.$$

De ahí la igualdad $a_{i-1} = e_i f_i a_i$.

Ahora, supongamos que se satisface la condición (2). Probemos que entonces se satisface la condición (1) y que $v_{r-1}(P-(\phi_{r-1})^{a_{r-2}}) > v_{r-1}(P)$; con lo cual quedará demostrado el resto de la proposición. Ponemos $\mathrm{gr}(P) = m_{r-1} a$, con $a \geq 1$ entero. Así, por la propiedad $(r-1.\mathrm{a})$ y el lema de 4.2 en orden $r-1$, podemos escribir

$$P(X) = \phi_{r-1}(X)^a + R(X),$$

donde el polinomio $R(X) \in \mathcal{O}[X]$ tiene grado menor que $m_{r-1} a$ y satisface que el valor $v_{r-1}(R) > v_{r-1}(P)$. Si $r = 2$, entonces $v_1(R) > 0$ y $\overline{P}(Y) = \psi_0(Y)^a$; con lo cual hemos acabado. Supongamos, por tanto, que $r \geq 3$. Por las propiedades (a) y (b) que satisface el polinomio $\phi_{r-1}(X)$ y el teorema del producto (cf. 6.1) en orden $r-2$, tenemos que el polinomio $\phi_{r-1}(X)^a$ satisface las propiedades $(r-2.\mathrm{a})$ y $(r-2.\mathrm{b})$ de la definición de 1.1, para $a_{r-2} = a$. Por la parte (e) de la proposición de 2.2 en orden $r-1$, obtenemos entonces que el polinomio $P(X)$ también satisface las propiedades $(r-2.\mathrm{a})$ y $(r-2.\mathrm{b})$ de la definición de 1.1, para $a_{r-2} = a$. Aplicando esta misma proposición en orden $r-1$, se tiene entonces que $P(X)$ tiene tipo de orden $r-2$ igual a $\{(\psi_0; h_1/e_1, \psi_1; \ldots; h_{r-2}/e_{r-2}, \psi_{r-2})\}$. Con esto vemos que se satisface la condición (1) y la desigualdad que queríamos. □

Del hecho que cada polinomio $\phi_i(X)$ es irreducible en $K[X]$ (cf. parte (a) del corolario de 3.4 en orden i) y del teorema del producto (cf. 6.1) en orden $r-1$, se deduce el siguiente

1.3. Corolario.

(a) *Si $P(X), Q(X) \in \mathcal{O}[X]$ son dos polinomios mónicos que tienen tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$, entonces su producto $P(X)\,Q(X)$ también lo tiene.*

(b) *Si $P(X) \in \mathcal{O}[X]$ es un polinomio mónico que tiene tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ y $Q(X) \in \mathcal{O}[X]$ es un polinomio mónico de grado ≥ 1 que divide a $P(X)$, entonces $Q(X)$ también lo tiene.* □

§2. El par de valoración (v_r, ω_r)

Comenzamos esta sección definiendo con el polígono de Newton una valoración discreta v_r de $K(X)$ asociada al tipo reducido $\mathbf{t}^o_{r-1}$ (o si se quiere, asociada a la terna $(v_{r-1}, \phi_{r-1}, h_{r-1}/e_{r-1})$) y una pseudo-valoración ω_r respecto de v_r (cf. §1 del capítulo 1) asociada al tipo $\mathbf{t}_{r-1}$ (o si se quiere, asociada a la cuaterna $(v_{r-1}, \phi_{r-1}, h_{r-1}/e_{r-1}, \psi_{r-1})$). Valoraciones de este tipo fueron introducidas, y estudiadas sus propiedades, por MacLane (cf. [**Ma 36a**]). Después calcularemos los valores de los polinomios $\phi_i(X)$ y de las fracciones racionales, definidas en la sección anterior, asociadas a nuestro tipo de orden $r-1$; en particular, veremos que $v_r(\pi_r) = 1$, lo cual nos dirá que el grupo de valores de v_r es $\mathbb{Z}$ y que $\pi_r(X)$ es un uniformizante para v_r. Finalmente, calcularemos explícitamente el cuerpo residual de esta valoración; en particular, recuperaremos con el polígono la estructura del cuerpo residual dada por MacLane (cf. corolario 12.2 de [**Ma 36a**]).

Denotamos por Γ_{r-1} al monoide formado por los segmentos del plano euclideo con pendiente $-h_{r-1}/e_{r-1}$ (cf. §2 del capítulo 1). Consideramos el homomorfismo de monoides

$$\mathbf{H}_{r-1} : \Gamma_{r-1} \to \mathbb{R}$$

definido por $\mathbf{H}_{r-1}(S) := h_{r-1}\alpha + e_{r-1}\beta$, donde (α, β) es un punto cualquiera

del segmento $S \in \Gamma_{r-1}$. De esta forma tenemos que la recta con pendiente $-h_{r-1}/e_{r-1}$ que contiene a S corta al eje de ordenadas en el punto $(0, \mathbf{H}_{r-1}(S)/e_{r-1})$, y que $\mathbf{H}_{r-1}(S) \in \mathbb{Z}$ si y sólo si esta recta contiene al menos un punto (y por tanto infinitos puntos) con coordenadas enteras.

Dado un polinomio no nulo $P(X) \in \mathcal{O}[X]$, denotamos por $\mathbf{S}_{r-1}(P)$ el segmento con pendiente $-h_{r-1}/e_{r-1}$ del polígono $\mathbf{N}_{r-1}(P)$ (cf. §4), por $\mathbf{L}_{r-1}(P)$ la recta con pendiente $-h_{r-1}/e_{r-1}$ que contiene a $\mathbf{S}_{r-1}(P)$, cuya ecuación es

$$\mathbf{L}_{r-1}(P): \ h_{r-1}x + e_{r-1}y = \mathbf{H}_{r-1}(\mathbf{S}_{r-1}(P)),$$

y por $\mathbf{F}_{r-1}(P)$ el polinomio asociado (en orden $r-1$) al polinomio $P(X)$ y al segmento $\mathbf{S}_{r-1}(P)$ (cf. §4). Por el teorema del producto (cf. 6.1) en orden $r-1$, tenemos definidos entonces dos homomorfismos de monoides

$$\mathbf{S}_{r-1} : \mathcal{O}[X] \setminus \{0\} \to \Gamma_{r-1}, \qquad \mathbf{F}_{r-1} : \mathcal{O}[X] \setminus \{0\} \to \mathbb{F}_{q_{r-1}}[Y] \setminus \{0\},$$

con la imagen $\mathrm{Im}\,(\mathbf{H}_{r-1} \circ \mathbf{S}_{r-1}) \subset \mathbb{N}$.

2.1. Definición. *Para un polinomio no nulo $P(X) \in \mathcal{O}[X]$, definimos*

$$v_r(P) := \mathbf{H}_{r-1}(\mathbf{S}_{r-1}(P)) \in \mathbb{N}, \qquad \omega_r(P) := v_{\psi_{r-1}}(\mathbf{F}_{r-1}(P)) \in \mathbb{N},$$

donde recordemos que $v_{\psi_{r-1}}$ denota la valoración de $\mathbb{F}_{q_{r-1}}(Y)$ asociada al polinomio irreducible $\psi_{r-1}(Y)$. Para una fracción racional $R(X) \in K(X)^*$, definimos

$$v_r(R) := v_r(P) - v_r(Q) \in \mathbb{Z}, \qquad \omega_r(R) := \omega_r(P) - \omega_r(Q) \in \mathbb{Z},$$

donde $P(X), Q(X) \in \mathcal{O}[X]$ son polinomios no nulos tales que $R(X) = P(X)/Q(X)$. Además, convenimos que $v_r(0) := +\infty$.

De este modo tenemos que las aplicaciones $v_r, \omega_r : K(X)^* \to \mathbb{Z}$ están bien definidas y son homomorfismos de grupos.

2.2. Proposición.

(a) *El homomorfismo $v_r : K(X)^* \to \mathbb{Z}$ determina una valoración discreta de $K(X)$ que extiende a la valoración $v_{|K}$ de K con índice $e_1 \cdots e_{r-1}$.*

(b) *Si* $P(X) = \sum A_i(X)\,\phi_{r-1}(X)^i$ *es el desarrollo* ϕ_{r-1}*-ádico de un polinomio* $P(X) \in \mathcal{O}[X]$ *(cf. §4), entonces*

$$v_r(P) = \min\{e_{r-1}v_{r-1}(A_i) + i(e_{r-1}v_{r-1}(\phi_{r-1}) + h_{r-1}) : i \geq 0\}.$$

En particular, se tiene que

$$\begin{aligned} v_r(P) &= e_{r-1}v_{r-1}(P) \text{ si } \operatorname{gr}(P) < m_{r-1}, \\ v_r(\phi_{r-1}) &= e_{r-1}v_{r-1}(\phi_{r-1}) + h_{r-1}, \\ v_r(P) &= \min\{v_r(A_i\,{\phi_{r-1}}^i) : i \geq 0\}. \end{aligned}$$

(c) *Si* $P(X) \in \mathcal{O}[X]$ *es un polinomio no nulo, entonces*

$$\begin{aligned} &v_r(P) \geq e_{r-1}v_{r-1}(P), \\ &v_r(P) = e_{r-1}v_{r-1}(P) \iff \omega_{r-1}(P) = 0. \end{aligned}$$

(d) *Sea* $\mathfrak{m} := \pi\mathcal{O}[X] + \phi_1(X)\mathcal{O}[X]$ *el ideal maximal de* $\mathcal{O}[X]$ *generado por* π *y por* $\phi_1(X)$*. Para todo polinomio* $P(X) \in \mathcal{O}[X]$ *tenemos que*

$$v_r(P) = 0 \iff v_2(P) = 0 \iff P(X) \notin \mathfrak{m}.$$

En particular, se tiene que

$$v_r(X) = 0 \iff \omega_1(X) = 0 \iff \psi_0(Y) \neq Y.$$

(e) *Si* $P(X), Q(X) \in \mathcal{O}[X]$ *son polinomios no nulos, entonces*

$$v_r(P-Q) > v_r(Q) \iff \mathbf{S}_{r-1}(P) = \mathbf{S}_{r-1}(Q) \text{ y } \mathbf{F}_{r-1}(P) = \mathbf{F}_{r-1}(Q).$$

DEMOSTRACIÓN. Por hipótesis de inducción, sabemos que v_{r-1} es una valoración de $K(X)$ que extiende a la valoración v de K con índice $e_1 \cdots e_{r-2}$. Para todo $A \in \mathcal{O}$, $A \neq 0$, tenemos que $\mathbf{S}_{r-1}(A) = \{(0, v_{r-1}(A))\}$; de donde, $v_r(A) = e_{r-1}v_{r-1}(A) = e_1 \cdots e_{r-1}v(A)$.

Sean $P(X), Q(X) \in \mathcal{O}[X]$ polinomios no nulos y supongamos que $v_r(P) \leq v_r(Q)$. Entonces los puntos del diagrama $\mathbf{D}_{r-1}(P+Q)$ (cf. §4) están por encima de o sobre la recta $\mathbf{L}_{r-1}(P)$; por tanto, $v_r(P+Q) \geq v_r(P)$. Con esto terminamos de probar la parte (a).

Para la parte (b) basta con observar que para cada i la recta con pendiente $-h_{r-1}/e_{r-1}$ que pasa por el punto $(i, v_{r-1}(A_i\,{\phi_{r-1}}^i))$ está por encima de o coincide con la recta $\mathbf{L}_{r-1}(P)$, y hay coincidencia cuando el punto pertenece al segmento $\mathbf{S}_{r-1}(P)$.

La parte (c) es una consecuencia inmediata de las partes (b) y (c) del lema de 4.2 en orden $r-1$.

Veamos la parte (d). Aplicando reiteradamente la parte (c), obtenemos que

$$\begin{aligned} v_r(P) = 0 &\iff v_{r-1}(P) = 0 \text{ y } \omega_{r-1}(P) = 0 \\ &\iff v_1(P) = 0 \text{ y } \omega_1(P) = \cdots = \omega_{r-1}(P) = 0. \end{aligned}$$

Pero, por la parte (b) de la proposición de 2.3 en orden $\leq r-1$, sabemos que

$$\omega_1(P) \geq \cdots \geq \omega_{r-1}(P).$$

Por consiguiente, se tiene que

$$\begin{aligned} v_r(P) = 0 &\iff v_1(P) = 0 \text{ y } \omega_1(P) = 0 \\ &\iff \psi_0(Y) \nmid \overline{P}(Y) \text{ en } \mathbb{F}_{q_0}[Y] \\ &\iff P(X) \notin \mathfrak{m}. \end{aligned}$$

Finalmente, vamos a demostrar la parte (e). Escribimos $P(X) = Q(X) + R(X)$, con $R(X) \in \mathcal{O}[X]$. Supongamos primero que $v_r(R) > v_r(Q)$. Entonces, por la parte (b), todos los puntos del diagrama $\mathbf{D}_{r-1}(R)$ están por encima de la recta $\mathbf{L}_{r-1}(Q)$. Por tanto, tenemos que $\mathbf{S}_{r-1}(P) = \mathbf{S}_{r-1}(Q) =: S$ y, por las observaciones (6) y (4) de 4.4 en orden $r-1$, que $\mathbf{F}_{r-1}(P) = P_S(Y) = Q_S(Y) + R_S(Y) = Q_S(Y) = \mathbf{F}_{r-1}(Q)$ en $\mathbb{F}_{q_{r-1}}[Y]$. Recíprocamente, supongamos ahora que $\mathbf{S}_{r-1}(P) = \mathbf{S}_{r-1}(Q) =: S$ y que $\mathbf{F}_{r-1}(P) = \mathbf{F}_{r-1}(Q)$. Entonces tenemos $v_r(P) = v_r(Q) =: u$, $v_r(R) \geq u$, $P_S(Y) = Q_S(Y) + R_S(Y)$ y $R_S(Y) = 0$. Hemos de ver que $v_r(R) > u$. Si fuera $v_r(R) = u$, entonces tendríamos que $\mathbf{S}_{r-1}(R) \subseteq S$; luego, por la observación (3) de 4.4 en orden $r-1$, para cierto $s \in \mathbb{N}$ tendría que ser $R_S(Y) = Y^s \mathbf{F}_{r-1}(R) \neq 0$. □

2.3. Proposición.

(a) *El homomorfismo* $\omega_r : K(X)^* \to \mathbb{Z}$ *es una pseudo-valoración de* $K(X)$ *respecto de la valoración* v_r *(cf. §1 del capítulo 1) que satisface* $\omega_r(K^*) = \{0\}$.

(b) *Para todo polinomio no nulo* $P(X) \in \mathcal{O}[X]$ *tenemos la desigualdad*

$$\omega_{r-1}(P) \geq v_{\phi_{r-1}}(P) + e_{r-1}f_{r-1}\omega_r(P).$$

(c) *Si* $P(X) \in \mathcal{O}[X]$ *es un polinomio no nulo, entonces*

$$\omega_r(P) = 0 \iff P_S(\zeta_{r-1}) \neq 0\,,$$

donde $P_S(Y) \in \mathbb{F}_{q_{r-1}}[Y]$ *es el polinomonio asociado (en orden* $r-1$*) al polinomio* $P(X)$ *y al segmento* $S := \mathbf{S}_{r-1}(P)$. *Además, tenemos*

$$\omega_r(P) = 0 \text{ si } \operatorname{gr}(P) < m_r.$$

DEMOSTRACIÓN. Si $A \in \mathcal{O}$, $A \neq 0$, entonces, como el segmento $\mathbf{S}_{r-1}(A) = \{(0, v_{r-1}(A))\}$, el polinomio $\mathbf{F}_{r-1}(A) = c \in \mathbb{F}^*_{q_{r-1}}$; por tanto, $\omega_r(A) = 0$. Esto prueba que $\omega_r(K^*) = \{0\}$.

Sean ahora $P(X), Q(X) \in \mathcal{O}[X]$ polinomios no nulos y supongamos que $v_r(P) = v_r(Q) =: u$ y que $\omega_r(P) < \omega_r(Q)$. Para acabar de demostrar la parte (a) de la proposición hemos de ver que $v_r(P+Q) = u$ y que $\omega_r(P+Q) = \omega_r(P)$. Consideremos el mínimo segmento S que contiene a $\mathbf{S}_{r-1}(P)$ y a $\mathbf{S}_{r-1}(Q)$; entonces tenemos que $\mathbf{H}_{r-1}(S) = u$ y que la abscisa α (resp. $\alpha + d\,e_{r-1}$) de su origen (resp. final) es igual al mínimo (resp. máximo) de las abscisas de los origenes (resp. finales) de $\mathbf{S}_{r-1}(P)$ y $\mathbf{S}_{r-1}(Q)$. Los puntos del diagrama $\mathbf{D}_{r-1}(P+Q)$ (cf. §4) con abscisa menor que α o mayor que $\alpha + d\,e_{r-1}$ están por encima de la recta con pendiente $-h_{r-1}/e_{r-1}$ que contiene a S. Si fuera $v_r(P+Q) > u$, tendríamos $\mathbf{S}_{r-1}(P) = \mathbf{S}_{r-1}(-Q)$ y $\mathbf{F}_{r-1}(P) = \mathbf{F}_{r-1}(-Q)$, por la parte (e) de la proposición anterior; de donde, obtendríamos que $\omega_r(P) = \omega_r(-Q) = \omega_r(Q)$. Por consiguiente, $v_r(P+Q) = u$ y $\mathbf{S}_{r-1}(P+Q) \subsetneq S$. Además, como claramente (por las observaciones (3) y (6) de 4.4 en orden $r-1$) tenemos que

$$\begin{aligned} Y^s\mathbf{F}_{r-1}(P+Q) &= (P+Q)_S(Y) \\ &= P_S(Y) + Q_S(Y) \\ &= Y^{s'}\mathbf{F}_{r-1}(P) + Y^{s''}\mathbf{F}_{r-1}(Q), \end{aligned}$$

para ciertos $s, s', s'' \in \mathbb{N}$, entonces $\omega_r(P+Q) = \omega_r(P)$.

La parte (b) es consecuencia de la partes (a) y (c) del lema de 4.2 en orden $r-1$, y del hecho que la longitud de la proyección sobre el eje de abscisas del segmento $\mathbf{S}_{r-1}(P)$ siempre es $\geq e_{r-1}f_{r-1}\omega_r(P)$.

Por último, la parte (c) se obtiene teniendo en cuenta que el polinomio $\psi_{r-1}(Y) = \mathrm{Irr}(\zeta_{r-1}, \mathbb{F}_{q_{r-1}}, Y)$, y que, si el grado $\mathrm{gr}(P) < m_r = m_{r-1}e_{r-1}f_{r-1}$, la longitud de la proyección sobre el eje de abscisas del segmento S es $< e_{r-1}f_{r-1}$ y el grado $\mathrm{gr}(P_S) < f_{r-1} = \mathrm{gr}(\psi_{r-1})$. □

A continuación, vamos a calcular la valoración v_r de los polinomios $\phi_i(X)$ y de las fracciones racionales $\Phi_i(X)$, $\gamma_i(X)$, $\Pi_{i+1}(X)$ y $\pi_{i+1}(X)$, para $1 \leq i \leq r-1$ (cf. §1). Antes veremos el siguiente

2.4. Lema. *Sean i, j enteros tales que $1 \leq i < j \leq r-1$.*

(a) *Si $m_i = m_{i+1}$, entonces $v_{i+1}(\phi_{i+1} - \phi_i) = v_{i+1}(\phi_{i+1}) = v_i(\phi_i) + h_i$.*

(b) *Si $m_i = m_j$, entonces $v_j(P) = v_i(P)$ para todo polinomio $P(X) \in \mathcal{O}[X]$ de grado menor que m_i.*

(c) *Si $m_i = m_j$, entonces $v_j(\phi_j - \phi_i) = v_{i+1}(\phi_{i+1})$.*

DEMOSTRACIÓN. Comenzamos probando la parte (a). Si $m_i = m_{i+1}$, el polinomio $\phi_{i+1}(X) - \phi_i(X)$ tiene grado menor que m_i y el desarrollo ϕ_i-ádico del polinomio $\phi_{i+1}(X)$ es

$$\phi_{i+1}(X) = (\phi_{i+1}(X) - \phi_i(X)) + \phi_i(X).$$

El polígono de Newton $\mathbf{N}_i(\phi_{i+1})$ consta, pues, de un solo lado con extremos $(0, v_i(\phi_{i+1}-\phi_i))$ y $(1, v_i(\phi_i))$. Por la propiedad (a) que satisface el polinomio $\phi_{i+1}(X)$ (cf. §1), este lado coincide con $\mathbf{S}_i(\phi_{i+1})$; por tanto, $v_{i+1}(\phi_{i+1}) = e_i v_i(\phi_{i+1} - \phi_i) = v_{i+1}(\phi_{i+1} - \phi_i)$. Por otra parte, como la pendiente de este lado tiene que ser $-h_i/e_i$, tenemos también que $v_i(\phi_{i+1}-\phi_i) - v_i(\phi_i) = h_i/e_i$ y, como $e_i = 1$, que $v_{i+1}(\phi_{i+1}) = v_i(\phi_{i+1} - \phi_i) = v_i(\phi_i) + h_i$.

Para demostrar la parte (b), es claro que podemos reducirnos al caso en que $j = i+1$. Por hipótesis, se tiene que $m_i = m_{i+1}$; en particular, $e_i = 1$. Pero, por la parte (b) de la proposición de 2.2 en orden $i+1$, tenemos que $v_{i+1}(P) = e_i v_i(P) = v_i(P)$.

Probemos ahora la parte (c). En primer lugar, observemos que podemos escribir

$$\phi_j(X) - \phi_i(X) = \sum_{k=i}^{j-1} (\phi_{k+1}(X) - \phi_k(X)).$$

Por hipótesis, sabemos que $m_k = m_{k+1} = m_j$, para cualquir entero k con $i \leq k \leq j-1$. Por las partes (b) y (a) anteriores, entonces obtenemos que $v_j(\phi_{k+1} - \phi_k) = v_{k+1}(\phi_{k+1} - \phi_k) = v_{k+1}(\phi_{k+1})$. Pero, para $k > i$ sabemos que $v_{k+1}(\phi_{k+1}) > v_{i+1}(\phi_{i+1})$, también por el apartado (a). Por consiguiente, $v_j(\phi_j - \phi_i) = v_j(\phi_{i+1} - \phi_i) = v_{i+1}(\phi_{i+1})$. □

2.5. Proposición. *Sea i un entero tal que $1 \leq i \leq r-1$. Entonces*

(a) $v_r(\phi_i) = \sum_{j=1}^{i} e_{j+1} \cdots e_{r-1} \cdot e_j f_j \cdots e_{i-1} f_{i-1} \cdot h_j$, *y* $\omega_r(\phi_i) = 0$.

(b) $v_r(\Phi_i) = e_{i+1} \cdots e_{r-1} h_i$, $v_r(\gamma_i) = 0$, $v_r(\pi_{i+1}) = e_{i+1} \cdots e_{r-1}$ *y*

$v_r(\Pi_{i+1}) = \sum_{j=1}^{i} e_{j+1} \cdots e_{r-1} \cdot e_j f_j \cdots e_i f_i \cdot h_j$. *En particular, tenemos que* $v_r(\Phi_{r-1}) = h_{r-1}$, $v_r(\gamma_{r-1}) = 0$ *y* $v_r(\pi_r) = 1$.

DEMOSTRACIÓN. Primeramente observemos que, por la parte (c) del corolario de 3.3 en orden i, para demostrar la primera igualdad de la parte (a) nos bastará con ver que $v_r(\phi_i) = e_{i+1} \cdots e_{r-1}(e_i v_i(\phi_i) + h_i)$.

Comenzemos por probar la parte (a) en el caso $i = r-1$. Ya sabemos, por la parte (b) de la proposición de 2.2, que $v_r(\phi_{r-1}) = e_{r-1} v_{r-1}(\phi_{r-1}) + h_{r-1}$. Además, como el diagrama $\mathbf{D}_{r-1}(\phi_{r-1})$ solamente contiene el punto $(1, v_{r-1}(\phi_{r-1}))$, el segmento $\mathbf{S}_{r-1}(\phi_{r-1})$ se reduce a este punto; por tanto, $\omega_r(\phi_{r-1}) = 0$.

Ahora, probemos la parte (a) por inducción sobre r. Para $r = 2$ ya está probada. Supongamos que el resultado es cierto para $r-1$, con $r \geq 3$. Consideremos un i tal que $1 \leq i \leq r-2$. Si $m_i < m_{r-1}$, el diagrama $\mathbf{D}_{r-1}(\phi_i)$ solo contiene el punto $(0, v_{r-1}(\phi_i))$; por tanto, $v_r(\phi_i) = e_{r-1} v_{r-1}(\phi_i)$ y $\omega_r(\phi_i) = 0$. La fórmula para $v_r(\phi_i)$ se deduce de la hipótesis de inducción. Si $m_i = m_{r-1}$ (es decir, $e_i = f_i = \cdots = e_{r-2} = f_{r-2} = 1$), entonces, por la parte (c) del lema anterior, $v_{r-1}(\phi_{r-1} - \phi_i) = v_{i+1}(\phi_{i+1})$; por tanto, el diagrama $\mathbf{D}_{r-1}(\phi_i)$ consta de los puntos $(0, v_{i+1}(\phi_{i+1}))$ y

$(1, v_{r-1}(\phi_{r-1}))$ y el segmento $\mathbf{S}_{r-1}(\phi_i)$ se reduce al primero de estos puntos (pues, por la parte (a) del lema anterior, $v_{i+1}(\phi_{i+1}) \leq v_{r-1}(\phi_{r-1})$). Así pues, tenemos $v_r(\phi_i) = e_{r-1}v_{i+1}(\phi_{i+1}) = e_{r-1}(v_i(\phi_i) + h_i)$ y $\omega_r(\phi_i) = 0$.

La primera y la tercera igualdad de la parte (b) las demostraremos a la vez por inducción sobre i. De la parte (a) y del hecho que $v_r(\pi_1) = v_r(\pi) = e_1 \cdots e_{r-1}$, deducimos que $v_r(\Phi_1) = v_r(\phi_1) = e_2 \cdots e_{r-1}h_1$ y que $v_r(\pi_2) = l_1 v_r(\Phi_1) - l_1' v_r(\pi_1) = l_1 h_1 e_2 \cdots e_{r-1} - l_1' e_1 e_2 \cdots e_{r-1} = e_2 \cdots e_{r-1}$. Supongamos ahora que estas dos igualdades son ciertas hasta $i-1$, con $i \geq 2$. Entonces, teniendo en cuenta la parte (a), se tiene que

$$\begin{aligned} v_r(\Phi_i) &= v_r(\phi_i) - \sum_{j=1}^{i-1} v_r(\pi_j) \cdot e_j f_j \cdots e_{i-1} f_{i-1} \cdot \frac{h_j}{e_j} \\ &= v_r(\phi_i) - \sum_{j=1}^{i-1} e_{j+1} \cdots e_{r-1} \cdot e_j f_j \cdots e_{i-1} f_{i-1} \cdot h_j \\ &= e_{i+1} \cdots e_{r-1} h_i \,, \end{aligned}$$

y, por tanto, que

$$\begin{aligned} v_r(\pi_{i+1}) &= l_i v_r(\Phi_i) - l_i' v_r(\pi_i) \\ &= l_i h_i e_{i+1} \cdots e_{r-1} - l_i' e_i e_{i+1} \cdots e_{r-1} \\ &= e_{i+1} \cdots e_{r-1} \,. \end{aligned}$$

Finalmente, de las dos igualdades ya probadas obtenemos entonces que $v_r(\gamma_i) = e_i v_r(\Phi_i) - h_i v_r(\pi_i) = 0$, y que

$$v_r(\Pi_{i+1}) = \sum_{j=1}^{i} v_r(\pi_j) \cdot e_j f_j \cdots e_i f_i \cdot \frac{h_j}{e_j} = \sum_{j=1}^{i} e_{j+1} \cdots e_{r-1} \cdot e_j f_j \cdots e_i f_i \cdot h_j \,;$$

con lo cual terminamos de probar la parte (b). □

Denotamos por $\mathcal{O}_{v_r}$, $\mathfrak{m}_{v_r}$ y k_{v_r} al anillo, al ideal maximal y al cuerpo residual, respectivamente, de la valoración v_r. La aplicación de reducción $\mathcal{O}_{v_r} \to k_{v_r}$ la denotaremos por $R(X) \mapsto \overline{R(X)}^r$.

2.6. Corolario. *El grupo de valores de la valoración v_r es $\mathbb{Z}$, y su ideal maximal es $\mathfrak{m}_{v_r} = \pi_r(X)\mathcal{O}_{v_r}$.* □

A continuación, vamos a calcular el cuerpo residual k_{v_r} de v_r. Primeramente observemos que $\mathfrak{m}_{v_r} \cap \mathcal{O} = \mathfrak{p}$, lo cual nos permite pensar el cuerpo finito $\mathbb{F}_{q_0} = \mathcal{O}/\mathfrak{p}$ como un subcuerpo de k_{v_r}. Además, por la parte (b) de la proposición de 2.5, sabemos que $v_r(\gamma_i) = 0$ para todo i, $1 \leq i \leq r-1$. Por tanto, los elementos $\overline{\gamma_1(X)}^r, \ldots, \overline{\gamma_{r-1}(X)}^r \in k_{v_r}$ son no nulos. El siguiente teorema nos dirá que de hecho estos elementos, junto con $\overline{\gamma_0(X)}^r = \overline{X}^r$, generan k_{v_r} sobre $\mathbb{F}_{q_0}$; es decir, que $k_{v_r} = \mathbb{F}_{q_0}\left(\overline{\gamma_0(X)}^r, \ldots, \overline{\gamma_{r-1}(X)}^r\right)$.

2.7. Teorema.

(a) *La aplicación*

$$\tau_r : \mathbb{F}_{q_{r-1}} = \mathbb{F}_{q_0}(\zeta_0, \ldots, \zeta_{r-2}) \to k_{v_r}$$

definida por $\tau_r(\varphi(\zeta_0, \ldots, \zeta_{r-2})) := \varphi\left(\overline{\gamma_0(X)}^r, \ldots, \overline{\gamma_{r-2}(X)}^r\right)$, *para cualquier* $\varphi(X_0, \ldots, X_{r-2}) \in \mathbb{F}_{q_0}[X_0, \ldots, X_{r-2}]$, *está bien definida y determina una* $\mathbb{F}_{q_0}$*-inmersión. En adelante, pensaremos* $\mathbb{F}_{q_{r-1}}$ *como un subcuerpo de* k_{v_r}.

(b) $k_{v_r} = \mathbb{F}_{q_{r-1}}\left(\overline{\gamma_{r-1}(X)}^r\right)$ *y el elemento* $\overline{\gamma_{r-1}(X)}^r$ *es transcendente sobre* $\mathbb{F}_{q_{r-1}}$.

Demostraremos este teorema junto con el siguiente

2.8. Teorema. *Sea* s *un entero tal que* $1 \leq s \leq r-1$. *Sean* $P(X) \in \mathcal{O}[X]$ *un polinomio no nulo y* S *un segmento con pendiente* $-h_s/e_s$ *para el que podemos definir el polinomio asociado (en orden* s*)* $P_S(Y) \in \mathbb{F}_{q_s}[Y]$ *(cf. definición de* 4.3*). Sea* $P^S(X) \in K(X)$ *la fracción racional asociada (en orden* s*) a* $P(X)$ *y a* S *(cf. definición de* 4.5*). Entonces* $v_r(P^S) \geq 0$ *y*

$$\overline{P^S(X)}^r = P_S\left(\overline{\gamma_s(X)}^r\right) \text{ en } k_{v_r}.$$

Para demostrar estos dos teoremas necesitaremos ver antes dos lemas sobre fracciones racionales. El primero de ellos hace referencia a las fracciones racionales de la forma $\Phi(\mathbf{n})(X)$, $\mathbf{n} \in \mathbb{Z}^r$ (cf. §1).

2.9. Lema. *Sea* $\mathbf{n} = (n_0, n_1, \ldots, n_{r-1}) \in \mathbb{Z}^r$ *tal que* $v_r(\Phi(\mathbf{n})) = 0$. *Entonces podemos escribir, y en forma única,*

$$\Phi(\mathbf{n})(X) = \gamma_1(X)^{t_1} \cdots \gamma_{r-1}(X)^{t_{r-1}},$$

con $t_1, \ldots, t_{r-1} \in \mathbb{Z}$. *Además, cada entero* t_i *depende sólo de* $n_i, \ldots, n_{r-1}$.

DEMOSTRACIÓN. Veamos primeramente la existencia por inducción sobre $r \geq 1$. Para $r = 1$, la hipótesis nos dice $n_0 = 0$; así, $\Phi(\mathbf{n})(X) = 1$. Supongamos que $r \geq 2$. Por la parte (a) de la proposición de 2.5, tenemos

$$v_r(\Phi(\mathbf{n})) = n_0 e_1 \cdots e_{r-1} + \sum_{i=1}^{r-1} n_i \left(\sum_{j=1}^{i} e_{j+1} \cdots e_{r-1} \cdot e_j f_j \cdots e_{i-1} f_{i-1} \cdot h_j \right)$$
$$\equiv n_{r-1} h_{r-1} \pmod{e_{r-1}};$$

luego, por la hipótesis, tenemos $n_{r-1} = e_{r-1} t_{r-1}$ para algún $t_{r-1} \in \mathbb{Z}$. Consideremos la fracción racional $R(X) := \Phi(\mathbf{n})(X) \cdot \gamma_{r-1}(X)^{-t_{r-1}} \in K(X)$. Como $\gamma_{r-1}(X) = \cdots \phi_{r-1}(X)^{e_{r-1}}$, entonces $R(X) = \Phi(\mathbf{n}')(X)$ para algún $\mathbf{n}' = (n'_0, \ldots, n'_{r-2}, 0) \in \mathbb{Z}^r$, donde cada entero n'_i depende sólo de n_i y de n_{r-1}; además, como $v_r(\gamma_{r-1}) = 0$ (por la parte (b) de la proposición de 2.5), seguimos teniendo $v_r(R) = 0$. Aplicando la hipótesis de inducción a $R(X)$, obtenemos la existencia y que cada entero t_i depende sólo de $n_i, \ldots, n_{r-1}$.

Para ver la unicidad, bastará con ver que si tenemos $t_1, \ldots, t_{r-1} \in \mathbb{Z}$ tales que

$$\gamma_1(X)^{t_1} \cdots \gamma_{r-1}(X)^{t_{r-1}} = 1\,, \qquad (*)$$

entonces $t_1 = \cdots = t_{r-1} = 0$. Como cada $\gamma_i(X) = \cdots \phi_i(X)^{e_i}$ y como los polinomios $\phi_i(X)$ són irreducibles y distintos (cf. parte (a) del corolario de 3.4 en orden i), entonces de la igualdad de $(*)$ se deduce que $t_{r-1} = 0$ y, por inducción, que $t_{r-2} = \cdots = t_1 = 0$. □

2.10. Lema. *Sean* $n'_1, \ldots, n'_r \geq 1$ *enteros, y sea* $m \geq 0$ *un entero. Entonces existen* r *enteros* $n_1, \ldots, n_r$ *tales que para todo entero* j, *con* $0 \leq j \leq m$, *la fracción racional* $\prod_{s=1}^{r} \pi_s(X)^{n_s - j\, n'_s} \in \mathcal{O}[X]$.

DEMOSTRACIÓN. Para cada entero s, $1 \leq s \leq r$, sabemos que la fracción racional $\pi_s(X) = \pi^{n_{s,0}} \phi_1(X)^{l_1 n_{s,1}} \cdots \phi_{s-1}(X)^{l_{s-1} n_{s,s-1}}$, para ciertos enteros $n_{s,0}, \ldots, n_{s,s-1}$, y que $n_{s,s-1} = 1$. Sean $n_1, \ldots, n_r \in \mathbb{Z}$, entonces para todo j, $0 \leq j \leq m$, el producto

$$\prod_{s=1}^{r} \pi_s(X)^{n_s - j\, n'_s} = \pi^{\nu_{j,0}} \phi_1(X)^{\nu_{j,1}} \cdots \phi_{r-1}(X)^{\nu_{j,r-1}},$$

donde $\nu_{j,t} := l_t \sum_{s=t+1}^{r} n_{s,t}(n_s - j\,n'_s) \in \mathbb{Z}$, para $0 \le t \le r-1$, y convenimos que $l_0 := 1$. Afirmamos que existen r enteros $n_1, \ldots, n_r$ tales que para cada j y para cada t es $\nu_{j,t} \ge 0$. En efecto, es claro que podemos elegir un entero n_r tal que $\nu_{j,r-1} \ge 0$ para cada j, después un entero n_{r-1} tal que $\nu_{j,r-2} \ge 0$ para cada j, y así sucesivamente. □

DEMOSTRACIÓN (de los teoremas de 2.7 y de 2.8). Consideremos un entero s tal que $1 \le s \le r-1$. Veamos por inducción sobre s que se satisfacen las siguientes propiedades

(i_s) $\overline{\Phi_s(X)}^r = c_{s-1} \cdot \psi_{s-1}\left(\overline{\gamma_{s-1}(X)}^r\right)$ en k_{v_r}, para algún $c_{s-1} \in k_{v_r}^*$.

(ii_s) La aplicación

$$\tau_{r,s} : \mathbb{F}_{q_s} = \mathbb{F}_{q_0}(\zeta_0, \ldots, \zeta_{s-1}) \to k_{v_r}$$

definida por $\tau_{r,s}(\varphi(\zeta_0, \ldots, \zeta_{s-1})) := \varphi\left(\overline{\gamma_0(X)}^r, \ldots, \overline{\gamma_{s-1}(X)}^r\right)$, para cualquier $\varphi(X_0, \ldots, X_{s-1}) \in \mathbb{F}_{q_0}[X_0, \ldots, X_{s-1}]$, está bien definida y determina una $\mathbb{F}_{q_0}$-inmersión. En adelante, pensaremos $\mathbb{F}_{q_s}$ como un subcuerpo de k_{v_r}.

(iii_s) $v_r(P^S) \ge 0$ y $\overline{P^S(X)}^r = P_S\left(\overline{\gamma_s(X)}^r\right)$ en k_{v_r}, para todo polinomio $P(X)$ y para cualquier segmento S como en el enunciado del teorema de 2.8.

Una vez hayan sido demostradas estas tres propiedades, quedarán entonces probados la parte (a) del teorema de 2.7 y el teorema de 2.8.

Por la parte (b) de la proposición de 2.5, sabemos que $v_r(\Phi_s) > 0$; por tanto, la propiedad (ii_s) se obtiene de (i_s) y (ii_{s-1}) (si $s \ge 2$).

Para $P(X)$ y S como antes, usaremos las notaciones, en orden s, $A_i(X)$, u_i, (α, β) y, para cada i con $(i, u_i) \in S$, $S(i)$, $t_s(i,1), \ldots, t_s(i, s-1)$, $P^o(X)$, $\Gamma_i(X)$ y $B_i(X)$, que utilizamos en la §4. Supongamos que $s = 1$. Es claro que $\overline{\Phi_1(X)}^r = \overline{\phi_1}\left(\overline{X}^r\right) = \psi_0\left(\overline{X}^r\right)$, lo que prueba ($\mathrm{i}_1$). Por la observación 2 de 1.7 del capítulo 1, tenemos que

$$P^S(X) = \sum_{i:(i,u_i)\in S} B_i(X)\,\gamma_1(X)^{(i-\alpha)/e_1}.$$

Pero, como cada $B_i(X) = A_i(X)/\pi^{\beta-(i-\alpha)h_1/e_1} \in \mathcal{O}[X]$ y como cada

$\overline{B_i(X)}^r = \overline{B_i}(\zeta_0)$ (via identificar $\mathbb{F}_{q_1}$ a un subcuerpo de k_{v_r}, por (ii_1)), entonces también es clara la propiedad (iii_1).

Supongamos que las propiedades (i_t) y (iii_t) son ciertas para todo t, $1 \leq t \leq s-1$. Comenzemos viendo la propiedad (i_s). Por el corolario de 3.3 (en orden s), el punto $(0, f_{s-1}v_s(\phi_{s-1}))$ es el origen del único lado, T, del polígono $\mathbf{N}_{s-1}(\phi_s)$. Entonces, por las definiciones del polinomio $(\phi_s)^o(X)$ y de la fracción racional $(\phi_s)^T(X)$, tenemos que $(\phi_s)^o(X)$ es mónico de grado igual a m_s y que

$$\phi_s(X) = (\phi_s)^o(X) + R_s(X) = \pi_{s-1}(X)^{f_{s-1}v_s(\phi_{s-1})}(\phi_s)^T(X) + R_s(X),$$

donde $R_s(X) \in \mathcal{O}[X]$ es de grado menor que m_s y $v_s(R_s) > v_s(\phi_s)$; así, por la parte (b) de la proposición de 2.2 y la proposición de 2.5, obtenemos que $v_r(R_s) = e_s \cdots e_{r-1}v_s(R_s) > e_s \cdots e_{r-1}v_s(\phi_s) = v_r(\Pi_s)$. Además, por la propiedad (iii_{s-1}), es

$$\overline{(\phi_s)^T(X)}^r = (\phi_s)_T\left(\overline{\gamma_{s-1}(X)}^r\right) = c_{s-1}\psi_{s-1}\left(\overline{\gamma_{s-1}(X)}^r\right),$$

para algún elemento $c_{s-1} \in \mathbb{F}^*_{q_{s-1}}$. Por consiguiente, se tiene que

$$\Phi_s(X) = \frac{\phi_s(X)}{\Pi_s(X)} = \rho_{s-1}(X)^{-e_{s-1}f_{s-1}}(\phi_s)^T(X) + \frac{R_s(X)}{\Pi_s(X)},$$

con $\rho_{s-1}(X) := \dfrac{\Pi_{s-1}(X)}{\pi_{s-1}(X)^{v_{s-1}(\phi_{s-1})}} \in K(X)$, y entonces, tomando clase módulo $\mathfrak{m}_{v_r}$, que

$$\overline{\Phi_s(X)}^r = \left(\overline{\rho_{s-1}(X)}^r\right)^{-e_{s-1}f_{s-1}} c_{s-1}\psi_{s-1}\left(\overline{\gamma_{s-1}(X)}^r\right).$$

Como $v_r(\rho_{s-1}) = 0$, entonces la propiedad (i_s) queda demostrada.

Veamos ahora la propiedad (iii_s). Por la proposición de 4.6 en orden s, se tiene que

$$P^S(X) = \sum_{i:(i,u_i)\in S} \Gamma_i(X)\, B_i(X)\, \gamma_s(X)^{(i-\alpha)/e_s}, \qquad (*)$$

con cada $\Gamma_i(X) = \gamma_1(X)^{t_s(i,1)} \cdots \gamma_{s-1}(X)^{t_s(i,s-1)}$; por consiguiente, es cada $\overline{\Gamma_i(X)}^r = \zeta_1^{t_s(i,1)} \cdots \zeta_{s-1}^{t_s(i,s-1)}$ (via la identificación propiciada por (ii_s)). Además, por la definición de las fracciones racionales $B_i(X)$ y $(A_i)^{S(i)}(X)$

y por la propiedad (iii$_{s-1}$), tenemos que el valor $v_r(B_i) = 0$ y las igualdades $\overline{B_i(X)}^r = \overline{(A_i)^{S(i)}(X)}^r = (A_i)_{S(i)}(\zeta_{s-1})$. Como también $v_r(\gamma_s) = 0$, tenemos en particular $v_r(P^S) \geq 0$. Tomando ahora clases módulo $\mathfrak{m}_{v_r}$ en la igualdad de $(*)$ se obtiene la propiedad (iii$_s$).

Sean $P(X), Q(X) \in \mathcal{O}[X]$ dos polinomios no nulos tales que $v_r(P) = v_r(Q) =: u$, veamos que $\overline{P(X)/Q(X)}^r \in \mathbb{F}_{q_{r-1}}\left(\overline{\gamma_{r-1}(X)}^r\right)$; lo cual demostrará que $k_{v_r} = \mathbb{F}_{q_{r-1}}\left(\overline{\gamma_{r-1}(X)}^r\right)$. Para $P(X)$ y $S := \mathbf{S}_{r-1}(P)$ seguiremos usando las notaciones anteriores en orden $s := r-1$. Por la definición de la fracción racional $P^S(X)$, tenemos que

$$P(X) = \Phi_{r-1}(X)^{\alpha}\pi_{r-1}(X)^{\beta}P^S(X) + R(X)$$

con $R(X) \in \mathcal{O}[X]$ y $v_r(R) > u$. Como $v_r(\Phi_{r-1}^{\alpha}\pi_{r-1}^{\beta}) = h_{r-1}\alpha + e_{r-1}\beta = u$, entonces $v_r(P^S) = 0$; además, por el teorema de 2.8 ya probado, obtenemos que $\overline{P^S(X)}^r \in \mathbb{F}_{q_{r-1}}\left[\overline{\gamma_{r-1}(X)}^r\right]$. Ponemos ahora $S' := \mathbf{S}_{r-1}(Q)$, y denotamos por (α', β') el origen de este lado. Repitiendo lo anterior para $Q(X)$ y S', se llega a que $0 \neq \overline{Q^{S'}(X)}^r \in \mathbb{F}_{q_{r-1}}\left[\overline{\gamma_{r-1}(X)}^r\right]$ y que

$$\overline{P(X)/Q(X)}^r = \overline{\Phi(X)}^r\,\overline{P^S(X)}^r / \overline{Q^{S'}(X)}^r,$$

donde $\Phi(X) := \Phi_{r-1}(X)^{\alpha-\alpha'}\pi_{r-1}(X)^{\beta-\beta'} \in K(X)$. Pero, como la fracción $\Phi(X) = \Phi(\mathbf{n})(X)$ para algún $\mathbf{n} \in \mathbb{Z}^r$ y $v_r(\Phi) = 0$, entonces, por el lema de 2.9, obtenemos que $\overline{\Phi(X)}^r \in \mathbb{F}_{q_{r-1}}\left(\overline{\gamma_{r-1}(X)}^r\right)$. Por consiguiente, ya hemos visto que $\overline{P(X)/Q(X)}^r \in \mathbb{F}_{q_{r-1}}\left(\overline{\gamma_{r-1}(X)}^r\right)$.

Finalmente, veamos la transcendencia del elemento $\overline{\gamma_{r-1}(X)}^r$. Será suficiente ver que este elemento es transcendente sobre el cuerpo $\mathbb{F}_{q_0}$. Sea $Q(X) = \sum_{j=0}^{m} b_j X^j \in \mathcal{O}[X]$ un polinomio tal que $v(b_m) = 0$, hemos de probar que $\overline{Q}\left(\overline{\gamma_{r-1}(X)}^r\right) \neq 0$. Ponemos $n'_s := e_s f_s \cdots e_{r-1} f_{r-1} h_s/(e_s f_{r-1}) \in \mathbb{Z}$, para $1 \leq s \leq r-1$. Entonces, por el lema de 2.10, existen $r-1$ enteros $n_1, \ldots, n_{r-1}$ tales que para todo j, $0 \leq j \leq m$, se tiene que el producto $\prod_{s=1}^{r-1} \pi_s(X)^{n_s - j\,n'_s} \in \mathcal{O}[X]$. Consideremos ahora el polinomio

$$Q_1(X) := \left(\prod_{s=1}^{r-1} \pi_s(X)^{n_s}\right) Q(\gamma_{r-1}(X)) = \sum_{j=0}^{m} B_{j\,e_{r-1}}(X)\phi_{r-1}(X)^{j\,e_{r-1}}, \quad (**)$$

donde $B_{j\,e_{r-1}}(X) := b_j \cdot \prod_{s=1}^{r-1} \pi_s(X)^{n_s - j\,n'_s} \in \mathcal{O}[X]$ (no necesariamente de grado menor que m_{r-1}); entonces lo que se ha de demostrar es que el valor $v_r(Q_1) = \sum_{s=1}^{r-1} n_s v_r(\pi_s)$. Ponemos ahora $u'_j := v_{r-1}(B_{j\,e_{r-1}} {\phi_{r-1}}^{j\,e_{r-1}})$, para $0 \le j \le m$. Utilizando las proposiciones de 2.5 y de 3.3 (en orden $r-1$), obtenemos que cada $u'_j = v_{r-1}(b_j) + u'_m + (m-j)h_{r-1}$. De aquí se sigue que los puntos del diagrama $\mathbf{D}_{r-1}(Q_1, \{B_i\})$ (cf. definición de 4.7) están por encima de o tocando a la recta con pendiente $-h_{r-1}/e_{r-1}$ que pasa por el punto $(0, \beta)$, con $\beta := u'_m + m\,h_{r-1} = u'_0 - v_{r-1}(b_0) = \sum_{s=1}^{r-1} n_s v_{r-1}(\pi_s)$, y que al menos uno (el correspondiente a $j = m$) toca a esta recta. Pero, como $\omega_r(b_j) = \omega_r(\pi_s) = 0$ para todo j, s (cf. proposiciones de 2.3 y de 2.5), entonces es $\omega_r(B_{j\,e_r}) = 0$ para todo j y, por tanto, el ϕ_{r-1}-desarrollo $(**)$ de $Q_1(X)$ es admisible (cf. definición de 5.2). Por consiguiente, aplicando el corolario de 5.3 en orden $r-1$, obtenemos que el segmento $\mathbf{S}_{r-1}(Q_1)$ también está sobre dicha recta; luego, el valor $v_r(Q_1) = e_{r-1}\beta = \sum_{s=1}^{r-1} n_s v_r(\pi_s)$. □

§3. Construcción de $\phi_r(X)$

En esta sección, vamos a construir con el polígono un polinomio mónico de $\mathcal{O}[X]$ con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ y de grado mínimo. Por la proposición de 1.2, sabemos que este grado debe ser igual a un múltiplo positivo del entero m_r.

3.1. Teorema. *Podemos construir un polinomio mónico $\phi_r(X) \in \mathcal{O}[X]$ de grado m_r que satisfaga las propiedades siguientes*

(a) *El polígono $\mathbf{N}_{r-1}(\phi_r)$ consta de un solo lado, con pendiente $-\dfrac{h_{r-1}}{e_{r-1}}$.*

(b) *El polinomio asociado (en orden $r-1$) al polinomio $\phi_r(X)$ y a este lado es $c\,\psi_{r-1}(Y)$, para algún elemento $c \in \mathbb{F}^*_{q_{r-1}}$.*

Para la demostración de este teorema necesitaremos la siguiente

3.2. Proposición. *Sea $V \geq e_{r-1}f_{r-1}v_r(\phi_{r-1})$ un entero, y sea $\varphi(Y) \in \mathbb{F}_{q_{r-1}}[Y]$ un polinomio no nulo de grado menor que f_{r-1}. Denotamos por T al segmento más largo con extremos de coordenadas enteras no negativas, con pendiente $-h_{r-1}/e_{r-1}$ y con $\mathbf{H}_{r-1}(T) = V$. Entonces podemos construir un polinomio $P(X) \in \mathcal{O}[X]$ de grado menor que m_r tal que $v_r(P) = V$ y tal que el polinomio asociado (en orden $r-1$) al polinomio $P(X)$ y al segmento T es $P_T(Y) = \varphi(Y)$ en $\mathbb{F}_{q_{r-1}}[Y]$.*

DEMOSTRACIÓN. Denotamos por (α, β) al origen de T; así, se tiene que $h_{r-1}\alpha + e_{r-1}\beta = V$ y que $\alpha < e_{r-1}$. Podemos escribir

$$\varphi(Y) = \sum_{j<f_{r-1}} c_j(\zeta_{r-2})Y^j\,,$$

con los $c_j(X) \in \mathbb{F}_{q_{r-2}}[X]$ polinomios de grado menor que f_{r-2} y con $c_{j_0}(X) \neq 0$ para algún $j_0 < f_{r-1}$.

La demostración la haremos por inducción sobre $r \geq 2$. En el caso $r = 2$, veamos que el polinomio

$$P(X) := \sum_{j<f_1} \pi^{\beta - j\,h_1} C_j(X)\,\phi_1(X)^{\alpha + j\,e_1}$$

satisface las propiedades requeridas, donde $C_j(X) \in \mathcal{O}[X]$ tiene grado menor que m_1 y satisface $\overline{C_j}(X) = c_j(X)$ en $\mathbb{F}_{q_0}[X]$. En primer lugar, como $\alpha < e_1$, para todo $j < f_1$ es $\alpha + j\,e_1 < e_1 f_1$; así, el polinomio $P(X) \in K[X]$ tiene grado menor que $m_1 e_1 f_1 = m_2$. La hipótesis $V \geq e_1 f_1 h_1$, prueba que para todo $j < f_1$ es $\beta - j\,h_1 = \dfrac{1}{e_1}(V - (\alpha + j\,e_1)h_1) \geq h_1/e_1$; por tanto, el polinomio $P(X) \in \mathcal{O}[X]$. Por construcción, es claro que $v_2(P) = V$ y que $P_T(Y) = \varphi(Y)$ en $\mathbb{F}_{q_1}[Y]$.

Supongamos ahora que la proposición es válida en orden $r-1$. Para $j < f_{r-1}$, sea $V_j := \beta - j\,h_{r-1} - (\alpha + j\,e_{r-1})v_{r-1}(\phi_{r-1})$, sea T_j el segmento más largo con extremos de coordenadas enteras no negativas, con pendiente $-h_{r-2}/e_{r-2}$ y con $\mathbf{H}_{r-2}(T_j) = V_j$, sea (α_j, β_j) el origen de este segmento, y sea $\varphi_j(Y) \in \mathbb{F}_{q_{r-2}}[Y]$ el único polinomio de grado menor que f_{r-2} tal que

$$\varphi_j(\zeta_{r-2}) = \zeta_1^{-t(j,1)} \cdots \zeta_{r-2}^{-t(j,r-2)} c_j(\zeta_{r-2}),$$

donde los enteros $t(j,s)$ están definidos por

$$t(j,s) := -(\alpha + j\,e_{r-1})e_{r-2}f_{r-2}\cdots e_{s+1}f_{s+1}l_s f_s(e_s v_s(\phi_s) + h_s),\ s < r-2,$$

$$t(j,r-2) := \frac{1}{e_{r-2}}(\alpha_j - l_{r-2}(\beta - j\,h_{r-1})).$$

En primer lugar, observemos que es $V_j \geq e_{r-2}f_{r-2}v_{r-1}(\phi_{r-2})$ para todo entero $j < f_{r-1}$. En efecto,

$$\begin{aligned}
V_j &= \frac{1}{e_{r-1}}(V - (\alpha + j\,e_{r-1})(e_{r-1}v_{r-1}(\phi_{r-1}) + h_{r-1})) \\
&= \frac{1}{e_{r-1}}(V - (\alpha + j\,e_{r-1})v_r(\phi_{r-1})) \quad \text{(por (b) de la proposición de 2.2)} \\
&\geq \frac{1}{e_{r-1}}(V - (e_{r-1}f_{r-1} - 1)v_r(\phi_{r-1})) \quad \text{(pues, } \alpha + je_{r-1} < e_{r-1}f_{r-1}) \\
&\geq \frac{1}{e_{r-1}}v_r(\phi_{r-1}) \quad \text{(por hipótesis)} \\
&= v_{r-1}(\phi_{r-1}) + \frac{h_{r-1}}{e_{r-1}} \\
&> v_{r-1}(\phi_{r-1}) \\
&= e_{r-2}f_{r-2}v_{r-1}(\phi_{r-2}) \quad \text{(por (b) del corolario de 3.3 en orden } r-1).
\end{aligned}$$

Si $c_j(X) = 0$, entonces ponemos $P_j(X) := 0$. Si $c_j(X) \neq 0$ (es decir, $\varphi_j(Y) \neq 0$), entonces, por la hipótesis de inducción, podemos construir un polinomio $P_j(X) \in \mathcal{O}[X]$ de grado menor que m_{r-1} que satisfaga $v_{r-1}(P_j) = V_j$ y $(P_j)_{T_j}(Y) = \varphi_j(Y)$ en $\mathbb{F}_{q_{r-2}}[Y]$. Ahora, es claro que el polinomio

$$P(X) := \sum_{j<f_{r-1}} P_j(X)\phi_{r-1}(X)^{\alpha+j\,e_{r-1}} \in \mathcal{O}[X],$$

es de grado menor que m_r y que los puntos del diagrama de Newton $\mathbf{D}_{r-1}(P)$ están por encima de o tocando a T; además, el punto correspondiente a un j está sobre T si y sólo si $c_j(X) \neq 0$. Por tanto, $v_r(P) = V$. Finalmente, tenemos que

$$\begin{aligned}
P_T(Y) &= \sum_{j<f_{r-1}} \zeta_1^{t_{r-1}(\alpha+j\,e_{r-1},1)} \cdots \zeta_{r-2}^{t_{r-1}(\alpha+j\,e_{r-1},r-2)} (P_j)_{T_j}(\zeta_{r-2})\, Y^j \\
&= \sum_{j<f_{r-1}} \zeta_1^{t(j,1)} \cdots \zeta_{r-2}^{t(j,r-2)} \varphi_j(\zeta_{r-2})\, Y^j \\
&= \sum_{j<f_{r-1}} c_j(\zeta_{r-2})\, Y^j \\
&= \varphi(Y),
\end{aligned}$$

pues, por definición (cf. 4.3), $t_{r-1}(\alpha+j\,e_{r-1}, s) = t(j,s)$ para todo j, s. Esto termina de probar la proposición. □

DEMOSTRACIÓN (del teorema de 3.1). Consideramos el entero $V := e_{r-1}f_{r-1}v_r(\phi_{r-1})$, y denotamos por T al segmento más largo con extremos de coordenadas enteras no negativas, con pendiente $-h_{r-1}/e_{r-1}$ y con $\mathbf{H}_{r-1}(T) = V$; así, el origen del segmento T es el punto $(0, f_{r-1}v_r(\phi_{r-1}))$. Consideramos ahora el polinomio $\varphi(Y) := c(\psi_{r-1}(Y) - Y^{f_{r-1}})$, donde

$$\begin{aligned} c &:= \prod_{s=1}^{r-2} \zeta_s^{t(s)} \in \mathbb{F}_{q_{r-1}}^*, \\ t(s) &:= -e_{r-1}f_{r-1}\cdots e_{s+1}f_{s+1}l_sf_s(e_sv_s(\phi_s) + h_s), \quad 1 \le s \le r-3, \\ t(r-2) &:= -\frac{1}{e_{r-2}}l_{r-2}e_{r-1}f_{r-1}v_{r-1}(\phi_{r-1}). \end{aligned}$$

Así, el polinomio $\varphi(Y) \in \mathbb{F}_{q_{r-1}}[Y]$ tiene término constante no nulo y es de grado menor que f_{r-1}. Por la proposición anterior, podemos construir un polinomio $P(X) \in \mathcal{O}[X]$ de grado menor que m_r tal que $v_r(P) = V$ y $P_T(Y) = \varphi(Y)$ en $\mathbb{F}_{q_{r-1}}[Y]$. Ahora, ponemos

$$\phi_r(X) := \phi_{r-1}(X)^{e_{r-1}f_{r-1}} + P(X).$$

Por construcción, se tiene que el polinomio $\phi_r(X) \in \mathcal{O}[X]$ es mónico de grado m_r. Además, el lado $S := \mathbf{S}_{r-1}(\phi_r) \subseteq T$ tiene el mismo origen que T y final el punto $(e_{r-1}f_{r-1}, e_{r-1}f_{r-1}v_{r-1}(\phi_{r-1}))$; por tanto, el polígono $\mathbf{N}_{r-1}(\phi_r)$ consta de un solo lado, S. Finalmente, observemos que el polinomio asociado (en orden $r-1$) $({\phi_{r-1}}^{e_{r-1}f_{r-1}})_T(Y) = cY^{f_{r-1}}$, pues, por definición (cf. 4.3), $t_{r-1}(e_{r-1}f_{r-1}, s) = t(s)$ para todo s, $1 \le s \le r-2$. Por consiguiente, tenemos que

$$\begin{aligned} (\phi_r)_S(Y) &= (\phi_r)_T(Y) \\ &= ({\phi_{r-1}}^{e_{r-1}f_{r-1}})_T(Y) + P_T(Y) \\ &= cY^{f_{r-1}} + \varphi(Y) \\ &= c\psi_{r-1}(Y). \end{aligned}$$

Con esto se acaba la demostración del teorema. □

Es interesante remarcar que las demostraciones anteriores, de la proposición y del teorema, nos enseñan a construir de manera efectiva y fácil de implementar un polinomio $\phi_r(X)$ que satisface las condiciones requeridas.

En el resto de este capítulo consideraremos fijado un polinomio arbitrario $\phi_r(X)$ cumpliendo las condiciones del teorema anterior, aunque no necesariamente construido como antes. Definimos la fracción racional $\Phi_r(X) := \dfrac{\phi_r(X)}{\Pi_r(X)} \in K(X)$.

Terminamos esta sección viendo tres corolarios, que nos proporcionarán más información sobre el polinomio $\phi_r(X)$.

3.3. Corolario.

(a) *El lado* $\mathbf{S}_{r-1}(\phi_r)$ *tiene por origen el punto* $(0, f_{r-1}v_r(\phi_{r-1}))$ *y por final el punto* $(e_{r-1}f_{r-1}, e_{r-1}f_{r-1}v_{r-1}(\phi_{r-1}))$.

(b) $v_r(\phi_r) = e_{r-1}f_{r-1}v_r(\phi_{r-1}) = e_{r-1}f_{r-1}(e_{r-1}v_{r-1}(\phi_{r-1}) + h_{r-1})$ *y* $\omega_r(\phi_r) = 1$.

(c) $v_r(\phi_r) = \displaystyle\sum_{i=1}^{r-1} e_{i+1}\cdots e_{r-1}\cdot e_i f_i \cdots e_{r-1}f_{r-1}\cdot h_i = v_r(\Pi_r)$.

(d) $v_r(\Phi_r) = 0$.

DEMOSTRACIÓN. Como el grado del polinomio $\phi_r(X)$ es igual al grado del polinomio $\phi_{r-1}(X)^{e_{r-1}f_{r-1}}$, entonces, por la propiedad (a) del teorema, el final del lado $\mathbf{S}_{r-1}(\phi_r)$ ha de ser el punto $(e_{r-1}f_{r-1}, e_{r-1}f_{r-1}v_{r-1}(\phi_{r-1}))$. Además, como el polinomio $\psi_{r-1}(Y)$ tiene grado igual a f_{r-1} y su término constante es no nulo, entonces, por la propiedad (b) del teorema, el origen del lado $\mathbf{S}_{r-1}(\phi_r)$ ha de ser el punto $(0, e_{r-1}f_{r-1}v_{r-1}(\phi_{r-1}) + h_{r-1}f_{r-1}) = (0, f_{r-1}v_r(\phi_{r-1}))$. Queda probada la parte (a).

La parte (b) se obtiene ahora aplicando las definiciones de v_r y ω_r.

Para probar la primera igualdad de la parte (c), por inducción sobre r, basta con observar que el sumatorio de la derecha satisface la misma relación de recurrencia que la obtenida en la parte (b) para $v_r(\phi_r)$, y que para $r = 2$ dicho sumatorio coincide con $e_1f_1h_1 = v_2(\phi_2)$. La segunda igualdad ya fue probada en la parte (b) de la proposición de 2.5.

La parte (d) es consecuencia directa de la parte (c) anterior. □

Del corolario de 9.3 en orden $r-1$ se sigue el siguiente

3.4. Corolario.

(a) *El polinomio $\phi_r(X)$ es irreducible en $K[X]$ y tiene tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$.*

(b) *Si $\eta \in \mathbb{Q}_p^{al}$ es una raíz de $\phi_r(X)$, entonces $e(K(\eta)/K) = e_0 \cdots e_{r-1}$ y $f(K(\eta)/K) = f_0 \cdots f_{r-1}$.* □

Del hecho que el polinomio $\phi_r(X)$ tenga tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ se sigue ahora el siguiente

3.5. Corolario. *Sea s un entero tal que $1 \leq s \leq r$. Entonces se tiene* $v_s(\phi_r) = \sum_{i=1}^{s-1} e_{i+1} \cdots e_{s-1} \cdot e_i f_i \cdots e_{r-1} f_{r-1} \cdot h_i$, $\omega_s(\phi_r) = e_s f_s \cdots e_{r-1} f_{r-1}$.

DEMOSTRACIÓN. Demostraremos las dos igualdades por inducción sobre s. Como $v_1(\phi_r) = 0$ y $m_r = \operatorname{gr}(\overline{\phi_r}) = f_0 \omega_1(\phi_r)$, las igualdades son claras para $s = 1$. Supongamos ahora que las dos igualdades son ciertas para un s, con $1 \leq s \leq r-1$. Por el lema de 4.2 en orden s, tenemos que los enteros $\omega_s(\phi_r)$, $\omega_s(\phi_r)h_s/e_s$ son las longitudes de la proyección del único lado del polígono $\mathrm{N}_s(\phi_r)$ sobre los ejes de abscisas y ordenadas, respectivamente, y que el valor $v_{s+1}(\phi_r) = e_s(v_s(\phi_r) + \omega_s(\phi_r)h_s/e_s)$. Por tanto, se tiene que $\omega_s(\phi_r) = e_s f_s \omega_{s+1}(\phi_r)$. Aplicando la hipótesis de inducción, se obtienen las dos igualdades para $s+1$. □

§4. Definición del polígono y del polinomio asociado

A partir de nuestro tipo de orden $r-1$, $\mathbf{t}_{r-1}$, en las dos secciones anteriores hemos definido una par de valoración (v_r, ω_r), y hemos construido de manera efectiva un polinomio mónico $\phi_r(X)$ con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ y de grado mínimo, m_r. Se recuerda que dicho polinomio está fijado y que no se supone necesariamente construido como en la demostración del teorema de 3.1. De la misma forma que en la §1 del capítulo 1 se definió el polígono de Newton respecto de la valoración v_1 y del polinomio $\phi_1(X)$, de un polinomio de $\mathcal{O}[X]$, ahora definimos el polígono de Newton respecto de la valoración v_r y del polinomio $\phi_r(X)$. El valor $v_r(\phi_r)$, que fue calculado

en la parte (c) del corolario de 3.3 y que en orden uno es nulo, actúa ahora como un "normalizador" del polígono. La definición clave del polinomio asociado (en orden r) que se dará está inspirada en los teoremas de 2.7 y de 2.8 y en la proposición de 4.6.

Sabemos que dado un polinomio no nulo $P(X) \in \mathcal{O}[X]$ hay una manera, y sólo una, de escribir

$$P(X) = \sum_{i=0}^{[\mathrm{gr}(P)/m_r]} A_i(X)\,\phi_r(X)^i \qquad (2.\,4.\,1)$$

con los $A_i(X) \in \mathcal{O}[X]$ de grado menor que m_r. Recordemos que a esta expresión la llamamos el desarrollo ϕ_r-ádico del polinomio $P(X)$.

4.1. Definición. *Llamaremos polígono de Newton del polinomio $P(X)$ respecto de la valoración v_r y del polinomio $\phi_r(X)$, y lo denotaremos por $\mathbf{N}_{(v_r,\phi_r)}(P)$ o abreviadamente por $\mathbf{N}_r(P)$, a la envolvente convexa inferior del conjunto de puntos del plano euclideo*

$$\mathbf{D}_r(P) = \mathbf{D}_{(v_r,\phi_r)}(P) := \{(i,u_i) : 0 \le i \le [\mathrm{gr}(P)/m_r], A_i(X) \neq 0\},$$

donde $u_i := v_r(A_i\,{\phi_r}^i) = v_r(A_i) + i\,v_r(\phi_r)$. Al conjunto $\mathbf{D}_r(P)$ le llamaremos el diagrama de Newton del polinomio $P(X)$ respecto de la valoración v_r y del polinomio $\phi_r(X)$.

Llamaremos parte principal del polígono $\mathbf{N}_r(P)$, y lo denotaremos por $\mathbf{N}_r^0(P)$, al polígono obtenido al considerar sólo los lados con pendiente negativa de $\mathbf{N}_r(P)$.

El polígono $\mathbf{N}_r^0(P)$ contiene la información sobre el polinomio $P(X)$, correspondiente al tipo $\mathbf{t}_{r-1}$, en la cual estamos interesados en orden r (cf. teoremas de 8.1, 9.1, 10.6 y 11.4). A continuación, calcularemos las proyecciones de este polígono sobre los ejes de coordenadas; en particular, veremos que la longitud de su proyección sobre el eje de abscisas es igual a $\omega_r(P) - v_{\phi_r}(P)$.

El siguiente lema nos indica cómo es la forma típica del polígono $\mathbf{N}_r(P)$, que es mostrada en la figura 2.1. En este polígono podemos leer los valores $v_{\phi_r}(P)$, $v_r(P)$ y $\omega_r(P)$ de la misma manera que en el polígono de

orden uno se leían los valores $v_{\phi_1}(P)$, $v_1(P)$ y $\omega_1(P)$ (cf. lema de 1.2 en el capítulo 1).

4.2. Lema. *Con las notaciones anteriores, tenemos*

(a) $v_{\phi_r}(P) = \min\{i : A_i(X) \not\equiv 0\}$.

(b) $v_r(P) = \min\{u_i : i\}$.

(c) $\omega_r(P) = \min\{i : u_i = v_r(P)\}$.

En particular, $\omega_r(P) = 0$ *si y sólo si* $v_r(P) = v_r(A_0)$.

DEMOSTRACIÓN. La parte (a) es evidente. Consideremos ahora el polinomio

$$Q(X) := \sum_{i\in I} A_i(X)\,\phi_r(X)^i\,, \quad I := \{i : u_i = u\}\,, \quad u := \min\{u_i : i\}\,;$$

así, el valor $v_r(P-Q) > u$. Puesto que cada $\omega_r(A_i) = 0$ (cf. parte (c) de la proposición de 2.3) y $\omega_r(\phi_r) = 1$ (cf. parte (b) del corolario de 3.3), entonces cada $\omega_r(A_i{\phi_r}^i) = \omega_r(A_i) + i\,\omega_r(\phi_r) = i$. Aplicando la segunda propiedad que satisface ω_r por ser pseudo-valoración respecto de la valoración v_r (cf. §1 del capítulo 1), deducimos que $v_r(Q) = u$ y que $\omega_r(Q) = \min I$. Luego, también es $v_r(P) = u$ y $\omega_r(P) = \min I$ (cf. parte (e) de la proposición de 2.2); con lo que quedan probadas las partes (b) y (c). □

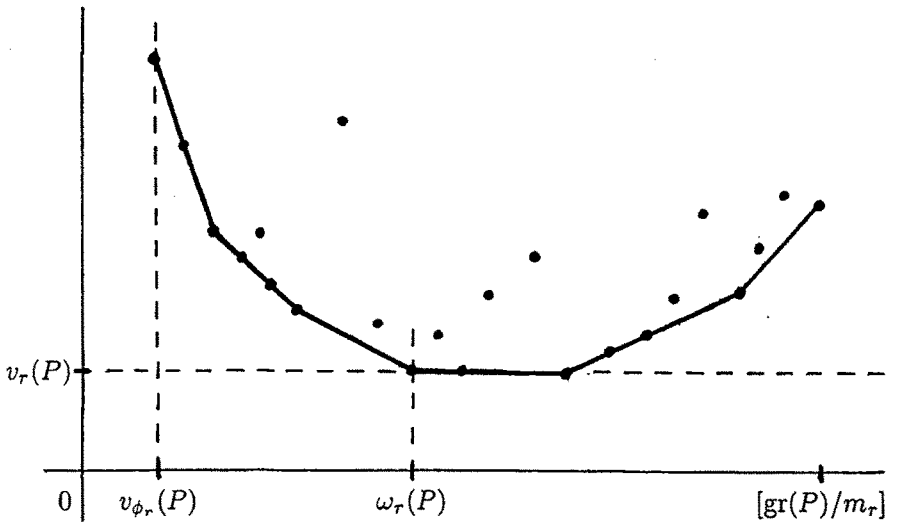


Figura 2.1. $\mathbf{D}_r(P)$, $\mathbf{N}_r(P)$ y $\mathbf{N}_r^0(P)$.

Sean $h, e \geq 1$ enteros primos entre si y S cualquier segmento del plano euclideo con pendiente $-h/e$, de origen (α, β) y final $(\alpha + d\,e, \beta - d\,h)$ con $\alpha, \beta, d \geq 0$ enteros. Para poder definir el *polinomio asociado (en orden r) al polinomio $P(X)$ y al segmento S* necesitaremos que se cumpla la siguiente condición:

Para todo entero j, $0 \leq j \leq d$, el punto $(\alpha + j\,e, u_{\alpha+j\,e})$ está por encima del segmento S o tocando a S (es decir, cada $u_{\alpha+j\,e} \geq \beta - j\,h$).

Desde luego, esta condición se cumple para los segmentos con pendiente $-h/e$ que contienen al segmento con pendiente $-h/e$ del polígono $\mathbf{N}_r^0(P)$.

El polinomio asociado (en orden r) $P_S(Y)$ va a tener sus coeficientes en el cuerpo finito $\mathbb{F}_{q_r}$. Vamos a asociar a cada término $A_i(X)\,\phi_r(X)^i$, con $\alpha \leq i \leq \alpha + d\,e$, $i \equiv \alpha \pmod{e}$, un elemento de $\mathbb{F}_{q_r}$. Si el punto (i, u_i) está por encima de S, le asociamos el elemento $0 \in \mathbb{F}_{q_r}$. Por tanto, nos fijamos en un i tal que el punto $(i, u_i) \in S$; así, es

$$v_r(A_i) = \beta - (i - \alpha)h/e - i\,v_r(\phi_r).$$

Consideramos la recta $L(i)$ con pendiente $-h_{r-1}/e_{r-1}$ que pasa por el punto $(0, v_r(A_i)/e_{r-1})$, cuya ecuación es $h_{r-1}x + e_{r-1}y = v_r(A_i)$. Entonces, por la definición de la valoración v_r, el segmento $\mathbf{S}_{r-1}(A_i)$ está sobre esta recta. Ahora, sea $S(i)$ el segmento más largo sobre la recta $L(i)$ con extremos de coordenadas enteras no negativas. Si $(\alpha(i), \beta(i))$ es el origen de este segmento, entonces es

$$h_{r-1}\alpha(i) + e_{r-1}\beta(i) = v_r(A_i)\,, \quad 0 \leq \alpha(i) < e_{r-1}\,.$$

Por tanto, $\alpha(i) \equiv l_{r-1}v_r(A_i) \equiv l_{r-1}(\beta - (i - \alpha)h/e)) \pmod{e_{r-1}}$, ya que $v_r(\phi_r)$ es un entero múltiplo de e_{r-1}. Por último, podemos considerar, por inducción, el polinomio asociado (en orden $r - 1$) al polinomio A_i y al segmento $S(i)$, $(A_i)_{S(i)}(Y) \in \mathbb{F}_{q_{r-1}}[Y]$. Sustituyendo en este polinomio la indeterminada Y por ζ_{r-1} obtenemos un elemento no nulo (por la parte (c) de la proposición de 2.3 y la observación (3) de 4.4 en orden $r - 1$) del cuerpo finito $\mathbb{F}_{q_r}$, que convenientemente "torzido" será el coeficiente $(i - \alpha)/e$-ésimo.

4.3. Definición. *Definimos el polinomio asociado (en orden r) al polinomio $P(X)$ y al segmento S como*

$$P_S(Y) := \sum_{i:(i,u_i)\in S} {\zeta_1}^{t_r(i,1)} \cdots {\zeta_{r-1}}^{t_r(i,r-1)} (A_i)_{S(i)}(\zeta_{r-1})\, Y^{(i-\alpha)/e} \in \mathbb{F}_{q_r}[Y],$$

donde

$$t_r(i,s) := -i\, e_{r-1}f_{r-1}\cdots e_{s+1}f_{s+1}l_sf_s(e_sv_s(\phi_s)+h_s),\ 1\le s\le r-2,$$
$$t_r(i,r-1) := \frac{1}{e_{r-1}}(\alpha(i) - l_{r-1}(\beta-(i-\alpha)h/e)) \in \mathbb{Z}.$$

4.4. Observaciones. (1). El segmento $S(i)$ y el entero $t_r(i,r-1)$ dependen únicamente del punto $(i,u_i) \in S$ y no dependen ni de la pendiente del segmento S ni de su origen ni de su final.

(2). Sea s un entero con $1 \le s \le r-1$. Entonces el signo de cada $t_r(i,s)$ es el opuesto del signo de l_s. Además, si $e_s = 1$, podemos tomar $l_s = 0$ y entonces cada $t_r(i,s) = 0$.

(3). Supongamos que el segmento S contiene al segmento con pendiente $-h/e$ del polígono $\mathrm{N}_r^0(P)$. Si S' es un segmento con pendiente $-h/e$ conteniendo a S de origen (α',β'), entonces $P_{S'}(Y) = Y^{(\alpha-\alpha')/e}P_S(Y)$, ya que la parte $S' \setminus S$ no contiene ningún punto (i,u_i).

(4). El coeficiente en $Y^{(i-\alpha)/e}$ del polinomio asociado es no nulo si y sólo si el punto $(i,u_i) \in S$. Por tanto, si S es el segmento con pendiente $-h/e$ del polígono $\mathrm{N}_r^0(P)$, $P_S(Y)$ es un polinomio de grado d y con término constante no nulo; pero, si S está por debajo de la recta que contiene al segmento con pendiente $-h/e$ del polígono $\mathrm{N}_r^0(P)$, el polinomio $P_S(Y) = 0$.

(5). Supongamos que $P_S(Y) \neq 0$, y sea $d' := \mathrm{gr}(P_S)$. Entonces para todo j, $0 \le j \le d'$, la recta $L(\alpha + j\,e)$ de ecuación $h_{r-1}x + e_{r-1}y = V_j$, donde $V_j := \beta - j\,h - (\alpha + j\,e)v_r(\phi_r) \le v_r(A_{\alpha+j\,e})$, contiene al menos un punto con coordenadas enteras no negativas, pues $V_j \ge V_{d'} + v_r(\phi_r) \ge e_{r-1}h_{r-1}$ para $j < d'$. Por tanto, podemos definir como antes el segmento $S(\alpha + j\,e)$ y los enteros $t_r(\alpha + j\,e, s)$, para $0 \le j \le d'$, y entonces tenemos que

$$P_S(Y) = \sum_{j=0}^{d'} {\zeta_1}^{t_r(\alpha+j\,e,1)} \cdots {\zeta_{r-1}}^{t_r(\alpha+j\,e,r-1)} (A_{\alpha+j\,e})_{S(\alpha+j\,e)}(\zeta_{r-1})\, Y^j\,,$$

ya que el polinomio $(A_{\alpha+j\,e})_{S(\alpha+j\,e)}(Y) = 0$ si el punto $(\alpha+j\,e, u_{\alpha+j\,e}) \notin S$.

(6). Si $Q(X) \in \mathcal{O}[X]$ es un polinomio no nulo distinto de $-P(X)$ para el cual podemos definir el polinomio asociado $Q_S(Y)$, entonces para $P(X)+Q(X)$ también podemos definir el polinomio asociado $(P+Q)_S(Y)$ y se tiene $(P+Q)_S(Y) = P_S(Y) + Q_S(Y)$.

(7). Si $0 \neq A \in \mathcal{O}$, entonces tenemos $\mathbf{N}_r(A) = \{(0, e_1 \cdots e_{r-1} v(A))\} =: S'$ y $A_{S'}(Y) = \zeta_1^{-l_1 v(A)} \cdots \zeta_{r-1}^{-l_{r-1} e_1 \cdots e_{r-2} v(A)} \overline{B} \in \mathbb{F}_{q_r}^*$, con $B := A/\pi^{v(A)} \in \mathcal{O}^*$. Además, si $A \in \mathcal{O}^*$, entonces es $\mathbf{N}_r(A\,P) = \mathbf{N}_r(P)$ y $(A\,P)_S(Y) = \overline{A}\,P_S(Y)$.

A continuación, veremos una propiedad clave del polinomio asociado (en orden r), que nos permitirá entender su definición. Para esto, introducimos una fracción racional asociada al polinomio $P(X)$ y al segmento S, que desempeñará el papel que hacía el polinomio $P^S(X) \in K[X]$ en primer orden (cf. definición de 1.6 en el capítulo 1).

4.5. Definición. *Definimos* $P^S(X) := \dfrac{P^o(X)}{\Phi_r(X)^\alpha \pi_r(X)^\beta} \in K(X)$, *donde* $P^o(X) := \displaystyle\sum_{i:(i,u_i)\in S} A_i(X)\,\phi_r(X)^i \in \mathcal{O}[X]$.

Observemos que, por definición, $P_S(Y) = (P^o)_S(Y)$ en $\mathbb{F}_{q_r}[Y]$.

Consideramos la fracción racional $\gamma_r(X) := \dfrac{\Phi_r(X)^e}{\pi_r(X)^h} \in K(X)$, y, para cada i tal que $(i;u_i) \in S$, consideramos también las fracciones racionales

$$\Gamma_i(X) := \frac{\Phi_{r-1}(X)^{\alpha(i)} \pi_{r-1}(X)^{\beta(i)} \Pi_r(X)^i}{\pi_r(X)^{\beta-(i-\alpha)h/e}} \in K(X),$$

$$B_i(X) := \frac{A_i(X)}{\Phi_{r-1}(X)^{\alpha(i)} \pi_{r-1}(X)^{\beta(i)}} \in K(X).$$

4.6. Proposición. *Con las notaciones anteriores, tenemos que*

$$P^S(X) = \sum_{i:(i,u_i)\in S} \Gamma_i(X)\,B_i(X)\,\gamma_r(X)^{(i-\alpha)/e},$$

cada $\Gamma_i(X) = \gamma_1(X)^{t_r(i,1)} \cdots \gamma_{r-1}(X)^{t_r(i,r-1)}$ *y cada* $B_i(X)$ *satisface que* $v_r(B_i) = 0$ *y que* $\overline{B_i(X)}^r = (A_i)_{S(i)}\left(\overline{\gamma_{r-1}(X)}^r\right)$ *en* k_{v_r}.

DEMOSTRACIÓN. La primera igualdad es clara por las definiciones dadas.

Consideramos un i tal que $(i, u_i) \in S$. Entonces sabemos que

$$v_r(A_i) = \beta - (i-\alpha)h/e - i\, v_r(\phi_r) = h_{r-1}\alpha(i) + e_{r-1}\beta(i).$$

Por la parte (b) de la proposición de 2.5 y la parte (c) del corolario de 3.3, sabemos también que $v_r(\Phi_{r-1}) = h_{r-1}$, $v_r(\pi_{r-1}) = e_{r-1}$, $v_r(\pi_r) = 1$ y $v_r(\Pi_r) = v_r(\phi_r)$. Por tanto, $v_r(\Gamma_i) = v_r(B_i) = 0$.

Veamos ahora la igualdad entre las fracciones racionales $\Gamma_i(X)$ y $\gamma_1(X)^{t_r(i,1)} \cdots \gamma_{r-1}(X)^{t_r(i,r-1)}$. Por el lema de 2.9, sabemos que $\Gamma_i(X)$ se puede expresar, y en forma única, como un producto de potencias enteras de los $\gamma_s(X)$ con $1 \le s \le r-1$. Vamos a calcular estas potencias. Expresando $\Gamma_i(X)$ en función de $\Phi_{r-1}(X)$, $\Pi_{r-1}(X)$ y $\pi_{r-1}(X)$, tenemos que

$$\Gamma_i(X) = \Phi_{r-1}(X)^{e_{r-1}t_r(i,r-1)}\Pi_{r-1}(X)^{i\,e_{r-1}f_{r-1}}\pi_{r-1}(X)^{n_i},$$

donde

$$\begin{aligned} n_i :&= \beta(i) + i\, h_{r-1}f_{r-1} + l'_{r-1}(\beta - (i-\alpha)h/e) \\ &= i(h_{r-1}f_{r-1} - v_r(\phi_r)/e_{r-1}) - h_{r-1}t_r(i, r-1) \\ &= -i\, e_{r-1}f_{r-1}v_{r-1}(\phi_{r-1}) - h_{r-1}t_r(i, r-1) \quad \text{(por 3.3 (b))}. \end{aligned}$$

Luego, se tiene que

$$\Gamma_i(X) = \rho_{r-1}(X)^{i\,e_{r-1}f_{r-1}}\gamma_{r-1}(X)^{t_r(i,r-1)}, \qquad (*)$$

donde $\rho_s(X) := \Pi_s(X)\pi_s(X)^{-v_s(\phi_s)} \in K(X)$, para $1 \le s \le r-1$. Si $r = 2$, entonces $\rho_{r-1}(X) = 1$ y hemos terminado. Supongamos que es $r \ge 3$. Expresando ahora $\rho_{s+1}(X)$ en función de $\Phi_s(X)$, $\Pi_s(X)$ y $\pi_s(X)$, y aplicando de nuevo la parte (b) del corolario de 3.3, tenemos que

$$\rho_{s+1}(X) = \rho_s(X)^{e_sf_s}\gamma_s(X)^{-l_sf_s(e_sv_s(\phi_s)+h_s)}, \quad 1 \le s \le r-2.$$

Procediendo recurrentemente, llegamos entonces a obtener una expresión explícita de $\rho_{r-1}(X)$ como producto de potencias enteras de las $\gamma_s(X)$ con $1 \le s \le r-2$. Substituyendo después en $(*)$ obtenemos nuestras tes.

Finalmente, observemos que $A_i(X) = (A_i)^\circ(X) + R_i(X)$, donde $R_i(X) \in \mathcal{O}[X]$ y $v_r(R_i) > v_r(A_i)$. Dividiendo por $\Phi_{r-1}(X)^{\alpha(i)}\pi_{r-1}(X)^{\beta(i)}$

cada miembro de la anterior igualdad y tomando después clases módulo el ideal $\mathfrak{m}_{v_r}$, obtenemos $\overline{B_i(X)}^r = \overline{(A_i)^{S(i)}(X)}^r = (A_i)_{S(i)}\left(\overline{\gamma_{r-1}(X)}^r\right)$, por el teorema de 2.8. Con esto queda probado el resto de la proposición. □

Para terminar esta sección, vamos a definir, de forma análoga, el polígono de Newton y el polinomio asociado para un ϕ_r-desarrollo arbitrario de $P(X)$,

$$P(X) = \sum_{i\geq 0} A_i'(X)\,\phi_r(X)^i \qquad (2.\,4.\,2)$$

con los polinomios $A_i'(X) \in \mathcal{O}[X]$ casi todos nulos (no necesariamente de grado menor que m_r).

4.7. Definición. *Llamaremos polígono de Newton del ϕ_r-desarrollo* (2.4.2) *del polinomio $P(X)$ respecto de la valoración v_r y del polinomio $\phi_r(X)$, y lo denotaremos por $\mathbf{N}_{(v_r,\phi_r)}(P,\{A_i'\})$ o abreviadamente por $\mathbf{N}_r(P,\{A_i'\})$, a la envolvente convexa inferior del conjunto finito de puntos del plano euclideo*

$$\mathbf{D}_r(P,\{A_i'\}) = \mathbf{D}_{(v_r,\phi_r)}(P,\{A_i'\}) := \{(i,u_i') : i \geq 0, A_i'(X) \neq 0\},$$

donde $u_i' := v_r(A_i'\,{\phi_r}^i)$. Al conjunto $\mathbf{D}_r(P,\{A_i'\})$ le llamaremos el diagrama de Newton del ϕ_r-desarrollo (2.4.2) *del polinomio $P(X)$ respecto de la valoración v_r y del polinomio $\phi_r(X)$.*

Llamaremos parte principal del polígono $\mathbf{N}_r(P,\{A_i'\})$, y lo denotaremos por $\mathbf{N}_r^0(P,\{A_i'\})$, al polígono obtenido al considerar sólo los lados con pendiente negativa de $\mathbf{N}_r(P,\{A_i'\})$.

Sea S un segmento con datos $(\alpha,\beta),d,e,h$. Suponemos ahora que para todo entero j, $0 \leq j \leq d$, el punto $(\alpha + j\,e, u'_{\alpha+j\,e})$ está por encima de o tocando a S.

4.8. Definición. *Definimos el polinomio asociado (en orden r) al ϕ_r-desarrollo* (2.4.2) *del polinomio $P(X)$ y al segmento S como*

$$(P,\{A_i'\})_S(Y) := \sum_{i:(i,u_i')\in S} {\zeta_1}^{t_r(i,1)} \cdots {\zeta_{r-1}}^{t_r(i,r-1)}\,(A_i')_{S(i)}(\zeta_{r-1})\,Y^{(i-\alpha)/e},$$

donde el segmento $S(i)$ y los enteros $t_r(i,s)$ están definidos como antes.

4.9. Observación. Ahora, el coeficiente en $Y^{(i-\alpha)/e}$ del polinomio asociado $(P,\{A_i'\})_S(Y) \in \mathbb{F}_{q_r}[Y]$ es no nulo si y sólo si $(i,u_i') \in S$ y $\omega_r(A_i') = 0$ (cf. parte (c) de la proposición de 2.3 y observación (3) de 4.4 en orden $r-1$).

§5. Desarrollos admisibles

En esta sección compararemos el polígono de Newton de un ϕ_r-desarrollo arbitrario de un polinomio con el del desarrollo ϕ_r-ádico. Como en primer orden (cf. §2 del capítulo 1), ello nos conducirá a definir, con la ayuda de nuestra pseudo-valoración ω_r, el concepto de ϕ_r-desarrollo admisible. Estos desarrollos tendrán la misma parte principal y el mismo polinomio asociado (en orden r) a cada lado; lo cual será utilizado en la sección siguiente para demostrar el teorema del producto.

5.1. Proposición. *Sea $P(X) \in \mathcal{O}[X]$ un polinomio no nulo. Consideramos los enteros (eventualmente $+\infty$) $u_i := v_r(A_i\,{\phi_r}^i)$ y $u_i' := v_r(A_i'\,{\phi_r}^i)$ correspondientes a los ϕ_r-desarrollos* (2.4.1) *y* (2.4.2)*, respectivamente, de $P(X)$. Sean $i_0 \le i_g$ las abscisas del primer y último vértice, respectivamente, del polígono $\mathbf{N}_r^0(P,\{A_i'\})$. Sean $h,e \ge 1$ enteros primos entre sí, S el segmento con pendiente $-h/e$ de $\mathbf{N}_r^0(P,\{A_i'\})$ y (α,β), $(\alpha+de,\beta-dh)$ los extremos de S. Entonces*

(a) *El polígono $\mathbf{N}_r(P)$ está "por encima" del polígono $\mathbf{N}_r^0(P,\{A_i'\})$; es decir,*

(i) *$A_i(X) = 0$, para $0 \le i < i_0$,*

(ii) *(i,u_i) está por encima de o tocando a S, para $\alpha \le i \le \alpha+de$, y*

(iii) *$u_i \ge u_{i_g}'$, para todo $i \ge 0$.*

(b) *Para todo i, $\alpha \le i \le \alpha+de$, se tiene que*

$$(i,u_i) \in S \iff (i,u_i') \in S \text{ y } \omega_r(A_i') = 0,$$

y, en tal caso, que $(A_i)_{S(i)}(\zeta_{r-1}) = (A_i')_{S(i)}(\zeta_{r-1})$ en $\mathbb{F}_{q_r}$, donde $S(i)$ es el segmento más largo sobre la recta $h_{r-1}x + e_{r-1}y = v_r(A_i)$ con extremos de coordenadas enteras no negativas.

DEMOSTRACIÓN. Sea $A'_j(X) = \sum_{k\geq 0} A'_{j,k}(X)\,\phi_r(X)^k$ el desarrollo ϕ_r-ádico del polinomio $A'_j(X)$, $j \geq 0$. Así, por la unicidad del desarrollo ϕ_r-ádico, obtenemos que

$$A_i(X) = \sum_{j\leq i} A'_{j,i-j}(X)\,, \quad i \geq 0; \tag{$*$}$$

por tanto, teniendo en cuenta que $A'_j(X) = 0$ para $j < i_0$, tenemos (i) de la parte (a). Además, por la parte (b) del lema de 4.2 aplicado al polinomio $A'_j(X)\,\phi_r(X)^j = \sum_{i\geq j} A'_{j,i-j}(X)\,\phi_r(X)^i$, se tiene que

$$u'_j \leq v_r(A'_{j,i-j}{\phi_r}^i)\,, \quad 0 \leq j \leq i; \tag{$**$}$$

de donde se deduce (iii) de la parte (a), teniendo presente la igualdad de $(*)$ y que $u'_j \geq u'_{i_g}$ para todo $j \geq 0$.

Ahora, consideremos un entero i tal que $\alpha \leq i \leq \alpha + de$, y ponemos $\mu_i := \beta - (i-\alpha)h/e \in \mathbb{Q}$. Entonces, por la igualdad de $(*)$, podemos escribir

$$A_i(X)\,\phi_r(X)^i = A'_{i,0}(X)\,\phi_r(X)^i + R_i(X)\,, \quad R_i(X) \in \mathcal{O}[X]\,, \quad v_r(R_i) > \mu_i\,,$$

por la desigualdad de $(**)$ y puesto que $u'_j > \mu_i$ para $j < i$. Por consiguiente, como $v_r(A'_{i,0}{\phi_r}^i) \geq u'_i \geq \mu_i$, obtenemos que $u_i \geq \mu_i$ y que

$$u_i = \mu_i \iff u'_i = \mu_i \text{ y } v_r(A'_{i,0}) = v_r(A'_i) \iff u'_i = \mu_i \text{ y } \omega_r(A'_i) = 0,$$

la última equivalencia por la parte (c) del lema de 4.2. Hemos probado (ii) de la parte (a), y la equivalencia de la parte (b).

Finalmente, consideremos un i tal que $(i, u_i) \in S$. Hemos visto que

$$v_r(A_i - A'_{i,0}) > V_i := \mu_i - i\,v_r(\phi_r) = v_r(A_i) = v_r(A'_{i,0}) = v_r(A'_i)\,;$$

así, por las observaciones (6) y (4) de 4.4, obtenemos las igualdades

$$(A_i)_{S(i)}(Y) = (A'_{i,0})_{S(i)}(Y) + (A_i - A'_{i,0})_{S(i)}(Y) = (A'_{i,0})_{S(i)}(Y) \text{ en } \mathbb{F}_{q_{r-1}}[Y].$$

Por consiguiente, para acabar de demostrar la proposición, hemos de probar ahora la igualdad

$$(A'_i)_{S(i)}(\zeta_{r-1}) = (A'_{i,0})_{S(i)}(\zeta_{r-1})\,, \quad \text{en } \mathbb{F}_{q_r}\,.$$

Si $v_r(A'_i - A'_{i,0}) > V_i$, entonces, procediendo como antes, tenemos que

$$(A'_i)_{S(i)}(Y) = (A'_{i,0})_{S(i)}(Y)\,, \quad \text{en } \mathbb{F}_{q_{r-1}}[Y]\,,$$

y hemos acabado. Si $v_r(A'_i - A'_{i,0}) = V_i$, el segmento $\mathbf{S}_{r-1}(A'_i - A'_{i,0}) \subseteq S(i)$ y, como el polinomio $\phi_r(X)$ divide a $A'_i(X) - A'_{i,0}(X)$ en $\mathcal{O}[X]$, entonces

$$\psi_{r-1}(Y) \mid (A'_i - A'_{i,0})_{S(i)}(Y) = (A'_i)_{S(i)}(Y) - (A'_{i,0})_{S(i)}(Y)\,, \quad \text{en } \mathbb{F}_{q_{r-1}}[Y]\,,$$

por el corolario de 6.2 en orden $r-1$ y por la elección de $\phi_r(X)$ (cf. §3), con lo cual también se acaba. □

5.2. Definición. *El ϕ_r-desarrollo* (2.4.2) *de un polinomio no nulo $P(X) \in \mathcal{O}[X]$ diremos que es admisible cuando $\omega_r(A'_i) = 0$ para todo entero i tal que el punto (i, u'_i) pertenece al conjunto de vértices del polígono $\mathbf{N}^0_r(P, \{A'_i\})$.*

Por la parte (c) de la proposición de 2.3, el desarrollo ϕ_r-ádico del polinomio $P(X)$ siempre es admisible. Pues bien, con la definición que acabamos de dar, de la proposición de 5.1 y la observación de 4.9 se deduce el siguiente

5.3. Corolario. *Sea $P(X) = \sum_{i\geq 0} A'_i(X)\,\phi_r(X)^i$ un ϕ_r-desarrollo admisible de un polinomio no nulo $P(X) \in \mathcal{O}[X]$. Entonces*

(a) $\mathbf{N}^0_r(P, \{A'_i\}) = \mathbf{N}^0_r(P)$.

(b) $(P, \{A'_i\})_S(Y) = P_S(Y)$ *para cada segmento S del polígono $\mathbf{N}^0_r(P)$.* □

§6. Teorema del producto

En esta sección vamos a ver que, al igual que para primer orden (cf. §2 del capítulo 1), en orden r también la parte principal del polígono de Newton de un producto de un número finito de polinomios se obtiene sumando las partes principales de cada factor, y que el polinomio asociado al producto es igual al producto de los polinomios asociados a cada factor. Para la demostración de este resultado, veremos que si tenemos ϕ_r-desarrollos admisibles de cada factor, entonces al hacer su producto el ϕ_r-desarrollo que nos sale también es admisible; después, aplicaremos el corolario de 5.3.

6.1. Teorema. (Teorema del producto) *Sean* $P_1(X),\dots,P_g(X) \in \mathcal{O}[X]$ *polinomios no nulos y* $P(X) := P_1(X)\cdots P_g(X)$ *su producto. Sean* $h, e \geq 1$ *enteros primos entre si,* S_ν *el segmento con pendiente* $-h/e$ *del polígono* $\mathrm{N}_r^0(P_\nu)$, $1 \leq \nu \leq g$, *y* $S := S_1 + \cdots + S_g$. *Entonces*

(a) S *es el segmento con pendiente* $-h/e$ *del polígono* $\mathrm{N}_r^0(P)$.

Por tanto, $\mathrm{N}_r^0(P) = \mathrm{N}_r^0(P_1) + \cdots + \mathrm{N}_r^0(P_g)$.

(b) $P_S(Y) = (P_1)_{S_1}(Y)\cdots(P_g)_{S_g}(Y)$ *en* $\mathbb{F}_{q_r}[Y]$.

DEMOSTRACIÓN. Por inducción sobre g, podemos suponer que $g = 2$. Sea $P_\nu(X) = \sum A_{\nu,i}(X)\,\phi_r(X)^i$ un ϕ_r-desarrollo admisible de $P_\nu(X)$ y ponemos $u_{\nu,i} := v_r(A_{\nu,i}{\phi_r}^i)$ $(\nu = 1, 2)$. Así, tenemos

$$P(X) = \sum A_k(X)\,\phi_r(X)^k, \qquad A_k(X) := \sum_{i+j=k} A_{1,i}(X)\,A_{2,j}(X) \in \mathcal{O}[X],$$

y $u_{1,i} + u_{2,j} = v_r(A_{1,i}A_{2,j}{\phi_r}^{i+j})$. Por el corolario de 5.3, para probar el teorema nos bastará con ver que

(a') S es el segmento con pendiente $-h/e$ del polígono $\mathrm{N}_r^0(P, \{A_k\})$.

Por tanto, $\mathrm{N}_r^0(P, \{A_k\}) = \mathrm{N}_r^0(P_1) + \mathrm{N}_r^0(P_2)$.

(b') $(P, \{A_k\})_S(Y) = (P_1)_{S_1}(Y)\,(P_2)_{S_2}(Y)$.

(c') El ϕ_r-desarrollo $P(X) = \sum A_k(X)\,\phi_r(X)^k$ es admisible.

Sean (α_ν, β_ν) y $(\alpha_\nu + d_\nu e, \beta_\nu - d_\nu h)$ el origen y final, respectivamente, del segmento S_ν, y ponemos $\alpha := \alpha_1 + \alpha_2$, $\beta := \beta_1 + \beta_2$ y $d := d_1 + d_2$. Así, los puntos (α, β) y $(\alpha + d\,e, \beta - d\,h)$ son el origen y final, respectivamente, del segmento S. Puesto que

$$u_{\nu,i} \geq \beta_\nu - (i - \alpha_\nu)h/e, \quad u_{\nu,i} = \beta_\nu - (i - \alpha_\nu)h/e \iff i \in I_\nu,$$

donde $I_\nu := \{i : (i, u_{\nu,i}) \in S_\nu\}$, entonces, si $k = i + j$, tenemos que

$$u_{1,i}+u_{2,j} \geq \beta-(k-\alpha)h/e,\ u_{1,i}+u_{2,j} = \beta-(k-\alpha)h/e \iff i \in I_1 \text{ y } j \in I_2.$$

Por tanto, para todo $k \geq 0$, podemos escribir

$$A_k(X) = \sum{}^{\circ} A_{1,i}(X)\,A_{2,j}(X) + R_k(X), \qquad (*)$$

donde la suma anterior $\sum^{o}$ está extendida a todas las parejas de índices $(i,j) \in I_1 \times I_2$ tales que $i+j=k$, y $R_k(X) \in \mathcal{O}[X]$ es un polinomio que satisface $v_r(R_k) > \beta - (k-\alpha)h/e - k\,v_r(\phi_r)$; de aquí obtenemos que

$$v_r(A_k{\phi_r}^k) \geq \beta - (k-\alpha)h/e,$$
$$v_r(A_k{\phi_r}^k) = \beta - (k-\alpha)h/e \iff v_r\left(\sum\nolimits^{o} A_{1,i}A_{2,j}{\phi_r}^k\right) = \beta - (k-\alpha)h/e.$$

Esta última igualdad se satisface si $k=\alpha$ o si $k=\alpha+de$, ya que entonces la suma $\sum^{o}$ tiene un único sumando,

$$A_{1,\alpha_1}(X)\,A_{2,\alpha_2}(X) \quad \text{o} \quad A_{1,\alpha_1+d_1e}(X)\,A_{2,\alpha_2+d_2e}(X),$$

respectivamente; pero, es falsa si $k<\alpha$ o si $k>\alpha+de$, puesto que en estos casos la suma $\sum^{o}$ carece de sumandos. Por consiguiente, hemos probado que el segmento con pendiente $-h/e$ del polígono $\mathrm{N}_r^0(P,\{A_k\})$ es S; con lo cual queda demostrado (a').

Ahora, probemos la admisibilidad del anterior ϕ_r-desarrollo del polinomio $P(X)$. Hemos de ver que $\omega_r(A_k)=0$ para $k=\alpha,\alpha+de$. Por la igualdad de $(*)$ y la parte (e) de la proposición de 2.2, obtenemos que $\omega_r(A_\alpha)=\omega_r(A_{1,\alpha_1}A_{2,\alpha_2})=\omega_r(A_{1,\alpha_1})+\omega_r(A_{2,\alpha_2})=0$, pues los desarrollos anteriores de cada polinomio $P_\nu(X)$ son admisibles. Análogamente se obtiene que $\omega_r(A_{\alpha+de})=0$.

Por último, veamos la afirmación referente a los polinomios asociados. En primer lugar, recordemos que

$$(P_\nu)_{S_\nu}(Y) = \sum_{i\in I_\nu} {\zeta_1}^{t_r^\nu(i,1)}\cdots{\zeta_{r-1}}^{t_r^\nu(i,r-1)}(A_{\nu,i})_{S_\nu(i)}(\zeta_{r-1})\,Y^{(i-\alpha_\nu)/e},$$

donde $S_\nu(i)$ es el segmento más largo sobre la recta de ecuación

$$h_{r-1}x + e_{r-1}y = \beta_\nu - (i-\alpha_\nu)h/e - i\,v_r(\phi_r)$$

con extremos de coordenadas enteras no negativas,

$$t_r^\nu(i,s) := -i\,e_{r-1}f_{r-1}\cdots e_{s+1}f_{s+1}l_sf_s(e_sv_s(\phi_s)+h_s),\ 1\leq s\leq r-2,$$
$$t_r^\nu(i,r-1) := \frac{1}{e_{r-1}}(\alpha_\nu(i) - l_{r-1}(\beta_\nu - (i-\alpha_\nu)h/e)),$$

y $\alpha_\nu(i)$ es la abscisa del origen del segmento $S_\nu(i)$; y, por la observación (5) de 4.4, que

$$(P,\{A_k\})_S(Y) = \sum_{k\in I} {\zeta_1}^{t_r(k,1)} \cdots {\zeta_{r-1}}^{t_r(k,r-1)} (A_k)_{S(k)}(\zeta_{r-1})\, Y^{(k-\alpha)/e},$$

donde $I := \{k : \alpha \le k \le \alpha + de, k \equiv \alpha \pmod e\}$, $S(k)$ es el segmento más largo sobre la recta de ecuación

$$h_{r-1}x + e_{r-1}y = \beta - (k-\alpha)h/e - k\, v_r(\phi_r)$$

con extremos de coordenadas enteras no negativas,

$$t_r(k,s) := -k\, e_{r-1}f_{r-1}\cdots e_{s+1}f_{s+1}l_s f_s(e_s v_s(\phi_s) + h_s),\ 1 \le s \le r-2,$$
$$t_r(k,r-1) := \frac{1}{e_{r-1}}(\alpha(k) - l_{r-1}(\beta - (k-\alpha)h/e)),$$

y $\alpha(k)$ es la abscisa del origen del segmento $S(k)$.

Para un $i \in I_1$ y $j \in I_2$, si ponemos

$$\varepsilon_{i,j} := \begin{cases} 1 & \text{si } \alpha_1(i) + \alpha_2(j) \ge e_{r-1}, \\ 0 & \text{si } \alpha_1(i) + \alpha_2(j) < e_{r-1}, \end{cases}$$

y $k = i + j \in I$, tenemos que

$$S_1(i) + S_2(j) \subseteq S(k),$$
$$\alpha_1(i) + \alpha_2(j) = \alpha(k) + \varepsilon_{i,j}e_{r-1},$$
$$t_r^1(i,s) + t_r^2(j,s) = t_r(k,s), \quad \text{para } 1 \le s \le r-2,$$
$$t_r^1(i,r-1) + t_r^2(j,r-1) = t_r(k,r-1) + \varepsilon_{i,j},$$

y, por la observación (3) de 4.4 y por este teorema en orden $r-1$, que

$${\zeta_{r-1}}^{t_r(k,r-1)}(A_{1,i}A_{2,j})_{S(k)}(\zeta_{r-1}) =$$
$${\zeta_{r-1}}^{t_r(k,r-1)+\varepsilon_{i,j}}(A_{1,i}A_{2,j})_{S_1(i)+S_2(j)}(\zeta_{r-1}) =$$
$${\zeta_{r-1}}^{t_r^1(i,r-1)}(A_{1,i})_{S_1(i)}(\zeta_{r-1}) \cdot {\zeta_{r-1}}^{t_r^2(j,r-1)}(A_{2,j})_{S_2(j)}(\zeta_{r-1});$$

es decir, el entero $t_r(k,r-1)$ corrige la no compatibilidad para el producto del origen $(\alpha(k),\beta(k))$ de $S(k)$. Por consiguiente, para probar la parte (b'), hemos de ver que para todo $k \in I$ se satisface la igualdad

$$(A_k)_{S(k)}(\zeta_{r-1}) = \sum\nolimits^{o} (A_{1,i}A_{2,j})_{S(k)}(\zeta_{r-1}).$$

Pero, por la igualdad de (∗) y la observación (6) de 4.4, se tiene que

$$(A_k)_{S(k)}(Y) = \left(\sum\nolimits^{o} A_{1,i}A_{2,j}\right)_{S(k)}(Y) = \sum\nolimits^{o}(A_{1,i}A_{2,j})_{S(k)}(Y)$$

y, por tanto, la igualdad deseada. □

Teniendo en cuenta la observación (3) de 4.4, del teorema del producto se deduce el siguiente

6.2. Corolario. *Sean $h, e \geq 1$ enteros primos entre si. Sea S (resp. T) el segmento con pendiente $-h/e$ del polígono $\mathbf{N}_r^0(P)$ (resp. $\mathbf{N}_r^0(Q)$) de un polinomio no nulo $P(X)$ (resp. $Q(X)$) de $\mathcal{O}[X]$, y sea S' un segmento con pendiente $-h/e$ conteniendo a S. Si $Q(X)$ divide a $P(X)$ en $\mathcal{O}[X]$, entonces $Q_T(Y)$ divide a $P_{S'}(Y)$ en $\mathbb{F}_{q_r}[Y]$.* □

§7. Cálculo del valor $v(R(\theta))$ con el polígono

En esta sección, consideraremos fijado un entero algebraico $\theta \in \mathbb{Q}_p^{al}$ con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ (cf. §1). Sean $F(X) := \mathrm{Irr}(\theta, K, X) \in \mathcal{O}[X]$ el polinomio irreducible de θ sobre K, y $L := K(\theta)$. Entonces tenemos que

(0.b) $\overline{F}(Y) = \psi_0(Y)^{a_0}$ en $\mathbb{F}_{q_0}[Y]$. Así, $\psi_0(Y) = \mathrm{Irr}\left(\overline{\theta}, \mathbb{F}_{q_0}, Y\right)$. Luego, existe un único automorfismo $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_1}/\mathbb{F}_{q_0})$ tal que $\sigma(\zeta_0) = \overline{\theta}$.

Y para cada i, $1 \leq i \leq r-1$, se tiene que

(i.a) El polígono $\mathbf{N}_i(F)$ consta de un solo lado S_i, cuya pendiente es igual a $-h_i/e_i$. Así, $F(X) \neq \phi_i(X)$ y, por la proposición de 8.4 en orden i,

$$v(\phi_i(\theta)) = \frac{1}{e_1 \cdots e_{i-1}}\left(v_i(\phi_i) + \frac{h_i}{e_i}\right) = \sum_{j=1}^{i} \frac{e_j f_j \cdots e_i f_i}{e_i f_i} \cdot \frac{h_j}{e_1 \cdots e_j}.$$

Además, es fácil comprobar inductivamente que

$$v(\Phi_i(\theta)) = \frac{h_i}{e_1 \cdots e_i},\ v(\gamma_i(\theta)) = 0,\ v(\pi_{i+1}(\theta)) = \frac{1}{e_1 \cdots e_i} \text{ y}$$

$$v(\Pi_{i+1}(\theta)) = \sum_{j=1}^{i} e_j f_j \cdots e_i f_i \cdot \frac{h_j}{e_1 \cdots e_j}.$$

(i.b) $F_{S_i}(Y) = c_i\,\psi_i(Y)^{a_i}$ en $\mathbb{F}_{q_i}[Y]$, para algún elemento $c_i \in \mathbb{F}_{q_i}^*$ y para algún entero $a_i \geq 1$. Así, por la proposición de 9.4 en orden i, $\psi_i^{\sigma}(Y) = \operatorname{Irr}\left(\overline{\gamma_i(\theta)}, \mathbb{F}_{q_i}, Y\right)$, donde $\sigma \in \operatorname{Gal}(\mathbb{F}_{q_i}/\mathbb{F}_{q_0})$ es el único automorfismo tal que $\sigma(\zeta_j) = \overline{\gamma_j(\theta)}$ para cada j, $0 \leq j \leq i-1$. Luego, existe un único automorfismo $\sigma \in \operatorname{Gal}(\mathbb{F}_{q_{i+1}}/\mathbb{F}_{q_0})$ que satisface $\sigma(\zeta_j) = \overline{\gamma_j(\theta)}$ para cada j, $0 \leq j \leq i$.

Por último, notemos que $\operatorname{gr}(F) = m_r a_{r-1}$, por la proposición de 1.2.

7.1. Proposición. *Sean $P(X) \in \mathcal{O}[X]$ un polinomio no nulo. Entonces*

(a) $e_1 \cdots e_{r-1} v(P(\theta)) \geq v_r(P)$.

(b) $e_1 \cdots e_{r-1} v(P(\theta)) = v_r(P)$ *si sólo si* $\omega_r(P) = 0$.

En particular, $e_1 \cdots e_{r-1} v(P(\theta)) = v_r(P)$ *si* $\operatorname{gr}(P) < m_r$.

DEMOSTRACIÓN. Si $r = 1$, la parte (a) es inmediata y la parte (b) se sigue de que $\psi_0(Y) = \operatorname{Irr}\left(\overline{\theta}, \mathbb{F}_{q_0}, Y\right)$, por la propiedad (0.b).

Sea $P(X) = \sum A_i(X)\,\phi_{r-1}(X)^i$ el desarrollo ϕ_{r-1}-ádico de $P(X)$. Para un i tal que $A_i(X) \neq 0$, por inducción y las conclusiones de $(r-1.\text{a})$, se tiene que

$$\begin{aligned} e_1 \cdots e_{r-1} v(A_i(\theta)\,\phi_{r-1}(\theta)^i) &= e_{r-1} v_{r-1}(A_i) + i\, e_1 \cdots e_{r-1} v(\phi_{r-1}(\theta)) \\ &= e_{r-1} v_{r-1}(A_i) + i(e_{r-1} v_{r-1}(\phi_{r-1}) + h_{r-1}) \\ &\geq v_r(P) \quad \text{(por la parte (b) de 2.2)}; \end{aligned}$$

además, la desigualdad anterior es una igualdad si y sólo si $i \in I$, donde $I := \{i : (i, v_{r-1}(A_i\,\phi_{r-1}^{\,i})) \in S\}$ y $S := \mathbf{S}_{r-1}(P)$. Por tanto, tenemos que $e_1 \cdots e_{r-1} v(P(\theta)) \geq v_r(P)$ y que $e_1 \cdots e_{r-1} v(P(\theta)) = v_r(P)$ si y sólo si

$$e_1 \cdots e_{r-1} v\left(\sum_{i \in I} A_i(\theta)\,\phi_{r-1}(\theta)^i\right) = v_r(P).$$

Pero, por los cálculos de $(r-1.\text{a})$, el miembro de la izquierda de la anterior igualdad coincide con $e_1 \cdots e_{r-1} v(P^S(\theta)) + v_r(P)$. Por consiguiente, si σ es el único $\mathbb{F}_{q_0}$-automorfismo de $\mathbb{F}_{q_r}$ que satisface $\sigma(\zeta_s) = \overline{\gamma_s(\theta)}$ para cada s

con $0 \leq s \leq r-1$ (cf. conclusiones de $(r-1.\text{b})$), obtenemos que

$$\begin{aligned} e_1 \cdots e_{r-1} v(P(\theta)) = v_r(P) &\iff v(P^S(\theta)) = 0 \\ &\iff P_S^\sigma\left(\overline{\gamma_{r-1}(\theta)}\right) \neq 0 \\ &\iff P_S(\zeta_{r-1}) \neq 0 \\ &\iff \omega_r(P) = 0\,, \end{aligned}$$

donde la segunda equivalencia se obtiene aplicando el corolario de 7.4 en orden $r-1$. Con esto ha quedado probada la proposición. □

7.2. Corolario.

(a) $e_1 \cdots e_{r-1} v(\phi_i(\theta)) = v_r(\phi_i)$ *para cada entero* i *con* $1 \leq i \leq r-1$.

(b) $e_1 \cdots e_{r-1} v(\phi_r(\theta)) > v_r(\phi_r)$.

DEMOSTRACIÓN. Se sigue inmediatamente de la proposición teniendo en cuenta que $\omega_r(\phi_i) = 0$ para $1 \leq i \leq r-1$ (cf. parte (a) de la proposición de 2.5), mientras que $\omega_r(\phi_r) = 1$ (cf. parte (b) del corolario de 3.3). □

Consideremos ahora el subanillo $\mathfrak{O}_r$ de $K(X)$ definido por

$$\mathfrak{O}_r := \{\frac{P(X)}{Q(X)} : P(X), Q(X) \in \mathcal{O}[X],\, Q(X) \neq 0,\, \omega_r(Q) = 0\} \subset K(X)\,;$$

es decir, $\mathfrak{O}_r$ es el anillo de fracciones de $\mathcal{O}[X]$ con respecto al subconjunto multiplicativamente cerrado

$$\{Q(X) : Q(X) \in \mathcal{O}[X] \setminus \{0\},\, \omega_r(Q) = 0\} \subset \mathcal{O}[X] \setminus \{0\}\,.$$

Notemos que, por las proposiciones de 2.3 y de 2.5, el anillo $\mathfrak{O}_r$ contiene al anillo $K[X]$ y a las fracciones racionales de la forma $\Phi(\mathbf{n})(X)$, $\mathbf{n} \in \mathbb{Z}^r$ (cf. §1). Además, para cada fracción racional $R(X) \in \mathfrak{O}_r$, tenemos bien definido el elemento $R(\theta) \in L$, ya que $Q(\theta) = 0$ implica que $\omega_r(Q) \geq 1$. En efecto, si $G(X) \in \mathcal{O}[X]$ es un polinomio no nulo, entonces se tiene $\omega_r(FG) = \omega_r(F) + \omega_r(G) \geq \omega_r(F) = a_{r-1} \geq 1$, por $(r-1.\text{b})$.

La proposición de 7.1 la podemos extender entonces a las fracciones racionales de $\mathfrak{O}_r$.

7.3. Corolario. *Con las notaciones anteriores, sea $R(X) \in \mathfrak{O}_r$ una fracción racional no nula. Entonces*

(a) $e_1 \cdots e_{r-1} v(R(\theta)) \geq v_r(R)$.

(b) $e_1 \cdots e_{r-1} v(R(\theta)) = v_r(R)$ *si y sólo si* $\omega_r(R) = 0$.

Luego, $e_1 \cdots e_{r-1} v(\Phi(\mathbf{n})(\theta)) = v_r(\Phi(\mathbf{n}))$ *para cada* $\mathbf{n} \in \mathbb{Z}^r$. □

Por este corolario, tenemos definido un homomorfismo de anillos

$$\begin{aligned} \mathfrak{O}_r \cap \mathcal{O}_{v_r} &\to \mathcal{O}_L \\ R(X) &\mapsto R(\theta) \end{aligned}$$

tal que la imagen del ideal $\mathfrak{m}_{v_r} \cap \mathfrak{O}_r$ está contenida en el ideal $\mathfrak{p}_L$. Consideramos el subanillo $\mathfrak{F}_r$ de k_{v_r} definido por

$$\mathfrak{F}_r := \{\overline{R(X)}^r : R(X) \in \mathfrak{O}_r \cap \mathcal{O}_{v_r}\} \subset k_{v_r}.$$

Observemos que $\mathbb{F}_{q_{r-1}}\left[\overline{\gamma_{r-1}(X)}^r\right] \subset \mathfrak{F}_r$, via la inmersión de $\mathbb{F}_{q_{r-1}}$ en k_{v_r} dada por la parte (a) del teorema de 2.7. En efecto, es claro que $\mathbb{F}_{q_0} \subset \mathfrak{F}_r$ y que para cada s, $0 \leq s \leq r-1$, la fracción racional $\gamma_s(X) \in \mathfrak{O}_r \cap \mathcal{O}_{v_r}$; luego, $\zeta_s = \overline{\gamma_s(X)}^r \in \mathfrak{F}_r$ para $0 \leq s \leq r-2$ y $\overline{\gamma_{r-1}(X)}^r \in \mathfrak{F}_r$.

El homomorfismo anterior nos induce entonces un homomorfismo de anillos

$$\begin{aligned} \mathfrak{F}_r &\to \mathbb{F}_L \\ \overline{R(X)}^r &\mapsto \overline{R(\theta)} \qquad (R(X) \in \mathfrak{O}_r \cap \mathcal{O}_{v_r}), \end{aligned}$$

cuya imagen contiene a $\mathbb{F}_{q_{r-1}}\left[\overline{\gamma_{r-1}(\theta)}\right] = \mathbb{F}_{q_r}$; además, la restricción de este homomorfismo a $\mathbb{F}_{q_{r-1}}$ es igual al único automorfismo $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_{r-1}}/\mathbb{F}_{q_0})$ que satisface $\sigma(\zeta_s) = \overline{\gamma_s(\theta)}$ para cada s, $0 \leq s \leq r-2$. De esta forma tenemos un diagrama conmutativo

$$\begin{array}{ccc} \mathfrak{F}_r & \longrightarrow & \mathbb{F}_L \\ \uparrow & & \uparrow \\ \mathbb{F}_{q_{r-1}} & \xrightarrow{\sigma} & \mathbb{F}_{q_{r-1}} \end{array}$$

donde las flechas verticales denotan las respectivas inclusiones.

Ahora, estamos en condiciones de probar el siguiente

7.4. Corolario. *Supongamos que* $F(X) \neq \phi_r(X)$. *Ponemos (cf. (b) de 7.2)*

$$e_1 \cdots e_{r-1} v(\phi_r(\theta)) - v_r(\phi_r) =: \frac{h}{e},$$

con $h, e \geq 1$ *enteros primos entre si, y* $\gamma_r(X) := \dfrac{\Phi_r(X)^e}{\pi_r(X)^h} \in K(X)$. *Entonces*

(a) $v(\Phi_r(\theta)) = \dfrac{h}{e_1 \cdots e_{r-1} e}$ *y* $v(\gamma_r(\theta)) = 0$.

(b) *Si* $P(X) \in \mathcal{O}[X]$ *es un polinomio no nulo y* S *es un segmento con pendiente* $-h/e$ *para el cual podemos definir el polinomio asociado (en orden* r*)* $P_S(Y)$, *entonces* $v(P^S(\theta)) \geq 0$ *y*

$$\overline{P^S(\theta)} = P_S^{\sigma}\left(\overline{\gamma_r(\theta)}\right) \text{ en } \mathbb{F}_L\,,$$

donde $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_r}/\mathbb{F}_{q_0})$ *es el único automorfismo tal que* $\sigma(\zeta_s) = \overline{\gamma_s(\theta)}$ *para cada* s, $0 \leq s \leq r-1$.

DEMOSTRACIÓN. Por los cálculos de $(r-1.\text{a})$ y la parte (c) del corolario de 3.3, tenemos que el valor $e_1 \cdots e_{r-1} v(\Pi_r(\theta)) = v_r(\Pi_r) = v_r(\phi_r)$ y que $v(\pi_r(\theta)) = \dfrac{1}{e_1 \cdots e_{r-1}}$. Así, $v(\Phi_r(\theta)) = v(\phi_r(\theta)) - v(\Pi_r(\theta)) = \dfrac{h}{e_1 \cdots e_{r-1} e}$ y $v(\gamma_r(\theta)) = e\, v(\Phi_r(\theta)) - h\, v(\pi_r(\theta)) = 0$; lo cual prueba la parte (a).

Por la proposición 4.6, tenemos que

$$P^S(\theta) = \sum_{i:(i,u_i)\in S} \Gamma_i(\theta)\, B_i(\theta)\, \gamma_r(\theta)^{(i-\alpha)/e}, \qquad (*)$$

cada $\Gamma_i(\theta) = \gamma_1(\theta)^{t_r(i,1)} \cdots \gamma_{r-1}(\theta)^{t_r(i,r-1)}$, y cada $B_i(X) \in \mathfrak{O}_r \cap \mathcal{O}_{v_r}$ y $\overline{B_i(X)}^{\tau} = (A_i)_{S(i)}\left(\overline{\gamma_{r-1}(X)}^{\tau}\right)$ en $\mathfrak{F}_r$. Aplicando el homomorfismo de anillos definido anteriormente, $\mathfrak{F}_r \to \mathbb{F}_L$, a los dos miembros de la anterior igualdad, obtenemos que $\overline{B_i(\theta)} = (A_i)^{\sigma}_{S(i)}\left(\overline{\gamma_{r-1}(\theta)}\right)$ en $\mathbb{F}_L$. Tomando ahora clases módulo $\mathfrak{p}_L$ en la igualdad de $(*)$ se obtiene la parte (b). □

Nótese que mientras el teorema de 2.8 hacía referencia a una igualdad en $\mathfrak{F}_r$ donde intervenían la fracción racional y el polinomio asociados en orden s, $1 \leq s \leq r-1$, la parte (b) del corolario anterior hace referencia a

una igualdad análoga en $\mathbb{F}_L$ en la que intervienen la fracción racional y el polinomio asociados en orden r.

7.5. Observación Tanto conceptualmente como a la hora de hacer demostraciones, siempre podemos suponer que los grados de los polinomios $\psi_0(Y), \psi_1(Y), \ldots, \psi_{r-1}(Y)$ del tipo $\mathbf{t}_{r-1}$ son todos iguales a 1; es decir, siempre podemos suponer que $f_0 = f_1 = \cdots = f_{r-1} = 1$. En efecto, sea $K' \subset \mathbb{Q}_p^{al}$ la extensión no ramificada de K de grado $f_0 \cdots f_{r-1}$. Por la parte (b) del corolario de 9.2 en orden $r-1$, sabemos que el entero $f_0 \cdots f_{r-1}$ divide al grado residual $f(L/K)$; luego, el cuerpo residual $\mathbb{F}_{K'} = \mathbb{F}_{q_r} \subseteq \mathbb{F}_L$ y $K' \subseteq L$. Entonces el polinomio $F(X)$ factoriza en $K'[X]$ de la forma

$$F(X) = \prod_{\tau \in \mathrm{Gal}(K'/K)} G^{\tau}(X), \qquad (*)$$

donde $G(X) := \mathrm{Irr}(\theta, K', X) \in \mathcal{O}_{K'}[X]$.

A continuación, veremos que el polinomio $G(X)$ tiene, sobre K', tipo de orden $r-1$ igual a $\{\mathbf{t}'_{r-1}\}$, donde $\mathbf{t}'_{r-1}$ es un tipo de orden $r-1$ definido sobre K' con los correspondientes grados $f'_0 = f'_1 = \cdots = f'_{r-1} = 1$. Después, se verán las relaciones que existen entre el polígono y el polinomio asociado (en orden r) de $F(X)$ sobre K y los de $G(X)$ sobre K'. Se aplicará el superíndice prima ($'$) a las notaciones que utilizamos sobre K, asociadas al tipo $\mathbf{t}_{r-1}$, para referirnos a las correspondientes notaciones sobre K', asociadas al tipo $\mathbf{t}'_{r-1}$.

Por inducción sobre i, $1 \leq i \leq r$, veamos que el polinomio $G(X)$ tiene, sobre K', tipo de orden $i-1$ igual a $\{\mathbf{t}'_{i-1}\}$, donde

$$\mathbf{t}'_{i-1} := (\psi'_0; h_1/e_1, \psi'_1; \ldots; h_{i-1}/e_{i-1}, \psi'_{i-1})$$

es un tipo que será construido y que satisface $\mathrm{gr}(\psi'_{j-1}) = 1$ y $\phi'_j(X)$ divide a $\phi_j(X)$ $(1 \leq j \leq i)$, y que para cada polinomio no nulo $P(X) \in \mathcal{O}[X]$ se satisfacen las propiedades siguientes

(i_a) $\mathbf{N}^0_{(v'_i,\phi'_i)}(P) = \mathbf{N}^0_{(v_i,\phi_i)}(P)$.

(i_b) Para cada segmento S del polígono $\mathbf{N}^0_{(v'_i,\phi'_i)}(P)$, con origen (α,β) y pendiente $-h/e$, su polinomio asociado (en orden i) es igual a $P'_S(Y) = \lambda_i P^g_S(\mu_i Y)$ en $\mathbb{F}_{q_i}[Y]$, para ciertos elementos $\lambda_i = \lambda_i(\alpha,\beta)$,

$\mu_i = \mu_i(h/e) \in \mathbb{F}_{q_i}^*$, donde $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_r}/\mathbb{F}_{q_0})$ es el único automorfismo tal que $\sigma(\zeta_s) = \overline{\gamma_s(\theta)}$ para cada s, $0 \le s \le r-1$.

Puesto que el polinomio $\psi_0(Y) = \mathrm{Irr}\,(\overline{\theta}, \mathbb{F}_{q_0}, Y)$ (cf. conclusiones de (0.b)), el elemento $\overline{\theta} \in \mathbb{F}_{q_1}$ y el polinomio $\overline{G}(Y) = (Y-\overline{\theta})^{a_0'}$ en $\mathbb{F}_{q_r}[Y]$, con $a_0' := \mathrm{gr}(G)$. Luego, hemos de tomar $\psi_0'(Y) := Y - \overline{\theta} \in \mathbb{F}_{q_1}[Y]$ y podemos elegir el polinomio mónico $\phi_1'(X) \in \mathcal{O}_{K'}[X]$ de forma que sea el factor de $\phi_1(X)$ que satisface $\overline{\phi_1'}(Y) = \psi_0'(Y)$ (lema de Hensel). Además, como la extensión K'/K es no ramificada, la valoración $v_{K'} = v$; por tanto, la valoración v_1' y la pseudo-valoración ω_1' de $K'(X)$ restringidas a $K(X)$ coinciden con v_1 y ω_1, respectivamente. Trabajando con el desarrollo ϕ_1-ádico de $P(X)$ y con el ϕ_1'-desarrollo admisible obtenido al substituir en él $\phi_1(X)$ por $(\phi_1(X)/\phi_1'(X)) \cdot \phi_1'(X)$, se ven entonces (1_a) y (1_b).

Consideremos ahora un entero i con $1 \le i \le r-1$. Supongamos construido el tipo $\mathbf{t}_{i-1}'$ y elegidos los polinomios $\phi_1'(X), \ldots, \phi_i'(X) \in \mathcal{O}_{K'}[X]$ de forma que $G(X)$ tenga (sobre K') tipo de orden $i-1$ igual a $\{\mathbf{t}_{i-1}'\}$, cada $\phi_j'(X)$ divida a $\phi_j(X)$ y v_i', ω_i' restringidas a $K(X)$ coincidan con v_i, ω_i, respectivamente; y supongamos que se satisfacen las propiedades (i_a) y (i_b). Por la parte (b) del corolario de 3.3 es $\omega_i'(\phi_i/\phi_i') = \omega_i(\phi_i) - \omega_i'(\phi_i') = 0$. Entonces por la parte (b) de la proposición de 7.1, aplicada al polinomio $\phi_i(X)/\phi_i'(X) \in \mathcal{O}_{K'}[X]$, y las conclusiones de $(i.a)$ obtenemos las igualdades

$$\begin{aligned} e_1 \cdots e_{i-1}\,(v(\phi_i(\theta)) - v(\phi_i'(\theta))) &= v_i(\phi_i) - v_i'(\phi_i') \\ &= e_1 \cdots e_{i-1} v(\phi_i(\theta)) - \frac{h_i}{e_i} - v_i'(\phi_i')\,, \end{aligned}$$

que muestran la relación

$$v(\phi_i'(\theta)) = \frac{1}{e_1 \cdots e_{i-1}} \left(v_i'(\phi_i') + \frac{h_i}{e_i} \right) ;$$

en particular, es $G(X) \neq \phi_i'(X)$. Por la proposición de 8.4 en orden i, se tiene entonces que el polígono $\mathrm{N}_{(v_i', \phi_i')}(G)$ consta de un solo lado T_i, con pendiente igual a $-h_i/e_i$. Luego, la valoración v_{i+1}' restringida a $K(X)$ coincide con v_{i+1} (por la propiedad (i_a)). Además, se tiene definida la fracción racional $\gamma_i'(X) \in K'(X)$ y, expresando $\gamma_i(X)$ en función de $\gamma_i'(X)$ y de las correspondientes fracciones racionales asociadas a los polinomios $\phi_j(X)/\phi_j'(X) \in \mathcal{O}_{K'}[X]$ $(1 \le j \le i)$ y aplicando el corolario de 7.4, tenemos

la igualdad

$$\overline{\gamma_i(\theta)} = \mu_i(h_i/e_i) \cdot \overline{\gamma_i'(\theta)}\,; \qquad (**)$$

en particular, $\overline{\gamma_i'(\theta)} \in \mathbb{F}_{q_{i+1}}^*$, pues $\overline{\gamma_i(\theta)} \in \mathbb{F}_{q_{i+1}}^*$ (por las conclusiones de $(i.\mathrm{b})$). Aplicando la proposición de 9.4 en orden i, obtenemos entonces que el polinomio asociado (en orden i) $G_{T_i}'(Y) = c_i' \left(Y - \overline{\gamma_i'(\theta)}\right)^{a_i'}$ en $\mathbb{F}_{q_r}[Y]$, para algún elemento $c_i' \in \mathbb{F}_{q_r}^*$ y para $a_i' := \mathrm{gr}(G)/(e_0 \cdots e_i)$. Por consiguiente, hemos de tomar $\psi_i'(Y) := Y - \overline{\gamma_i'(\theta)} \in \mathbb{F}_{q_{i+1}}[Y]$; de esta forma, la pseudo-valoración ω_{i+1}' restringida a $K(X)$ coincide con ω_{i+1} (por las propiedades (i_a) y (i_b), las conclusiones de $(i.\mathrm{b})$ y la igualdad de $(**)$) y el valor $\omega_{i+1}'(\phi_{i+1}) = \omega_{i+1}(\phi_{i+1}) = 1$. Podemos elegir el polinomio $\phi_{i+1}'(X) \in \mathcal{O}_{K'}[X]$ de forma que sea el factor de $\phi_{i+1}(X)$ correspondiente al tipo $\mathbf{t}_i' = (\mathbf{t}_{i-1}'; h_i'/e_i', \psi_i')$, dado por el teorema del polinomio asociado en orden i (cf. 9.1 y 9.2). Trabajando como antes (en el caso $i = 1$) y utilizando el teorema del producto (cf. 6.1) y la propiedad (i_b), se obtienen ahora las propiedades $(i+1_\mathrm{a})$ y $(i+1_\mathrm{b})$.

Finalmente, aplicando las propiedades (r_a) y (r_b) a nuestro polinomio $F(X)$ y el teorema del producto sobre K' a la factorización de $F(X)$ dada por la igualdad de $(*)$, y teniendo en cuenta que $\omega_r(F) = \omega_r'(G)$, se obtienen las relaciones

(a) $\mathbf{N}_{(v_r,\phi_r)}(F) = \mathbf{N}_{(v_r',\phi_r')}(G) + \{(0,\nu)\}$, donde $\nu := v_r(F) - v_r'(G)$.

(b) Para cada segmento $S = T + \{(0,\nu)\}$ del polígono $\mathbf{N}_{(v_r,\phi_r)}(F)$, es $F_S(Y) = \lambda \cdot (G_T')^\tau(\mu Y)$ en $\mathbb{F}_{q_r}[Y]$, para ciertos elementos $\lambda, \mu \in \mathbb{F}_{q_r}^*$, donde $\tau := \sigma^{-1} \in \mathrm{Gal}(\mathbb{F}_{q_r}/\mathbb{F}_{q_0})$.

Queda justificada entonces la afirmación del comienzo de esta observación.

§8. Teorema del polígono

En esta sección vamos a probar el teorema del polígono en orden r. Este teorema nos proporcionará una descomposición del factor $Q_{r-1}(X)$ de $P(X)$ correspondiente al tipo $\mathbf{t}_{r-1}$, dado por el teorema del polinomio asociado en orden $r-1$ (cf. 3.5 y 3.6 del capítulo 1 si $r = 2$, y 9.1 y 9.2 si $r > 2$), a partir de la descomposición en lados de su polígono de Newton $\mathbf{N}_r(Q_{r-1})$,

el cual coincide (salvo una traslación vertical) con el polígono $\mathrm{N}_r^0(P)$.

8.1. Teorema. (Teorema del polígono) *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico tal que el polígono $\mathrm{N}_r^0(P)$ no se reduce a un solo punto; es decir, tal que $v_{\phi_r}(P) < \omega_r(P)$. Sean $S_{r,1}, \ldots, S_{r,g}$ los lados de $\mathrm{N}_r^0(P)$ y sean $d_{r,i}$, $e_{r,i}$, $h_{r,i}$ los datos asociados a $S_{r,i}$ $(1 \leq i \leq g)$. Entonces el factor $Q_{r-1}(X)$ de $P(X)$ correspondiente al tipo t_{r-1}, dado por el teorema del polinomio asociado en orden $r-1$ (cf. 9.1 y 9.2), admite una factorización de la forma*

$$Q_{r-1}(X) = \phi_r(X)^{v_{\phi_r}(P)} \cdot P_{r,1}(X) \cdots P_{r,g}(X)\,,$$

donde cada $P_{r,i}(X) \in \mathcal{O}[X]$ es un polinomio mónico, no divisible por $\phi_r(X)$, de grado $m_r e_{r,i} d_{r,i}$, con tipo de orden $r-1$ igual a $\{\mathrm{t}_{r-1}\}$, cuyo polígono $\mathrm{N}_r(P_{r,i})$ consta de un solo lado $S'_{r,i}$, con datos $d_{r,i}$, $e_{r,i}$, $h_{r,i}$, y cuyo polinomio asociado (en orden r) a este lado es $(P_{r,i})_{S'_{r,i}}(Y) = c_i P_{S_{r,i}}(Y)$, para algún elemento $c_i \in \mathbb{F}_{q_r}^*$. Además, para todo i, $1 \leq i \leq g$, si $\theta \in \mathbb{Q}_p^{al}$ es una raíz de $P_{r,i}(X)$, tenemos que el valor

$$v(\phi_r(\theta)) = \frac{1}{e_1 \cdots e_{r-1}} \left(v_r(\phi_r) + \frac{h_{r,i}}{e_{r,i}} \right).$$

8.2. Definición. *Al polinomio $P_{r,i}(X)$ le llamaremos el factor de $P(X)$ correspondiente al tipo reducido de orden r*

$$\mathrm{t}_{r,i}^{\circ} := (\psi_0; h_1/e_1, \psi_1; \ldots; h_{r-1}/e_{r-1}, \psi_{r-1}; h_{r,i}/e_{r,i}).$$

8.3. Corolario. *Con las mismas hipótesis y notaciones que en el teorema anterior. Para cada i, $1 \leq i \leq g$, se tiene*

(a) *El número de factores mónicos e irreducibles del polinomio $P_{r,i}(X)$ en $K[X]$ es menor o igual que $d_{r,i}$. Cada uno de estos factores tiene grado múltiplo de $m_r e_{r,i}$ y tipo reducido de orden r igual a $\{\mathrm{t}_{r,i}^{\circ}\}$.*

(b) *Sea $\theta \in \mathbb{Q}_p^{al}$ una raíz de $P_{r,i}(X)$ y ponemos $L := K(\theta)$. Entonces el entero $e_0 \cdots e_{r-1} e_{r,i}$ divide al índice de ramificación $e(L/K)$ de la extensión L/K. Además, si $d_{r,i} = 1$, entonces el polinomio $P_{r,i}(X)$ es irreducible en $K[X]$, $e(L/K) = e_0 \cdots e_{r-1} e_{r,i}$ y $f(L/K) = f_0 \cdots f_{r-1}$.*

DEMOSTRACIÓN. Las afirmaciones de la parte (a) son consecuencia directa de la parte (b) del corolario de 1.3 y del teorema del producto (cf. 6.1).

Probemos ahora las afirmaciones de la parte (b). Sabemos, por inducción, que el entero $e_0 \cdots e_{r-1}$ divide a $e(L/K)$ y, por el corolario de 9.3 en orden $r-1$, que el entero $f_0 \cdots f_{r-1}$ divide al grado residual $f(L/K)$. Además, por el teorema de 8.1, el grado $\mathrm{gr}(P_{r,i}) = m_r e_{r,i} d_{r,i}$ y la fracción

$$\frac{v_L(\phi_r(\theta))}{e(L/K)/(e_0 \cdots e_{r-1})} = e_0 \cdots e_{r-1} v(\phi_r(\theta)) = \frac{e_{r,i} v_r(\phi_r) + h_{r,i}}{e_{r,i}}.$$

Por consiguiente, como el $\mathrm{mcd}(e_{r,i} v_r(\phi_r) + h_{r,i}, e_{r,i}) = \mathrm{mcd}(h_{r,i}, e_{r,i}) = 1$, entonces $e_{r,i}$ divide a $e(L/K)/(e_0 \cdots e_{r-1})$ y tenemos

$$\left(\frac{e(L/K)}{e_0 \cdots e_{r-1} e_{r,i}}\right)\left(\frac{f(L/K)}{f_0 \cdots f_{r-1}}\right) = \frac{\mathrm{gr}(\mathrm{Irr}(\theta, K))}{m_r e_{r,i}} \leq \frac{\mathrm{gr}(P_{r,i})}{m_r e_{r,i}} = d_{r,i}.$$

Supongamos ahora que $d_{r,i} = 1$. Por lo anterior obtenemos que $P_{r,i}(X)$ es irreducible en $K[X]$, $e(L/K) = e_0 \cdots e_{r-1} e_{r,i}$ y $f(L/K) = f_0 \cdots f_{r-1}$. □

En el caso $d_{r,i} = 1$, con la parte (b) del corolario anterior podemos calcular, a partir del tipo reducido $\mathbf{t}^o_{r,i}$, el índice de ramificación y el grado residual correspondientes a la extensión L/K definida por el polinomio irreducible $P_{r,i}(X)$. Más adelante, veremos que también podemos hallar en este caso, a partir del tipo reducido $\mathbf{t}^o_{r,i}$, una base del $\mathcal{O}$-módulo libre $\mathcal{O}_L$ y un generador del ideal primo $\mathfrak{p}_L$ (cf. 11.12).

A continuación, probaremos el teorema de 8.1 en el caso particular de un polinomio irreducible de $\mathcal{O}[X]$.

8.4. Proposición. *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico, irreducible, con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ y distinto de $\phi_r(X)$. Entonces el polígono $\mathbf{N}_r(P)$ consta de un solo lado, cuya pendiente es negativa. Además, si $\theta \in \mathbb{Q}_p^{al}$ es una raíz de $P(X)$, entonces*

$$v(\phi_r(\theta)) = \frac{1}{e_1 \cdots e_{r-1}}\left(v_r(\phi_r) + \frac{h_r}{e_r}\right) = \sum_{i=1}^{r} \frac{e_i f_i \cdots e_r f_r}{e_r f_r} \cdot \frac{h_i}{e_1 \cdots e_i},$$

donde $-h_r/e_r$ es la pendiente de este lado.

DEMOSTRACIÓN. En primer lugar, observemos que los polígonos $\mathbf{N}_r(P)$ y $\mathbf{N}^0_r(P)$ coinciden y no se reducen a un solo punto. En efecto, por las

hipótesis sobre el polinomio $P(X)$, se tiene que $v_{\phi_r}(P) = 0 < \omega_r(P)$ y, por la proposición de 1.2, que $\mathrm{gr}(P) = m_r\omega_r(P)$; lo cual prueba lo que queríamos aplicando el lema de 4.2.

Observemos también que $e_1 \cdots e_{r-1} v(\phi_r(\theta)) > v_r(\phi_r)$, por la parte (b) del corolario de 7.2; en particular, $v(\phi_r(\theta)) > 0$.

Consideremos entonces el polinomio irreducible de $\phi_r(\theta)$ sobre K,

$$Q(X) := \mathrm{Irr}(\phi_r(\theta), K, X) = \sum_{i=0}^{m} b_i X^i \in \mathcal{O}[X], \quad b_m = 1, \quad b_0 \neq 0.$$

Por el teorema del polígono en primer orden (cf. 3.1 del capítulo 1), el polígono $\mathrm{N}_{(v_1,X)}(Q)$ consta de un solo lado, cuya pendiente es igual a $-v(b_0)/m = -v(\phi_r(\theta))$. Por tanto, el valor $v(b_i) \geq (m-i)v(\phi_r(\theta))$ para cada entero i, $0 \leq i \leq m$.

Consideremos ahora el polinomio mónico

$$Q_1(X) := Q(\phi_r(X)) = \sum_{i=0}^{m} b_i\, \phi_r(X)^i \in \mathcal{O}[X].$$

Observemos que para todo i se tiene

$$\begin{aligned} v_r(b_i {\phi_r}^i) &= v_r(b_i) + i\, v_r(\phi_r) \\ &= e_1 \cdots e_{r-1} v(b_i) + i\, v_r(\phi_r) \\ &\geq e_1 \cdots e_{r-1}(m-i) v(\phi_r(\theta)) + i\, v_r(\phi_r) \\ &= v_r({\phi_r}^m) + (m-i)(e_1 \cdots e_{r-1} v(\phi_r(\theta)) - v_r(\phi_r)), \end{aligned}$$

y que la anterior desigualdad es una igualdad si $i = 0$ o si $i = m$. Por tanto, el polígono $\mathrm{N}_r(Q_1)$ consta de un solo lado, cuya pendiente es igual a

$$-(e_1 \cdots e_{r-1} v(\phi_r(\theta)) - v_r(\phi_r)) < 0.$$

Por otra parte, como $Q_1(\theta) = 0$, el polinomio $P(X)$ ha de dividir al polinomio $Q_1(X)$ en $\mathcal{O}[X]$ y entonces, por el teorema del producto (cf. 6.1), el polígono $\mathrm{N}_r(P) = \mathrm{N}_r^0(P)$ ha de constar también de un sólo lado, con la misma pendiente.

Por último, aplicando la fórmula explícita que calcula el valor $v_r(\phi_r)$ (cf. parte (c) del corolario de 3.3), obtenemos la última igualdad de la proposición. □

Pasemos ahora a demostrar el teorema de 8.1 en general; es decir, para cualquier polinomio de $\mathcal{O}[X]$ (no necesariamente irreducible).

DEMOSTRACIÓN (del teorema de 8.1). Por el teorema del polinomio asociado en orden $r-1$ (cf. 9.1), sabemos que nuestro polinomio $P(X)$ factoriza en la forma

$$P(X) = Q_{r-1}(X)\, R(X)\,,$$

donde $Q_{r-1}(X) \in \mathcal{O}[X]$ es un polinomio mónico, de grado $m_r\omega_r(P) = m_r\omega_r(Q_{r-1})$ y con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$, y donde $R(X) \in \mathcal{O}[X]$. Luego, $\omega_r(R) = 0$, el polígono $\mathbf{N}_r^0(R) = \{(0, v_r(R))\} =: T$, el polinomio asociado (en orden r) $R_T(Y) = c \in \mathbb{F}_{q_r}^*$ y el polígono $\mathbf{N}_r(Q_{r-1}) = \mathbf{N}_r^0(Q_{r-1})$, por el lema de 4.2. Por el teorema del producto (cf. 6.1), obtenemos entonces las igualdades

$$\begin{aligned} \mathbf{N}_r^0(P) &= \mathbf{N}_r(Q_{r-1}) + \{(0, v_r(R))\}\,, \\ P_{S_{r,i}}(Y) &= c \cdot (Q_{r-1})_{T_i}(Y)\,, \quad 1 \le i \le g\,, \end{aligned}$$

donde $(Q_{r-1})_{T_i}(Y)$ es el polinomio asociado (en orden r) al lado, T_i, con pendiente $-h_{r,i}/e_{r,i}$ del polígono $\mathbf{N}_r(Q_{r-1})$.

Consideremos ahora un polinomio $Q(X) \in \mathcal{O}[X]$ mónico, irreducible, que divida a $Q_{r-1}(X)$ y distinto de $\phi_r(X)$. Por la parte (b) del corolario de 1.3, el polinomio $Q(X)$ ha de tener tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$. Por la proposición de 8.4, el polígono $\mathbf{N}_r(Q)$ ha de constar de un solo lado y para cada raíz θ de $Q(X)$ ha de ser $e_1 \cdots e_{r-1} v(\phi_r(\theta)) = v_r(\phi_r) + h/e$, donde $-h/e$ es la pendiente de este lado. Además, esta pendiente $-h/e$ ha de ser igual a $-h_{r,i}/e_{r,i}$ para algún único i, de nuevo por el teorema del producto.

Finalmente, para cada i definimos el polinomio

$$P_{r,i}(X) := \prod_{Q(X) \in C_i} Q(X)^{v_Q(Q_{r-1})} \in \mathcal{O}[X]\,,$$

donde C_i denota el conjunto formado por todos los polinomios $Q(X) \in \mathcal{O}[X]$ mónicos, irreducibles, que dividen a $Q_{r-1}(X)$, distintos de $\phi_r(X)$ y tales que la pendiente del único lado del polígono $\mathbf{N}_r(Q)$ es igual a $-h_{r,i}/e_{r,i}$. Por lo anterior se tiene que

$$Q_{r-1}(X) = \phi_r(X)^{v_{\phi_r}(P)} \cdot P_{r,1}(X) \cdots P_{r,g}(X)\,,$$

y que cada polinomio $P_{r,i}(X)$ satisface las propiedades del teorema, por la parte (a) del corolario de 1.3 y, otra vez, por el teorema del producto. □

§9. Teorema del polinomio asociado

Veremos ahora el teorema del polinomio asociado en orden r, que nos facilitará una ulterior descomposición del factor $P_{r,i}(X)$ de $P(X)$ correspondiente al tipo reducido $\mathbf{t}^o_{r,i}$ (cf. 8.1 y 8.2) a partir de la descomposición en $\mathbb{F}_{q_r}[Y]$ de su polinomio asociado (en orden r) $(P_{r,i})_{S'_{r,i}}(Y) = c_i P_{S_{r,i}}(Y)$.

9.1. Teorema. (Teorema del polinomio asociado) *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico tal que el polígono $\mathbf{N}^0_r(P)$ no se reduce a un solo punto; es decir, tal que $v_{\phi_r}(P) < \omega_r(P)$. Sea S_r un lado de $\mathbf{N}^0_r(P)$ y sean d_r, e_r, h_r sus datos. Sea*

$$P_{S_r}(Y) = c\,\psi_{r,1}(Y)^{a_{r,1}} \cdots \psi_{r,g}(Y)^{a_{r,g}}\,, \quad c \in \mathbb{F}^*_{q_r}\,,$$

la factorización del polinomio asociado (en orden r) $P_{S_r}(Y)$ en producto de potencias de distintos polinomios mónicos irreducibles de $\mathbb{F}_{q_r}[Y]$ con grado $f_{r,i} := \mathrm{gr}(\psi_{r,i})$. Entonces el factor $P_r(X)$ de $P(X)$ correspondiente al tipo reducido de orden r

$$\mathbf{t}^o_r := (\psi_0; h_1/e_1, \psi_1; \ldots; h_{r-1}/e_{r-1}, \psi_{r-1}; h_r/e_r)\,,$$

dado por el teorema del polígono (cf. 8.1 y 8.2), admite una factorización de la forma

$$P_r(X) = Q_{r,1}(X) \cdots Q_{r,g}(X),$$

donde cada $Q_{r,i}(X) \in \mathcal{O}[X]$ es un polinomio mónico, de grado $m_r e_r f_{r,i} a_{r,i}$, con tipo reducido de orden r igual a $\{\mathbf{t}^o_r\}$, cuyo polígono $\mathbf{N}_r(Q_{r,i})$ consta de un solo lado $T_{r,i}$, con datos $f_{r,i}a_{r,i}$, e_r, h_r, y cuyo polinomio asociado (en orden r) a este lado es $(Q_{r,i})_{T_{r,i}}(Y) = c_i \psi_{r,i}(Y)^{a_{r,i}}$, para algún elemento $c_i \in \mathbb{F}^*_{q_r}$. Además, para todo i, $1 \le i \le g$, si $\theta \in \mathbb{Q}^{al}_p$ es una raíz de $Q_{r,i}(X)$ y ponemos $\gamma_r(X) := \dfrac{\Phi_r(X)^{e_r}}{\pi_r(X)^{h_r}} \in K(X)$, tenemos que el valor $v(\gamma_r(\theta)) = 0$ y que $\psi^\sigma_{r,i}(Y) = \mathrm{Irr}\left(\overline{\gamma_r(\theta)}, \mathbb{F}_{q_r}, Y\right)$, donde $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_r}/\mathbb{F}_{q_0})$ es el único automorfismo tal que $\sigma(\zeta_s) = \overline{\gamma_s(\theta)}$ para $0 \le s \le r-1$ (cf. §7).

9.2. Definición. *Al polinomio $Q_{r,i}(X)$ le llamaremos el factor de $P(X)$ correspondiente al tipo de orden r*

$$\mathbf{t}_{r,i} := (\psi_0; h_1/e_1, \psi_1; \ldots; h_{r-1}/e_{r-1}, \psi_{r-1}; h_r/e_r, \psi_{r,i}).$$

9.3. Corolario. *Con las mismas hipótesis y notaciones que en el teorema anterior. Para cada i, $1 \leq i \leq g$, se tiene*

(a) *El número de factores mónicos e irreducibles del polinomio $Q_{r,i}(X)$ en $K[X]$ es menor o igual que $a_{r,i}$. Cada uno de estos factores tiene grado múltiplo de $m_r e_r f_{r,i}$ y tipo de orden r igual a $\{\mathbf{t}_{r,i}\}$.*

(b) *Sea $\theta \in \mathbb{Q}_p^{al}$ una raíz de $Q_{r,i}(X)$ y ponemos $L := K(\theta)$. Entonces el entero $f_0 \cdots f_{r-1} f_{r,i}$ divide al grado residual $f(L/K)$ de la extensión L/K. Además, si $a_{r,i} = 1$, entonces el polinomio $Q_{r,i}(X)$ es irreducible en $K[X]$, $e(L/K) = e_0 \cdots e_r$ y $f(L/K) = f_0 \cdots f_{r-1} f_{r,i}$.*

DEMOSTRACIÓN. La parte (a) se sigue de la parte (b) del corolario de 1.3 y del teorema del producto (cf. 6.1).

Pasemos a ver la parte (b). Por el corolario de 8.3, sabemos que el entero $e_0 \cdots e_r$ divide al índice de ramificación $e(L/K)$. Por inducción, el entero $f_0 \cdots f_{r-1}$ divide a $f(L/K)$; o equivalentemente, el cuerpo $\mathbb{F}_{q_r} \subseteq \mathbb{F}_L$. Entonces, por el teorema de 9.1, obtenemos que el cuerpo $\mathbb{F}_{q_r}\left(\overline{\gamma_r(\theta)}\right) \subseteq \mathbb{F}_L$ y que el grado $\left[\mathbb{F}_{q_r}\left(\overline{\gamma_r(\theta)}\right) : \mathbb{F}_{q_r}\right] = f_{r,i}$. Por consiguiente, se tiene que $f_{r,i}$ divide a $f(L/K)/(f_0 \cdots f_{r-1})$ y que

$$\left(\frac{e(L/K)}{e_0 \cdots e_r}\right)\left(\frac{f(L/K)}{f_0 \cdots f_{r-1} f_{r,i}}\right) = \frac{\mathrm{gr}(\mathrm{Irr}(\theta, K))}{m_r e_r f_{r,i}} \leq \frac{\mathrm{gr}(Q_{r,i})}{m_r e_r f_{r,i}} = a_{r,i}.$$

Ahora, supongamos que $a_{r,i} = 1$. Es claro por lo anterior que entonces el polinomio $Q_{r,i}(X)$ ha de ser irreducible en $K[X]$, $e(L/K) = e_0 \cdots e_r$ y $f(L/K) = f_0 \cdots f_{r-1} f_{r,i}$. □

En la parte (b) del corolario anterior hemos visto que en el caso $a_{r,i} = 1$ podemos calcular, a partir del tipo $\mathbf{t}_{r,i}$, el índice de ramificación y el grado residual de la extensión L/K definida por el polinomio irreducible $Q_{r,i}(X)$. En la §11, veremos que en este caso ($a_{r,i} = 1$) también podemos

hallar, a partir del tipo $\mathbf{t}_{r,i}$, una base del $\mathcal{O}$-módulo libre $\mathcal{O}_L$ y un generador del ideal primo $\mathfrak{p}_L$ (cf. 11.12).

Pasemos a probar el teorema de 9.1 en el caso particular de un polinomio irreducible de $\mathcal{O}[X]$.

9.4. Proposición. *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico, irreducible, con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ y distinto de $\phi_r(X)$. Sean S_r el único lado del polígono $\mathbf{N}_r(P)$ (cf. 8.4), d_r, e_r, h_r sus datos y $P_{S_r}(Y) \in \mathbb{F}_{q_r}[Y]$ su polinomio asociado (en orden r), y ponemos $\gamma_r(X) := \dfrac{\Phi_r(X)^{e_r}}{\pi_r(X)^{h_r}} \in K(X)$. Por último, sean $\theta \in \mathbb{Q}_p^{al}$ una raíz de $P(X)$ y $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_r}/\mathbb{F}_{q_0})$ el único automorfismo tal que $\sigma(\zeta_s) = \overline{\gamma_s(\theta)}$ para $0 \le s \le r-1$. Entonces tenemos*

(a) $v(\gamma_r(\theta)) = 0$ *y* $P^{\sigma}_{S_r}\left(\overline{\gamma_r(\theta)}\right) = 0$.

(b) $P_{S_r}(Y) = c\psi_r(Y)^{a_r}$ *en* $\mathbb{F}_{q_r}[Y]$, *para algún elemento* $c \in \mathbb{F}_{q_r}^*$ *y para algún entero* $a_r \ge 1$, *donde* $\psi_r^{\sigma}(Y) = \mathrm{Irr}\left(\overline{\gamma_r(\theta)}, \mathbb{F}_{q_r}, Y\right)$.

DEMOSTRACIÓN. Como $e_1 \cdots e_{r-1} v(\phi_r(\theta)) = v_r(\phi_r) + h_r/e_r$ (cf. proposición de 8.4), entonces el valor $v(\gamma_r(\theta)) = 0$ y $P^{\sigma}_{S_r}\left(\overline{\gamma_r(\theta)}\right) = \overline{P^{S_r}(\theta)}$, por el corolario de 7.4. Veamos que $v(P^{S_r}(\theta)) > 0$, lo cual probará la parte (a). Sea $P(X) = \sum A_i(X)\,\phi_r(X)^i$ el desarrollo ϕ_r-ádico de $P(X)$ y sea $(0, \beta_r)$ el origen del lado S_r. Por la proposición de 7.1, se tiene entonces que

$$e_1 \cdots e_{r-1} v(A_i(\theta)\,\phi_r(\theta)^i) = v_r(A_i\,{\phi_r}^i) + i\,\frac{h_r}{e_r} > \beta_r$$

para cada i tal que $(i, v_r(A_i\,{\phi_r}^i)) \notin S_r$. Por tanto, tenemos que

$$P(X) = \pi_r(X)^{\beta_r} P^{S_r}(X) + R(X)\,,$$

donde $R(X) \in \mathcal{O}[X]$ y $e_1 \cdots e_{r-1} v(R(\theta)) > \beta_r$. Substituyendo ahora la indeterminada X por θ en la anterior igualdad y teniendo en cuenta que $e_1 \cdots e_{r-1} v(\pi_r(\theta)) = 1$ (cf. cálculos de $(r-1.\mathrm{a})$ en la §7), obtenemos que el valor $v(P^{S_r}(\theta)) > 0$.

Pasemos a demostrar la parte (b). Por la observación de 7.5, podemos suponer que los grados $f_0 = \cdots = f_{r-1} = 1$; así, $q_r = q_0$. Consideremos el polinomio irreducible de $\gamma_r(\theta)$ sobre K

$$Q(X) := \mathrm{Irr}(\gamma_r(\theta), K, X) = \sum_{j=0}^{m} b_j X^j \in \mathcal{O}[X]\,, \quad b_m = 1\,.$$

Entonces $v(b_0) = m\,v(\gamma_r(\theta)) = 0$ y $\overline{Q}(Y) = \psi_r(Y)^b$ en $\mathbb{F}_{q_0}[Y]$, para algún entero $b \geq 1$. Ponemos $n'_s := e_s f_s \cdots e_r f_r h_s/(e_s f_r) \in \mathbb{Z}$, para $1 \leq s \leq r$. Por el lema de 2.10, existen r enteros $n_1, \ldots, n_r$ tales que para todo j, $0 \leq j \leq m$, la fracción racional $\prod_{s=1}^{r} \pi_s(X)^{n_s - j\,n'_s} \in \mathcal{O}[X]$. Consideremos ahora el polinomio

$$Q_1(X) := \left(\prod_{s=1}^{r} \pi_s(X)^{n_s}\right) Q(\gamma_r(X)) = \sum_{j=0}^{m} B_{j\,e_r}(X)\,\phi_r(X)^{j\,e_r},$$

donde cada $B_{j\,e_r}(X) := b_j \cdot \prod_{s=1}^{r} \pi_s(X)^{n_s - j\,n'_s} \in \mathcal{O}[X]$ (no necesariamente de grado menor que m_r).

En primer lugar, veamos que el polígono $\mathbf{N}_r(Q_1, \{B_i\})$ consta de un solo lado T, cuya pendiente es igual a $-h_r/e_r$ y cuyo origen es el punto $(0, \beta)$, donde $\beta := \sum_{s=1}^{r} n_s v_r(\pi_s)$. En efecto, para todo j tenemos que el valor

$$\begin{aligned} v_r(B_{j\,e_r}\phi_r{}^{j\,e_r}) &= v_r(b_j) + \sum_{s=1}^{r}(n_s - j\,n'_s)v_r(\pi_s) + j\,e_r v_r(\phi_r) \\ &\geq \sum_{s=1}^{r}(n_s - j\,n'_s)v_r(\pi_s) + j\,e_r v_r(\phi_r) \\ &= \beta - j\,h_r\,, \end{aligned}$$

donde la última igualdad se obtiene aplicando la parte (b) de la proposición de 2.5 y la parte (c) del corolario de 3.3; además, la anterior desigualdad es una igualdad si $j = 0$ o si $j = m$.

En segundo lugar, veamos que el polinomio asociado (en orden r) $(Q_1, \{B_i\})_T(Y) = c\,\overline{Q}(Y)$ en $\mathbb{F}_{q_0}[Y]$, para algún elemento $c \in \mathbb{F}_{q_0}^*$. Recordemos que el polinomio

$$(Q_1, \{B_i\})_T(Y) := \sum_{j=0}^{m} \zeta_1{}^{t_r(j\,e_r,1)} \cdots \zeta_{r-1}{}^{t_r(j\,e_r,r-1)} (B_{j\,e_r})_{T(j\,e_r)}(\zeta_{r-1})\,Y^j$$

donde el segmento $T(j\,e_r)$ y los enteros $t_r(j\,e_r, s)$ $(1 \leq s \leq r-1)$ están definidos como siempre (cf. §4). Consideremos un entero j con $0 \leq j \leq m$,

ponemos $i := j\,e_r$ y denotemos por $(\alpha(i), \beta(i))$ el origen del segmento $T(i)$. Por la proposición de 4.6, se tiene que la fracción racional

$$\Gamma_i(X) := \frac{\Phi_{r-1}(X)^{\alpha(i)}\pi_{r-1}(X)^{\beta(i)}\Pi_r(X)^i}{\pi_r(X)^{\beta - j\,h_r}} = \gamma_1(X)^{t_r(i,1)}\cdots\gamma_{r-1}(X)^{t_r(i,r-1)}$$

y que la fracción racional

$$C_i(X) := \frac{B_i(X)}{\Phi_{r-1}(X)^{\alpha(i)}\pi_{r-1}(X)^{\beta(i)}} \in K(X)$$

satisface la igualdad

$$\overline{C_i(X)}^r = (B_i)_{T(i)}(Z)\,, \quad Z := \overline{\gamma_{r-1}(X)}^r \in k_{v_r}\,.$$

Por las definiciones dadas, tenemos que el producto

$$\Gamma_i(X)\,C_i(X) = \rho(X)\,b_j\,, \qquad (*)$$

donde $\rho(X) := \pi_r(X)^{-\beta}\prod_{s=1}^{r}\pi_s(X)^{n_s} \in K(X)$ es independiente de j. Además, como el valor $v_r(\rho) = 0$, podemos escribir

$$\rho(X) = \gamma_1(X)^{t_1}\cdots\gamma_{r-1}(X)^{t_{r-1}}\,,$$

para ciertos enteros $t_1, \ldots, t_{r-1}$ (cf. lema de 2.9). Tomando clases módulo $\mathfrak{m}_{v_r}$ en la igualdad de $(*)$, obtenemos entonces la igualdad

$$\zeta_1{}^{t_r(i,1)}\cdots\zeta_{r-2}{}^{t_r(i,r-2)}Z^{t_r(i,r-1)}(B_i)_{T(i)}(Z) = \zeta_1{}^{t_1}\cdots\zeta_{r-2}{}^{t_{r-2}}Z^{t_{r-1}}\,\overline{b_j}\,,$$

via la inmersión de $\mathbb{F}_{q_{r-1}}$ en k_{v_r} dada en la parte (a) del teorema de 2.7. Substituyendo en esta última igualdad el elemento Z, transcendente sobre $\mathbb{F}_{q_{r-1}}$ (cf. parte (b) del teorema de 2.7), por el elemento ζ_{r-1}, obtenemos que el coeficiente j-ésimo de $(Q_1, \{B_\nu\})_T(Y)$ es

$$\zeta_1{}^{t_r(i,1)}\cdots\zeta_{r-1}{}^{t_r(i,r-1)}(B_i)_{T(i)}(\zeta_{r-1}) = c\,\overline{b_j}\,,$$

para $c := \zeta_1{}^{t_1}\cdots\zeta_{r-1}{}^{t_{r-1}} \in \mathbb{F}_{q_0}^*$ independiente de j; lo cual prueba lo que queríamos ver.

Observemos ahora que el anterior ϕ_r-desarrollo de $Q_1(X)$ es admisible. En efecto, si el polinomio $B_{j\,e_r}(X)$ es no nulo, entonces $\omega_r(B_{j\,e_r}) = 0$, puesto que $\omega_r(K^*) = (0)$ y que $\omega_r(\phi_1) = \cdots = \omega_r(\phi_{r-1}) = 0$.

Finalmente, como $Q_1(\theta) = 0$, entonces $P(X)$ divide a $Q_1(X)$ en $\mathcal{O}[X]$, y, por el corolario de 6.2, el polinomio asociado $P_{S_r}(Y)$ dividirá al polinomio asociado $(Q_1)_T(Y) = (Q_1, \{B_i\})_T(Y) = c\overline{Q}(Y) = c\psi_r(Y)^b$ en $\mathbb{F}_{q_0}[Y]$. Con esto queda probada la parte (b). □

El siguiente corolario, válido también cuando $r = 1$ (cf. observación (5) de 3.8 en el capítulo 1), nos dice como podemos obtener explícitamente todas las raíces del polinomio asociado (en orden r) $P_{S_r}(Y)$ a partir de las raíces del polinomio irreducible $P(X)$.

9.5. Corolario. *Con las notaciones e hipótesis de la proposición anterior, se tiene la igualdad*

$$P_{S_r}(Y)^{e_0\cdots e_r} = c \prod_{\theta\in Z_r(P)} \left(Y - \overline{\gamma_r(\theta)}\right),$$

para algún elemento $c \in \mathbb{F}_{q_r}^*$, *donde*

$$Z_r(P) := \{\theta \in \mathbb{Q}_p^{al} : P(\theta) = 0,\ \overline{\gamma_s(\theta)} = \zeta_s \text{ para } 0 \le s \le r-1\}.$$

DEMOSTRACIÓN. Haciendo uso de este mismo corolario en orden $r-1$, de la propiedad $(r-1.b)$ (cf. definición de 1.1) que por hipótesis satisface $P(X)$ y de la proposición de 1.2, obtenemos que el cardinal

$$t := \#Z_r(P) = e_0\cdots e_{r-1}a_{r-1} = \mathrm{gr}(P)/(f_0\cdots f_{r-1}).$$

Fijemos un elemento $\theta \in Z_r(P)$ (siempre existe al menos uno). Ponemos $L := K(\theta)$, $\psi_r(Y) := \mathrm{Irr}\left(\overline{\gamma_r(\theta)}, \mathbb{F}_{q_r}, Y\right)$ y $f_r := \mathrm{gr}(\psi_r)$. Entonces, por la proposición de 9.4, sabemos que el polinomio $P_{S_r}(Y) = c\psi_r(Y)^{a_r}$ para algún elemento $c \in \mathbb{F}_{q_r}^*$ y para algún entero $a_r \ge 1$; además, por el lema de 4.2, es $a_{r-1} = \omega_r(P) = e_r d_r = e_r f_r a_r$. Sea K_r la extensión no ramificada de K de grado $f_0\cdots f_{r-1}$; así, el cuerpo $K_r \subseteq L$, el grado $[L : K_r] = t$ y el cuerpo residual $\mathbb{F}_{K_r} = \mathbb{F}_{q_r}$. Para cada entero s, $0 \le s \le r$, ponemos ahora $F_s(X) := \mathrm{Irr}(\gamma_s(\theta), K_r, X) \in \mathcal{O}_{K_r}[X]$, $n_s := \mathrm{gr}(F_s)$ y $n'_s := [L : K_r(\gamma_s(\theta))]$. Entonces $\overline{F_s}(Y) = (Y - \zeta_s)^{n_s}$ para $0 \le s \le r-1$ (ya que $\overline{\gamma_s(\theta)} = \zeta_s \in \mathbb{F}_{q_r}$), y $\overline{F_r}(Y) = \psi_r(Y)^{n_r/f_r}$.

Veamos a continuación la igualdad entre los conjuntos

$$Z_r(P) = \{\sigma_1(\theta), ..., \sigma_t(\theta)\} =: C,$$

donde $\sigma_1, ..., \sigma_t$ son las t K_r-inmersiones de L en $\mathbb{Q}_p^{al}$. Como los elementos de C son exactamente los conjugados de θ sobre K_r, entonces el cardinal $\#C = t = \#Z_r(P)$. Por tanto, nos bastará con probar que $\sigma_i(\theta) \in Z_r(P)$ para cada i, $1 \leq i \leq t$. Es claro que cada $P(\sigma_i(\theta)) = \sigma_i(P(\theta)) = 0$. Además, para cada s, $0 \leq s \leq r-1$, se tiene que el polinomio

$$\prod_{i=1}^{t} \left(Y - \overline{\gamma_s(\sigma_i(\theta))}\right) = \prod_{i=1}^{t} \left(Y - \overline{\sigma_i(\gamma_s(\theta))}\right) = \overline{F_s}(Y)^{n'_s} = (Y - \zeta_s)^t ;$$

lo cual demuestra que cada $\overline{\gamma_s(\sigma_i(\theta))} = \zeta_s$ para $0 \leq s \leq r-1$. Luego, queda probado que cada $\sigma_i(\theta) \in Z_r(P)$ y que $Z_r(P) = C$.

Finalmente, veamos la igualdad afirmada en el corolario. De lo visto anteriormente se obtienen las igualdades

$$P_{S_r}(Y)^{e_0 \cdots e_r} = c' \, \psi_r(Y)^{a_r e_0 \cdots e_r} = c' \, \psi_r(Y)^{t/f_r} = c' \, \overline{F_r}(Y)^{n'_r} ,$$

para algún $c' \in \mathbb{F}_{q_r}^*$, así como las igualdades

$$\overline{F_r}(Y)^{n'_r} = \prod_{i=1}^{t} \left(Y - \overline{\sigma_i(\gamma_r(\theta))}\right) = \prod_{\theta' \in Z_r(P)} \left(Y - \overline{\gamma_r(\theta')}\right) ;$$

las cuales prueban el corolario. □

Ya estamos en condiciones de poder probar el teorema de 9.1.

DEMOSTRACIÓN (del teorema de 9.1). Recordemos (cf. 8.1) que el polinomio $P_r(X) \in \mathcal{O}[X]$ es mónico, de grado $m_r e_r d_r$, con tipo reducido de orden r igual a $\{\mathrm{t}_r^o\}$ y cuyo polinomio asociado (en orden r) al único lado lado, S'_r, del polígono $\mathrm{N}_r(P_r)$ es igual a

$$(P_r)_{S'_r}(Y) = c P_{S_r}(Y) , \quad c \in \mathbb{F}_{q_r}^* .$$

Además, $e_1 \cdots e_{r-1} v(\phi_r(\theta)) = v_r(\phi_r) + h_r/e_r$ para cada raíz θ de $P_r(X)$.

Ahora, consideremos un polinomio $Q(X) \in \mathcal{O}[X]$ mónico, irreducible y que divida a $P_r(X)$. Por la parte (b) del corolario de 1.3 y por el teorema del producto (cf. 6.1), el polinomio $Q(X)$ tiene tipo reducido de orden r igual a $\{\mathrm{t}_r^o\}$. Por la proposición de 9.4, su polinomio asociado (en orden r) al único lado del polígono $\mathrm{N}_r(Q)$ es (salvo constante de $\mathbb{F}_{q_r}^*$) igual a una

potencia de $\psi(Y)$, donde $\psi^\sigma(Y) = \mathrm{Irr}\left(\overline{\gamma_r(\theta)}, \mathbb{F}_{q_r}, Y\right)$, $\theta \in \mathbb{Q}_p^{al}$ es una raíz cualquiera de $Q(X)$ y $\sigma \in \mathrm{Gal}(\mathbb{F}_{q_r}/\mathbb{F}_{q_0})$ es el único automorfismo tal que $\sigma(\zeta_s) = \overline{\gamma_s(\theta)}$ para $0 \leq s \leq r-1$. Además, por el corolario de 6.2, el polinomio $\psi(Y) = \psi_{r,i}(Y)$ para algún único i.

Para cada i definimos entonces el polinomio

$$Q_{r,i}(X) := \prod_{Q(X) \in C_i} Q(X)^{v_Q(P_r)} \in \mathcal{O}[X],$$

donde C_i denota el conjunto formado por todos los polinomios $Q(X) \in \mathcal{O}[X]$ mónicos, irreducibles, que dividen a $P_r(X)$ y tales que el polinomio asociado (en orden r) al único lado del polígono $\mathbf{N}_r(Q)$ es (salvo constante de $\mathbb{F}_{q_r}^*$) igual a una potencia del polinomio $\psi_{r,i}(Y)$. Por lo visto anteriormente tenemos que

$$P_r(X) = Q_{r,1}(X) \cdots Q_{r,g}(X),$$

y que cada polinomio $Q_{r,i}(X)$ satisface las propiedades del teorema, por la parte (a) del corolario de 1.3 y por el teorema del producto. □

§10. Teorema de la resultante

En esta sección y la siguiente volveremos a interesarnos por el problema de determinar con el polígono el índice local de un polinomio mónico y sin raíces multiples de $\mathcal{O}[X]$, el cual resuelve el problema de determinar la valoración p-ádica del discriminante absoluto de un cuerpo de números (cf. §4 del capítulo 1). En esta sección veremos que en orden r también es válido un teorema de la resultante, análogo al de Nart para el polígono de orden 1. Este teorema será utilizado en la próxima sección para probar un teorema del índice en orden r, análogo a su vez al de Ore para primer orden.

Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico. Comenzamos definiendo recurrentemente el conjunto, $\mathbf{t}_{r-1}(P)$, de tipos de orden $r-1$ del polinomio $P(X)$. Pensamos cada tipo de orden s, $0 \leq s \leq r-1$, junto con una elección de los correspondientes polinomios $\phi_i(X)$, $1 \leq i \leq s+1$, que mantendremos al alargar el tipo.

10.1. Definición. *Definimos* $\mathbf{t}_0(P)$ *como el conjunto de todos los tipos* (ψ_0) *de orden* 0, *para los cuales el polinomio* $\psi_0(Y)$ *divide a* $\overline{P}(Y)$.

Supongamos ahora definido el conjunto $\mathbf{t}_{r-2}(P)$ $(r \geq 2)$. *Definimos* $\mathbf{t}_{r-1}(P)$ *como el conjunto de todos los tipos* $(\mathbf{t}_{r-2}; h_{r-1}/e_{r-1}, \psi_{r-1})$ *de orden* $r-1$, *para los cuales el tipo* $\mathbf{t}_{r-2} \in \mathbf{t}_{r-2}(P)$ *y satisface que el polígono* $\mathbf{N}^0_{(v_{r-1},\phi_{r-1})}(P)$ *no se reduce a un solo punto, el número racional* $-h_{r-1}/e_{r-1}$ *es la pendiente de un lado* S *de este polígono, y el polinomio* $\psi_{r-1}(Y)$ *es un factor de su polinomio asociado (en orden* $r-1$*)* $P_S(Y)$.

Podemos imaginar el conjunto $\mathbf{t}_{r-1}(P)$ como todos los caminos de longitud $2(r-1)$ de un árbol que empieza con los factores irreducibles de $\overline{P}(Y)$. A cada uno le asignamos tantas ramas como lados tiene la parte principal del polígono, a cada rama le "salen" tantas ramas como factores irreducibles tiene el polinomio asociado, etc. Por lo que hemos visto (cf. 9.1) a cada uno de esos caminos le corresponde un factor de $P(X)$ en $\mathcal{O}[X]$.

10.2. Observaciones. (1). Observemos que el conjunto $\mathbf{t}_{r-1}(P)$ es finito (eventualmente igual al vacio) y coincide con el conjunto de los tipos de orden $r-1$ para los que la correspondiente pseudo-valoración ω_r cumple $\omega_r(P) > 0$ (recordar que $\omega_r(P) \leq \omega_{r-1}(P)$, por la parte (b) de la proposición de 2.3).

(2). Si $Q(X) \in \mathcal{O}[X]$ es otro polinomio mónico, entonces

$$\mathbf{t}_{r-1}(P \cdot Q) = \mathbf{t}_{r-1}(P) \cup \mathbf{t}_{r-1}(Q)\,.$$

(3). Si $P(X)$ es irreducible en $K[X]$, entonces el conjunto $\mathbf{t}_{r-1}(P)$ tiene a lo sumo un elemento, por el teorema del polígono y el teorema del polinomio asociado. Así, por ejemplo, el conjunto $\mathbf{t}_{r-1}(\phi_{r-1}) = \{\emptyset\}$ para el correspondiente polinomio $\phi_{r-1}(X)$ de un tipo de orden $r-1$.

(4). Sea $\mathbf{t}_{r-1}$ un tipo de orden $r-1$. Si $P(X)$ tiene tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ (cf. definición de 1.1), entonces, por definición, el conjunto $\mathbf{t}_{r-1}(P) = \{\mathbf{t}_{r-1}\}$. Pero, el recíproco no es cierto en general, como muestra claramente el polinomio $\phi_r(X)\,\phi_{r-1}(X)$ (cf. parte (a) del corolario de 3.4). Sin embargo, por el teorema del polinomio asociado, tenemos que el conjunto $\mathbf{t}_{r-1}(P) = \{\mathbf{t}_{r-1}\}$ si y sólo si $P(X) = Q(X)\,R(X)$, donde $Q(X) \in \mathcal{O}[X]$ es un polinomio mónico que tiene tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ y

$R(X) \in \mathcal{O}[X]$ es un polinomio mónico con $\mathbf{t}_{r-1}(R) = \{\emptyset\}$. En particular, si $P(X)$ es irreducible en $K[X]$, entonces el conjunto $\mathbf{t}_{r-1}(P) = \{\mathbf{t}_{r-1}\}$ si y sólo si $P(X)$ tiene tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$.

Fijados un tipo $\mathbf{t}_{r-1}$ de orden $r-1$ y un polinomio $\phi_r(X) \in \mathcal{O}[X]$ que satisface las condiciones del teorema de 3.1 ($r \geq 1$), vamos a definir ahora un entero $\mathrm{R}_{\mathbf{t}_{r-1}}(P,Q) \geq 0$ para cada par de polinomios $P(X), Q(X) \in \mathcal{O}[X]$ mónicos y sin raíces comunes. Sean $S_{r,1}, \ldots, S_{r,g}$ (resp. $S'_{r,1}, \ldots, S'_{r,g'}$) los lados del polígono $\mathrm{N}_r^0(P)$ (resp. $\mathrm{N}_r^0(Q)$), y sean $E_{r,i}$, $H_{r,i}$ (resp. $E'_{r,j}$, $H'_{r,j}$) las proyecciones sobre los ejes de abscisas y ordenadas, respectivamente, de cada lado $S_{r,i}$ (resp. $S'_{r,j}$).

10.3. Definición. *Definimos*

$$\mathrm{R}_{\mathbf{t}_{r-1}}(P,Q) := f_0 \cdots f_{r-1} \left(\sum_{i,j} \min\{E_{r,i}H'_{r,j}, E'_{r,j}H_{r,i}\} + \varepsilon_{\mathbf{t}_{r-1}}(P,Q) \right) \in \mathbb{N},$$

donde el entero

$$\varepsilon_{\mathbf{t}_{r-1}}(P,Q) := v_{\phi_r}(Q) \cdot \sum_{i=1}^{g} H_{r,i} + v_{\phi_r}(P) \cdot \sum_{j=1}^{g'} H'_{r,j} \in \mathbb{N}.$$

10.4. Observaciones. (1). Si alguna de las dos partes principales $\mathrm{N}_r^0(P)$ y $\mathrm{N}_r^0(Q)$ se reduce a un solo punto, entonces entenderemos que el entero $\mathrm{R}_{\mathbf{t}_{r-1}}(P,Q) := f_0 \cdots f_{r-1} \cdot \varepsilon_{\mathbf{t}_{r-1}}(P,Q)$. Por consiguiente, se tiene que

$$\mathrm{R}_{\mathbf{t}_{r-1}}(P,Q) > 0 \iff \omega_r(P)\omega_r(Q) > 0 \iff \mathbf{t}_{r-1} \in \mathbf{t}_{r-1}(P) \cap \mathbf{t}_{r-1}(Q)$$

(cf. lema de 4.2 y observación (1) de 10.2).

(2). En nuestras aplicaciones, el entero $\varepsilon_{\mathbf{t}_{r-1}}(P,Q)$ será siempre nulo, ya que tendremos que los polinomios $P(X)$ y $Q(X)$ nunca serán divisibles por el polinomio $\phi_r(X)$.

A continuación, para cada par de polinomios mónicos y sin raíces comunes $P(X), Q(X) \in \mathcal{O}[X]$, definimos un entero $\mathrm{R}_r(P,Q) \geq 0$ ($r \geq 1$), que medirá lo que nos "comemos" del entero $v(\mathrm{Res}(P,Q))$ con el polígono de orden r.

10.5. Definición. *Definimos*

$$\mathrm{R}_r(P,Q) := \sum_{\mathbf{t}_{r-1}} \mathrm{R}_{\mathbf{t}_{r-1}}(P,Q) = \sum_{\mathbf{t}_{r-1}\in \mathbf{t}_{r-1}(P)\cap \mathbf{t}_{r-1}(Q)} \mathrm{R}_{\mathbf{t}_{r-1}}(P,Q) \in \mathbb{N},$$

donde la primera suma se extiende a todos los tipos $\mathbf{t}_{r-1}$ *de orden* $r-1$, *mientras que la segunda solamente se extiende a aquellos que pertenecen al conjunto finito* $\mathbf{t}_{r-1}(P)\cap \mathbf{t}_{r-1}(Q)$.

Ya podemos enunciar ahora el teorema de la resultante en orden r.

10.6. Teorema. (Teorema de la resultante) *Sean* $P(X), Q(X) \in \mathcal{O}[X]$ *dos polinomios mónicos y sin raíces comunes.*

(a) *Tenemos*

$$v(\mathrm{Res}(P,Q)) \geq \mathrm{R}_1(P,Q) + \cdots + \mathrm{R}_r(P,Q).$$

(b) *La igualdad vale en* (a) *si y sólo si para cada tipo* $\mathbf{t}_{r-1}$ *que pertenece al conjunto* $\mathbf{t}_{r-1}(P)\cap \mathbf{t}_{r-1}(Q)$ *no hay dos lados,* S *y* S', *de los polígonos* $\mathbf{N}_r^0(P)$ *y* $\mathbf{N}_r^0(Q)$ *con la misma pendiente y polinomios asociados (en orden* r*),* $P_S(Y)$ *y* $Q_{S'}(Y)$, *con factores comunes (en* $\mathbb{F}_{q_r}[Y]$*).*

Notemos que para dos polinomios concretos cualesquiera con este teorema también podemos calcular el entero $v(\mathrm{Res}(P,Q))$ en un número finito de pasos (sin necesidad de calcular toda la resultante $\mathrm{Res}(P,Q)$). En efecto, por inducción, sabemos que no habíamos acabado de calcularlo en orden $r-1$ si y sólo si el conjunto $\mathbf{t}_{r-1}(P)\cap \mathbf{t}_{r-1}(Q)$ es no vacio, si y sólo si el entero $\mathrm{R}_r(P,Q) > 0$ (cf. observación 1 de 10.4).

Ahora, comenzamos probando el teorema en el caso de dos polinomios irreducibles con $C := \mathbf{t}_{r-1}(P) = \mathbf{t}_{r-1}(Q) \neq \{\emptyset\}$. En este caso, hay un solo tipo en el conjunto C, un solo lado en los respectivos polígonos $\mathbf{N}_s(P)$ y $\mathbf{N}_s(Q)$, con la misma pendiente $H_s/E_s = H_s'/E_s'$, y el entero

$$\mathrm{R}_s(P,Q) = f_0 \cdots f_{s-1} \cdot E_s' H_s$$

para todo $s = 1, \ldots, r-1$.

10.7. Proposición. *Sean* $P(X), Q(X) \in \mathcal{O}[X]$ *dos polinomios mónicos, irreducibles, con el mismo tipo,* $\{\mathbf{t}_{r-1}\}$, *de orden* $r-1$ *y distintos de* $\phi_r(X)$.

Para cada entero i, $1 \le i \le r$, sea S_i (resp. S_i') el único lado del polígono $\mathrm{N}_i(P)$ (resp. $\mathrm{N}_i(Q)$) (cf. 8.4) y sean E_i, H_i (resp. E_i', H_i') las longitudes de su proyección sobre los ejes de abscisas y de ordenadas, respectivamente.

(a) *Tenemos*

$$v(\mathrm{Res}(P,Q)) \ge \sum_{s=1}^{r-1} f_0 \cdots f_{s-1} \cdot E_s' H_s + f_0 \cdots f_{r-1} \cdot \min\{E_r H_r', E_r' H_r\}.$$

(b) *La igualdad vale en* (a) *si y sólo si o bien* $\dfrac{H_r}{E_r} \ne \dfrac{H_r'}{E_r'}$ *o bien los polinomios* $P_{S_r}(Y), Q_{S_r'}(Y)$ *no tienen factores comunes (en* $\mathbb{F}_{q_r}[Y]$*).*

DEMOSTRACIÓN. Sin pérdida de generalidad podemos suponer que la pendiente $\dfrac{H_r}{E_r} \le \dfrac{H_r'}{E_r'}$. Recordemos que la resultante

$$\mathrm{Res}(P,Q) = \pm \prod_{\theta' \in Z(Q)} P(\theta'),$$

donde $Z(Q)$ denota el conjunto de las raíces de $Q(X)$ en $\mathbb{Q}_p^{al}$; por tanto,

$$v(\mathrm{Res}(P,Q)) = \sum_{\theta' \in Z(Q)} v(P(\theta')) = \mathrm{gr}(Q)\, v(P(\theta')),$$

para cualquier $\theta' \in Z(Q)$ (pues los elementos $P(\theta')$ son conjugados sobre K). Recordemos también que, por la proposición de 8.4, para cada $\theta' \in Z(Q)$ es

$$v(\phi_r(\theta')) = \frac{1}{e_1 \cdots e_{r-1}} \left(v_r(\phi_r) + \frac{H_r'}{E_r'} \right).$$

Fijemos un elemento $\theta' \in Z(Q)$ cualquiera. Consideremos los enteros $u_i := v_r(A_i\, {\phi_r}^i)$ correspondientes al ϕ_r-desarrollo (2.4.1) de $P(X)$. Entonces para cada i tenemos que $e_1 \cdots e_{r-1} v(A_i(\theta')) = v_r(A_i)$, por la parte (b) de la proposición de 7.1, y que

$$\begin{aligned} v(A_i(\theta')\, \phi_r(\theta')^i) &= \frac{1}{e_1 \cdots e_{r-1}} \left(u_i + i \frac{H_r'}{E_r'} \right) \\ &\ge \frac{1}{e_1 \cdots e_{r-1}} \left(u_i + i \frac{H_r}{E_r} \right) \qquad (*_i) \\ &\ge \frac{1}{e_1 \cdots e_{r-1}} (v_r(P) + H_r); \end{aligned}$$

además, la penúltima desigualdad $(*_i)$ es una igualdad si y solamente si $i = 0$ o $\dfrac{H_r}{E_r} = \dfrac{H'_r}{E'_r}$, y la última desigualdad es una igualdad si y sólo si el punto $(i, u_i) \in S_r$. Por consiguiente, teniendo en cuenta que el grado $\mathrm{gr}(Q) = e_0 f_0 \cdots e_{r-1} f_{r-1} E'_r$ (cf. 1.2), que el valor $v_r(P) = \sum_{s=1}^{r-1} e_s \cdots e_{r-1} H_s$ (pues, $v_1(P) = 0$ y cada $v_{s+1}(P) = e_s(v_s(P) + H_s)$) y que para cada s, $1 \le s \le r-1$, el entero $E'_s = e_s f_s \cdots e_{r-1} f_{r-1} E'_r$ (cf. 4.2), se tiene que

$$\begin{aligned} v(\mathrm{Res}(P,Q)) &\ge \frac{\mathrm{gr}(Q)}{e_1 \cdots e_{r-1}}(v_r(P) + H_r) \\ &= f_0 \cdots f_{r-1} E'_r \sum_{s=1}^{r} e_s \cdots e_{r-1} H_s \\ &= \sum_{s=1}^{r} f_0 \cdots f_{s-1} E'_s H_s; \end{aligned}$$

además, la desigualdad anterior es una igualdad si y sólo si

$$v\left(\sum_{i:(i,u_i)\in S_r} A_i(\theta')\,\phi_r(\theta')^i\right) = \frac{1}{e_1 \cdots e_{r-1}}(v_r(P) + H_r). \qquad (*)$$

Hemos demostrado la parte (a) y puesto los cimientos para la parte (b).

La igualdad de $(*)$ se satisface siempre si $\dfrac{H_r}{E_r} < \dfrac{H'_r}{E'_r}$, puesto que entonces la desigualdad de $(*_i)$ sólo es igualdad para un i $(i = 0)$.

Supongamos, por tanto, que $\dfrac{H_r}{E_r} = \dfrac{H'_r}{E'_r}$; así, la correspondiente fracción racional $\gamma_r(X) \in K(X)$ (cf. 9.4) es la misma para los dos polinomios. Puesto que $e_1 \cdots e_{r-1} v(\pi_r(\theta')) = 1$ (cf. cálculos de $(r-1.\mathrm{a})$ en la §7), el miembro de la izquierda de la igualdad de $(*)$ coincide exactamente con

$$v(P^{S_r}(\theta')) + \frac{1}{e_1 \cdots e_{r-1}}(v_r(P) + H_r).$$

Entonces, por la proposición de 7.4, obtenemos que la igualdad de $(*)$ se satisface si y sólo si $P^{\tau}_{S_r}\left(\overline{\gamma_r(\theta')}\right) \neq 0$, donde $\tau \in \mathrm{Gal}(\mathbb{F}_{q_r}/\mathbb{F}_{q_0})$ es el único automorfismo tal que $\tau(\zeta_s) = \overline{\gamma_s(\theta')}$ para cada s, $0 \le s \le r-1$. Finalmente, por la proposición de 9.4 aplicada a los polinomios $P(X)$ y $Q(X)$, se tiene la equivalencia

$$P^{\tau}_{S_r}\left(\overline{\gamma_r(\theta')}\right) \neq 0 \iff P_{S_r}(Y), Q_{S'_r}(Y) \text{ no tienen factores comunes.}$$

Luego, hemos acabado de probar la parte (b). □

10.8. Observaciones. (1). Sea $\mathbf{t}_{r-1}$ un tipo de orden $r-1$. Por el teorema del producto, la proposición anterior es válida a posteriori para dos polinomios mónicos, no necesariamente irreducibles, con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ (el mismo para los dos), no divisibles por $\phi_r(X)$ y cuyos polígonos en orden r consten de un único lado.

(2). Sea $P(X)$ un polinomio como en la proposición anterior. Por una parte, como para cada s, $1 \leq s \leq r-1$, es $v_{\phi_s}(\phi_r) = 0$ (cf. (a) de 3.4) y $\omega_s(\phi_r) = e_s f_s \cdots e_{r-1} f_{r-1}$ (cf. 3.5), tenemos las igualdades

$$\mathrm{R}_s(P, \phi_r) = f_0 \cdots f_{s-1} \cdot e_s f_s \cdots e_{r-1} f_{r-1} \cdot H_s\,, \quad 1 \leq s \leq r-1\,,$$
$$\mathrm{R}_r(P, \phi_r) = f_0 \cdots f_{r-1} \cdot \varepsilon_{\mathbf{t}_{r-1}}(P, \phi_r) = f_0 \cdots f_{r-1} \cdot H_r\,.$$

Por otra, procediendo como en la demostración de la parte (a) de la proposición anterior (cambiando en ella los polinomios $P(X)$ y $Q(X)$ por $\phi_r(X)$ y $P(X)$, respectivamente), obtenemos la igualdad

$$v(\mathrm{Res}(P, \phi_r)) = f_0 \cdots f_{r-1} E_r \left(v_r(\phi_r) + \frac{H_r}{E_r} \right)\,.$$

Por consiguiente, utilizando la fórmula para $v_r(\phi_r)$ dada en la parte (c) del corolario de 3.3 y que cada $H_s = e_s f_s \cdots e_{r-1} f_{r-1} E_r h_s / e_s$, vemos que

$$v(\mathrm{Res}(P, \phi_r)) = \mathrm{R}_1(P, \phi_r) + \cdots + \mathrm{R}_r(P, \phi_r)\,.$$

Además, a posteriori, la igualdad anterior sigue siendo válida para cualquier polinomio mónico $P(X) \in \mathcal{O}[X]$, no necesariamente irreducible, con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$, no divisible por $\phi_r(X)$ y cuyo polígono $\mathbf{N}_r(P)$ conste de un único lado.

Ya estamos en condiciones de poder probar el teorema de la resultante en orden r para dos polinomios cualesquiera.

DEMOSTRACIÓN (del teorema de 10.3). La demostración se hace por inducción sobre el cardinal del conjunto finito $C := \mathbf{t}_{r-1}(P) \cap \mathbf{t}_{r-1}(Q)$. Si C es el conjunto vacio, entonces sabemos que $\mathrm{R}_r(P, Q) = 0$, y acabamos aplicando la parte (b) de este mismo teorema en orden $r-1$.

Supongamos pues que el conjunto C es no vacio, y que el teorema es válido para cualquier par de polinomios cuyo correspondiente conjunto intersección de tipos de orden $r-1$ tenga cardinal menor que C. Elegimos entonces un tipo $\mathbf{t}_{r-1} \in C$. Sin pérdida de generalidad podemos suponer que $0 = v_{\phi_r}(P) \leq v_{\phi_r}(Q) =: \alpha$. Por el teorema del polígono, sabemos que nuestros polinomios admiten en $\mathcal{O}[X]$ factorizaciones de la forma

$$P(X) = P_{r,1}(X) \cdots P_{r,g}(X) \cdot R(X),$$
$$Q(X) = \phi_r(X)^\alpha \cdot Q_{r,1}(X) \cdots Q_{r,g'}(X) \cdot R'(X),$$

donde los polinomios $P_{r,i}(X)$ y $Q_{r,j}(X)$ son mónicos, con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$, no divisibles por $\phi_r(X)$, cuyos polígonos en orden r constan de un único lado, con los mismos datos que $S_{r,i}$ y $S'_{r,j}$, y cuyos polinomios asociados en orden r coinciden (salvo constante) con $P_{S_{r,i}}(Y)$ y $Q_{S_{r,j}}(Y)$, y donde los polinomios $R(X)$ y $R'(X)$ satisfacen que $\omega_r(R) = \omega_r(R') = 0$; así, $\mathbf{t}_{r-1} \notin \mathbf{t}_{r-1}(R) \cup \mathbf{t}_{r-1}(R')$.

Teniendo en cuenta la bilinealidad de la resultante respecto del producto, descomponemos $v(\mathrm{Res}(P,Q))$ en varios sumandos, de acuerdo con las factorizaciones anteriores de los dos polinomios. Conocemos cada uno de los sumandos $v(\mathrm{Res}(P_{r,i}, R'))$, $v(\mathrm{Res}(R, \phi_r))$ y $v(\mathrm{Res}(R, Q_{r,j}))$, ya que los correspondientes conjuntos intersección de tipos de orden $r-1$ son vacios. Por las observaciones de 10.8, también conocemos cada sumando $v(\mathrm{Res}(P_{r,i}, \phi_r))$, y tenemos la información que buscamos de cada sumando $v(\mathrm{Res}(P_{r,i}, Q_{r,j}))$. Por tanto, de los sumandos de $v(\mathrm{Res}(P,Q))$ tan sólo nos resta por analizar a $v(\mathrm{Res}(R,R'))$. Pero, como el conjunto intersección $\mathbf{t}_{r-1}(R) \cap \mathbf{t}_{r-1}(R') = C \setminus \{\mathbf{t}_{r-1}\}$ tiene un elemento menos que C, entonces, por la hipótesis de inducción, sabemos que el teorema es válido para el par de polinomios $R(X)$ y $R'(X)$. Ahora, sólo es cuestión de comprobar. □

§11. Teorema del índice

Con la ayuda del teorema de la resultante de la sección anterior, vamos a ver ahora un teorema del índice en orden r, análogo al de Ore para primer orden, que nos permitirá calcular el índice local de cualquier polinomio. En

el próximo capítulo este teorema se utilizará para ver que el algoritmo de descomposición de primos que se obtiene termina en un número finito de pasos.

Fijados un tipo $\mathbf{t}_{r-1}$ de orden $r-1$ y un polinomio $\phi_r(X) \in \mathcal{O}[X]$ que satisface las condiciones del teorema de 3.1 ($r \geq 1$), vamos a definir un entero $\mathrm{i}_{\mathbf{t}_{r-1}}(P) \geq 0$ para cada polinomio $P(X) \in \mathcal{O}[X]$ mónico y sin raíces múltiples. Sean $S_{r,1}, \ldots, S_{r,g}$ los lados del polígono $\mathbf{N}_r^0(P)$, y para cada lado $S_{r,i}$ sean $d_{r,i}$, $e_{r,i}$, $h_{r,i}$, $E_{r,i} := d_{r,i}e_{r,i}$, $H_{r,i} := d_{r,i}h_{r,i}$ los datos asociados. Suponemos ordenadas las pendientes de forma que se satisfaga $-h_{r,1}/e_{r,1} < \cdots < -h_{r,g}/e_{r,g}$.

11.1. Definición. *Definimos*

$$\mathrm{i}_{\mathbf{t}_{r-1}}(P) := f_0 \cdots f_{r-1} \left(\mathrm{i}^0_{\mathbf{t}_{r-1}}(P) + \epsilon_{\mathbf{t}_{r-1}}(P) \right) \in \mathbb{N},$$

donde

$$\mathrm{i}^0_{\mathbf{t}_{r-1}}(P) := \frac{1}{2} \sum_{i=1}^{g} (E_{r,i}H_{r,i} - E_{r,i} - H_{r,i} + d_{r,i}) + \sum_{1 \leq i < j \leq g} E_{r,i}H_{r,j} \in \mathbb{N},$$

$$\epsilon_{\mathbf{t}_{r-1}}(P) := v_{\phi_r}(P) \cdot \sum_{i=1}^{g} H_{r,i} \in \mathbb{N}.$$

11.2. Observaciones. (1). Si el polígono $\mathbf{N}_r^0(P)$ se reduce a un solo punto (es decir, $v_{\phi_r}(P) = \omega_r(P)$), entonces entenderemos que $\mathrm{i}_{\mathbf{t}_{r-1}}(P) := 0$; así, $\mathrm{i}_{\mathbf{t}_{r-1}}(\phi_r) = 0$. Por tanto, $\mathrm{i}_{\mathbf{t}_{r-1}}(P) = 0$ si y sólo si o bien el polígono $\mathbf{N}_r^0(P)$ se reduce a un solo punto o bien este polígono consta de un solo lado con alguna de sus dos proyecciones sobre los ejes igual a 1 y $P(X)$ no es divisible por $\phi_r(X)$. Luego, el entero $\mathrm{i}_{\mathbf{t}_{r-1}}(P) \neq 0$ solamente para tipos $\mathbf{t}_{r-1}$ de orden $r-1$ del conjunto finito $\mathbf{t}_{r-1}(P)$ (cf. observación (1) de 10.2).

(2). El entero $\mathrm{i}^0_{\mathbf{t}_{r-1}}(P)$ es igual al número de puntos de coordenadas enteras del recinto acotado delimitado por el polígono $\mathbf{N}_r^0(P)$, la recta horizontal de ecuación $y = v_r(P)$ y la recta vertical de ecuación $x = v_{\phi_r}(P)$, incluyendo los puntos que están sobre los lados del polígono $\mathbf{N}_r^0(P)$, excepto el origen del primer lado y el final del último lado, y excluyendo los puntos que están sobre estas rectas.

Ahora, para cada polinomio $P(X) \in \mathcal{O}[X]$ mónico y sin raíces múltiples, vamos a definir un entero $\mathrm{i}_r(P) \geq 0$ $(r \geq 1)$, que medirá lo que nos "comemos" del índice $\mathrm{i}(P)$ con el polígono de orden r.

11.3. Definición. *Definimos*

$$\mathrm{i}_r(P) := \sum_{\mathbf{t}_{r-1}} \mathrm{i}_{\mathbf{t}_{r-1}}(P) = \sum_{\mathbf{t}_{r-1} \in \mathbf{t}_{r-1}(P)} \mathrm{i}_{\mathbf{t}_{r-1}}(P) \in \mathbb{N},$$

donde la primera suma se extiende a todos los tipos $\mathbf{t}_{r-1}$ *de orden* $r-1$, *mientras que la segunda solamente se extiende a aquellos que pertenecen al conjunto finito* $\mathbf{t}_{r-1}(P)$.

Ahora, ya podemos enunciar el teorema del índice.

11.4. Teorema. (Teorema del índice) *Sea* $P(X) \in \mathcal{O}[X]$ *un polinomio mónico y sin raíces múltiples.*

(a) *Tenemos*

$$\mathrm{i}(P) \geq \mathrm{i}_1(P) + \cdots + \mathrm{i}_r(P).$$

(b) *Si para cada tipo* $\mathbf{t}_{r-1}$ *de orden* $r-1$ *que pertenece al conjunto* $\mathbf{t}_{r-1}(P)$ *todos los polinomios asociados (en orden* r*) al polinomio* $P(X)$ *y a los lados del polígono* $\mathrm{N}_r^0(P)$ *no tienen raíces múltiples, entonces vale la igualdad en* (a).

Con este teorema también podemos obtener una condición computable, necesaria y suficiente para que valga la igualdad en (a) en un orden menos.

11.5. Corolario. *Sea* $P(X) \in \mathcal{O}[X]$ *un polinomio mónico y sin raíces múltiples. Entonces* $\mathrm{i}(P) = \mathrm{i}_1(P) + \cdots + \mathrm{i}_{r-1}(P)$ *si y sólo si* $\mathrm{i}_r(P) = 0$.

DEMOSTRACIÓN. La necesidad se obtiene de la parte (a) del teorema. Para ver la suficiencia basta con observar que, por la observación (1) de 11.2, si $\mathrm{i}_r(P) = 0$ se satisface la condición de la parte (b) del teorema anterior. □

Este corolario y el teorema anterior nos permiten computar el índice $\mathrm{i}(P)$ para cualquier polinomio concreto $P(X)$ en un número finito de pasos.

En efecto, por el corolario sabemos que no habíamos terminado de computar $\mathrm{i}(P)$ en orden $r-1$ si y sólo si $\mathrm{i}_r(P) > 0$.

Pasemos a probar el teorema de 11.4 para el caso de un polinomio irreducible cuyo conjunto de tipos de orden $r-1$ sea no vacio. En este caso, hay un solo tipo en el conjunto $\mathbf{t}_{r-1}(P)$, un solo lado en el polígono $\mathbf{N}_s(P)$, cuyos datos los denotaremos por $d_s, e_s, h_s, E_s := d_s e_s, H_s := d_s h_s$, y el entero

$$\mathrm{i}_s(P) = \frac{1}{2} f_0 \cdots f_{s-1}(E_s H_s - E_s - H_s + d_s),$$

para todo $s = 1, \ldots, r-1$.

11.6. Proposición. *Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico, irreducible, con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$ y distinto de $\phi_r(X)$. Para cada s, $1 \le s \le r$, sean d_s, e_s, h_s, E_s, H_s los datos del único lado del polígono $\mathbf{N}_s(P)$, y sea $\psi_s(Y)^{a_s}$ la potencia de $\psi_s(Y)$ que coincide (salvo constante) con su polinomio asociado en orden s (cf. 8.4 y 9.4).*

(a) *Tenemos*

$$\mathrm{i}(P) \ge \frac{1}{2} \sum_{s=1}^{r} f_0 \cdots f_{s-1}(E_s H_s - E_s - H_s + d_s).$$

(b) *Si $a_r = 1$, entonces vale la igualdad en* (a).

La demostración de esta proposición requiere algunos preliminares. Sea $\theta \in \mathbb{Q}_p^{al}$ una raíz fijada de nuestro polinomio irreducible $P(X)$, y ponemos $L := K(\theta)$. Para todo $\mathbf{j} = (j_0, j_1, \ldots, j_r) \in \mathbb{N}^{r+1}$ ponemos

$$\Phi(\mathbf{j}) := \frac{\phi_0(\theta)^{j_0} \phi_1(\theta)^{j_1} \cdots \phi_r(\theta)^{j_r}}{\pi^{[j_1\nu_1 + \cdots + j_r\nu_r]}} \in \mathcal{O}_L,$$

donde $\nu_s := v(\phi_s(\theta))$ $(1 \le s \le r)$. Consideramos el sub-$\mathcal{O}$-módulo $\mathcal{O}'_L$ de $\mathcal{O}_L$ generado por el conjunto $\{\Phi(\mathbf{j}) : \mathbf{j} \in J\}$, donde

$$J := \{\mathbf{j} \in \mathbb{N}^{r+1} : 0 \le j_s < e_s f_s \text{ para } 0 \le s < r, 0 \le j_r < e_r f_r a_r\}.$$

Es claro que $\mathcal{O}[\theta] \subset \mathcal{O}'_L$ y que $\mathcal{O}'_L$ es un $\mathcal{O}$-módulo libre de rango igual al grado del polinomio $P(X)$. Además, tenemos la igualdad

$$\frac{v((\mathcal{O}'_L : \mathcal{O}[\theta]))}{[K : \mathbb{Q}_p]} = f_0 \sum_{(0, j_1, \ldots, j_r) \in J} \left[\sum_{s=1}^{r} j_s \nu_s \right].$$

Por otra parte, puesto que $\mathrm{i}(P) = \dfrac{v((\mathcal{O}_L : \mathcal{O}[\theta]))}{[K:\mathbb{Q}_p]}$, entonces tenemos

$$\mathrm{i}(P) \geq \frac{v((\mathcal{O}'_L : \mathcal{O}[\theta]))}{[K:\mathbb{Q}_p]}; \qquad \mathrm{i}(P) = \frac{v((\mathcal{O}'_L : \mathcal{O}[\theta]))}{[K:\mathbb{Q}_p]} \iff \mathcal{O}_L = \mathcal{O}'_L.$$

Por consiguiente, si vemos las afirmaciones

(a') $f_0 \sum_{(0,j_1,\dots,j_r)\in J} \left[\sum_{s=1}^{r} j_s \nu_s\right] = \mathrm{i}_1(P) + \cdots + \mathrm{i}_r(P).$

(b') $a_r = 1$ implica que $\mathcal{O}_L = \mathcal{O}'_L$.

quedará probada la proposición de 11.6.

Para la demostración de (a') necesitaremos el siguiente lema de partes enteras.

11.7. Lema. *Sea $e \geq 1$ un número entero, y sea $x \geq 0$ un número racional. Entonces* $\sum_{k=0}^{e-1} \left[\frac{k}{e} + \frac{1}{e}x\right] = [x]$.

DEMOSTRACIÓN. Escribimos $x = \dfrac{a}{b}$, con $a \geq 0$, $b \geq 1$ enteros. Para cada entero k, $0 \leq k < e$, escribimos $k\,b + a = i_k e\,b + s_k$ con $0 \leq s_k < e\,b$; así, $\left[\dfrac{k}{e} + \dfrac{1}{e}\dfrac{a}{b}\right] = i_k$. Sumando para k se tiene $e\,a = \left(\sum_{k=0}^{e-1} i_k\right) e\,b + s$, donde $s := \sum_{k=0}^{e-1}(s_k - k\,b)$. Para probar el lema nos bastará con ver que $0 \leq s < e\,b$; ya que entonces tendremos $\sum_{k=0}^{e-1} i_k = \left[\dfrac{a}{b}\right]$.

Veamos pues que $0 \leq s < e\,b$. Ponemos ahora $a \equiv a' \pmod{b}$ con $0 \leq a' < b$. Puesto que para todo $0 \leq k < e$ es $s_k \equiv a \equiv a' \pmod{b}$, y dado que la igualdad $s_k = s_{k'}$ para $0 \leq k, k' < e$ implica $k = k'$, entonces $\{s_k : 0 \leq k < e\} = \{a' + k\,b : 0 \leq k < e\}$ (tal vez en distinto orden). Por consiguiente, $s = \sum_{k=0}^{e-1} s_k - \sum_{k=0}^{e-1} k\,b = \sum_{k=0}^{e-1}(a' + k\,b) - \sum_{k=0}^{e-1} k\,b = e\,a'$, lo que prueba que $0 \leq s < e\,b$. □

Para la demostración de (b') necesitaremos el siguiente resultado fundamental.

11.8. Proposición. *Con las hipótesis y notaciones anteriores, $\mathcal{O}'_L$ es un subanillo (y, por tanto, un orden) de $\mathcal{O}_L$.*

Para demostrar esta proposición necesitaremos a su vez otros dos lemas más.

11.9. Lema. *Con las hipótesis y notaciones anteriores, sea $Q(X) \in \mathcal{O}[X]$ un polinomio de grado menor que m_r.*

(a) *Podemos escribir, y en forma única,*

$$Q(X) = \sum_{\mathbf{j}=(j_0,\dots,j_{r-1},0)\in J} Q_{\mathbf{j}}\,\phi_0(X)^{j_0}\cdots\phi_{r-1}(X)^{j_{r-1}},$$

con los $Q_{\mathbf{j}} \in \mathcal{O}$.

(b) *Si $v_r(Q) \geq e_1\cdots e_{r-1}\mu$, donde μ es un número racional, entonces $v(Q_{\mathbf{j}}) \geq \mu - (j_1\nu_1 + \cdots + j_{r-1}\nu_{r-1})$ para cada $\mathbf{j} = (j_0,\dots,j_{r-1},0) \in J$.*

DEMOSTRACIÓN. La parte (a) es clara, considerando recurrentemente desarrollos ϕ_{r-2}-ádicos de los coeficientes del desarrollo ϕ_{r-1}-ádico de $Q(X)$, etc.

Veamos por inducción sobre $r \geq 1$ la parte (b). El caso $r = 1$ se obtiene directamente de la definición de la valoración v_1. Supongamos ahora que el resultado es cierto para $r-1$. Para cada j_{r-1}, $0 \leq j_{r-1} < e_{r-1}f_{r-1}$, consideramos el polinomio, de grado menor que m_{r-1},

$$Q_{j_{r-1}}(X) := \sum_{(j_0,\dots,j_{r-2},0,0)\in J} Q_{\mathbf{j}}\,\phi_0(X)^{j_0}\cdots\phi_{r-2}(X)^{j_{r-2}} \in \mathcal{O}[X];$$

así, $Q(X) = \sum_{j_{r-1}=0}^{e_{r-1}f_{r-1}-1} Q_{j_{r-1}}(X)\,\phi_{r-1}(X)^{j_{r-1}}$ es el desarrollo ϕ_{r-1}-ádico de $Q(X)$. Como $v_r(Q) \geq e_1\cdots e_{r-1}\mu$, entonces los puntos del diagrama $\mathbf{D}_{r-1}(Q)$ están por encima de la recta con pendiente $-h_{r-1}/e_{r-1}$ que corta al eje de ordenadas en el punto $(0, e_1\cdots e_{r-2}\mu)$. Por tanto, para todo j_{r-1}, $0 \leq j_{r-1} < e_{r-1}f_{r-1}$, se tiene

$$\begin{aligned} v_{r-1}(Q_{j_{r-1}}) &\geq e_1\cdots e_{r-2}\mu - j_{r-1}\left(\frac{h_{r-1}}{e_{r-1}} + v_{r-1}(\phi_{r-1})\right) \\ &= e_1\cdots e_{r-2}(\mu - j_{r-1}\nu_{r-1}) \quad \text{(por la proposición de 8.4).} \end{aligned}$$

Ahora, se termina aplicando la hipótesis de inducción a los $Q_{j_{r-1}}(X)$. □

11.10. Corolario. *Continuamos con las hipótesis y notaciones anteriores.*

(a) $\phi_r(X) = \phi_{r-1}(X)^{e_{r-1}f_{r-1}} + \sum_{\mathbf{j}=(j_0,\dots,j_{r-1},0)\in J} C_{\mathbf{j}}\,\phi_0(X)^{j_0}\cdots\phi_{r-1}(X)^{j_{r-1}}$, *donde cada* $C_{\mathbf{j}} \in \mathcal{O}$ *y* $v(C_{\mathbf{j}}) \geq e_{r-1}f_{r-1}\nu_{r-1} - (j_1\nu_1 + \cdots + j_{r-1}\nu_{r-1})$.

(b) $P(X) = \phi_r(X)^{E_r} + \sum_{\mathbf{j}\in J} A_{\mathbf{j}}\,\phi_0(X)^{j_0}\cdots\phi_r(X)^{j_r}$, *donde cada* $A_{\mathbf{j}} \in \mathcal{O}$ *y* $v(A_{\mathbf{j}}) \geq E_r\nu_r - (j_1\nu_1 + \cdots + j_r\nu_r)$.

DEMOSTRACIÓN. Consideramos el polinomio (de grado menor que m_r)

$$Q(X) := \phi_r(X) - \phi_{r-1}(X)^{e_{r-1}f_{r-1}} \in \mathcal{O}[X].$$

Por el corolario de 3.3 y la proposición de 8.4, obtenemos la igualdad $v_r(Q) = e_1\cdots e_{r-1}e_{r-1}f_{r-1}\nu_{r-1}$. Aplicando el lema anterior al polinomio $Q(X)$ deducimos la parte (a).

Escribimos $P(X) = \phi_r(X)^{E_r} + \sum_{j_r=0}^{E_r-1} A_{j_r}(X)\,\phi_r(X)^{j_r}$, con los polinomios $A_{j_r}(X) \in \mathcal{O}[X]$ de grado menor que m_r. Entonces, de nuevo por la proposición 8.4, tenemos que $v_r(A_{j_r}) \geq e_1\cdots e_{r-1}(E_r\nu_r - j_r\nu_r)$. Aplicando ahora el lema anterior a los polinomios $A_{j_r}(X)$ obtenemos la parte (b). □

11.11. Lema. *Con las hipótesis y notaciones anteriores, consideramos un elemento* $\mathbf{j} = (j_0,\dots,j_r) \in \mathbb{N}^{r+1}$.

(a) *Sea* s *un entero tal que* $0 \leq s \leq r-1$. *Entonces*

$$\Phi(j_0,\dots,j_{s-1},j_s + e_sf_s, j_{s+1},\dots,j_r) =$$
$$\pi^{\delta_{\mathbf{j}}^s}\,\Phi(j_0,\dots,j_s,j_{s+1}+1,j_{s+2},\dots,j_r) + \sum_{\mathbf{j}'=(j_0',\dots,j_s',0,\dots,0)\in J} c_{\mathbf{j},\mathbf{j}'}\,\Phi(\mathbf{j}+\mathbf{j}'),$$

con $\delta_{\mathbf{j}}^s \geq 0$ *entero y los* $c_{\mathbf{j},\mathbf{j}'} \in \mathcal{O}$.

(b) *Tenemos que*

$$\Phi(j_0,\dots,j_{r-1},E_r+j_r) = \sum_{\mathbf{j}'\in J} a_{\mathbf{j},\mathbf{j}'}\,\Phi(\mathbf{j}+\mathbf{j}'),$$

con los $a_{\mathbf{j},\mathbf{j}'} \in \mathcal{O}$.

DEMOSTRACIÓN. Ponemos $V_{\mathbf{j}} := j_1\nu_1 + \cdots + j_r\nu_r$. Por la parte (a) del corolario anterior podemos escribir

$$\phi_s(X)^{e_sf_s} = \phi_{s+1}(X) - \sum_{\mathbf{j}'=(j'_0,\ldots,j'_s,0,\ldots,0)\in J} C_{\mathbf{j}'}\,\phi_0(X)^{j'_0}\cdots\phi_s(X)^{j'_s} \qquad (*)$$

con cada $C_{\mathbf{j}'} \in \mathcal{O}$ y $v(C_{\mathbf{j}'}) \geq e_sf_s\nu_s - (j'_1\nu_1 + \cdots + j'_s\nu_s)$; por tanto, cada $c_{\mathbf{j},\mathbf{j}'} := -C_{\mathbf{j}'}/\pi^{[e_sf_s\nu_s+V_{\mathbf{j}}]-[j'_1\nu_1+\cdots+j'_s\nu_s+V_{\mathbf{j}}]} \in \mathcal{O}$. Ahora, remplazando en la definición de $\Phi(j_0,\ldots,j_{s-1},e_sf_s+j_s,j_{s+1},\ldots,j_r)$ el factor $\phi_s(\theta)^{e_sf_s}$ por el segundo miembro de igualdad $(*)$ substituido en $X=\theta$, y teniendo en cuenta que el entero $\delta^s_{\mathbf{j}} := [\nu_{s+1}+V_{\mathbf{j}}] - [e_sf_s\nu_s + V_{\mathbf{j}}]$ no es negativo (pues, por 8.4 es $\nu_{s+1} \geq e_sf_s\nu_s$), obtenemos la parte (a).

La parte (b) se demuestra de la misma manera teniendo en cuenta la parte (b) del corolario anterior. □

DEMOSTRACIÓN (de la proposición de 11.8). Como $\Phi(\mathbf{j})\Phi(\mathbf{j}') = \pi^{\delta}\Phi(\mathbf{j}+\mathbf{j}')$, con $\delta = 0$ o 1, para demostrar que $\mathcal{O}'_L$ es un subanillo será suficiente ver que $\Phi(\mathbf{j}) \in \mathcal{O}'_L$ para todo $\mathbf{j} \in \mathbb{N}^{r+1}$.

Sea s un entero tal que $1 \leq s \leq r$. Comenzamos demostrando por inducción sobre s que, para todo $(j_0,\ldots,j_{s-1}) \in \mathbb{N}^s$ y para todo $(0,\ldots,0,j_s,\ldots,j_r) \in J$, se satifacen las propiedades

(i_s) $\Phi(j_0,\ldots,j_{s-1},j_s,\ldots,j_r) \in \mathcal{O}'_L$.

(ii_s) $\Phi(j_0,\ldots,j_{s-1},e_sf_s,j_{s+1},\ldots,j_r) \in \mathcal{O}'_L$, si $1 \leq s \leq r-1$.

(ii_r) $\Phi(j_0,\ldots,j_{r-1},E_r) \in \mathcal{O}'_L$.

Supongamos que $s=1$. Por la parte (b) del lema anterior, tenemos $\Phi(0,\ldots,0,E_r) \in \mathcal{O}'_L$. De aquí, aplicando reiteradamente la parte (a) del lema anterior, obtenemos que $\Phi(0,e_1f_1,j_2,\ldots,j_r) \in \mathcal{O}'_L$, $\mathcal{O}'_L$ es un $\mathcal{O}[\theta]$-módulo, (i_1) y (ii_1).

Supongamos ahora ciertas (i_{s-1}) y (ii_{s-1}). Si $j_{s-1} < e_{s-1}f_{s-1}$, entonces (i_s) es cierta por (i_{s-1}). Veamos, por inducción sobre $j_{s-1} \geq e_{s-1}f_{s-1}$, que ($\mathrm{i}_s$) es cierta. Si $j_{s-1} = e_{s-1}f_{s-1}$, entonces (i_s) es cierta por (ii_{s-1}). Supongamos que (i_s) es cierta cambiando el entero j_{s-1} por un entero j con $0 \leq j < j_{s-1}$. Entonces, por la parte (b) del lema anterior, $\Phi(j_0,\ldots,j_{s-2},j_{s-1}-e_{s-1}f_{s-1},0,\ldots,0,E_r) \in \mathcal{O}'_L$, y, aplicando la parte (a) del lema anterior, $\Phi(j_0,\ldots,j_{s-2},j_{s-1}-e_{s-1}f_{s-1},e_sf_s,j_{s+1},\ldots,j_r) \in \mathcal{O}'_L$

(si $s \leq r-1$) y (i_s). Además, hemos demostrado también (ii_s).

Finalmente, demostremos que $\Phi(j_0,\ldots,j_{r-1},j_r) \in \mathcal{O}'_L$, para todo $(j_0,\ldots,j_{r-1},j_r) \in \mathbb{N}^{r+1}$. Si $j_r < E_r$, entonces ya está por (i_r). Veamos la propiedad anterior por inducción sobre $j_r \geq E_r$. Si $j_r = E_r$, entonces hemos acabado por (ii_{r-1}). Supongamos que la propiedad anterior es cierta cambiando el entero j_r por un entero j, $0 \leq j < j_r$. Entonces, por la parte (b) del lema anterior, $\Phi(j_0,\ldots,j_{r-1},j_r) \in \mathcal{O}'_L$. □

Ya estamos en condiciones de probar las afirmaciones (a') y (b') a las que habíamos reducido la demostración de la proposición de 11.6.

DEMOSTRACIÓN (de la proposición de 11.6). Por la proposición de 8.4, para todo s, $1 \leq s \leq r$, tenemos que

$$\nu_s = \sum_{i=1}^{s} \frac{e_i f_i \cdots e_s f_s}{e_s f_s} \cdot \frac{h_i}{e_1 \cdots e_i};$$

por tanto, ν_s es un número racional que depende de $e_1,\ldots,e_s$, $f_1,\ldots,f_{s-1}$, $h_1,\ldots,h_s$.

Para cada entero $s \geq 1$, introducimos ahora la función V_s, de $3s-1$ variables, definida por

$$V_s(\mathbf{X}_s,\mathbf{Y}_{s-1},\mathbf{Z}_s) := \sum_{i=1}^{s} \frac{X_i Y_i \cdots X_s Y_s}{X_s Y_s} \cdot \frac{Z_i}{X_1 \cdots X_i},$$

donde $\mathbf{T}_s := (T_1,\ldots,T_s)$; así, $V_1(X_1,Z_1) = \dfrac{Z_1}{X_1}$. Observemos que $\nu_s = V_s(\mathbf{e}_s,\mathbf{f}_{s-1},\mathbf{h}_s)$ para $1 \leq s \leq r$. Claramente, para $s \geq 1$, tenemos

$$V_{s+1}(\mathbf{X}_{s+1},\mathbf{Y}_s,\mathbf{Z}_{s+1}) = X_s Y_s\, V_s(\mathbf{X}_s,\mathbf{Y}_{s-1},\mathbf{Z}_s) + \frac{Z_{s+1}}{X_1 \cdots X_{s+1}};$$

o equivalentemente, para $s \geq 2$, tenemos

$$V_s(\mathbf{X}'_s,\mathbf{Y}'_{s-1},\mathbf{Z}'_s) = X_s Y_s\, V_{s-1}(\mathbf{X}'_{s-1},\mathbf{Y}'_{s-2},\mathbf{Z}'_{s-1}) + \frac{Z_{s+1}}{X_2 \cdots X_{s+1}},$$

donde, para $s \geq 1$, $\mathbf{T}'_s := (T_2,\ldots,T_{s+1})$.

Veamos ahora que, para $2 \leq s \leq r$, tenemos

$$V_s(\mathbf{e}_s,\mathbf{f}_{s-1},\mathbf{h}_s) - \frac{m_s}{m_2} f_1 h_1 = \frac{1}{e_1} V_{s-1}(\mathbf{e}'_{s-1},\mathbf{f}'_{s-2},\mathbf{h}'_{s-1}). \qquad (*)$$

En efecto, para $s = 2$ tenemos $V_2(\mathbf{e}_2, \mathbf{f}_1, \mathbf{h}_2) - f_1 h_1 = \dfrac{h_2}{e_1 e_2} = \dfrac{1}{e_1} V_1(e_2, h_2)$. Supuesto cierto para un s, $2 \leq s < r$, entonces

$$\begin{aligned} & V_{s+1}(\mathbf{e}_{s+1}, \mathbf{f}_s, \mathbf{h}_{s+1}) - \frac{m_{s+1}}{m_2} f_1 h_1 \\ &= e_s f_s V_s(\mathbf{e}_s, \mathbf{f}_{s-1}, \mathbf{h}_s) + \frac{h_{s+1}}{e_1 \cdots e_{s+1}} - e_s f_s \frac{m_s}{m_2} f_1 h_1 \\ &= e_s f_s \frac{1}{e_1} V_{s-1}(\mathbf{e}'_{s-1}, \mathbf{f}'_{s-2}, \mathbf{h}'_{s-1}) + \frac{h_{s+1}}{e_1 \cdots e_{s+1}} \\ &= \frac{1}{e_1} V_s(\mathbf{e}'_s, \mathbf{f}'_{s-1}, \mathbf{h}'_s). \end{aligned}$$

Para probar la afirmación (a'), veamos por inducción sobre $r \geq 1$, para todos $\mathbf{e}_r$, $\mathbf{f}_r$, $\mathbf{h}_r$ (con los $h_s, e_s \geq 1$ primos entre si) y para todo a_r que

$$f_0 \sum_{(0, j_1, \ldots, j_r) \in J} \left[\sum_{s=1}^{r} j_s V_s(\mathbf{e}_s, \mathbf{f}_{s-1}, \mathbf{h}_s) \right] = \mathrm{i}_1(P) + \cdots + \mathrm{i}_r(P).$$

Para $r = 1$ ya lo sabemos (cf. observación (2) de 4.7 en capítulo 1). Supongamos ahora que la igualdad anterior es válida para $r - 1$, para todos $\mathbf{e}_{r-1}$, $\mathbf{f}_{r-1}$, $\mathbf{h}_{r-1}$ y para todo a_{r-1}. Escribimos $j_1 = j\, e_1 + k$, con $0 \leq j < f_1$, $0 \leq k < e_1$, y ponemos $k\, h_1 \equiv s_k \pmod{e_1}$, con $0 \leq s_k < e_1$. Entonces la parte entera que aparece en la igualdad que queremos probar se puede escribir como

$$\begin{aligned} &= \left[j\, h_1 + k \frac{h_1}{e_1} + \sum_{s=2}^{r} j_s V_s(\mathbf{e}_s, \mathbf{f}_{s-1}, \mathbf{h}_s) \right] \\ &= \sum_{s=2}^{r} j_s \frac{m_s}{m_2} f_1 h_1 + j\, h_1 + \left[k \frac{h_1}{e_1} + \sum_{s=2}^{r} j_s (V_s(\mathbf{e}_s, \mathbf{f}_{s-1}, \mathbf{h}_s) - \frac{m_s}{m_2} f_1 h_1) \right] \\ &= \sum_{s=2}^{r} j_s \frac{m_s}{m_2} f_1 h_1 + j\, h_1 + \left[k \frac{h_1}{e_1} + \frac{1}{e_1} \sum_{s=2}^{r} j_s V_{s-1}(\mathbf{e}'_{s-1}, \mathbf{f}'_{s-2}, \mathbf{h}'_{s-1}) \right] \\ &= \sum_{s=2}^{r} j_s \frac{m_s}{m_2} f_1 h_1 + j\, h_1 + \left[k \frac{h_1}{e_1} \right] + \left[\frac{s_k}{e_1} + \frac{1}{e_1} \sum_{s=2}^{r} j_s V_{s-1}(\mathbf{e}'_{s-1}, \mathbf{f}'_{s-2}, \mathbf{h}'_{s-1}) \right], \end{aligned}$$

donde la penúltima igualdad se obtiene de la igualdad (*) anterior. Por consiguiente, nos bastará con ver las igualdades

$$f_0 \sum_{j, k, j_2, \ldots, j_r} \Big(\sum_{s=2}^{r} j_s \frac{m_s}{m_2} f_1 h_1 + j\, h_1 + \left[k \frac{h_1}{e_1} \right] \Big) = \mathrm{i}_1(P), \tag{1}$$

$$f_0 \sum_{j,k,j_2,\dots,j_r} \left[\frac{s_k}{e_1} + \frac{1}{e_1} \sum_{s=1}^{r-1} j_{s+1} V_s(\mathbf{e}'_s, \mathbf{f}'_{s-1}, \mathbf{h}'_s) \right] = \mathrm{i}_2(P) + \cdots + \mathrm{i}_r(P), \quad (2)$$

donde las sumas anteriores están extendidas sobre los índices $j, k, j_2, \cdots, j_r$ tales que $0 \leq j < f_1$, $0 \leq k < e_1$, $(0, 0, j_2, \cdots, j_r) \in J$.

Para ver la igualdad de (1), observemos primeramente que para cada $(0, 0, j_2, \cdots, j_r) \in J$ se satisface

$$0 \leq \sum_{s=2}^{r} j_s \frac{m_s}{m_2} < \frac{m_r}{m_2} e_r f_r a_r = e_2 f_2 \cdots e_r f_r a_r = a_1;$$

y recíprocamente, cualquier entero l, con $0 \leq l < a_1$, puede ser escrito en forma única en la forma $l = \sum_{s=2}^{r} j_s \frac{m_s}{m_2}$, con $(0, 0, j_2, \cdots, j_r) \in J$. Por consiguiente, el primer miembro de la igualdad de (1) es igual a

$$\begin{aligned}
&= f_0 \sum_{j=0}^{f_1-1} \sum_{k=0}^{e_1-1} \sum_{l=0}^{a_1-1} (l\, f_1 h_1 + j\, h_1 + \left[k \frac{h_1}{e_1} \right]) \\
&= f_0 e_1 h_1 \sum_{j=0}^{f_1-1} \sum_{l=0}^{a_1-1} (l\, f_1 + j) + f_0 f_1 a_1 \sum_{k=0}^{e_1-1} \left[k \frac{h_1}{e_1} \right] \\
&= \frac{1}{2} f_0 e_1 h_1 f_1 a_1 (f_1 a_1 - 1) + \frac{1}{2} f_0 f_1 a_1 (e_1 h_1 - e_1 - h_1 + 1) \\
&= \mathrm{i}_1(P).
\end{aligned}$$

Veamos la igualdad de (2). Como el conjunto $\{s_k : 0 \leq k < e_1\} = \{0, 1, \dots, e_1 - 1\}$ (tal vez en distinto orden), el primer miembro de la igualdad de (2) es igual a

$$\begin{aligned}
&= f_0 f_1 \sum_{(0,0,j_2,\dots,j_r) \in J} \sum_{k=0}^{e_1-1} \left[\frac{k}{e_1} + \frac{1}{e_1} \sum_{s=1}^{r-1} j_{s+1} V_s(\mathbf{e}'_s, \mathbf{f}'_{s-1}, \mathbf{h}'_s) \right] \\
&= f_0 f_1 \sum_{(0,0,j_2,\dots,j_r) \in J} \left[\sum_{s=1}^{r-1} j_{s+1} V_s(\mathbf{e}'_s, \mathbf{f}'_{s-1}, \mathbf{h}'_s) \right] \\
&= \mathrm{i}_2(P) + \cdots + \mathrm{i}_r(P),
\end{aligned}$$

donde la penúltima igualdad se obtiene por el lema de 11.7 y la última por la hipótesis de inducción, para $\mathbf{e}'_{r-1}$, $\mathbf{f}'_{r-1}$, $\mathbf{h}'_{r-1}$ y para a_r. Con esto queda probado la afirmación (a') y, por tanto, la parte (a) de la proposición.

Antes de demostrar la afirmación (b'), veremos algunas propiedades de los enteros $\Phi(\mathbf{j})$, $\mathbf{j} \in J$.

Consideramos el conjunto $J_0 := \{\mathbf{j} \in J : v(\Phi(\mathbf{j})) = 0\}$. Nos interesará tener una descripción explícita del conjunto J_0. Sea $\mathbf{j} = (j_0, \ldots, j_r) \in J$. Definimos el entero

$$\lambda_{\mathbf{j}} := e_1 \cdots e_r \sum_{t=1}^{r} j_t \nu_t = \sum_{i=1}^{r} (\sum_{t=i}^{r} j_t e_i f_i \cdots e_{t-1} f_{t-1}) e_{i+1} \cdots e_r h_i,$$

y ponemos $\lambda_{\mathbf{j}} \equiv \mu_{\mathbf{j}} \pmod{e_1 \cdots e_r}$, con $0 \leq \mu_{\mathbf{j}} < e_1 \cdots e_r$; así, $v(\Phi(\mathbf{j})) = \dfrac{\mu_{\mathbf{j}}}{e_1 \cdots e_r}$. Para cada entero s, con $1 \leq s \leq r$, definimos el entero

$$\lambda_{\mathbf{j},s} := j_s h_s e_{s+1} \cdots e_r + \sum_{i=s+1}^{r} (\sum_{t=i}^{r} j_t e_i f_i \cdots e_{t-1} f_{t-1}) e_{i+1} \cdots e_r h_i;$$

por tanto, $\lambda_{\mathbf{j},s}$ depende sólo de $j_s, \ldots, j_r$, y $\lambda_{\mathbf{j}} \equiv \lambda_{\mathbf{j},s} \pmod{e_s \cdots e_r}$. Observemos que

$$\lambda_{\mathbf{j},s} = j_s h_s e_{s+1} \cdots e_r + (\sum_{t=s+2}^{r} j_t e_{s+1} f_{s+1} \cdots e_{t-1} f_{t-1}) e_{s+2} \cdots e_r h_{s+1} + \lambda_{\mathbf{j},s+1}$$

para cada s, $1 \leq s < r$. Por consiguiente, tenemos que

$$\begin{aligned}
\mathbf{j} \in J_0 &\iff \lambda_{\mathbf{j}} \equiv 0 \pmod{e_1 \cdots e_r}, \\
&\iff \lambda_{\mathbf{j},s} \equiv 0 \pmod{e_s \cdots e_r}, \text{ para } 1 \leq s \leq r, \\
&\iff \frac{\lambda_{\mathbf{j},s}}{e_{s+1} \cdots e_r} \equiv 0 \pmod{e_s}, \text{ para } 1 \leq s \leq r, \\
&\iff \mathbf{j} \text{ satisface el sistema } \Lambda,
\end{aligned}$$

donde

$$\Lambda \begin{cases} j_r h_r \equiv 0 \pmod{e_r}, \\ j_s h_s + (\sum_{t=s+2}^{r} j_t e_{s+1} f_{s+1} \cdots e_{t-1} f_{t-1}) \dfrac{h_{s+1}}{e_{s+1}} + \dfrac{\lambda_{\mathbf{j},s+1}}{e_{s+1} \cdots e_r} \equiv 0 \pmod{e_s} \\ \text{para } 1 \leq s < r. \end{cases}$$

En particular, tenemos que $\#J_0 = f_0 \ldots f_r a_r$.

Consideramos ahora los subconjuntos de J

$$\begin{aligned}
K &:= \{\mathbf{k} \in \mathbb{N}^{r+1} : 0 \leq k_s < f_s \text{ para } 0 \leq s < r, 0 \leq k_r < f_r a_r\}, \\
J' &:= \{\mathbf{j}' \in \mathbb{N}^{r+1} : 0 \leq j'_s < e_s \text{ para } 0 \leq s \leq r\}.
\end{aligned}$$

Claramente $\#\mathcal{K} = f_0 \dots f_r a_r$, $\#J' = e_1 \dots e_r$ y $J' \cap J_0 = \{(0,\dots,0)\}$. Analizando el sistema anterior Λ, vemos que para todo $\mathbf{k} \in \mathcal{K}$ existe un único $\mathbf{j}'(\mathbf{k}) = (j_0'(\mathbf{k}),\dots,j_r'(\mathbf{k})) \in J'$ tal que $(j_0'(\mathbf{k}) + e_0k_0,\dots,j_r'(\mathbf{k}) + e_rk_r) \in J_0$; además, $j_0'(\mathbf{k}) = j_r'(\mathbf{k}) = 0$, y $j_s'(\mathbf{k})$ depende sólo de $k_{s+1},\dots,k_r$, para $1 \le s \le r-1$. Y recíprocamente, cualquier $\mathbf{j} \in J_0$ se puede escribir en la forma $\mathbf{j} = \mathbf{j}'(\mathbf{k}) + \mathbf{e}\cdot\mathbf{k}$ (con las operaciones definidas coordenada a coordenada) para algún (único) $\mathbf{k} \in \mathcal{K}$. Por tanto, tenemos la igualdad $J_0 = \{\mathbf{j}'(\mathbf{k}) + \mathbf{e}\cdot\mathbf{k} : \mathbf{k} \in \mathcal{K}\}$.

Veamos ahora las propiedades siguientes

(i) Para todo $\mathbf{j} = \mathbf{j}'(\mathbf{k}) + \mathbf{e}\cdot\mathbf{k} \in J_0$ existen $r-1$ enteros $i_1',\cdots,i_{r-1}'$, donde cada entero i_s' depende sólo de $k_{s+1},\dots,k_r$, tales que

$$\Phi(\mathbf{j}) = \gamma_0(\theta)^{k_0}\cdots\gamma_r(\theta)^{k_r}\cdot\gamma_1(\theta)^{i_1'}\cdots\gamma_{r-1}(\theta)^{i_{r-1}'}.$$

(ii) $\{v(\Phi(\mathbf{j}')) : \mathbf{j}' \in J'\} = \{0, \dfrac{1}{e_1\cdots e_r},\dots,\dfrac{e_1\cdots e_r - 1}{e_1\cdots e_r}\}$.

Comenzemos viendo la propiedad (i). Observemos que el elemento $c(k_2,\dots,k_r) := \Phi(\mathbf{j})\gamma_0(\theta)^{-k_0}\cdots\gamma_r(\theta)^{-k_r} \in \mathcal{O}_L$ tiene valor cero, y puede ser escrito en la forma $\pi^i\phi_1(\theta)^{i_1}\cdots\phi_{r-1}(\theta)^{i_{r-1}}$, para ciertos enteros $i = i(k_2,\dots,k_r), i_1 = i_1(k_2,\dots,k_r),\dots,i_{r-1} = i_{r-1}(k_r)$. Por inducción vemos que $c(k_2,\dots,k_r) = \gamma_1(\theta)^{i_1'}\cdots\gamma_{r-1}(\theta)^{i_{r-1}'}$, para ciertos enteros $i_1' = i_1'(k_2,\dots,k_r),\dots,i_{r-1}' = i_{r-1}'(k_r)$.

Para ver la propiedad (ii), desde luego bastará con ver que si tenemos $v(\Phi(\mathbf{j})) = v(\Phi(\mathbf{j}'))$, con $\mathbf{j},\mathbf{j}' \in J'$, entonces $\mathbf{j} = \mathbf{j}'$. La hipótesis nos dice $\mu_{\mathbf{j}} = \mu_{\mathbf{j}'}$; es decir, $\lambda_{\mathbf{j}} \equiv \lambda_{\mathbf{j}'} \pmod{e_1\cdots e_r}$. Por tanto, $\mathbf{j}-\mathbf{j}'$ ha de satisfacer el sistema Λ; lo cual nos dá $j_s - j_s' = 0$ para todo s, $1 \le s \le r$.

Para terminar, demostremos la afirmación (b'); con lo cual quedará probada la parte (b) de la proposición. Supongamos que $a_r = 1$, y veamos que $\mathcal{O}_L = \mathcal{O}_L'$. Por la parte (b) del corolario de 9.3, tenemos las igualdades $e(L/K) = e_1\cdots e_r$, $f(L/K) = f_0\cdots f_r$. Las propiedades (i) y (ii) anteriores nos dicen que el conjunto $\{\overline{\Phi(\mathbf{j})} : \mathbf{j} \in J_0\}$ es una $\mathbb{F}_{q_0}$-base de $\mathbb{F}_L = \mathbb{F}_{q_0}\left(\overline{\gamma_0(\theta)},\dots,\overline{\gamma_r(\theta)}\right)$, y que se tiene la igualdad

$$\{v_L(\Phi(\mathbf{j}')) : \mathbf{j}' \in J'\} = \{0,1,\dots,e(L/K)-1\}.$$

Entonces el sub-$\mathcal{O}$-módulo $\mathcal{O}_L''$ de $\mathcal{O}_L$ generado por el conjunto

$$\{\Phi(\mathbf{j})\,\Phi(\mathbf{j}') : \mathbf{j} \in J_0, \mathbf{j}' \in J'\}$$

ha de ser todo $\mathcal{O}_L$. Por otra parte, puesto que $\mathcal{O}'_L$ es un subanillo de $\mathcal{O}_L$ (cf. proposición de 11.8), tenemos $\mathcal{O}''_L \subseteq \mathcal{O}'_L$. Por consiguiente, $\mathcal{O}_L = \mathcal{O}'_L$, que es lo que queríamos probar. □

De la demostración anterior se obtiene una base de enteros de $\mathcal{O}_L$ y un generador del ideal primo $\mathfrak{p}_L$ cuando el exponente a_r es uno.

11.12. Corolario. *Con las mismas hipótesis y notaciones que en la proposición de* 11.6. *Supongamos que* $a_r = 1$. *Sean* $\theta \in \mathbb{Q}_p^{al}$ *una raíz del polinomio* $P(X)$, *y* $L := K(\theta)$. *Definimos los números racionales*

$$\nu_s := v(\phi_s(\theta)) = \sum_{i=1}^{s} \frac{e_i f_i \cdots e_s f_s}{e_s f_s} \cdot \frac{h_i}{e_1 \cdots e_i}, \quad s = 1, \ldots, r \quad (cf.\ 8.4),$$

los elementos

$$\Phi(\mathbf{j}) := \frac{\phi_0(\theta)^{j_0} \phi_1(\theta)^{j_1} \cdots \phi_r(\theta)^{j_r}}{\pi^{[j_1\nu_1 + \cdots + j_r\nu_r]}} \in \mathcal{O}_L, \quad \mathbf{j} = (j_0, j_1, \ldots, j_r) \in \mathbb{N}^{r+1},$$

y el conjunto

$$J := \{(j_0, j_1, \ldots, j_r) \in \mathbb{N}^{r+1} : 0 \leq j_s < e_s f_s \text{ para } 0 \leq s \leq r\}.$$

Entonces

(a) *El conjunto* $\{\Phi(\mathbf{j}) : \mathbf{j} \in J\}$ *es una* $\mathcal{O}$*-base de* $\mathcal{O}_L$.

(b) *Si la extensión* L/K *es ramificada (es decir, si* $e_1 \ldots e_r > 1$*), se tiene que* $\mathfrak{p}_L = \Phi(\mathbf{j})\,\mathcal{O}_L$ *para cualquier* $\mathbf{j} \in \mathbb{N}^{r+1}$ *que satisfaga la igualdad* $e_1 \cdots e_r v(\Phi(\mathbf{j})) = 1$ *(en la demostración de* 11.6 *se ha visto que siempre existe al menos un* $\mathbf{j}$ *de estos).* □

Finalmente, probemos el teorema del índice en orden r para cualquier polinomio.

DEMOSTRACIÓN (del teorema de 11.4). Procedemos por inducción sobre el cardinal del conjunto finito $\mathbf{t}_{r-1}(P)$. Supongamos primero que $\mathbf{t}_{r-1}(P)$ es vacio. Entonces el entero $\mathrm{i}_r(P) = 0$ y para cada tipo $\mathbf{t}_{r-2} \in \mathbf{t}_{r-2}(P)$ el polígono $\mathbf{N}^0_{r-1}(P)$ se reduce a un solo punto. Aplicando la parte (b) de este teorema en orden $r-1$ se obtiene que $\mathrm{i}(P) = \mathrm{i}_1(P) + \cdots + \mathrm{i}_{r-1}(P)$, lo que prueba el teorema.

Supongamos ahora que $\mathbf{t}_{r-1}(P)$ es no vacio, y que el teorema es válido para cualquier polinomio cuyo conjunto de tipos de orden $r-1$ tenga menos elementos que $\mathbf{t}_{r-1}(P)$. Sean $\mathbf{t}_{r-1} \in \mathbf{t}_{r-1}(P)$, y $\alpha := v_{\phi_r}(P) = 0$ ó 1. Por el teorema del polígono, tenemos una factorización de la forma

$$P(X) = \phi_r(X)^{\alpha} P_{r,1}(X) \cdots P_{r,g}(X) \cdot R(X),$$

donde cada polinomio $P_{r,i}(X) \in \mathcal{O}[X]$ es mónico, con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$, no divisible por $\phi_r(X)$, cuyo polígono en orden r consta de un único lado $S'_{r,i}$, con los mismos datos que $S_{r,i}$, y cuyo polinomio asociado (en orden r) es $(P_{r,i})_{S'_{r,i}}(Y) = c_i P_{S_{r,i}}(Y)$ $(c_i \in \mathbb{F}_{q_r}^*)$, y donde el polinomio $R(X) \in \mathcal{O}[X]$ y $\omega_r(R) = 0$; luego, $\mathbf{t}_{r-1} \notin \mathbf{t}_{r-1}(R)$.

Descomponemos el índice $\mathrm{i}(P)$ en sumandos según nos marca la factorización anterior (cf. observación (1) de 4.2 del capítulo 1). Por el teorema de la resultante de la sección anterior tenemos calculados los sumandos donde interviene ésta. Por la parte (b) del presente teorema en orden $r-1$, también tenemos computado $\mathrm{i}(\phi_r)$. Del teorema del polinomio asociado, la proposición de 11.6 y la parte (b) del teorema de la resultante, se deduce que para cada polinomio $P_{r,i}(X)$ se satisface la desigualdad de la parte (a), y que si $P_{S_{r,i}}(Y)$ no tiene raíces múltiples entonces hay igualdad. Ahora ya sólo nos queda por mirar el índice $\mathrm{i}(R)$. Por nuestra hipótesis de inducción, sabemos que para $R(X)$ el teorema es cierto, puesto que en $\mathbf{t}_{r-1}(R)$ hay un tipo menos que en $\mathbf{t}_{r-1}(P)$ (a saber, $\{\mathbf{t}_{r-1}\}$). Una simple comprobación nos proporciona ya el teorema. □

CAPÍTULO 3

Descomposición de números primos

En este capítulo aplicamos la teoría de los polígonos de Newton de orden superior, expuesta en el capítulo anterior, a desarrollar un algoritmo eficiente que permite computar la descomposición de los primos racionales en un cuerpo de números dado por una ecuación definidora arbitraria.

§1. Introducción

A lo largo de este capítulo consideraremos fijado un primo $p \in \mathbb{Z}$, y denotaremos por $\mathbb{Q}^{al}$ y $\mathbb{Q}_p^{al}$ a clausuras algebraicas fijadas de $\mathbb{Q}$ y $\mathbb{Q}_p$, respectivamente. Sean $F(X) \in \mathbb{Z}[X]$ un polinomio mónico e irreducible, $\theta \in \mathbb{Q}^{al}$ una raíz de $F(X)$, $K := \mathbb{Q}(\theta)$ y $\mathcal{O}$ su anillo de enteros.

Partiendo del polinomio $F(X)$ y del primo p, nuestros objetivos en este capítulo son los siguientes:

(a) Determinar el tipo de descomposición de p en K

$$p\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} .$$

(b) Determinar generadores de los ideales primos $\mathfrak{p}_i$.

(c) Determinar la valoración p-ádica del discriminante absoluto $\Delta(K)$ del cuerpo de números K.

En la sección 3 daremos un algoritmo para determinar el tipo de descomposición de p en K, que nos permitirá obtener también la valoración p-ádica de $\Delta(K)$. En la sección 5 determinaremos dos generadores de cada ideal primo $\mathfrak{p}_i$. La última sección está dedicada a ejemplos.

§2. Determinación de buenos representantes

En esta sección denotaremos provisionalmente por K a una extensión finita de $\mathbb{Q}_p$ y por $\mathcal{O}$ a su anillo de enteros. Usaremos las notaciones introducidas en el capítulo anterior.

Dado un tipo $\mathbf{t}_{r-1}$ de orden $r-1$ y un polinomio $P(X) \in \mathcal{O}[X]$, sabemos que el polígono de Newton $\mathbf{N}_{(v_r,\phi_r)}(P)$ depende del "representante" $\phi_r(X) \in \mathcal{O}[X]$ que hayamos elegido del tipo $\mathbf{t}_{r-1}$; por tanto, la información que nos proporcionan los teoremas del polígono y del polinomio asociado depende de esta elección (cf. observación (2) de 1.3 en capítulo 1). En esta sección estudiaremos un procedimiento para elegir este representante $\phi_r(X)$ de manera optimal. La filosofía de esta estrategia es la de obtener en un determinado nivel la máxima información posible antes de verse obligados a cambiar de nivel. Con eso se consigue evitar en gran parte la recursividad del algoritmo y agilizar su rendimiento.

Consideremos un polinomio mónico $P(X) \in \mathcal{O}[X]$, un entero $r \geq 1$ y un tipo $\mathbf{t}_r = (\mathbf{t}_{r-1}; h_r/e_r, \psi_r) \in \mathbf{t}_r(P)$. Se tiene pues elegido un polinomio $\phi_r(X) \in \mathcal{O}[X]$ mónico, de grado m_r y con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$, y los datos $-h_r/e_r$, $\psi_r(Y)$ corresponden a la pendiente de un lado del polígono $\mathbf{N}^0_{(v_r,\phi_r)}(P)$ y a un factor irreducible de su polinomio asociado (en orden r), respectivamente. Sean $Q(X) \in \mathcal{O}[X]$ el factor de $P(X)$ correspondiente al tipo $\mathbf{t}_r$ dado por el teorema del polinomio asociado, $\theta \in \mathbb{Q}_p^{al}$ una raíz cualquiera de $Q(X)$, y $\sigma = \sigma_\theta \in \mathrm{Gal}(\mathbb{F}_{q_r}/\mathbb{F}_{q_0})$ el único automorfimo tal que $\sigma(\zeta_s) = \overline{\gamma_s(\theta)}$ para $0 \leq s \leq r-1$ (cf. §7 del capítulo anterior). Por 3.3 (c) del capítulo 2, sabemos que $\nu := v_r(\phi_r)$ sólo depende del tipo $\mathbf{t}_{r-1}$. Por 9.1 y 8.1 del capítulo anterior, sabemos que el polígono $\mathbf{N}_{(v_r,\phi_r)}(Q)$ consta de un solo lado T, con pendiente $-h_r/e_r$, cuyo polinomio asociado (en orden r) $Q_T(Y)$ es (salvo constante) igual a $\psi_r(Y)^{a_r}$, y que

$$e_1 \cdots e_{r-1} v(\phi_r(\theta)) = \nu + \frac{h_r}{e_r}, \quad v(\gamma_r(\theta)) = 0, \quad \psi_r^\sigma(Y) = \mathrm{Irr}\left(\overline{\gamma_r(\theta)}, \mathbb{F}_{q_r}, Y\right).$$

Además, también sabemos que θ tiene tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$, por 1.3 (b) del capítulo 2.

A continuación, vamos a ver que si $e_r f_r > 1$, entonces no hay ningún otro representante del tipo $\mathbf{t}_{r-1}$ que dé mayor información para este orden

sobre el polinomio $Q(X)$. Sea $\phi'_r(X) \in \mathcal{O}[X]$ otro polinomio mónico, de grado m_r y con tipo de orden $r-1$ igual a $\{\mathbf{t}_{r-1}\}$. Escribimos

$$\phi'_r(X) = \phi_r(X) + M(X), \quad M(X) \in \mathcal{O}[X], \quad \mathrm{gr}(M) < m_r .$$

Por 7.1 (b) del capítulo 2, sabemos que

$$e_1 \cdots e_{r-1} v(M(\theta)) = v_r(M) .$$

Para este representante $\phi'_r(X)$ aplicaremos el superíndice prima ($'$) a las notaciones que utilizamos para $\phi_r(X)$.

2.1. Teorema. *Con las notaciones anteriores, supongamos que $e_r f_r > 1$. Entonces tenemos*

(a) *El polígono $\mathbf{N}_{(v_r,\phi'_r)}(Q)$ consta de un solo lado T', con pendiente $-h'_r/e'_r \geq -h_r/e_r$.*

(b) *El polinomio asociado (en orden r) $Q_{T'}(Y)$, obtenido a partir del desarrollo ϕ'_r-ádico, es (salvo constante) una potencia $\psi'_r(Y)^{a'_r}$ de un polinomio mónico e irreducible $\psi'_r(Y) \in \mathbb{F}_{q_r}[Y]$.*

(c) *Si $h'_r/e'_r < h_r/e_r$, entonces $e'_r = f'_r = 1$.*

Si $h'_r/e'_r = h_r/e_r$, entonces $e'_r = e_r$, $f'_r = f_r$ (luego, $a'_r = a_r$).

Para la demostración de este teorema necesitaremos el siguiente resultado fundamental.

2.2. Proposición. *Si $e_r f_r > 1$, entonces $v(\phi_r(\theta)) \geq v(\phi'_r(\theta))$.*

Para la demostración de esta proposición necesitaremos a su vez un lema en el que intervienen las fracciones racionales del tipo $\Phi(\mathbf{n})(X)$, con $\mathbf{n} = (n_0, n_1, \ldots, n_{r-1}) \in \mathbb{Z}^r$ (cf. §1 del capítulo 2).

2.3. Lema. *Continuamos con las notaciones anteriores. Sea $\mathbf{n} \in \mathbb{Z}^r$ tal que $v(\Phi(\mathbf{n})(\theta)) = v(M(\theta))$, y ponemos $R(X) := M(X)/\Phi(\mathbf{n})(X) \in K(X)$. Entonces $\overline{R(\theta)} \in \mathbb{F}_{q_r}^*$ y el elemento $\sigma_\theta^{-1}\left(\overline{R(\theta)}\right) \in \mathbb{F}_{q_r}^*$ es independiente de la raíz θ de $Q(X)$.*

DEMOSTRACIÓN. Consideremos el conjunto

$$J := \{\mathbf{j} = (j_0, j_1, \ldots, j_{r-1}) \in \mathbb{N}^r : 0 \leq j_s < e_s f_s \text{ para } 0 \leq s \leq r-1\} .$$

Por la proposición de 11.9 del capítulo 2, podemos escribir

$$M(X) = \sum_{\mathbf{j}\in J} \lambda_{\mathbf{j}}\, X^{j_0}\, \Phi(0, j_1, \ldots, j_{r-1})(X)\,,$$

con los $\lambda_{\mathbf{j}} \in \mathcal{O}$ tales que $v(\lambda_{\mathbf{j}}) \geq v(M(\theta)) - v(\Phi(0, j_1, \ldots, j_{r-1})(\theta)) =: \delta_{\mathbf{j}}$. Notemos que el número racional $\delta_{\mathbf{j}}$ no depende de la raíz θ de $Q(X)$ (cf. §7 del capítulo 2). Consideremos ahora el subconjunto

$$J_0 := \{\mathbf{j} \in J : v(\lambda_{\mathbf{j}}) = \delta_{\mathbf{j}}\} \subseteq J\,,$$

y ponemos $\lambda_{\mathbf{j}}^0 := \lambda_{\mathbf{j}}/\pi^{\delta_{\mathbf{j}}} \in \mathcal{O}^*$ para cada $\mathbf{j} \in J_0$. Entonces podemos escribir

$$M(X) = \sum_{\mathbf{j}\in J_0} \lambda_{\mathbf{j}}^0\, X^{j_0}\, \Phi(\delta_{\mathbf{j}}, j_1, \ldots, j_{r-1})(X) + N(X)\,,$$

con $N(X) \in \mathcal{O}[X]$ y $v(N(\theta)) > v(M(\theta)) = v(\Phi(\mathbf{n})(\theta))$. Dividiendo en la anterior expresión de $M(X)$ por $\Phi(\mathbf{n})(X)$ obtenemos la igualdad

$$R(X) = \sum_{\mathbf{j}\in J_0} \lambda_{\mathbf{j}}^0\, X^{j_0}\, \rho(\mathbf{j})(X) + \frac{N(X)}{\Phi(\mathbf{n})(X)}\,, \qquad (*)$$

donde para cada $\mathbf{j} \in J_0$ es

$$\begin{aligned}\rho(\mathbf{j})(X) :&= \frac{\Phi(\delta_{\mathbf{j}}, j_1, \ldots, j_{r-1})(X)}{\Phi(\mathbf{n})(X)} \\ &= \Phi(\delta_{\mathbf{j}} - n_0, j_1 - n_1, \ldots, j_{r-1} - n_{r-1})(X)\,.\end{aligned}$$

Puesto que $v(\rho(\mathbf{j})(\theta)) = \delta_{\mathbf{j}} + v(\Phi(0, j_1, \ldots, j_{r-1})(\theta)) - v(\Phi(\mathbf{n})(\theta)) = 0$, entonces $v_r(\rho(\mathbf{j})) = 0$ (por 7.3 (b) del capítulo 2); por tanto, la fracción $\rho(\mathbf{j})(X)$ puede expresarse como un producto de potencias enteras de las fracciones $\gamma_s(X)$ con $1 \leq s \leq r-1$ (cf. 2.9 del capítulo 2). Substituyendo ahora la indeterminada X por θ en la igualdad $(*)$ y tomando después clases, obtenemos entonces el lema. □

DEMOSTRACIÓN (de la proposición de 2.2). Demostraremos la proposición por contrarrecíproco. Supongamos que $v(\phi_r(\theta)) < v(\phi_r'(\theta))$, y veamos que $e_r = f_r = 1$. En primer lugar, tenemos que $v(M(\theta)) = v(\phi_r(\theta))$ y, multiplicando por $e_1 \cdots e_{r-1}$, que $v_r(M) = \nu + h_r/e_r$; luego, $e_r = 1$, ya que h_r, e_r son primos entre si.

Veamos ahora que $\overline{\gamma_r(\theta)} \in \mathbb{F}_{q_r}$, con lo cual quedará probado que $f_r = 1$. Recordemos que por definición es

$$\gamma_r(X) = \frac{\Phi_r(X)^{e_r}}{\pi_r(X)^{h_r}} = \frac{\phi_r(X)^{e_r}}{\Pi_r(X)^{e_r}\pi_r(X)^{h_r}} = \frac{\phi_r(X)}{\Pi_r(X)\pi_r(X)^{h_r}},$$

y que la fracción racional $\Pi_r(X)\pi_r(X)^{h_r}$ puede ser expresada en la forma $\Phi(\mathbf{n})(X)$ para cierto elemento $\mathbf{n} \in \mathbb{Z}^r$ (cf. §1 del capítulo 2); además, ha de ser $v(\Phi(\mathbf{n})(\theta)) = v(\phi_r(\theta))$, ya que $v(\gamma_r(\theta)) = 0$. Por tanto, tenemos que

$$\frac{\phi_r'(X)}{\Phi(\mathbf{n})(X)} = \gamma_r(X) + R(X), \quad R(X) := \frac{M(X)}{\Phi(\mathbf{n})(X)}.$$

Substituyendo en esta igualdad la X por θ y tomando clases, obtenemos que $\overline{\gamma_r(\theta)} = -\overline{R(\theta)}$, el cual pertenece a $\mathbb{F}_{q_r}$ por el lema de 2.3. □

DEMOSTRACIÓN (del teorema de 2.1). En primer lugar, veamos que el valor $v(\phi_r'(\theta))$ es el mismo para todas las raíces θ de $Q(X)$; con lo cual quedará probada, por 8.1 del capítulo 2 y la proposición de 2.2, la parte (a) del teorema. En efecto, si para alguna raíz θ_0 de $Q(X)$ es $v(\phi_r'(\theta_0)) < v(\phi_r(\theta_0))$, a la fuerza $v(\phi_r'(\theta_0)) = v(M(\theta_0))$ y el resultado es claro, puesto que ya sabemos que los valores $v(\phi_r(\theta))$ y $v(M(\theta))$ no dependen de la raíz θ de $Q(X)$. En caso contrario, por la proposición de 2.2, ha de ser $v(\phi_r'(\theta)) = v(\phi_r(\theta))$ para cada raíz θ de $Q(X)$, y el resultado también es claro por la razón anterior.

En segundo lugar, observemos que ahora tenemos

$$e_1 \cdots e_{r-1} v(\phi_r'(\theta)) = \nu + \frac{h_r'}{e_r'}, \quad v(\gamma_r'(\theta)) = 0,$$

donde $-h_r'/e_r'$ es la pendiente del único lado del polígono $\mathbf{N}_{(v_r,\phi_r')}(Q)$, y donde $\gamma_r'(X) = \dfrac{\Phi_r'(X)^{e_r'}}{\pi_r(X)^{h_r'}} = \dfrac{\phi_r'(X)^{e_r'}}{\Pi_r(X)^{e_r'}\pi_r(X)^{h_r'}}$ es la correspondiente fracción racional obtenida a partir de $\phi_r'(X)$.

Pasemos a probar la parte (b). Por 9.1 del capítulo 2, nos bastará ver que el polinomio irreducible, $\psi_r'(Y)$, obtenido al aplicar el automorfismo σ^{-1} a los coeficientes del polinomio $\mathrm{Irr}\left(\overline{\gamma_r'(\theta)}, \mathbb{F}_{q_r}, Y\right)$ es el mismo para cada raíz θ de $Q(X)$. Para ello distinguiremos dos casos, según que h_r'/e_r' sea menor o igual que h_r/e_r, y demostraremos también la parte (c).

Supongamos primero que $h'_r/e'_r < h_r/e_r$; es decir, que $v(\phi'_r(\theta)) < v(\phi_r(\theta))$. Procediendo como en la demostración de la proposición de 2.2 (intercambiando los papeles de $\phi_r(X)$ y $\phi'_r(X)$), obtenemos que $e'_r = 1$, $\overline{\gamma'_r(\theta)} \in \mathbb{F}_{q_r}$ y el elemento $\sigma^{-1}\left(\overline{\gamma'_r(\theta)}\right)$ es independiente de la raíz θ de $Q(X)$ (por el lema de 2.3). Con esto queda pues probada la parte (b) y que $\psi'_r(Y) = Y - \sigma^{-1}\left(\overline{\gamma'_r(\theta)}\right)$; en particular, es $f'_r = 1$, lo que acaba de demostrar la parte (c).

Supongamos ahora que $h'_r/e'_r = h_r/e_r$; es decir, que $v(\phi'_r(\theta)) = v(\phi_r(\theta))$. Entonces $h'_r = h_r$, $e'_r = e_r$ y $v_r(M) \geq \nu + h_r/e_r$. En este caso distinguiremos a su vez dos subcasos, según que el valor $v_r(M)$ sea igual o mayor que $\nu + h_r/e_r$.

Si $v_r(M) = \nu + h_r/e_r$, entonces $e_r = 1$ y, procediendo de nuevo como en la demostración de 2.2 y aplicando 2.3, obtenemos la igualdad $\overline{\gamma'_r(\theta)} = \overline{\gamma_r(\theta)} + c(\theta)$, para algún elemento $c(\theta) \in \mathbb{F}^*_{q_r}$ tal que $\sigma^{-1}(c(\theta))$ es independiente de la raíz θ de $Q(X)$. Por tanto, obtenemos

$$\operatorname{Irr}\left(\overline{\gamma'_r(\theta)}, \mathbb{F}_{q_r}, Y\right) = \operatorname{Irr}\left(\overline{\gamma_r(\theta)}, \mathbb{F}_{q_r}, Y - c(\theta)\right) = \psi^\sigma_r(Y - c(\theta))\,;$$

lo cual demuestra la parte (b) y que $\psi'_r(Y) = \psi_r(Y - \sigma^{-1}(c(\theta)))$. Así, $f'_r = f_r$ y se termina de probar (c).

Finalmente, si $v_r(M) > \nu + h_r/e_r$ (es decir, si $v(M(\theta)) > v(\phi_r(\theta))$), entonces podemos escribir

$$\phi'_r(X)^{e_r} = \phi_r(X)^{e_r} + N(X)\,,$$

con $N(X) \in \mathcal{O}[X]$ tal que $v(N(\theta)) > v(\phi_r(\theta)^{e_r})$. Entonces, procediendo como antes, obtenemos que $\overline{\gamma'_r(\theta)} = \overline{\gamma_r(\theta)}$; con lo que se obtiene la parte (b) y que $\psi'_r(Y) = \psi_r(Y)$. Luego, $f'_r = f_r$ y se acaba de ver (c).

En todos los casos han quedado pues demostradas las partes (b) y (c) del teorema. □

En cambio, veremos a continuación que cuando el polinomio $P(X)$ no tiene raíces múltiples, $a_r \geq 2$ y $e_r = f_r = 1$, el propio polinomio $\phi_{r+1}(X)$ que construimos a partir del tipo $\mathbf{t}_r$ nos proporciona más información en orden r sobre el polinomio $Q(X)$ que $\phi_r(X)$. Veremos, más concretamente, que el polígono y los polinomios asociados de orden $r+1$ se pueden expresar

en términos del polígono y los polinomios asociados de orden r obtenidos con el polinomio $\phi_{r+1}(X)$. Tendremos pues que los eslabones con $e_r = f_r = 1$ no suben el nivel. En la práctica esto supone, además de ahorrarse algunas operaciones, eliminar en gran parte la recursividad del algoritmo, ya que este caso se da siempre antes de saltar de nivel (cf. teorema de 2.1).

Supongamos ahora que $e_r = f_r = 1$. Entonces el polinomio

$$\phi'_r(X) := \phi_{r+1}(X)$$

es un polinomio mónico, de grado $m_{r+1} = m_r$ y tiene tipo de orden $r-1$ igual a $\mathbf{t}_{r-1}$; es decir, este polinomio también es un representante de grado mínimo del tipo $\mathbf{t}_{r-1}$. En este caso tenemos pues definido el polígono de Newton (en orden r) $\mathrm{N}_{(v_r,\phi'_r)}(P)$, y podemos considerar el polígono, que denotaremos por $\mathrm{N}^{h_r}_{(v_r,\phi'_r)}(P)$, obtenido al quedarse sólo con los lados con pendiente menor que $-h_r$ de $\mathrm{N}_{(v_r,\phi'_r)}(P)$. Además, el entero fijado l_r es arbitrario (luego, podemos tomar $l_r = 0$ cuando convenga), y el polinomio $\psi_r(Y) = Y - \zeta_r$ (cf. §1 del capítulo 2).

Sea $\mathfrak{H} : \mathbb{R}^2 \to \mathbb{R}^2$ la afinidad del plano euclideo definida por

$$\mathfrak{H}(x,y) := (x, y - h_r x), \qquad (x,y) \in \mathbb{R}^2 .$$

Observemos que la afinidad $\mathfrak{H}$ deja fijas las rectas verticales y que su restricción a cada una de estas rectas es una traslación.

2.4. Proposición. *Supongamos que $e_r = f_r = 1$. Sean $h, e \geq 1$ enteros primos entre si, y S el segmento con pendiete $-h/e$ del polígono (en orden $r+1$) $\mathrm{N}_{(v_{r+1},\phi_{r+1})}(P)$. Entonces*

(a) *$S' := \mathfrak{H}(S)$ es el segmento con pendiente $-(h_r + h/e)$ del polígono $\mathrm{N}_{(v_r,\phi'_r)}(P)$.*

Por tanto, $\mathrm{N}^{h_r}_{(v_r,\phi'_r)}(P) = \mathfrak{H}(\mathrm{N}^0_{(v_{r+1},\phi_{r+1})}(P))$ (ver figura 3.1).

(b) *$P_{S'}(Y) = \zeta_r^{l_r\beta} P_S(\zeta_r^{-l_r h} Y)$, en $\mathbb{F}_{q_r}[Y]$, donde $P_{S'}(Y)$ (resp. $P_S(Y)$) indica el polinomio asociado en orden r (resp. en orden $r+1$) y β es la ordenada del origen de S.*

(c) *El entero* $\mathrm{i}^0_{\mathrm{t}_r}(P)$, *definido a partir de los datos de los lados del polígono* $\mathrm{N}^0_{(v_{r+1},\phi_{r+1})}(P)$ *(cf. definición* 11.1 *del capítulo* 2*), es igual al número de puntos de coordenadas enteras del recinto acotado delimitado por el polígono* $\mathrm{N}^{h_r}_{(v_r,\phi'_r)}(P)$, *la recta con pendiente* $-h_r$ *que pasa por el punto* $(0, v_{r+1}(P))$ *(es decir, la recta que contiene al lado con pendiente* $-h_r$ *de* $\mathrm{N}^0_{(v_r,\phi_r)}(P)$*) y la recta vertical de ecuación* $x = v_{\phi'_r}(P)$, *incluyendo los puntos que están sobre los lados de este polígono, excepto el origen del primer lado y el final del último lado, y excluyendo los puntos que están sobre estas rectas. Además, el entero* $\epsilon_{\mathrm{t}_r}(P)$ *es igual a* $v_{\phi'_r}(P)$ *veces el número de puntos de coordenadas enteras de este recinto que estan sobre esta recta vertical excluyendo el punto de menor ordenada.*

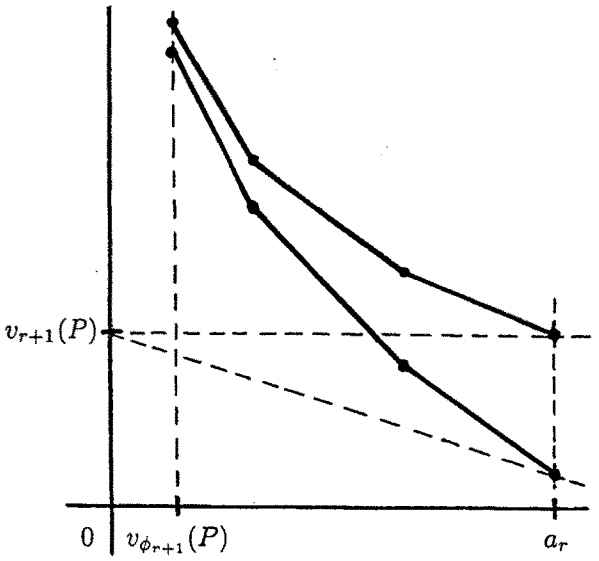


Figura 3.1. $\mathrm{N}^{h_r}_{(v_r,\phi'_r)}(P)$ y $\mathrm{N}^0_{(v_{r+1},\phi_{r+1})}(P)$.

DEMOSTRACIÓN. Sea $P(X) = \sum A_i(X)\,\phi_{r+1}(X)^i$ el desarrollo ϕ_{r+1}-ádico de $P(X)$ Por 2.2 (b) y 3.5 del capítulo 2 tenemos $v_{r+1}(A_i) = v_r(A_i)$ y $v_{r+1}(\phi_{r+1}) = v_r(\phi'_r) + h_r$. Luego, $v_{r+1}(A_i\,{\phi_{r+1}}^i) = v_r(A_i\,{\phi'_r}^i) + ih_r$; es decir, el diagrama de Newton $\mathbf{D}_{(v_r,\phi'_r)}(P) = \mathfrak{H}(\mathbf{D}_{(v_{r+1},\phi_{r+1})}(P))$. Además, si (α, β), $(\alpha + de, \beta - dh)$ son el origen y final, respectivamente, del segmento S, entonces $(\alpha, \beta - h_r\alpha)$, $(\alpha + de, \beta - h_r\alpha - d(h_re + h))$ son el origen y final, respectivamente, del segmento S'. Por tanto, S' es el segmento con pen-

diente $-(h_r + h/e)$ del polígono $\mathrm{N}_{(v_r,\phi'_r)}(P)$, por la propiedad mencionada anteriormente de la afinidad $\mathfrak{H}$; con lo que obtenemos la parte (a).

A partir de la definición del polinomio asociado (cf. 4.3 del capítulo 2) se comprueba ahora sin dificultad la parte (b).

Finalmente, la parte (c) se obtiene de la propiedad anterior de $\mathfrak{H}$, observando que un punto $(x, y) \in \mathbb{R}^2$ es de coordenadas enteras si y sólo si su imagen $\mathfrak{H}(x, y)$ también lo es. □

Supongamos finalmente que $P(X)$ no tiene raíces múltiples, $a_r \geq 2$ y $e_r = f_r = 1$. Entonces por la proposición anterior queda claro que el polinomio $\phi'_r(X)$ nos da más información sobre $Q(X)$ que $\phi_r(X)$. En efecto, en el peor de los casos en que se tenga $v_{\phi'_r}(P) = 0$, el polígono $\mathrm{N}^{h_r}_{(v_r,\phi'_r)}(P)$ conste un solo lado, cuya pendiente sea entera, y su polinomio asociado sea potencia de un polinomio irreducible de grado uno, tendríamos que el entero $\mathrm{i}_{\mathbf{t}_r}(P) = f_0 \cdots f_{r-1} \cdot \mathrm{i}^0_{\mathbf{t}_r}(P)$ es positivo (cf. 11.2 (1) del capítulo 2), y por el teorema del índice estaríamos más cerca de factorizar $Q(X)$ (cf. 11.4 y 11.5 del capítulo 2).

Además, en el peor de los casos citado anteriormente, tenemos que el polinomio $\phi'_r(X)$ nos proporciona un tipo $\mathbf{t}'_r = (\mathbf{t}_{r-1}; h'_r/e'_r, \psi'_r)$ de orden r con $h'_r > h_r$, $e'_r = f'_r = 1$ y el correspondiente entero $a'_r = a_r \geq 2$. En este caso, de nuevo podemos obtener más información en orden r sobre $Q(X)$, remplazando ahora el polinomio $\phi'_r(X)$ por el polinomio $\phi''_r(X) := \phi'_{r+1}(X)$ que construimos a partir del tipo $\mathbf{t}'_r$, y pasando a trabajar con el polígono $\mathrm{N}^{h'_r}_{(v_r,\phi''_r)}(P)$. Pues bien, por el teorema del índice, no podemos permanecer indefinidamente en el peor de los casos al repetir el proceso anterior. Por consiguiente, en un número finito de pasos con este procedimiento llegamos a obtener, si no hemos acabado de factorizar $Q(X)$, al menos un representante de grado mínimo del tipo $\mathbf{t}_{r-1}$, un lado de su polígono de Newton y un factor irreducible de su polinomio asociado para los cuales se tiene $a_r \geq 2$ y $e_r f_r > 1$. Así, para el correspondiente factor de $Q(X)$ dado por el teorema del polinomio asociado, ya no podremos obtener más información en orden r con otro representante (cf. teorema de 2.1).

§3. Determinación del tipo de descomposición

En esta sección presentamos el algoritmo obtenido con el método de los polígonos de Newton de orden superior para computar el tipo de descomposición de primos racionales en cuerpos de números. Para ejecutar este algoritmo debe usarse un algoritmo de factorización de polinomios sobre cuerpos finitos; por ejemplo, el determinístico de Berlekamp dado en **[Be 70]** o el probabilístico de Cantor y Zassenhauss de **[Ca-Za 81]**.

Este algoritmo no necesita tener calculada de antemano una base p-minimal (siendo p el primo a descomponer) del cuerpo con el que se trabaja, como, en cambio, sí necesita para su ejecución el algoritmo obtenido con el método de Buchmann y Lenstra (cf. **[Bu-Le]**, **[Co 95]**). Desde luego, una tal base puede ser computada, por ejemplo, con una combinación de las rutinas 2 y 4 de Zassenhauss (cf. **[Po-Za 89]**, **[Po 93]**). Sin embargo, en general esta obtención es costosa en la práctica cuando se trabaja con cuerpos de números de grado alto.

El algoritmo fue implementado por J. Guàrdia en el paquete *Newton* para *Mathematica*, basandose en el paquete *FF (Finite Fields)* del mismo autor. Los detalles de la implementación se encuentran en **[Gu 98]**. Ambos paquetes se pueden obtener mediante ftp anónimo en las direcciones **drac.mat.ub.es/pub/Newton** y **drac.mat.ub.es/pub/FF**.

Aunque no se ha hecho un estudio de la complejidad del algoritmo, experimentalmente se ha comprobado la eficiencia del mismo con polinomios de grado alto (cf. §6).

3.1. Algoritmo. Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números dado por un entero algebráico θ que es raíz de un polinomio mónico e irreducible $F(X) \in \mathbb{Z}[X]$, y sea $\mathcal{O}$ el anillo de enteros de K. Sean $p \in \mathbb{Z}$ un número primo y

$$p\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

su descomposición en $\mathcal{O}$. El algoritmo descrito a continuación computa el número g de ideales primos de $\mathcal{O}$ que dividen a p, los índices de ramificación $e_i = e(\mathfrak{p}_i/p)$ y los grados residuales $f(\mathfrak{p}_i/p)$.

Paso 0 (nivel 0)

Sea $\overline{F}(Y) = \psi_{0,1}(Y)^{a_{0,1}} \cdots \psi_{0,g_0}(Y)^{a_{0,g_0}}$ la factorización de $\overline{F}(Y)$ en $\mathbb{F}_p[Y]$. Para cada i, $1 \leq i \leq g_0$, sea $\phi_{1,i}(X) \in \mathbb{Z}[X]$ un polinomio mónico tal que $\overline{\phi_{1,i}}(Y) = \psi_{0,i}(Y)$, y pongamos $f_{0,i} := \psi_{0,i}(Y)$. Sea $G(X)$ el polinomio definido por $G(X) := \frac{1}{p}(F(X) - \phi_{1,1}(X)^{a_{0,1}} \cdots \phi_{1,g_0}(X)^{a_{0,g_0}}) \in \mathbb{Z}[X]$. De los resultados de Kummer, Dedekind y Hensel se obtiene una primera descomposición del ideal $p\mathcal{O}$. Concretamente, se tiene

(a) $p\mathcal{O} = \mathfrak{b}_{0,1} \cdots \mathfrak{b}_{0,g_0}$, donde cada $\mathfrak{b}_{0,i} := p\mathcal{O} + \phi_{1,i}(\theta)^{a_{0,i}}\mathcal{O}$. Además, los ideales $\mathfrak{b}_{0,i}$ son coprimos dos a dos, y el grado $f_{0,i}$ divide a $f(\mathfrak{p}/p)$ para cada ideal primo $\mathfrak{p}$ de $\mathcal{O}$ que divide al ideal $\mathfrak{b}_{0,i}$.

(b) Consideremos un i fijo. Si $a_{0,i} = 1$ o si $\psi_{0,i}(Y)$ no divide a $\overline{G}(Y)$ en $\mathbb{F}_p[Y]$, entonces el ideal $\mathfrak{b}_{0,i}$ es una potencia de un ideal primo $\mathfrak{p}_i$, con $e(\mathfrak{p}_i/p) = a_{0,i}$ y $f(\mathfrak{p}_i/p) = f_{0,i}$. Además, $\mathfrak{p}_i = p\mathcal{O} + \phi_{1,i}(\theta)\mathcal{O}$.

Por tanto, hemos de seguir y descomponer el ideal $\mathfrak{b}_{0,i}$ en $\mathcal{O}$ cuando la condición anterior de la parte (b) no se satisface.

Paso 1 (nivel 1)

1.1 Fijemos un i tal que $a_{0,i} \geq 2$ y $\psi_{0,i}(Y)$ divida a $\overline{G}(Y)$ en $\mathbb{F}_p[Y]$. Simplifiquemos las notaciones escribiendo $\mathfrak{b}_0, \psi_0(Y), \phi_1(X), a_0, f_0$ en lugar de $\mathfrak{b}_{0,i}, \psi_{0,i}(Y), \phi_{1,i}(X), a_{0,i}, f_{0,i}$, respectivamente.

Sea v_1 la extensión a $\mathbb{Q}(X)$ de la valoración p-ádica de $\mathbb{Q}$ de forma que $v_1(X) = 0$. Construimos la parte principal, $\mathrm{N}^0_{(v_1,\phi_1)}(F)$, del polígono de Newton de $F(X)$ respecto el par (v_1, ϕ_1) (cf. 1.1 del capítulo 1). Sean $S_{1,1}, \ldots, S_{1,g_1}$ los lados de esta parte principal, y $d_{1,i}, e_{1,i}, h_{1,i}$ los datos asociados a cada lado $S_{1,i}$. Del teorema del polígono de Ore (cf. 3.1 y 3.3 del capítulo 1) se obtiene la descomposición del ideal $\mathfrak{b}_0$ siguiente

(a) $\mathfrak{b}_0 = \mathfrak{a}_{1,1}^{e_{1,1}} \cdots \mathfrak{a}_{1,g_1}^{e_{1,g_1}}$, donde los ideales $\mathfrak{a}_{1,i}$ son coprimos dos a dos.

(b) Consideremos un i fijo. Si $d_{1,i} = 1$, entonces $\mathfrak{a}_{1,i}$ es un ideal primo $\mathfrak{p}_i$, con $e(\mathfrak{p}_i/p) = e_{1,i}$ y $f(\mathfrak{p}_i/p) = f_0$.

Hemos de descomponer pues el ideal $\mathfrak{a}_{1,i}$ si el entero $d_{1,i} \geq 2$.

1.2 Fijemos un i tal que $d_{1,i} \geq 2$. Escribimos $\mathfrak{a}_1, S_1, d_1, e_1, h_1$ en lugar de $\mathfrak{a}_{1,i}, S_{1,i}, d_{1,i}, e_{1,i}, h_{1,i}$, respectivamente, y ponemos $q_1 := p^{f_0}$. Construimos

el polinomio asociado, $F_{S_1}(Y) \in \mathbb{F}_{q_1}[Y]$, al polinomio $F(X)$ y al lado S_1 (cf. 1.4 del capítulo 1). Sea $F_{S_1}(Y) = c_1\,\psi_{1,1}(Y)^{a_{1,1}} \cdots \psi_{1,g_1'}(Y)^{a_{1,g_1'}}$ la factorización de $F_{S_1}(Y)$ en $\mathbb{F}_{q_1}[Y]$, y ponemos $f_{1,i} := \mathrm{gr}(\psi_{1,i})$. Del teorema del polinomio asociado de Ore (cf. 3.5 y 3.7 del capítulo 1) se obtiene ahora una descomposición del ideal $\mathfrak{a}_1$. Se tiene

(a) $\mathfrak{a}_1 = \mathfrak{b}_{1,1} \cdots \mathfrak{b}_{1,g_1'}$, donde los ideales $\mathfrak{b}_{1,i}$ son coprimos dos a dos, y $f_0 f_{1,i}$ divide a $f(\mathfrak{p}/p)$ para cada ideal primo $\mathfrak{p}$ de $\mathcal{O}$ que divide a $\mathfrak{b}_{1,i}$.

(b) Consideremos un i fijo. Si $a_{1,i} = 1$, entonces $\mathfrak{b}_{1,i}$ es un ideal primo $\mathfrak{p}_i$, con $e(\mathfrak{p}_i/p) = e_1$ y $f(\mathfrak{p}_i/p) = f_0 f_{1,i}$.

Se ha de descomponer ahora $\mathfrak{b}_{1,i}$ cuando el exponenete $a_{1,i} \geq 2$.

Fijemos un entero i tal que $a_{1,i} \geq 2$. Escribimos $\mathfrak{b}_1, \psi_1(Y), a_1, f_1$ en lugar de $\mathfrak{b}_{1,i}, \psi_{1,i}(Y), a_{1,i}, f_{1,i}$. Construimos un polinomio $\phi_2(X) \in \mathbb{Z}[X]$ mónico y de grado mínimo con tipo de orden 1 igual a $\mathbf{t}_1 := (\psi_0; h_1/e_1, \psi_1)$ (cf. §3 del capítulo 2).

1.3 Si $e_1 = f_1 = 1$, entonces para obtener la descomposición del ideal $\mathfrak{b}_1$ (como hemos visto en la sección anterior) remplazamos el polinomio $\phi_1(X)$ por el polinomio $\phi_1'(X) := \phi_2(X)$ y volvemos al principio del paso 1 pasando a trabajar con el polígono $\mathbf{N}^{h_1}_{(v_1,\phi_1')}(F)$. En caso contrario, continuamos el algoritmo.

Paso r (nivel r)

r.1 Sea $r \geq 2$ un entero, y supongamos realizado el paso $r-1$ y definido todos los datos. Por tanto, tenemos un exponente $a_{r-1} \geq 2$, un ideal $\mathfrak{b}_{r-1}$ a descomponer, y un tipo de orden $r-1$

$$\mathbf{t}_{r-1} = (\psi_0; h_1/e_1, \psi_1; \ldots; h_{r-1}/e_{r-1}, \psi_{r-1}),$$

con $e_s f_s > 1$ para $s = 1, \cdots, r-1$. Ponemos $e_0 := 1$.

Sea v_r la valoración de $\mathbb{Q}(X)$ asociada al correspondiente tipo reducido $\mathbf{t}^o_{r-1}$ (cf. 2.1 del capítulo 2). Construimos un polinomio mónico $\phi_r(X) \in \mathbb{Z}[X]$ de grado mínimo con tipo de orden $r-1$ igual a $\mathbf{t}_{r-1}$ (cf. §3 del capítulo 2). En este paso el par (v_r, ϕ_r) desempeñará el papel que hacía el par (v_1, ϕ_1) en el paso 1.

Construimos la parte principal, $\mathbf{N}^0_{(v_r,\phi_r)}(F)$, del polígono de Newton de $F(X)$ respecto del par (v_r, ϕ_r) (cf. 4.1 del capítulo 2). Sean $S_{r,1}, \ldots, S_{r,g_r}$

los lados de esta parte principal, y $d_{r,i}, e_{r,i}, h_{r,i}$ los datos de cada lado $S_{r,i}$. Por el teorema del polígono en orden r (cf. 8.1 y 8.3 del capítulo 2) se obtiene

(a) $\mathfrak{b}_{r-1} = \mathfrak{a}_{r,1}^{e_{r,1}} \cdots \mathfrak{a}_{r,g_r}^{e_{r,g_r}}$, donde los ideales $\mathfrak{a}_{r,i}$ son coprimos dos a dos.

(b) Consideremos un i fijo. Si $d_{r,i} = 1$, entonces $\mathfrak{a}_{r,i}$ es un ideal primo $\mathfrak{p}_i$, con $e(\mathfrak{p}_i/p) = e_0 \cdots e_{r-1}e_{r,i}$ y $f(\mathfrak{p}_i/p) = f_0 \cdots f_{r-1}$.

Por tanto, tenemos que descomponer $\mathfrak{a}_{r,i}$ cuando $d_{r,i} \geq 2$.

r.2 Fijemos un i tal que $d_{r,i} \geq 2$. Escribimos $\mathfrak{a}_r, S_r, d_r, e_r, h_r$ en lugar de $\mathfrak{a}_{r,i}, S_{r,i}, d_{r,i}, e_{r,i}, h_{r,i}$, respectivamente, y ponemos $q_r := p^{f_0 \cdots f_{r-1}}$. Construimos el polinomio asociado (en orden r), $F_{S_r}(Y) \in \mathbb{F}_{q_r}[Y]$, a $F(X)$ y S_r (cf. 4.3 del capítulo 2). Sea $F_{S_r}(Y) = c_r\, \psi_{r,1}(Y)^{a_{r,1}} \cdots \psi_{r,g'_r}(Y)^{a_{r,g'_r}}$ la factorización de $F_{S_r}(Y)$ en $\mathbb{F}_{q_r}[Y]$, y ponemos $f_{r,i} := \mathrm{gr}(\psi_{r,i})$. El teorema del polinomio asociado en orden r (cf. 9.1 y 9.3 del capítulo 2) muestra

(a) $\mathfrak{a}_r = \mathfrak{b}_{r,1} \cdots \mathfrak{b}_{r,g'_r}$, donde los ideales $\mathfrak{b}_{r,i}$ son coprimos dos a dos, y $f_0 \cdots f_{r-1}f_{r,i}$ divide a $f(\mathfrak{p}/p)$ para cada ideal primo $\mathfrak{p}$ que divide al ideal $\mathfrak{b}_{r,i}$.

(b) Consideremos un i fijo. Si $a_{r,i} = 1$, entonces $\mathfrak{b}_{r,i}$ es un ideal primo $\mathfrak{p}_i$, con $e(\mathfrak{p}_i/p) = e_0 \cdots e_r$ y $f(\mathfrak{p}_i/p) = f_0 \cdots f_{r-1}f_{r,i}$.

Todavía nos queda descomponer $\mathfrak{b}_{r,i}$ cuando $a_{r,i} \geq 2$.

Fijemos un i tal que $a_{r,i} \geq 2$. Escribimos $\mathfrak{b}_r, \psi_r(Y), a_r, f_r$ en lugar de $\mathfrak{b}_{r,i}, \psi_{r,i}(Y), a_{r,i}, f_{r,i}$. Construimos un polinomio $\phi_{r+1}(X) \in \mathbb{Z}[X]$ mónico y de grado mínimo con con tipo de orden r igual a $\mathbf{t}_r := (\mathbf{t}_{r-1}; h_r/e_r, \psi_r)$.

r.3 Si $e_r = f_r = 1$, entonces para obtener la descomposición del ideal $\mathfrak{b}_r$ (como hemos visto en la sección anterior) remplazamos el polinomio $\phi_r(X)$ por el polinomio $\phi'_r(X) := \phi_{r+1}(X)$ y volvemos al principio del paso r trabajando con el polígono $\mathbf{N}^{h_r}_{(v_r,\phi'_r)}(F)$. En caso contrario, continuamos el algoritmo ejecutando el paso $r+1$.

El proceso iterativo anterior permite computar el tipo de descomposición de p en K en un número finito de pasos. En efecto, por una parte, al final de la sección anterior hemos visto que, para un determinado nivel $r \geq 1$, en número finito de pasos se llega o bien a descomponer completamente el ideal $\mathfrak{b}_r$, o bien a obtener al menos un ideal que divide a $\mathfrak{b}_r$ para

el cual es $a_r \geq 2$ y $e_r f_r > 1$; en este último caso para descomponer el ideal se debe saltar de nivel y ejecutar el paso $r+1$. Por otra, es claro que cada vez que saltamos de nivel, del nivel r al paso $r+1$, se tiene

$$2 \leq a_r < e_r f_r a_r \leq e_r d_r \leq a_{r-1} \quad \text{(cf. 4.4 (4) y 4.2 del capítulo 2);}$$

por tanto, no podemos estar indefinidamente saltando de nivel. □

3.2. Observaciones. (1). Por el teorema del índice (cf. 11.4 del capítulo 2) y la proposición de 2.4, cuando se acaba de ejecutar este algoritmo se conoce el valor p-ádico del discriminate absoluto del cuerpo K, una vez se ha calculado la valoración p-ádica del discriminante del polinomio $F(X)$.

(2). Para ejecutar este algoritmo necesitamos factorizar cada polinomio asociado sobre el cuerpo finito correspondiente. Los cardinales de estos cuerpos están controlados por el primo p y el grado del polinomio $F(X)$, ya que son de la forma p^f, con $f \geq 1$ diviendo al grado residual $f(\mathfrak{p}/p)$ de un ideal primo $\mathfrak{p}$ de $\mathcal{O}$ que divide a $p\mathcal{O}$.

§4. Profundidad de un polinomio

En esta sección de nuevo denotaremos por K a una extensión finita de $\mathbb{Q}_p$ y por $\mathcal{O}$ a su anillo de enteros, y usaremos las notaciones introducidas en el capítulo 2.

Sea $P(X) \in \mathcal{O}[X]$ un polinomio mónico e irreducible. Partiendo de $P(X)$, podemos ejecutar también el algoritmo de 3.1 y obtener, en este caso, un entero $r \geq 0$ y un tipo de orden r

$$\mathbf{t}_r := (\psi_0; h_1/e_1, \psi_1; \ldots; h_r/e_r, \psi_r)\,,$$

con $e_i f_i > 1$ para $i = 1, \ldots, r$, y con el correspondiente exponente $a_r = 1$ (cf. 8.4 y 9.4 del capítulo 2). Para ello ha sido necesario construir en cada nivel i del algoritmo un *buen representante* del tipo $\mathbf{t}_{i-1}$; es decir, un polinomio $\phi_i(X) \in \mathcal{O}[X]$ mónico, de grado mínimo (igual a $m_i = e_0 f_0 \cdots e_{i-1} f_{i-1}$) con tipo de orden $i-1$ igual a $\{\mathbf{t}_{i-1}\}$, y tal que para los correspondientes datos $-h_i/e_i, \psi_i(Y)$ (pendiente del único lado S_i de su polígono de Newton

$\mathbf{N}_{(v_i,\phi_i)}(P)$, y único factor mónico e irreducible de su polinomio asociado $P_{S_i}(Y)$, respectivamente) se satisface la condición anterior $e_i f_i > 1$. La teoría desarrollada en la §3 del capítulo 2 y en la §2 nos enseña un procedimiento para construir de manera efectiva tales representantes; pero, ya sabemos, por el capítulo anterior, que para poder ejecutar el algoritmo no nos importa como hayan sido construidos estos representantes.

Si elegimos ahora otro buen representante $\phi'_j(X)$ en cada nivel, obtendremos, en principio, un entero $s \geq 0$ y un tipo de orden s

$$\mathbf{t}'_s := (\psi_0; h'_1/e'_1, \psi'_1; \ldots; h'_s/e'_s, \psi'_s)\,,$$

con $e'_j f'_j > 1$ para $j = 1, \ldots, s$, y con el exponente $a'_s = 1$ (para el tipo $\mathbf{t}'_s$ aplicamos el superíndice prima a las notaciones que utilizamos para $\mathbf{t}_r$). Pues bien, de la demostración del teorema de 2.1, se obtiene el siguiente

4.1. Corolario. *Con las notaciones anteriores, tenemos*

$$s = r,\ h'_1 = h_1,\ e'_1 = e_1,\ f'_1 = f_1,\ \ldots,\ h'_r = h_r,\ e'_r = e_r,\ f'_r = f_r.$$

DEMOSTRACIÓN. Sin pérdida de generalidad podemos suponer que se tiene $1 \leq s \leq r$. Puesto que $\mathrm{gr}(P) = e_0 f_0 e_1 f_1 \cdots e_r f_r = e_0 f_0 e'_1 f'_1 \cdots e'_s f'_s$, bastará con ver por inducción sobre i, $1 \leq i \leq s$, que se tienen las igualdades $h'_i/e'_i = h_i/e_i$, $f'_i = f_i$. Si $i = 1$, las igualdades se obtienen aplicando directamente el teorema de 2.1, ya que $e_1 f_1, e'_1 f'_1 > 1$.

Consideremos ahora un i con $2 \leq i \leq s$, y supongamos que para $1 \leq j \leq i-1$ se dan las igualdades $h'_j/e'_j = h_j/e_j$, $f'_j = f_j$. Entonces, por 3.3 (c) del capítulo 2, es $v'_i(\phi'_i) = v_i(\phi_i)$; además, por 7.1($b$) del capítulo 2, es $v'_i(M) = v_i(M)$ para cada polinomio $M(X) \in \mathcal{O}[X]$ de grado menor que m_i. Procediendo ahora como en la demostración del teorema 2.1, y teniendo en cuenta que $e_i f_i, e'_i f'_i > 1$, se obtiene $h'_i/e'_i = h_i/e_i$ y $f'_i = f_i$. □

El corolario anterior nos permite dar la siguiente definición.

4.2. Definición. *Llamaremos profundidad del polinomio $P(X)$ al nivel r que hemos de llegar para ejecutar el algoritmo de* 3.1 *con $P(X)$; es decir, hasta llegar a que el exponente $a_r = 1$.*

4.3. Observación. Okutsu define también un concepto de profundidad para un polinomio irreducible con coeficientes en un anillo de valoración discreta completo (cf. [**Ok 82**]). Aunque no se ha llegado a demostrar, pensamos que en nuestro caso los dos conceptos deben ser equivalentes.

Con la definición que acabamos de dar es claro ahora el siguiente

4.4. Corolario.

(a) *Si* $\mathrm{gr}(P) = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ *es la factorización del grado de* $P(X)$ *en* $\mathbb{Z}$, *entonces la profundidad de* $P(X)$ *es menor o igual que* $\alpha_1 + \cdots + \alpha_t$.

(b) *Si* $F(X) \in \mathbb{Z}[X]$ *es un polinomio mónico e irreducible, y*

$$F(X) = F_1(X) \cdots F_g(X)\,,$$

es su factorización en producto de irreducibles en $\mathbb{Q}_p[X]$, *entonces el número total de niveles a ejecutar en el algoritmo de* 3.1 *para el polinomio* $F(X)$ *es menor o igual que uno más la suma de las profundidades de los polinomios* $F_i(X)$ *en* $\mathbb{Q}_p$. □

§5. Generadores de los ideales primos

Sean $F(X) \in \mathbb{Z}[X]$ un polinomio mónico e irreducible, $\theta \in \mathbb{Q}^{al}$ una raíz cualquiera de $F(X)$, $K := \mathbb{Q}(\theta)$ y $\mathcal{O}$ su anillo de enteros. En esta sección nuestro objetivo será determinar para cada ideal primo $\mathfrak{p}$ de $\mathcal{O}$ diviendo a $p\mathcal{O}$ un elemento $\alpha \in \mathfrak{p}$ tal que p y α generen el ideal $\mathfrak{p}$; es decir, tal que

$$\mathfrak{p} = p\mathcal{O} + \alpha\mathcal{O}\,.$$

Utilizaremos las notaciones del capítulo 2 tomando como cuerpo base el cuerpo $\mathbb{Q}_p$; así, v denotará la valoración p-ádica de $\mathbb{Q}_p^{al}$ normalizada de forma que $v(p) = 1$. Para un ideal primo no nulo $\mathfrak{p}$ de $\mathcal{O}$, denotaremos por $\mathcal{O}_\mathfrak{p}$ al localizado de $\mathcal{O}$ en $\mathfrak{p}$, y por $v_\mathfrak{p}$ a la valoración de K determinada por el anillo de valoración discreta $\mathcal{O}_\mathfrak{p}$. Además, para un ideal fraccionario no nulo $\mathfrak{a}$ de $\mathcal{O}$, denotaremos por $v_\mathfrak{p}(\mathfrak{a})$ al exponente de $\mathfrak{p}$ en la descomposición

de $\mathfrak{a}$ como producto de potencias enteras de ideales primos no nulos de $\mathcal{O}$. Recordemos que se satisfacen las propiedades

$$v_{\mathfrak{p}}(\mathfrak{a}\cdot\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b}),$$
$$v_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b}) = \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\},$$
$$v_{\mathfrak{p}}(\alpha\mathcal{O}) = v_{\mathfrak{p}}(\alpha) \quad (\alpha \in K^*).$$

Por comodidad en la exposición haremos las hipótesis (H1) y (H2) siguientes.

(H1) Imaginamos que ejecutamos el algoritmo de 3.1, partiendo del polinomio $F(X)$ y del primo p, sin realizar los pasos $*.3$ (correspondientes a la obtención de representantes optimales en cada nivel).

Entonces obtenemos igualmente el tipo de descomposición de p en K

$$p\mathcal{O} = \mathfrak{p}_1^{e(\mathfrak{p}_1/p)} \cdots \mathfrak{p}_g^{e(\mathfrak{p}_g/p)},$$

y g tipos $\mathbf{t}_{r_1}^1, \ldots, \mathbf{t}_{r_g}^g$, con cada tipo

$$\mathbf{t}_{r_i}^i := (\psi_0^i; h_1^i/e_1^i, \psi_1^i; \ldots; h_{r_i}^i/e_{r_i}^i, \psi_{r_i}^i)$$

tal que los correspondientes exponentes satisfacen $a_{r_i-1}^i > 1 = a_{r_i}^i$ (utilizamos el superíndice i para los datos del tipo $\mathbf{t}_{r_i}^i$).

(H2) Suponemos que $r_1 = \cdots = r_g =: r$; es decir, que las "ramas" del algoritmo correspondientes a los g ideales primos acaban en el mismo orden.

5.1. Observación. Las hipótesis únicamente han tenido por finalidad simplificar la exposición del método para hallar para cada ideal primo un elemento que, junto con p, genera el ideal. En la práctica, hallamos un tal elemento sin modificar la estructura del algoritmo tal como la hemos descrito en la sección 3 (cf. observaciones (1) y (2) de 5.7).

Para cada par i, s con $1 \le i \le g$, $1 \le s \le r$, tenemos por tanto definidos el correspondiente par de valoración (v_s^i, ω_s^i), y elegido un polinomio mónico $\phi_s^i(X) \in \mathbb{Z}[X]$ de grado mínimo con tipo de orden $s-1$ igual a $\{\mathbf{t}_{s-1}^i\}$. Observemos que la igualdad de tipos $\mathbf{t}_{s-1}^j = \mathbf{t}_{s-1}^i$ (es decir, las

mismas pendientes y los mismos polinomios $\psi(Y)$'s) implica las igualdades $v_s^j = v_s^i$, $\omega_s^j = \omega_s^i$ y $\phi_s^j(X) = \phi_s^i(X)$; además, observemos que la igualdad $\mathrm{t}_r^j = \mathrm{t}_r^i$ solamente se da para $j = i$.

Consideremos ahora la factorización de $F(X)$

$$F(X) = F_1(X) \cdots F_g(X)\,,$$

en producto de polinomios mónicos e irreducibles en $\mathbb{Q}_p[X]$, y sea $\theta_i \in \mathbb{Q}_p^{al}$ una raíz cualquiera de $F_i(X)$ $(1 \le i \le g)$. Aunque no conocemos los polinomios $F_i(X)$, sí que sabemos que cada $F_i(X)$ tiene tipo de orden r igual a $\{\mathrm{t}_r^i\}$, y que su grado es $\mathrm{gr}(F_i) = e_0^i \cdots e_r^i f_0^i \cdots f_r^i = e(\mathfrak{p}_i/p)\, f(\mathfrak{p}_i/p)$ (cf. §9 del capítulo 2). Además, para cada polinomio $G(X) \in \mathbb{Q}[X]$ tenemos definidos los elementos $G(\theta) \in K$, $G(\theta_i) \in \mathbb{Q}_p^{al}$, y se tiene la igualdad

$$v_{\mathfrak{p}_i}(G(\theta)) = e(\mathfrak{p}_i/p)\, v(G(\theta_i))\,.$$

Fijamos un entero i con $1 \le i \le g$. Para realizar nuestro objetivo será suficiente que construyamos un elemento $\alpha_i \in \mathcal{O}$ satisfaciendo las igualdades

$$v_{\mathfrak{p}_i}(\alpha_i) = 1\,, \quad v_{\mathfrak{p}_j}(\alpha_i) = 0 \quad \text{para } j \ne i\,.$$

En efecto, las igualdades anteriores nos dicen que el ideal $\alpha_i \mathcal{O}$ tiene una descomposición de la forma

$$\alpha_i \mathcal{O} = \mathfrak{p}_i \cdot \mathfrak{a}_i\,,$$

para algún ideal $\mathfrak{a}_i$ de $\mathcal{O}$ coprimo con $p\mathcal{O}$; de donde se obtiene

$$p\mathcal{O} + \alpha_i \mathcal{O} = \mathfrak{p}_i\,.$$

5.2. Observación. A partir de los polinomios $\phi_1^i(X), \ldots, \phi_r^i(X)$, el corolario de 11.12 del capítulo 2 nos proporciona un elemento de la forma

$$\frac{\Phi_i(\theta)}{p^{\nu_i}} \in K\,, \quad \Phi_i(X) \in \mathbb{Z}[X]\,, \quad \nu_i \in \mathbb{N},$$

que satisface la igualdad

$$v_{\mathfrak{p}_i}(\Phi_i(\theta)/p^{\nu_i}) = 1\,.$$

Si $g = 1$ (es decir, si nuestro polinomio $F(X)$ es irreducible en $\mathbb{Q}_p[X]$), este elemento ya es suficiente para nuestros propósitos. Sin embargo, este elemento no nos sirve cuando $g > 1$.

Para obtener un elemento α_i como antes, construimos ahora un polinomio $\phi^i_{r+1}(X) \in \mathbb{Z}[X]$ mónico, de grado $e^i_0 f^i_0 \cdots e^i_r f^i_r = \mathrm{gr}(F_i)$ y con tipo de orden r igual a $\{\mathbf{t}^i_r\}$ (cf. §3 del capítulo 2). Observemos que el polígono de Newton $\mathbf{N}_{(v^i_{r+1},\phi^i_{r+1})}(F_i)$ consta de un solo lado, con extremos $(0, v^i_{r+1}(F_i - \phi^i_{r+1}))$ y $(1, v^i_{r+1}(\phi^i_{r+1}))$; luego, la longitud de su proyección sobre el eje de ordenadas es $H^i_{r+1} := v^i_{r+1}(F_i - \phi^i_{r+1}) - v^i_{r+1}(\phi^i_{r+1}) \geq 1$.

Para realizar nuestro objetivo, tendremos que "estropear" antes el representante $\phi^i_{r+1}(X)$ del tipo $\mathbf{t}^i_r$.

5.3. Lema. *Con las notaciones anteriores, podemos construir el polinomio* $\phi^i_{r+1}(X)$ *de forma que* $H^i_{r+1} = 1$.

DEMOSTRACIÓN. En primer lugar, sabemos que el polígono $\mathbf{N}_{(v^i_{r+1},\phi^i_{r+1})}(F_i)$ coincide (salvo una traslación vertical) con el polígono $\mathbf{N}^0_{(v^i_{r+1},\phi^i_{r+1})}(F)$ (cf. §8 del capítulo 2); por tanto, podemos calcular H^i_{r+1} a partir de este último polígono.

Si nos hemos encontrado con $H^i_{r+1} > 1$, remplazamos el polinomio $\phi^i_{r+1}(X)$ por el nuevo representante

$$\phi^i_{r+1}(X) + M(X)\,,$$

donde $M(X) \in \mathbb{Z}[X]$ es un polinomio que construimos de grado menor que $\mathrm{gr}(F_i)$ y tal que $v^i_{r+1}(M) = v^i_{r+1}(\phi^i_{r+1}) + 1$ (cf. 3.2 del capítulo 2). Entonces obtenemos

$$v^i_{r+1}(F_i - \phi^i_{r+1} - M) = v^i_{r+1}(\phi^i_{r+1}) + 1 = v^i_{r+1}(\phi^i_{r+1} + M) + 1\,;$$

así, la longitud de la proyección sobre el eje de ordenadas del nuevo polígono $\mathbf{N}_{(v^i_{r+1},\phi^i_{r+1}+M)}(F_i)$ es uno. Con esto queda probado el lema. □

Suponemos pues que hemos contruido el polinomio $\phi^i_{r+1}(X)$ de forma que la $H^i_{r+1} = 1$. Tenemos entonces el siguiente resultado.

5.4. Proposición. *Con las notaciones e hipótesis anteriores, definimos el elemento*

$$\beta_i := \frac{\phi_{r+1}^i(\theta)}{\phi_r^i(\theta)^{e_r^i f_r^i}} \in K^* .$$

Entonces el ideal fraccionario $\beta_i \mathcal{O}$ descompone de la forma

$$\beta_i \mathcal{O} = \mathfrak{p}_i \cdot \prod_{j \in C_i} \mathfrak{p}_j^{-n_{i,j}} \cdot \mathfrak{b}_i ,$$

donde C_i es el conjunto (eventualmente vacio) definido por

$$C_i := \{ j : 1 \leq j \leq g,\, \mathbf{t}_{r-1}^j = \mathbf{t}_{r-1}^i,\, h_r^j/e_r^j > h_r^i/e_r^i \} ,$$

los enteros $n_{i,j}$, para $j \in C_i$, están definidos por

$$n_{i,j} := f_r^i(e_r^i h_r^j - e_r^j h_r^i) \geq 1 ,$$

y donde $\mathfrak{b}_i$ es un ideal fraccionario de $\mathcal{O}$ tal que $v_{\mathfrak{p}}(\mathfrak{b}_i) = 0$ para cada ideal primo $\mathfrak{p}$ de $\mathcal{O}$ que divide a $p\mathcal{O}$.

Para demostrar la proposición anterior necesitaremos un lema.

5.5. Lema. *Con las notaciones anteriores, tenemos*

$$v_r^j(\phi_{r+1}^i) = e_r^i f_r^i v_r^j(\phi_r^i) \quad (1 \leq i \leq g, 1 \leq j \leq g) .$$

DEMOSTRACIÓN. Para probar el lema, veremos por inducción sobre s, con $1 \leq s \leq r$, que se satisface la igualdad $v_s^j(\phi_{r+1}^i) = e_r^i f_r^i v_s^j(\phi_r^i)$.

Si $s = 1$, ambos miembros de la igualdad son nulos (ya que los dos polinomios son mónicos) y hemos acabado.

Consideremos un entero s, con $1 \leq s \leq r-1$, y supongamos que la igualdad es cierta para s. Vamos a ver que también es cierta para $s+1$. Distinguiremos dos casos, según que los tipos $\mathbf{t}_{s-1}^j$, $\mathbf{t}_{s-1}^i$ coincidan o sean diferentes.

Supongamos primero que $\mathbf{t}_{s-1}^j = \mathbf{t}_{s-1}^i$. Entonces $v_s^j = v_s^i$ y $\phi_s^j(X) = \phi_s^i(X)$. Aplicando el lema de 4.2 del capítulo 2, la igualdad supuesta para s y que $\mathrm{gr}(\phi_{r+1}^i) = e_r^i f_r^i \,\mathrm{gr}(\phi_r^i)$, vemos que las coordenadas de los extremos del

único lado del polígono $\mathbf{N}_{(v_s^i,\phi_s^i)}(\phi_{r+1}^i)$ se obtienen multiplicando por $e_r^i f_r^i$ las coordenadas de los extremos del único lado del polígono $\mathbf{N}_{(v_s^i,\phi_s^i)}(\phi_r^i)$. La definición de la valoración v_{s+1}^j, muestra entonces la igualdad para $s+1$.

Supongamos ahora que $\mathbf{t}_{s-1}^j \neq \mathbf{t}_{s-1}^i$. Entonces, por 2.2 (c) del capítulo 2, tenemos $v_{s+1}^j(\phi_\nu^i) = e_s^j v_s^j(\phi_\nu^i)$ para $\nu = r, r+1$, ya que al tener $\phi_\nu^i(X)$ tipo de orden $s-1$ igual a $\{\mathbf{t}_{s-1}^i\}$ es $\omega_s^j(\phi_\nu^i) = 0$. Por consiguiente, aplicando la igualdad para s obtenemos

$$v_{s+1}^j(\phi_{r+1}^i) = e_s^j v_s^j(\phi_{r+1}^i) = e_s^j e_r^i f_r^i v_s^j(\phi_r^i) = e_r^i f_r^i v_{s+1}^j(\phi_r^i);$$

lo que prueba la igualdad para $s+1$. □

DEMOSTRACIÓN (de la proposición de 5.4). En primer lugar, observemos que β_i está bien definido, ya que $\phi_r^i(\theta) \neq 0$. En efecto, en caso contrario, tendríamos $F(X) = \phi_r^i(X)$ y $g = 1$, ya que $\phi_r^i(X)$ es irreducible en $\mathbb{Q}_p[X]$ (por 3.4 (a) del capítulo 2); luego, habríamos acabado el algoritmo de 3.1 en orden $r-1$, y no en orden r como suponemos. Además, observemos que $\phi_{r+1}^i(\theta) \neq 0$. En efecto, en caso contrario, como antes tendríamos $F(X) = \phi_{r+1}^i(X)$, $g = 1$; luego, sería $F_i(X) = \phi_{r+1}^i(X)$, en contradicción con la construcción de $\phi_{r+1}^i(X)$.

En segundo lugar, veamos que para cada entero j, con $1 \leq j \leq g$, tenemos

$$v_{\mathfrak{p}_j}(\phi_r^i(\theta)) = \begin{cases} e_r^j v_r^i(\phi_r^i) + h_r^j & \text{si } \mathbf{t}_{r-1}^j = \mathbf{t}_{r-1}^i, \\ e_r^j v_r^j(\phi_r^i) & \text{si } \mathbf{t}_{r-1}^j \neq \mathbf{t}_{r-1}^i. \end{cases}$$

Recordemos antes que $v_{\mathfrak{p}_j}(\phi_r^i(\theta)) = e(\mathfrak{p}_j/p)\, v(\phi_r^i(\theta_j)) = e_1^j \cdots e_r^j v(\phi_r^i(\theta_j))$. Si $\mathbf{t}_{r-1}^j = \mathbf{t}_{r-1}^i$, entonces $v_r^j = v_r^i$, $\phi_r^j(X) = \phi_r^i(X)$ y

$$e_1^j \cdots e_{r-1}^j v(\phi_r^j(\theta_j)) = v_r^j(\phi_r^j) + \frac{h_r^j}{e_r^j},$$

por 8.4 del capítulo 2. Si $\mathbf{t}_{r-1}^j \neq \mathbf{t}_{r-1}^i$, entonces $\omega_r^j(\phi_r^i) = 0$ y, por 7.1 (b) del capítulo 2, tenemos

$$e_1^j \cdots e_{r-1}^j v(\phi_r^i(\theta_j)) = v_r^j(\phi_r^i).$$

En tercer lugar, probemos que para cada entero j, $1 \leq j \leq g$, el valor

$v_{\mathfrak{p}_j}(\phi^i_{r+1}(\theta)) = e^j_1 \cdots e^j_r\, v(\phi^i_{r+1}(\theta_j))$ es igual a

$$\begin{cases} e^i_r f^i_r (e^i_r v^i_r(\phi^i_r) + h^i_r) + 1 & \text{si } \mathbf{t}^j_r = \mathbf{t}^i_r \text{ (es decir, si } j = i), \\ e^i_r f^i_r (e^i_r v^i_r(\phi^i_r) + h^i_r) & \text{si } \mathbf{t}^j_{r-1} = \mathbf{t}^i_{r-1},\ h^j_r/e^j_r = h^i_r/e^i_r,\ \psi^j_r(Y) \neq \psi^i_r(Y), \\ e^i_r f^i_r (e^j_r v^i_r(\phi^i_r) + h^j_r) & \text{si } \mathbf{t}^j_{r-1} = \mathbf{t}^i_{r-1},\ h^j_r/e^j_r < h^i_r/e^i_r, \\ e^j_r f^i_r (e^i_r v^i_r(\phi^i_r) + h^i_r) & \text{si } \mathbf{t}^j_{r-1} = \mathbf{t}^i_{r-1},\ h^j_r/e^j_r > h^i_r/e^i_r, \\ e^i_r f^i_r e^j_r v^j_r(\phi^i_r) & \text{si } \mathbf{t}^j_{r-1} \neq \mathbf{t}^i_{r-1}. \end{cases}$$

Si $\mathbf{t}^j_r = \mathbf{t}^i_r$, entonces $j = i$ y, por 8.4 y 3.3 (b) del capítulo 2, obtenemos

$$e^i_1 \cdots e^i_r\, v(\phi^i_{r+1}(\theta_i)) = v^i_{r+1}(\phi^i_{r+1}) + 1 = e^i_r f^i_r (e^i_r v^i_r(\phi^i_r) + h^i_r) + 1$$

(recordar que hemos construido el polinomio $\phi^i_{r+1}(X)$ con la $H^i_{r+1} = 1$). Supongamos pues que $\mathbf{t}^j_r \neq \mathbf{t}^i_r$. Entonces es $\omega^j_{r+1}(\phi^i_{r+1}) = 0$ y, por 7.1 (b) del capítulo 2, es

$$e^j_1 \cdots e^j_r\, v(\phi^i_{r+1}(\theta_j)) = v^j_{r+1}(\phi^i_{r+1})\,.$$

Por tanto, ahora estamos interesados en el valor $v^j_{r+1}(\phi^i_{r+1})$. Si $\mathbf{t}^j_{r-1} = \mathbf{t}^i_{r-1}$, entonces $v^j_r = v^i_r$, $\phi^j_r(X) = \phi^i_r(X)$ y, aplicando la definición de la valoración v^j_{r+1}, obtenemos en cada caso la igualdad que nos interesa. Si $\mathbf{t}^j_{r-1} \neq \mathbf{t}^i_{r-1}$, entonces $\omega^j_r(\phi^i_{r+1}) = 0$ y, por 2.2 (c) del capítulo 2 y el lema de 5.5, tenemos

$$v^j_{r+1}(\phi^i_{r+1}) = e^j_r v^j_r(\phi^i_{r+1}) = e^j_r e^i_r f^i_r v^j_r(\phi^i_r)\,.$$

Por último, aplicando los resultados anteriores, calculamos ahora el valor $v_{\mathfrak{p}_j}(\beta_i) = v_{\mathfrak{p}_j}(\phi^i_{r+1}(\theta)) - e^i_r f^i_r v_{\mathfrak{p}_j}(\phi^i_r(\theta))$, para $j = 1, \ldots, g$; de donde se sigue la proposición. □

A continuación veremos que, a partir del elemento β_i y de los elementos β_j para $j \in C_i$, podemos construir un elemento α_i con las propiedades que deseamos.

5.6. Teorema. *Continuamos con las notaciones e hipótesis anteriores. Por inducción sobre el cardinal del conjunto finito C_i, definiremos un elemento $\alpha'_i \in K^*$ de la forma siguiente. Si $C_i = \{\emptyset\}$, definimos $\alpha'_i := \beta_i$. Supongamos que $C_i \neq \{\emptyset\}$, y que para cada $j \in C_i$ (al estar $C_j \subsetneq C_i$) ya tenemos definido el elemento α'_j; entonces definimos*

$$\alpha'_i := \beta_i \cdot \prod_{j \in C_i} (\alpha'_j)^{n_{i,j}}\,.$$

Tenemos

(a) *El ideal fraccionario $\alpha_i' \mathcal{O}$ descompone de la forma*

$$\alpha_i' \mathcal{O} = \mathfrak{p}_i \cdot \mathfrak{a}_i',$$

donde $\mathfrak{a}_i'$ es un ideal fraccionario de $\mathcal{O}$ tal que $v_\mathfrak{p}(\mathfrak{a}_i') = 0$ para cada ideal primo $\mathfrak{p}$ de $\mathcal{O}$ que divide al ideal $p\mathcal{O}$.

(b) *Expresamos el elemento α_i' en la forma*

$$\alpha_i' = \frac{G_i(\theta)}{b_i},$$

con $G_i(X) \in \mathbb{Z}[X]$ de grado menor que el grado de $F(X)$ y $b_i \in \mathbb{Z}$ no nulo (utilizando, por ejemplo, el algoritmo de Euclides), y definimos

$$\alpha_i := \frac{G_i(\theta)}{p^{v(b_i)}}.$$

Entonces el elemento $\alpha_i \in \mathcal{O}$ y

$$\mathfrak{p}_i = p\mathcal{O} + \alpha_i \mathcal{O}.$$

DEMOSTRACIÓN. La parte (a) se obtiene por inducción sobre el cardinal del conjunto C_i, utilizando la proposición de 5.4.

Pasemos a ver la parte (b). Calculemos el valor $v_\mathfrak{p}(\alpha_i)$ para un ideal primo $\mathfrak{p}$ de $\mathcal{O}$. Si $\mathfrak{p}$ divide a $p\mathcal{O}$, por la parte (a) tenemos

$$v_\mathfrak{p}(\alpha_i) = v_\mathfrak{p}(\alpha_i') = \begin{cases} 1 & \text{si } \mathfrak{p} = \mathfrak{p}_i, \\ 0 & \text{si } \mathfrak{p} \neq \mathfrak{p}_i. \end{cases}$$

Si $\mathfrak{p}$ no divide a $p\mathcal{O}$, $v_\mathfrak{p}(\alpha_i) = v_\mathfrak{p}(G_i(\theta)) \geq 0$. Por tanto, $\alpha_i \in \bigcap \mathcal{O}_\mathfrak{p} = \mathcal{O}$ y $\mathfrak{p}_i = p\mathcal{O} + \alpha_i \mathcal{O}$. □

5.7. Observaciones. (1). La hipótesis (H2) anterior no es necesaria suponerla para obtener los α_i. En efecto, si definimos en general (es decir, cuando los ordenes $r_1, \ldots, r_g$ son cualesquiera)

$$\beta_i := \frac{\phi^i_{r_i+1}(\theta)}{\phi^i_{r_i}(\theta)^{e^i_{r_i} f^i_{r_i}}},$$

$$C_i := \{j : 1 \leq j \leq g,\ r_j \geq r_i,\ \mathfrak{t}^j_{r_i-1} = \mathfrak{t}^i_{r_i-1},\ h^j_{r_i}/e^j_{r_i} > h^i_{r_i}/e^i_{r_i}\},$$

$$n_{i,j} := e^j_{r_j} \cdots e^j_{r_i+1} f^i_{r_i}(e^i_{r_i} h^j_{r_i} - e^j_{r_i} h^i_{r_i}) \geq 1 \quad (j \in C_i),$$

entonces obtenemos el mismo resultado en la proposición de 5.4 y, por tanto, en el teorema de 5.6.

(2). Tampoco es necesario suponer la hipótesis (H1) para obtener los α_i. En efecto, si ejecutamos el algoritmo de 3.1 tal como se ha descrito en la sección 3, entonces, por la proposición de 2.4, también conocemos los datos que nos interesan de los tipos $\mathbf{t}^i_{r_i}$; así, podemos obtener los α_i como antes.

(3). En el caso $r_1, \cdots, r_g \leq 1$, Ore halla con otro método una familia finita de generadores de cada ideal primo (cf. [**Or 23**]).

§6. Ejemplos

En la presente sección daremos ejemplos que ilustran la aplicación y eficencia del algoritmo de 3.1. Los cálculos se han llevado a cabo usando el paquete *Newton* con un ordenador personal Pentium II a 300 Mhz.

6.1. Ejemplo 1. *Construcción de polinomios con tipos prefijados.* Dado un entero $r \geq 0$ y un tipo $\mathbf{t}_r$ de orden r con $q_0 = p$, la teoría desarrollada en la §3 del capítulo 2 nos enseña a construir un polinomio $\phi_{r+1}(X) \in \mathbb{Z}[X]$ mónico, irreducible, de grado m_{r+1} y con tipo de orden r igual a $\{\mathbf{t}_r\}$. (Pensamos cada tipo $\mathbf{t}_r$ con una elección fija de los correspondientes polinomios $\phi_s(X)$ para $s = 1, \ldots, r+1$.)

Más generalmente, dado un número finito de tipos $\mathbf{t}^1_{r_1}, \ldots, \mathbf{t}^g_{r_g}$, de ordenes respectivos $r_1, \ldots, r_g$, y con $q^1_0 = \cdots = q^g_0 = p$, entonces podemos construir un polinomio $F(X) \in \mathbb{Z}[X]$ mónico, irreducible, de grado $n := m^1_{r_1+1} + \cdots + m^g_{r_g+1}$ y tal que

$$\mathbf{t}(F) = \{\mathbf{t}^1_{r_1}, \ldots, \mathbf{t}^g_{r_g}\},$$

donde $\mathbf{t}(F)$ denota el conjunto de tipos que obtenemos al imaginar que, partiendo del polinomio $F(X)$ y del primo p, ejecutamos el algoritmo sin ejecutar los pasos $*.3$. En efecto, nos basta tomar

$$F(X) := \phi^1_{r_1+1}(X) \cdots \phi^g_{r_g+1}(X) + p^\nu M(X),$$

con $\nu \in \mathbb{Z}$ suficientemente grande para que $\mathbf{t}(F) = \mathbf{t}(\phi^1_{r_1+1} \cdots \phi^g_{r_g+1})$, y

con $M(X) \in \mathbb{Z}[X]$ de grado menor que n elegido de forma que $F(X)$ sea irreducible en $\mathbb{Q}$. □

6.2. Ejemplo 2. El siguiente ejemplo ilustra como funciona el algoritmo. Consideremos el polinomio

$$\begin{aligned} F(X) :=& X^{12} - 588X^{10} + 476X^9 + 130095X^8 - 172872X^7 - 12522636X^6 + \\ & 24745392X^5 + 486721116X^4 - 1583408736X^3 - 641009376X^2 + \\ & 10978063488X + 59914669248\,. \end{aligned}$$

Con el *Mathematica*, por ejemplo, obtenemos que el polinomio $F(X)$ es irreducible en $\mathbb{Q}$ y que su discriminante es

$$\Delta(F) = 2^{84} \cdot 3^{64} \cdot 7^{52} \cdot 79^4 \cdot 14159^2 \cdot 644173^2 \cdot 3352073^2\,.$$

Ejecutamos el algoritmo para obtener la descomposición del primo $p = 2$ en el anillo de enteros $\mathcal{O}$ del cuerpo de números K, definido por una raíz θ de $F(X)$. En primer lugar, vemos que

$$\overline{F}(Y) = (Y+1)^4\, Y^8\,, \quad \text{en } \mathbb{F}_2[Y]\,.$$

El paso 1.1 nos permite acabar ya para el factor $Y + 1$, puesto que la parte principal del polígono $\mathrm{N}_{(v_1, X+1)}(F)$ consta de dos lados, con pendientes $-3/2$ y $-1/2$. Con este factor obtenemos pues dos ideales primos, $\mathfrak{p}_1$ y $\mathfrak{p}_2$, diviendo a $2\,\mathcal{O}$, ambos con índice de ramificación 2 y grado residual igual a 1.

Sin embargo, para el factor Y la parte principal $\mathrm{N}^0_{(v_1, X)}(F)$ consta de dos lados, con pendientes -1 y $-1/2$, y con polinomios asociados $(Y+1)^4$ y $(Y+1)^2$, respectivamente. Por tanto, para el tipo $(Y; 1, Y+1)$ hemos de volver al paso 1.1 remplazando el polinomio X por un representante del tipo anterior, por ejemplo $X + 2$; mientras que para el tipo $(Y; 1/2, Y+1)$ hemos de seguir con el paso 2. Una vez remplazado X por $X + 2$, el nuevo polígono $\mathrm{N}^1_{(v_1, X+2)}(F)$ consta de un único lado, con pendiente $-3/2$ y con polinomio asociado $(Y+1)^2$; así, hemos de continuar ahora con el paso 2 para el nuevo tipo $(Y; 3/2, Y+1)$.

Aplicamos primero el paso 2 al tipo $(Y; 3/2, Y+1)$. Empezamos construyendo un representante de este tipo; por ejemplo, el polinomio $\phi_2(X) = (X+2)^2 + 8$. Entonces el polígono de segundo orden correspondiente $\mathrm{N}^0_{(v_2,\phi_2)}(F)$ consta de un solo lado, de pendiente -4 y su polinomio asociado es $(Y+1)^2$; por tanto, hemos de volver al paso 2.1 y remplazar el polinomio $\phi_2(X)$ por un representante del tipo $(Y; 3/2, Y+1; 4, Y+1)$, por ejemplo $\phi_2'(X) = \phi_2(X) + 32 = (X+2)^2 + 40$. Puesto que el nuevo polígono $\mathrm{N}^4_{(v_2,\phi_2')}(F)$ consta de dos lados, con pendientes -9 y -5, entonces hemos acabado para ese tipo, y obtenemos otros dos ideales primos, $\mathfrak{p}_3$ y $\mathfrak{p}_4$, diviendo a $2\mathcal{O}$ con índice de ramificación 2 y grado residual 1.

Aplicamos ahora el paso 2 al tipo $(Y; 1/2, Y+1)$. Empezamos tomando el polinomio $\phi_2(X) = X^2 + 2$ como representante de este tipo. Entonces el polígono $\mathrm{N}^0_{(v_2,\phi_2)}(F)$ consta de un solo lado, con pendiente -4 y con polinomio asociado $(Y+1)^2$; por tanto; hemos de volver al paso 2.1 sustituyendo el polinomio $\phi_2(X)$ por un representante del tipo $(Y; 1/2, Y+1; 4, Y+1)$; por ejemplo, $\phi_2'(X) = \phi_2(X) + 8 = X^2 + 10$. El nuevo polígono $\mathrm{N}^4_{(v_2,\phi_2')}(F)$ consta de un solo lado, con pendiente -5 y con polinomio asociado $(Y+1)^2$; luego, hemos de volver de nuevo al paso 2.1 remplazando $\phi_2'(X)$ por un representante del tipo $(Y; 1/2, Y+1; 5, Y+1)$; por ejemplo, el polinomio $\phi_2''(X) = \phi_2'(X) + 8X = X^2 + 8X + 10$. Puesto que el nuevo polígono $\mathrm{N}^5_{(v_2,\phi_2'')}(F)$ consta de dos lados, con pendientes -8 y -7, entonces hemos terminado, obteniendo también dos ideales primos, $\mathfrak{p}_5$ y $\mathfrak{p}_6$, diviendo a $2\mathcal{O}$ con índice de ramificación 2 y grado residual 1.

De lo anterior, obtenemos que $2\mathcal{O} = (\mathfrak{p}_1 \cdots \mathfrak{p}_6)^2$. El tiempo que se tarda con el ordenador en calcular esta descomposición es de 1,87 segundos.

Por otra parte, utilizando el procedimiento descrito en la sección anterior, obtenemos que cada ideal primo $\mathfrak{p}_i$ está generado por el 2 y el elemento $\alpha_i \in \mathcal{O}$ obtenido como en la parte (b) del teorema de 5.5 a partir del elemento $\alpha_i' \in K$ siguiente

$$\alpha_1' = \frac{(\theta+1)^2 + 4(\theta+1) + 8}{(\theta+1)^2}, \qquad \alpha_2' = \frac{(\theta+1)^2 + 2(\theta+1) + 2}{(\theta+1)^2} \cdot (\alpha_1')^4,$$

$$\alpha_3' = \frac{(\theta+2)^2 + 64(\theta+2) + 40}{(\theta+2)^2 + 40}, \qquad \alpha_4' = \frac{(\theta+2)^2 + 16(\theta+2) + 40}{(\theta+2)^2 + 40} \cdot (\alpha_3')^4,$$

$$\alpha_5' = \frac{\theta^2 + 40\theta + 42}{\theta^2 + 8\theta + 10}, \qquad \alpha_6' = \frac{\theta^2 + 24\theta + 10}{\theta^2 + 8\theta + 10} \cdot \alpha_5';$$

así, por ejemplo,

$$\begin{aligned}\alpha_1 =&(-7745402847023433068 + 11936731852894431472\,\theta + \\ &2408925593604709648\,\theta^2 - 1397663438300544528\,\theta^3 - \\ &15483873086627356\,\theta^4 + 32343278396987828\,\theta^5 - 69087017194464\,\theta^6 - \\ &323347524815768\,\theta^7 + 11018795871101\,\theta^8 + 1436408393889\,\theta^9 - \\ &3865496711\,\theta^{10} - 2425598303\,\theta^{11})/4\,.\end{aligned}$$

Además, el valor 2-ádico del discriminante absoluto del cuerpo es $v(\Delta(K)) = 18$, ya que $v(\mathrm{ind}(F)) = 21 + 12 = 33$ por el teorema del índice.

Con este polinomio para los primos 3 y 7 también necesitamos llegar a nivel dos, mientras que para el resto de los primos que dividen al discriminante de $F(X)$ acabamos en nivel uno. En la tabla 3.1 siguiente se da el tipo de descomposición de p en K, el valor p-ádico ν del discriminante absoluto de K, y el tiempo T en segundos necesario para obtener el tipo de descomposición de cada uno de estos primos.

Tabla 3.1.

p	$p\mathcal{O}$	ν	T
3	$(\mathfrak{p}_1 \cdots \mathfrak{p}_4)^3$	16	4,56
7	$(\mathfrak{p}_1 \cdots \mathfrak{p}_4)^3$	8	0,66
79	$\mathfrak{p}_1 \cdots \mathfrak{p}_{12}$	0	1,15
14159	$\mathfrak{p}_1 \cdots \mathfrak{p}_{12}$	0	1,16
644173	$\mathfrak{p}_1 \cdots \mathfrak{p}_{12}$	0	7,57
3352073	$\mathfrak{p}_1 \cdots \mathfrak{p}_{12}$	0	8,02

Para los dos últimos primos de la tabla anterior la mayor parte del tiempo se consume factorizando el polinomio $\overline{F}(Y)$ en $\mathbb{F}_p[Y]$.

6.3. Ejemplo 3. El siguiente ejemplo pone de manifiesto la potencia del polígono. Consideremos el polinomio

$$F(X) := (X^3 + X + 5)^{50} + 2^{89}(X^3 + X + 5)^{25} + 2^{178}\,.$$

En principio, no sabemos que este polinomio sea irreducible en $\mathbb{Q}$. Ejecutamos igualmente el algoritmo con este polinomio para el primo 2. De la expresión del polinomio obtenemos que el polígono $\mathbf{N}_{(v_1,X^3+X+5)}(F)$ consta de un solo lado, con pendiente $-89/25$, y su polinomio asociado es Y^2+Y+1. Los resultados de Ore nos dicen ya que este polinomio es irreducible en $\mathbb{Q}_2$, luego en $\mathbb{Q}$, y que el primo 2 descompone en la forma $\mathfrak{p}^{25}$.

El tiempo que se tarda en el ordenador con el paquete *Newton* es de $11,21$ segundos (tener presente que lo primero que se hace es expandir el polinomio y que al comenzar se toma el polinomio X^3+X+1 como representante). Si hubiéramos procedido con el método de Buchmann-Lenstra, habríamos necesitado calcular previamente una base 2-minimal; lo cual es verdaderamente costoso con este polinomio de grado 150 teniendo en cuenta que el valor 2-ádico del índice del polinomio es 13011.

6.4. Ejemplo 4. Consideremos ahora el polinomio 3-Eisenstein

$$F(X) := X^{2000} + 3 \cdot 2^{20} X^{200} + 3 \cdot 2^{40}\,.$$

Al ejecutar el algoritmo para el primo 2 obtenemos la descomposición

$$(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^{180}\,(\mathfrak{p}_4\mathfrak{p}_5)^{40}\,,$$

con los grados residuales

$$f(\mathfrak{p}_1/2) = f(\mathfrak{p}_2/2) = f(\mathfrak{p}_4/2) = 4\,, \quad f(\mathfrak{p}_3/2) = 2\,, \quad f(\mathfrak{p}_5/1) = 1\,.$$

Los ideales primos $\mathfrak{p}_1$ y $\mathfrak{p}_2$ se obtienen en nivel 2, y los restantes en nivel 3. El tiempo de cálculo es de $535,9$ segundos. De nuevo tenemos un polinomio con grado muy alto y valor 2-ádico del índice muy grande (a saber, 24650); por lo tanto, para este polinomio se tardaría mucho tiempo en hallar el tipo de descomposición anterior computando previamente una base 2-minimal.

El algoritmo ha necesitado llegar hasta el tercer nivel para el 2 porque este ejemplo ha sido elegido con ese propósito. Sin embargo, si escogemos un primo p al azar, lo más probable es que terminemos en el paso cero o en el nivel uno. Por ejemplo, para el primo 5, que también divide al discriminante del polinomio, en el paso cero ya obtenemos la descomposición

$$(\mathfrak{p}_1 \cdots \mathfrak{p}_7)^{25}\,,$$

con grado residual 3 para cuatro ideales primos, 6 para otros dos, y 56 para el restante. El tiempo en calcularla es de 122, 4 segundos.

Guàrdia en [**Gu 98**] usa el paquete *Newton*, con polinomios de grado muy alto y coeficientes muy grandes, para obtener el tipo de descomposición de los primos de mala reducción de una superficie aritmética concreta sobre el cuerpo de números donde tiene reducción estable. De este cuerpo no se dispone de un polinomio definidor, y sólo se conocen los polinomios irreducibles de seis elementos algebraicos que lo generan sobre $\mathbb{Q}$.

CAPÍTULO 4

Ramificación en cuerpos cuárticos

La determinación del tipo de descomposición de los primos racionales en el anillo de enteros de un cuerpo de números K y el cálculo del valor del discriminante de K, en terminos de un polinomio definidor de K, son dos problemas clásicos de la teoría algebraica de números que, como se ha visto en los capítulos anteriores, están estrechamente relacionados. La solución completa a estos problemas, en forma no algorítmica, es bien conocida para el caso de un cuerpo cuadrático y para el caso de un cuerpo cúbico (cf. [**Wa 22**], [**Ll-Na 83**]).

Usando las técnicas del polígono de Newton (de primer orden), Llorente-Nart-Vila en [**Ll-Na-Vi 84**] y [**Ll-Na-Vi 91**] obtienen en forma no algorítmica la solución completa a cada problema en los cuerpos de números definidos por trinomiales (salvo para unos pocos casos especiales en cuerpos de grado mayor que cinco). Roberson, usando el carácter aditivo de Weil del anillo de Witt racional, obtiene un criterio para decidir cuando el primo 2 ramifica en los cuerpos cuárticos definidos por polinomios bicuadráticos (cf. [**Ro 93**]).

Utilizando las técnicas del polígono de Newton (hasta segundo orden), en este capítulo daremos la solución completa, en forma no algorítmica, a estos dos problemas para el caso de cualquier cuerpo cuártico.

§1. Introducción

Sea $p \in \mathbb{Z}$ un número primo fijo. Sean K un cuerpo cuártico y $\mathcal{O}$ el anillo de los enteros de K. Sea $F(X) \in \mathbb{Z}[X]$ un polinomio mónico, irreducible y

de grado 4 definiendo K; es decir, $K = \mathbb{Q}(\theta)$ donde θ es una raíz de $F(X)$. Denotaremos por $\Delta = \Delta(F)$ (resp. $\Delta(K)$) al discriminante del polinomio $F(X)$ (resp. al discriminante absoluto de K). Tenemos la relación

$$\Delta = \mathrm{ind}(F)^2 \Delta(K),$$

donde $\mathrm{ind}(F) := (\mathcal{O} : \mathbb{Z}[\theta])$ es el índice de $F(X)$.

Denotaremos por v_p a la valoración p-ádica de $\mathbb{Q}_p$. Para un entero p-ádico $u \in \mathbb{Z}_p$, $u \neq 0$, denotaremos por u_p a la unidad p-ádica $u/p^{v_p(u)}$ y por $\overline{u}$ a la clase de $u \pmod{p}$.

El objetivo de este capítulo es obtener el tipo de descomposición de p en $\mathcal{O}$ y calcular $v_p(\Delta(K))$, en terminos de los coeficientes del polinomio $F(X)$. Para un polinomio $F(X)$ "concreto" (es decir, donde sus coeficientes son números enteros dados) esto puede ser hecho usando, por ejemplo, el algoritmo de 3.1 del capítulo 3. Sin embargo, en nuestro caso $F(X)$ es un polinomio "genérico" (es decir, donde sus coeficientes son parametros), lo cual presenta una dificultad adicional. En efecto, en este caso $v_p(\Delta)$ puede ser arbitrariamente grande; por tanto, si aplicamos sin más el algoritmo, nos podría pasar que estuvieramos distinguiendo casos indefinidamente. Esta dificultad la solucionaremos, principalmente, eligiendo representantes adecuados de los distintos tipos que nos saldran. También nos será útil para resolver esta dificultad una serie de resultados previos que daremos en la siguiente sección.

El estudio de estos problemas para el primo 2 esta hecho en las secciones 3 y 4. El excepcional comportamiento de este primo, debido sobre todo a sus diversos casos de ramificación salvaje, hace su estudio mucho más complejo que para el resto de los primos.

La sección 5 esta dedicada al estudio del primo 3, con un único caso de ramificación salvaje; mientras que la sección 6 esta dedicada al estudio de los primos $p > 3$, siempre moderadamente ramificados.

§2. Resultados previos

Teniendo en cuenta, para nuestro caso, la fórmula

$$\sum_{\mathfrak{p}|p} e_{\mathfrak{p}} f_{\mathfrak{p}} = 4,$$

donde $e_{\mathfrak{p}}$ y $f_{\mathfrak{p}}$ denotan, respectivamente, el índice de ramificación y el grado residual de un ideal primo $\mathfrak{p} \mid p$, vemos que p puede descomponerse en $\mathcal{O}$ en una de las once formas siguientes

$$\mathfrak{p},\ \mathfrak{p}^2,\ \mathfrak{p}^4,\ \mathfrak{p}_{(1)}\mathfrak{q}_{(3)},\ \mathfrak{p}_{(2)}\mathfrak{q}_{(2)},\ \mathfrak{pq}^2,\ \mathfrak{pq}^3,\ \mathfrak{p}^2\mathfrak{q}^2,\ \mathfrak{pqr},\ \mathfrak{pqr}^2,\ \mathfrak{pqrs},$$

donde $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \mathfrak{s}$ son ideales primos de $\mathcal{O}$ distintos, y entre paréntesis como subíndice figuran los grados residuales en las descomposiciones en que estos no quedan determinados por el número de primos que dividen a p y sus respectivos índices de ramificación.

A continuación, vamos a calcular los posibles valores de $v_p(\Delta(K))$ a partir del tipo de descomposición de p en $\mathcal{O}$. Después de los resultados de Dedekind, Hensel y Ore, sabemos que, para cualquier cuerpo de números K, el valor

$$v_p(\Delta(K)) = \sum_{\mathfrak{p}|p} f_{\mathfrak{p}}(e_{\mathfrak{p}} - 1 + c_{\mathfrak{p}}),$$

donde la componente salvaje $c_{\mathfrak{p}}$ es un entero que verifica

$$e_{\mathfrak{p}} v_p(l) \leq c_{\mathfrak{p}} \leq e_{\mathfrak{p}} v_p(e_{\mathfrak{p}}),$$

siendo l el único entero tal que $1 \leq l \leq e_{\mathfrak{p}}$ y $l \equiv c_{\mathfrak{p}} \pmod{e_{\mathfrak{p}}}$ (cf. **[Nar 90]**, **[Tr 85]**). En particular, para nuestro caso, obtenemos el siguiente lema.

2.1. Lema. *Con las notaciones anteriores, tenemos que*

(a) *Si* $p\mathcal{O} = \mathfrak{p},\ \mathfrak{p}_{(1)}\mathfrak{q}_{(3)},\ \mathfrak{p}_{(2)}\mathfrak{q}_{(2)},\ \mathfrak{pqr}$ *o* $\mathfrak{pqrs}$, *entonces* $v_p(\Delta(K)) = 0$.

(b) *Si* $p\mathcal{O} = \mathfrak{pq}^2$ *o* $\mathfrak{pqr}^2$ *y* $p \neq 2$, *entonces* $v_p(\Delta(K)) = 1$.

Si $p\mathcal{O} = \mathfrak{p}^2$ *o* $\mathfrak{p}^2\mathfrak{q}^2$ *y* $p \neq 2$, *entonces* $v_p(\Delta(K)) = 2$.

Si $p\mathcal{O} = \mathfrak{pq}^3$ *y* $p \neq 3$, *entonces* $v_p(\Delta(K)) = 2$.

Si $p\mathcal{O} = \mathfrak{p}^4$ *y* $p \neq 2$, *entonces* $v_p(\Delta(K)) = 3$.

(c) *Si* $2\mathcal{O} = \mathfrak{pq}^2$ *o* $\mathfrak{pqr}^2$, *entonces* $v_2(\Delta(K)) = 2$ *ó* 3.

Si $2\mathcal{O} = \mathfrak{p}^2$, *entonces* $v_2(\Delta(K)) = 4$ *ó* 6.

Si $2\mathcal{O} = \mathfrak{p}^2\mathfrak{q}^2$, *entonces* $v_2(\Delta(K)) = 4, 5$ *ó* 6.

Si $2\mathcal{O} = \mathfrak{p}^4$, *entonces* $v_2(\Delta(K)) = 4, 6, 8, 9, 10$ *ó* 11.

(d) *Si* $3\mathcal{O} = \mathfrak{pq}^3$, *entonces* $v_3(\Delta(K)) = 3, 4$ *ó* 5. □

Por tanto, sólo necesitamos conocer $v_p(\Delta(K))$ cuando p ramifica salvajemente en K; es decir, para $p = 2$ cuando $2\mathcal{O} = \mathfrak{p}^2$, $\mathfrak{p}^4$, $\mathfrak{pq}^2$, $\mathfrak{p}^2\mathfrak{q}^2$ o $\mathfrak{pqr}^2$ y para $p = 3$ cuando $3\mathcal{O} = \mathfrak{pq}^3$.

El tipo de descomposición de p en $\mathcal{O}$ no determina, en general, si Δ es o no un cuadrado en $\mathbb{Q}_p$; sin embargo, ciertos tipos de descomposición si lo hacen, lo cual nos será útil posteriormente.

2.2. Lema. *Con las notaciones anteriores, tenemos que*

(a) *Si* $p\mathcal{O} = \mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$, $\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$ *o* $\mathfrak{pqrs}$, *entonces* $\Delta \in (\mathbb{Q}_p^*)^2$.

(b) *Si* $p\mathcal{O} = \mathfrak{p}$, $\mathfrak{pqr}$ *o* $\mathfrak{pqr}^2$, *entonces* $\Delta \notin (\mathbb{Q}_p^*)^2$.

DEMOSTRACIÓN. Si $p\mathcal{O} = \mathfrak{pqr}^2$, entonces $F(X) = (X - \theta)(X - \theta')H(X)$, con $\theta, \theta' \in \mathbb{Q}_p$ y $H(X) \in \mathbb{Q}_p[X]$ irreducible y de grado 2. Por tanto,

$$\Delta = (\theta - \theta')^2 H(\theta)^2 H(\theta')^2 \Delta(H) \notin (\mathbb{Q}_p^*)^2.$$

En los restantes casos, p no ramifica en $\mathcal{O}$; por tanto, en nuestro caso, $\Delta(K) \in (\mathbb{Q}_p^*)^2$ si y sólo si $g \equiv 4 \pmod 2$, donde g es el número de primos de $\mathcal{O}$ que dividen a p (cf. [Sw 62]). □

Dado un entero 2-ádico $u \in \mathbb{Z}_2$, $u \neq 0$, recordemos que $u \in (\mathbb{Q}_2^*)^2$ si $v_2(u)$ es par y $u_2 \equiv 1 \pmod 8$, y que $\mathbb{Q}_2(\sqrt{u})/\mathbb{Q}_2$ es una extensión cuadrática no ramificada (resp. totalmente ramificada) si $v_2(u)$ es par y $u_2 \equiv 5 \pmod 8$ (resp. $v_2(u)$ es impar o $u_2 \equiv 3 \pmod 4$). Cuando $2\mathcal{O} = \mathfrak{p}$ o $\mathfrak{pqr}$, por ejemplo, el lema anterior tan sólo nos dice que $\Delta_2 \not\equiv 1 \pmod 8$. Para el primo 2, nos interesará refinar y ampliar el lema de 2.2.

2.3. Lema. *Con las notaciones anteriores, tenemos que*

(a) *Si* $2\mathcal{O} = \mathfrak{pq}^2$ *o* $\mathfrak{pqr}^2$ *y* $v_2(\Delta)$ *es par, entonces* $\Delta_2 \equiv 3 \pmod 4$.

(b) *Si* $2\mathcal{O} = \mathfrak{p}$, $\mathfrak{pqr}$ *o* $\mathfrak{pq}^3$, *entonces* $\Delta_2 \equiv 5 \pmod 8$.

DEMOSTRACIÓN. Si $2\mathcal{O} = \mathfrak{pq}^2$ o $\mathfrak{pqr}^2$, entonces $F(X) = H_1(X)H_2(X)$, con los polinomios $H_i(X) \in \mathbb{Q}_2[X]$ de grado 2, y tales que $v_2(\Delta(H_1))$ es par, $\Delta(H_1)_2 \equiv 1 \pmod 4$ y la extensión $\mathbb{Q}_2(\sqrt{\Delta(H_2)})/\mathbb{Q}_2$ es de grado 2 y totalmente ramificada. Como

$$\Delta = \Delta(H_1)\,\Delta(H_2)\,\mathrm{Res}(H_1, H_2)^2,$$

entonces tenemos que

$$v_2(\Delta) \equiv v_2(\Delta(H_1)) + v_2(\Delta(H_2)) \pmod 2,$$
$$\Delta_2 \equiv \Delta(H_1)_2\,\Delta(H_2)_2 \pmod 8.$$

Por tanto, si además $v_2(\Delta)$ es par, entonces $v_2(\Delta(H_2))$ es par, $\Delta(H_2)_2 \equiv 3 \pmod 4$ y $\Delta_2 \equiv 3 \pmod 4$. Esto prueba la parte (a).

Si $2\mathcal{O} = \mathfrak{p}$, entonces $F(X)$ es irreducible en $\mathbb{Q}_2$ y $\mathbb{Q}_2(\theta)/\mathbb{Q}_2$ es una extensión no ramificada y, por tanto, cíclica. Por consiguiente, la extensión $\mathbb{Q}_2(\sqrt{\Delta})/\mathbb{Q}_2$ es de grado 2 y no ramificada y, por tanto, $\Delta_2 \equiv 5 \pmod 8$.

Si $2\mathcal{O} = \mathfrak{pqr}$, entonces $F(X) = H_1(X)H_2(X)$, con los $H_i(X) \in \mathbb{Q}_2[X]$ polinomios de grado 2 tales que $\Delta(H_1)_2 \equiv 1 \pmod 8$ y $\Delta(H_2)_2 \equiv 5 \pmod 8$. Por tanto, $\Delta_2 \equiv 5 \pmod 8$.

Finalmente, si $2\mathcal{O} = \mathfrak{pq}^3$, entonces $F(X) = (X-\theta)H(X)$, con $\theta \in \mathbb{Q}_2$ y $H(X) \in \mathbb{Q}_2[X]$ irreducible y de grado 3; además, si $\theta' \in \mathbb{Q}_2^{ur}$ es una raíz de $H(X)$, entonces la extensión cúbica $\mathbb{Q}_2(\theta')/\mathbb{Q}_2$ es totalmente ramificada. Como

$$\Delta = \Delta(H)H(\theta)^2,$$

entonces $\Delta_2 \equiv \Delta(H)_2 \pmod 8$. Por otra parte, del teorema 1 de [**Ll-Na 83**] se deduce, utilizando el lema de Krasner, que $\Delta(H)_2 \equiv 5 \pmod 8$. Por consiguiente, tenemos que también $\Delta_2 \equiv 5 \pmod 8$, lo que acaba de probar la parte (b). □

Para nuestros propósitos también nos será útil el siguiente lema sobre la resolvente cúbica formulado en un contexto general.

2.4. Lema. *Sea* $F(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in L[X]$ *un polinomio sin raíces múltiples, con coeficientes en un cuerpo* L *de característica diferente de* 2. *Suponemos que* $F(X)$ *tiene al menos una raíz* $\theta \in L$. *Consideramos el polinomio (una resolvente cúbica de* $F(X)$*)*

$$G(X) := X^3 - 2a_2X^2 + (a_1a_3 + a_2^2 - 4a_0)X + a_0a_3^2 - a_1a_2a_3 + a_1^2 \in L[X].$$

Entonces

(a) $G(X)$ *no tiene raíces múltiples, y el número de raíces de* $F(X)$ *en* L *excede en una unidad al número de raíces de* $G(X)$ *en* L.

(b) *Si* $G(X)$ *es irreducible en* $L[X]$, *entonces para cada raíz* θ' *de* $F(X)$, $\theta' \neq \theta$, *existe una raíz* η *de* $G(X)$ *tal que* $L(\theta') = L(\eta)$.

(c) *Si* $G(X)$ *tiene una única raíz en* L, *entonces el cuerpo de descomposición de* $F(X)$ *sobre* L *coincide con el cuerpo cuadrático* $L(\sqrt{\Delta})$, *donde* Δ *indica el discriminante del polinomio* $F(X)$.

DEMOSTRACIÓN. Sean $\theta_1, \theta_2, \theta_3, \theta_4 = \theta$ las raíces de $F(X)$ en una clausura algebraica fijada del cuerpo L. Entonces los elementos

$$\eta_1 := (\theta_1 + \theta_2)(\theta_3 + \theta_4),\ \eta_2 := (\theta_1 + \theta_3)(\theta_2 + \theta_4),\ \eta_3 := (\theta_1 + \theta_4)(\theta_2 + \theta_3)$$

son las raíces de $G(X)$ (esto se puede ver expresando con el método de Waring los coeficientes del polinomio $(X - \eta_1)(X - \eta_2)(X - \eta_3)$ en función de los a_i). Además, puesto que

$$\begin{aligned}
\eta_1 - \eta_2 &= -(\theta_1 - \theta_4)(\theta_2 - \theta_3),\\
\eta_1 - \eta_3 &= -(\theta_1 - \theta_3)(\theta_2 - \theta_4),\\
\eta_2 - \eta_3 &= -(\theta_1 - \theta_2)(\theta_3 - \theta_4),
\end{aligned}$$

entonces $\Delta(G) = \Delta$; en particular, $G(X)$ no tiene raíces múltiples.

En primer lugar, es claro que si $F(X)$ tiene las cuatro raíces en L, entonces $G(X)$ también tiene las tres raíces en L.

Supongamos ahora que $\theta_3 \in L$, pero $\theta_1, \theta_2 \notin L$. Veamos entonces que $\eta_1 \in L$, $\eta_2, \eta_3 \notin L$ y que $L(\theta_1, \theta_2, \theta_3, \theta_4) = L(\sqrt{\Delta})$. En efecto, como el polinomio

$$(X - \theta_1)(X - \theta_2) = F(X)(X - \theta_3)^{-1}(X - \theta_4)^{-1} \in L[X]$$

y no tiene raíces en L, entonces $\theta_1+\theta_2 \in L$ y $\theta_1-\theta_2 \notin L$. Por tanto, tenemos $\eta_1 \in L$, $\eta_2+\eta_3 = 2a_2-\eta_1 \in L$ y $\eta_2-\eta_3 = (\theta_1-\theta_2)(\theta_4-\theta_3) \notin L$; así, $\eta_2, \eta_3 \notin L$. Además, $L(\theta_1,\theta_2,\theta_3,\theta_4) = L(\theta_1,\theta_2) = L(\theta_1-\theta_2) = L(\sqrt{\Delta})$.

Por último, supongamos que $\theta_1, \theta_2, \theta_3 \notin L$. Veamos entonces que $L(\theta_i) = L(\eta_{4-i})$ para cada i, $1 \leq i \leq 3$; lo cual probará también que $\eta_1, \eta_2, \eta_3 \notin L$. Puesto que $\eta_{4-i} = -(a_3+\theta_i+\theta_4)(\theta_i+\theta_4)$, entonces obtenemos $L(\eta_{4-i}) \subseteq L(\theta_i)$ y $[L(\theta_i) : L(\eta_{4-i})] = 1$ ó 2. Pero, de la hipótesis se deduce $[L(\theta_i) : L] = 3$; por consiguiente, ha de ser $[L(\theta_i) : L(\eta_{4-i})] = 1$. □

Este lema será aplicado al cuerpo $L = \mathbb{Q}_p$ y cuando nuestro polinomio $F(X) \in \mathbb{Z}[X]$ tenga una (única) raíz simple (mod p); así, por el lema de Hensel, $F(X)$ tendra al menos una raíz en $\mathbb{Q}_p$.

§3. Ramificación diádica (primera parte)

Esta sección y la próxima están dedicadas al estudio de la ramificación 2-ádica en el cuerpo cuártico K; por tanto, suponemos que $p = 2$.

Por comodidad, denotamos por v a la valoración 2-ádica extendida a $\mathbb{Q}_2(X)$ de forma que $v(X) = 0$, y ponemos $\nu := v(\Delta(K))$. Además, recordemos que dado un entero 2-ádico $u \neq 0$ denotamos por u_2 a la unidad 2-ádica $u/2^{v(u)}$ y por $\overline{u}$ a la clase de u (mod 2).

En esta sección suponemos que el polinomio $F(X)$ es de la forma

$$F(X) = X^4 + aX^2 + bX + c,$$

con $a, b, c \in \mathbb{Z}$. Además, suponemos también que las condiciones

$$v(a) \geq 2,\ v(b) \geq 3,\ v(c) \geq 4,$$

no se dan simultaneamente (en caso contrario, remplazamos el polinomio $F(X)$ por el polinomio $F(2X)/16$). El discriminante del polinomio $F(X)$ es

$$\Delta = 16a^4c - 4a^3b^2 - 128a^2c^2 + 144ab^2c - 27b^4 + 256c^3.$$

El siguiente teorema nos da la respuesta, excepto en un caso que será estudiado en la siguiente sección, a las dos problemas en que estamos interesados.

3.1. Teorema. *Con las anteriores hipótesis y notaciones, suponemos además que no estamos en el caso*

$$a, b \text{ pares, } c \text{ impar.}$$

Entonces el tipo de descomposición del primo 2 en $\mathcal{O}$ y, cuando 2 ramifica salvajemente en K, el valor 2-ádico del discriminante absoluto de K, ν, vienen dados en las siguientes tablas:

Tabla 4.1. $p = 2$.

Condiciones			$2\mathcal{O}$	ν
$v(a)$	$v(b)$	$v(c)$		
0	0		$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$	
	≥ 1	0	*Ver tabla* 4.2	
		≥ 1	*Ver tabla* 4.3	
≥ 1	0	0	$\mathfrak{p}$	
		≥ 1	$\mathfrak{pqr}$	
	≥ 1	0	*Ver* §4 *	
		≥ 1	*Ver tabla* 4.4	

* *Antes cambiar* $F(X)$ *por* $F(X+1)$

Tabla 4.2. $p = 2$; a, c *impares,* b *par.*

$v(-a+b+1)$	$v(-a+c)$		$2\mathcal{O}$	ν
1			$\mathfrak{p}^2$	4
	1			
2	≥ 2	$v(3a-c+2)=2$	$\mathfrak{p}$	
		$v(3a-c+2)\geq 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	
≥ 3	2		$\mathfrak{p}$	
	≥ 3		$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	

Tabla 4.3. $p = 2$; *a impar, b, c pares.*

$v(c_0)$ *	$v(\Delta)$		$2\mathcal{O}$	ν
1	*impar*		$\mathfrak{p}^2\mathfrak{q}^2$	5
	par **	$v(\delta\Delta_2 - 1) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	4
		$v(\delta\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}^2$	2
		$v(\delta\Delta_2 - 1) \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	2
2	*impar*		$\mathfrak{p}\mathfrak{q}^2$	3
	par	$v(\Delta_2 - 1) = 1$	$\mathfrak{p}\mathfrak{q}^2$	2
		$v(\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}$	
		$v(\Delta_2 - 1) \geq 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	
≥ 3	*impar*		$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	3
	par	$v(\Delta_2 - 1) = 1$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	2
		$v(\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}$	
		$v(\Delta_2 - 1) \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}\mathfrak{s}$	

* $c_0 := \begin{cases} c & si\ v(b) = 1, \\ a + b + c + 1 & si\ v(b) \geq 2. \end{cases}$

** $\delta := 5 - a_0 c_0$, $a_0 := \begin{cases} a & si\ v(b) = 1, \\ a + 6 & si\ v(b) \geq 2. \end{cases}$

Tabla 4.4. $p = 2$; a, b, c *pares.*

$v(a)$	$v(b)$	$v(c)$	$2\mathcal{O}$	*Otras condiciones*	ν
		1	$\mathfrak{p}^4$	$v(b) = 1$	4
				$v(b) = 2$	8
				$v(a) = 1, v(b) \geq 3$	9
				$v(a) \geq 2, v(b) \geq 3$	11
	1	≥ 2	$\mathfrak{pq}^3$		
1	≥ 2	2	$\mathfrak{p}^2$	$v(b) = 2$	4
				$v(b) \geq 3$	6
≥ 2	≥ 2	2	*Ver tabla* 4.5		
1	2	3	$\mathfrak{pq}^2$		2
1	2	≥ 4	$\mathfrak{pqr}^2$		2
1	≥ 3	≥ 3	*Ver tabla* 4.7		
≥ 2	2	≥ 3	$\mathfrak{pq}^3$		
≥ 2	≥ 3	3	$\mathfrak{p}^4$	$v(b) = 3$	6
				$v(a) = 2, v(b) \geq 4$	9
				$v(a) \geq 3, v(b) = 4$	10
				$v(a) \geq 3, v(b) \geq 5$	11

Tabla 4.5. $p = 2$; $v(a), v(b) \geq 2$, $v(c) = 2$.

$v(a)$	$v(b)$	$v(c-4)$		$2\mathcal{O}$		ν
	2			$\mathfrak{p}^4$		4
2	3	3	$v(2a+c-4)=4$	$\mathfrak{p}^2\mathfrak{q}^2$		4
			$v(2a+c-4)\geq 5$	$\mathfrak{p}^2$		4
≥ 3	3			$\mathfrak{p}^4$		6
	3	≥ 4				
2	≥ 4	3		$\mathfrak{p}^4$	$v(b)=4$	11
					$v(b)\geq 5$	10
≥ 3	≥ 4	3	$v(2a+c+4)=4$	$\mathfrak{p}^2$		6
			$v(2a+c+4)\geq 5$	$\mathfrak{p}^2\mathfrak{q}^2$		6
2	≥ 4	≥ 4		*Ver tabla* 4.6		
≥ 3	≥ 4	≥ 4 *	$t=8$	$\mathfrak{p}^4$		6
			$t=9$	$\mathfrak{p}^2$		4
			$t\geq 10$	$\mathfrak{p}^2\mathfrak{q}^2$		4

* $t := v(4(a+4)^2 - b^2 - 16c)$ (≥ 8)

Tabla 4.6. $p = 2$; $v(a) = 2$, $v(b), v(c-4) \geq 4$.

r, s *		$2\mathcal{O}$		ν
$r \leq s-2$		$\mathfrak{p}^4$	$r = 4$	8
			$r = 5$, $s = 7$	11
			$6 \leq r \leq s-3$	
			$r = 5$, $s \geq 8$	10
			$6 \leq r = s-2$	
$r = 6$, $s = 7$	$v(a_2 + d_2) = 1$	$\mathfrak{p}^4$		8
	$v(a_2 + d_2) = 2$	$\mathfrak{p}^2$		6
	$v(a_2 + d_2) \geq 3$	$\mathfrak{p}^2\mathfrak{q}^2$		6
$r = s-1$, $s > 7$ *impar*	$v(a_2 + d_2 - 2) = 1$	$\mathfrak{p}^4$		8
	$v(a_2 + d_2 - 2) = 2$	$\mathfrak{p}^2$		6
	$v(a_2 + d_2 - 2) \geq 3$	$\mathfrak{p}^2\mathfrak{q}^2$		6
$r \geq s = 7$	$v(a_2 + d_2 - 2) = 1$	$\mathfrak{p}^4$		8
	$v(a_2 + d_2 - 2) = 2$	$\mathfrak{p}^2\mathfrak{q}^2$		6
	$v(a_2 + d_2 - 2) \geq 3$	$\mathfrak{p}^2$		6
$r \geq s$, $s > 7$ *impar*	$v(a_2 + d_2) = 1$	$\mathfrak{p}^4$		8
	$v(a_2 + d_2) = 2$	$\mathfrak{p}^2$		6
	$v(a_2 + d_2) \geq 3$	$\mathfrak{p}^2\mathfrak{q}^2$		6
$r = 5$, $s = 6$	$v(2a_2 + d_2 - 1) = 1$	$\mathfrak{p}^4$		8
	$v(2a_2 + d_2 - 1) = 2$	$\mathfrak{p}^2\mathfrak{q}^2$		6
	$v(2a_2 + d_2 - 1) \geq 3$	$\mathfrak{p}^2$		6
$r = s-1$, $s > 6$ *par*	$v(2a_2 + d_2 - 1) = 1$	$\mathfrak{p}^4$		8
	$v(2a_2 + d_2 - 1) = 2$	$\mathfrak{p}^2$		6
	$v(2a_2 + d_2 - 1) \geq 3$	$\mathfrak{p}^2\mathfrak{q}^2$		6
$r \geq s$, s *par*	$v(d_2 - 1) = 1$	$\mathfrak{p}^4$		8
	$v(d_2 - 1) = 2$	$\mathfrak{p}^2$		6
	$v(d_2 - 1) \geq 3$	$\mathfrak{p}^2\mathfrak{q}^2$		6

* $r := v(b)\ (\geq 4)$, $s := v(d)\ (\geq 6)$, $d := a^2 - 4c$

Tabla 4.7. $p = 2$; $v(a) = 1$, $v(b), v(c) \geq 3$.

$v(\Delta)$		$2\mathcal{O}$	ν
impar *	$v(\delta\Delta_2 - 1) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	5
	$v(\delta\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}^2$	3
	$v(\delta\Delta_2 - 1) \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	3
par		$\mathfrak{p}^2\mathfrak{q}^2$	6

* $\delta := 2(b/8)^2 - a_2(c/4 + 1)$

DEMOSTRACIÓN. Primero de todo observemos que $\Delta \equiv b \pmod 2$. Para la demostración de este teorema distinguiremos inicialmente cuatro casos:

I: b impar.

II: a, c impares, b par.

III: a impar, b, c pares.

IV: a, b, c pares.

Caso I: b impar. En este caso Δ es impar y terminamos con el lema de Kummer, teniendo en cuenta que $F(X)$ factoriza (mod 2) en la forma

$$F(X) \equiv \begin{cases} (X + c)(X^3 + cX^2 + (c+1)X + 1) & \text{si } a \text{ impar,} \\ X^4 + X + 1 & \text{si } a \text{ par, } c \text{ impar,} \\ X(X+1)(X^2 + X + 1) & \text{si } a, c \text{ pares.} \end{cases}$$

Caso II: a, c impares, b par. En este caso $F(X) \equiv \phi(X)^2 \pmod 2$, donde $\phi(X) := X^2 + X + 1$, y $v(\Delta) = 4$. Como

$$F(X) = \phi(X)^2 + (-2X + a - 1)\phi(X) + (-a + b + 1)X - a + c$$

y como $v(-2X + a - 1) = 1$, el análisis del polígono $\mathbf{N}_{(v,\phi)}(F)$ nos permite acabar este caso. En efecto, sea $\zeta \in \mathbb{F}_2^{al}$ una raíz de $\overline{\phi}(X)$ y ponemos $t := \min\{v(-a + b + 1), v(-a + c)\}$, entonces tenemos que:

Si $t = 1$, el polígono consta de un solo lado, cuya pendiente es $-1/2$; por tanto, $2\mathcal{O} = \mathfrak{p}^2$ y $v(\mathrm{ind}(F)) = 0$.

Si $t = 2$, entonces el polígono consta de un solo lado S, cuya pendiente es -1, y el polinomio asociado a este lado es

$$F_S(Y) = Y^2 + (\zeta + \overline{(a-1)/2})Y + \overline{(-a+b+1)/4}\,\zeta + \overline{(-a+c)/4},$$

el cual no tiene raíces múltiples. Además, si $v(-a+b+1) = 2$, el polinomio $F_S(Y)$ es irreducible en $\mathbb{F}_4[Y]$ si y sólo si $v(3a - c + 2) = 2$; por tanto, $2\mathcal{O} = \mathfrak{p}$ o $\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$ según que $v(3a - c + 2) = 2$ ó ≥ 3, respectivamente. Mientras que si $v(-a+b+1) \geq 3$, el polinomio $F_S(Y)$ es siempre irreducible en $\mathbb{F}_4[Y]$; por tanto, $2\mathcal{O} = \mathfrak{p}$.

Si $t \geq 3$, el polígono consta de dos lados; por tanto, $2\mathcal{O} = \mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$.

Caso III: a impar, b, c pares. En este caso $F(X) \equiv X^2(X+1)^2 \pmod 2$, pero el valor $v(\Delta)$ puede ser arbitrariamente grande. Entonces tenemos que $F(X) = G(X)H(X)$ con $G(X), H(X) \in \mathbb{Q}_2[X]$ de grado 2 tales que $G(X) \equiv X^2 \pmod 2$ y $H(X) \equiv (X+1)^2 \pmod 2$.

Supongamos que $v(b) = 1$, y consideremos el polígono $\mathbf{N}_{(v,X)}(F)$. Si $v(c) = 1$, entonces la parte principal del polígono consta de un solo lado, cuya pendiente es $-1/2$; por tanto, $2\mathcal{O} = \mathfrak{p}\mathfrak{q}^2$, $\mathfrak{p}^2\mathfrak{q}^2$ o $\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$. Además, tenemos que $G(X) = X^2 + 2UX + 2V$ donde $U \in \mathbb{Z}_2$, $V \in \mathbb{Z}_2^*$ satisfacen las igualdades

$$b = 2U(a + 4U^2 - 4V), \quad c = 2V(a + 4U^2 - 2V).$$

De aquí se deduce que $v(U) = 0$ y que $2V \equiv ac + 4 \pmod 8$, con lo que se obtiene que

$$v(\Delta(G)) = 2, \quad \Delta(G)_2 \equiv 5 - ac \pmod 8;$$

por tanto, se tiene que

$$v(\Delta(H)) \equiv v(\Delta) \pmod 2, \quad \Delta(H)_2 \equiv (5 - ac)\Delta_2 \pmod 8,$$

lo que nos permite acabar. Si $v(c) = 2$, entonces la parte principal del polígono consta de un solo lado, cuya pendiente -1, y su polinomio asociado es irreducible en $\mathbb{F}_2[Y]$; por tanto, $2\mathcal{O} = \mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$, $\mathfrak{p}\mathfrak{q}^2$ o $\mathfrak{p}\mathfrak{q}\mathfrak{r}$, y terminamos con los lemas de 2.1, 2.2 y 2.3. Si $v(c) \geq 3$, entonces la parte principal del polígono consta de dos lados; por tanto, $2\mathcal{O} = \mathfrak{p}\mathfrak{q}\mathfrak{r}$, $\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$ o $\mathfrak{p}\mathfrak{q}\mathfrak{r}\mathfrak{s}$, y terminamos de nuevo con los lemas de 2.1, 2.2 y 2.3.

Cuando $v(b) \geq 2$, acabamos de forma análoga considerando el polígono $\mathbf{N}_{(v,X-1)}(F)$.

Caso IV: a, b, c pares. En este caso $F(X) \equiv X^4 \pmod 2$. El análisis del polígono $\mathbf{N}_{(v,X)}(F)$ y, cuando 2 ramifica salvajemente en K, el cálculo

explícito del valor $v(\Delta)$ nos permiten terminar excepto en dos nuevos casos:

$$\text{IV.1: } v(a), v(b) \geq 2,\ v(c) = 2.$$
$$\text{IV.2: } v(a) = 1,\ v(b), v(c) \geq 3.$$

En ambos casos el valor $v(\Delta)$ puede ser arbitrariamente grande.

Subcaso IV.1: $v(a), v(b) \geq 2$, $v(c) = 2$. En este caso el polígono $\mathbf{N}_{(v,X)}(F)$ consta de un solo lado, cuya pendiente es $-1/2$, y su polinomio asociado es $(Y + \overline{1})^2$; por tanto, $2\mathcal{O} = \mathfrak{p}^2$, $\mathfrak{p}^4$ o $\mathfrak{p}^2\mathfrak{q}^2$ y debemos continuar con el polígono en segundo orden.

El análisis del polígono (de segundo orden) $\mathbf{N}_{(v_2,\phi_2)}(F)$ (cf. capítulo 2), donde v_2 indica la valoración asociada a la terna $(v, X, 1/2)$ y $\phi_2(X)$ es el polinomio dado, en cada caso, en las tablas 4.5.0 y 4.6.0 siguientes, nos permite acabar. En efecto, es fácil comprobar que entonces sólo se pueden dar tres casos:

(i) El polígono $\mathbf{N}_{(v_2,\phi_2)}(F)$ consta de un solo lado, cuya pendiente es entera, y su polinomio asociado es $Y^2 + Y + \overline{1}$.

(ii) El polígono $\mathbf{N}_{(v_2,\phi_2)}(F)$ consta de un solo lado, cuya pendiente es no entera.

(iii) El polígono $\mathbf{N}_{(v_2,\phi_2)}(F)$ consta de dos lados.

En el primer caso $2\mathcal{O} = \mathfrak{p}^2$, en el segundo $2\mathcal{O} = \mathfrak{p}^4$ y en el tercero $2\mathcal{O} = \mathfrak{p}^2\mathfrak{q}^2$. Además, el cálculo, en cada caso, del valor $v(\mathrm{ind}(F))$ nos proporciona el valor de ν.

Por ejemplo, cuando $v(a) = 2$, $v(b), v(c-4) \geq 4$ y $r \leq s - 3$, donde $r := v(b)$, $s := v(d)$ y $d := a^2 - 4c$, entonces según la tabla 4.6.0 tomamos $\phi_2(X) := X^2 + a/2$. Puesto que

$$F(X) = \phi_2(X)^2 + bX - d/4,$$

$v_2(\phi_2) = 2$ y $v_2(bX - d/4) = 2r + 1$, entonces el polígono $\mathbf{N}_{(v_2,\phi_2)}(F)$ consta de un solo lado, de origen el punto $(0, 2r+1)$ y de final el punto $(2, 4)$. Por tanto, estamos en el caso (ii) y tenemos que $2\mathcal{O} = \mathfrak{p}^4$. Además, $v(\mathrm{ind}(F)) = 2 + r - 2 = r$; así, como $v(\Delta) = 16, 20$ ó $11 + 2r$ según que $r = 4, 5$ ó ≥ 6 respectivamente, obtenemos que $\nu = v(\Delta) - 2v(\mathrm{ind}(F)) = 8, 10$ ó 11 según que $r = 4, 5$ ó ≥ 6 respectivamente.

Tabla 4.5.0. $p = 2$; $v(a), v(b) \geq 2$, $v(c) = 2$.

$v(a)$	$v(b)$	$v(c-4)$		$\phi_2(X)$
	2			$X^2 - 2$
	3		$v(2a+c-4) = 3$	$X^2 - 2$
			$v(2a+c-4) \geq 4$	$X^2 - 2X - 2$
2	≥ 4	3		$X^2 - 2X - 2$
≥ 3	≥ 4	3		$X^2 - 2$
2	≥ 4	≥ 4		Ver tabla 4.6.0
≥ 3	≥ 4	≥ 4	$v(2a+c-4) = 4$	$X^2 - 2X - 2$
			$v(2a+c-4) \geq 5$	$X^2 - 2X - 6$

Tabla 4.6.0 $p = 2$; $v(a) = 2$, $v(b), v(c-4) \geq 4$.

r, s *		$\phi_2(X)$
$r \leq s - 3$		$X^2 + a/2$
$r = s - 2$, s impar		$X^2 + 2^{(s-3)/2}X + a/2$
$r \geq s - 1$, s impar	$v(a_2 + d_2) = 1$	$X^2 + 2^{(s-3)/2}X + a/2 + 2^{(s-1)/2}$
	$v(a_2 + d_2) \geq 2$	$X^2 + 2^{(s-3)/2}X + a/2$
$r = s - 2$, s par		$X^2 + a/2 + 2^{(s-2)/2}$
$r \geq s - 1$, s par	$v(d_2 - 1) = 1$	$X^2 + 2^{(s-2)/2}X + a/2 + 2^{(s-2)/2}$
	$v(d_2 - 1) \geq 2$	$X^2 + a/2 + 2^{(s-2)/2}$

* $r := v(b)$ (≥ 4), $s := v(d)$ (≥ 6), $d := a^2 - 4c$

Subcaso IV.2: $v(a) = 1$, $v(b), v(c) \geq 3$. En este caso el polígono $\mathrm{N}_{(v,X)}(F)$ consta de al menos dos lados, y uno de ellos tiene pendiente $-1/2$; por tanto, $2\mathcal{O} = \mathfrak{pq}^2$, $\mathfrak{p}^2\mathfrak{q}^2$ o $\mathfrak{pqr}^2$. Además, $F(X) = G(X)H(X)$ donde $G(X), H(X) \in \mathbb{Q}_2[X]$ de grado 2, y el polígono $\mathrm{N}_{(v,X)}(G)$ consta de un sólo lado, cuya pendiente es $-1/2$. Entonces obtenemos que

$$v(\Delta(G)) = 3, \quad \Delta(G)_2 \equiv \delta \pmod 8,$$

donde $\delta := 2(b/8)^2 - a_2(c/4 + 1)$; por tanto, tenemos que

$$v(\Delta(H)) \not\equiv v(\Delta) \pmod 2, \quad \Delta(H)_2 \equiv \delta\Delta_2 \pmod 8,$$

lo que nos permite acabar.

Esto termina la demostración del teorema. □

3.2. Observación. En el caso que todavía nos falta por estudiar en el teorema de 3.1,

$$a, b \text{ pares, } c \text{ impar,}$$

tenemos que $F(X) \equiv (X-1)^4 \pmod 2$ y que

$$F(X+1) = X^4 + 4X^3 + a'X^2 + b'X + c',$$

donde

$$a' := a+6,\ b' := 2a+b+4,\ c' := a+b+c+1$$

son enteros pares. Por consiguiente, nos queda por estudiar el caso, equivalente al anterior, en que el cuerpo K viene definido por un polinomio de la forma

$$X^4 + 4X^3 + aX^2 + bX + c,$$

con $a, b, c \in \mathbb{Z}$ pares; el cual será estudiado en la siguiente sección.

§4. Ramificación diádica (segunda parte)

Mantenemos las notaciones de la sección anterior. En esta sección estudiaremos la ramificación 2-ádica de un cuerpo cuártico K definido por un polinomio $F(X)$ de la forma

$$F(X) = X^4 + 4X^3 + aX^2 + bX + c,$$

con $a, b, c \in \mathbb{Z}$ pares. Como ya hemos mencionado anteriormente en la observación de 3.2, esto completará el estudio de la ramificación 2-ádica de cualquier cuerpo cuártico.

En este caso, el discriminante del polinomio $F(X)$ es

$$\begin{aligned}\Delta =& 16a^4c - 4a^3b^2 - 64a^3c + 16a^2b^2 - 320a^2bc - 128a^2c^2 + \\ & 72ab^3 + 144ab^2c - 27b^4 + 1152abc + 2304ac^2 - 256b^3 - \\ & 96b^2c - 768bc^2 + 256c^3 - 6912c^2.\end{aligned}$$

El teorema siguiente nos proporciona la respuesta a las questiones en que estamos interesados excepto en un caso, el cual será estudiado más adelante (cf. observación de 4.2, teorema de 4.3, observación de 4.4 y teorema de 4.5).

4.1. Teorema. *Con las hipótesis y notaciones anteriores, suponemos además que no estamos en el caso*

$$v(a) \geq 2,\ v(b) \geq 3,\ v(c) \geq 4.$$

Entonces el tipo de descomposición del primo 2 en $\mathcal{O}$ y, cuando 2 ramifica salvajemente en K, el valor 2-ádico del discriminante absoluto de K, ν, vienen dados en las siguientes tablas:

Tabla 4.8. *$p = 2$; a, b, c pares.*

$v(a)$	$v(b)$	$v(c)$	$2\mathcal{O}$		ν
		1	$\mathfrak{p}^4$	$v(b) = 1$	4
				$v(b) = 2$	8
				$v(a) = 1, v(b) \geq 3$	9
				$v(a) \geq 2, v(b) \geq 3$	10
	1	≥ 2	$\mathfrak{pq}^3$		
1	≥ 2	2	$\mathfrak{p}^2$	$v(b) = 2$	4
				$v(b) \geq 3$	6
≥ 2	≥ 2	2	*Ver tabla* 4.9		
1	2	3	$\mathfrak{pq}^2$		2
1	2	≥ 4	$\mathfrak{pqr}^2$		2
1	≥ 3	≥ 3	*Ver tabla* 4.11		
≥ 2	2	≥ 3	$\mathfrak{pq}^3$		
≥ 2	≥ 3	3	$\mathfrak{p}^4$	$v(b) = 3$	6
				$v(b) \geq 4$	8
≥ 2	≥ 3	≥ 4	*Ver teorema de* 4.3 *		

* *Antes cambiar $F(X)$ por $F(2X)/16$*
(cf. observación de 4.2*)*

Tabla 4.9. $p = 2$; $v(a), v(b) \geq 2$, $v(c) = 2$.

$v(a)$	$v(b)$	$v(c-4)$		$2\mathcal{O}$	ν
	2			$\mathfrak{p}^4$	4
2	3	3		$\mathfrak{p}^4$	8
≥ 3	3	3	$v(2a+c+4)) = 4$	$\mathfrak{p}^2$	6
			$v(2a+c+4)) \geq 5$	$\mathfrak{p}^2\mathfrak{q}^2$	6
2	3	≥ 4 *	$t' = 8$	$\mathfrak{p}^4$	9
			$t' = 9$	$\mathfrak{p}^2$	6
			$t' \geq 10$	$\mathfrak{p}^2\mathfrak{q}^2$	6
≥ 3	3	≥ 4		*Ver tabla* 4.10	
2	≥ 4	3	$v(2a+c-4) = 4$	$\mathfrak{p}^2$	4
			$v(2a+c-4) \geq 5$	$\mathfrak{p}^2\mathfrak{q}^2$	4
≥ 3	≥ 4			$\mathfrak{p}^4$	6
	≥ 4	≥ 4			

* $t' := v(4ab - b^2 - 16c)$ (≥ 8)

Tabla 4.10. $p = 2$; $v(a) \geq 3$, $v(b) = 3$, $v(c-4) \geq 4$.

r', s *			$2\mathcal{O}$		ν
$r' \leq s-3$			$\mathfrak{p}^4$	$r'=4$	8
				$r'>4$	9
$r'=5$, $s=7$	$v(b_2'-1)=1$	$v(a+4d_2-4)=3$	$\mathfrak{p}^4$		6
		$v(a+4d_2-4)=4$	$\mathfrak{p}^2$		4
		$v(a+4d_2-4)\geq 5$	$\mathfrak{p}^2\mathfrak{q}^2$		4
	$v(b_2'-1)\geq 2$	$v(a+4d_2+4)=3$	$\mathfrak{p}^4$		6
		$v(a+4d_2+4)=4$	$\mathfrak{p}^2$		4
		$v(a+4d_2+4)\geq 5$	$\mathfrak{p}^2\mathfrak{q}^2$		4
$r'=s-2$, $s>7$ *impar*	$v(b_2'-1)=1$	$v(a+4d_2+4)=3$	$\mathfrak{p}^4$		6
		$v(a+4d_2+4)=4$	$\mathfrak{p}^2\mathfrak{q}^2$		4
		$v(a+4d_2+4)\geq 5$	$\mathfrak{p}^2$		4
	$v(b_2'-1)\geq 2$	$v(a+4d_2-4)=3$	$\mathfrak{p}^4$		6
		$v(a+4d_2-4)=4$	$\mathfrak{p}^2$		4
		$v(a+4d_2-4)\geq 5$	$\mathfrak{p}^2\mathfrak{q}^2$		4
$r'\geq s-1$, s *impar*			$\mathfrak{p}^4$		8
$r'=s-2$, s *par*			$\mathfrak{p}^4$	$r'=4$	9
				$r'>4$	8
$r'=s-1$, s *par*			$\mathfrak{p}^4$		6
$r'\geq s=6$	$v((d_2-1)(a+2d_2+2))=4$		$\mathfrak{p}^2$		4
	$v((d_2-1)(a+2d_2+2))\geq 5$		$\mathfrak{p}^2\mathfrak{q}^2$		4
$r'\geq s$, $s>6$ *par*	$v((d_2-1)(a+2d_2-6))=4$		$\mathfrak{p}^2$		4
	$v((d_2-1)(a+2d_2-6))\geq 5$		$\mathfrak{p}^2\mathfrak{q}^2$		4

* $r' := v(b')\,(\geq 4)$, $b' := -2a+b+8$, $s := v(d)\,(\geq 6)$, $d := (a-4)^2-4c$

Tabla 4.11. $p = 2$; $v(a) = 1$, $v(b), v(c) \geq 3$.

$v(\Delta)$		$2\mathcal{O}$	ν
impar *	$v(\delta\Delta_2-1)=1$	$\mathfrak{p}^2\mathfrak{q}^2$	5
	$v(\delta\Delta_2-1)=2$	$\mathfrak{p}\mathfrak{q}^2$	3
	$v(\delta\Delta_2-1)\geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	3
par		$\mathfrak{p}^2\mathfrak{q}^2$	6

* $\delta := 2(b/8+1)^2 - a_2(c/4+1)$

DEMOSTRACIÓN. La demostración de este teorema es análoga a la del caso IV de la demostración del teorema de 3.1. De nuevo, el análisis del polígono $\mathbf{N}_{(v,X)}(F)$ y, cuando 2 ramifica salvajemente en K, el cálculo explícito del valor $v(\Delta)$ nos permiten acabar excepto en dos casos:

$$1\text{: } v(a), v(b) \geq 2,\ v(c) = 2.$$
$$2\text{: } v(a) = 1,\ v(b), v(c) \geq 3.$$

También en ambos casos el valor $v(\Delta)$ puede ser arbitrariamente grande.

Caso 1: $v(a), v(b) \geq 2$, $v(c) = 2$. En este caso el polígono $\mathbf{N}_{(v,X)}(F)$ consta de un solo lado, cuya pendiente es $-1/2$, y su polinomio asociado es $(Y + \overline{1})^2$; por consiguiente, $2\mathcal{O} = \mathfrak{p}^2$, $\mathfrak{p}^4$ o $\mathfrak{p}^2\mathfrak{q}^2$ y hemos de seguir con el polígono en segundo orden.

Al igual que en el subcaso IV.1 de la demostración del teorema de 3.1, el análisis del polígono (de segundo orden) $\mathbf{N}_{(v_2,\phi_2)}(F)$, donde v_2 indica la valoración asociada a la terna $(v, X, 1/2)$ y $\phi_2(X)$ es el polinomio dado, en cada caso, en las tablas 4.9.0 y 4.10.0 siguientes, nos permite terminar.

Tabla 4.9.0. $p = 2$; $v(a), v(b) \geq 2$, $v(c) = 2$.

$v(a)$	$v(b)$	$v(c-4)$		$\phi_2(X)$
	2			$X^2 - 2$
2	3	3		$X^2 - 2X - 2$
≥ 3	3	3		$X^2 - 2$
2	3	≥ 4	$v(2a + c + 4) = 4$	$X^2 - 6$
			$v(2a + c + 4) \geq 5$	$X^2 - 2$
≥ 3	3	≥ 4		Ver tabla 4.10.0
	≥ 4		$v(2a + c - 4) = 3$	$X^2 - 2$
			$v(2a + c - 4) \geq 4$	$X^2 - 2X - 2$

Tabla 4.10.0 $p = 2$; $v(a) \geq 3$, $v(b) = 3$, $v(c-4) \geq 4$.

r', s *		$\phi_2(X)$
$r' \leq s-3$		$X^2 + 2X + a/2 - 2$
$r' = s-2$, s impar	$v(a+4d_2-4) = 3$	$X^2 + (2^{(s-3)/2}+2)X + a/2 + 2^{(s-1)/2} - 2$
	$v(a+4d_2-4) \geq 4$	$X^2 + (2^{(s-3)/2}+2)X + a/2 - 2$
$r' \geq s-1$, s impar		$X^2 + (2^{(s-3)/2}+2)X + a/2 - 2$
$r' = s-2$, s par		$X^2 + 2X + a/2 + 2^{(s-2)/2} - 2$
$r' \geq s-1$, s par	$v(d_2-1) = 1$	$X^2 + (2^{(s-2)/2}+2)X + a/2 + 2^{(s-2)/2} - 2$
	$v(d_2-1) \geq 2$	$X^2 + 2X + a/2 + 2^{(s-2)/2} - 2$

* $r' := v(b')\,(\geq 4)$, $b' := -2a+b+8$, $s := v(d)\,(\geq 6)$, $d := (a-4)^2 - 4c$

Caso 2: $v(a) = 1$, $v(b), v(c) \geq 3$. Aquí el polígono $\mathbf{N}_{(v,X)}(F)$ consta de al menos dos lados, uno de ellos con pendiente $-1/2$; luego, $2\mathcal{O} = \mathfrak{pq}^2$, $\mathfrak{p}^2\mathfrak{q}^2$ o $\mathfrak{pqr}^2$. Ahora, el cálculo de los datos (la clase (mod 2) del valor 2-ádico del discriminante y la clase (mod 8) del impar obtenido al dividir el discriminante entre su valor 2-ádico) del factor local correspondiente al lado de pendiente $-1/2$, nos permite obtener los datos del otro factor local y, por tanto, finalizar. □

4.2. Observación. En el caso que nos falta todavía por cubrir en el teorema de 4.1,

$$v(a) \geq 2,\ v(b) \geq 3,\ v(c) \geq 4,$$

se tiene que

$$\frac{1}{16}F(2X) = X^4 + 2X^3 + a'X^2 + b'X + c',$$

donde

$$a' := \frac{a}{4},\ b' := \frac{b}{8},\ c' := \frac{c}{16}$$

son enteros.

Nos interesará estudiar el caso más general en que el cuerpo K viene definido por un polinomio de la forma

$$X^4 + 2mX^3 + aX^2 + bX + c,$$

con $a, b, c \in \mathbb{Z}$ y con $m \in \mathbb{Z}$ impar, supuesto igual a 1 siempre que sea a impar y b par. Además, para el estudio de este último caso podemos

suponer que las condiciones

$$a, b \text{ pares, } c \text{ impar}$$

no se dan simultaneamente. En efecto, si las condiciones anteriores se dan a la vez, entonces cambiando la indeterminada X por $X+1$ en el polinomio anterior se obtiene el polinomio

$$X^4 + 2m'X^3 + a'X^2 + b'X + c',$$

donde

$$a' := a + 6m + 6,\ b' := 2a + b + 6m + 4,\ c' := a + b + c + 2m + 1$$

son enteros pares y $m' := m + 2$ es un entero impar.

Después de la observación anterior, el teorema siguiente nos cubre el caso que nos falta por estudiar en el teorema de 4.1, excepto en un ulterior caso que trataremos más adelante (cf. observación de 4.4 y teorema de 4.5).

4.3. Teorema. *Supongamos que el cuerpo K viene definido por un polinomio $F(X)$ de la forma*

$$F(X) = X^4 + 2mX^3 + aX^2 + bX + c,$$

con $a, b, c \in \mathbb{Z}$ tales que c es par siempre que sean a, b pares, y con $m \in \mathbb{Z}$ impar, supuesto igual a 1 siempre que sea a impar y b par. Supongamos además que no estamos en el caso

$$v(a) \geq 2,\ v(b) \geq 3,\ v(c) \geq 4.$$

Entonces el tipo de descomposición del primo 2 en $\mathcal{O}$ y, cuando 2 ramifica salvajemente en K, el valor 2-ádico del discriminante absoluto de K, v, vienen dados en las siguientes tablas:

Tabla 4.12. $p = 2$.

$v(a)$	$v(b)$	$v(c)$	m	$2\mathcal{O}$	ν
0	0		*impar*	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$	
	≥ 1	0	1	*Ver tabla* 4.13	
		≥ 1	1	*Ver tabla* 4.15	
≥ 1	0	0	*impar*	$\mathfrak{p}$	
		≥ 1	*impar*	$\mathfrak{pqr}$	
	≥ 1	0	*impar*	*Ver tabla* 4.17 *	
		≥ 1	*impar*	*Ver tabla* 4.17	

* *Antes cambiar* $F(X)$ *por* $F(X+1)$

Tabla 4.13. $p = 2$; $m = 1$, a, c *impares*, b *par*.

t *	$v(a-3)$		$2\mathcal{O}$		ν
1			$\mathfrak{p}^2$	$v(b) = 1$	6
				$v(b) \geq 2$	4
≥ 2	1	$v(-a+b+1) = 2$	$\mathfrak{p}$		
		$v(-a+b+1) \geq 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$		
	≥ 2		*Ver tabla* 4.14		

* $t := \min\{v(-a+b+1), v(-a+c+2)\}$

Tabla 4.14. $p = 2$; $m = 1$, $v(a-3), v(c-1) \geq 2$, $v(b) = 1$.

r', s *			$2\mathcal{O}$	ν
$\min\{r', s-2\}$ *impar*			$\mathfrak{p}^2$	6
$r' < s-2$, r' *par* *1	$t' = 2$		$\mathfrak{p}^2$	4
	$t' \geq 3$	$v(\Delta_2 - 1) = 2$	$\mathfrak{p}$	
		$v(\Delta_2 - 1) \geq 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	
$r' = s-2$, r' *par* *2	$t'' = 2$		$\mathfrak{p}^2$	4
	$t'' \geq 3$	$v(\Delta_2 - 1) = 2$	$\mathfrak{p}$	
		$v(\Delta_2 - 1) \geq 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	
$r' > s-2$, s *par* *3	$t''' = 1$		$\mathfrak{p}^2$	4
	$t''' \geq 2$	$v(\Delta_2 - 1) = 2$	$\mathfrak{p}$	
		$v(\Delta_2 - 1) \geq 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	

* $r' := v(b')$, $b' := -a + b + 1$, $s := v(d)$, $d := (a-1)^2 - 4c$

*1 $t' := \min\{v(b_2' + 1 - 2^{r'/2}) + 1, v(d/2^{r'+1} + a - 3 + 2^{(r'+2)/2})\}$

*2 $t'' := \min\{v(b_2' - 1 - 2^{r'/2}) + 1, v(2d_2 + a - 1)\}$

*3 $t''' := \min\{v(b'/2^{s-2}), v(d_2 - 1)\}$

Tabla 4.15. $p = 2$; $m = 1$, *a impar, b, c pares.*

$v(b)$	$v(c)$	$v(a-1)$	$v(\Delta)$		$2\mathcal{O}$	ν
1 *	1			$v(c') = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	4
				$v(c') = 2$	$\mathfrak{p}\mathfrak{q}^2$	2
				$v(c') \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	2
	2			$v(c') = 1$	$\mathfrak{p}\mathfrak{q}^2$	2
				$v(c') = 2$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	
				$v(c') \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}$	
	≥ 3			$v(c') = 1$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	2
				$v(c') = 2$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}$	
				$v(c') \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}\mathfrak{s}$	
≥ 2	1		*impar* *1	$v(\delta'\Delta_2 - 1) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	5
				$v(\delta'\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}^2$	3
				$v(\delta'\Delta_2 - 1) \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	3
			par		$\mathfrak{p}^2\mathfrak{q}^2$	6
	≥ 2	1	*impar* *2	$v(\delta''\Delta_2 - 1) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	5
				$v(\delta''\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}^2$	3
				$v(\delta''\Delta_2 - 1) \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	3
			par		$\mathfrak{p}^2\mathfrak{q}^2$	6
		≥ 2			*Ver tabla* 4.16	

* $c' := a + b + c + 3$

*1 $\delta' := 2(b/4 + 1)^2 - a(c_2 + 2)$

*2 $\delta'' := 2(b/4 + 1)^2 - (a - b - c + 3)/2$

Tabla 4.16. $p = 2$; $m = 1$, $v(a-1), v(b), v(c) \geq 2$.

r', s *		$v(\Delta)$		$2\mathcal{O}$	ν
$r' \leq s-2$, r' *impar*		*impar* *1	$v(\delta'\Delta_2 - 1) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	5
			$v(\delta'\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}^2$	3
			$v(\delta'\Delta_2 - 1) \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	3
		par		$\mathfrak{p}^2\mathfrak{q}^2$	6
$r' \leq s-2$, r' *par* *2	$t'' = 1$	*impar*		$\mathfrak{p}^2\mathfrak{q}^2$	5
		par	$v(\delta''\Delta_2 - 1) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	4
			$v(\delta''\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}^2$	2
			$v(\delta''\Delta_2 - 1) \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	2
	$t'' = 2$	*impar*		$\mathfrak{p}\mathfrak{q}^2$	3
		par	$v(\Delta_2 - 1) = 1$	$\mathfrak{p}\mathfrak{q}^2$	2
			$v(\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}$	
			$v(\Delta_2 - 1) \geq 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	
	$t'' \geq 3$	*impar*		$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	3
		par	$v(\Delta_2 - 1) = 1$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	2
			$v(\Delta_2 - 1) = 2$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}$	
			$v(\Delta_2 - 1) \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}\mathfrak{s}$	
$r' \geq s-1$, s *impar*				$\mathfrak{p}^2\mathfrak{q}^2$	6
$r' = s-1$, s *par* *3			$t''' = 3$	$\mathfrak{p}\mathfrak{q}^2$	2
			$t''' \geq 4$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$	2
$r' = s$, s *par*			$v(d_2 - 1) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	4
			$v(d_2 - 1) \geq 2$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}$	
$r' \geq s+1$, s *par*			$v(d_2 - 1) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	4
			$v(d_2 - 1) = 2$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	
			$v(d_2 - 1) \geq 3$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}\mathfrak{s}$	

* $r' := v(b')$, $b' := -a + b + 1$, $s := v(d)$, $d := (a-1)^2 - 4c$

*1 $\delta' := d/2^{r'+2} + b'_2 a_0 + 2^{r'-2}$, $a_0 := \begin{cases} (a+1)/2 & si\ r' < s-2, \\ (1-a)/2 & si\ r' = s-2. \end{cases}$

*2 $t'' := v(\delta'' - 1)$, $\delta'' := \begin{cases} d/16 + b'_2(1-a_0) + 1 & si\ r' = 2, \\ d/2^{r'+2} + b'_2 a_0 + 2^{r'/2} & si\ r' > 2. \end{cases}$

*3 $t''' := v((d_2-1)^2 + 2b'_2(d_2 + a + 2^{s/2} - 2))$

Tabla 4.17. $p = 2$; *m impar*, a, b, c *pares*.

$v(a)$	$v(b)$	$v(c)$	$2\mathcal{O}$		ν
		1	$\mathfrak{p}^4$	$v(b) = 1$	4
				$v(b) \geq 2$	6
	1	≥ 2	$\mathfrak{pq}^3$		
1	≥ 2	2	$\mathfrak{p}^2$		4
≥ 2	≥ 2	2	*Ver tabla* 4.18		
1	2	3	$\mathfrak{pq}^2$		3
1	2	≥ 4	$\mathfrak{pqr}^2$		3
1	≥ 3	≥ 3	*Ver tabla* 4.19		
≥ 2	2	≥ 3	$\mathfrak{pq}^3$		
≥ 2	≥ 3	3	$\mathfrak{p}^4$		4
≥ 2	≥ 3	≥ 4	*Ver teorema de* 4.5 *		

* *Antes cambiar* $F(X)$ *por* $F(2X)/16$

Tabla 4.18. $p = 2$; *m impar*, $v(a), v(b) \geq 2$, $v(c) = 2$.

$v(b)$		$2\mathcal{O}$	ν
2	$v(2a + c + 4) = 3$	$\mathfrak{p}^2$	4
	$v(2a + c + 4) \geq 4$	$\mathfrak{p}^2\mathfrak{q}^2$	5
≥ 3		$\mathfrak{p}^4$	4

Tabla 4.19. $p = 2$; *m impar*, $v(a) = 1$, $v(b), v(c) \geq 3$.

$v(\Delta)$		$2\mathcal{O}$	ν
impar		$\mathfrak{p}^2\mathfrak{q}^2$	5
par *	$v(\delta\Delta_2 - 1) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$	4
	$v(\delta\Delta_2 - 1) = 2$	$\mathfrak{pq}^2$	2
	$v(\delta\Delta_2 - 1) \geq 3$	$\mathfrak{pqr}^2$	2

* $\delta := 1 - 2a_2(c/4 + 1)$

DEMOSTRACIÓN. En primer lugar, observemos que el discriminante del polinomio $F(X)$ es

$$\begin{aligned}\Delta =&16a^4c - 4a^3b^2 - 16m^2a^3c + 4m^2a^2b^2 - 160ma^2bc - 128a^2c^2 + \\ &36mab^3 + 144ab^2c - 27b^4 + 144m^3abc + 576m^2ac^2 - 32m^3b^3 - \\ &24m^2b^2c - 384mbc^2 + 256c^3 - 432m^4c^2;\end{aligned}$$

en particular, tenemos que $\Delta \equiv b \pmod 2$. Comenzamos distinguiendo cuatro casos:

$$\begin{aligned}&\text{I: } m, b \text{ impares.}\\ &\text{II: } m = 1,\ a, c \text{ impares, } b \text{ par.}\\ &\text{III: } m = 1,\ a \text{ impar, } b, c \text{ pares.}\\ &\text{IV: } m \text{ impar, } a, b, c \text{ pares.}\end{aligned}$$

Caso I: m, b impares. En este caso Δ es impar y acabamos con el lema de Kummer.

Caso II: $m = 1$, a, c impares, b par. En este caso tenemos que $F(X) \equiv (X^2+X+1)^2 \pmod 2$ y que el valor $v(\Delta)$ puede ser arbitrariamente grande; concretamente

$$v(\Delta) = \begin{cases} 4 & \text{si } v(b) \geq 2,\\ 6 & \text{si } v(b) = 1,\ c \equiv a \pmod 4\\ & \text{o si } v(b) = 1,\ c \not\equiv a \equiv 1 \pmod 4,\\ 4 + 2\min\{r', s-2\} & \text{si } v(b) = 1,\ c \not\equiv a \equiv 3 \pmod 4,\end{cases}$$

donde $r' := v(b')$, $b' := -a + b + 1$, $s := v(d)$ y $d := (a-1)^2 - 4c$.

El análisis del polígono $\mathbf{N}_{(v,\phi)}(F)$, donde $\phi(X)$ es el polinomio dado, en cada caso, en la tabla 4.13.0 siguiente, nos permite terminar. En efecto, es fácil comprobar que entonces sólo se pueden dar tres casos:

(i) El polígono $\mathbf{N}_{(v,\phi)}(F)$ consta de un solo lado, cuya pendiente es entera, y su polinomio asociado es de la forma $Y^2 + \alpha Y + \beta$, con $\alpha, \beta \in \mathbb{F}_4^*$.

(ii) El polígono $\mathbf{N}_{(v,\phi)}(F)$ consta de un solo lado, cuya pendiente es no entera.

(iii) El polígono $\mathbf{N}_{(v,\phi)}(F)$ consta de dos lados.

En el primer caso el polinomio asociado no tiene raíces múltiples. Además, este polinomio es irreducible en $\mathbb{F}_4[Y]$ si y sólo si $\beta \neq \alpha^2$; por tanto, $2\mathcal{O} = \mathfrak{p}$ o $\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$ según que $\beta \neq \alpha^2$ o $\beta = \alpha^2$, respectivamente. En el segundo caso $2\mathcal{O} = \mathfrak{p}^2$ y el cálculo del valor $v(\mathrm{ind}(F))$ nos da el valor de ν. En el tercer caso $2\mathcal{O} = \mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$.

Tabla 4.13.0 $p = 2$; $m = 1$, a, c impares, b par.

t *	$v(a-3)$		$\phi(X)$
1			$X^2 + X + 1$
	1		
≥ 2	≥ 2	$\min\{r', s-2\}$ impar	$X^2 + X + (a-1)/2$
		$r' < s-2$, r' par	$X^2 + (2^{r'/2}+1)X + (a-1)/2 + 2^{r'/2}$
		$r' = s-2$, r' par	$X^2 + (2^{r'/2}+1)X + (a-1)/2$
		$r' > s-2$, s par	$X^2 + X + (a-1)/2 + 2^{(s-2)/2}$

* $t := \min\{r', v(-a+c+2)\}$

Caso III: $m = 1$, a impar, b, c pares. En este caso tenemos que $F(X) \equiv X^2(X+1)^2 \pmod 2$ y que el valor $v(\Delta)$ puede ser arbitrariamente grande. Por tanto, tenemos que $F(X) = G(X)H(X)$ con $G(X), H(X) \in \mathbb{Q}_2[X]$ de grado 2 tales que $\overline{G}(X) = X^2$ y $\overline{H}(X) = (X+\overline{1})^2$.

Si $v(b) = 1$, entonces $v(\Delta) = 4$ y el análisis simultaneo de los polígonos $\mathbf{N}_{(v,X)}(F)$ y $\mathbf{N}_{(v,X-1)}(F)$ nos permite acabar.

Si $v(b) \geq 2$ y $v(c) = 1$, entonces la parte principal del polígono $\mathbf{N}_{(v,X)}(F)$ consta de un solo lado, cuya pendiente es $-1/2$; por tanto, $2\mathcal{O} = \mathfrak{pq}^2$, $\mathfrak{p}^2\mathfrak{q}^2$ o $\mathfrak{pqr}^2$. Además, es fácil ver que

$$v(\Delta(G)) = 3, \quad \Delta(G)_2 \equiv \delta' \pmod 8;$$

donde $\delta' := 2(b/4+1)^2 - a(c_2+2)$; por tanto, se tiene que

$$v(\Delta(H)) \not\equiv v(\Delta) \pmod 2, \quad \Delta(H)_2 \equiv \delta'\Delta_2 \pmod 8,$$

lo que nos permite terminar.

Si $v(a-1)=1$ y $v(b),v(c)\geq 2$, entonces acabamos de forma análoga que en el caso anterior considerando ahora la parte principal del polígono $\mathrm{N}_{(v,X-1)}(F)$ y calculando los datos del correspondiente factor local.

Por último, supongamos que $v(a-1),v(b),v(c)\geq 2$. La principal obstrucción en este caso es que no sólo el valor $v(\Delta)=v(\Delta(G))+v(\Delta(H))$ puede ser arbitrariamente grande, sino que también los valores $v(\Delta(G))$ y $v(\Delta(H))$ pueden ser arbitrariamente grandes simultaneamente. Para solucionar este caso ponemos $b':=-a+b+1$, $r':=v(b')$, $d:=(a-1)^2-4c$, $s:=v(d)$, y distinguimos dos subcasos:

$$\text{III.1: } r'\leq s-2.$$
$$\text{III.2: } r'\geq s-1.$$

Subcaso III.1: $r'\leq s-2$. Elegimos (siempre lo podemos hacer) enteros M y N tales que $v(8M^2+4M+a-1)>r'$ y $v(8N^2+12N+a+3)>r'$, y definimos los polinomios

$$\phi^0(X):=\begin{cases} X-2M & \text{si } r' \text{ impar o } r'=2,\\ X-(2M+2^{r'/2}) & \text{si } r'>2 \text{ par},\end{cases}$$
$$\phi^1(X):=\begin{cases} X-(2N+1) & \text{si } r' \text{ impar o } r'=2,\\ X-(2N+2^{r'/2}+1) & \text{si } r'>2 \text{ par}.\end{cases}$$

Entonces el análisis de uno de los polígonos $\mathrm{N}_{(v,\phi^i)}(F)$, y el cálculo de los datos del correspondiente factor local (cuando ya sabemos que $2\mathcal{O}=\mathfrak{pq}^2$, $\mathfrak{p}^2\mathfrak{q}^2$ o $\mathfrak{pqr}^2$) o los lemas de 2.1, 2.2 y 2.3 (cuando ya sabemos que $2\mathcal{O}=\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$, $\mathfrak{pq}^2$ o $\mathfrak{pqr}$, o que $2\mathcal{O}=\mathfrak{pqr}$, $\mathfrak{pqr}^2$ o $\mathfrak{pqrs}$) nos permiten terminar en este subcaso. Concretamente, cuando $2=r'<s-2$ o cuando $2<r'=s-2$ procedemos con el polígono $\mathbf{N}_{(v,\phi^0)}(F)$, mientras que en el resto de los casos lo hacemos con el $\mathrm{N}_{(v,\phi^1)}(F)$.

Subcaso III.2: $r'\geq s-1$. Aquí $v(\Delta)=2s$. Elegimos enteros M y N tales que $v(8M^2+4M+a-1)>s/2$ y $v(8N^2+12N+a+3)>s/2$, y definimos los polinomios

$$\phi^0(X):=\begin{cases} X-2M & \text{si } s \text{ impar},\\ X-(2M+2^{(s-2)/2}) & \text{si } s \text{ par},\end{cases}$$
$$\phi^1(X):=\begin{cases} X-(2N+1) & \text{si } s \text{ impar},\\ X-(2N+2^{(s-2)/2}+1) & \text{si } s \text{ par}.\end{cases}$$

Entonces es fácil comprobar que el análisis simultaneo de los polígonos $\mathrm{N}_{(v,\phi^0)}(F)$ y $\mathrm{N}_{(v,\phi^1)}(F)$ nos permite terminar.

Caso IV: m impar, a, b, c pares. En este caso $F(X) \equiv X^4 \pmod 2$. Como siempre, el análisis del polígono $\mathrm{N}_{(v,X)}(F)$ y, cuando 2 ramifica salvajemente en K, el cálculo explícito del valor $v(\Delta)$ nos permiten terminar excepto en dos subcasos:

$$\text{IV.1: } v(a), v(b) \geq 2,\ v(c) = 2.$$
$$\text{IV.2: } v(a) = 1,\ v(b), v(c) \geq 3.$$

Subcaso IV.1: $v(a), v(b) \geq 2$, $v(c) = 2$. En este caso tenemos que

$$v(\Delta) = \begin{cases} 8 & \text{si } v(b) \geq 3, \\ 10 & \text{si } v(b) = 2,\ v(2a + c + 4) = 3, \\ 11 & \text{si } v(b) = 2,\ v(2a + c + 4) \geq 4, \end{cases}$$

y que el polígono $\mathrm{N}_{(v,X)}(F)$ consta de un solo lado, cuya pendiente es $-1/2$, y su polinomio asociado es $(Y + \overline{1})^2$; por tanto, $2\mathcal{O} = \mathfrak{p}^2$, $\mathfrak{p}^4$ o $\mathfrak{p}^2\mathfrak{q}^2$ y hemos de continuar con el polígono en segundo orden.

Consideramos la valoración v_2 asociada a la terna $(v, X, 1/2)$ y definimos el polinomio $\phi_2(X) := X^2 - 2$. Entonces el análisis del polígono (de segundo orden) $\mathrm{N}_{(v_2,\phi_2)}(F)$ nos permite acabar.

Subcaso IV.2: $v(a) = 1$, $v(b), v(c) \geq 3$. En este caso el valor $v(\Delta)$ puede ser arbitrariamente grande y tenemos que el polígono $\mathrm{N}_{(v,X)}(F)$ consta de al menos dos lados, uno de ellos con pendiente $-1/2$; por tanto, $2\mathcal{O} = \mathfrak{p}\mathfrak{q}^2$, $\mathfrak{p}^2\mathfrak{q}^2$ o $\mathfrak{p}\mathfrak{q}\mathfrak{r}^2$. Además, si $G(X) \in \mathbb{Q}_2[X]$ es el factor de $F(X)$ correspondiente al lado con pendiente $-1/2$, entonces obtenemos que

$$v(\Delta(G)) = 2, \quad \Delta(G)_2 \equiv \delta \pmod 8,$$

donde $\delta := 1 - 2a_2(c/4 + 1)$; por tanto, si ponemos $H(X) := F(X)/G(X)$, tenemos que

$$v(\Delta(H)) \equiv v(\Delta) \pmod 2, \quad \Delta(H)_2 \equiv \delta\Delta_2 \pmod 8,$$

con lo que acabamos en este subcaso.

Con esto queda terminada la demostración del teorema. □

4.4. Observación. En el caso que nos falta todavía por estudiar en el teorema de 4.3, m impar y

$$v(a) \geq 2,\ v(b) \geq 3,\ v(c) \geq 4,$$

se tiene que

$$\frac{1}{16}F(2X) = X^4 + mX^3 + a'X^2 + b'X + c',$$

donde

$$a' := \frac{a}{4},\ b' := \frac{b}{8},\ c' := \frac{c}{16},$$

son enteros. Por consiguiente, ahora nos queda por estudiar el caso, equivalente al anterior, en que el cuerpo K viene definido por un polinomio de la forma

$$X^4 + mX^3 + aX^2 + bX + c,$$

con $a, b, c \in \mathbb{Z}$ y $m \in \mathbb{Z}$ impar.

Después de la observación anterior, con el próximo teorema completamos, sin excepciones, el caso que nos falta por estudiar en el teorema de 4.3. Por consiguiente, quedará cubierto finalmente el caso que nos faltaba en el teorema de 4.1.

4.5. Teorema. *Supongamos que el cuerpo K viene definido por un polinomio $F(X)$ de la forma*

$$F(X) = X^4 + mX^3 + aX^2 + bX + c,$$

con $a, b, c \in \mathbb{Z}$ y $m \in \mathbb{Z}$ impar. Entonces el tipo de descomposición del primo 2 en $\mathcal{O}$ y, cuando 2 ramifica salvajemente en K, el valor 2-ádico del discriminante absoluto de K, ν, vienen dados en las siguientes tablas:

Tabla 4.20. *$p = 2$; m impar.*

a, b, c		$2\mathcal{O}$	ν
$a \equiv b \pmod 2$	*c impar*	$\mathfrak{p}$	
	c par	*Ver tabla* 4.21	
$a \not\equiv b \equiv c \pmod 2$		*Ver tabla* 4.22	
$a \not\equiv b \not\equiv c \pmod 2$		$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$	

Tabla 4.21. $p = 2$; *m impar*, $a \equiv b \pmod 2$, *c par*.

$v(U)$, $v(V)$, $v(\Delta)$ *		$2\mathcal{O}$	ν
$3v(U) < 2v(V)$, $v(\Delta)$ *impar*		$\mathfrak{pqr}^2$	3
$3v(U) < 2v(V)$, $v(\Delta)$ *par*	$v(\Delta_2 - 1) = 1$	$\mathfrak{pqr}^2$	2
	$v(\Delta_2 - 1) = 2$	$\mathfrak{pqr}$	
	$v(\Delta_2 - 1) \geq 3$	$\mathfrak{pqrs}$	
$3v(U) = 2v(V)$		$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$	
$3v(U) > 2v(V)$, $3 \nmid v(V)$		$\mathfrak{pq}^3$	
$3v(U) > 2v(V)$, $3 \mid v(V)$		$\mathfrak{pqr}$	

* $U := 3(a^2 - 3mb + 12c)$,
$V := 2a^3 - 9mab - 72ac + 27b^2 + 27m^2c$

Tabla 4.22. $p = 2$; *m impar*, $a \not\equiv b \equiv c \pmod 2$.

$v(\Delta)$		$2\mathcal{O}$	ν
impar		$\mathfrak{pq}^2$	3
par	$v(\Delta_2 - 1) = 1$	$\mathfrak{pq}^2$	2
	$v(\Delta_2 - 1) = 2$	$\mathfrak{pqr}$	
	$v(\Delta_2 - 1) \geq 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	

DEMOSTRACIÓN. Primero de todo, observemos que el discriminante del polinomio $F(X)$ es

$$\begin{aligned}\Delta =& 16a^4c - 4a^3b^2 - 4m^2a^3c + m^2a^2b^2 - 80ma^2bc - 128a^2c^2 + \\ & 18mab^3 + 144ab^2c - 27b^4 + 18m^3abc + 144m^2ac^2 - 4m^3b^3 - \\ & 6m^2b^2c - 192mbc^2 + 256c^3 - 27m^4c^2;\end{aligned}$$

en particular, tenemos que $\Delta \equiv ab + b + c \pmod 2$. Para la demostración del teorema distinguimos tres casos:

$$\text{I: } ab + b + c \text{ impar.}$$
$$\text{II: } a \equiv b \pmod 2,\ c \text{ par.}$$
$$\text{III: } a \not\equiv b \equiv c \pmod 2.$$

Caso I: $ab + b + c$ impar. En este caso Δ es impar y, por tanto, se acaba con el lema de Kummer, teniendo presente que $F(X)$ factoriza

(mod 2) en la forma

$$F(X) \equiv \begin{cases} X^4 + X^3 + aX^2 + aX + 1 & \text{si } a \equiv b \pmod 2, \\ (X+a)(X^3 + (a+1)X^2 + aX + 1) & \text{si } a \not\equiv b \pmod 2. \end{cases}$$

Caso II: $a \equiv b \pmod 2$, c par. En este caso tenemos que $F(X) \equiv (X+a)^3(X+a+1) \pmod 2$ y que el valor $v(\Delta)$ puede ser arbitrariamente grande. Entonces $F(X) = (X-\theta)H(X)$ con $\theta \in \mathbb{Q}_2$ y $H(X) \in \mathbb{Q}_2[X]$ tales que $\theta \equiv a+1 \pmod 2$ y $H(X) \equiv (X+a)^3 \pmod 2$.

Para el estudio del factor $H(X)$, consideramos la resolvente cúbica del polinomio $F(X)$

$$G(X) := X^3 - 2aX^2 + (a^2 + mb - 4c)X - (mab - b^2 - m^2c)$$

(cf. lema de 2.4) y el polinomio

$$G_0(X) := 27G((X+2a)/3) = X^3 - UX + V,$$

donde $U := 3(a^2 - 3mb + 12c)$, $V := 2a^3 - 9mab - 72ac + 27b^2 + 27m^2c$ son ambos enteros pares. Notemos que $\Delta(G_0) = 3^6\Delta(G) = 3^6\Delta$. El análisis del polígono $\mathbf{N}_{(v,X)}(G_0)$ junto con la aplicación del lema de 2.4 (al cuerpo $L = \mathbb{Q}_2$) y de los lemas de 2.1, 2.2 y 2.3 nos permitirán terminar este caso.

Supongamos que $3v(U) < 2v(V)$. Entonces el polígono $\mathbf{N}_{(v,X)}(G_0)$ consta de dos lados; por tanto, el polinomio $G_0(X)$ tiene al menos una raíz en $\mathbb{Q}_2$. Entonces, por la parte (a) del lema de 2.4, $F(X)$ tiene al menos dos raíces en $\mathbb{Q}_2$; por consiguiente, $2\mathcal{O} = \mathfrak{pqr}$, $\mathfrak{pqr}^2$ o $\mathfrak{pqrs}$ y acabamos con los lemas de 2.1, 2.2 y 2.3.

Ahora, supongamos que $3v(U) = 2v(V)$ (resp. que $3v(U) > 2v(V)$ y $3 \nmid v(V)$). Entonces el polígono $\mathbf{N}_{(v,X)}(G_0)$ consta de un solo lado, cuya pendiente es entera (resp. es no entera), y su polinomio asociado es irreducible en $\mathbb{F}_2[Y]$; por tanto, la extensión $\mathbb{Q}_2(\eta_0)/\mathbb{Q}_2$, donde η_0 es una raíz de $G_0(X)$, es cúbica y no ramificada (resp. es cúbica y totalmente ramificada). Entonces, por la parte (b) del lema de 2.4, la extensión $\mathbb{Q}_2(\theta')/\mathbb{Q}_2$, donde θ' es una raíz de $H(X)$, es cúbica y no ramificada (resp. es cúbica y totalmente ramificada); luego, $2\mathcal{O} = \mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$ (resp. $2\mathcal{O} = \mathfrak{pq}^3$).

Finalmente, supongamos que $3v(U) > 2v(V)$ y $3 \mid v(V)$. Entonces el polígono $\mathbf{N}_{(v,X)}(G_0)$ consta de un solo lado, cuya pendiente es entera,

y su polinomio asociado es $Y^3 + \overline{1} = (Y + \overline{1})(Y^2 + Y + \overline{1})$ en $\mathbb{F}_2[Y]$; por consiguiente, $G_0(X)$ tiene una única raíz en $\mathbb{Q}_2$ y la extensión cuadrática $\mathbb{Q}_2(\sqrt{\Delta(G_0)})/\mathbb{Q}_2$ es no ramificada. Entonces, de nuevo por la parte (a) del lema de 2.4, $F(X)$ tiene exactamente dos raíces en $\mathbb{Q}_2$ y la extensión cuadrática $\mathbb{Q}_2(\sqrt{\Delta})/\mathbb{Q}_2$ es no ramificada; así, $2\mathcal{O} = \mathfrak{pqr}$.

Caso III: $a \not\equiv b \equiv c \pmod 2$. En este caso se tiene en cambio que $F(X) \equiv (X + a + 1)^2(X^2 + X + 1) \pmod 2$. Por tanto, tenemos que $2\mathcal{O} = \mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$, $\mathfrak{pq}^2$ o $\mathfrak{pqr}$ y acabamos con los lemas de 2.1, 2.2 y 2.3.

Queda, por tanto, terminada la demostración del teorema. □

Desde luego, para ciertas familias de cuerpos cuárticos (como, por ejemplo, los cuerpos cuárticos definidos por polinomios bicuadráticos o los procedentes del estudio de los puntos de 3-torsión de una curva elíptica definida sobre $\mathbb{Q}$) la división anterior de casos se simplifica extraordinariamente. Finalizamos esta sección poniendo un ejemplo de ello.

Supongamos que partimos de una curva elíptica E definida sobre $\mathbb{Q}$ de ecuación $y^2 = x^3 - Ax + B$, con $A, B \in \mathbb{Z}$. Entonces las abscisas de los puntos de 3-torsión de E han de satisfacer la ecuación

$$X^4 + aX^2 + bX + c = 0,$$

con $a := -18A$, $b := 108B$, $c := -27A^2$. Observemos que tenemos que $a^2 + 12c = 0$. De los resultados de la sección anterior y de ésta, obtenemos el siguiente criterio simple para decidir cuando el primo 2 descompone en la forma $\mathfrak{p}^2\mathfrak{q}^2$ en el cuerpo cuártico obtenido al adjuntar a $\mathbb{Q}$ la abscisa de un punto de 3-torsión de la curva elíptica E, supuesto irreducible el polinomio $X^4 + aX^2 + bX + c$ en $\mathbb{Q}[X]$.

4.6. Corolario. *Supongamos que el cuerpo K viene definido por un polinomio de la forma $X^4 + aX^2 + bX + c$, donde $a, b, c \in \mathbb{Z}$ con $a^2 + 12c = 0$ y tales que las condiciones*

$$v(a) \geq 2,\ v(b) \geq 3,\ v(c) \geq 4,$$

no se dan simultaneamente. Entonces

$$2\mathcal{O} = \mathfrak{p}^2\mathfrak{q}^2 \iff v(a-4) \geq 4 \text{ y } v(b) = 5;$$

además, en tal caso, el valor 2-ádico del discriminante del cuerpo es 6. □

§5. Ramificación triádica

Dedicamos esta sección al estudio de la ramificación 3-ádica en el cuerpo cuártico K; luego, suponemos que $p = 3$.

Denotamos por v, en esta sección, a la valoración 3-ádica extendida a $\mathbb{Q}_3(X)$ de forma que $v(X) = 0$, y ponemos $\nu := v(\Delta(K))$. Recordemos que dado un entero 3-ádico $u \neq 0$ denotamos por u_3 a la unidad 3-ádica $u/3^{v(u)}$ y por $\overline{u}$ a la clase de u (mod 3).

En esta sección suponemos (siempre lo podemos hacer) que el polinomio $F(X)$ es de la forma

$$F(X) = X^4 + aX^2 + bX + c,$$

con $a, b, c \in \mathbb{Z}$ tales que las condiciones

$$v(a) \geq 2,\ v(b) \geq 3,\ v(c) \geq 4,$$

no se dan a la vez. Además, definimos el entero

$$d := a^2 - 4c.$$

El primo 3 sólo tiene un tipo de ramificación salvaje en K; a saber, $3\mathcal{O} = \mathfrak{p}\mathfrak{q}^3$. El siguiente teorema nos da, en todos los casos, la respuesta a las dos questiones en que estamos interesados.

5.1. Teorema. *Con las hipótesis y notaciones anteriores, el tipo de descomposición del primo 3 en $\mathcal{O}$ y, cuando $3\mathcal{O} = \mathfrak{p}\mathfrak{q}^3$, el valor 3-ádico del discriminante absoluto de K, ν, vienen dados en las siguientes tablas:*

Tabla 4.23. $p = 3$.

$v(a)$	$v(b)$	$v(c)$		$3\mathcal{O}$	ν
0	0	0	$a \equiv c \equiv 1 \pmod 3$	$\mathfrak{p}$	
			$a \equiv c \equiv -1 \pmod 3$	*Ver tabla* 4.24	
			$a \not\equiv c \pmod 3$	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$	
		≥ 1	$a \equiv 1 \pmod 3$	$\mathfrak{pqr}$	
			$a \equiv -1 \pmod 3$	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$	
	≥ 1	0	$a \equiv c \equiv 1 \pmod 3$	*Ver tabla* 4.25	
			$a \not\equiv c \equiv 1 \pmod 3$	*Ver tabla* 4.26	
			$c \equiv -1 \pmod 3$	$\mathfrak{p}$	
		≥ 1	$a \equiv 1 \pmod 3$	*Ver tabla* 4.24	
			$a \equiv -1 \pmod 3$	*Ver tabla* 4.27	
≥ 1	0	0	$c \equiv 1 \pmod 3$	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$	
			$c \equiv -1 \pmod 3$	$\mathfrak{p}$	
		≥ 1		*Ver tabla* 4.28	
	≥ 1	0	$c \equiv 1 \pmod 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$	
			$c \equiv -1 \pmod 3$	$\mathfrak{pqr}$	
		≥ 1		*Ver tabla* 4.30	

Tabla 4.24. $p = 3$; *o bien* $a \equiv c \equiv -1 \pmod 3$, $v(b) = 0$ *o bien* $a \equiv 1 \pmod 3$, $v(b), v(c) \geq 1$.

$v(\Delta)$		$3\mathcal{O}$
impar		$\mathfrak{pq}^2$
par	$\Delta_3 \equiv 1 \pmod 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
	$\Delta_3 \equiv -1 \pmod 3$	$\mathfrak{pqr}$

Tabla 4.25. $p = 3$; $a \equiv c \equiv 1 \pmod 3$, $v(b) \geq 1$.

r, s *	$v(\Delta)$			$3\mathcal{O}$
$r < s$, r *impar*				$\mathfrak{p}^2\mathfrak{q}^2$
$r < s$, r *par*				$\mathfrak{pqr}$
$r = s$ *impar*	*impar*	$d_3\Delta_3 \equiv 1 \pmod 3$		$\mathfrak{pq}^2$
		$d_3\Delta_3 \equiv -1 \pmod 3$		$\mathfrak{pqr}^2$
	par			$\mathfrak{p}^2\mathfrak{q}^2$
$r = s$ *par*	*impar*	$d_3 \equiv 1 \pmod 3$		$\mathfrak{pq}^2$
		$d_3 \equiv -1 \pmod 3$		$\mathfrak{pqr}^2$
	par	$\Delta_3 \equiv 1 \pmod 3$	$d_3 \equiv 1 \pmod 3$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
			$d_3 \equiv -1 \pmod 3$	$\mathfrak{pqs}$
		$\Delta_3 \equiv -1 \pmod 3$		$\mathfrak{pqr}$
$r > s$, s *impar*				$\mathfrak{p}^2\mathfrak{q}^2$
$r > s$, s *par*		$d_3 \equiv 1 \pmod 3$		$\mathfrak{pqs}$
		$d_3 \equiv -1 \pmod 3$		$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$

* $r := v(b)$, $s := v(d)$

Tabla 4.26. $p = 3$; $a \equiv -1 \pmod 3$, $v(b) \geq 1$, $c \equiv 1 \pmod 3$.

H *		$3\mathcal{O}$
impar		$\mathfrak{p}^2$
par	$v(b) = v(d)$	$\mathfrak{p}$
	$v(b) \neq v(d)$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$

* $H := \min\{v(b), v(d)\}$

Tabla 4.27. $p = 3$; $a \equiv -1 \pmod 3$, $v(b), v(c) \geq 1$.

$v(\Delta)$		$3\mathcal{O}$
impar		$\mathfrak{pqr}^2$
par	$\Delta_3 \equiv 1 \pmod 3$	$\mathfrak{pqs}$
	$\Delta_3 \equiv -1 \pmod 3$	$\mathfrak{pqr}$

Tabla 4.28. $p = 3$; $v(a), v(c) \geq 1$, $v(b) = 0$.

i, j *			$3\mathcal{O}$		ν
$3i < 2j$, i *impar*			$\mathfrak{pqr}^2$		
$3i < 2j$, i *par*	$U_3 \equiv 1 \pmod 3$		$\mathfrak{pqrs}$		
	$U_3 \equiv -1 \pmod 3$		$\mathfrak{pqr}$		
$3i = 2j$	$U_3 \equiv 1 \pmod 3$		$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$		
	$U_3 \equiv -1 \pmod 3$		$\mathfrak{pqr}$		
$3i > 2j$, $3 \nmid j$			$\mathfrak{pq}^3$	$3i = 2j + 1$	3
				$3i = 2j + 2$	4
				$3i > 2j + 2$	5
$3i > 2j$, $3 \mid j$ **	$A \equiv 3 \pmod 9$	$t \leq 2$	$\mathfrak{pq}^3$	$t = 1$	4
				$t = 2$	3
		$t \geq 3$	*Ver tabla* 4.29		
	$A \not\equiv 3 \pmod 9$	$t = 1$	$\mathfrak{pq}^3$		3
		$t \geq 2$	$\mathfrak{pqr}^2$		

* $i := v(U)$, $U := 3(a^2 + 12c)$, $j := v(V)$, $V := 2a^3 - 72ac + 27b^2$

** $A := U/3^{2(j/3)}$, $B := V_3$, $t := v(B^2 - A - 1)$

Tabla 4.29. $p = 3$; $v(a), v(c) \geq 1$, $v(b) = 0$,
$3i > 2j$, $3 \mid j$, $A \equiv 3 \pmod 9$, $B^2 \equiv A + 1 \pmod{27}$ *(cf. tabla* 4.28*)*.

$v(\Delta)$			$3\mathcal{O}$
impar			$\mathfrak{pqr}^2$
par	$\Delta_3 \equiv 1 \pmod 3$	$v(\Delta) = 2j$	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$
		$v(\Delta) > 2j$	$\mathfrak{pqrs}$
	$\Delta_3 \equiv -1 \pmod 3$		$\mathfrak{pqr}$

Tabla 4.30. $p = 3$; $v(a), v(b), v(c) \geq 1$.

$v(a)$	$v(b)$	$v(c)$		$3\mathcal{O}$		ν
		1		$\mathfrak{p}^4$		
	1	≥ 2		$\mathfrak{pq}^3$	$v(a) = 1$	3
					$v(a) \geq 2$, $v(c) = 2$	4
					$v(a) \geq 2$, $v(c) \geq 3$	5
1	≥ 2	2	$c_3 \equiv 1 \pmod 3$	*Ver tabla* 4.31		
			$c_3 \equiv -1 \pmod 3$	$\mathfrak{p}^2$		
1	≥ 2	≥ 3		*Ver tabla* 4.32		
≥ 2	≥ 2	2	$c_3 \equiv 1 \pmod 3$	$\mathfrak{p}^2$		
			$c_3 \equiv -1 \pmod 3$	$\mathfrak{p}^2\mathfrak{q}^2$		
≥ 2	2	≥ 3		$\mathfrak{pq}^3$	$v(c) = 3$	3
					$v(a) = 2$, $v(c) \geq 4$	4
					$v(a) \geq 3$, $v(c) \geq 4$	5
≥ 2	≥ 3	3		$\mathfrak{p}^4$		

Tabla 4.31. $p = 3$; $v(a) = 1$, $v(b) \geq 2$, $v(c) = 2$, $c_3 \equiv 1 \pmod 3$.

$v(b)$, $v(d)$		$3\mathcal{O}$
$v(b) < v(d)$		$\mathfrak{p}^4$
$v(b) \geq v(d)$	$a_3{}^{v(d)} d_3 \equiv 1 \pmod 3$	$\mathfrak{p}^2\mathfrak{q}^2$
	$a_3{}^{v(d)} d_3 \equiv -1 \pmod 3$	$\mathfrak{p}^2$

Tabla 4.32. $p = 3$; $v(a) = 1$, $v(b) \geq 2$, $v(c) \geq 3$.

$v(\Delta)$		$3\mathcal{O}$
impar	$a_3\Delta_3 \equiv 1 \pmod 3$	$\mathfrak{pq}^2$
	$a_3\Delta_3 \equiv -1 \pmod 3$	$\mathfrak{pq}^2$
par		$\mathfrak{p}^2\mathfrak{q}^2$

DEMOSTRACIÓN. Primeramente, observemos que $\Delta \equiv a^2c^2 + a^2c - ab^2 + c \pmod 3$. En función de las diferentes factorizaciones de $F(X) \pmod 3$, comenzamos distinguiendo siete casos:

I: $v(a^2c^2 + a^2c - ab^2 + c) = 0$.

II: $a \equiv c \equiv -1 \pmod 3$, $v(b) = 0$ o bien $a \equiv 1 \pmod 3$, $v(b), v(c) \geq 1$.

III: $a \equiv c \equiv 1 \pmod 3$, $v(b) \geq 1$.

IV: $a \equiv -1 \pmod 3$, $v(b) \geq 1$, $c \equiv 1 \pmod 3$.

V: $a \equiv -1 \pmod 3$, $v(b), v(c) \geq 1$.

VI: $v(a), v(c) \geq 1$, $v(b) = 0$.

VII: $v(a), v(b), v(c) \geq 1$.

Caso I: $v(a^2c^2 + a^2c - ab^2 + c) = 0$. En este caso $v(\Delta) = 0$ y, por tanto, acabamos con el lema de Kummer, teniendo en cuenta que el polinomio $F(X)$ factoriza $\pmod 3$ en la forma

$$\begin{cases} X^4 + X^2 + bX + 1 & \text{si } a \equiv c \equiv 1 \pmod 3, \\ (X+b)(X^3 - bX^2 + (a+1)X - ab) & \text{si } a \equiv -c \not\equiv 0 \pmod 3,\ v(b) = 0, \\ X(X-b)(X^2 + bX - 1) & \text{si } a \equiv 1 \pmod 3,\ v(c) \geq 1, \\ X(X^3 - X + b) & \text{si } a \equiv -1 \pmod 3,\ v(c) \geq 1, \\ X^4 + aX^2 - 1 & \text{si } v(a) = 0,\ v(b) \geq 1,\ c \equiv -1 \pmod 3, \\ (X-b)(X^3 + bX^2 + X - b) & \text{si } v(a) \geq 1,\ v(b) = 0,\ c \equiv 1 \pmod 3, \\ X^4 + bX - 1 & \text{si } v(a) \geq 1,\ v(b) = 0,\ c \equiv -1 \pmod 3, \\ (X^2 + X - 1)(X^2 - X - 1) & \text{si } v(a) \geq 1,\ v(b) \geq 1,\ c \equiv 1 \pmod 3, \\ (X-1)(X+1)(X^2+1) & \text{si } v(a) \geq 1,\ v(b) \geq 1,\ c \equiv -1 \pmod 3. \end{cases}$$

Caso II: $a \equiv c \equiv -1 \pmod 3$, $v(b) = 0$ o bien $a \equiv 1 \pmod 3$, $v(b), v(c) \geq 1$. En este caso tenemos que $F(X) \equiv (X-b)^2(X^2 - bX - 1) \pmod 3$ o bien que $F(X) \equiv X^2(X^2+1) \pmod 3$, respectivamente; por tanto, $3\mathcal{O} = \mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$, $\mathfrak{pq}^2$ o $\mathfrak{pqr}$ y terminamos con los lemas de 2.1 y 2.2.

Caso III: $a \equiv c \equiv 1 \pmod 3$, $v(b) \geq 1$. Aquí tenemos que $F(X) \equiv (X-1)^2(X+1)^2 \pmod 3$; luego, $F(X) = G(X)H(X)$ con $G(X), H(X) \in \mathbb{Q}_3[X]$ de grado 2 tales que $\overline{G}(X) = (X - \overline{1})^2$ y $\overline{H}(X) = (X + \overline{1})^2$. Además, no sólo el valor $v(\Delta) = v(\Delta(G)) + v(\Delta(H))$ puede ser arbitrariamente grande, sino que también los valores $v(\Delta(G))$ y $v(\Delta(H))$ pueden ser arbitrariamente grandes a la vez.

Para resolver este caso ponemos $r := v(b)$, $s := v(d)$, y distinguimos dos subcasos:

$$\text{III.1: } r = s.$$
$$\text{III.2: } r \neq s.$$

Subcaso III.1: $r = s$. En este primer subcaso elegimos (siempre lo podemos hacer) un entero M tal que $v(M^2 + a/2) > r/2$ y $M \not\equiv d_3/(4b_3) \pmod 3$; así,

$$v(F(M)) = v((M^2 + a/2)^2 + bM - d/4) = r,$$
$$F(M)_3 \equiv b_3 M - d_3/4 \equiv d_3 \pmod 3.$$

Entonces es fácil comprobar que con el análisis del polígono $\mathbf{N}_{(v,X-M)}(F)$, y el cálculo de los datos del correspondiente factor local (cuando r es impar) o los lemas de 2.1 y 2.2 (cuando r es par) acabamos en este subcaso.

Subcaso III.2: $r \neq s$. En este segundo subcaso elegimos un entero M tal que $v(M^2 + a/2) > \min\{r, s\}/2$. Entonces también es fácil comprobar que el análisis simultaneo de los polígonos $\mathbf{N}_{(v,X-M)}(F)$ y $\mathbf{N}_{(v,X+M)}(F)$ nos permite de nuevo terminar.

Caso IV: $a \equiv -1 \pmod 3$, $v(b) \geq 1$, $c \equiv 1 \pmod 3$. En este caso tenemos que $F(X) \equiv \phi(X)^2 \pmod 3$, donde $\phi(X) := X^2 + a/2 \in \mathbb{Z}_3[X]$, y que $v(\Delta)$ puede ser arbitrariamente grande.

Con el análisis del polígono $\mathbf{N}_{(v,\phi)}(F)$ acabamos este caso. En efecto, como

$$F(X) = \phi(X)^2 + bX - d/4$$

y $v(bX - d/4) = \min\{v(b), v(d)\} =: H$, entonces el polígono consta de un solo lado, de origen el punto $(0, H)$ y de final el punto $(2, 0)$. Si H es impar, $3\mathcal{O} = \mathfrak{p}^2$. Supongamos por tanto que H es par, y sea $\zeta \in \mathbb{F}_3^{nr}$ una raíz de $\overline{\phi}(X)$. Entonces el polinomio asociado a este lado es

$$Y^2 + \overline{b/3^H}\,\zeta - \overline{d/3^H} \in \mathbb{F}_9[Y],$$

el cual no tiene raíces múltiples. Además, este polinomio es irreducible en $\mathbb{F}_9[Y]$ si y sólo si $v(b) = v(d)$; por consiguiente, $3\mathcal{O} = \mathfrak{p}$ o $\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$ según que $v(b) = v(d)$ o $v(b) \neq v(d)$, respectivamente.

Caso V: $a \equiv -1 \pmod 3$, $v(b), v(c) \geq 1$. Aquí tenemos que $F(X) \equiv X^2(X-1)(X+1) \pmod 3$; luego, $3\mathcal{O} = \mathfrak{pqr}$, $\mathfrak{pqr}^2$ o $\mathfrak{pqrs}$ y terminamos de nuevo con los lemas de 2.1 y 2.2.

Caso VI: $v(a), v(c) \geq 1$, $v(b) = 0$. En este caso tenemos que $F(X) \equiv (X+b)^3 X \pmod 3$ y que el valor $v(\Delta)$ puede ser arbitrariamente grande. Por tanto, $F(X) = (X-\theta)H(X)$ con $\theta \in \mathbb{Q}_3$ y $H(X) \in \mathbb{Q}_3[X]$ tales que $v(\theta) > 0$ y $H(X) \equiv (X+b)^3 \pmod 3$.

Para el estudio del factor $H(X)$ procedemos como en el caso II de la demostración del teorema de 4.5. Consideramos la resolvente cúbica del polinomio $F(X)$

$$G(X) := X^3 - 2aX^2 + (a^2 - 4c)X + b^2$$

y el polinomio

$$G_0(X) := 27G((X+2a)/3) = X^3 - UX + V,$$

donde $U := 3(a^2+12c)$, $V := 2a^3 - 72ac + 27b^2$ son ambos enteros divisibles por tres. Ponemos $i := v(U)$ y $j := v(V)$.

El análisis del polígono $\mathrm{N}_{(v,X)}(G_0)$ junto con la aplicación del lema de 2.4 (al cuerpo $L = \mathbb{Q}_3$) nos permiten terminar si $3i \leq 2j$.

Supongamos que $3i > 2j$ y $3 \nmid j$. Entonces el polígono $\mathrm{N}_{(v,X)}(G_0)$ consta de un solo lado, cuya pendiente es no entera; por tanto, la extensión $\mathbb{Q}_3(\eta_0)/\mathbb{Q}_3$, donde η_0 es una raíz de $G_0(X)$, es cúbica y totalmente ramificada. Además, si denotamos por δ al discriminante de esta extensión, entonces, como $v(\mathrm{ind}(G_0)) = j-1$, tenemos que

$$v(\delta) = v(\Delta(G_0)) - 2v(\mathrm{ind}(G_0)) = \begin{cases} 3 & \text{si } 3i = 2j+1, \\ 4 & \text{si } 3i = 2j+2, \\ 5 & \text{si } 3i > 2j+2. \end{cases}$$

Entonces, por la parte (b) del lema de 2.4, la extensión $\mathbb{Q}_3(\theta')/\mathbb{Q}_3$, donde θ' es una raíz de $H(X)$, es cúbica y totalmente ramificada; luego, $3\mathcal{O} = \mathfrak{pq}^3$. Además, el valor de $\nu = v(\delta)$ ya lo tenemos calculado.

Por último, supongamos que $3i > 2j$ y $3 \mid j$. Entonces el polígono $\mathrm{N}_{(v,X)}(G_0)$ consta de un solo lado, cuya pendiente es entera, y su polinomio

asociado es $(Y+\overline{V_3})^3$ en $\mathbb{F}_3[Y]$. Esta información nos lleva a considerar el polinomio

$$G_1(X) := 3^{-j}\,G_0(3^{j/3}X) = X^3 - AX + B,$$

donde $A := U/3^{2(j/3)}$ es un entero múltiplo de 3 y $B := V_3$ es un entero no divisible por 3, y a proceder como en el caso III de la demostración del teorema 1 de [**LL-Na 83**]. El análisis del polígono $\mathbf{N}_{(v,X+B)}(G_1)$ junto con la aplicación del lema de 2.4 nos permiten acabar si $A \not\equiv 3 \pmod 9$ o si $B^2 \not\equiv A+1 \pmod{27}$. Por tanto, supongamos además que $A \equiv 3 \pmod 9$ y $B^2 \equiv A+1 \pmod{27}$, y consideremos el polinomio

$$G_2(X) := 3^{-3}\,G_1(3X-B) = X^3 - BX^2 + A'X - B',$$

donde $A' := (3B^2-A)/9 \in \mathbb{Z}, B' := B(B^2-A-1)/27 \in \mathbb{Z}$. Observemos que $\Delta = \Delta(G) = 3^{-6}\Delta(G_0) = 3^{2(j-3)}\Delta(G_1) = 3^{2j}\Delta(G_2)$, y que el polinomio $\overline{G_2}(X)$ no puede tener una raíz triple ni tres raíces simples en $\mathbb{F}_3$. Ahora, la aplicación del lema de 2.4 y de los lemas de 2.1 y 2.2 nos permite también acabar.

Caso VII: $v(a), v(b), v(c) \geq 1$. Aquí es $F(X) \equiv X^4 \pmod 3$. El análisis del polígono $\mathbf{N}_{(v,X)}(F)$ y, cuando $3\mathcal{O} = \mathfrak{p}\mathfrak{q}^3$, el cálculo explícito del valor $v(\Delta)$ nos permiten acabar excepto en dos nuevos casos:

VII.1: $v(a) = 1,\ v(b) \geq 2,\ v(c) = 2,\ c_3 \equiv 1 \pmod 3$.

VII.2: $v(a) = 1,\ v(b) \geq 2,\ v(c) \geq 3$.

En ambos casos el valor $v(\Delta)$ puede ser arbitrariamente grande.

Subcaso VII.1: $v(a) = 1,\ v(b) \geq 2,\ v(c) = 2,\ c_3 \equiv 1 \pmod 3$. En este subcaso el polígono $\mathbf{N}_{(v,X)}(F)$ consta de un solo lado, cuya pendiente es $-1/2$, y su polinomio asociado es $(Y-\overline{a_3})^2$ en $\mathbb{F}_3[Y]$; por tanto, hemos de seguir con el polígono en segundo orden.

Consideramos la valoración v_2 asociada a la terna $(v, X, 1/2)$ y el polinomio $\phi_2(X) := X^2 + a/2 \in \mathbb{Z}_3[X]$. Entonces el análisis del polígono (de segundo orden) $\mathbf{N}_{(v_2,\phi_2)}(F)$ nos permite terminar este subcaso.

Subcaso VII.2: $v(a) = 1,\ v(b) \geq 2,\ v(c) \geq 3$. En este subcaso el polígono $\mathbf{N}_{(v,X)}(F)$ consta de al menos dos lados, y uno de ellos tiene pendiente $-1/2$. Por consiguiente, $F(X) = G(X)H(X)$ donde $G(X), H(X) \in \mathbb{Q}_3[X]$

de grado 2, y el polígono $\mathrm{N}_{(v,X)}(G)$ consta de un sólo lado, cuya pendiente es $-1/2$. Entonces obtenemos que

$$v(\Delta(G)) = 1, \quad \Delta(G)_3 \equiv -a_3 \pmod 3$$

y, por tanto,

$$v(\Delta(H)) \not\equiv v(\Delta) \pmod 2, \quad \Delta(H)_3 \equiv -a_3\Delta_3 \pmod 3,$$

lo que nos permite acabar.

Queda por tanto probado el teorema. □

§6. Ramificación de los primos mayores que tres

Esta última sección está dedicada al estudio del resto de la ramificación p-ádica en el cuerpo cuártico K; por tanto, suponemos que tenemos dado un primo $p \geq 5$. Entonces p es moderadamente ramificado en K y, por tanto, nuestro interés se centra en obtener el tipo de descomposición de p en $\mathcal{O}$.

En esta sección denotamos por v a la valoración p-ádica extendida a $\mathbb{Q}_p(X)$ de forma que $v(X) = 0$. Recordemos que dado un entero p-ádico $u \neq 0$ denotamos por u_p a la unidad p-ádica $u/p^{v(u)}$ y por $\overline{u}$ a la clase de u (mod p).

Si $p \equiv 1 \pmod m$ para algún entero $m \geq 2$, entonces para un entero α no divisible por p definimos el símbolo $(\alpha/p)_m$ como

$$(\alpha/p)_m := \overline{\alpha}^{(p-1)/m} \in \mu_m\,,$$

donde $\mu_m \subseteq \mathbb{F}_p^*$ denota el grupo de las raíces m-ésimas de la unidad. Notemos que $(\alpha/p)_m = 1$ si y sólo si $\overline{\alpha} \in \left(\mathbb{F}_p^*\right)^m$. Utilizaremos este símbolo sólo para $m = 2$, en cuyo caso coincide con el símbolo de Legendre (α/p), para $m = 3$, y para $m = 4$ y $(\alpha/p) = 1$, en cuyo caso $(\alpha/p)_4 = 1$ ó -1.

Suponemos que el polinomio $F(X)$ es de la forma

$$F(X) = X^4 + aX^2 + bX + c,$$

con $a, b, c \in \mathbb{Z}$ tales que las condiciones

$$v(a) \geq 2,\ v(b) \geq 3,\ v(c) \geq 4,$$

no se dan simultaneamente. Además, definimos los enteros

$$d := a^2 - 4c,\ u := 2ad + 9b^2,\ \delta := -2b^2(a^2 + 12c)^2 - au^2.$$

6.1. Teorema. *Con las hipótesis y notaciones anteriores, el tipo de descomposición del primo p en $\mathcal{O}$ viene dado en las siguientes tablas:*

Tabla 4.33. $p \geq 5$.

$v(a)$	$v(b)$	$v(c)$	$v(\Delta)$			$p\mathcal{O}$
0	0	0	0			*Ver tablas* 4.34
			≥ 1	$v(u) = 0$	$(\delta/p) = 1$	*Ver tabla* 4.35
					$(\delta/p) = -1$	*Ver tabla* 4.36
				$v(u) \geq 1$		*Ver tabla* 4.37
		≥ 1	0			*Ver tablas* 4.34
			≥ 1			*Ver tabla* 4.35
	≥ 1	0	0			*Ver tablas* 4.34
			≥ 1	$(-2a/p) = 1$		*Ver tabla* 4.38
				$(-2a/p) = -1$		*Ver tabla* 4.39
		≥ 1		$(-a/p) = 1$		*Ver tabla* 4.35
				$(-a/p) = -1$		*Ver tabla* 4.36
≥ 1	0	0	0			*Ver tablas* 4.34
			≥ 1	$p \equiv 1$ ó $3 \pmod 8$		*Ver tabla* 4.35
				$p \equiv -1$ ó $-3 \pmod 8$		*Ver tabla* 4.36
		≥ 1				*Ver tablas* 4.34
	≥ 1	0				*Ver tablas* 4.34
		≥ 1				*Ver tabla* 4.40

Tablas 4.34. $p \geq 5$; $v(\Delta) = 0$.

$v(b) = v(c) = 0$; $v(\Delta) = 0$		$p\mathcal{O}$
$(\Delta/p) = 1$	$F(X)$ *no tiene raíces* (mod p)	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
	$F(X)$ *tiene una única raíz* (mod p)	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$
	$F(X)$ *tiene más de una raíz* (mod p)	$\mathfrak{pqrs}$
$(\Delta/p) = -1$	$F(X)$ *no tiene raíces* (mod p)	$\mathfrak{p}$
	$F(X)$ *tiene alguna raíz* (mod p)	$\mathfrak{pqr}$

$v(a) = v(b) = 0$, $v(c) \geq 1$; $v(\Delta) = 0$		$p\mathcal{O}$
$(\Delta/p) = 1$	$X^3 + aX + b$ *no tiene raíces* (mod p)	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$
	$X^3 + aX + b$ *tiene alguna raíz* (mod p)	$\mathfrak{pqrs}$
$(\Delta/p) = -1$		$\mathfrak{pqr}$

$v(a) = v(c) = 0$, $v(b) \geq 1$; $v(\Delta) = 0$			$p\mathcal{O}$
$(c/p) = 1$	$(d/p) = 1$	$F(X)$ *no tiene raíces* (mod p)	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
		$F(X)$ *tiene alguna raíz* (mod p)	$\mathfrak{pqrs}$
	$(d/p) = -1$		$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
$(c/p) = -1$	$(d/p) = 1$		$\mathfrak{pqr}$
	$(d/p) = -1$		$\mathfrak{p}$

$v(a), v(c) \geq 1$, $v(b) = 0$		$p\mathcal{O}$
$p \equiv 1 \pmod 3$	$(b/p)_3 = 1$	$\mathfrak{pqrs}$
	$(b/p)_3 \neq 1$	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$
$p \equiv -1 \pmod 3$		$\mathfrak{pqr}$

$v(a), v(b) \geq 1$, $v(c) = 0$			$p\mathcal{O}$
$p \equiv 1 \pmod 4$	$(c/p) = 1$	$(-c/p)_4 = 1$	$\mathfrak{pqrs}$
		$(-c/p)_4 \neq 1$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
	$(c/p) = -1$		$\mathfrak{p}$
$p \equiv -1 \pmod 4$	$(c/p) = 1$		$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
	$(c/p) = -1$		$\mathfrak{pqr}$

Tabla 4.35. $p \geq 5$; $v(\Delta) \geq 1$, $v(u) = 0$, $(\delta/p) = 1$.

$v(\Delta)$		$p\mathcal{O}$
impar		$\mathfrak{pq}^2$
par	$(\Delta_p/p) = 1$	$\mathfrak{pqrs}$
	$(\Delta_p/p) = -1$	$\mathfrak{pqr}$

Tabla 4.36. $p \geq 5$; $v(\Delta) \geq 1$, $v(u) = 0$, $(\delta/p) = -1$.

$v(\Delta)$		$p\mathcal{O}$
impar		$\mathfrak{pq}^2$
par	$(\Delta_p/p) = 1$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
	$(\Delta_p/p) = -1$	$\mathfrak{pqr}$

Tabla 4.37. $p \geq 5$; $v(a) = v(b) = v(c) = 0$, $v(\Delta), v(u) \geq 1$.

$v(U)$, $v(V)$, $v(\Delta)$ *			$p\mathcal{O}$
$3v(U) < 2v(V)$, $v(U)$ *impar*			$\mathfrak{pqr}^2$
$3v(U) < 2v(V)$, $v(U)$ *par*	$(U_p/p) = 1$		$\mathfrak{pqrs}$
	$(U_p/p) = -1$		$\mathfrak{pqr}$
$3v(U) = 2v(V)$, $v(\Delta)$ *impar*			$\mathfrak{pqr}^2$
$3v(U) = 2v(V)$, $v(\Delta)$ *par*	$(\Delta_p/p) = 1$ **	$n = 0$	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$
		$n \geq 1$	$\mathfrak{pqrs}$
	$(\Delta_p/p) = -1$		$\mathfrak{pqr}$
$3v(U) > 2v(V)$, $3 \nmid v(V)$			$\mathfrak{pq}^3$
$3v(U) > 2v(V)$, $3 \mid v(V)$	$p \equiv 1 \pmod 3$	$(V_p/p)_3 = 1$	$\mathfrak{pqrs}$
		$(V_p/p)_3 \neq 1$	$\mathfrak{p}_{(1)}\mathfrak{q}_{(3)}$
	$p \equiv -1 \pmod 3$		$\mathfrak{pqr}$

* $U := 3(a^2 + 12c), V := 2a^3 - 72ac + 27b^2$

** $n :=$ *número de raíces de* $X^3 - U_pX + V_p \pmod p$

Tabla 4.38. $p \geq 5$; $v(a) = v(c) = 0$, $v(b), v(\Delta) \geq 1$, $(-2a/p) = 1$.

r, s *	$v(\Delta)$			$p\mathcal{O}$
$r < s$, r *impar*				$\mathfrak{p}^2\mathfrak{q}^2$
$r < s$, r *par*		$p \equiv 1 \pmod 4$	$(-8a/p)_4 = (b_p/p)$	$\mathfrak{pqrs}$
			$(-8a/p)_4 \neq (b_p/p)$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
		$p \equiv -1 \pmod 4$		$\mathfrak{pqr}$
$r = s$ *impar*	*impar*	$(2d_p\Delta_p/p) = 1$		$\mathfrak{pqr}^2$
		$(2d_p\Delta_p/p) = -1$		$\mathfrak{pq}^2$
	par			$\mathfrak{p}^2\mathfrak{q}^2$
$r = s$ *par*	*impar*	$(2d_p/p) = 1$		$\mathfrak{pqr}^2$
		$(2d_p/p) = -1$		$\mathfrak{pq}^2$
	par	$(\Delta_p/p) = 1$ **	$(\delta'/p) = 1$	$\mathfrak{pqrs}$
			$(\delta'/p) = -1$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
		$(\Delta_p/p) = -1$		$\mathfrak{pqr}$
$r > s$, s *impar*				$\mathfrak{p}^2\mathfrak{q}^2$
$r > s$, s *par*		$(d_p/p) = 1$		$\mathfrak{pqrs}$
		$(d_p/p) = -1$		$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$

* $r := v(b)$, $s := v(d)$

** $\delta' :\equiv d_p - 2b_p\sqrt{-2a} \not\equiv 0 \pmod p$

Tabla 4.39. $p \geq 5$; $v(a) = v(c) = 0$, $v(b), v(\Delta) \geq 1$, $(-2a/p) = -1$.

H *		$p\mathcal{O}$
impar		$\mathfrak{p}^2$
par	$(\Delta_p/p) = 1$	$\mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$
	$(\Delta_p/p) = -1$	$\mathfrak{p}$

* $H := \min\{v(b), v(d)\}$

Tabla 4.40. $p \geq 5$; $v(a), v(b), v(c) \geq 1$.

$v(a)$	$v(b)$	$v(c)$			$p\mathcal{O}$
		1			$\mathfrak{p}^4$
	1	≥ 2			$\mathfrak{pq}^3$
1	≥ 2	2	$v(d) = 2$	$(d_p/p) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$
				$(d_p/p) = -1$	$\mathfrak{p}^2$
			$v(d) \geq 3$		*Ver tabla* 4.41
1	≥ 2	≥ 3			*Ver tabla* 4.42
≥ 2	≥ 2	2	$(-c_p/p) = 1$		$\mathfrak{p}^2\mathfrak{q}^2$
			$(-c_p/p) = -1$		$\mathfrak{p}^2$
≥ 2	2	≥ 3			$\mathfrak{pq}^3$
≥ 2	≥ 3	3			$\mathfrak{p}^4$

Tabla 4.41. $p \geq 5$; $v(b) \geq 2$, $v(c) = 2$, $v(d) \geq 3$.

$v(b)$, $v(d)$		$p\mathcal{O}$
$v(b) < v(d)$		$\mathfrak{p}^4$
$v(b) \geq v(d)$ *	$(\zeta_1^{v(d)} d_p/p) = 1$	$\mathfrak{p}^2\mathfrak{q}^2$
	$(\zeta_1^{v(d)} d_p/p) = -1$	$\mathfrak{p}^2$

* $\zeta_1 :\equiv -a_p/2 \pmod{p}$

Tabla 4.42. $p \geq 5$; $v(a) = 1$, $v(b) \geq 2$, $v(c) \geq 3$.

$v(\Delta)$		$p\mathcal{O}$
impar	$(-a_p\Delta_p/p) = 1$	$\mathfrak{pqr}^2$
	$(-a_p\Delta_p/p) = -1$	$\mathfrak{pq}^2$
par		$\mathfrak{p}^2\mathfrak{q}^2$

DEMOSTRACIÓN (del teorema de 4.1). En función de los diferentes tipos de factorización de $F(X) \pmod p$ distinguimos siete casos:

$$\begin{aligned}
&\text{I: } v(\Delta) = 0.\\
&\text{II: } v(\Delta) \geq 1,\ v(u) = 0,\ (\delta/p) = 1.\\
&\text{III: } v(\Delta) \geq 1,\ v(u) = 0,\ (\delta/p) = -1.\\
&\text{IV: } v(a) = v(b) = v(c) = 0,\ v(\Delta), v(u) \geq 1.\\
&\text{V: } v(a) = v(c) = 0,\ v(b), v(\Delta) \geq 1,\ (-2a/p) = 1.\\
&\text{VI: } v(a) = v(c) = 0,\ v(b), v(\Delta) \geq 1,\ (-2a/p) = -1.\\
&\text{VII: } v(a), v(b), v(c) \geq 1.
\end{aligned}$$

Más adelante veremos que cuando $v(\Delta) \geq 1$ y $v(u) = 0$, es $v(\delta) = 0$ (cf. *Casos* II y III). Entonces, con la ayuda de la tabla 4.33, vemos que la distinción anterior cubre todos los casos, una vez hemos comprobado los "seguimientos" que indica esta tabla. La comprobación de estos seguimientos no ofrece dificultad.

Caso I: $v(\Delta) = 0$. En este caso acabamos con el lema de Kummer. Notemos que el lema de 2.2 nos permite reducir el estudio de la factorización de $F(X) \pmod p$, y que en algunos casos particulares podemos incluso determinarla (cf. tablas 4.34).

Casos II y III: $v(\Delta) \geq 1$, $v(u) = 0$. En los dos casos tenemos que

$$F(X) \equiv (X - \zeta)^2 (X^2 + 2\zeta X + 3\zeta^2 + a) \pmod p,$$

donde $\zeta :\equiv -b(a^2 + 12c)u^{-1} \pmod p$. Además, tenemos también que el factor $X^2 + 2\zeta X + 3\zeta^2 + a \pmod p$ no tiene raíces múltiples. En efecto, en caso contrario se tendría que

$$F(X) \equiv (X - \zeta)^2 (X + \zeta)^2 \equiv X^4 - 2\zeta^2 X^2 + \zeta^4 \pmod p,$$

lo cual nos diría que

$$a \equiv -2\zeta^2 \pmod p, \quad b \equiv 0 \pmod p, \quad c \equiv \zeta^4 \pmod p;$$

luego, tendríamos $d = a^2 - 4c \equiv 0 \pmod p$ y $u = 2ad + 9b^2 \equiv 0 \pmod p$, lo cual contradiría la hipótesis $v(u) = 0$.

Como el discriminante de este factor es $-4(2\zeta^2+a) \equiv 4\delta u^{-2} \pmod{p}$, ha de ser $v(\delta) = 0$; además, si $(\delta/p) = 1$ (resp. $(\delta/p) = -1$), entonces $p\mathcal{O} = \mathfrak{pqr}$, $\mathfrak{pqr}^2$ o $\mathfrak{pqrs}$ (resp. $p\mathcal{O} = \mathfrak{p}_{(2)}\mathfrak{q}_{(2)}$, $\mathfrak{pq}^2$ o $\mathfrak{pqr}$) y terminamos con los lemas de 2.1 y 2.2.

Caso IV: $v(a) = v(b) = v(c) = 0$, $v(\Delta), v(u) \geq 1$. Observemos primero que tenemos que $v(a^2 + 12c), v(8a^3 + 27b^2) \geq 1$. En efecto, de la condición $v(u) \geq 1$ se sigue que

$$9\Delta \equiv -4d(a^2 + 12c)^2 \pmod{p};$$

luego, como $v(\Delta) \geq 1$, es $v(d) \geq 1$ o $v(a^2 + 12c) \geq 1$. Si fuera $v(d) \geq 1$, entonces tendríamos que $v(b) \geq 1$, en contradicción con una de nuestras hipótesis. Por consiguiente, ha de ser $v(a^2 + 12c) \geq 1$ y, por tanto, también $v(8a^3 + 27b^2) \geq 1$.

Ahora, es fácil ver que $F(X) \equiv (X - \zeta)^3(X + 3\zeta) \pmod{p}$, donde $\zeta :\equiv -3b(4a)^{-1} \pmod{p}$. Entonces este caso se termina procediendo de la misma manera que en el caso II de la demostración del teorema de 4.5.

Casos V y VI: $v(a) = v(c) = 0$, $v(b), v(\Delta) \geq 1$. En ambos casos tenemos que $v(d) \geq 1$ y, por tanto, $F(X) \equiv (X^2 + a/2)^2 \pmod{p}$. Ahora concluimos procediendo de la misma forma que en los casos III y IV, respectivamente, de la demostración del teorema de 5.1.

Caso VII: $v(a), v(b), v(c) \geq 1$. Aquí $F(X) \equiv X^4 \pmod{p}$ y terminamos de la misma manera que en el caso VII de la demostración del teorema de 5.1. □

Bibliografía

[Ba 07] Bauer, M.: Zur allgemeinen Theorie der algebraischen Größen, *J. Reine Angew. Math.* **132** (1907), 21–32.

[Ber 70] Berlekamp, M.: Factoring polynomials over large finite fields, *Math. Comp.* **24**, n. 111 (1970), 713–715.

[Be 27] Berwick, W. E. H.: *Integral Bases*, Cambridge Tracts in Mathematics and Mathematical Physics, n. 22, Cambridge Univ. Press, 1927. Repr. Stechert-Hafner, 1964.

[Bö-Re 87] Böffgen, R.; Reichert, M. A.: Computing the decomposition of primes p and p-adic absolute values in semi-simple algebras over $\mathbb{Q}$, *J. Symbolic Computation* **4** (1987), 3–10.

[Bu-Le] Buchmann, J.; Lenstra, H.W.: Computing maximal orders and factoring over $\mathbb{Z}_p$, preprint.

[Ca-Za 81] Cantor, D.; Zassenhauss, H.: A new algorithm for factoring polynomials over finite fields, *Math. Comp.* **36** (1981), 587–592.

[Co 95] Cohen, H.: *A Course in Computacional Algebraic Number Theory*, GTM, n. 138, Springer, 1995.

[De 78] Dedekind, R.: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, *Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen* **23** (1878), 1–23.

[Gu 98] Guàrdia, J.: *Geometria Aritmètica en una família de corbes de gènere tres*, Barcelona, 1998. Tesi Doctoral.

[Ll-Na 83] Llorente, P.; Nart, E.: Effective determination of the decomposition of the rational primes in a cubic field, *Proc. A.M.S.* **87**, n. 4 (1983).

[Ll-Na-Vi 84] Llorente, P.; Nart, E.; Vila, N.: Discriminants of number fields defined by trinomials, *Acta Arithmetica* **43** (1984), 367–373.

[Ll-Na-Vi 91] Llorente, P.; Nart, E.; Vila, N.: Decomposition of primes in number fields defined by trinomials, *Séminaire de Théorie des Nombres de Bordeaux* **3**, n. 1 (1991), 27–41.

[Ma 36a] MacLane, S.: A construction for absolute values in polynomial rings, *Trans. Amer. Math. Soc.* **40** (1936), 363–395.

[Ma 36b] MacLane, S.: A construction for prime ideals as absolute values of an algebraic field, *Duke Math. Journal* **2** (1936), 492–510.

[Mo-Na 92] Montes, J.; Nart, E.: On a theorem of Ore, *Journal of Algebra* **146** (1992), 318–334.

[Nar 90] Narkiewicz, W.: *Elementary and Analytic Theory of Algebraic Numbers*, Springer, PWN-Polish Scientific Publishers, 1990. 2nd edition.

[Na 83] Nart, E.: Sobre l'índex d'un cos de nombres, *Pub. Mat. UAB* **27**, n. 1 (1983).

[Ok 82] Okutsu, K.: Construction of integral basis I-IV, *Proc. Japan Acad.* **58** (1982), 47–49, 87-89, 117-119, 167-169.

[Or 23] Ore, Ö.: Zur Theorie der algebraischen Körper, *Acta Math.* **44** (1923), 219–314.

[Or 24] Ore, Ö.: Weitere untersuchungen zur Theorie der algebraischen Körper, *Acta Math.* **45** (1924-25), 145–160.

[Or 26] Ore, Ö.: Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern, *Math. Ann.* **96** (1926), 313–352.

[Or 28] Ore, Ö.: Newtonsche Polygone in der Theorie der algebraischen Körper, *Math. Ann.* **99** (1928), 84–117.

[Po-Za 89] Pohst, M.; Zassenhaus, H.: *Algorithmic Algebraic Number Theory*, Cambridge Univ. Press, 1989.

[Po 93] Pohst, M.: *Computacional Algebraic Number Theory*, Birkhäuser, 1993.

[Ro 93] Roberson, S.: Dyadic ramification and quartic number fields, *J. Number Theory* **45** (1993), 68–91.

[Sw 62] Swan, R.: Factorization of polynomials over finite fields, *Pacific Journal of Mathematics* **12** (1962), 1099–1106.

[Se 79] Serre, J.-P.: *Local Fields*, GTM, n. 67, Springer, 1979.

[Tr 85] Travesa, A.: Sobre el número de extensiones de grado dado de un cuerpo local, *Actas de las X Jornadas Hispano-Lusas de Matemáticas* (1986), 235–247.

[Wa 22] Wahlin, G. E.: The factorization of the rational primes in a cubic domain, *Amer. Journal of Math.* **44** (1922), 191–203.