USC
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

ESCUELA DE DOCTORADO
INTERNACIONAL EN CIENCIAS
Y TECNOLOGÍAS DE LA USC

Ana
Mascato García

Tesis doctoral

Sobre leyes de reciprocidad clásicas, períodos π-ádicos y reciprocidades sobre módulos formales p-divisibles

Santiago de Compostela, 2018

CENTRO INTERNACIONAL DE ESTUDOS
DE DOUTORAMENTO E AVANZADOS
DA USC (CIEDUS)

TESE DE DOUTORAMENTO

Sobre leyes de reciprocidad clásicas, períodos π-ádicos y reciprocidades sobre módulos formales p-divisibles

ANA MASCATO GARCÍA

ESCOLA DE DOUTORAMENTO INTERNACIONAL

PROGRAMA DE DOUTORAMENTO EN MATEMÁTICAS

SANTIAGO DE COMPOSTELA

ANO 2018

DECLARACIÓN DO AUTOR DA TESE

[Sobre leyes de reciprocidad clásicas, períodos π-ádicos y reciprocidades sobre módulos formales p-divisibles]

D./Dna. .Ana Mascato García

Presento miña tese, seguindo o procedemento adecuado ao Regulamento, e declaro que:

1) A tese abarca os resultados da elaboración do meu traballo.
2) No seu caso, na tese se fai referencia as colaboracións que tivo este traballo.
3) A tese é a versión definitiva presentada para a súa defensa e coincide ca versión enviada en formato electrónico.
4) Confirmo que a tese non incorre en ningún tipo de plaxio de outros autores nin de traballos presentados por min para a obtención de outros títulos.

En Santiago de Compostela, 8 de xaneiro de 2018

Asdo: Ana Mascato García

AUTORIZACIÓN DO DIRECTOR / TITOR DA TESE

[Sobre leyes de reciprocidad clásicas, períodos π-ádicos y reciprocidades sobre módulos formales p-divisibles]

D. José Manuel Fernández Vilaboa e
D. Leoncio Franco Fernández

INFORMA/N:

Que a presente tese, correspóndese co traballo realizado por D/Dna. ***Ana Mascato García****, baixo a miña dirección, e autorizo a súa presentación, considerando que reúne os requisitos esixidos no Regulamento de Estudos de Doutoramento da USC, e que como director desta non incorre nas causas de abstención establecidas na Lei 40/2015.*

En Santiago de Compostela, 8 de xaneiro de 2018

Asdo. José Manuel Fernández Vilaboa

Asdo. Leoncio Franco Fernández

Prefacio

Esta tesis consta de dos partes bien diferenciadas e independientes, pero dentro de un campo común, el de las leyes de reciprocidad de la Teoría de Números. La primera versa sobre leyes de reciprocidad particulares, con fórmulas en términos de coordenadas/parámetros de los argumentos, mientras que la segunda lo hace sobre leyes de reciprocidad explícitas con fórmulas analíticas, sobre grupos formales p-divisibles y con el método de períodos p-ádicos, en el marco del 9º Problema de Hilbert. Se tratan así dos facetas diferentes de las varias que tiene el campo de las leyes de reciprocidad. Los métodos en cada una de ellas son pues muy diferentes.

Cada una de las partes tiene sus propios índice, introducción, lista de símbolos y bibliografía. Comparten, no obstante, el paginado y el índice alfabético.

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Parte I: Una demostración local de las leyes de reciprocidad óctica y bióctica

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Introducción

Sobre la historia de las leyes de reciprocidad, dentro de la Teoría de Números, podría decirse que aquélla comenzó con un teorema de Fermat sobre el conductor de la representación de números primos como suma de dos cuadrados. Legendre planteó la existencia de un conductor para el símbolo que lleva su nombre, lo que culminó con las seis demostraciones de Gauss de la ley de reciprocidad cuadrática.

Empezó así, a comienzos del s. XIX, una carrera hacia generalizaciones de la ley de reciprocidad cuadrática a reciprocidades de orden superior, motivadas por las potenciales aplicaciones diofánticas, y con el empleo de nuevos métodos más sofisticados (ciclotomía, sumas de Gauss y Jacobi, y funciones elípticas), pasando a ser el de las leyes de reciprocidad un tema central en la Teoría de Números, por sus aplicaciones, pero también en sí mismo, al ser aquéllas resultados finales. Así (a diferencia de otros teoremas) dar demostraciones nuevas de las leyes de reciprocidad pasó a ser también un objetivo primordial, muestra de que éstas son resultados profundos.

Todo esto culminó en 1900 con la reformulación por Hilbert de la clásica ley de reciprocidad cuadrática como fórmula producto para su símbolo de residuo nórmico, y sobre todo el llamado 9º *Problema de Hilbert* sobre "la demostración de la ley de reciprocidad más general". Un punto culminante fue la ley de reciprocidad de Artin (1927) de la teoría de cuerpos de clases. Esta teoría unifica todas las leyes de reciprocidad, reduciéndolas a un problema puramente local: el del cálculo explícito de los símbolos de Hilbert no moderados[1].

A lo largo del s. XX las leyes de reciprocidad continuaron siendo un problema central, tanto la obtención de *leyes de reciprocidad explícitas* cada vez más *generales*, basadas en la mencionada reducción dada por la teoría de cuerpos de clases, en orden a cerrar el 9º Problema (ie, a expresar el símbolo de Hilbert mediante fórmulas analíticas, para hacer aquella teoría completamente explícita), como la incorporación de nuevas demostraciones de las *leyes de reciprocidad particulares*. De las primeras, y por aproximación de sus fórmulas analíticas, se derivarían algunas de las segundas, en términos clásicos, más explícitos y próximos a las aplicaciones diofánticas.

[1] Apuntemos un hecho significativo a este respecto. Las demostraciones clásicas de la ley de reciprocidad de Kummer p-potencial tenían especial dificultad con los primos irregulares. Con el poder de la teoría de cuerpos de clases emergente "esas irregularidades de los primos pasaron a ser irrelevantes".

El interés por las leyes de reciprocidad explícitas más generales cobró un nuevo impulso con la conjetura de Birch y Swinerton-Dyer. Iwasawa en [26] formuló su ley de reciprocidad para ser aplicada a tal conjetura. La misma conjetura llevo a Wiles en 1978 a generalizar la ley de reciprocidad de Iwasawa a grupos formales de Lubin-Tate. (Ver la segunda parte de esta tesis).

La primera parte de esta tesis versa sobre las leyes de reciprocidad clásicas, sus demostraciones y sus aplicaciones, tema que está activo todavía (como muestra véanse [5], [34], [11], [16], [12]). Hemos observado una falta de demostraciones directas desde la fórmula producto de la teoría de cuerpos de clases de las reciprocidades particulares clásicas (ie, de cálculos directos de los símbolos de Hilbert no moderados, como, eg, el sencillo caso cúbico del ejemplo 1.1). Tomando como punto de partida esa fórmula producto, tratamos de establecer métodos generales para obtener demostraciones nuevas y para *encontrar* fórmulas explícitas en términos clásicos de ciertas leyes de reciprocidad particulares. De esta forma más elemental se acortarían las demostraciones que se podrían obtener vía la aproximación de las fórmulas analíticas (éstas últimas requieren cálculos masivos, y su aproximación solo fue realizada en ciertos casos, concretamente para el carácter 2^n-potencial de 2 [21] y [13], y para los casos principales de las leyes de reciprocidad bicuadrática y óctica [23]). Nuestros métodos, además, han de permitir *encontrar* las fórmulas, y no meramente verificar candidatos a fórmulas esperadas.

En el capítulo 1 por una parte se reúnen y organizan aquellas nociones y resultados fundamentales necesarios, los cuales pueden ser encontrados en referencias usuales, que se citan adecuadamente. Así en este capítulo se incluyen breves demostraciones solamente de aquellos resultados que aquí hemos presentado de una forma menos conocida (eg, el lema 1.2). Como prerrequisitos están los de conocimientos básicos de Teoría de Números Algebraicos y nociones generales de la teoría de cuerpos de clases local y global. Aquí exponemos algunos temas más específicos para tratar de hacer, en lo posible, la memoria autocontenida, tales como la estructura de las unidades de un cuerpo local (secciones 1.1 y 1.4) y la formulación general de las leyes de reciprocidad para el símbolo de Hilbert y para el símbolo de residuo potencial (secciones 1.2 y 1.3). Por otro parte, en la sección 1.5 introducimos y desarrollamos uno de los métodos ya anunciados, el *método lineal*. El otro método, el que llamaremos *log-lineal*, lo introduciremos en el momento en que se ve necesario por no ser aplicable el primero (subsección (2.1.3)).

En el capítulo 2 se aplican los resultados y métodos desarrollados en el capítulo 1 para obtener aquellas nuevas demostraciones y para encontrar aquellas fórmulas explícitas en términos clásicos, antes comentadas, de las reciprocidades bicuadrática, óctica y de 16-potencias (bióctica). Apuntemos que estos métodos también podrían ser aplicados, no con más dificultad, a leyes de reciprocidad m-potenciales para $m = 3, 5, 7$ y 9. Pero nos hemos limitado a potencias de 2 por ser estos casos suficientemente ilustrativos y también de los más interesantes históricamente.

De la ley de reciprocidad bicuadrática hay hasta ahora algo más de 20 demostraciones (desde la original de Gauss (1828)). Aquí reencontramos las fórmulas

clásicas por nuestros métodos basados en la teoría de cuerpos de clases (ver la nota 2.3).

Desde la de Eisenstein de 1850 existen varias demostraciones de la ley de reciprocidad óctica, tanto por métodos clásicos, o bien basados en la teoría de cuerpos de clases. Aquí nuestro procedimiento (basado en esa teoría) es directo y permite trabajar exclusivamente en el dominio aditivo. Se han reencontrado las fórmulas clásicas, con nuevas demostraciones. Las fórmulas ócticas suplementarias (teorema 2.3, corolario 2.1(c) y (2.2.5)) solo las habíamos visto en sus restricciones a $\mathbb{Z}$ (Eisenstein 1850) y en el carácter óctico de 2. Para comentarios más detallados ver las notas 2.6 y 2.7.

Así como las otras leyes de reciprocidad particulares tienen varias demostraciones, sobre la ley de reciprocidad para 16-potencias (bióctica) solo se tiene, en versión *ciclotómica*, la ley de reciprocidad de Western 1907-1908 (reformulada en [5]), particularizada al caso $p^n = 16$, siendo ésta solo el caso principal y restricción a $\mathbb{Z}$. En su versión *racional*, la de Leonard-Williams [30]. Pero los residuos 16-potenciales sí han sido objeto específico de estudio. Cabe mencionar el carácter bióctico de 2 obtenido por Cunnhingam 1896, [1], [20] y otros.

Aquí hemos encontrado por primera vez fórmulas para la ley de reciprocidad bióctica ciclotómica (más fuerte y general que la racional), y en términos de coordenadas aditivas (los teoremas 2.4 y 2.5 y la proposición 2.3). Además las fórmulas biócticas principal, así como las restricciones a $\mathbb{Z}$ de ésta y de las suplementarias han resultado en términos clásicos y sencillos, paralelos a los de las leyes de reciprocidades cuadrática, bicuadrática y óctica. Resolvemos así, para el caso $p^n = 16$, el *problema de un dominio de definición explícito* de la mencionada reciprocidad de Western. Además extendemos al caso bióctico la ley de reciprocidad óctica de Eisenstein 1850.

En definitiva, se han encontrado fórmulas inéditas para la reciprocidad de 16-potencias, y se han reencontrado, con nuevas demostraciones, fórmulas clásicas bicuadrática, óctica y bióctica. Para más detalles sobre todo esto ver la nota 2.10.

El paralelismo que puede apreciarse en la obtención de las fórmulas bicuadrática, óctica y bióctica es una muestra de que los métodos que hemos usado son algorítmicos, y que podrían ser realizados también, sin mayor dificultad, en los otros casos ya citados con anterioridad. Nuestro procedimiento, en definitiva, reduce de forma sistemática y elemental la obtención de las fórmulas a un problema de cálculo rutinario/automático (aunque a veces enorme).

Esta primera parte estuvo inspirada originalmente en el caso cúbico de [10], Exercise 2.14 (ver el ejemplo 1.1), y en el intento de extender esa vía, basada en teoría de cuerpos de clases, al caso bicuadrático, donde, como puede apreciarse en la sección 2.1, ya aparecen dificultades esenciales respecto al cúbico.

Para los cálculos masivos involucrados en las fórmulas suplementarias óctica y bióctica ha sido necesario recurrir al uso de un programa de cálculo simbólico.

En cuanto a la notación (aparte de la lista de símbolos) apuntemos que, cuando en una fórmula se utilicen :=, o =:, se está definiendo un símbolo dentro de ella. Ejemplos, $(a, b) =: \zeta^{[a,b]}$ es para definir $[a, b]$; $N_1 a =: x + yi$ es para definir x e y.

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Capítulo 1

Resultados básicos

1.1. Sobre la estructura de las unidades de un cuerpo local

La estructura del grupo multiplicativo de un cuerpo local está involucrada en la teoría de cuerpos de clases, esencialmente porque sobre tal grupo está definido el símbolo de residuo nórmico local. En particular tal estructura es la clave para los cálculos locales del símbolo de Hilbert, lo cual, a su vez, es la vía de aquella teoría a las leyes de reciprocidad superiores y explícitas (ver las secciones 1.3,1.4 y 1.5). La referencia clásica es [22], pero véanse también [32] y [33] Chap. I, VI. En esta sección estableceremos brevemente la "estructura de subgrupos", dejando para la sección 1.4 la "estructura de generadores".

1.1.1. Sea $(A, \mathfrak{m}, \bar{k})$ un anillo local arbitrario y denotemos

$$U_i := 1 + \mathfrak{m}^i, i \geq 1, \quad U_0 := \mathcal{U}(A),$$

la filtración del grupo de unidades $\mathcal{U}(A)$ de A. Así se tiene una sucesión exacta de grupos $1 \to U_i \to \mathcal{U}(A) \to \mathcal{U}(A/\mathfrak{m}^i) \to 1$, en particular $\mathcal{U}(A)/U_1 \cong \dot{\bar{k}}$. La siguiente proposición es directa

Proposición 1.1. *Sea k un cuerpo con un valor absoluto discreto v, de cuerpo residual $\bar{k} = A/\pi A$.*

(a) *Para $i \geq 1$ y $0 \leq j \leq i$ la aplicación $a \mapsto x$, donde $a = 1 + \pi^i x \in U_i$, $x \in A$, da una sucesión exacta de grupos*

$$1 \to U_{i+j} \to U_i \to A/\pi^j A \to 1.$$

En particular $U_i/U_{i+1} \cong \bar{k}$, $i \geq 1$.

(b) *La topología de k es lineal y los subgrupos $\pi^i A$, $i \geq 0$, forman una base de entornos abiertos de k, así como del subgrupo abierto A.*

(c) *$\dot{k}$ es un grupo topológico lineal con la topología relativa de la de k. Los subgrupos U_i, $i \geq 0$, forman una base de entornos abiertos de $\dot{k}$, así como del subgrupo abierto $\mathcal{U}(k) := \mathcal{U}(A)$.*

(d) *Se tiene un isomorfismo de grupos topológicos*

$$\dot{k} =< \pi > \times \mathcal{U}(k) \cong \mathbb{Z} \times \mathcal{U}(k)$$

(donde la topología de $\mathbb{Z}$ *es la discreta).* □

La proposición 1.1 reduce la estructura de $\dot{k}$ a la de $\mathcal{U}(A)$. Sea ahora k un *cuerpo completo discreto* (valor absoluto discreto) *con cuerpo residual* $\bar{k}$ *perfecto.* La estructura de tales cuerpos ([32], Chap. II, §§4 y 5) da que es escindida la sucesión exacta anterior para $i = 1$, ie, se tiene un isomorfismo

$$\mathcal{U}(k) \cong \dot{\bar{k}} \times U_1.$$

Proposición 1.2 ([32], Chap. XIV, §3)**.** *En la situación previa sea* $m > 1$ *un entero primo con* char $\bar{k}$*. Entonces las siguientes condiciones son equivalentes*

(i) k *contiene al grupo* μ_m*.*

(ii) $\bar{k}$ *contiene al grupo* μ_m*.*

En este caso el homomorfismo canónico $\mathcal{U}(k) \to \dot{\bar{k}}$ *induce un isomorfismo entre los correspondientes grupos de unidades en* k *y en* $\bar{k}$*.* □

En lo que sigue supondremos que *el cuerpo residual* $\bar{k} = A/\pi A$ *es finito*, ie, k es un *cuerpo local discreto.* Denotemos $q := |\bar{k}| =: p^f$.

Nota 1.1. (a) $\mathcal{U}(k)/U_1 \cong \dot{\bar{k}}$ es un grupo cíclico de orden $q - 1$.

(b) $U_i/U_{i+1} \cong \bar{k} \cong (\mathbb{Z}/p\mathbb{Z})^f$, $i \geq 1$.

(c) U_i/U_{i+j} ($\cong A/\pi^j A$ para $j \leq i$), $i \geq 1$, es un grupo abeliano de orden $q^j = p^{fj}$ y de tipo $(p^s, \ldots, p^s)$, donde $s \leq j$. En particular $U_i^{p^s} \subset U_{i+j}$.

Corolario 1.1. *Sea* k *un cuerpo local y* $m \geq 1$ *primo con* $q = |\bar{k}|$*. Entonces* $k \supset \mu_m$ *si y solo si* $q \equiv 1$ (mód m)*. En particular la sucesión exacta*

$$1 \to U_1 \to \mathcal{U}(k) \to \dot{\bar{k}} \to 1$$

escinde con una única sección, y así

$$\mathcal{U}(k) \cong \mu_{q-1} \times U_1.$$

En cuanto a la torsión se tiene: $t(\mathcal{U}(k)) = \mu_{q-1} \times t(U_1)$*, y* $t(U_1) = \dot{k} \cap \mu_{p^\infty}$ *(la p-torsión de* $\dot{k}$*).* □

1.1.2. En lo que sigue supondremos, además, que k *es de distinta característica*, ie, k es *una extensión finita de* $\mathbb{Q}_p$, y denotaremos $e := e(k|\mathbb{Q}_p) = v(p)$, el índice de ramificación absoluto de k. También $f(k|\mathbb{Q}_p) = f$, donde $q = p^f$. Así $Nv := N_{k|\mathbb{Q}_p} v = p^f = q$ (ie, N denota la norma absoluta de k).

Proposición 1.3 ([32], Chap. XIV, §4)**.** *En la situación anterior, para* $i > e/(p-1)$*, la aplicación* $(-)^p \colon k \to k$ *induce un isomorfismo de grupos*

$$(-)^p \colon U_i \cong U_i^p = U_{i+e}.$$ □

Proposición 1.4 ([32], Chap. XIV, §4)**.** *Para $i > e/(p-1)$, se tiene que $U_i \cong A$ (como $\mathbb{Z}_p$-módulos topológicos). Por lo tanto U_i es un $\mathbb{Z}_p$-módulo libre de rango $[k:\mathbb{Q}_p]$.* □

Una demostración alternativa de la proposición 1.4 puede ser obtenida mediante las *funciones exponencial y logarítmica p-ádicas*

$$\exp(x) := \sum_{i=0}^{\infty} \frac{x^i}{i!} \quad \text{y} \quad \log(1+x) := \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i} x^i$$

(esta última es la involucrada en las fórmulas analíticas de las leyes de reciprocidad explícitas). La siguiente proposición, que da las propiedades básicas de esas series de potencias, es bien conocida ([8], Chap. IV, §5.2 y [3], Chap. XII, §2)

Proposición 1.5. (a) *La serie* $\log(1+x)$ *converge para* $1+x \in U_1$*. Además, si* $v(x) > e/(p-1)$*, entonces* $v\log(1+x) = v(x)$*.*

(b) *La serie* $\exp(x)$ *converge si* $v(x) > e/(p-1)$*.*

(c) *Las funciones* $\log\colon U_1 \to k$ *y* $\exp\colon \pi^i A \to U_i$*, $i > e/(p-1)$, son homomorfismos continuos de grupos y, para $i > e/(p-1)$, inducen isomorfismos inversos*

$$\pi^i A \cong U_i$$

(d) $\ker(\log\colon U_1 \to k) = t(U_1)$. □

Proposición 1.6. *El grupo U_1 es un $\mathbb{Z}_p$-módulo de tipo finito y rango $[k:\mathbb{Q}_p]$. Su grupo de torsión es μ_{p^n} para algún $n \geq 0$. ($U_1 = \mu_{p^n} \times F$, $F \cong A \cong \pi^i A \cong (\exp) U_i$, $i > e/(p-1)$).*

Demostración. Se sigue del corolario 1.1, de la proposición 1.4 y de la nota 1.1(c). □

En cuanto a la filtración de potencias $\dot{k}^m$ y al *índice potencial* $(\dot{k} : \dot{k}^m)$ es fácil deducir de la estructura de las unidades obtenida anteriormente

$$(\dot{k}:\dot{k}^m) = m\frac{((q-1)p^m, m)}{|m|_v} \quad \text{y} \quad (U_1 : U_1^m) = p^{\min(n, v_p(m)) + [k:\mathbb{Q}_p]v_p(m)}, \quad (1.1)$$

siendo $t(U_1) = \mu_{p^n}$ (ver la proposición 1.6). La proposición 1.3 se reformula como sigue

Proposición 1.7. *Para k como antes y $m \geq 1$ se tiene*

(a) $U_i^m = U_{i+v(m)}$*, para $i > e/(p-1)$.*

(b) *Para $i \geq 0$ fijo, los subgrupos U_i^m, $m \geq 1$, forman una base de entornos abiertos de $\dot{k}$.*

Demostración. (a) Es consecuencia de la proposición 1.3.

(b) Para el grupo profinito $U_i = \varprojlim U_i/U_{i+j}$, se sigue de (a). □

Aunque aquí no va a ser necesario el uso de la misma (de uso en teoría de cuerpos de clases) es ilustrativo incluir la siguiente

Proposición 1.8 ([3], p. XX)**.** *Sea ahora k un cuerpo local (discreto de cualquier característica, $\mathbb{R}$ o $\mathbb{C}$) y $m \geq 1$. Entonces el cociente de Herbrand trivial $h(-)$ verifica*

$$(\dot{k}:\dot{k}^m)/|\dot{k} \cap \mu_m| = h(\mathbb{Z}/m\mathbb{Z}, \dot{k}) = m/|m|_v$$

$$(= mh(\mathbb{Z}/m\mathbb{Z}, \mathcal{U}(k)) \text{ en el caso discreto}),$$

donde $|m|_v$ denota el valor absoluto normalizado ($|a|_v = |a|$ si $k = \mathbb{R}$, $|a|_v = |a|^2$ si $k = \mathbb{C}$ y $|a|_v = 1/q^{v(a)} (= 1/Na) = 1/(A:\pi A)^{v(a)} = 1/(A:aA)$, en el caso discreto). En particular, el índice potencial es finito si y solo si m es primo con char k. □

1.2. El símbolo de Hilbert

El símbolo de Hilbert es de hecho un caso del símbolo de residuo nórmico (de la teoría de cuerpos de clases local). Pero originalmente fue introducido por Hilbert para reformular la ley de reciprocidad cuadrática sobre cuerpos de números arbitrarios como una fórmula producto. Hilbert reemplazó los clásicos residuos potenciales por residuos nórmicos. De esta forma una ley de reciprocidad potencial quedaba reducida al cálculo local de ciertos símbolos de Hilbert. Este es el principio que utilizaremos para obtener las leyes de reciprocidad del capítulo 2.

1.2.1. Sea k un cuerpo de característica cero y $m \geq 1$. La sucesión exacta de la cohomología de Galois para la sucesión exacta $1 \to \mu_m \to \dot{\bar{k}} \xrightarrow{(-)^m} \dot{\bar{k}} \to 1$ da

$$0 \to \mu_m \cap k \to \dot{k} \xrightarrow{(-)^m} \dot{k} \to H^1(\ /k, \mu_m) \to H^1(\ /k) = 0$$

Así $\kappa\colon \dot{k}/\dot{k}^m \cong H^1(\ /k, \mu_m)$ es la llamada *aplicación de Kummer*. En el caso $\mu_m \subset k$ se tiene

$$\kappa\colon \dot{k}/\dot{k}^m \cong H^1(\ /k, \mu_m) = \mathrm{Hom}_{\mathrm{Top}}(G_k, \mu_m). \tag{1.2}$$

Así la aplicación de Kummer está dada explícitamente por la construcción de la *teoría de Kummer*

$$(\ ,\ ] : G_k \times \dot{k} \to \mu_m,$$

donde $(\sigma, b\,] := \beta^\sigma/\beta = \kappa(b)(\sigma)$, $\beta \in \dot{\bar{k}}$ tal que $\beta^m = b$.

Sea ahora k una *extensión finita de $\mathbb{Q}_p$*, $k \supset \mu_m$. De esta forma se puede usar la teoría de cuerpos de clases local, y sea pues $\psi := (\ ,\ /k)\colon \dot{k} \to (G_k)_{ab}$ el símbolo de residuo nórmico. Se define el *m-símbolo de Hilbert de k* como la composición

$$(\ ,\ ) = (\ ,\ )_v\colon \dot{k} \times \dot{k} \xrightarrow{\psi\times 1} (G_k)_{ab} \times \dot{k} \xrightarrow{(\ ,\ ]} \mu_m.$$

(G_K denota el grupo de Galois absoluto de un cuerpo K). Ie, $(a, b) := (\psi(a), b\,] = \beta^{\psi(a)}/\beta = \kappa(b)(\psi(a))$, donde $\beta \in \dot{\bar{k}}$ es tal que $\beta^m = b$.

Así el *símbolo de Hilbert es exactamente el símbolo de residuo nórmico para extensiones cíclicas de Kummer*. En el caso de un cuerpo de números todos los

símbolos de Hilbert del mismo están involucrados en un resultado global, la llamada *fórmula producto* para los mismos, que es un caso de la ley de reciprocidad de Artin, como veremos en la sección 1.3.

Proposición 1.9. *Sean k una extensión finita de $\mathbb{Q}_p$ y $m \geq 1$ tales que $\mu_m \subset k$.*

(a) *El símbolo de Hilbert*

$$(\ ,\ ): \dot{k}/\dot{k}^m \times \dot{k}/\dot{k}^m \to \mu_m$$

es una aplicación bilineal anticonmutativa. Si m es impar, entonces es antisimétrica, y es simétrica si $m \leq 2$. Además es una paridad topológica y tiene núcleos cero (el $\dot{k}/\dot{k}^m$ izquierdo considerado discreto), ie, si $(a,-) = 1$, entonces $a \in \dot{k}^m$.

(b) *$(a,b) = 1$ si y solo si $b \in N_{k(\alpha)|k}\dot{k}(\alpha)$, donde $\alpha^m = a$.*

(c) *$(a, x^m - a) = 1$ si $x \in k$ y $a, x^m - a \in \dot{k}$. En particular, $(a,-a) = (a, 1-a) = 1$. Además $(a,a) = (a,-1)$, y es un elemento de exponente 2. Si m es impar entonces $(a,a) = (a,-1) = 1$.*

(d) *Si $d|m$, entonces $(a,b)^d$ (para m) $= (a,b)$ (éste para m/d).*

(e) *$(a,\dot{k}) = \mu_m$ cuando $|a| = m$ (en $\dot{k}/\dot{k}^m$). Por lo tanto $(\ ,\ ): \dot{k} \times \dot{k} \to \mu_m$ es sobreyectivo. Además $(\pi, \mathcal{U}(k)) = \mu_m$ si π es un uniformizante de k.*

Demostración. (b) Por su definición vía el símbolo de residuo nórmico.

(c) Usar el argumento de [32], Chap. XIV, Proposition 4(iv), y luego (b).

(a) Que es anticonmutativa se sigue de (c) como en [32], Chap. XIV, Proposition 4(v). Que es de núcleos cero se sigue de que es anticonmutativa y del isomorfismo (1.2). □

Nota 1.2. 1. La propiedad (c) de la proposición 1.9 es la más peculiar de este símbolo al involucrar, siendo éste multiplicativo, a la estructura aditiva de k. En particular, la propiedad $(a,-a) = (a,1-a) = 1$ es, exactamente, el conjunto de axiomas de una *teoría de símbolos (de Steinberg)*, lo cual a su vez llevó a la *K-teoría de Milnor* (1971).

2. Si $k(a^{1/m})|k$ es no ramificada, entonces

$$(a,b) = (\alpha^F/\alpha)^{vb},\ \alpha \in \dot{k},\ \alpha^m = a,$$

donde $F := (v, k_{nr}|k)$ es el automorfismo de Fröbenius. Es decir, *el símbolo de Hilbert no ramificado de k es el automorfismo de Fröbenius para extensiones cíclicas de Kummer de k.*

1.2.2. *Cálculo del símbolo de Hilbert.* Este problema tiene dos casos de tratamiento muy diferente. Sea k una *extensión finita de* $\mathbb{Q}_p$ de cuerpo residual $\bar{k} = A/\pi A$ y $\mu_m \subset k$.

(1) *Caso moderado*: m es primo con char $\bar{k}$. En este caso $k(a^{1/m})|k$ es moderadamente ramificada. Además $U_1^m = U_1$ (ver (1.1)), y así $(U_1, \dot{k}) = 1$.

(2) *Caso no moderado*: char $\bar{k}|m$. El cálculo en este caso es el que daría las leyes de reciprocidad superiores y explícitas partiendo de la fórmula producto para el símbolo de Hilbert. Es el que necesitaremos realizar para obtener las leyes de reciprocidad del capítulo 2.

Proposición 1.10 ([32], Chap. XIV, §3)**.** *En el caso moderado se tiene la siguiente expresión para el símbolo de Hilbert de k*

$$(a,b) = (\overline{(-1)^{va\cdot vb}a^{vb}/b^{va}})^{(q-1)/m} \in \mu_m,$$

donde $\bar{u}$ denota la imagen por $\mathcal{U}(k) \to \dot{\bar{k}}$ (que envía μ_m en k a su isomorfo μ_m en $\bar{k}$ por la proposición 1.2*). Así (a,b) es la raíz m-ésima de la unidad en k determinada por*

$$(a,b) \equiv ((-1)^{va\cdot vb}a^{vb}/b^{va})^{(q-1)/m} \text{ mód } \pi. \qquad \square$$

1.2.3. *Símbolo de residuo potencial.* El *símbolo de residuo m-potencial* (clásico) de k, éste como en (1.2.2), se define, para $v(ma) = 0$, como la raíz m-ésima de la unidad determinada por

$$\left(\frac{a}{v}\right) \equiv a^{(q-1)/m} (= a^{(Nv-1)/m}) \text{ mód } \pi$$

(ie, se tiene la sucesión exacta $1 \to \dot{\bar{k}}^m \to \dot{\bar{k}} \xrightarrow{(\ /a):=(-)^{(q-1)/m}} \mu_m \to 1$, ver la proposición 1.2).

Puesto que $k(a^{1/m})|k$ es no ramificada (ver [27], Chap. II, Proposition 7) se sigue que el símbolo de residuo potencial (a/v), $v(ma) = 0$, de k es el automorfismo de Fröbenius $(v, k(a^{1/m})|k)(= F|_{k(a^{1/m})})$. Teniendo en cuenta la nota 1.2.2, se podría esperar que el símbolo de Hilbert diese el símbolo de residuo potencial como caso particular. Así definimos ahora el *símbolo de residuo potencial (local)* de k para $v(m) = 0$

$$\left(\frac{\cdot}{v}\right) : \mathcal{U}(k) \to \mu_m$$

mediante el símbolo de Hilbert moderado

$$\left(\frac{a}{v}\right) := (a,\pi) = \alpha^F/\alpha \in \mu_m,\ \alpha^m = a.$$

De la proposición 1.10 y de la nota 1.2.2 se obtienen las principales propiedades del símbolo de residuo potencial

Proposición 1.11. *Supongamos k y m en el caso moderado.*

(a) *Sean $a = u\pi^\mu$ y $b = u'\pi^\nu \in \dot{k}$, $u, u' \in \mathcal{U}(k)$. Entonces*

$$(a,b) = \left(\frac{-1}{v}\right)^{\mu\nu} \left(\frac{u}{v}\right)^{\nu} \left(\frac{u'}{v}\right)^{-\mu}.$$

En particular, si $a \in \mathcal{U}(k)$, entonces $(a,b) = \left(\frac{a}{v}\right)^{vb}$, y $\left(\frac{a}{v}\right)$ es la raíz m-ésima de la unidad determinada por

$$\left(\frac{a}{v}\right) \equiv a^{(q-1)/m} \text{ (mód } \pi).$$

Por lo tanto este $\left(\frac{a}{v}\right)$, definido vía el símbolo de Hilbert, coincide con el clásico (definido más arriba)*. En particular para $\zeta \in \mu_m$, se tiene $(\zeta/v) = \zeta^{(q-1)/m}$. Así ahora*

$$(a,b) = (-1)^{\mu\nu\frac{q-1}{m}} \left(\frac{u}{v}\right)^{\nu} \left(\frac{u'}{v}\right)^{-\mu}.$$

(b) *Para $a \in \mathcal{U}(k)$ las siguientes condiciones son equivalentes*

(i) $\left(\frac{a}{v}\right) = 1$

(ii) *La congruencia binómica $x^m \equiv a$* mód π *tiene solución en $\mathcal{U}(k)$ (o en A, o en k)*

(iii) $a \in \dot{k}^m$ *(o $a \in \mathcal{U}(k)^m$)*

Por lo tanto el símbolo de residuo potencial da una sucesión exacta

$$1 \to \mathcal{U}(k)^m \to \mathcal{U}(k) \xrightarrow{(-/v)} \mu_m \to 1$$

e isomorfismos $(-/v)\colon \mathcal{U}(k)/\mathcal{U}(k)^m \cong \mu_m$ y $v \times (-/v)\colon \dot{k}/\dot{k}^m \cong \mathbb{Z}/m\mathbb{Z} \times \mu_m$. Así el símbolo de residuo potencial divide al grupo $\mathcal{U}(k)$ en m clases de residuos módulo los residuos m-potenciales (lo que justifica su denominación).

(c) *El símbolo de residuo potencial es el automorfismo de Fröbenius para extensiones cíclicas de Kummer. Si $a \in \mathcal{U}(k)$, entonces la* ley de factorización (local) *para la extensión no ramificada $k(a^{1/m})|k$ es*

$$f(k(a^{1/m})|k) = |(a/v)| = |a| \text{ en } \bar{\dot{k}}/\bar{\dot{k}}^m \ .$$ □

1.3. Ley de reciprocidad potencial y fórmula producto para el símbolo de Hilbert

En esta sección se va a formular la ley de reciprocidad potencial (general) sobre un cuerpo de números (generalización amplia de la ley de reciprocidad cuadrática sobre $\mathbb{Q}$) y a mostrar cómo la teoría de cuerpos de clases (global) es una importante etapa de reducción de aquella reciprocidad a la fórmula producto para el símbolo de Hilbert. En este punto la obtención de una ley de reciprocidad potencial se reduce al cálculo de ciertos símbolos de Hilbert no moderados, lo que es un problema puramente local (que será realizado en los casos especiales que nos conciernen en las secciones y capítulo siguientes).

1.3.1. *El símbolo de residuo potencial* (global, ver [10], Exercise 1). Sea k un cuerpo de números algebraicos tal que $k \supset \mu_m$, $m \geq 1$. Denotemos $\mathcal{M}(k)$ el conjunto de divisores primos de k. Para $v \in \mathcal{M}(k)$, se denota k_v la v-completación de k y $\mathcal{U}_v := \mathcal{U}(k_v)$. Se va a globalizar el símbolo de residuo potencial local

$$\left(\frac{-}{v}\right) : \mathcal{U}_v \to \mu_m,$$

donde $v \nmid \infty$ (v discreto) y $v \nmid m$ (ie, char $\bar{k_v} \nmid m$).

Para un conjunto finito S de $\mathcal{M}(k)$ conteniendo a los diversos primos arquimedianos se denota

$$I_S := \{ \prod_{v \notin S} v^{n_v},\ n_v \in \mathbb{Z} \text{ casi todos cero } \}.$$

Para $a \in \dot{k}$ se denota $S(a) := \{v \in \mathcal{M}(k),\ v$ arquimediano o $v(m) \neq 0$ o

$v(a) \neq 0$ }. Se define, para $\mathfrak{b} \in I_{S(a)}$, el *símbolo de residuo potencial*

$$\left(\frac{a}{\mathfrak{b}}\right) := \prod_{v\nmid\infty} \left(\frac{a}{v}\right)^{\mathfrak{b}(v)} = \prod_{v\nmid m\cdot\infty} \left(\frac{a}{v}\right)^{\mathfrak{b}(v)} = \prod_{v\notin S(a)} \left(\frac{a}{v}\right)^{\mathfrak{b}(v)} \in \mu_m,$$

donde $\mathfrak{b} = \prod_{v\nmid\infty} v^{\mathfrak{b}(v)} = \prod_{v\nmid m\cdot\infty} v^{\mathfrak{b}(v)} = \prod_{v\notin S(a)} v^{\mathfrak{b}(v)}$. De esta forma

$$\left(\frac{a}{\mathfrak{b}}\right) = \alpha^{(\mathfrak{b},k(\alpha)|k)}/\alpha,$$

donde $\alpha^m = a$, y $(\ ,k(\alpha)|k)\colon I_{S(a)} \to G(k(\alpha)|k)$ es el símbolo de Artin. Usando la proposición 1.11(a) y que $a \in 1 + m\mathbb{Z} \mapsto (a-1)/m \in \mathbb{Z}/m\mathbb{Z}$ es totalmente multiplicativa (directo, o por la proposición 1.1(a)) se sigue

Proposición 1.12 (Segunda suplementaria de la ley de reciprocidad potencial)**.** *Sea $\zeta \in \mu_m$ y $\mathfrak{b}$ un ideal entero de k primo con m. Entonces*

$$(\zeta/\mathfrak{b}) = \zeta^{(N\mathfrak{b}-1)/m}$$

(donde se denota $N\mathfrak{b} := \prod_{v\nmid\infty} Nv^{\mathfrak{b}(v)}$, ver al comienzo de (1.1.2)). □

Para $a \in \dot{k}$ el símbolo de residuo potencial define un carácter sobre ideales

$$(a/-)\colon I_{S(a)} \to \mu_m.$$

Al estar éste dado por el símbolo de Artin de una extensión cíclica de Kummer, $(\ ,k(a^{1/m})|k)\colon I_{S(a)} \to G(k(a^{1/m})|k)$, la ley de reciprocidad potencial puede verse como un caso de la ley de reciprocidad de Artin para ideales.

Pero si (como para la ley de reciprocidad cuadrática) se quiere establecer la ley de reciprocidad potencial como una ley de inversión del símbolo $(a/\mathfrak{b})$ es necesario ante todo derivar de este un símbolo adecuado (a/b), para $a, b \in \dot{k}$. Así se define el carácter potencial $(a/-)$ sobre $\dot{k}$ como

$$\dot{k} \to I_{S(a)} \xrightarrow{(a/-)} \mu_m,$$

$b \in \dot{k} \mapsto (b)^{S(a)} := \prod_{v\notin S(a)} v^{v(b)} \in I_{S(a)}$, y se tiene un *símbolo de residuo potencial* (global)

$$\left(\frac{a}{b}\right) := \left(\frac{a}{(b)^{S(a)}}\right) = \prod_{v\notin S(a)} \left(\frac{a}{v}\right)^{v(b)} = \prod_{v\notin S(a)} (a,b)_v$$

(la última igualdad por la proposición 1.11(a)).

1.3.2. *Fórmula producto y ley de reciprocidad potencial* (ver [10], Exercise 2). Para establecer la ley de reciprocidad potencial para el símbolo (a/b) desde la ley de reciprocidad de Artin se debe tomar de esta última su *versión idélica*, particularmente su forma de *fórmula producto* para el símbolo de residuo nórmico.

Teorema 1.1 (Fórmula producto para el símbolo de Hilbert)**.** *Sea k un cuerpo de números algebraicos conteniendo a μ_m, $m \geq 1$. Entonces, para $a, b \in \dot{k}$, se*

tiene

$$\prod_{v\in\mathcal{M}(k)} (a,b)_v = 1.$$

Demostración. Se sigue de la fórmula producto para el símbolo de residuo nórmico de la teoría de cuerpos de clases, [10], Chap. VII, Theorem A, p. 168. Ver [3], Chap. XII, Theorem 13. □

Corolario 1.2 (Ley de reciprocidad potencial general)**.** *Sean* $a, b \in \dot{k}$.

(a) *Si* $S(a) \cap S(b) = \{v \in \mathcal{M}(k),\ v|m\cdot\infty\}$, *entonces*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v|m\cdot\infty} (b,a)_v.$$

(b) (Un caso de (a)). *Sea* $\lambda \in \dot{k}$ *tal que* $S(\lambda) = \{v \in \mathcal{M}(k),\ v|m\cdot\infty\}$. *Entonces* $(\lambda/b) = \prod_{v|m\cdot\infty}(b,\lambda)_v$.

(c) *Sea* $\zeta \in \mu_m$. *Entonces* $(\zeta/b) = \zeta^{(N(b)^{\{v|m\cdot\infty\}}-1)/m}$. *En particular, si* b *es primo con* m, *entonces* $(\zeta/b) = \zeta^{(|Nb|-1)/m}$. □

Nota 1.3. La ley de reciprocidad potencial del corolario 1.2 es una decisiva y unificadora etapa de reducción, proporcionada por la teoría de cuerpos de clases, hacia la ley de reciprocidad explícita más general (9º problema de Hilbert). Por lo tanto esa ley de reciprocidad queda reducida al cálculo explícito de los símbolos de Hilbert no moderados siguientes

$$(a,b)_v,\ v|m.$$

Así el 9º problema está reducido al cálculo de fórmulas explícitas para los símbolos de Hilbert p^n-potenciales no moderados de todos los cuerpos locales finitos sobre $\mathbb{Q}_p$, $p \geq 2$, $n \geq 1$.

1.4. Sobre la estructura de las unidades de un cuerpo local II: "Bases" de la filtración

1.4.1. *Reducción de la ley de reciprocidad potencial al caso local* ([3], Chap. XII; [10], Exercise 2). En lo que sigue nos vamos a restringir al *caso ciclotómico local* $k = \mathbb{Q}_p(\zeta)$, $p \geq 2$, $n \geq 1$, donde ζ es una raiz primitiva p^n-ésima de la unidad, es decir, $<\zeta>=\mu_{p^n}$. Entonces $\lambda := 1-\zeta$ *es un uniformizante* (ver [27], Chap. IV, Theorem 1). Así $p\mathbb{Z}_p[\zeta] = \lambda^{\varphi(p^n)}\mathbb{Z}_p[\zeta]$ y $N\lambda = p$. Como acabamos de ver en la nota 1.3, la ley de reciprocidad potencial está reducida, en este caso, al cálculo de los p^n-símbolos de Hilbert $(a,b)_\lambda$, $a, b \in \dot{k}$. Por los resultados de la sección 1.1 se tiene

$$\dot{k} = <\lambda> \times \mathcal{U}(k) = <\lambda> \times \mu_{p-1} \times U_1, \quad U_1 = <\zeta> \times F,$$

siendo F un $\mathbb{Z}_p$-módulo libre de rango $\varphi(p^n) = (p-1)p^{n-1}$, $F \cong \mathbb{Z}_p[\zeta] \cong U_i = 1+\lambda^i\mathbb{Z}_p[\zeta]$ (si $i > p^{n-1}$). Por lo tanto el cálculo de $(a,b)_\lambda$, $a, b \in \dot{k}$, está reducido

al de

$$(a,b)_\lambda,\ (b,\lambda)_\lambda,\ (b,\zeta)_\lambda,\ a,b\in F.$$

El primer problema está en que no se conoce, en general, una componente libre canónica F de U_1. Sería deseable que, como tal F, pudiese ser tomado algún U_i, $i>p^{n-1}$.

Lema 1.1. *Para $k=\mathbb{Q}_p(\zeta)$, $p\geq 2$, $n\geq 1$, se tiene*

(a) *$t(U_i)=<\zeta^{p^s}>$ para $p^{s-1}<i\leq p^s$, $0\leq s$. En consecuencia*

$$U_i \text{ es libre} \Leftrightarrow i>p^{n-1}$$

(b) *U_i es una componente libre de U_1 ($U_1=<\zeta>\times U_i$) si y solo si $n=1$ ó $p=n=2$, e $i=p^{n-1}+1$.*

(c) *Algún U_i es una componente libre de U_1 si y solo si U_i es una componente libre de U_1 para $i=p^{n-1}+1$ si y solo si $n=1$ ó $p=n=2$.*

Demostración. Se sigue fácilmente de la proposición 1.6. □

1.4.2. *Bases de la filtración* ([22]; [3], Chap. XII). Llegados a este punto de reducción en el cálculo de símbolos de Hilbert no moderados, es apropiado realizar tal cálculo sobre "bases" adecuadas de los U_i's (*bases de Hensel*). Volvamos momentáneamente al caso general $[k:\mathbb{Q}_p]=ef<\infty$ de cuerpo residual $\bar{k}=A/\pi A$.

Proposición 1.13 ([22], p. 238)**.** *En la situación anterior*

$$e/(p-1)<1\Rightarrow \mu_p\not\subset k\Leftrightarrow U_1 \text{ es un } \mathbb{Z}_p\text{-módulo libre.}$$

En este último caso una $\mathbb{Z}_p$-base de U_1 es

$$\left\{1+b_i\pi^j,\ i=1,\dots,f,\ j=1,\dots,pe/(p-1),\ p\nmid i\right\},$$

donde $b_1,\dots,b_f$ son representantes de una base de $\bar{k}$ sobre $\mathbb{Z}/p\mathbb{Z}$. □

Proposición 1.14 ([22], p. 239)**.** *Si $\mu_p\subset k$, entonces U_1 no es $\mathbb{Z}_p$-libre, y una $\mathbb{Z}_p$-"base" de U_1 es*

$$\{\ 1+b_i\pi^j\ (i=0,1,\dots,f,\ j=1,\dots,pe/(p-1),\ p\nmid i);\ 1+b_0\pi^{pe/(p-1)}\ \},$$

donde $b_1,\dots,b_f$ son representantes de una base de $\bar{k}$ sobre $\mathbb{Z}/p\mathbb{Z}$ tal que

$$b_1^{p^{\bar{\mu}}}-\epsilon b_1^{p^{\bar{\mu}-1}}\equiv 0,\ b_1\not\equiv 0 \text{ mód } \pi,$$

$\epsilon\in\mathcal{U}(k)$, $\bar{\mu}$ máximo para $\varphi(p^{\bar{\mu}})|e$, y $b_0\in A$ tal que $x^p-\epsilon x\equiv b_0$ mód π no es resoluble en k. □

Volvemos al caso ciclotómico local $k=\mathbb{Q}_p(\zeta)$, $p\geq 2$, $n\geq 1$, donde ahora $\pi=\lambda=1-\zeta$, $f=1$, $e=(p-1)p^{n-1}$, $\bar{\mu}=n$, $A=\mathbb{Z}_p[\zeta]$ y los b_i $(i=0,1)$ están en $\mathbb{Z}-p\mathbb{Z}$. Para ser coherentes con el uniformizante $\lambda=1-\zeta$, en la expresión de la $\mathbb{Z}_p$-"base" de U_1, deberíamos tomar $b_i=-1$. Denótese

$$\eta_i:=1-\lambda^i\in U_i,\ i\geq 1.$$

Corolario 1.3. *Para $k=\mathbb{Q}_p(\zeta)$, $p\geq 2$, $n\geq 1$, una $\mathbb{Z}_p$-"base" de U_1 es*

$$\{\eta_i,\ i=1,\dots,p^n,\ \text{tal que: } p|i\Rightarrow i=p^n\}.$$

Consta de $\zeta = \eta_1$ $(i = 1)$, que es una "base" de $t(U_1) =< \zeta >$, y de los restantes η_i, que forman una $\mathbb{Z}_p$-base de la componente libre F de U_1. □

Nota 1.4. En los casos en los que $F = U_i$, del lema 1.1(b) y del corolario 1.3, se obtiene

Si $n = 1$, entonces $i = 2$, $U_1 =< \zeta > \times U_2$ y $U_2 =< \eta_2, \ldots, \eta_p >$.
Si $p = n = 2$, entonces $i = 3$, $U_1 =< \zeta > \times U_3$ y $U_3 =< \eta_3, \eta_4 >$.

Vamos a tratar de dar "bases" de U_i mód $U_i^{p^n}$, suficientes para nuestro objetivo, evitando el uso de las proposiciones 1.13 y 1.14. Sea ahora $i > p^{n-1}$. Puesto que $U_i/U_{i+1} \cong \mathbb{Z}/p\mathbb{Z}$ se tiene que $U_i =< \eta_i > \cdot U_{i+1}$. Por lo tanto, inductivamente y usando la proposición 1.3, obtenemos $U_i =< \eta_i, \ldots, \eta_{i+\varphi(p^n)-1} > \cdot U_{i+\varphi(p^n)} =< \eta_i, \ldots, \eta_{i+\varphi(p^n)-1} > \cdot U_i^p$. Hemos obtenido

$$U_i =< \eta_i, \ldots, \eta_{i+\varphi(p^n)-1} > \cdot U_i^{p^r},\ i > p^{n-1}, \forall r \geq 0 \tag{1.3}$$

Ahora trataremos de obtener "bases" para todos los U_j, $j \geq i$, en términos de la "base" de U_i mód $U_i^{p^n}$ de (1.3)

$$\begin{gathered} U_j =< \eta_i^{p^{s+1}}, \ldots, \eta_{i+r-1}^{p^{s+1}}, \eta_{i+r}^{p^s}, \ldots, \eta_{i+\varphi(p^n)-1}^{p^s} > \cdot U_i^{p^t}, \\ j \geq i > p^{n-1},\ j - i = s\varphi(p^n) + r,\ 0 \leq r < \varphi(p^n), \forall t > s \end{gathered} \tag{1.4}$$

Se obtiene recursivamente partiendo de (1.3) teniendo en cuenta que

$$U_i \supset U_{i+1} \supset < \eta_i^p, \eta_{i+1}, \ldots, \eta_{i+\varphi(p^n)-1} > \cdot U_i^{p^r},\ r \geq 1,$$

los índices en U_i son p y $\leq p$, respectivamente.

Nota 1.5. En (1.3) y (1.4) son particularmente interesantes los casos $r = n$ y $t = n$, respectivamente, puesto que el símbolo de Hilbert se anula sobre $U_i^{p^n}$.

1.5. El método de las "bases". El método lineal

1.5.1. Seguimos en el caso ciclotómico local $k = \mathbb{Q}_p(\zeta)$, $p \geq 2$, $n \geq 1$ de (1.4.1). En la sección 1.4 se han mostrado "bases" adecuadas de los U_i, de forma que, para calcular el símbolo $(a, b)_\lambda$, sólo quedarían las dos etapas siguientes

Primera etapa: calcular el símbolo en esas "bases".
Segunda etapa: partiendo de esto, obtener fórmulas explícitas para el símbolo.

Llamaremos a esto el *método de las "bases"*. Distinguiremos entre *encontrar* una fórmula desconocida y *verificar* un candidato bimultiplicativo a la misma. "Encontrar" significa no disponer de un tal candidato.

El método de las bases se fundamenta en

a) El uso de las propiedades axiomáticas del símbolo de Hilbert (ver la nota 1.2.1).

b) La estructura del grupo $\dot{k}$, y las "bases" de los U_i.

1.5.2. *Descripción de los métodos.* Lo que precede, **a)** y **b)**, va a reducir la primera etapa de (1.5.1) al cálculo de los $(\eta_j, \lambda)_\lambda$. Vamos a perfilar algunos puntos y procedimientos a este respecto, así como de la segunda etapa.

A) *Términos explícitos requeridos para una fórmula.* Los de las *coordenadas multiplicativas*: coordenadas respecto a la base de los η_j.

Los de las *coordenadas aditivas*: las *coordenadas absolutas*, respecto a la $\mathbb{Z}_p$-base $1, \zeta, \ldots, \zeta^{\varphi(p^n)-1}$ de $\mathbb{Z}_p[\zeta]$. Los *parámetros*, coordenadas absolutas en $U_i := 1 + \lambda^i \mathbb{Z}_p[\zeta]$. Las coordenadas en términos de subcuerpos especiales de $\mathbb{Q}_p(\zeta)$, como las "*cuadráticas*" de Golsheider [15], y, en general, las *de Hasse* de [20]. Y las (más adecuadas para el caso general) de [13]. (Ver (2.2.5)). Un caso de esto es el de *en términos de la norma absoluta* (ver, eg, el teorema 2.1(a)).

Para las fórmulas explícitas generales los adecuados y requeridos son los *términos en objetos analíticos*, lo que llamaremos *fórmulas* log, o *analíticas*.

B) *Uso de la segunda suplementaria a la ley de reciprocidad potencial general* (para la primera y la segunda etapa de (1.5.1)).

Nota 1.6. 1. Del corolario 1.2(c) se sigue

$$(b, \zeta)_\lambda = (\zeta/b) = \zeta^{(Nb-1)/p^n},$$

para $b \in \mathbb{Z}[\zeta]$ primo con p, ie, para $b \in \mathbb{Z}[\zeta] - \lambda\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta] \cap \mathcal{U}(k)$ (para $p^n = 2$ suprimir (ζ/b)).

2. Si ahora se quiere extender la fórmula global de la nota 1 a una fórmula local para $b \in \mathcal{U}(k)$ probemos que $Nb \equiv 1$ (mód p^n), y así $\zeta^{(Nb-1)/p^n}$ *resulta multiplicativo sobre* $\mathcal{U}(k)$ (usar la proposición 1.1(a)). En efecto, de la versión local del teorema de Kronecker-Weber (ver [32], Chap. XIV §7) se sigue que el grupo de normas de $k = \mathbb{Q}_p(\zeta)$ es $N\dot{k} =< p > \times U_{\mathbb{Q}_p,n}$. Puesto que $N\lambda = p$, y $\mathcal{U}(k) = \mu_{q-1} \times U_1$ (corolario 1.1) obtiene que

$$N\mathcal{U}(k) = NU_1 = NF = U_{\mathbb{Q}_p,n}$$

(donde F es una componente libre de U_1).

Proposición 1.15 (Segunda suplementaria local)**.** *Se tiene*

$$(b, \zeta)_\lambda = \zeta^{(Nb-1)/p^n}, \ b \in \mathcal{U}(k).$$

En particular, para $p = 2$, $n \geq 1$, *se tiene*

$$(b, b)_\lambda = (-1)^{(Nb-1)/2^n}, \ b \in \mathcal{U}(k).$$

Demostración. Para la segunda afirmación usar la primera y la proposición 1.9(c). En cuanto a la primera basta probar la igualdad sobre U_1. Pero U_1 está generado (mód $\mathcal{U}(k)^{p^n}$) por algunos η_j (uso de (1.3) y del lema 1.1), los cuales están en $\mathbb{Z}[\zeta] \cap \mathcal{U}(k)$. Que sobre éste se verifica la fórmula se sigue del corolario 1.2(c). Finalmente, por la multiplicatividad dada por la nota 1.6.2, se verifica sobre U_1. □

C) *Reducción de los* (η_i, η_j) *a los* (η_j, λ) ("K-teoría", para la primera etapa de (1.5.1)). Esto está basado en **a)** y **b)** de (1.5.1).

En lo que sigue eliminamos la referencia al primo λ en la notación $(a, b) = (a, b)_\lambda$. De **a)**, ie, de la proposición 1.9(c) se obtiene la

Proposición 1.16 ([18]; [19]; [10], Exercise 2)**.** *Sea* $[k:\mathbb{Q}_p(\zeta)] < \infty$*,* $p \geq 2$*,* ζ *una raiz primitiva* m*-ésima de la unidad,* $m \geq 1$*. Fijemos* $\alpha \in \dot{k}$ *y denotemos* $\beta_i := 1 - \alpha^i$*,* $i \geq 1$*. Entonces*

(a) $(\beta_i, \beta_j) = (\beta_i, \beta_{i+j})(\beta_{i+j}, \beta_j)(\beta_{i+j}, \alpha)^{-j}(\beta_{i+j}, \beta_{i+j})$

(b) *El orden de* (β_i, α) *divide a* $\mathrm{mcd}(i, m)$*. En particular, si* i *es primo con* m*, entonces* $(\beta_i, \alpha) = 1$*.* □

Nota 1.7. Eisenstein en 1850 probó las fórmulas de la proposición 1.16 directamente en el caso particular del símbolo de residuo potencial (ver [18], p. 56). Sin embargo el contexto local, introducido por Hensel y Hasse, permite usar propiedades de un cuerpo completo, tales como la existencia de raíces m-ésimas, y así la anulación del símbolo.

Proposición 1.17. *Sea ahora* $k = \mathbb{Q}_p(\zeta)$*,* $p \geq 2$*,* $n \geq 1$*. Si* $i+j > p^{n-1}+n\varphi(p^n)$*, entonces*

$$(a, b) = 1 \text{ para } a \in U_i \text{ y } b \in U_j.$$

Demostración. Puesto que el segundo miembro de la igualdad requerida es (obviamente) bimultiplicativo, basta probar aquélla sobre los generadores. Usando (1.3) podemos trabajar módulo $\mathcal{U}(k)^{p^n}$, y sean η_k y η_l generadores de U_i y U_j, respectivamente. Entonces (η_k, η_l) es producto de símbolos que tienen una variable en U_{k+l} por la proposición 1.16(a), y $U_{k+l} \subset U_{i+j} \subset U_{p^{n-1}+1+n\varphi(p^n)} = U_{p^{n-1}+1}^{p^n}$ (uso de la proposición 1.3). Por lo tanto $(U_i, U_j) = 1$. □

Una aplicación sistemática de las proposiciones 1.16 y 1.17 reduce los símbolos (η_i, η_j) a los (η_j, λ).

D) *Cálculo de los símbolos* (η_j, λ)*: Reducción a los* (η_j, ζ) (primera y segunda etapas). Esto consiste en invertir el procedimiento de **C)** para luego apoyarse en **B)**. Por las proposiciones 1.16 y 1.9(c) se tiene

$$\begin{aligned}(\eta_j, \zeta) &= (\eta_j, \eta_{j+1})(\eta_{j+1}, \zeta)(\eta_{j+1}, \lambda)^{-1}(\eta_{j+1}, \eta_{j+1}) \\ &= (\eta_j, \eta_{j+1})(\eta_{j+1}, \zeta)(\eta_{j+1}, \lambda)^{-1}(\eta_{j+1}, -1).\end{aligned}$$

Si ahora se redujese (η_j, η_{j+1}) a (η_k, λ), entonces varios (η_k, λ) podrían aparecer en la expresión final, y así no podría ser expresado uno de ésos (η_k, λ) en términos exclusivos de los (η_l, ζ). Sin embargo este proceso puede ser mejorado, incluso de forma concluyente, teniendo en cuenta lo siguiente

(1) $(\eta_j, \lambda) = 1$ si $p \nmid j$ (proposición 1.16(b))

(2) (a, b) es antisimétrico si $p > 2$ (proposición 1.9(a))

(3) Si $p = 2$, entonces $(\eta_i, \eta_i) = (\eta_i, -1) = (\eta_i, \zeta)^{2^{n-1}}$ (proposición 1.9(c))

(4) El cálculo de los (η_j, λ) es requerido tanto para reducir al mismo la primera suplementaria de la ley de reciprocidad potencial (segunda etapa) como para calcular los (η_i, η_j) (primera etapa). Para lo primero, por (1) y por el corolario 1.3, basta calcular (η_{p^n}, λ). Para lo segundo podrían estar involucrados varios (η_j, λ). En ciertos casos particulares todos los que fuesen requeridos pueden ser calculados por el procedimiento que se acaba de describir (como se va a mostrar en los casos del capítulo 2).

E) *Aproximación de la función* log. Esto va a ser necesario en el uso de lo que llamaremos "método log-lineal", descrito en (2.1.3). Se va a acotar el resto en la aproximación por la serie de potencias de $\log(1+x)$, $v(x) > 0$. Es fácil obtener la siguiente acotación

$$v(\log(1+x) - \sum_{i=1}^{s}(-1)^{i-1}x^i/i) \geq$$
$$\text{mín}\,\{(s+1)v(x), (c+1)pv(x) - (p-1)(1+v_p(c+1))\}$$

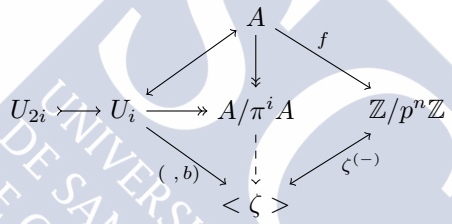
donde $s = cp + r$, $0 \leq r < p$, y v_p denota la valoración de $\mathbb{Q}_p$.

F) *El método lineal* (segunda etapa). El método lineal, en aquellos casos a los que se pueda aplicar, nos permite *encontrar* fórmulas explícitas para el símbolo de Hilbert partiendo de los cálculos en los generadores.

Sea $[k:\mathbb{Q}_p(\zeta)] < \infty$, $p \geq 2$, $n \geq 1$, A su anillo de enteros y π un uniformizante. Para $i \geq 1$, dado, la aplicación $a \mapsto x$, donde $a = 1 + \pi^i x \in U_i$, $x \in A$, da una biyección $U_i \leftrightarrow A$, que no es un homomorfismo de grupos, y una sucesión exacta de grupos abelianos (ver la proposición 1.1(a))

$$1 \to U_{2i} \to U_i \to A/\pi^i A \to 1.$$

Sea $b \in \dot{k}$, fijo, y consideremos el siguiente diagrama



donde $f(= f_b)\colon A \to \mathbb{Z}/p^n\mathbb{Z}$ es la aplicación que hace ese diagrama conmutativo, ie, $(a,b) =: \zeta^{f(x)}$.

Lema 1.2. *En la situación anterior, para $i \geq 1$ y $b \in \dot{k}$ dados, las siguientes condiciones son equivalentes*

(i) *f es una aplicación $\mathbb{Z}$-lineal (o $\mathbb{Z}_p$-lineal)*

(ii) *$(a,b) = 1$ para todo $a \in U_{2i}$*

Cuando esas condiones son satisfechas se dice que k es lineal en b (rel. i).

Demostración. Nótese que si f es $\mathbb{Z}$-lineal, entonces es $\mathbb{Z}_p$-lineal por completación.

(i)⇒(ii): Para $x \in A$ se tiene $f(\pi^i x) = f(x+1+\pi^i x) - f(x+1)$. Poniendo $a = 1+\pi^i x$ y $a' = 1+\pi^i$ se tiene $aa' = 1+\pi^i(x+1+\pi^i x)$. Así $f(\pi^i x) = 0$ puesto que $(a,b) = \zeta^{f(x)}$, y $(a',b) = \zeta^{f(1)}$ y $(aa',b) = \zeta^{f(x+1+\pi^i x)}$. Por lo tanto $(a,b) = 1$ si $a \in U_{2i}$.

(ii)⇒(i): Puesto que U_{2i} está contenido en el núcleo de $(\ ,b)\colon U_i \to <\zeta>$, esta aplicación tiene la factorización $A/\pi^i A \dashrightarrow <\zeta>$ indicada en el diagrama previo. Entonces f es la composición $A \to A/\pi^i A \to <\zeta> \to \mathbb{Z}/p^n\mathbb{Z}$, y así un homomorfismo de grupos. □

Nota 1.8. 1. *Organización del método lineal.* Sea k lineal en b (rel. i). Se va a hacer uso del lema 1.2.

• Entonces $f\colon A \to \mathbb{Z}/p^n\mathbb{Z}$ se factoriza vía $A/\pi^i A$, y así vía $A/(p^nA+\pi^iA)$, por lo que f está determinada por su factor $A/(p^nA+\pi^iA) \to \mathbb{Z}/p^n\mathbb{Z}$. Pero $a = 1+\pi^i x$ da el isomorfismo $A/\pi^i A \cong U_i/U_{2i}$, y así $A/(p^nA+\pi^iA) \cong U_i/(U_i^{p^n}\cdot U_{2i})$.

• Por lo tanto los generadores $\eta_j = 1+\pi^i x_j$ de U_i (mód $U_i^{p^n}$) dan generadores x_j de $A/(p^nA+\pi^iA)$, y así $f(x)$ está determinada por los $f(x_j)$. El cálculo de $(\eta_j, b) = \zeta^{f(x_j)}$ da la matriz $(f(x_j))$ de $f(x)$ respecto a la base (x_j).

• Ahora, un simple cambio de base (el de los x_j a una base entera de A, ésta dando las coordenadas de $x \in A$) en el $\mathbb{Z}/p^n\mathbb{Z}$-módulo libre $A/p^nA \cong (\mathbb{Z}/p^n\mathbb{Z})^{[k:\mathbb{Q}_p]}$ proporciona (la matriz de $f(x)$ respecto a (ζ^j) y así) una fórmula explícita para $f(x)$, y por lo tanto para $(a,b) = \zeta^{f(x)}$, $a \in U_i$, en términos de coordenadas de x, ie, de parámetros de a.

2. Del lema 1.2 se sigue "k es lineal en b (rel i), para todo $b \in \dot{k}$ si y solo si $p = 2$ ó 3 y $n = 1$". Pero, para $p = n = 2$, k no es lineal en $b = \lambda$ (rel. 3).

3. Las restricciones de este método lineal serán solventadas, de una forma simple, sustituyendo la anterior biyección no lineal $U_i \leftrightarrow A$ por su 'linealización' $\log\colon U_i \to \lambda^i A$. El procedimiento es formalmente el mismo que el que se acaba de exponer (ver (2.1.3)). Este procedimiento será usado también en las reciprocidades particulares del capítulo 2.

4. El método local a leyes de reciprocidad explícitas comenzó en [17]. El uso sistemático del método de las 'bases' para reducir (η_i, η_j) a (η_j, λ) de [2] comenzó en [18].

Ejemplo 1.1 (Ley de reciprocidad cúbica)**.** Mostremos cómo con la base de este capítulo esta reciprocidad es particularmente simple (no así las del capítulo 2). Sea $k = \mathbb{Q}_3(\zeta)$, donde $< \zeta >= \mu_3$. De (1.3) y de la proposición 1.3 se tiene $U_2 =< \eta_2, \eta_3 >$ (mód $U_2^3 = U_4$). De la proposición 1.17 se obtiene la *ley de reciprocidad cúbica principal*

$$(a,b) = 1 \text{ si } a, b \in U_2.$$

Sea $a = x + y\zeta$. Entonces $(Na-1)/3 \equiv (1-x-y)/3$ y así por la proposición 1.15 $(a,\zeta) = \zeta^{(1-x-y)/3}$ (*segunda suplementaria*). Usando las notas 1.8.1 y 2, sea $(a,\lambda) = \zeta^{f(x)}$, $a = 1 + 3\mathbf{x} = 1 + 3(m + ni) \in U_2$. Para los generadores η_2 y η_3 se tiene $f(\mathbf{x}_2) = 0$ y $f(\mathbf{x}_3) = 1$ por la proposición 1.16(b), y **D)** de (1.5.2). Por linealidad se obtiene $f(\mathbf{x}) = m$, y así $(a,\lambda) = \zeta^{(x-1)/3}$, la *primera suplementaria*.

Ver [10], Exercise 2.14.

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Capítulo 2

Casos particulares: reciprocidades para 4, 8 y 16-potencias

En el capítulo 1 se formuló la ley de reciprocidad general y se desarrollaron métodos específicos para (partiendo de la fórmula producto) demostrar leyes de reciprocidad clásicas particulares y para encontrar las fórmulas explícitas. En este capítulo aplicaremos tales métodos para obtener nuevas demostraciones de ciertas leyes de reciprocidad particulares notables. Aunque se podrían incluir más casos, nos vamos a limitar a los de potencia de 2. Éstos han sido objeto de estudio primordial desde Euler (1783), Legendre y Gauss (el primo 2 es diferente). También son los más adecuados para ilustrar los métodos del capítulo 1 (y el de (2.1.3)).

2.1. Ley de reciprocidad bicuadrática. El método log-lineal

2.1.1. Sea $k = \mathbb{Q}_2(i)$ ($p = n = 2$). Usando el corolario 1.1, la proposición 1.6 y el lema 1.1 se tiene

$$\mathcal{U}(k) = U_1 = < i > \times U_3.$$

Además éste es un caso ciclotómico cuadrático $2\mathbb{Z}_2[i] = \lambda^2\mathbb{Z}_2[i]$ ($\lambda = 1 - i$)

$$\lambda^2 = -2i,\ 2 = \lambda^2 i \quad \text{y} \quad \lambda^4 = -4.$$

El cálculo del símbolo de Hilbert $(a, b) = (a, b)_\lambda$ sobre k está reducido al de

$$(a, b),\ (a, \lambda),\ (a, i),\ a, b \in U_3$$

(ver (1.4.1)). Además $U_3 =< \eta_3, \eta_4 = 5 >$ (mód $U_3^4 = U_7$) por la proposición 1.3 y por (1.3). Sin embargo en este caso el símbolo (a, b) no es ni simétrico ni antisimétrico (ver la proposición 1.9(a)). Entonces, para calcular el símbolo

sobre los generadores en orden a aplicar luego el método lineal ((1.5.2)**F)**), se hará uso de los procedimientos **B)** y **D)** de (1.5.2).

Sea $a = x+yi = 1+\lambda(m+ni) \in U_1 = \mathcal{U}(k)$, así $x = 1+m+n$ e $y = -(m-n)$. Entonces $Na = x^2 + y^2 \equiv 1$ (mód 4), y $(Na-1)/4 = (m^2+n^2+m+n)/2 \equiv Na^2 - 1/8$ (mód 2). Por la proposición 1.15, se tiene

$$(a, i) = i^{(Na-1)/4} = i^{(m^2+n^2+m+n)/2}.$$

En el caso $a \in U_3$, se tiene $a = x + yi = 1 + \lambda^3(m + ni) = 1 + \lambda(2n - 2mi)$. Así

$$\begin{array}{ll} x = 1 - 2(m-n) & y = -2(m+n) \\ m = (1-x-y)/4 & n = (-1+x-y)/4. \end{array}$$

Entonces $(Na-1)/4 = 2(m^2+n^2) - m + n \equiv m - n \equiv (1-x)/2$ (mód 4), y así

$$(a, i) = i^{m-n} = i^{(1-x)/2}$$

En particular, $(\eta_3, i) = -i$ y $(\eta_4, i) = -1$. Usando ahora **D)** de (1.5.2) y la proposición 1.17 se tiene

$$(\eta_4, \lambda) = (\eta_3, i)^{-1}(\eta_4, i) = -i \tag{2.1}$$

Análogamente $-1 = (\eta_4, i) = (\eta_5, i) = (\eta_6, \lambda)^{-1}$. Así **C)** de (1.5.2) da

$$(\eta_3, \eta_3) = (\eta_6, \lambda)^{-3} = -1.$$

(Más directamente, de la proposición 1.15, $(\eta_3, \eta_3) = (-1)^{(N\eta_3-1)/4} = -1$).

Por el lema 1.2 y la proposición 1.17 se tiene que *k es lineal en b* (rel. 3) *para todo $b \in \mathcal{U}(k) = U_1$*. Puesto que conocemos la matriz

$$(\eta_i, \eta_j) = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix},\ i, j = 3, 4,$$

y dado que $\eta_3 = 1+\lambda^3(-1)$ y $\eta_4 = 1+\lambda^3(-1+i)$, entonces, por linealidad y un cambio de base rutinario para formas bilineales (ver la nota 1.8.1) *encontramos*

$$(a, b) = i^{2(m+n)(m'+n')} = (-1)^{(m+n)(m'+n')},$$

para $a = x + yi = 1 + \lambda^3(m + ni)$ y $b = x' + y'i = 1 + \lambda^3(m' + n'i) \in U_3$. Como ya se mostró más arriba tenemos

$$(Na-1)/4 = (1-x)/2 \text{ (mód 4)} \equiv (Na^2-1)/8 \equiv m+n = y/2 \text{ (mód 2)} \tag{2.2}$$

Además $(a-1)/\lambda^3 = m + ni \in \mathbb{Z}_2[i]$ y $m + n$ son iguales en $\mathbb{Z}/2\mathbb{Z}$, ya que $m+ni \equiv m+n$ (mód λ). Así resulta la siguiente ley de reciprocidad bicuadrática principal (uso de (2.2))

$$\begin{aligned} (a, b) &= (-1)^{(Na-1)/4\cdot(Nb-1)/4} = (-1)^{(m+n)(m'+n')} \\ &= (-1)^{\frac{x-1}{2}\cdot\frac{x'-1}{2}} = (-1)^{\frac{y}{2}\cdot\frac{y'}{2}} = (-1)^{\frac{a-1}{\lambda^3}\cdot\frac{b-1}{\lambda^3}}. \end{aligned}$$

2.1.2. *La suplementaria primera.* El de la obtención de una fórmula para (a, λ), $a \in U_3$, no es un caso lineal (ie, uso del lema 1.2 y de la proposición 1.17). Puesto que k es lineal (rel. 4) en λ, usando el método lineal se obtiene

$$(a, \lambda) = i^m,\ a = 1 + \lambda^3(m + ni) \in U_4,\ \text{ie, } m + n \equiv 0 \text{ (mód 2)} \tag{2.3}$$

Se va a obtener una fórmula para (a,λ) en términos de coordenadas multiplicativas

$$a = \eta_3^{\alpha_1}\eta_4^{\alpha_2} \pmod{U_3^4 = U_7}$$

$\alpha_1, \alpha_2 = 0,1,2,3$. Por la proposición 1.16(b) se tiene $(\eta_3,\lambda) = 1$, que con (2.1) da

$$(a,\lambda) = i^{-\alpha_2},\ a \in U_3 \tag{2.4}$$

El símbolo sólo depende de $U_3/U_3^4 = U_3/U_7 \cong (\mathbb{Z}/4\mathbb{Z})^2$. El problema ahora es *transcribir coordenadas multiplicativas a aditivas*. Esto significa hacer explícita la biyección entre las 16 clases de U_3/U_7 en U_3 y las 16 clases de $\mathbb{Z}_2^2/(4\mathbb{Z}_2)^2$ en $\mathbb{Z}_2^2$, inducida por la biyección

$$U_3 \leftrightarrow \mathbb{Z}_2[i] \leftrightarrow \mathbb{Z}_2^2,$$

dada por $a = 1+\lambda^3 x = 1+\lambda^3(m+ni)$. Por (2.3) podemos limitarnos a las 8 clases de U_3/U_7 en $U_3 - U_4$. Sobre sus representantes la correspondencia, obtenida por cálculo de los parámetros de aquellos, es como sigue

$$\begin{array}{rl}
\eta_3 = 1+\lambda^3(-1+0i) & (-1,0)\\
\eta_3\eta_4 = 1+\lambda^3(-6+i) & (2,1)\\
\eta_3\eta_4^2 = 1+\lambda^3(-31+6i) & (1,2)\\
\eta_3\eta_4^3 = 1+\lambda^3(-156+31i) & (0,-1)\\
\eta_3^3 = 1+\lambda^3(-9-14i) & (-1,2)\\
\eta_3^3\eta_4 = 1+\lambda^3(-46-69i) & (2,-1)\\
\eta_3^3\eta_4^3 = 1+\lambda^3(-231-344i) & (1,0)\\
\eta_3^3\eta_4^3 = 1+\lambda^3(-1156-1719i) & (0,1)
\end{array}$$

Denotemos $(a,\lambda) = i^{-\alpha_2} = i^{f(m,n)}$, $a \in U_3$. Por (2.3), $f(m,n) \equiv m \pmod 4$ si $m+n \equiv 0 \pmod 2$, ie, si $(m+n)^2 \equiv 0 \pmod 4$. De los anteriores datos y aplicando (2.4) sobre los representantes, se tiene

$$\begin{array}{ll}
f(-1,0) = f(-1,2) = 0, & f(0,-1) = f(0,1) = 1,\\
f(1,2) = f(1,0) = 2, & f(2,1) = f(2,-1) = -1.
\end{array}$$

Por lo tanto, poniendo $f(m,n) = m + h(m,n)$, se tiene

$$h(m,n) \equiv \begin{cases} 0 \pmod 4 & \text{si } m+n \equiv 0 \pmod 2\\ 1 \pmod 4 & \text{si } m+n \equiv 1 \pmod 2 \end{cases}$$

Así $h(m,n) = k(m+n)$ donde $k\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ verifica $k(0) = k(2) = 0$, $k(\pm 1) = 1$. Pero esto es exactamente la función $k(x) = x^2$. Hemos obtenido

$$(a,\lambda) = i^{m+(m+n)^2},\ a \in U_3.$$

2.1.3. *El método* log-*lineal*. Vamos a mostrar un segundo procedimiento para buscar y encontrar una fórmula para la suplementaria primera bicuadrática, que tenga validez general y así pueda ser aplicado a casos no lineales.

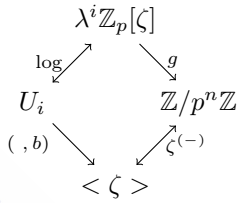
Cuando en (2.1.2) se trascribieron coordenadas multiplicativas a aditivas estaba involucrada la función $\beta\colon U_i \to \lambda^i\mathbb{Z}_2[i]$ dada por $a = 1+\lambda^i x \in U_i$, $x \in \mathbb{Z}_2[i]$, que es no lineal. Así, si se busca un tratamiento general de los casos no lineales, la tarea natural será la "linealización" de esa función. Esto está

proporcionado por los logaritmos λ-ádicos de Kummer (ver la proposición 1.5)

$$\log\colon U_i \to \lambda^i\mathbb{Z}_2[i]\,,\ i > e/(p-1)$$

(la función β anterior es la parte de grado 1 de log).

Sea $k = \mathbb{Q}_p(\zeta)$, $p \geq 2$, $n \geq 1$. Para $b \in \dot{k}$ e $i > e/(p-1)$, fijos, sea $g\colon \lambda^i\mathbb{Z}_p[\zeta] \to \mathbb{Z}/p^n\mathbb{Z}$ dada por la conmutatividad de



ie, $(a,b) = \zeta^{g(\log a)}$. Así g es lineal en todos los casos en los que esté definida. Por lo tanto el mismo procedimiento del método lineal ((1.5.2)**F**)) permitirá *encontrar* g, procedimiento que organizamos como sigue

• Los cálculos (η_j, b) sobre la "base" η_j de U_i dan la matriz de g respecto a la "base" $(\log \eta_j)$ de $\lambda^i\mathbb{Z}_2[i]$.

• Para cambiar a la "base" $(\lambda^i\zeta^j)$ es necesario aproximar los $\log \eta_j$ (uso de **E)** de (1.5.2)) para poder así utilizar la nota 2.1, que sigue.

• Por linealidad esto da una fórmula explícita para $g(\log\, a) = g(\lambda^i(m_0 + m_1\zeta + \cdots))$ en términos de parámetros $(m_0, m_1, \ldots)$ de $\log\, a$.

• Finalmente, aproximando $\log\, a$ y usando la nota 2.1, de nuevo, de aquélla fórmula explícita se encuentra una para $(a,\lambda)(= \zeta^{g(\log\, a)})$ en términos de los parámetros de $a = 1 + \lambda^i(n_0 + n_1\zeta + \cdots)$.

Al procedimiento que se acaba de describir lo llamaremos el *método log-lineal*. Permitirá extender el método lineal a casos no lineales.

Nota 2.1. Una aplicación lineal $g\colon \lambda^i\mathbb{Z}_p[\zeta] \to \mathbb{Z}/p^n\mathbb{Z}$ se anula sobre $\lambda^j\mathbb{Z}_p[\zeta]$, donde $j = i + n(p-1)p^{n-1}$, puesto que $p\mathbb{Z}_p[\zeta] = \lambda^{(p-1)p^{n-1}}\mathbb{Z}_p[\zeta]$.

Vamos a aplicar e ilustrar este método log-lineal sobre el caso de la primera suplementaria bicuadrática. Ahora tenemos $(a,\lambda) = i^{g(\log\, a)}$, $a \in U_3$, donde $g\colon \lambda^3\mathbb{Z}_2[i] \to \mathbb{Z}/4\mathbb{Z}$. Pongamos $\log\, a = \lambda^3(m + ni) \in \lambda^3\mathbb{Z}_2[i]$. Por linealidad $g(\log\, a) = g(\lambda^3(m+ni)) = xm + yn$, y determinemos x e y de los cálculos en la base. En (2.1.2) ya se obtuvieron $(\eta_3,\lambda) = 1$ y $(\eta_4,\lambda) = i^{-1}$. Para usar la nota 2.1 ahora se tiene

$$\log\,\eta_3 \equiv -\lambda^3 - \lambda^6/2 \ (\text{mód}\ \lambda^8) \quad \text{y} \quad \log\,\eta_4 \equiv -\lambda^4 - \lambda^8/2 \ (\text{mód}\ \lambda^{12})$$

(usar **E)** de (1.5.2)). Así se tiene (uso también de la proposición 1.16(b) y de (2.1))

$$0 = g(\log\,\eta_3) = g(-\lambda^3 - \lambda^6/2) = g(\lambda^3(0+i)) = y$$
$$-1 = g(\log\,\eta_4) = g(-\lambda^4 - \lambda^8/2) = g(\lambda^3(1-i)) = x - y.$$

Por lo tanto $x = -1$ e $y = 0$, y así la aplicación lineal g ha sido calculada

$$g(\log\, a) = g(\lambda^3(m+ni)) = -m. \tag{2.5}$$

Nótese que log jugó aquí un papel auxiliar para tener una aplicación lineal $g\colon \lambda^3\mathbb{Z}_2[i] \to \mathbb{Z}/4\mathbb{Z}$ y así calcular esta última. Pero ahora, aproximando log, se tiene

$$g(\log a) = g(a - 1 - (a-1)^2/2),$$

por la nota 2.1 y por **E)** de (1.5.2), de nuevo. Así, puesto que, para $a = 1 + \lambda^3(m' + n'i)$, se tiene que $a - 1 - (a-1)^2/2 = \lambda^3(m' + m'^2 - n'^2 - 2m'n' + (n' + m'^2 - n'^2 + 2m'n')i)$, de (2.5) se obtiene otra vez la fórmula de (2.1.2)

$$(a, \lambda) = i^{g(\log a)} = i^{m' + (m'+n')^2}.$$

Si ahora se quiere encontrar una fórmula log, nótese que ya se obtuvo $(a, \lambda) = i^{-m}$, $\log a = \lambda^3(m + ni)$, $a \in U_3$ en (2.5). Puesto que $m = S((\log a)/\lambda^3)/2 = S(\lambda^{-1}i \log a)/4$ (S denota la traza ("Spur") de una extensión de cuerpos), se tiene

Proposición 2.1. *Sea $k = \mathbb{Q}_2(i)$. Para $a \in U_1$ se tiene*

(a) $(a, \lambda) = i^{-S(\lambda^{-1}i \log a)/4)}$

(b) $(a, i) = i^{-S(\log a)/4}$

Demostración. Las fórmulas para U_1 se reducen fácilmente a las ya obtenidas para U_3, y así (a).

(b) Con el mismo procedimiento que para (a) (método log-lineal) se llega ahora a $(a, i) = i^{m-n}$, $a \in U_3$. Puesto que $m = S(m + ni)/2$ y $n = s(-i(m + ni))/2$, se tiene

$$m - n = S((1 + i)(m + ni))/2 = S((-\lambda^3/2)(m + ni))/2 = -S(\log a)/4. \quad \square$$

Nota 2.2. Se han reencontrado (como era de esperar) las fórmulas suplementarias del caso $p = n = 2$ de [2]. Nótese que en [2] la segunda suplementaria general se *ha encontrado* con facilidad y directamente, partiendo del contenido de la proposición 1.15, teniendo en cuenta que

$$\log N(a) = S(\log a)$$

(es lo que subyace en el hecho de que las fórmulas explícitas generales para (a, b), multiplicativo, deben tener exponentes aditivos, en términos de traza de logaritmos). No ocurre lo mismo con la primera suplementaria, que en [2] involucró cálculos masivos y muy complicados.

Reunamos ahora todas las fórmulas explícitas ya obtenidas

Teorema 2.1 (Ley de reciprocidad bicuadrática completa en términos de coordenadas aditivas)**.** *Sea $k = \mathbb{Q}_2(i)$. Entonces, para $a = x + yi = 1 + \lambda^3(m + ni)$ y $b = x' + y'i = 1 + \lambda^3(m' + n'i) \in U_3$ se tiene*

(a) $(a, b) = (-1)^{(Na-1)/4 \cdot (Nb-1)/4} = (-1)^{(m+n)(m'+n')} = (-1)^{(x-1)/2 \cdot (x'-1)/2}$
$= (-1)^{y/2 \cdot y'/2} = (-1)^{(a-1)/\lambda^3 \cdot (b-1)/\lambda^3}$.

(b) $(a, \lambda) = i^{m+(m+n)^2} = i^{(y^2 - x - y + 1)/4}$.

(c) $(a, i) = i^{(Na-1)/4} = i^{m-n} = i^{(1-x)/2}$.

Además

$$(a, 2) = i^{m+n} = i^{-y/2}$$

es el carácter bicuadrático de 2 en $\mathbb{Q}(i)$, *y*

$$(a,-1)=(-1)^{m+n}=(-1)^{(1-x)/2}=(-1)^{y/2}=(-1)^{(Na^2-1)/8}=(Na,2)_2. \ \square$$

Nota 2.3. 1. En el teorema 2.1 hemos reencontrado las fórmulas bicuadráticas tal como pueden verse en las referencias bien conocidas [25], Chap. 9, §9 y Exercises, [5] y [29], Theorem 6.9. Fueron Gauss (1828) y Jacobi (1837-1938) los primeros en establecer la ley de reciprocidad bicuadrática completa. Eisenstein en los 1840's dio por primera vez demostraciones geométricas de leyes de reciprocidad. Usó la aritmética de las curvas elípticas (en lugar de métodos ciclotómicos y las funciones circulares para la ley de reciprocidad cuadrática) para probar los casos bicuadrático y cúbico[2].

En cuanto a la vía de la teoría de cuerpos de clases, la que seguimos aquí, Bohnicek [6] obtiene la ley de reciprocidad bicuadrática completa, partiendo de la fórmula producto para el símbolo de Hilbert, en términos de coordenadas multiplicativas, que luego transcribe a aditivas (ver también la nota 2.6.4). [19] (pp. 105-106) usa la fórmula producto y el método de las 'bases' para verificar en los generadores la fórmula (a) del teorema 2.1. Esta fórmula fue derivada por aproximación de una fórmula log general en [23], Corollary 3, p. 86. Ver también [5], Notes to Chap. 8 y [29], Notes to Chap. 6. (Ver la nota 2.6.2).

2. Del teorema 2.1 se sigue que, si $a\in 1+4\mathbb{Z}$ y $b\in 1+2\lambda\mathbb{Z}[i]$ son coprimos, entonces $(a/b)=(b/a)$ (Eisenstein). Además si $a\in\dot{\mathbb{Z}}$ y $b\in 1+2\mathbb{Z}$ son coprimos, entonces $(a/b)=1$.

2.2. Ley de reciprocidad óctica

2.2.1. Sea $k=\mathbb{Q}_2(\zeta)$, con $\zeta=\frac{\sqrt{2}}{2}(1+i)$, raiz primitiva óctica de la unidad. Se tiene $\mathbb{Q}(\zeta)=\mathbb{Q}(i,\sqrt{2})$, $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(\zeta)\cap\mathbb{R}=\mathbb{Q}(\zeta+\zeta^{-1})$ y $\mathcal{U}(\mathbb{Q}(\sqrt{2}))=\{\pm1\}\times <1+\sqrt{2}>$, donde $1+\sqrt{2}$ es la unidad fundamental de $\mathbb{Q}(\sqrt{2})$ (ecuación de Pell, $N_{\mathbb{Q}(\sqrt{2})|\mathbb{Q}}(1+\sqrt{2})=-1$). El teorema de las unidades ([27], Chap. V, §1) da que el rango de $\mathcal{U}(\mathbb{Q}(\zeta))$ es 1, y así $\mathcal{U}(\mathbb{Q}(\zeta))=<\zeta>\times<\epsilon>$. Usando [35], Proposition 7.6.3 y Exercise 7.6.4, se sigue que $1+\sqrt{2}$ también es una unidad fundamental de $\mathbb{Q}(\zeta)$, y así

$$\mathcal{U}(\mathbb{Q}(\zeta))=<\zeta>\times<1+\sqrt{2}>.$$

[2] De hecho existe un paralelismo entre

(a) el uso de funciones circulares para probar la ley de reciprocidad cuadrática, junto con que el teorema de Kronecker-Weber involucra a la función exponencial compleja, y que Kronecker-Weber cuadrático da una prueba de la ley de reciprocidad cuadrática por comparación de leyes de factorización de primos de $\mathbb{Q}$, y

(b) el uso de cierta función elíptica, el *seno lemniscato* (prolongación meromorfa del seno lemniscato real, inversa de $\int_0^x dt/\sqrt{1-t^4}$, involucrada en la longitud de arco de la *lemniscata* $\rho^2=\cos 2\theta$), para probar la ley de reciprocidad bicuadrática, junto con que Kronecker-Jugendtraum para $\mathbb{Q}(i)$ involucra a esa función elíptica, y que Kronecker-Jugendtraum bicuadrático da una prueba de la ley de reciprocidad bicuadrática por comparación de leyes de factorización de primos de $\mathbb{Q}(i)$. Ver [29], Chap. 8.

Por otro lado se tiene

$$2\mathbb{Z}_2[\zeta] = \lambda^4\mathbb{Z}_2[\zeta] \quad \text{y} \quad (1+i)\mathbb{Z}_2[\zeta] = \sqrt{2}\mathbb{Z}_2[\zeta] = \lambda^2\mathbb{Z}_2[\zeta]\,.$$

Por lo tanto $1+\sqrt{2} \in U_2 - U_3$. También $(1+\sqrt{2})^2 = 1+2(1+\sqrt{2}) \in U_4 - U_5$, y así $< 1+\sqrt{2} > \cap U_5 =< (1+\sqrt{2})^4 >$. Se sigue que $(\mathcal{U}(k) :< 1+\sqrt{2} > \cdot U_5) = 4$, y así $< 1+\sqrt{2} > \cdot U_5$ no es libre, y

$$\mathcal{U}(k) =< \zeta > \cdot < 1+\sqrt{2} > \cdot U_5 = \mathcal{U}(\mathbb{Q}(\zeta)) \cdot U_5 \tag{2.6}$$
$$\mathbb{Z}[\zeta] - \lambda\mathbb{Z}[\zeta] =< \zeta > \cdot < 1+\sqrt{2} > \cdot (1+\lambda^5\mathbb{Z}[\zeta])$$

(así los números de U_5 son llamados *semiprimarios* de $\mathbb{Q}(\zeta)$).

Por lo tanto el dominio de definición de la ley de reciprocidad óctica es U_5, de forma que, para tener una ley de reciprocidad óctica completa se deberían tener fórmulas para los símbolos de Hilbert no moderados siguientes

$$(a,b),\ (a,\lambda),\ (a,\zeta),\ \text{y}\ (a,1+\sqrt{2}),\ a,b \in U_5.$$

Comparado esto con lo expuesto en (1.4.1) se ve que está involucrado un símbolo más, $(a,1+\sqrt{2})$, debido a que ahora U_5 no es una componente libre de $\mathcal{U}(k)$ (lema 1.1).

Denotando

$$\mathcal{H} :=< 1+\sqrt{2} > \cdot U_5$$

y puesto que $< \zeta > \cap\, \mathcal{H} =< -1 >$, respecto al retículo de subgrupos de $\mathcal{U}(k)/U_5$ se tiene

$$\begin{array}{ccc} U_1 = \mathcal{U}(k) & = & < \zeta > \cdot \mathcal{H} \\ | & & | \\ < i > \cdot \mathcal{H} & = & U_2 \\ | & & | \\ \mathcal{H} & & U_3 \\ & \diagdown & | \\ & & U_4 =< -1 > \cdot U_5 \\ & & | \\ & & U_5 \end{array}$$

Sea $U_2/U_4 = \left\{ bU_4 = b + 2\mathbb{Z}_2[\zeta]\,,\ b = 1, 1+\lambda^2, 1+\lambda^3, 1+\lambda^2+\lambda^3 \right\} (\cong (\mathbb{Z}/2\mathbb{Z})^2)$ $\subset \mathcal{U}(k)/U_4 = \mathcal{U}(\mathbb{Z}_2[\zeta]\,/(2))$. Es fácil ver, para el subgrupo $\mathcal{H}/U_4$ de U_2/U_4, que

$$\mathcal{H}/U_4 =< (1+\sqrt{2})U_4 = (1+i\sqrt{2})U_4 = (1+\lambda^2+\lambda^3)U_4 > \tag{2.7}$$

(En particular, se tiene [29], Exercise 9.4).

Teorema 2.2 (Ley de reciprocidad óctica de Eisenstein: restricción parcial del caso principal a $\mathbb{Z}_2[i]$)**.** *Sean $a,b \in U_5$ tales que $a \in \mathbb{Q}_2(i)$ (ie, $a \in U_{\mathbb{Q}_2(i),3}$). Entonces*

$$(a,b) = (-1)^{(Na-1)/8\cdot(Nb-1)/8}.$$

En particular, si $a \in U_{\mathbb{Q}_2(i),4}$, entonces $(a,b) = 1$.

Nota 2.4. 1. Se tiene que *k es lineal en b* (rel. 6) *y también $\mathbb{Q}_2(i)$ es lineal en b* (rel. 3) *para todo $b \in U_5$* (se sigue del lema 1.2 y de la proposición 1.17, teniendo en cuenta que $U_{\mathbb{Q}_2(i),3} = \mathbb{Q}_2(i) \cap U_6$ y $U_{\mathbb{Q}_2(i),6} = \mathbb{Q}_2(i) \cap U_{12}$). A diferencia del caso bicuadrático, la falta de simetría en la anterior linealidad va a impedir calcular una fórmula por bilinealidad. Aún así, con la restricción

impuesta en la clásica ley de reciprocidad óctica de Eisenstein, el método lineal llevará indirectamente a encontrar aquélla.

2. Ante todo nótese que la linealidad no permite *encontrar* directamente una fórmula para (a,b), $a \in U_{\mathbb{Q}_2(i),3} = \mathbb{Q}_2(i) \cap U_6$, $b \in U_5$, puesto que el recíproco del enunciado sobre linealidad de la nota 1 no es verdadero, ie, k *no* es lineal en $U_{\mathbb{Q}_2(i),3}$ (rel 5). *Aunque sí* (rel 6). Así vamos a usar el método lineal para encontrar fórmulas para (a,η_j), $a \in U_{\mathbb{Q}_2(i),3}$, $j = 5, 6, 7$ y 8, sobre los generadores de U_5 mód U_5^8. Entonces la fórmula del teorema 2.2 se seguirá inmediatamente.

2.2.2. *Cálculos: la norma de k y la suplementaria segunda.* Se tiene $\sqrt{2} = \zeta + \bar{\zeta} = \zeta - \zeta^3 = (1-i)\zeta$, $2 = (1-i)^2 i$, $i\sqrt{2} = \zeta + \zeta^3$ y $(1+i)\sqrt{2} = 2\zeta$.

Las que siguen son unidades a considerar en $\mathbb{Q}(\zeta)$ (además de las de $<\zeta>$)

$$\begin{array}{ll} 1+\sqrt{2} = 1+\zeta-\zeta^3 & (1+\sqrt{2})^{-1} = -1+\zeta-\zeta^3 \\ \zeta(1+\sqrt{2}) = 1+\zeta+\zeta^2 & (1+\sqrt{2})^2 = 3+2\zeta-2\zeta^3 \\ i(1+\sqrt{2}) = \zeta+\zeta^2+\zeta^3 & \zeta(1+\sqrt{2})^2 = 2+3\zeta+2\zeta^2 \end{array}$$

Respecto a las potencias λ^i, $i \geq 1$, se tiene

$$\begin{array}{l} \lambda^2 = 1-2\zeta+i = \cdots = (1-i)i(1-\sqrt{2}), \\ \lambda^3 = (1-i)(1-\zeta)(1-\sqrt{2}) = -(1-i)(1-\sqrt{2})^2 = (1-i)(-2+\zeta+\zeta^2-2\zeta^3) \\ \lambda^4 = -(1-i)^2(1-\sqrt{2})^2 = 2i(1-\sqrt{2})^2 \\ -\lambda^4(2\zeta+3\zeta^2+2\zeta^3) = 2 = N\lambda = \lambda(1+\zeta)(1+i) = (\lambda(1+\zeta)\zeta)^2 \\ 1+\zeta = \lambda i(1+\sqrt{2}) = \lambda\zeta(1+\zeta+\zeta^2). \end{array}$$

También

$$\begin{array}{l} \lambda^5 = -4-4\zeta+10\zeta^2-10\zeta^3 \\ \lambda^6 = -(1-i)^3 i(1-\sqrt{2})^3 = -2(1-i)(1-\sqrt{2})^3 \\ \lambda^8 = (1-i)^4(1-\sqrt{2})^4 = -4(1-\sqrt{2})^4. \end{array}$$

Puesto que la reducción de los cálculos del símbolo sobre los generadores lleva a cálculos particulares de $(a,\zeta) = \zeta^{(Na-1)/8}$, $a \in \mathcal{U}(k)$ (proposición 1.15), vamos a explicitar la expresión general de la norma $N\colon \dot{k} \to \dot{\mathbb{Q}}_2$.

Para $a \in \dot{k}$ vamos a considerar los siguientes sistemas de coordenadas aditivas:

$$\begin{array}{l} a = x_0 + x_1\zeta + x_2\zeta^2 + x_3\zeta^3 \\ \quad = 1 + 2(y_0 + y_1\zeta + y_2\zeta^2 + y_3\zeta^3) \text{ si } a \in U_4 \\ \quad = 1 + \lambda^5(n_0 + n_1\zeta + n_2\zeta^2 + n_3\zeta^3) \text{ si } a \in U_5 \text{ (ie, } y_0+y_1+y_2+y_3 \equiv 0 \text{ (mód 2))} \\ \quad = 1 + 4(z_0 + z_1\zeta + z_2\zeta^2 + z_3\zeta^3) \text{ si } a \in U_8 \end{array}$$

También las coordenadas 'cuadráticas' (x,y,z,t) de las normas relativas N_1 y N_2 para los subcuerpos $\mathbb{Q}_2(i)$ y $\mathbb{Q}_2(\sqrt{-2})$ de k

$$N_1 a := x + yi, \quad N_2 a := z + t\sqrt{-2}.$$

Así

$$\begin{array}{l} x = x_0^2 + 2x_1x_3 - x_2^2 = 4y_0^2 + 8y_1y_3 - 4y_2^2 + 4y_0 + 1 =: 1 + 4A \\ y = -x_1^2 + 2x_0x_2 + x_3^2 = 8y_0y_2 - 4y_1^2 + 4y_3^2 + 4y_2 =: 4B \\ z = x_0^2 - x_1^2 + x_2^2 - x_3^2 = 4y_0^1 - 4y_1^2 + 4y_2^2 - 4y_3^2 + 4y_0 + 1 \end{array} \tag{2.8}$$

$$\begin{aligned} t &= x_0x_1 + x_0x_3 - x_1x_2 + x_2x_3 \\ &= 4y_0y_1 + 4y_0y_3 - 4y_1y_2 + 4y_2y_3 + 2y_1 + 2y_3 \end{aligned}$$

Entonces $A = (x_0^2 + 2x_1x_3 - x_2^2 - 1)/4$ y $B = (-x_1^2 + 2x_0x_2 + x_3^2)/4$

$$Na = x^2 + y^2 = z^2 + 2t^2 = 16(A^2 + B^2) + 8A + 1 \tag{2.9}$$

Si $a \in U_4 = 1 + 2\mathbb{Z}_2[\zeta]$, entonces $N_1 a \in U_{\mathbb{Q}_2(i),4}$, y A y B son enteros, y así

$$(Na - 1)/8 = 2(A^2 + B^2) + A \equiv A \equiv y_2 \text{ (mód 2)}. \tag{2.10}$$

Ahora es fácil obtener una fórmula para la suplementaria segunda (a, ζ), $a \in U_4$, en términos de las coordenadas absolutas de a, pero su expresión es complicada (ver (2.2.4)). Sin embargo los dos casos que siguen son más simples. Por la proposición 1.15 se tiene

$$(a, a) = (a, -a) = (-1)^{(Na-1)/8} = (-1)^{y_2},\ a \in U_4. \tag{2.11}$$

Además, para $a \in U_8$, (2.9) da

$$(Na - 1)/8 \equiv 6z_0 + 4z_2 = (3/2)(x_0 - 1) + x_2 \text{ (mód 8)}. \tag{2.12}$$

Por lo tanto la proposición 1.15 da

$$(a, \zeta) = i^{3z_0+2z_2} = i^{3(x_0-1)/4+x_2/2},\ a \in U_8.$$

Vamos a usar todo esto para calcular la matriz (η_i, η_j) sobre la "base" de $U_5 =< \eta_5, \eta_6, \eta_7, \eta_8 >$ mód U_5^8 (ver (1.3)). Puesto que el símbolo (a, b) es anti-conmutativo (proposición 1.9(a)) estamos reducidos a $i \leq j$. Para $\eta_5 = 1 - \lambda^5 = 5 + 4\zeta - 10\zeta^2 + 10\zeta^3$ se tiene que $A = 1$. Por lo tanto de (2.11) se sigue que $(\eta_5, \eta_5) = -1$. Análogamente $(\eta_6, \eta_6) = (\eta_7, \eta_7) = -1$ y $(\eta_8, \eta_8) = 1$.

Por otro lado, aplicando **C)** de (1.5.2), se obtiene

$$\begin{aligned} &(\eta_5, \eta_6) = (\eta_{16}, \lambda)^5, \quad (\eta_5, \eta_7) = (\eta_{12}, \lambda) \\ &(\eta_5, \eta_8) = (\eta_6, \eta_7) = (\eta_6, \eta_8) = (\eta_7, \eta_8) = 1. \end{aligned}$$

Ahora, por la reducción **D)** de (1.5.2) y por la proposición 1.16(b) se obtiene

$$(\eta_{10}, \zeta) = (\eta_{11}, \zeta)(\eta_{11}, \lambda)^{-1} = (\eta_{11}, \zeta) = (\eta_{12}, \zeta)(\eta_{12}, \lambda)^{-1}.$$

Análogamente $(\eta_{12}, \zeta) = (\eta_{16}, \zeta)(\eta_{16}, \lambda)^{-1}$. Por lo tanto todo está reducido a $(\eta_{10}, \zeta), (\eta_{12}, \zeta), (\eta_{14}, \zeta)$ y (η_{16}, ζ). Para estos símbolos calculemos $(\eta_j - 1)/4 = -\lambda^j/4$

$$\begin{aligned} &-\lambda^8/4 = (1 - \sqrt{2})^4 = 17 - 12\zeta + 12\zeta^3 \equiv 1 + 4\zeta + 4\zeta^3 \text{ (mód 8)} \\ &-\lambda^{10}/4 \equiv (1 + 4\zeta + 4\zeta^3)\lambda^2 \equiv 1 + 6\zeta + \zeta^2 \equiv \lambda^2 \text{ (mód 8)} \\ &-\lambda^{12}/4 \equiv \lambda^2\lambda^2 \equiv 4\zeta + 6\zeta^2 + 4\zeta^3 \text{ (mód 8)} \\ &-\lambda^{14}/4 \equiv 2 + 6\zeta^2 + 4\zeta^3 \text{ (mód 8)} \\ &-\lambda^{16}/4 \equiv 4 \text{ (mód 8)} \end{aligned}$$

Por lo tanto (2.12) da $(\eta_{10}, \zeta) = i,\ (\eta_{12}, \zeta) = 1,\ (\eta_{14}, \zeta) = -1$ y $(\eta_{16}, \zeta) = 1$, y así $(\eta_{12}, \lambda) = \zeta^6$ y $(\eta_{16}, \lambda) = -1$. En conclusión, hemos obtenido la matriz

$$(\eta_i, \eta_j) = \begin{pmatrix} -1 & -1 & -i & 1 \\ -1 & -1 & 1 & 1 \\ i & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix},\ i, j = 5, 6, 7, 8. \tag{2.13}$$

2.2.3. *Demostración del* teorema 2.2. Denotemos N_0 la norma de $\mathbb{Q}_2(i)$. La segunda afirmación se sigue de la primera y de que $(Na-1)/8 \equiv (N_0a^2-1)/4 \equiv 0$ (mód 2), la última congruencia por (2.3).

Se va a usar ahora el *método lineal* (**F**) de (1.5.2)) para encontrar fórmulas para (a,η_j), $a \in U_6 = <\eta_5^2,\eta_6,\eta_7,\eta_8>$ mód U_5^8 (ver (1.4) y la nota 1.5), para $j = 5,6,7,8$. Póngase $a = 1+\lambda^6(m_0+m_1\zeta+m_2\zeta^2+m_3\zeta^3) \in U_6$, y así, por linealidad, se tiene que $(a,\eta_5) = \zeta^{xm_0+ym_1+zm_2+tm_3}$. Puesto que $\eta_5^2 = 1+\lambda^6(-1-5\zeta+5\zeta^2-5\zeta^3)$, $\eta_6 = 1+\lambda^6(-1)$, $\eta_7 = 1+\lambda^6(-1+\zeta)$, $\eta_8 = 1+\lambda^6(-1+2\zeta-\zeta^2)$, la matriz (2.13) da $x=4$, $y=t=6$ y $z=0$. Por lo tanto

$$(a,\eta_5) = \zeta^{4m_0+6m_1+6m_3},\ a \in U_6.$$

Análogamente

$$(a,\eta_6) = (-1)^{m_0+m_1+m_2+m_3},\ (a,\eta_7) = (-1)^{m_1} \text{ y } (a,\eta_8) = 1,\ a \in U_6.$$

Vamos ahora a reformular para (a,η_j), $a \in U_{\mathbb{Q}_2(i),3}$, $j = 5,6,7,8$, las fórmulas que se acaban de encontrar. Pongamos $a = 1+(1-i)^3(m+ni) = 1+\lambda^6(7n-5(m-n)\zeta-7m\zeta^2-5(m+n)\zeta^3)$. Así

$$(a,\eta_j) = \begin{cases} (-1)^{(m+n)\cdot 1} & j = 5,6,7 \\ (-1)^{(m+n)\cdot 0} & j = 8. \end{cases} \tag{2.14}$$

Pero en términos del propio $a \in U_{\mathbb{Q}_2(i),3}$ y también de los propios η_j's, se tiene (uso de (2.2))

$$m+n \equiv (N_0a-1)/4 \equiv ((N_0a)^2-1)/8 = (Na-1)/8 \text{ (mód 2)}.$$

Por otro lado, para $b \in \mathcal{U}(k)$ se tiene $(Nb-1)/8 \equiv ((Nb)^2-1)/16$ (mód 4), y puesto que $\eta_j^2 \in U_8$, $j = 5,6,7,8$, aplicación de (2.12) da $(N\eta_j-1)/8 \equiv 1$ (mód 2), $j = 5,6,7$ y $(N\eta_8-1)/8 \equiv 0$ (mód 2). Por lo tanto hemos encontrado las fórmulas

$$(a,\eta_j) = (-1)^{(Na-1)/8\cdot(N\eta_j-1)/8},\ a \in U_{\mathbb{Q}_2(i),3},\ j = 5,6,7,8.$$

Estas fórmulas se extienden a todo $b \in U_5$ por bimultiplicatividad (ver la nota 1.6.2), encontrando pues la fórmula del teorema 2.2. □

Nota 2.5. 1. Una vía alternativa para encontrar la fórmula del teorema 2.2 es como sigue. Puesto que $U_5 =< \eta_5 > \cdot U_6$, basta encontrar fórmulas para (a,η_5) (ya encontrada) y para (a,b), $a \in U_{\mathbb{Q}_2(i),3}$, $b \in U_6$. Para esta última se puede usar bilinealidad (ver la nota 2.4.2), y así sean

$$a = 1+(1-i)^3(m+ni) \in U_{\mathbb{Q}_2(i),3} =< \beta_3 = 1-(1-i)^3,\ \beta_4 = 5 > \text{ (mód } U^4_{\mathbb{Q}_2(i),3})$$

$$b = 1+\lambda^6(m_0+m_1\zeta+m_2\zeta^2+m_3\zeta^3) \in U_6 =< \eta_5^2,\eta_6,\eta_7,\eta_8 > \text{ (mód } U_5^8).$$

Las fórmulas (2.14) da ahora la matriz

$$(\beta_i,\gamma_j) = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix},\ \gamma_j := \eta_5^2,\eta_6,\eta_7,\eta_8.$$

Por lo tanto, haciendo

$$(a,b) = \zeta^{mm_0x_0+mm_1x_1+mm_2x_2+mm_3x_3+nm_0y_0+nm_1y_1+nm_2y_2+nm_3y_3},$$

y teniendo en cuenta los parámetros de los γ_j (calculados al comienzo de esta

subsección), la matriz anterior da $x_0 = x_2 = y_0 = y_2 = 4$, $x_1 = x_3 = y_1 = y_3 = 0$. En consecuencia

$$(a, b) = \zeta^{4(mm_0+mm_2+nm_0+nm_2)} = (-1)^{(m+n)(m_0+m_2)}.$$

Ya sabemos que $m + n \equiv (Na - 1)/8$ (mód 2), $a \in U_{\mathbb{Q}_2(i),3}$ (ver más arriba). Además por (2.10) $m_0 + m_2 \equiv (Nb - 1)/8$ (mód 2), $b \in U_6$. Hemos encontrado pues la fórmula del teorema 2.2 para $a \in U_{\mathbb{Q}_2(i),3}$ y $b \in U_6$. Puesto que la fórmula vale también para (a, η_5), por multiplicatividad también valdrá para todo $a \in U_{\mathbb{Q}_2(i),3}$ y $b \in U_5$.

2. El método lineal, usado en nota 1 (que da además una fórmula en términos de parámetros), llevaría a una fórmula (bilineal) para (a, b), $a, b \in U_6$, en términos de parámetros (que no vamos a ultimar). (Nótese que en este último caso no vale la fórmula del teorema 2.2; falla, eg, para (η_5^2, η_7), incluso falla para $U_7 \times U_6$).

2.2.4. *Fórmulas suplementarias.*

• Si ahora se ultima lo propuesto ya en (2.2.2) para la suplementaria segunda se obtendrá

$$(a, \zeta) = \zeta^{y_0+y_0^2+2(y_1^2+y_3^2)+3y_2^2+6y_1y_3+4y_2(y_1+y_3)}, \tag{2.15}$$

para $a = 1 + 2(y_0 + y_1\zeta + y_2\zeta^2 + y_3\zeta^3) \in U_4 = 1 + 2\mathbb{Z}_2[\zeta]$.

• En cuando a la suplementaria primera, tal como se había procedido ya en el caso bicuadrático, vamos a hacer uso del *método log-lineal* (2.1.3). Para su aplicación son necesarios todavía algunos cálculos adicionales del símbolo sobre los generadores, los de (η_6, λ) y (η_8, λ). Aplicación sistemática de la reducción **D)** de (1.5.2) lleva a $(\eta_8, \lambda) = \zeta^2(\eta_6, \zeta)^{-1}$ y $(\eta_6, \lambda) = (\eta_6, \zeta)(\eta_4, \zeta)^{-1}$. Aplicando ahora (2.15) se obtiene $(\eta_4, \zeta) = (\eta_6, \zeta) = \zeta^3$, y así

$$(\eta_8, \lambda) = \zeta^{-1} \text{ y } (\eta_6, \lambda) = 1. \tag{2.16}$$

• Sea ahora $(a, \lambda) = \zeta^{g(\log a)}$, $a \in U_5 =< \eta_5, \eta_6, \eta_7, \eta_8 >$ mód U_5^8, donde $g\colon \lambda^5\mathbb{Z}_2[\zeta] \to \mathbb{Z}/8\mathbb{Z}$, como en el caso general de (2.1.3). Pongamos $\log a = \lambda^5(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^3) \in \lambda^5\mathbb{Z}_2[\zeta]$. Por linealidad $g(\log a) = g(\lambda^5(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^3)) = xm_0 + ym_1 + zm_2 + tm_3$, y determínense x, y, z, t de los cálculos sobre los generadores.

• Para aplicar el método log-lineal sobre este caso óctico se necesitan aproximaciones de los $\log \eta_k$ mód $\lambda^j\mathbb{Z}_2[\zeta]$, $j \geq 17$ (ver la nota 2.1). Así ponemos (usando **E)** de (1.5.2))

$$\begin{aligned}
\log \eta_5 &\equiv -\lambda^5 - \lambda^{10}/2 - \lambda^{15}/3 - \lambda^{20}/4 \text{ (mód } \lambda^{25}) \\
\log \eta_6 &\equiv -\lambda^6 - \lambda^{12}/2 - \lambda^{24}/4 \text{ (mód } \lambda^{18}) \\
\log \eta_7 &\equiv -\lambda^7 - \lambda^{14}/2 \text{ (mód } \lambda^{20}) \\
\log \eta_8 &\equiv -\lambda^8 - \lambda^{16}/2 \text{ (mód } \lambda^{24})
\end{aligned}$$

Por lo tanto (uso también de la proposición 1.16(b) y de (2.16))

$$\begin{aligned}
0 = g(\log \eta_5) &= g(-\lambda^5 - \lambda^{10}/2 - \lambda^{15}/3 - \lambda^{20}/4) = {}^3g(\lambda^5(3 - 3\zeta^2 + 3\zeta^3)) \\
&= 3x - 3z + 3t
\end{aligned}$$

[3] Si $g\colon A \to B$ es un homomorfismo de grupos abelianos únicamente divisibles por $n > 0$, entonces $g(a/n) = g(a)/n$.

$$\begin{aligned}
0 &= g(\log \eta_6) = g(-\lambda^6 - \lambda^{12}/2 - \lambda^{24}4) = g(\lambda^5(4 - 2\zeta - 3\zeta^2 - 3\zeta^3)) \\
&= 4x - 2y - 3z - 3t \\
0 &= g(\log \eta_7) = g(-\lambda^7 - \lambda^{14}/2) = g(\lambda^5(1 - \zeta^2)) = x - z \\
-1 &= g(\log \eta_8) = g(-\lambda^8 - \lambda^{16}2) = g(\lambda^5(1 - 3\zeta + 3\zeta^2 - \zeta^3)) = x - 3y + 3z - t
\end{aligned}$$

Esto da $x = z = -2$, $y = 3$ y $t = 0$. Así la aplicación lineal g ha sido calculada

$$g(\log a) = -2(m_0 + m_2) + 3m_1. \tag{2.17}$$

• Ahora, para encontrar una fórmula para (a, λ) en términos de los parámetros de $a = 1 + \lambda^5(n_0 + n_1\zeta + n_2\zeta^2 + n_3\zeta^3)$ debemos aproximar $\log a$. Puesto que $a - 1 \in \lambda^5\mathbb{Z}_2[\zeta]$ se tiene (por **E)** de (1.5.2), de nuevo)

$$\log a \equiv (a-1) - (a-1)^2/2 + (a-1)^3/3 - (a-1)^4/4 \text{ (mód } \lambda^{25}),$$

y así $g(\log a) = g(a - 1 - (a-1)^2/2 + (a-1)^3/3 - (a-1)^4/4)$, de nuevo por la nota 2.1. Un tedioso cálculo[4] lleva a

• $a-1-(a-1)^2/2+(a-1)^3/3-(a-1)^4/4 = \lambda^5(\underline{m}_0+\underline{m}_1\zeta+\underline{m}_2\zeta^2+\underline{m}_3\zeta^3)$ donde

$$\begin{aligned}
\underline{m}_0 &= -n_1^2 - 3n_3^2 - 2n_0n_1 + 2(-n_0n_2 + 2n_0n_3 + 2n_1n_2 + n_2n_3) + 5n_0 \\
\underline{m}_1 &= -3n_1^2 - n_3^2 + 2(2n_0n_1 + n_0n_2 + n_0n_3 + n_1n_2 + 2n_2n_3) - 3n_1 + 4(n_2 + n_3) \\
\underline{m}_2 &= n_0^2 + 3n_2^2 + 2(2n_0n_1 - n_0n_3 - n_1n_2 - n_1n_3 + 2n_2n_3) + 4(n_0 + n_1) - 3n_2 \\
\underline{m}_3 &= -n_0^2 - 3n_2^2 + 2(-n_0n_1 + 2n_0n_3 + 2n_1n_2 + n_1n_3 + n_2n_3) + 4n_1 + n_3
\end{aligned} \tag{2.18}$$

Finalmente de (2.17) se obtiene

$$\begin{aligned}
(a, \lambda) &= \zeta^{g(\log a)} \\
&= \zeta^{2(n_0+n_2+n_0^2+n_2^2)-n_1+n_1^2-n_3^2+2(n_0n_2+n_0n_3+n_1n_2+2n_1n_3)}.
\end{aligned} \tag{2.19}$$

El procedimiento para la suplementaria primera que se acaba de describir podría ser aplicado también a la suplementaria $(a, 1+\sqrt{2})$, $a \in U_5$, si se tuvieran los cálculos en los generadores. No es fácil calcular los $(\eta_j, 1 + \sqrt{2})$ mediante las propiedades axiomáticas del símbolo. Sin embargo, puesto que $1 + \sqrt{2} = (1 + \zeta)/i\lambda$ (ver al comienzo de (2.2.2)), para obtener esa suplementaria basta obtener la fórmula para $(a, 1 + \zeta)$, $a \in U_5$. Pero esto último no es otra cosa que la primera suplementaria (a, λ), $a \in U_5$, si se elige $-\zeta = \zeta^5$ como la raíz octava primitiva de la unidad. Así, por (2.17), se tiene

$$(a, 1 + \zeta) = (-\zeta)^{-2(m_0' + m_2') + 3m_1'}, \ a \in U_5,$$

si $\log a = (1 + \zeta)^5(m_0' - m_1'\zeta + m_2'\zeta^2 - m_3'\zeta^3)$. Puesto que $\lambda^5/(1 + \zeta)^5 = i(1 - \sqrt{2})^5 \equiv 3\zeta + \zeta^2 + 3\zeta^3$ (mód 8) se tiene

$$m_0' - m_1'\zeta + m_2'\zeta^2 - m_3'\zeta^3 \equiv (3\zeta + \zeta^2 + 3\zeta^3)(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^3) \text{ (mód 8)}.$$

Por lo tanto hemos encontrado

$$(a, 1 + \zeta) = \zeta^{m_0 - m_2 + 3m_3}, \ a \in U_5 \tag{2.20}$$

[4]Programa de cálculo simbólico

(donde ahora $\log a = \lambda^5(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^3)$). Como en el caso previo, las fórmulas (2.18), junto con (2.20) da

$$(a, 1+\zeta) = \zeta^{3n_1^2+n_3^2+2(2n_0n_1-n_0n_2+n_0n_3+n_1n_2+2n_2n_3)-3n_0+4n_1-n_2-n_3} \tag{2.21}$$

Una fórmula en términos de los (n_i) para (a, ζ) puede ser obtenida de (2.15), o bien de forma paralela a las anteriores (uso del método log-lineal). Se obtiene entonces

$$(a, \zeta) = \zeta^{n_0^2+3n_1^2+3n_2^2+n_3^2+2(-n_0n_2+2n_0n_3+2n_1n_2-n_1n_3)-2n_0-3n_1+3n_2+2n_3} \tag{2.22}$$

Todo esto, junto con (2.19), da

$$(a, 1+\sqrt{2}) = \zeta^{2(2n_0n_1-n_0n_2+2n_2n_3)+3(n_0+n_1+n_2+n_3)} \tag{2.23}$$

Si ahora se quiere usar (2.17) para encontrar una fórmula log para (a, λ), puesto que $m_0 = S(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^3)/4$, $m_1 = S(-\zeta^2(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^)))/4$, $m_2 = S(-\zeta^2(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^))/4$ y $m_3 = S(-\zeta(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^))/4$, se tiene

$$2(m_0 + m_2) - 3m_1 = S((2 - 2\zeta^2 + 2\zeta^3)(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^))/4.$$

Relacionemos $2 - 2\zeta^2 + 3\zeta^3$ con λ^5. Puesto que $\lambda^4 = 2(-2\zeta + 3\zeta^2 - 2\zeta^3)$ se tiene $\lambda^4\zeta = 2(2 - 2\zeta^2 + 3\zeta^3)$. Por lo tanto se ha encontrado la fórmula

$$(a, \lambda) = \zeta^{-S(\lambda^{-1}\zeta \log a)/8}, \ a \in U_5. \tag{2.24}$$

Agrupando ahora todo lo anterior se tiene

Teorema 2.3 (Ley de reciprocidad óctica suplementaria)**.** *Sea* $a = 1 + \lambda^5(n_0 + n_1\zeta + n_2\zeta^2 + n_3\zeta^3) = 1 + 2(y_0 + y_1\zeta + y_2\zeta^2 + y_3\zeta^3) = x_0 + x_1\zeta + x_2xi^2 + x_3\zeta^3 \in U_5$. *Denotamos* $(a, b) =: \zeta^{[a,b]}$.

(a) $[a, \lambda] = 2(n_0 + n_2 + n_0^2 + n_2^2) - n_1 + n_1^2 - n_3^2 + 2(n_0n_2 + n_0n_3 + n_1n_2 + 2n_1n_3)$
$= \frac{1}{8}(-19x_0^2 + 57x_1^2 + 7x_2^2 + 59x_3^2 - 29) + \frac{1}{4}(-27x_0x_1 + x_0x_2 + 25x_0x_3$
$+13x_1x_2 + 11x_1x_3 + 11x_2x_3) + 2(-x_0 + x_1) + 3(x_2 + x_3)$
$= \frac{1}{2}(-3y_0^2 - 7y_1^2 + 7y_2^2 - 5y_3^2 + 5y_0 - 3y_1 - 3y_2 + 5y_3) + 5y_0y_1 + y_0y_2$
$-7y_0y_3 - 3y_1y_2 + 3y_1y_3 + 3y_2y_3$
$= -S(\lambda^{-1}\zeta \log a)/8$

(b) $[a, 1+\zeta] = 3n_1^2 + n_3^2 + 2(2n_0n_1 - n_0n_2 + n_0n_3 + n_1n_2 + 2n_2n_3) - 3n_0$
$+4n_1 - n_2 - n_3$
$= 5S((1+\zeta)^{-1}\zeta \log a)/8.$

(c) $[a, \zeta] = n_0^2 + 3n_1^2 + 3n_2^2 + n_3^2 + 2(-n_0n_2 + 2n_0n_3 + 2n_1n_2 - n_1n_3) - 2n_0$
$-3n_1 + 3n_2 + 2n_3$
$= y_0 + y_0^2 + 2(y_1^2 + y_3^2) + 3y_2^2 + 6y_1y_3 + 4y_2(y_1 + y_3)$
$= 5S(\log a)/8,$

la segunda igualdad válida para $a \in U_4$.

(d) $\left[a, 1+\sqrt{2}\right] = 2(2n_0n_1 - n_0n_2 + 2n_2n_3) + 3(n_0 + n_1 + n_2 + n_3)$
$= S((\lambda^{-1} + 5(1+\zeta)^{-1})\zeta \log a - 2\log a)/8.$

(e) *Todas las fórmulas* log *anteriores valen para todo* $a \in U_1$ $(= \mathcal{U}(k))$.

Demostración. (a) Se sigue de (2.19) y (2.24). (b) Se sigue de (2.21), y luego de (2.24), ésta ahora para el uniformizante $1 + \zeta$.

(c) La primera igualdad es (2.22) y la segunda es (2.15). (Ver también la nota 2.2).

(d) La primera igualdad es (2.23). La segunda se sigue de (a), (b) y (c) teniendo en cuenta que $1+\sqrt{2} = (1+\zeta)/i\lambda$.

(e) Nótese que $U_1 =< \zeta, \eta_3 > \cdot U_5$, lo que se sigue del corolario 1.3. Como en el caso bicuadrático (proposición 2.1), la fórmula para $< \zeta > \times U_5$ se reduce fácilmente a la de U_5. Por lo tanto sólo resta comprobar sobre η_3 la fórmula para U_5. Como $(\eta_3, \lambda) = 1$ (proposición 1.17) se debe probar $S(\lambda^{-1}\zeta \log \eta_3)/8 \equiv 0$ (mód 8). Como una aproximación suficiente basta probar que la primera coordenada de $\lambda^{-1}\zeta(\lambda^3 + \lambda^6/2 + \lambda^9/3 + \lambda^{12}/4 + \lambda^{24}/8)$ es divisible por 16, lo que es una rutina. □

Corolario 2.1 (Ley de reciprocidad óctica: formulación global)**.** (a) *Sean* $a \in 1 + 2(1-i)\mathbb{Z}[i]$ *y* $b \in 1 + 2\lambda\mathbb{Z}[\zeta]$ *coprimos. Entonces*

$$(b/a)(a/b)^{-1} = (a,b)_\lambda = (-1)^{(Na-1)/8 \cdot (Nb-1)/8}$$

(b) *Si* $a \in 1 + 4\mathbb{Z}[i]$ *y* $b \in 1 + 2\lambda\mathbb{Z}[\zeta]$*, o bien si* $a \in 1 + 4\mathbb{Z}$ *y* $b \in \mathbb{Z}[\zeta] \cap \mathcal{H}$*, ie,* $b \equiv 1,\ 1 + \zeta + \zeta^3$ (mód 2) (ver (2.7))*, son coprimos, entonces*

$$(a/b) = (b/a).$$

(c) (Restricción a $\mathbb{Z}$ de las fórmulas suplementarias). *Si* $a \in 1 + 4\mathbb{Z}$*, entonces*

$(\lambda/a) = (a,\lambda)_\lambda = \zeta^{(a^2-1)/8}(-1)^{(a-1)/4} = \zeta^{5(a^2-1)/8}$
$(1+\zeta/a) = (a, 1+\zeta)_\lambda = \zeta^{(a^2-1)/8}$
$(\zeta/a) = (a,\zeta)_\lambda = (1+\zeta/a)^2 = i^{(a^2-1)/8}$
$(1+\sqrt{2}/a) = (a, 1+\sqrt{2})_\lambda = 1$
$(2/a) = (a,2)_\lambda = 1.$

Demostración. El corolario 1.2 y la nota 1.3 reducen este corolario al caso local. Así (a) y (b) se siguen del teorema 2.2. Para el segundo caso de (b) usar el primer caso de (b) junto con los casos $(a,-1)_\lambda$ y $(a, 1+\sqrt{2})_\lambda$ de (c). Así se tiene $(a, 1+\sqrt{2})_\lambda = (a, U_4)_\lambda = 1$, de donde $(a,\mathcal{H})_\lambda = 1$. Usar ahora (2.7).

(c) Las fórmulas para (λ/a), $(1+\zeta/a)$, (ζ/a) y $(1+\sqrt{2}/a)$ se siguen del teorema 2.3 (aunque para (ζ/a) se puede obtener directamente de $(a,\zeta)_\lambda = \zeta^{(Na-1)/8}$ y de que $Na = a^4$). Para $(2/a)$ se sigue de la proposición 2.2, más adelante, teniendo en cuenta que aquí $a^4 = Na = x^2 + y^2$, y así en aquélla fórmula se tiene $y = 0$, y además $Na \equiv 1$ (mód 16) (o también se sigue directamente de las fórmulas anteriores)[5]. □

Nota 2.6. *Comparación con las otras fórmulas ócticas.* 1. Han sido dadas varias demostraciones de la ley de reciprocidad óctica, unas en términos de coordenadas aditivas (Eisenstein 1850, Western 1907-1908, éstos para la restricción a $\mathbb{Z}$ de la principal, [15], [7], y [23], §5, este último para la principal) y otras en términos log ([2], para las suplementarias, y [31] y [23], completa). Unas con demostraciones clásicas (Eisenstein 1850, [15]) y otras apoyadas en teoría de

[5] Apuntemos que estas fórmulas se pueden derivar directamente de las fórmulas (2.17) y (2.20) ya que en el caso $a \in 1 + 4\mathbb{Z}$ la aproximación de $\log a$ es más sencilla. (Así también directamente de la fórmula log).

cuerpos de clases vía la fórmula producto ([7], [2], para las suplementarias, [31] y [23]). Las demostraciones que hemos dado aquí están en ésta última línea, y son para términos de coordenadas aditivas.

Por nuestro procedimiento hemos reencontrado de forma alternativa las fórmulas clásicas. Para la fórmula principal (teorema 2.2) ver [29], Theorem 9.18. Las fórmulas (b) y (c) del corolario 2.1 son las clásicas de la restricción a $\mathbb{Z}$ de la ley de reciprocidad óctica de Eisenstein (1850). Ver [29], Porposition 9.4 y Notes de Chap. 9, [5], Notes on Chap. 14, y notas 2.10.1 y 3. Ver también la nota 2.7.2.

El corolario 2.1, segundo caso de (b), es equivalente a la ley de reciprocidad de Western (1908), caso $p^n = 8$, versión de [5], Theorem 14.3.1(b), ie, $(a, b)_\lambda = (b, (-1)^{(a-1)/2})_\lambda$ si $a \in 1 + 2\mathbb{Z}$ y b es "primario" de $\mathbb{Q}(\zeta)$, teniendo en cuenta la caracterización de los "primarios" ócticos dada en [5], Theorem 14.2.1. Así la ley de reciprocidad de Western, caso óctico, resulta equivalente a la óctica de Eisenstein principal restringida a $\mathbb{Z}$, más la suplementaria $(a, 1 + \sqrt{2})$. Ver también la nota 2.10.3.

2. Para la aplicación de las fórmulas de reciprocidad a problemas diofánticos (eg, residuos potenciales racionales) es necesario que aquéllas estén en términos de coordenadas aditivas. Esto también podría obtenerse por aproximación de las fórmulas log de las leyes de reciprocidad explícitas de [31] y [2], lo que se hace para la bicuadrática y óctica principales en [23], §5, y para $(a, 2)_{2^r}$ en [20] y [13] (ver la nota 2.7.3).

En este sentido nótese que, siendo reversible el argumento para pasar de (2.17) a (2.24), de las fórmulas log de [2] se derivarían fácilmente las fórmulas en términos de los parámetros m_i de $\log a$. Luego por aproximación se obtendría el teorema 2.3 (paso de (2.17) a (2.19)). Pero esto sería dar un rodeo vía esas fórmulas log, de obtención ardua. Nuestro procedimiento es más directo, y con un método general, unificado y elemental, aplicado, no obstante, caso a caso, permite *encontrar* (no sólo verificar) las fórmulas en coordenadas aditivas (lo que es la base para las aplicaciones). Así las demostraciones resultan notablemente acortadas (las fórmulas de [2] necesitan cálculos masivos, muy complicados). Así lo nuestro es una alternativa a las célebres fórmulas de referencia de [2], siendo éstas las adecuadas para una expresión analítica para toda potencia, y que marcaron una línea de fórmulas, la de Artin-Hasse.

Lo mismo podría decirse de la fórmula principal del teorema 2.2 respecto a [31] y [23]. En este último se deriva la reciprocidad óctica de Eisenstein (teorema 2.2, aquí) aproximando la 2^n-reciprocidad explícita principal de [31] (un caso más de uso de teoría de cuerpos de clases en reciprocidades particulares). Obtiene así una fórmula en el dominio multiplicativo, que finalmente transcribe al aditivo. Nuestro método permite trabajar sólo en el lado aditivo, y además las fórmulas se obtienen directamente, y no vía las fórmulas analíticas.

3. Las fórmulas de Goldscheider [15] para la ley de reciprocidad óctica, por métodos clásicos, ciclotómicos, tienen la ventaja frente a otras de estar dadas en términos de coordenadas 'cuadráticas', más próximas a sus aplicaciones diofánticas. Nuestras fórmulas son fácilmente intercambiables con las de Goldscheider, aún siendo obtenidas en ambos casos por métodos totalmente distintos. Ver la

nota 2.7.2.

4. Hemos mencionado en la nota 1 la ley de reciprocidad óctica de [7], la primera en ser obtenida vía la fórmula producto de la teoría de cuerpos de clases, que Bohnicek prueba en los casos que estudia, bicuadrático [6] y óctico. Luego obtiene fórmulas para el símbolo de Hilbert (a,b) en términos de coordenadas multiplicativas. A continuación transcribe las coordenadas multiplicativas a las aditivas A, B de (2.8) y $s := (x_0+x_1+x_2+x_3-1)/4$. Así es fácil intercambiar las fórmulas de [7] con las nuestras de los teoremas 2.2 y 2.3. Nuestro procedimiento resulta así una vía diferente. Aquí, al trabajar en el marco de los métodos locales de Hensel-Hasse (existencia de logaritmo y de raíces), en lugar de necesitar un complicado cambio a la base aditiva del cuerpo desde la multiplicativa de sus unidades (lo que es "ad hoc", como hace Bohnicek, con ingeniosos trucos en cada caso), nuestras fórmulas son obtenidas directamente en el lado aditivo. Además damos un método unificado para todos los casos a los que se aplique, en los cuales permite reducir a potencia de cálculo.

2.2.5. *Carácter óctico de* 2. Teniendo en cuenta que $2 = (\lambda\zeta(1+\zeta))^2$ (ver (2.2.2)), del teorema 2.3 se obtiene

$$(a,2) =: \zeta^{[a,2]} = \zeta^{2(-n_0^2-n_1^2+n_2^2+n_3^2+2n_0n_2+2n_1n_3+n_0+n_3)}.$$

Vamos a reformular esto en coordenadas 'cuadráticas' $N_1a =: x+yi \in \mathbb{Q}_2(i)$ y $N_2a =: z+t\sqrt{-2} \in \mathbb{Q}_2(\sqrt{-2})$. Así de (2.8) se sigue

$$\begin{aligned}
x &= -4n_0^2+4n_1^2+4n_2^2-4n_3^2-8n_0n_2-8n_1n_3-8n_0+20n_1-20n_2+8n_3+1\\
y &= 4n_0^2+4n_1^2-4n_2^2-4n_3^2-8n_0n_2+8n_1n_3+20n_0-8n_1-8n_2+20n_3\\
z &= 8n_0n_1+8n_0n_3-8n_1n_2+8n_2n_3-8n_0+20n_1-20n_2+8n_3+1 \qquad (2.25)\\
t &= -4n_0^2+4n_1^2-4n_2^2+4n_3^2-14n_0+6n_1+6n_2-14n_3\\
&\equiv 4(n_0+n_1+n_2+n_3)+2(n_0-n_1-n_2+n_3) \text{ (mód 8)}
\end{aligned}$$

Se ve que $[a,2] \equiv -\frac{y}{2}+4(n_0+n_1+n_2+n_3)$ (mód 8). Pero $t^2 \equiv 4(n_0+n_1+n_2+n_3) \equiv y+x-1 \equiv y+(Na-1)/2$ (mód 8) (ver (2.10)). Se ha obtenido

Proposición 2.2 (Carácter óctico de 2)**.** *Sea $a \in U_5$. Con la notación anterior se tiene*

$$\begin{aligned}
(a,2) &= \zeta^{2(-n_0^2-n_1^2+n_2^2+n_3^2+2n_0n_2+2n_1n_3+n_0+n_3)}\\
&= \zeta^{x_0^2+x_0x_2-\frac{5}{2}x_1^2-2x_1x_2-2x_1x_3-3x_2^2-2x_2x_3-\frac{3}{2}x_3^2+2x_0+2x_1+2x_2-2x_3-3}\\
&= \zeta^{-y/2+t^2} = \zeta^{y/2+x-1} = \zeta^{\frac{y+Na-1}{2}} = \begin{cases}\zeta^{y/2} & \text{si } Na \equiv 1 \text{ (mód 16)}\\ \zeta^{y/2+4} & \text{si } Na \equiv 9 \text{ (mód 16)}\end{cases} \quad \square
\end{aligned}$$

Corolario 2.2 (Carácter óctico racional de 2)**.** *Sea $p = x^2+y^2 \equiv 1$ (mód 8), $y \equiv 0$ (mód 2), un número primo.*

(a) $2^{(p-1)/8} = \zeta^{y/2+(p-1)/8}$ *en* $\mu_8 \subset (\mathbb{Z}/\dot{p}\mathbb{Z})$ (ver la proposición 1.2 para la inclusión).

(b) $2 \in (\mathbb{Z}/\dot{p}\mathbb{Z})^8$ *si y solo si p está representado por formas cuadráticas binarias como sigue*

$p = x^2 + 256y^2 \equiv 1 \pmod{16}$ *o*
$p = x^2 + 64y^2 \equiv 9 \pmod{16}$ *y no está representado por* $x^2 + 256y^2$.

Demostración. (a) Puesto que $\mathbb{Q}(\zeta)$ tiene número de clase 1 existe un número primo w de $\mathbb{Q}(\zeta)$ tal que $Nw = p$. Puesto que $\mathcal{U}(k) = U_1 = \mathcal{U}(\mathbb{Q}(\zeta)) \cdot U_5$ (ver (2.6)) se puede suponer que $w \in U_5$ (y así se puede aplicar la proposición 2.2). Sea $N_1 w = x + yi$. Puesto que $p \equiv 1 \pmod 8$, la ley de factorización ciclotómica da $f(w|p) = 1$, ie, $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[\zeta]/w\mathbb{Z}[\zeta]$. Así

$$2^{(p-1)/8} \pmod{\text{p}} = 2^{(p-1)/8} \pmod{w} = (2/w) = (w, 2)$$

(es en esta última igualdad donde se usa la teoría de cuerpos de clases global vía el corolario 1.2(b)). Ahora basta aplicar la proposición 2.2.

(b) De (a), $2 \in (\mathbb{Z}/p\mathbb{Z})^{\cdot 8}$ si y solo si

$$\begin{cases} y/2 \equiv 0 \pmod 8 & \text{si } p \equiv 1 \pmod{16} \\ y/2 + 4 \equiv 0 \pmod 8, \text{ ie, } 2^3 || y, & \text{si } p \equiv 9 \pmod{16}. \end{cases}$$ □

Nota 2.7. 1. El corolario 2.2 podría considerarse como la suplementaria de la ley de reciprocidad óctica racional de [36] (en las reciprocidades racionales sólo suele considerarse la fórmula principal).

2. Las tres últimas fórmulas de la proposición 2.2, así como el corolario 2.2, coinciden con los correspondientes resultados clásicos de [20], §12, [13], (11), y [5], Corollary 7.5.8 (ver la nota 4). Las fórmulas coinciden también con las que se derivarían de las fórmulas suplementarias ócticas de Goldsheider [15] (ver [29], Theorem 9.19). Así aquí hemos dado una demostración alternativa (vía el teorema 2.3) a la fórmula para $(a, 2)$, y usando métodos generales. Lo mismo podría hacerse, usando también (2.25) de forma atinada, con las citadas fórmulas suplementarias de Goldsheider, que tendrían así una demostración alternativa. Recíprocamente, de las fórmulas suplementarias (y de la principal) de Goldsheider se siguen las nuestras sin más que sustituir los parámetros, x, y, z, t de las primeras.

3. Hemos elegido el carácter óctico de 2 solo como una muestra de una línea de aplicaciones diofánticas racionales de las leyes de reciprocidad particulares, que arranca desde la reciprocidad óctica de Eisenstein 1850. Usamos las fórmulas encontradas en términos de coordenadas aditivas como *la base para derivar otras fórmulas* en coordenadas "cuadráticas", más cercanas a aquellas aplicaciones.

4. El carácter óctico de 2 fue establecido en Western 1911 (ver [20] y [13]). En este sentido cabe mencionar a Beeger [4], que deduce el 16-carácter de 2 de las fórmulas de Goldsheider. Por otra parte [1] y [20] deducen el carácter 16, y los caracteres 2, 4, 8 y 16, respectivamente, de 2. Además [20] trata el 32-carácter de 2, pero sin ultimar totalmente debido a que las dificultades computacionales crecen de forma considerable[6]. En ambos casos, para 16 y 32 potencias, se procede utilizando las fórmulas obtenidas por teoría de cuerpos de clases (las nuestras son en esa línea). [20] hace también un estudio extenso del símbolo $(a, 2)_{2^n}$, que trata de representar en términos de coordenadas de subcuerpos de $\mathbb{Q}(\zeta_{2^n})$. Luego aproxima los logaritmos involucrados. Puesto que trata de abarcar casos superiores la complicación es enorme, incluso cuando particulariza

[6] Ver en §2.3 el incremento de la complicación de cálculos y de fórmulas para 16-potencias.

al caso $n = 3$. (Lo paralelo en el caso óctico sería la proposición 2.2, donde, al ser tratado un caso particular, el proceso resultó relativamente sencillo desde el teorema 2.3).

Demostraciones elementales (sin teoría de cuerpos de clases) del carácter 2^n-potencial de 2 hasta el caso óctico eran ya conocidas. Finalmente en [13] se obtivieron, en particular, los casos 16 y 32 de Aigner y Hasse, resolviendo primero una conjetura previa sobre el caso 2^n. Luego se dio una demostración elemental, y también otra usando teoría de cuerpos de clases vía [2]. Como en [20], en [13] se aproximan las fórmulas log de [2] para obtener $(a, 2)_{2^n}$ en términos de coordenadas (w_i) de un primo $w|p \equiv 1 \pmod{2^n}$, ahora adecuadas para el caso general $n \geq 1$. Como acabamos de apuntar (nota 3), lo que exponemos en esta subsección es sólo una muestra de todo esto. Nuestro objetivo son las fórmulas (n_i) del teorema 2.3, como base.

2.3. Ley de reciprocidad para 16-potencias (bióctica)

2.3.1. Sea $k = \mathbb{Q}_2(\zeta)$, donde $< \zeta >= \mu_{16}$, ie, $\zeta = \left[\frac{1}{2}(\sqrt{2+\sqrt{2}} + i\sqrt{2-\sqrt{2}})\right]^k$, $2 \nmid k$. Se tiene $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2+\sqrt{2}})$ y $\mathcal{U}(k) =< \zeta > \times(< \eta_3, \eta_5, \eta_7 >\cdot U_9)$, y U_9 es un $\mathbb{Z}_2$-módulo libre de rango 8 (proposición 1.4). Se tiene

$$2\mathbb{Z}_2[\zeta] = \lambda^8\mathbb{Z}_2[\zeta]\,,\ (1-i)\mathbb{Z}_2[\zeta] = \lambda^4\mathbb{Z}_2[\zeta] \text{ y } \sqrt{2+\sqrt{2}}\mathbb{Z}_2[\zeta] = \lambda^2\mathbb{Z}_2[\zeta]\,.^7$$

Se sigue que $U_{\mathbb{Q}_2(i),3} = \mathbb{Q}_2(i) \cap U_9 = \mathbb{Q}_2(i) \cap U_{12}$ y $U_{\mathbb{Q}_2(i),4} = \mathbb{Q}_2(i) \cap U_{13} = \mathbb{Q}_2(i) \cap U_{16}$. De esto, del lema 1.2 y de la proposición 1.17 se sigue que

$$k \textit{ es lineal en } b \text{ (rel. 16) y } \mathbb{Q}_2(i) \textit{ es lineal en } b \text{ (rel. 4)}, \forall b \in U_9.$$

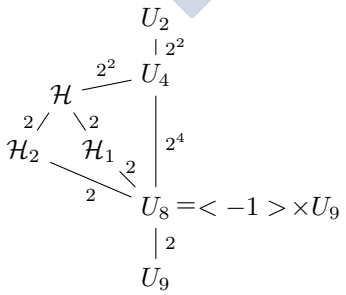
Nota 2.8. Consideremos las siguientes unidades de $\mathbb{Q}(\zeta)$

$$1 + \sqrt{2} = 1 + \zeta^2 - \zeta^6 \in U_4 - U_5$$
$$1 + \sqrt{2+\sqrt{2}} = 1 + \zeta - \zeta^7 \in U_2 - U_3$$
$$(1+\zeta)/\zeta^2\lambda = 1 + \sqrt{2+\sqrt{2}} + \zeta^2(1 + \zeta + \zeta^2 + \zeta^3) \in U_2 - U_3.$$

Así, denotando

$$\mathcal{H}_1 :=< 1 + \sqrt{2} >\cdot U_9, \quad \mathcal{H}_2 :=< 1 + \sqrt{2+\sqrt{2}} >\cdot U_9 \quad \text{y} \quad \mathcal{H} := \mathcal{H}_1\mathcal{H}_2$$

se tiene $\mathcal{H}_1 \neq \mathcal{H}_2$, y por lo tanto en el retículo de U_2/U_9 se tiene



[7] $N_{\mathbb{Q}(\sqrt{2+\sqrt{2}})|\mathbb{Q}}(\sqrt{2+\sqrt{2}}) = N_{\mathbb{Q}(\sqrt{2})|\mathbb{Q}}(2+\sqrt{2}) = 2$.

donde los índices son los indicados en el diagrama. En efecto, $\mathcal{H}_1/U_9$ y $\mathcal{H}_2/U_9$ son isomorfos a $\mathbb{Z}/4\mathbb{Z}$, y $\mathcal{H}_1 \supset U_8$ (ver diagrama de (2.2.1)), de donde también $\mathcal{H}_2 \supset U_8$, y $\mathcal{H}/U_9 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Se sigue que

$$\mathcal{H}/U_8 = \left\{ bU_8 = b + 2\mathbb{Z}_2[\zeta]\,;\ b = 1, 1+\zeta+\zeta^7, 1+\zeta^2+\zeta^6, 1+\zeta^3+\zeta^6 \right\} \quad (2.26)$$

(isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$). Este subgrupo $\mathcal{H}$ va a intervenir en la versión que vamos a dar (en la proposición 2.3(b), ver también la nota 2.10.3) de la ley de reciprocidad bióctica principal restringida a $\mathbb{Z}$.

Teorema 2.4 (Ley de reciprocidad para 16-potencias: restricción parcial del caso principal a $\mathbb{Z}_2[i]$)**.** (a) *Sean $a \in U_{\mathbb{Q}_2(i),3}$ y $b \in U_{10}$. Entonces*

$$(a,b) = (-1)^{(Na-1)/16\cdot(Nb-1)/16}$$

(b) *Sean ahora $a \in U_{\mathbb{Q}_2(i),4}$ y $b \in U_9$. Entonces*

$$(a,b) = (-1)^{(Na-1)/16\cdot(Nb-1)/16} = 1.$$

La demostración de este teorema necesita ante todo (paralelamente al caso óctico (2.2.2)) varias etapas de cálculo.

• Para $a \in \dot{k}$ denotemos

$$\begin{aligned} a &= x_0 + x_1\zeta + x_2\zeta^2 + x_3\zeta^3 + x_4\zeta^4 + x_5\zeta^5 + x_6\zeta^6 + x_7\zeta^7 \\ &= 1 + 2(y_0 + y_1\zeta + y_2\zeta^2 + y_3\zeta^3 + y_4\zeta^4 + y_5\zeta^5 + y_6\zeta^6 + y_7\zeta^7) \\ &= 1 + \lambda^9(n_0 + n_1\zeta + n_2\zeta^2 + n_3\zeta^3 + n_4\zeta^4 + n_5\zeta^5 + n_6\zeta^6 + n_7\zeta^7) \\ &= 1 + 4(z_0 + z_1\zeta + z_2\zeta^2 + z_3\zeta^3 + z_4\zeta^4 + z_5\zeta^5 + z_6\zeta^6 + z_7\zeta^7) \end{aligned}$$

En cuanto a la norma absoluta $N\colon \dot{k} \to \dot{\mathbb{Q}}_2$ se tiene

$$\begin{aligned} Na &= N_{\mathbb{Q}_2(\zeta^2)|\mathbb{Q}_2}(1 + 2(y_0 + y_1\zeta + y_2\zeta^2 + y_3\zeta^3 + y_4\zeta^4 + y_5\zeta^5 + y_6\zeta^6 + y_7\zeta^7))\cdot \\ &\quad (1 + 2(y_0 - y_1\zeta + y_2\zeta^2 - y_3\zeta^3 + y_4\zeta^4 - y_5\zeta^5 + y_6\zeta^6 - y_7\zeta^7)) \\ &=: N_{\mathbb{Q}_2(\zeta^2)|\mathbb{Q}_2}(1 + 2(\underline{y_0} + \underline{y_1}\zeta^2 + \underline{y_2}\zeta^4 + \underline{y_3}\zeta^6)) \\ &= (\text{ver } (2.9))16(\underline{A}^2 + \underline{B}^2) + 8\underline{A} + 1 \end{aligned} \quad (2.27)$$

donde $\underline{A} = \underline{y_0}^2 + 2\underline{y_1}\,\underline{y_3} - \underline{y_2}^2 + \underline{y_0}$, $\underline{B} = 2\underline{y_0}\,\underline{y_2} - \underline{y_1}^2 + \underline{y_3}^2 + \underline{y_2}$, $\underline{y_0} = 2y_0^2 + 4y_1y_7 - 4y_2y_6 + 4y_3y_5 - 2y_4^2 + 2y_0$, $\underline{y_1} = 4y_0y_2 - 2y_1^2 + 4y_3y_7 - 4y_4y_6 + 2y_5^2 + 2y_2$, $\underline{y_2} = \ldots$.

• Así, para $a \in U_8$, usando la proposición 1.15, de (2.27) y reduciendo a módulo 16, se obtiene la siguiente expresión para la segunda suplementaria

$$(a,\zeta) = \zeta^{(Na-1)/16} =: \zeta^{[a,\zeta]}, \text{ donde}$$

$$\begin{aligned} [a,\zeta] &= 2(3y_0^4 + y_2^4 + 3y_4^4 + y_6^4) + 8(y_0y_1y_6 + y_0y_2y_3 + y_0y_2y_4 + y_0y_2y_7 + y_0y_4y_6 \\ &\quad + y_0y_5y_6 + y_1y_2y_3 + y_1y_2y_4 + y_1y_2y_5 + y_1y_3y_4 + y_1y_3y_6 + y_1y_4y_7 \\ &\quad + y_2y_4y_5 + y_2y_4y_6 + y_2y_5y_7 + y_3y_4y_5 + y_3y_4y_6 + y_3y_6y_7 + y_4y_5y_7 \\ &\quad + y_4y_6y_7 + y_5y_6y_7) + 4(-y_0^2y_4^2 - y_1^2y_3^2 + y_1^2y_7^2 + y_2^2y_6^2 + y_3^2y_5^2 - y_5^2y_7^2 \\ &\quad - y_0y_4^2 - y_1^2y_6 - y_2^2y_4 - y_2y_3^2 + y_2y_7^2 + y_4y_5^2 + y_5^2y_6) - 4y_0^3 + 7y_0^2 \\ &\quad + y_4^2 + 2y_1y_7 + 2y_2y_6 + 2y_3y_5 + y_0 \end{aligned} \quad (2.28)$$

En el caso $a \in U_{16}$ se tiene

$$(a,\zeta) = \zeta^{2z_0-4z_0^2+8(z_1z_7+z_2z_6+z_3z_5)+4z_4^2}. \tag{2.29}$$

• Para $a \in U_8$, usando de nuevo la proposición 1.15 y reduciendo a módulo 2, de (2.27) y de (2.10) se obtiene

$$(a,a) = (-1)^{(Na-1)/16} = (-1)^{y_4} \tag{2.30}$$

Con esta fórmula para los generadores de U_9 mód $U_9^8 (= U_{41})$ se obtiene la diagonal de la matriz (η_i,η_j)

$$(\eta_j,\eta_j) = \begin{cases} -1, & j = 9,\dots,15 \\ 1, & j = 16 \end{cases}$$

• Ahora se va a usar (2.29), así como de forma sistemática las reducciones de las proposiciones 1.16 y 1.17, para calcular lo que resta de la matriz (η_i,η_j). Se obtiene $(\eta_9,\eta_{10}) = (\eta_{28},\lambda)^{-1}$, $(\eta_9,\eta_{11}) = (\eta_{20},\lambda)^5$, $(\eta_9,\eta_{12}) = (\eta_{30},\lambda)^{-5}$, y así sucesivamente. Por lo tanto van a estar involucrados los símbolos

$$(\eta_j,\lambda),\ j = 20,22,24,26,28,30,32,34,36,38 \text{ y } 40.$$

Los (η_j,ζ) involucrados en el cálculo de los anteriores (η_j,λ) serían para $j = 18,20,22,24,26,28,30,32,34,36$ y 38. Para estos calculemos $(\eta_j-1)/4 = -\lambda^j/4$

$$-\lambda^{18}/4 \equiv 5 + 2\zeta + 5\zeta^2 + 8\zeta^3 + 4\zeta^4 - 4\zeta^6 + 8\zeta^7 \text{ (mód 16)}.$$

La fórmula (2.29) da $(\eta_{18},\zeta) = \zeta^6$. Procediendo análogamente para los restantes (η_j,ζ) se obtendría, en definitiva

$$\begin{array}{llll} (\eta_{20},\lambda) = -\zeta^4 & (\eta_{22},\lambda) = -1 & (\eta_{24},\lambda) = \zeta^6 & (\eta_{36},\lambda) = -1 \\ (\eta_{28},\lambda) = \zeta^4 & (\eta_{30},\lambda) = -1 & (\eta_{32},\lambda) = -\zeta^4 & (\eta_{34},\lambda) = 1 \\ (\eta_{36},\lambda) = 1 & (\eta_{38},\lambda) = 1 & (\eta_{40},\lambda) = -1. & \end{array}$$

Por lo tanto hemos calculado la matriz (usando que la misma es anticonmutativa, por la proposición 1.9(a))

$$(\eta_i,\eta_j) = \begin{pmatrix} 1 & -\zeta^4 & -\zeta^4 & -1 & 1 & -\zeta^4 & \zeta^6 & 1 \\ \zeta^4 & -1 & -\zeta^4 & -1 & 1 & -\zeta^4 & -1 & 1 \\ \zeta^4 & \zeta^4 & -1 & 1 & \zeta^2 & 1 & -1 & 1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -\zeta^6 & 1 & -1 & -1 & -\zeta^4 & 1 \\ \zeta^4 & \zeta^4 & 1 & 1 & -1 & -1 & 1 & 1 \\ -\zeta^2 & -1 & -1 & 1 & \zeta^4 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{2.31}$$

2.3.2. *Demostración del* teorema 2.4. (a) Se va a usar el método log-lineal (2.1.3) para encontrar fórmulas para (a,η_j), $a \in U_{12} =< \eta_9^2, \eta_{10}^2, \eta_{11}^2, \eta_{12}, \eta_{13}, \eta_{14}, \eta_{15}, \eta_{16} >$ mód U_9^{16} y $j = 9,\dots,16$.

• Sea $(a,\eta_9) = \zeta^{g(\log a)}$, $a \in U_{12}$, donde $g\colon \lambda^{12}\mathbb{Z}_2[\zeta] \to \mathbb{Z}/16\mathbb{Z}$, como en el caso general. Pongamos $\log a = \lambda^{12}(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^3 + m_4\zeta^4 + m_5\zeta^5 + m_6\zeta^6 + m_7\zeta^7) \in \lambda^{12}\mathbb{Z}_2[\zeta]$. Por linealidad $g(\log a) = x_0m_0 + x_1m_1 + x_2m_2 + x_3m_3 + x_4m_4 + x_5m_5 + x_6m_6 + x_7m_7$ y determinaremos $x_0, x_1, \dots, x_7$ de los cálculos en los generadores.

• Para aplicar el método log-lineal en este caso de 16-potencias se necesitan aproximaciones de los $\log \eta_k^2$, $k = 9, 10, 11$ y $\log \eta_k$, $k = 12, \ldots, 16$ mód $\lambda^j \mathbb{Z}_2[\zeta]$, $j \geq 44$ (ver la nota 2.1). Así ponemos (usando **E)** de (1.5.2))

$$\begin{aligned}
\log \eta_9^2 &= 2\log \eta_9 \equiv (-\lambda^{17} - \lambda^{26}/2 - \lambda^{35}/3 - \lambda^{44}/4) \cdot u \ (\text{mód } \lambda^{53}) \\
\log \eta_{10}^2 &= 2\log \eta_{10} \equiv (-\lambda^{18} - \lambda^{28}/2 - \lambda^{38}/3 - \lambda^{48}/4) \cdot u \ (\text{mód } \lambda^{58}) \\
\log \eta_{11}^2 &= 2\log \eta_{11} \equiv (-\lambda^{19} - \lambda^{30}/2 - \lambda^{41}/3 - \lambda^{52}/4) \cdot u \ (\text{mód } \lambda^{63}) \\
\log \eta_{12} &\equiv -\lambda^{12} - \lambda^{24}/2 - \lambda^{36}/3 - \lambda^{48}/4 \ (\text{mód } \lambda^{60}) \\
\log \eta_{13} &\equiv -\lambda^{13} - \lambda^{26}/2 - \lambda^{39}/3 - \lambda^{52}/4 \ (\text{mód } \lambda^{65}) \\
\log \eta_{14} &\equiv -\lambda^{14} - \lambda^{28}/2 - \lambda^{42}/3 - \lambda^{56}/4 \ (\text{mód } \lambda^{70}) \\
\log \eta_{15} &\equiv -\lambda^{15} - \lambda^{30}/2 \ (\text{mód } \lambda^{44}) \\
\log \eta_{16} &\equiv -\lambda^{16} - \lambda^{32}/2 \ (\text{mód } \lambda^{48}),
\end{aligned}$$

donde $u \equiv -4\zeta - 2\zeta^2 + 4\zeta^3 - 3\zeta^4 + 4\zeta^5 - 2\zeta^6 - 4\zeta^7$ (mód 16). Por lo tanto (uso de (2.31))

$$\begin{aligned}
0 = g(\log \eta_9^2) &= g((-\lambda^{17} - \lambda^{26}/2 - \lambda^{35}/3 - \lambda^{44}/4) \cdot u) \\
&= g(\lambda^{12}(9\zeta - 3\zeta^2 + 8\zeta^3 + 7\zeta^5 + 5\zeta^6 - 6\zeta^7)) \\
&\equiv -7x_1 - 3x_2 + 8x_3 + 7x_5 + 5x_6 - 6x_7 \ (\text{mód } 16)
\end{aligned}$$

Análogamente

$$\begin{aligned}
8 &\equiv -x_0 - 6x_1 - 3x_2 + 8x_3 + 5x_4 + 6x_5 - 7x_6 + 4x_7 \ (\text{mód } 16) \\
8 &\equiv -5x_0 + 7x_1 + 3x_2 + 7x_3 + 5x_4 + 3x_5 - 3x_6 + 7x_7 \ (\text{mód } 16) \\
8 &\equiv 2x_0 + 8x_1 + 8x_2 + 8x_3 - 3x_4 - 4x_5 + 2x_6 - 4x_7 \ (\text{mód } 16) \\
0 &\equiv --4x_0 - x_1 + 7x_2 - 7x_4 - 6x_5 - 5x_6 - 4x_7 \ (\text{mód } 16) \\
4 &\equiv x_0 + 2x_1 - x_2 \ (\text{mód } 16) \\
-6 &\equiv -7x_0 - x_1 + 7x_2 + x_3 + 8x_4 + 8x_6 \ (\text{mód } 16) \\
0 &\equiv x_0 - 4x_1 + 6x_2 - 4x_3 + x_4 \ (\text{mód } 16)
\end{aligned}$$

• Esto da $x_0 = x_4 = 8$, $x_2 = x_5 = x_6 = 2$, $x_3 = 6$, $x_7 = -2$, $x_1 = 0$. Así la aplicación lineal g ha sido calculada, y

$$(a, \eta_9) = \zeta^{2(4m_0 + 2m_2 + 3m_3 + 4m_4 + 2m_5 + 2m_6 - m_7)} \tag{2.32}$$

• Ahora, para encontrar una fórmula para (a, η_9) en términos de los parámetros de $a = 1 + \lambda^{12}(n_0 + n_1\zeta + n_2\zeta^2 + n_3\zeta^3 + n_4\zeta^4 + n_5\zeta^5 + n_6\zeta^6 + n_7\zeta^7)$ debemos aproximar $\log a$. Puesto que $a - 1 \in \lambda^{12}\mathbb{Z}_2[\zeta]$ (por **E)** de (1.5.2), de nuevo)

$$\log a \equiv a - 1 - (a-1)^2/2 + (a-1)^3/3 - (a-1)^4/4 \ (\text{mód } \lambda^{60}),$$

y así $g(\log a) = g(a - 1 - (a-1)^2/2 + (a-1)^3/3 - (a-1)^4/4)$, de nuevo por la nota 2.1. Un tedioso cálculo[8] lleva a

• $a - 1 - (a-1)^2/2 + (a-1)^3/3 - (a-1)^4/4 = \lambda^{12}(\underline{m}_0 + \underline{m}_1\zeta + \underline{m}_2\zeta^2 +$

[8]Programa de cálculo simbólico

$\underline{m}_3\zeta^3 + \underline{m}_4\zeta^4 + \underline{m}_5\zeta^5 + \underline{m}_6\zeta^6 + \underline{m}_7\zeta^7)$, donde

$$\begin{aligned}
\underline{m}_0 &= 3n_0^2 + 2n_1^2 - 5n_2^2 - 4n_3^2 + 5n_4^2 + 6n_5^2 - 3n_6^2 - 4n_7^2 + 8n_0n_1 - 4n_0n_2 \\
&\quad + 8n_0n_3 - 2n_0n_4 + 6n_1n_3 + 8n_1n_5 - 6n_1n_7 + 8n_2n_4 + 8n_2n_5 - 6n_2n_6 \\
&\quad + 8n_2n_7 - 6n_3n_5 - 4n_3n_7 + 8n_4n_4 - 4n_4n_6 + 8n_4n_7 + 8n_5n_6 - 6n_5n_7 \\
&\quad + 8n_6n_7 + n_0 + 8n_4 \\
\underline{m}_1 &= 4(n_1^2 + n_2^2 - n_5^2 - n_6^2) - 2n_0n_1 + 8n_0n_2 - 4n_0n_3 + 8n_0n_4 + 6n_0n_5 \\
&\quad + 4n_1n_2 - 2n_1n_4 + 8n_1n_6 - 2n_2n_3 + 2n_2n_7 + 8n_3n_5 + 2n_3n_6 - 6n_4n_5 \\
&\quad + 8n_4n_6 + 4n_4n_7 + 4n_5n_6 + 8n_5n_7 + 2n_6n_7 + 8n_0 + n_1 + 8n_3 + 8n_4 \\
&\cdots \\
\underline{m}_7 &= 4(-n_0^2 - n_1^2 + n_4^2 + n_5^2) + 2(2n_0n_1 + 4n_0n_2 - 3n_0n_3 - n_0n_7 + n_1n_2 \\
&\quad + 4n_1n_5 - n_1n_6 + 4n_1n_7 - n_2n_5 + 4n_2n_6 + 2n_2n_7 + 3n_3n_4 - 2n_3n_6 \\
&\quad + 4n_3n_7 - 2n_4n_5 + 4n_4n_6 - n_4n_7 - n_5n_6 + 4n_5n_7 + 4n_6n_7) + 8n_1 \\
&\quad + 8n_2 + 8n_3 + 8n_6 - 7n_7
\end{aligned}$$

Finalmente de (2.32) se obtiene

$$(a, \eta_9) = \zeta^{g(\log a)} = \zeta^{8(n_0n_7+n_1n_6+n_2n_5+n_3n_4)+2(4n_0+4n_1+2n_2+3n_3+4n_4-2n_5+2n_6-n_7)}$$

El mismo procedimiento permite encontrar fórmulas para $(a, \eta_{10}), \ldots, (a, \eta_{16})$, $a \in U_{12}$.

Vamos ahora a reformular todas esas expresiones restringiéndolas a $U_{\mathbb{Q}_2(i),3}$. Pongamos $a = 1 + (1-i)^3(m+ni) = 1 + \lambda^{12}(n_0 + n_1\zeta + n_2\zeta^2 + n_3\zeta^3 + n_4\zeta^4 + n_5\zeta^5 + n_6\zeta_6 + n_7\zeta^7)$. Se obtiene

$$(a, \eta_j) = \begin{cases} (-1)^{(m+n)\cdot 1} & \text{si } j = 10, \ldots, 15 \\ (-1)^{(m+n)\cdot 0} & \text{si } j = 9, 16 \end{cases} \tag{2.33}$$

Por otra parte, $(Na-1)/16 = (N_0a^4 - 1)/4 \equiv m + n \ (2)$ (la última congruencia es (2.2)). Usando (2.30) se obtiene

$$(-1)^{(N\eta_j - 1)/16} = \begin{cases} -1 & \text{si } j = 9, \ldots, 15 \\ 1 & \text{si } j = 16. \end{cases}$$

Por lo tanto se ha encontrado la fórmula buscada para $a \in U_{\mathbb{Q}_2(i),3}$ y $b = \eta_9^2$, $\eta_{10}, \ldots, \eta_{16}$, que se extiende por bimultiplicatividad a $U_{10} = <\eta_9^2, \eta_{10}, \ldots, \eta_{16}>$ mód U_9^{16}.

(b) Se va a usar ahora el *método lineal* (**F**) de (1.5.2)) para encontrar fórmulas para (a, η_j), $a \in U_{16} =< \eta_9^2, \eta_{10}^2, \eta_{11}^2, \eta_{12}^2, \eta_{13}^2, \eta_{14}^2, \eta_{15}^2, \eta_{16} >$ mód U_9^{16} (ver (1.4) y la nota 1.5), para $j = 9, 10, 11, 12, 13, 14, 15, 16$. Póngase $a = 1 + \lambda^{16}(m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^3 + m_4\zeta^4 + m_5\zeta^5 + m_6\zeta^6 + m_7\zeta^7) \in U_{16}$, y así por linealidad se sigue que

$$(a, \eta_9) = \zeta^{x_0m_0+x_1m_1+x_2m_2+x_3m_3+x_4m_4+x_5m_5+x_6m_6+x_7m_7}.$$

Puesto que

$$\begin{aligned}
\eta_9^2 &= 1 + \lambda^{16}(5 + 2\zeta - \zeta^2 - 6\zeta^3 + 7\zeta^4 - 7\zeta^5 + 6\zeta^6 + 2\zeta^7) \\
\eta_{10}^2 &= 1 + \lambda^{16}(7 - 4\zeta + 8\zeta^3 - 2\zeta^4 + 2\zeta^5 - 3\zeta^6 - 4\zeta^7)
\end{aligned}$$

$$\eta_{11}^2 = 1+\lambda^{16}(-5-4\zeta-7\zeta^2-2\zeta^3+8\zeta^5+3\zeta^5+4\zeta^6+5\zeta^7)$$
$$\eta_{12}^2 = 1+\lambda^{16}(1-4\zeta^2+5\zeta^4-4\zeta^5+2\zeta^6-4\zeta^7)$$
$$\eta_{13}^2 = 1+\lambda^{16}(-7+7\zeta+4\zeta^2-7\zeta^4-7\zeta^5+4\zeta^6+6\zeta^7)$$
$$\eta_{14}^2 = 1+\lambda^{16}(5+2\zeta+\zeta^2-3\zeta^4+6\zeta^5-7\zeta^6+4\zeta^7)$$
$$\eta_{15}^2 = 1+\lambda^{16}(5+3\zeta+\zeta^2-\zeta^3-3\zeta^4-5\zeta^5-7\zeta^6+7\zeta^7)$$
$$\eta_{16} = 1+\lambda^{16}(-1),$$

la matriz (2.31) da $x_0 = x_2 = x_4 = 0$, $x_1 = x_5 = x_6 = x_7 = 8$, $x_3 = -4$. Por lo tanto para $a \in U_{16}$, se obtiene

$$(a, \eta_9) = \zeta^{8m_1-4m_3+8m_5+8m_6+8m_7}.$$

Análogamente

$$(a,\eta_{10}) = \zeta^{8(m_2+m_3)} \qquad (a,\eta_{11}) = \zeta^{4(-m_1+m_3+2m_5+2m_6)}$$
$$(a,\eta_{12}) = 1 = (a,\eta_{16}) \qquad (a,\eta_{13}) = \zeta^{4(2m_2-m_3+2m_5-m_7)} \tag{2.34}$$
$$(a,\eta_{14}) = \zeta^{8(m_2+m_3+m_6+m_7)} \qquad (a,\eta_{15}) = \zeta^{4(-m_1+2m_2-m_3-m_5+2m_6-m_7)}$$

Reformulemos, para (a, η_j), $a \in U_{\mathbb{Q}_2(i),4}$, $j = 9, \ldots, 16$, las expresiones que se acaban de encontrar. Pongamos $a = 1+(1-i)^4(m+ni) = 1+\lambda^{16}(-7m+(8m+8n)\zeta+4(m+n)\zeta^2+8n\zeta^3-7n\zeta^4+8(m+n)\zeta^5+4(n-m)\zeta^6+8m\zeta^7)$. Así, usando (2.34), se obtiene $(a, \eta_j) = 1$ $\forall j$. Por lo tanto se ha encontrado $(a, b) = 1$, $\forall b \in U_9$. La segunda igualdad del teorema 2.4 se sigue de $\frac{Na-1}{16} \equiv \frac{N_0a-1}{4} \equiv 0$ (mód 2), la última congruencia por (2.2) y (2.3). □

Nota 2.9. 1. La fórmula del teorema 2.4(a) es falsa para $U_{\mathbb{Q}_2(i),3} \times U_9$, tal como se desprende de la demostración (a pesar de que $(U_{\mathbb{Q}_2(i),3}, U_9) = \pm 1$).

2. El teorema 2.4(b) se seguiría de forma inmediata de las fórmulas (2.33) (o bien de la fórmula (a), de $(Na-1)/16 \equiv (Na-1)/4 \equiv 0$ (mód 2) (por (2.3)) y de $(U_{\mathbb{Q}_2(i),3}, \eta_9) = 1$ (caso $j = 9$ de (2.33))). Sin embargo, hemos incluido una demostración directa ya que en ella pudo ser empleado el, más sencillo, método lineal.

2.3.3. *Fórmulas suplementarias.* Para la primera suplementaria se va a hacer también uso del *método log-lineal*. Para su aplicación se necesitan los cálculos adicionales (η_j, λ), $j = 10, 12, 14, 16$. La aplicación sistemática de la reducción **D)** de (1.5.2) involucra a los símbolos (η_j, ζ), $j = 8, 10, 12, 14$. El cálculo de estos últimos se deriva de la segunda suplementaria (2.28). En definitiva

$$(\eta_{10}, \lambda) = (\eta_{12}, \lambda) = (\eta_{14}, \lambda) = 1 \text{ y } (\eta_{16}, \lambda) = \zeta^{-1}. \tag{2.35}$$

• Sea ahora $(a, \lambda) = \zeta^{g(\log a)}$, $a \in U_9 =< \eta_9, \eta_{10}, \eta_{11}, \eta_{12}, \eta_{13}, \eta_{14}, \eta_{15}, \eta_{16} >$ mód U_9^{16}, donde $g\colon \lambda^9\mathbb{Z}_2[\zeta] \to \mathbb{Z}/16\mathbb{Z}$, como en el caso general de (2.1.3). Pongamos $\log a = \lambda^9(m_0+m_1\zeta+m_2\zeta^2+m_3\zeta^3+m_4\zeta^4+m_5\zeta^5+m_6\zeta^6+m_7\zeta^7) \in \lambda^9\mathbb{Z}_2[\zeta]$. Por linealidad $g(\log a) = x_0m_0+x_1m_1+x_2m_2+x_3m_3+x_4m_4+x_5m_5+x_6m_6+x_7m_7$, y determínense $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7$ de los cálculos sobre los generadores.

• Para aplicar el método log-lineal en este caso de 16-potencias se necesitan aproximaciones de los $\log \eta_k$ mód $\lambda^j\mathbb{Z}_2[\zeta]$, $j \geq 41$ (ver la nota 2.1). Así, pro-

cediendo como en la demostración del teorema 2.4(a) y, haciendo uso de **E)** de (1.5.2), y también de la proposición 1.16 y de (2.35), se llega ahora a

$$\begin{aligned}
0 =& g(\log \eta_9) = g(-\lambda^9 - \lambda^{18}/2 - \lambda^{27}/3 - \lambda^{36}/4)\\
=& g(\lambda^9(3 - 2\zeta^2 - 2\zeta^3 + 3\zeta^4 - 7\zeta^5 - 4\zeta^6))\\
\equiv& 3x_0 - 2x_2 - 2x_3 + 3x_4 - 7x_5 - 4x_6 \text{ (mód 16)}\\
0 \equiv& -5x_0 - 3x_1 + 8x_3 + 5x_4 - 7x_5 + 7x_6 + 3x_7 \text{ (mód 16)}\\
0 \equiv& -2x_0 - x_1 - 5x_2 - 4x_3 - 7x_4 + 3x_5 + 6x_6 - 6x_7 \text{ (mód 16)}\\
0 \equiv& -4x_0 + 2x_2 + 6x_3 + 5x_4 + 5x_5 - 3x_6 - 3x_7 \text{ (mód 16)}\\
0 \equiv& -7x_0 + 2x_1 - 6x_2 - 4x_3 - x_4 + 8x_5 + 8x_6 \text{ (mód 16)}\\
0 \equiv& x_0 - x_1 - 4x_2 + 8x_3 - 5x_4 + x_5 \text{ (mód 16)}\\
0 \equiv& x_0 - 4x_1 + 5x_2 - 5x_4 + 4x_5 - x_6 \text{ (mód 16)}\\
-1 \equiv& x_0 - 7x_1 + 5x_2 - 3x_3 + 3x_4 - 5x_5 + 7x_6 - x_7 \text{ (mód 16)}
\end{aligned}$$

• Esto da $x_0 = x_6 = 4$, $x_1 = x_5 = -2$, $x_2 = x_4 = -4$, $x_3 = 3$, $x_7 = 0$. Así la aplicación lineal g ha sido calculada

$$g(\log a) = 2(2m_0 - m_1 - 2m_2 - 2m_4 - m_5 + 2m_6) + 3m_3 \tag{2.36}$$

• Ahora, para encontrar una fórmula para (a, λ) en términos de los parámetros de $a = 1 + \lambda^9(n_0 + n_1\zeta + n_2\zeta^2 + n_3\zeta^3 + n_4\zeta^4 + n_5\zeta^5 + n_6\zeta^6 + n_7\zeta^7)$, debemos aproximar $\log a$. Procediendo como en la demostración del teorema 2.4(a), de (2.36) se obtiene

$$(a, \lambda) = \zeta^{g(\log a)} =: \zeta^{[a,\lambda]}, \text{ donde}$$

$$\begin{aligned}
[a, \lambda] =\ & 2(n_1^4 + n_3^4 + n_5^4 + n_7^4) + 8(n_0n_1n_2 + n_0n_1n_3 + n_0n_1n_7 + n_0n_2n_4 + \\
& n_0n_2n_6 + n_0n_2n_7 + n_0n_3n_4 + n_0n_3n_5 + n_0n_3n_6 + n_0n_3n_7 + n_0n_4n_5 + n_0n_4n_6 + \\
& n_0n_5n_6 + n_0n_5n_7 + n_1n_2n_3 + n_1n_2n_5 + n_1n_2n_7 + n_1n_3n_4 + n_1n_3n_5 + n_1n_3n_6 + \\
& n_1n_4n_6 + n_1n_4n_7 + n_1n_5n_6 + n_1n_6n_7 + n_2n_3n_4 + n_2n_3n_5 + n_2n_3n_6 + n_2n_4n_5 + \\
& n_2n_4n_6 + n_2n_5n_6 + n_2n_5n_7 + n_3n_4n_5 + n_3n_4n_7 + n_3n_5n_6 + n_4n_5n_7 + n_4n_6n_7 + \\
& n_5n_6n_7) + 4(-n_0^2n_2^2 + n_0^2n_3^2 - n_0^2n_6^2 + n_0^2n_7^2 - n_1^2n_2^2 - n_1^2n_5^2 - n_1^2n_6^2 - n_2^2n_4^2 + n_2^2n_5^2 + \\
& n_3^2n_4^2 - n_3^2n_7^2 + n_4^2n_6^2 + n_4^2n_7^2 + n_5^2 + n_6^2) + 4(-n_0^2n_1 - n_0^2n_3 + n_1^2n_7 - n_1n_4^2 + n_1n_5^2 - \\
& n_2^2n_5 + n_2^2n_7 + n_3^2n_5 + n_3n_4^2 + n_3n_7^2 - n_5^2n_7 - n_5n_6^2 - n_5n_7^2 + n_6^2n_7) + 2(4n_0n_4 + \\
& 4n_0n_5 - n_0n_6 - 3n_0n_7 + 4n_1n_4 - n_1n_5 + n_1n_6 - n_2n_4 + n_2n_5 + n_3n_4) + 4(n_1^3 + n_3^3 + n_0^2 + \\
& n_2^2 + n_4^2 + n_6^2) + 4n_0 + 6n_1 - 4n_2 + 3n_3 - 4n_4 - 2n_5 - 4n_6 + 8n_7 - n_3^2 - n_7^2
\end{aligned} \tag{2.37}$$

Si ahora se quiere usar (2.36) para encontrar una fórmula log para (a, λ), puesto que

$$m_k := S(\zeta^{-k}(\sum_{i=0}^{7} m_i\zeta^i)),\ k = 0, \ldots, 7.$$

se tiene

$$2(2m_0 - m_1 - 2m_2 - 2m_4 - m_5 + 2m_6) + 3m_3 =$$
$$S((4 - 4\zeta^2 + 2\zeta^3 + 4\zeta^4 - 3\zeta^5 + 4\zeta^6 + 2\zeta^7)(\sum_{i=0}^{7} m_i\zeta^i))/8 =: S(\alpha\tfrac{\log a}{\lambda^9})/8$$

Relacionemos α con λ^9. Puesto que $\lambda^8 \equiv 2(-4\zeta - 2\zeta^2 + 4\zeta^3 + 3\zeta^4 + 4\zeta^5 - 2\zeta^6 - 4\zeta^7)$ (mód 16) se tiene $\lambda^8\zeta \equiv 2(4 - 4\zeta^2 - 2\zeta^3 + 4\zeta^4 + 3\zeta^5 + 4\zeta^6 - 2\zeta^7) =: 2\beta$ (mód

16). Se ve que $\alpha \equiv -\beta$ (mód 8), y así $2\alpha \equiv -2\beta$ (mód 16). Por lo tanto se ha encontrado la fórmula

$$(a,\lambda) = \zeta^{-S(\lambda^{-1}\zeta \log\, a)/16},\ a \in U_9. \tag{2.38}$$

Agrupando ahora todo lo anterior se tiene

Teorema 2.5 (Ley de reciprocidad de 16-potencias suplementaria)**.** *Sea* $a = 1+\lambda^9(n_0+n_1\zeta+n_2\zeta^2+n_3\zeta^3+n_4\zeta^4+n_5\zeta^5+n_6\zeta^6+n_7\zeta^7) = 1+2(y_0+y_1\zeta+y_2\zeta^2+y_3\zeta^3+y_4\zeta^4+y_5\zeta^5+y_6\zeta^6+y_7\zeta^7) \in U_9$. *Denotemos* $(a,b) =: \zeta^{[a,b]}$.

(a) $[a,\lambda] = -S(\lambda^{-1}\zeta \log\, a)/16 = (2.37)$.

(b) $[a,1+\zeta] = 2(n_1^4-n_3^4+n_5^4-n_7^4)+8(n_0n_1n_2+n_0n_1n_3+n_0n_1n_7+n_0n_2+n_4+n_0n_2n_6+n_0n_2n_7+n_0n_3n_4+n_0n_3n_5+n_0n_3n_6+n_0n_3n_7+n_0n_4n_5+n_0n_4n_6+n_0n_5n_6+n_0n_5n_7+n_1n_2n_3+n_1n_2n_5+n_1n_2n_7+n_1n_3n_4+n_1n_3n_5+n_1n_3n_6+n_1n_3n_7+n_1n_4n_6+n_1n_4n_7+n_1n_5n_6+n_1n_6n_7+n_2n_3n_4+n_2n_3n_5+n_2n_3n_6+n_2n_4n_5+n_2n_4n_6+n_2n_5n_6+n_2n_5n_7+n_3n_4n_5+n_3n_4n_7+n_3n_5n_6+n_4n_5n_7+n_4n_6n_7+n_5n_6n_7)+4(-n_0^2n_2^2+n_0^2n_3^2+n_0^2n_6^2-n_0^2n_7^2+n_1^2n_2^2+n_1^2n_5^2-n_1^2n_6^2+n_2^2n_4^2-n_2^2n_5^2-n_3^2n_4^2-n_3^2n_7^2-n_4^2n_6^2+n_4^2n_7^2+n_5^2n_6^2-n_0^2n_1+n_0^2n_3+n_1^2n_7+n_1n_4^2-n_1n_5^2+n_2^2n_5-n_2^2n_7-n_3^2n_5+n_3n_4^2-n_3n_7^2-n_5^2n_7-n_5n_6^2+n_5n_7^2+n_6^2n_7)-4n_1^3-4n_3^3+6n_0^2+2n_1^2-2n_2^2-7n_3^2-6n_4^2-2n_5^2+2n_6^2+7n_7^2+2(2n_0n_1-2n_0n_2-2n_0n_3-2n_0n_4-2n_0n_5-3n_0n_6-3n_0n_7+2n_1n_2+2n_1n_3+2n_1n_4-3n_1n_5-3n_1n_6+2n_1n_7-2n_2n_3-3n_2n_4+n_2n_5+2n_2n_6-2n_2n_7+n_3n_4+2n_3n_5+2n_3n_6+2n_3n_7+2n_4n_5+2n_4n_6-2n_4n_7+2n_5n_6-2n_5n_7-2n_6n_7)-5n_0-n_1-n_2+n_4-7n_5+5n_6-n_7$.

(c) $[a,\zeta] = 9S(log\ a)/16 = (2.28)$, *para* $a \in U_8$.

(d) *Las fórmulas* log *anteriores valen para todo* $a \in U_1$ $(= \mathcal{U}(k))$.

Demostración. (a) Ver (2.37) y (2.38). (b) Análogamente a (a) para el uniformizante $1+\zeta$. (c) La primera igualdad es (2.28). La segunda, como para (a,λ), se deriva de la fórmula que el método log-lineal daría en términos de parámetros de log a. (Ver también la nota 2.2).

(d) Se obtiene con un argumento paralelo al de los casos bicuadrático y óctico (la proposición 2.1 y el teorema 2.3). □

Proposición 2.3 (Ley de reciprocidad para 16-potencias: formulación global)**.**
(a) *Sea* $a \in 1+2(1-i)\mathbb{Z}[i]$ *y* $b \in 1+2\lambda\mathbb{Z}[\zeta]$ *coprimos. Entonces*

$$(a/b)(b/a)^{-1} = (b,a)_\lambda = (-1)^{(Na-1)/16\cdot(Nb-1)/16}$$

(b) *Si* $a \in 1+4\mathbb{Z}[i]$ *y* $b \in 1+2\lambda\mathbb{Z}[\zeta]$, *o bien, si* $a \in 1+4\mathbb{Z}$ *y* $b \in \mathbb{Z}[\zeta]\cap\mathcal{H}$, *ie,* $b \equiv 1, 1+\zeta+\zeta^7, 1+\zeta^2+\zeta^6, 1+\zeta^3+\zeta^6$ (mód 2), *son coprimos. Entonces*

$$(a/b) = (b/a).$$

(c) (Restricción a $\mathbb{Z}$ de las fórmulas suplementarias). *Si* $a \in 1+4\mathbb{Z}$, *entonces*

(c1) $(\lambda/a) = (a,\lambda)_\lambda = \zeta^{a(a^2-1)/8} = \zeta^{(7a^2-12a+5)/8} = \zeta^{(-a^2+4a-3)/8}$
$= \zeta^{7(a^2-1)/8-6(a-1)/4} = \zeta^{-(a^2-1)/8+2(a-1)/4}$

(c2) $(1+\zeta/a) = \zeta^{(7a^2+4a-11)/8} = \zeta^{7(a^2-1)/8+2(a-1)/4} = \zeta^{(3a^2-4a+1)/8}$
$= \zeta^{3(a^2-1)/8-2(a-1)/4} = \zeta^{a(a^2-1)/8}(-1)^{(a-1)/4}$
$= (\lambda/a)\zeta^{a(a^2-1)}$

(c3) $(\zeta/a) = (\lambda/a)^2 = \zeta^{a(a^2-1)/4} = \zeta^{(3a^2-4a+1)/4} = \zeta^{3(a^2-1)/4}i^{(a-1)/4}$

(c4) $(a, 1+\sqrt{2})_\lambda = (a, 1+\sqrt{2+\sqrt{2}})_\lambda = 1$
(c5) $(a, 1+\sqrt{2+\sqrt{2}}+\zeta^2(1+\zeta+\zeta^2+\zeta^3))_\lambda = (a, (1+\zeta)/\zeta^2\lambda) = i^{(1-a)/4}$
(c6) $(a, 2) = 1$.

Demostración. (a) y (b) se siguen del teorema 2.4. Para el caso $a \in 1+4\mathbb{Z}$, $b \in \mathbb{Z}[\zeta] \cap \mathcal{H}$ de (b), la nota 2.8 permite interpretar en la situación local las congruencias, y además en términos de un subgrupo (el $\mathcal{H}$). Usar ahora el primer caso de (b) junto con el caso $(a, -1)$ de (c3) y el caso (c4). Así $(a, \mathcal{H}) = 1$. Usar ahora (2.26).

(c1) y (c3) se siguen del teorema 2.5 (aunque para (c3) se seguiría directamente de $(a, \zeta)_\lambda = \zeta^{(Na-1)/16}$ y de $Na = a^8$).

(c2) Para mostrar el procedimiento para la restricción a $\mathbb{Z}$ que sigue vamos a obtener este caso, no del teorema 2.5(b) (como se hizo para (c1)), ni de $(a, \lambda)_\lambda$, cambiando ζ por $-\zeta$ (argumento que emplearemos en (c4)), si no directamente de (2.36) usando que la aproximación de $\log a$ es ahora más simple (como podría haberse procedido para $(a, \lambda)_\lambda$). Sea $a = 1+4b$. Así $\log a \equiv 4b - 8b^2$ (mód λ^{48}). Puesto que $4b - 8b^2 = 4(b-2b^2) \equiv (1+\zeta)^9(7+\zeta-5\zeta^2-3\zeta^3-3\zeta^4-5\zeta^5+\zeta^6+7\zeta^7)(b-2b^2)$, se tiene $g(\log a) = g(4b-8b^2) =$ (usando ahora (2.36)) $(2(2\cdot 7-(-1)-2\cdot(-5)-2\cdot(-2)-5+2)+3\cdot 3)(b-2b^2) = b-2b^2$. Así

$$(a, 1+\zeta) = (-\zeta)^{g(\log a)} = (-\zeta)^{-2b^2+b} = \zeta^{(7a^2+4a-11)/8}$$

(c5) Se sigue directamente de los casos (c1), (c2) y (c3).

(c4) Puesto que $1+\sqrt{2} = (1+\zeta^2)/\zeta^4(1-\zeta^2)$ se sigue de la fórmula (c3) y la de $(a, \lambda)_\lambda$, cambiando la primitiva ζ por las $-\zeta, \pm\zeta^5$. Por otra parte $1+\sqrt{2+\sqrt{2}} = \frac{(1+\zeta^5)\zeta^{10}}{1-\zeta}$. Basta usar las fórmulas ya empleadas en el caso $1+\sqrt{2}$.

(c6) Se sigue de lo anterior al expresar 2 como producto de uniformizantes y raíces de la unidad. □

Nota 2.10. *Comparación con otras fórmulas biócticas.* 1. Sobre la ley de reciprocidad de 16-potencias *ciclotómica* (teoremas 2.4 y 2.5, y proposición 2.3), con fórmulas explícitas en términos de coordenadas aditivas, ie, lo paralelo a las fórmulas bicuadrática y óctica clásicas de Gauss, Eisenstein, Goldsheider, Boniceck (teoremas 2.1, 2.2 y 2.3), lo que se tiene hasta ahora es lo siguiente:

Western (1907-1908) extiende la ley de reciprocidad de Eisenstein (1850) p-potencial, $p > 2$, y por métodos ciclotómicos, a p^n potencias, $p \geq 2$, $n \geq 1$, fórmula principal, y con un argumento restringido a $\mathbb{Z}$. Luego aplica su teoría general a los casos $p^n = 8$ (obtiene la ley de reciprocidad óctica principal de Eisenstein (1850), aquí el corolario 2.1(b)) y $p^n = 16$ "con considerable detalle" ([5], Theorem 14.3.1 y notas al Chap. 14). Ver también [29], p. 393, y [34].

También se obtuvieron el carácter 16-potencial $(a, 2)$ de 2, que comentaremos en la nota 4, así como las fórmulas log explícitas para 2^n-potencias en [2], [31] y otros (uso de teoría de cuerpos de clases), que luego habría que aproximar para encontrar fórmulas clásicas en cada caso. [23] lo hace para 4 y 8, con un procedimiento para cada caso. Para 16-potencias sería bastante más complicado. Ver también la nota 2.6.2.

2. Nuestro procedimiento (directo, unificado y con método general), permitió encontrar fórmulas biócticas inéditas (la principal del teorema 2.4, y las suplementarias del teorema 2.5 y de la proposición 2.3), así como reencontrar fórmulas clásicas con demostraciones nuevas (proposición 2.3(b)). En el caso principal de la reciprocidad de 16-potencias ciclotómica (que es elemental si se compara con la potencial vía de la aproximación de las avanzadas fórmulas analíticas de [31], que se llevó a cabo en [23] para los casos bicuadrático y óctico) nos permitió encontrar por primera vez una fórmula clásica en términos de la norma absoluta (teorema 2.4), y no restringida a $\mathbb{Z}$ (lo era la de Westerm, nota 1), análoga a las cuadrática, bicuadrática y óctica principales (teoremas 2.1 y 2.2).

Aunque, como acabamos de obtener aquí, la fórmula principal y las restricciones a $\mathbb{Z}$ de las suplementarias de la reciprocidad 16-potencial ciclotómica son fórmulas clásicas, sencillas, y paralelas a las de las reciprocidades bicuadráticas y óctica, y habiendo sido los residuos 16-potenciales objeto de estudio desde Cunningham (1896) hasta [13] (ver la nota 4), sin embargo no hemos encontrado ninguna referencia con dichas fórmulas. Ni obtenidas por métodos clásicos ni por aproximación de las fórmulas explícitas log, ni vía la fórmula producto (ésta disponible desde Hilbert), con la excepción de la de Western (1908) (ver las notas 1 y 3).

3. La ley de reciprocidad de Westerm (1907-1908), reformulada en [5], Chap. 14 con gran claridad (ver la nota 1), tiene el inconveniente (además de el de sus restricciones) de que *lo que no es explícito es el dominio de definición*. En efecto, este dominio es el de los elementos "primarios" de $\mathbb{Q}(\zeta_{p^n})$. [5], Theorem 14.2.1, lo hace explícito solo para $p^n = 8$. Ver aquí la nota 2.6.1. Sin embargo, en general, "una definición explícita de elemento primario en el sentido de Western es todavía un desiderátum" [29], p. 393.

Nuestra proposición 2.3(b), restringida a $\mathbb{Z}$, es una solución (quizá no completa) a aquel problema para el caso bióctico. En efecto, en la misma se da una versión *con dominio explícito* (nuestro grupo $\mathcal{H}$, en términos de congruencias, como en el caso óctico) del caso $p^n = 16$ de la ley de reciprocidad de Western, versión de [5].

La proposición 2.3 contiene además la *extensión al caso bióctico* (proposición 2.3(b) restringida a $\mathbb{Z}$ y a U_9, y (c2), (c3) y (c4)) de la ley de reciprocidad óctica de Eisenstein (1850) (corolario 2.1(b) y (c)).

Sobre uno y otro item del caso bióctico no habíamos encontrado nada hasta la fecha. Ver también en la nota 2 (ver, no obstante, la nota 2.7.4). La alternativa hubiera sido vía la aproximación de las elaboradas fórmulas log de [2] y de [31]. O haber extendido a 16-potencias la mencionada primaridad explícita del caso óctico.

4. Sobre ley de reciprocidad, carácter y residuacidad 16-potenciales se tiene (además de lo de la nota 1) lo siguiente. En [30] se probó la ley de reciprocidad *racional* principal para 16-potencias. Ver también [14], y [5] Chap. 8 §3. En [14] se estableció una ley de recirpocidad 2^n-potencial racional, de la que se derivan los casos 4, 8 y 16. Sobre el carácter 16-potencial, o criterios de residuacidad 16-potencial de 2 (u otros primos pequeños) ver Cunningham 1896, [1], [4], [20],

[21], [28] y [13]. En [20] y [13] se resuelve completamente el carácter 2^n-potencial de 2. (Ver también la nota 2.7.4).

5. Las fórmulas suplementarias en coordenadas aditivas del teorema 2.5, a pesar de su tamaño, y así de su poca utilidad directa, deben ser incluidas. Por un lado son las paralelas a las bicuadráticas del teorema 2.1(b) y (c) y a las ócticas del teorema 2.3 (el tamaño crece "exponencialmente"). Por otro lado porque son fórmulas base, aquí para la proposición 2.3, o para la posible reducción de las mismas a 'coordenadas más cercanas'. Además nuestra vía del teorema 2.5 podría dar (como en el caso óctico de (2.2.5)) el carácter bióctico de 2, alternativa a la particularización de $(a,2)_{2^n}$ de [13]. Sin embargo las fórmulas para $(a,2)$ en coordenadas aditivas que resultasen del teorema 2.5, serían demasiado largas para ser reducidas fácilmente a las coordenadas (w_i) de [13] (ver la nota 2.7.2). Para aplicaciones aquí del teorema 2.5 ver las notas 3 y 6.

6. En [24] se establece un método general para derivar leyes de reciprocidad racionales de las correspondientes ciclotómicas, lo que da una vía alternativa a las primeras. Luego se aplica ese método a los casos bicuadrático y óctico, obteniendo las leyes racionales de [9] y [36], respectivamente. En ese momento estaba disponible la ley de reciprocidad ciclotómica bióctica principal restringida a $\mathbb{Z}$ (ver la nota 1). En [24] los casos bicuadrático y óctico (aunque no el bióctico) se derivan partiendo de las correspondientes leyes de reciprocidad ciclotómicas, restringidas a $\mathbb{Z}$ (de Eisenstein (1850)). Así, con la proposición 2.3(b) como punto de partida, se podría derivar la ley de reciprocidad bióctica racional de [30] imitando el argumento de [24] para la óctica. Evidentemente con un mayor grado de complicación, ya que la fórmula de [30] está en términos de normas relativas de subcuerpos cuadráticos y cuárticos de $\mathbb{Q}(\zeta)$. (Ver [5], Theorem 8.3.6, para una exposición optimizada de [30]).

En cualquier caso en [24] y en los casos bicuadrático y óctico a los que aplica su método se ve que las leyes de reciprocidad ciclotómicas son claramente más fuertes que las correspondientes racionales: estas últimas se derivan de la restricción a $\mathbb{Z}$ de las primeras. (Ver también [29], p. 296).

Lista de símbolos

$\bar{k}$	cuerpo residual de un cuerpo local k	9
$\mathcal{U}(k)$	grupo de unidades del cuerpo valorado k	9
U_i	filtración de $\mathcal{U}(A)$	9
π	uniformizante de un anillo de valoración discreta	9
$\dot{k}$	grupo multiplicativo de un cuerpo k	9
v	valoración, o valor absoluto discretos	9
μ_m	grupo de raíces m-ésimas de la unidad	10
$t(-)$	torsión de un grupo abeliano	10
μ_{p^∞}	p-torsión de $\dot{k}$	10
$e(K\|k)$	índice de ramificación de la extensión $K\|k$	10
$f(K\|k)$	grado residual de la extensión $K\|k$	10
N	norma absoluta	10
log	logaritmo p-ádico	11
$\|\cdot\|_v$	valor absoluto normalizado	12
κ	aplicación de Kummer	12
$(\ ,\ ]$	paridad de Kummer	12
ψ	símbolo de residuo nórmico	12
$(\ ,\ )$	símbolo de Hilbert	12
F	automorfismo de Fröbenius	13
$\left(\frac{=}{v}\right)$	símbolo de residuo potencial (local)	14
ζ	raíz primitiva m-ésima de la unidad	14
$\mathcal{M}(k)$	conjunto de divisores primos de un cuerpo k	15
k_v	v-completación de k	15
$\mathcal{U}_v$	unidades de k_v	15
I_S		15
$S(\mathfrak{a})$		15
$\left(\frac{a}{\mathfrak{b}}\right)$, $\left(\frac{a}{b}\right)$	símbolo de residuo potencial	16
$(\ , k(\alpha)\|k)$	símbolo de Artin	16
$(b)^{S(a)}$		16
λ	uniformizante de un cuerpo ciclotómico local	17
$\eta_i := 1 - \lambda^i$		18
v_p	valoración p-ádica de $\mathbb{Q}_p$	22

S	traza ("spur") de una extensión de cuerpos	29
$\mathcal{H}$		31, 42
N_1	norma de $\mathbb{Q}_2(\zeta)\|\mathbb{Q}_2(i)$	32
N_2	norma de $\mathbb{Q}_2(\zeta)\|\mathbb{Q}_2(\sqrt{-2})$	32
N_0	norma de $\mathbb{Q}_2(i)$	34
$[\ ,\ ]$	exponente del símbolo de Hilbert	37

Bibliografía

[1] Aigner, A. (1939). *Kriterien zum* 8. *und* 16. *Potenzcharakter der Reste* 2 *und* -2, Deutsche Math., 4, 44-52.

[2] Artin, E. and Hasse, H. (1928). *Die beiden Ergänzungssätze zum reziprozitätsgesetz der* l^n*-ten potenzreste im körper der* l^n*-ten Einheitswurzeln.* (German). Abh. Math. Sem. Univ. Hamburg 6, no. 1, 146-162.

[3] Artin, E. and Tate, J. *Class field theory.* Reprinted with corrections from the 1967 original. AMS Chelsea Publishing, Providence, RI, 2009.

[4] Beeger, N. G. W. H. (1948). *A problem in the theory of numbers and it's history*, Nieuw Arch. Wiskunde (2), 22, 306-309.

[5] Berdt, B. C., Evans, R. J. and Williams, K. S. *Gauss and Jacobi sums*, John Wiley & Sons, 1998.

[6] Bohnicek, S. (1907). *Zur Theorie des relativbiquadratischen Zahlkörpers*, Math. Ann., 63, 85-144; translate from Agram. Ak. (Coat.), 163, 41-112.

[7] Bohnicek, S. (1911). *Zur Theorie der achten Einheitswurzeln*, Wiener Sitzungsber. Abt. IIa, 120, 25-47.

[8] Borevic, A. I. and Shafarevich, I. R. *Théorie des Nombres.* Monographies Internationales de Mathématiques Modernes, no. 8, Gauthier-Villars, Paris 1967.

[9] Burde, K. (1969). *Ein rationales biquadratisches Reziprozitätsgesetz.* J. Reine Angew. Math. 235, 175-184.

[10] Cassels, J. W. S. and Fröhlich, A. *Algebraic Number Theory*, Academic Press, 1967.

[11] Clement Fernández, R., Echarri Hernández, J. M. and Gómez Ayala, E. J. (2011). *A geometric proof of Kummer's reciprocity law for seventh powers.*, Acta Arith. 146, no. 4, 299-318.

[12] Deng, Y. and Huang, D. (2016). *Explicit primality criteria for* $h \cdot 2^{\pm}1$. (English, French summary), J. Théor. Nombres Bordeaux 28, no. 1, 55-74.

[13] Evans, R. (1980). *The* 2^r*-th power character of* 2, J. Reine Angew. Math., 315, 174-189.

[14] Evans, R. (1981). *Rational reciprocity laws*, Acta Arith., 39, 281-24.

[15] Goldscheider, F. *Das Reciprocitätsgesetz der achten Potenzreste*, Wissench. Beil. z. Progr. d. Luisenstädt. Realgymn, 1889.

[16] Halter-Koch, F. *Quadratic irrationals. An introduction to classical number theory.* Pure and Applied Mathematics. CRC Press, Boca Raton, FL, 2013.

[17] Hasse, H. (1924). *Das allgemeine Reziprozitätsgesetz und seine Ergänzungssätze in beliebigen algebraischen Zahlkörpern für gewisse nicht-primäre Zahlen*, J. Reine Angew. Math., 153, 192-207.
[18] Hasse, H. (1929). *Zum expliziten Reziprozitätsgesetz*, Abh. Math. Sem. Hamburg 7, 52-63.
[19] Hasse, H. (1930). *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jber. dt. Math.-Verein, Ergänzungsbans, 6, 1-204; Teil II: Reziprozitätgesetz. Reprint: Physica Verlag, Würzburg, 1965.
[20] Hasse, H. (1958). *Der 2^n-te Potenzcharakter von 2 im Körper der 2^n-ten Einheitswurzeln.*, Rend. Circ. Mat. Palermo, (2) 7, 185-243.
[21] Hasse, H. (1962). *Zum expliziten Reziprozitätsgesetz*, Arch. Math., 13, 479-485.
[22] Hasse, H. *Number theory.* Translated from the third German edition and with a preface by Horst Günter Zimmer. Grundlehren der Mathematischen Wissenschaften, 229. Springer-Verlag, Berlin-New York, 1980.
[23] Helou, C. (1988). *An explicit 2^n-th reciprocity law*, J. Reine Angew. Math. 389, 64-89.
[24] Helou, C. (1990). *On rational reciprocity*, Proc. Amer. Math. Soc., 108, 861-866.
[25] Ireland, K. F. and Rosen, M. I. *A classical introduction to modern number theory. Revised edition of Elements of number theory.* Graduate Texts in Mathematics, 84. Springer-Verlag, New York-Berlin, 1982.
[26] Iwasawa, K. (1968). *On explicit formulas for the norm residue symbol*, J. Math. Soc. Japan, 20, 151-165.
[27] Lang, S. *Algebraic number theory* Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.
[28] Lehmer, E. (1978). *Rational reciprocity laws*, Amer. Math. Month., 85, 467-472.
[29] Lemmermeyer, F. *Reciprocity laws. From Euler to Eisenstein*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.
[30] Leonard, Ph. A. and Williams, K. S. (1977) *A rational sixteenth power reciprocity law*, Acta Arith., 33, 351-362.
[31] Sen, Sh. (1980). *On explicit reciprocity laws I*, J. Reine Angew. Math., 313, 1-26.
[32] Serre, J.-P. *Local fields.* Graduate Texts in Mathematics, vol. 67. Springer-Verlag, New York-Berlin, 1979.
[33] Vostokov, S. V. and Fesenko, I. B. *Local fields and their extensions.* With a foreword by I. R. Shafarevich. Second edition. Translations of Mathematical Monographs, 121. American Mathematical Society, Providence, RI, 2002.
[34] Vostokov, S. V. and Orlova, K. Yu. (2008). *Generalization and application of the Eisenstein reciprocity law*, Vestnik St. Petersburg Univ. Math. 41, no. 1, 15-20.
[35] Weiss, E. *Algebraic number theory.* McGraw-Hill Book Co., Inc., New York-San Francisco-Toronto-London, 1963.
[36] Williams, K. S. (1976). *A rational octic reciprocity law*, Pacific J. Math., 63, 563-570.

Parte II: Períodos π-ádicos y fórmulas explícitas para el símbolo de Hilbert de un módulo formal p-divisible

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Introducción

En la evolución del 9º problema de Hilbert sobre leyes de reciprocidad explícitas se produjo en la década de 1970 un acontecimiento que replanteó el problema clásico (ya entonces prácticamente cerrado) desde un punto de vista que daba un salto cualitativo. Coates y Wiles en [15] y Wiles en [74] vieron cómo la obtención de leyes de reciprocidad explícitas para módulos de Lubin-Tate (las clásicas del 9º problema resultan entonces meramente para el grupo multiplicativo) podría estar relacionado con análogos para unidades elípticas (los cuales a su vez ellos aplicaron a la conjetura de Birch y Swinnerton-Dyer) a ciertos teoremas de Kummer e Iwasawa sobre unidades ciclotómicas (los de éste último autor habían usado la ley de reciprocidad de Artin-Hasse y habían motivado la ley de reciprocidad de Iwasawa de 1968). Esto constituyó el punto de partida de una *nueva línea* de investigación, la de *obtener leyes de reciprocidad explícitas* (fórmulas analíticas para el símbolo de Hilbert) *sobre grupos formales* en situaciones cada vez más generales. Además cada etapa de generalización requería casi siempre el desarrollo de un método nuevo. La motivación de estas generalizaciones estaba, a parte de las potenciales, incluso actuales, aplicaciones, en que, por un lado cada ley de reciprocidad es siempre un resultado difícil y, por otro, en que las leyes de reciprocidad son resultados por sí mismos, a priori, terminales de la Teoría de Números (aunque, además, sean aplicadas a otros resultados).

La primera etapa de la citada nueva línea fue cubierta por Vostokov en [69], quien dio fórmulas tipo Kummer-Shafarevich para módulos Lubin-Tate (correspondientes a las tipo Artin-Hasse de [74]), que otros autores iban a extender a módulos Lubin-Tate relativos, tanto para el tipo Kummer-Shafarevich como para el tipo Artin-Hasse, e incluyendo al caso $p = 2$. Luego las fórmulas fueron generalizadas a módulos formales de altura relativa y dimensión superiores como pasamos a ver.

En el tipo Artin-Hasse cabe destacar a Kolyvagin [48], que extiende a [74] a módulos formales 1-dimensionales (sería lo análogo a [71] pero para fórmulas Artin-Hasse). Un punto culminante es [46], que reformula cohomológicamente la ley de reciprocidad de Wiles y la generaliza a grupos p-divisibles (1-dimensionales) sobre cuerpos locales multidimensionales, y a esquemas, en K-teoría superior, con la motivación de su aplicación a la conjetura de Iwasawa para formas modulares.

Algunos de los resultados tipo Kummer-Shafarevich más avanzados son, en

una dirección, los de Abrashkin [2] y Tavares Ribeiro [68], mediante el *método de períodos p-ádicos*, pero con *las restricciones al caso absolutamente no ramificado y para grupos formales* (como se señala en [71], p. 2927, y en [72], p. 143, ver la nota 2.7.3). A su vez, la motivación principal de [68] fue la de eliminar otra restricción de [2], la de que el cuerpo base contenga a las raíces de la unidad. En otra dirección, y por un método totalmente diferente, se tiene la ley de reciprocidad de [71], para módulos formales, y libre de la restricción anterior, pero ahora con la de "dimensión uno". Períodos p-ádicos en leyes de reciprocidad también habían sido usados en [6], sin las anteriores restricciones ($e = 1$ ó $d = 1$), pero con la de ser sobre grupos formales y solo para p^n-potencias (las originales de [74] son sobre módulos formales y para π^n-potencias, y una sola componente al ser uno la altura relativa, mientras que las de Benois en este caso darían tantas componentes como la altura absoluta), y para fórmulas tipo Artin-Hasse. (Una de las ventajas de las fórmulas tipo Kummer-Shafarevich está en que son en términos de series de potencias asociadas a los argumentos, ver la nota 3.2)[9,10].

No obstante ni las fórmulas de [2] ni las de [68] incluyen, por sus restricciones al caso absolutamente no ramificado, siquiera al de [69] para módulos de Lubin-Tate (sí incluído en la de [71], que tiene la restricción a dimensión uno). Por lo tanto se puede observar todavía una deficiencia en la mencionada línea de investigación. Falta obtener un "mínimo común múltiplo" de los casos mencionados. Ie, obtener una fórmula sobre un caso general, libre de todas las restricciones anteriores, que incluya a todos los casos citados, y por un método unificado. A este respecto [2] sugirió extender su método a módulos formales desarrollando una teoría paralela de períodos π-ádicos, y así eliminar su propia restricción e incluir a [69].

El objetivo de esta segunda parte de la memoria es doble. En primer lugar se van a establecer para módulos formales los análogos a ciertos resultados usuales sobre grupos formales, muchos de los cuales sobre estos últimos constituyen la base decisiva/crucial para el método de períodos p-ádicos de [2] y [68]. Los módulos formales tienen interés en sí mismos y por su utilidad (eg, los módulos formales de Lubin-Tate, que dan la teoría de cuerpos de clases local explícita, y los grupos formales Honda son casos de módulos formales). Además las reciprocidades que sucedieron a la inaugural [74] son sobre módulos formales, excepto las que usan períodos p-ádicos (que son sobre grupos formales). A pesar de que los módulos formales (sobre dominios de característica 0) son grupos formales especiales, determinados resultados sobre grupos formales no se trasladan ni adaptan fácilmente a módulos formales, ni aquéllos sobre módulos formales se reducen fácilmente a los de grupos formales. Esas dificultades pueden apreciarse en las primeras etapas sobre este asunto, llevadas a cabo en [18] y [19] (ver aquí los teoremas 1.12 y 1.13), donde los módulos formales fueron clasificados

[9] Los métodos geométricos en leyes de reciprocidad se remontan a Einsenstein, ver la nota 2.3.1 de la parte I.

[10] Obsérvese cómo las leyes de reciprocidad son resultados profundos, que llegan a relacionar temas de las Matemáticas tan alejados a priori como los restos pontenciales (en el origen de aquéllas) y la versión p-ádica de los clásicos períodos complejos. "Una ley de reciprocidad explícita es una relación misteriosa entre símbolos de Hilbert y formas diferenciales", [45].

como lo habían sido los grupos formales desde el trabajo de Dieudonné, Cartier, Grothendieck, Honda, Fontaine y otros (aunque no referente a módulos formales, nótese también la dificultad para pasar de un contexto p-ádico absoluto a uno π-ádico relativo en [31], §§7 y 8). En la misma línea en esta parte de la memoria se obtienen aquellas versiones para módulos formales p-divisibles de resultados de grupos p-divisibles (en especial sobre períodos π-ádicos), versiones que, completando a las de [19] (estas no involucraban períodos), van a resultar suficientes en orden a sentar la base para nuestro segundo objetivo. (Ver la nota 2.4.2).

Consiste ese objetivo en la eliminación de todas las restricciones antes mencionadas de [2], [68] y [71], y en mostrar cómo los métodos de [2] y [68] pueden ser extendidos del caso absolutamente no ramificado de grupos formales al caso relativamente no ramificado de módulos formales, admitiendo así ramificación absoluta (ejecución de la mencionada sugerencia de [2], que ahora resultará más completa ya que, cuando [2] no estaba disponible [71]). De esta forma se consigue la unificación de las dos líneas mencionadas de fórmulas, la de Abrashkin y Tavares Ribeiro, y la de Vostokov y Demchemko [71], que resultarán así casos de una fórmula general (teorema 3.1), y además por un método también unificado, el de períodos π-ádicos (ya hemos apuntado que el de [71] era totalmente distinto).

Así el capítulo 2 está dedicado a establecer una teoría de períodos π-ádicos, relativización de la clásica de períodos p-ádicos a módulos formales p-divisibles. Como ya se apuntó, se completan así resultados de [19][11] (aquí el teorema 1.13), para disponer de todos los necesarios para adaptar directamente los métodos a fórmulas explícitas de [2] y [68]. (Ver la introducción a capítulo 3 y a (3.2.2)).[12]

Para adaptar el método de [68] (que priorizamos sobre el de [2], ya que aquél elimina la restricción de las raíces de la unidad de éste) para obtener fórmulas explícitas para el símbolo de Hilbert sobre módulos formales, lo cual se hace en el capítulo 3 (ya sin demostraciones, las cuales con la preparación previa resultan paralelas a las de [68]), es necesario realizar un cambio del módulo formal F por otro $F_{\mathcal{A}}$, lo que se hace en la sección 2.3, cuyo logaritmo y períodos sean los adecuados para conseguir las citadas fórmulas explícitas. Para efectuar tal sustitución, y siguiendo el caso p-ádico de [2], se hace imprescindible un resultado adecuado sobre la estructura de $D^{*}_{cris,A}(F)$, el módulo filtrado de períodos π-ádicos. Este resultado está dado por el teorema 2.5, el cual, a su vez, se va a derivar como una versión reticular del teorema de comparación de períodos π-ádicos para módulos formales (teorema 2.4). Este teorema se obtiene con el uso de su versión p-ádica (el resultado principal de [27], su Théorème 6.2) así como de algunos hechos de [19] (sus Proposition 2, Théorème 2 y Remarque 3(c)).

En la subsección (2.2.2) se establece la relación entre las categorías $\underline{\mathrm{SH}}^{E}_{A}$ y $\varphi\underline{\mathrm{MF}}^{ff2\oplus}_{AB}$ (principalmente la proposición 2.3, involucrada en la comparación

[11] Nótese que [19] (resumen de la tesis del autor) no es sobre períodos, ni siquiera estaban entonces disponibles los anillos de períodos.

[12] Una teoría de períodos π-ádicos, paralela a la de períodos p-ádicos para variedades y esquemas, no se había hecho necesaria al no ser consideradas estructuras de módulos para aquéllos (a diferencia de para grupos formales).

reticular de períodos del teorema 2.5, ver la nota 2.7) puesto que esto, a su vez, está relacionado con el cambio de módulo formal, tal como se muestra en (2.3.4) donde, además, se afina y discute tal cambio. Así en la proposición 2.10 se caracteriza el isomorfismo de sustitución del módulo formal, reduciéndolo a [2], Proposition 1.5.2 (ver la nota 2.12).

En (2.2.4) se analiza la relación (conocida en el caso p-ádico, ver [16] y [2], (1.5.2)) entre períodos π-ádicos y cohomología de de Rham (corolario 2.1). Esta va a intervenir en la adaptación de la sustitución del grupo formal de [2] a nuestro caso (ver (2.3.1) y (2.3.3)).

En definitiva la fórmula unificada del teorema 3.1 ha involucrado a la relativización realizada en [19], a la teoría de períodos π-ádicos (capítulo 2, secciones 1 y 2) y a la adaptación al caso relativo, apoyada en lo anterior, de [2] y [68] (capítulo 2, sección 3 y capítulo 3).

Ahora algunas observaciones sobre el capítulo 1 (y sección 2.1). Las estructuras base para las fórmulas explícitas, objeto final de esta parte de la memoria, son los módulos formales p-divisibles. Aunque esta segunda parte se sitúa en el campo de la Teoría de Números Algebraicos, los grupos p-divisibles los situaríamos entre la Geometría aritmética y aquélla. Por su relación con los esquemas y variedades abelianos y puesto que se pueden ver como grupos formales, es conveniente incluir un primer capítulo en el marco de éstos últimos (y así de "Geometría Algebraica formal"). La finalidad general de este primer capítulo es tratar de hacer autocontenida, en alguna medida, esta parte de la memoria para lectores menos familiarizados con los temas de la misma, y además tener incluida una fuente de referencias a conceptos, resultados y otros items para los capítulos 2 y 3. Así este capítulo puede ser visto como un survey, estructurado para tal finalidad, de material ya conocido sobre grupos formales y módulos formales p-divisibles, material incluido en varias referencias, las cuales trataremos en todo momento de citar bastante al detalle. Así no se trata de incluir demostraciones (se envía al lector adecuadamente), ni se trata de ser exhaustivo en los items tratados. La finalidad específica consiste en recopilar y completar (parcialmente) material de las referencias usuales, reformulándolo y adaptándolo a nuestras necesidades, para los objetivos buscados. Estas necesidades son las que marcaron la selección del material incluido.

La aportación de este capítulo 1 respecto al material original está, además, y en términos más concretos, en forma de las notas incluidas (algunas como notas históricas), también la matización de algunos resultados y de sus demostraciones (citando las fuentes). Alguna vez se incluyen demostraciones alternativas.

La sección 1 está dentro de la "Geometría Algebraica formal", y la hemos adecuado para enmarcar a los grupos p-divisibles. A éstos y a los módulos formales está dedicado el resto del capítulo 1, especialmente a los teoremas principales de clasificación (teoría de Dieudonné, Grothendieck y otros, y teoría Honda). Incluimos en la sección 4 una adaptación de la cohomología de de Rham formal, que sirve de transición entre las secciones 3 y 5 y que se utilizará en (2.2.4).

La sección 2.1 está también en la misma línea del capítulo 1, ahora incluyendo las herramientas básicas de los períodos p-ádicos.

Completemos ahora las observaciones ya hechas sobre las fórmulas en la otra

línea, la de Artin-Hasse. Recientemente [24] generaliza las técnicas de [48] para obtener fórmulas Artin-Hasse para módulos formales 1-dimensionales sobre cuerpos locales multidimensionales (para tipo Kummer-Shafarevich lo análogo es [72]). Además de ser fórmulas de distinto tipo, los métodos difieren completamente tanto de los de [71] como de los de períodos p-ádicos. Dentro del mismo tipo Artin-Hasse también difieren de los de [46].

Algún comentario en cuanto a la notación y terminología. Se utilizará en alguna medida el lenguaje de categorías, funtores y diagramas. Las categorías se distinguen en el texto al estar subrayadas. Hemos optado porque el símbolo de ciertas categorías sugiriera su propia definición (a costa de ser aquél más largo). Eg, $\underline{k\text{-alg.loc.libre.finita}}$ denota la categoría de k-álgebras que son localmente libres y finitas (de tipo finito como k-módulos). Esto evita tener que definir "ad hoc" muchas de las categorías y subcategorías que hemos involucrado y abrevia la mención reiterada de las estructuras de sus objetos. También así los funtores resultan más claros. Algunas categorías juegan un papel meramente contextual (como la del ejemplo previo), pero otras tienen un rol esencial. En cualquier caso se incluyen al final un amplio listado de símbolos e índice de términos.

Para las transformaciones naturales se utilizarán las notaciones $f\colon X \to Y$ o $f\colon X \Rightarrow Y$, según el contexto, y $f_R\colon X(R) \to Y(R)$ para su evaluación en un objeto R. El símbolo "$\blacksquare$" en un diagrama indica "cuadrado cartesiano".

Para los distintos morfismos de Fröbenius usaremos genéricamente la notación φ, distinguiéndose por el contexto.

Hasta la sección 1.5, inclusive, se utilizará "k" para un anillo local y "$\bar{k}$" para su cuerpo residual. A partir de la sección 1.6 pasaremos a usar en su lugar "A" y "k", respectivamente.

La "X" se utilizará tanto para denotar un esquema, para una sola variable, como para el elemento particular construido en la nota 2.10 (el elemento denotado "Y" se define en (2.1.2)).

Salvo indicación de lo contrario "*anillo/álgebra*" *significa* "*anillo/álgebra conmutativo*".

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Capítulo 1

Grupos y módulos formales p-divisibles

1.1. Grupos formales

Los grupos formales son los objetos grupo en la categoría de esquemas formales (funtoriales). Por lo tanto comenzaremos esta sección exponiendo brevemente estos últimos.

Aunque los períodos p-ádicos y las fórmulas explícitas se van a establecer sobre la base de las leyes de grupo formal (ie, de los grupos formales originales tal como surgieron en los años 50 de los grupos de Lie clásicos, de la mano de Lazard y Dieudonné) interesa dar una definición intrínseca (independiente de coordenadas) de los grupos formales y así se van a contextualizar aquellas leyes dentro de los esquemas formales, de los grupos formales funtoriales y del espectro formal. Esto, por una parte, porque el aspecto funtorial es relevante y unificador, y también porque los grupos p-divisibles (en especial los asociados a los esquemas abelianos, aquellos siendo la completación formal de estos, por lo que son espectros formales) se definieron en un principio del lado funtorial, y, además, a diferencia de otros grupos formales, tienen una dualidad. Luego los grupos p-divisibles se "unen" con las leyes de grupo formal mediante un teorema de Serre-Tate (teorema 1.5).

1.1.1. *Esquemas formales* ([21], [25], [38]). Un anillo *seudo-compacto* es un anillo topológico lineal Hausdorff (T_2) y completo $k = \varprojlim k/I$, k/I anillos artinianos (ie, de longitud finita). El conjunto de ideales primos abiertos (y así maximales) de k con la topología discreta, se denota $\mathrm{Spf}(k)$, el *espectro formal* de k. Se tiene

$$k = \prod_{\mathfrak{m}\in \mathrm{Spf}(k)} k_{\mathfrak{m}},$$

siendo $k_{\mathfrak{m}} = \varprojlim (k/I)_{\mathfrak{m}}$ el localizado usual de k en $\mathfrak{m}$, que es local seudo-compacto y se denomina la *componente local* de k en $\mathfrak{m}$ ([21], $\mathrm{VII}_{\mathrm{B}}$, 0.1).

Nota 1.1. De la factorización anterior se sigue que, para un anillo seudo-compacto, equivalen "local", "local completo" y "no factorizable". Ver [21], $\mathrm{VII_B}$, 0.1.2 Remarque (b).

Para k seudo-compacto, se denota y se tienen las igualdades ([21], $\mathrm{VII_B}$, 0.1.2)

$$r(k) := \bigcap_{\mathrm{Spf}(k)} \mathfrak{m} = J(k) = \prod_{\mathfrak{m}\in \mathrm{Spf}(k)} \mathfrak{m}k_{\mathfrak{m}} = \bigcap_{\text{primos abiertos}} \mathfrak{p}$$
$$= \{x \in k,\ x \text{ es topológicamente nilpotente}\}$$

Sea k un anillo seudo-compacto, en particular local seudo-compacto y de cuerpo residual $\bar{k}$, en particular un anillo local noetheriano completo. Un *k-módulo profiní* es un k-módulo completo límite inverso de k-módulos de longitud finita. Un *k-módulo finí* es un k-módulo profiní de longitud finita. Ha de ser discreto. Si k es un producto finito de anillos locales noetherianos, entonces "k-módulo finí equivale a k-módulo de longitud finita discreto" ([25], Chap. I §3.4)[13].

Una *k-álgebra profiní (finí)* es una k-álgebra topológica que es un k-módulo profiní (finí). Así si k es producto finito de anillos locales noetherianos, entonces "k-álgebra finí equivale a k-álgebra artiniana discreta". Denotemos

$\underline{\mathrm{PRO}}_k$ la categoría de k-álgebras profiní y $\underline{\mathrm{FI}}_k$ la de k-álgebras finí

Así $A \in \underline{\mathrm{PRO}}_k$ si y solo si $A = \varprojlim A/I$, $A/I \in \underline{\mathrm{FI}}_k$. Equivalentemente, $A = \varprojlim A/I$, $\mathrm{long}_k A/I < \infty$. ([25], Chap. I §3.7).

Nota 1.2. Si $A \in \underline{\mathrm{PRO}}_k$, entonces A es seudo-compacto ([25], Chap. I §3.7) (pero si $k \to A$ es k-álgebra topológica, A seudo-compacta, puede no ser A profiní aunque sí lo es k). Por lo tanto si $B \to A$ es un morfismo en $\underline{\mathrm{PRO}}_k$, entonces $A \in \underline{\mathrm{PRO}}_B$.

El encaje de Yoneda (fiel y pleno) da el funtor *espectro formal*

$$\mathrm{Spf}\colon \underline{\mathrm{PRO}}_k^{\mathrm{op}} \hookrightarrow \underline{\mathrm{Set}}^{\underline{\mathrm{PRO}}_k} \to \underline{\mathrm{Set}}^{\underline{\mathrm{FI}}_k}.$$

Es decir, para $A \in \underline{\mathrm{PRO}}_k$ se tiene $\mathrm{Spf}(A) := \mathrm{Hom}_{\mathrm{Top}k\text{-}\underline{\mathrm{álg}}}(A, -)\colon \underline{\mathrm{FI}}_k \to \underline{\mathrm{Set}}$ (ver la nota 1.4 para su relación con el Spf del comienzo). Este último se extiende a $\underline{\mathrm{PRO}}_k$ como sigue. Si $B = \varprojlim B/J \in \underline{\mathrm{PRO}}_k$, $B/J \in \underline{\mathrm{FI}}_k$, se tiene ([25], Chap. I §4.1):

$$\mathrm{Spf}(A)(B) := \varprojlim \mathrm{Hom}_{\mathrm{Top}\underline{k\text{-álg}}}(A, B/J) = \mathrm{Hom}_{\mathrm{Top}\underline{k\text{-álg}}}(A, B).$$

Un *esquema formal* sobre k es un funtor $X \in \underline{\mathrm{Set}}^{\underline{\mathrm{FI}}_k}$ naturalmente isomorfo a un espectro formal, ie, para el cual existe una k-álgebra profiní A tal que $X \cong \mathrm{Spf}(A)$. Es decir, un funtor $X \in \underline{\mathrm{Set}}^{\underline{\mathrm{FI}}_k}$ que es representable en $\underline{\mathrm{PRO}}_k$. ([25], Chap. I §4.6). Equivalentemente, un funtor $X \in \underline{\mathrm{Set}}^{\underline{\mathrm{FI}}_k}$ que es límite directo de funtores representables $X = \varinjlim X_i$, $X_i \cong \mathrm{Spf}(A_i) \in \underline{\mathrm{Set}}^{\underline{\mathrm{FI}}_k}$, $A_i \in \underline{\mathrm{FI}}_k$ ([25],Chap. I §4.2).

Denotemos $\widehat{\underline{\mathrm{Sch}}}_k$ la categoría de k-esquemas formales.

[13] Aquí vamos a usar los galicismos "profiní" y "finí" puesto que sus conceptos no son exactamente los de "profinito" y "finito" usuales.

Proposición 1.1 ([25] Chap. I §4.6)**.** *Se tiene una equivalencia de categorías*

$$\mathrm{Spf}\colon \underline{\mathrm{PRO}}_k^{\mathrm{op}} \;\simeq\; \widehat{\underline{\mathrm{Sch}}}_k \qquad \square$$

Nota 1.3. 1. Siendo un morfismo en $\widehat{\underline{\mathrm{Sch}}}_k$ una transformación natural $f\colon X = \mathrm{Spf}(A) \to Y = \mathrm{Spf}(B)$, por la proposición 1.1 corresponde a un morfismo $f^*\colon B \to A$ en $\underline{\mathrm{PRO}}_k$. Un esquema formal $X = \mathrm{Spf}(A)$ puede ser visto como un morfismo $X = \mathrm{Spf}(A) \to \mathrm{Spf}(k)$ (el correspondiente a $k \to A$). Y el morfismo $f\colon X \to Y$ como un esquema formal $X \in \widehat{\underline{\mathrm{Sch}}}_B$ $(=: \widehat{\underline{\mathrm{Sch}}}_Y)$ (nota 1.2).

2. La equivalencia de la Proposición 1.1, junto con la análoga para esquemas afines ordinarios, $\mathrm{Spec}\colon \underline{k\text{-álg}}^{\mathrm{op}} \simeq \underline{\mathrm{Sch}}_k$, inducen el siguiente diagrama funtorial conmutativo (para k localmente noetheriano, y así "un módulo de tipo finito es localmente libre si y solo si es plano")

$$\begin{array}{ccccc}
\underline{k\text{-álg.loc.libre.finita}}^{\mathrm{op}} & \overset{\mathrm{Spec}}{\simeq} & & & \underline{\mathrm{Sch}_k\mathrm{finito}} \\
\downarrow & & & & \downarrow \\
 & & \underline{\mathrm{FI}}_k^{\mathrm{op}} \overset{\mathrm{Spf=Spec}}{\simeq} \widehat{\underline{\mathrm{Sch}}}_k\underline{\mathrm{fin\acute{i}}} & & \\
 & \swarrow & & \searrow & \\
\underline{k\text{-álg.finita}}^{\mathrm{op}} & \overset{\mathrm{Spec}}{\simeq} & & & \underline{\mathrm{Sch}}_k\underline{k\text{-álg.finita}} \\
\downarrow & & & & \downarrow \\
\underline{\mathrm{PRO}}_k^{\mathrm{op}} & \overset{\mathrm{Spf}}{\simeq} & & & \widehat{\underline{\mathrm{Sch}}}_k
\end{array}$$

Nótese que cada k-álgebra finita puede ser considerada como una k-álgebra profiní al ser $k \in \underline{\mathrm{PRO}}_k$.

3. Para $X = \mathrm{Spec}(A) \in \underline{\mathrm{Sch}}_k\underline{\mathrm{finito}}$ se define el *orden* de X como $|X| := \mathrm{rango}_k A$.

4. Si (X_i) es un sistema inductivo de k-esquemas finitos, entonces (puesto que X_i es k-esquema formal por la nota 1) $\varinjlim X_i = \varinjlim \mathrm{Spec} A_i = \varinjlim \mathrm{Spf} A_i = \mathrm{Spf}(\varprojlim A_i)$ es un k-esquema formal.

Se define el funtor *completación formal* $\underline{\mathrm{Sch}}_k \xrightarrow{\wedge} \widehat{\underline{\mathrm{Sch}}}_k$ por restricción

$$\begin{array}{ccc}
\underline{\mathrm{FI}}_k & & \\
\downarrow & \overset{\hat{X}}{\searrow} & \\
\underline{k\text{-álg}} & \xrightarrow[X]{} & \underline{\mathrm{Set}}
\end{array}$$

Si $X = \mathrm{Spec}(A)$, entonces $\hat{X} = \mathrm{Spf}(\hat{A})$, siendo $\hat{A} = \varprojlim A/I$, $A/I \in \underline{\mathrm{FI}}_k$, la completación profiní de la k-álgebra A, y así $\hat{X}$ es un k-esquema formal ([25], Chap. I §4.8).

Se tiene, para $X = \mathrm{Spf}(A)$ e $Y = \mathrm{Spf}(B)$, que $X \times_k Y := \mathrm{Spf}(A \hat{\otimes}_k B)$ es el producto en la categoría $\widehat{\underline{\mathrm{Sch}}}_k$. Así $(X \times_k Y)(R) = X(R) \times Y(R)$. (Respecto al *producto tensorial completo* $\hat{\otimes}$ ver [25], Chap. I §3.2, o [21], $\mathrm{VII_B}$, §0.3).

En cuanto al cambio de anillo sea $k \to k'$ un homomorfismo continuo de anillos seudo-compactos. Si $X = \mathrm{Spf}(A)$, $A \in \underline{\mathrm{PRO}}_k$, se define

$$X_{k'} := X \times_k k' = \mathrm{Spf}(k' \hat{\otimes}_k A),$$

obteniéndose así el funtor extensión de escalares

$$(-)_{k'}\colon \underline{\widehat{\mathrm{Sch}}}_k \to \underline{\widehat{\mathrm{Sch}}}_{k'}.$$

Nótese que el *orden de un esquema finito* (nota 1.3.3) *se conserva en extensión de escalares.*

Si k es un dominio local de cuerpo de fracciones K y cuerpo residual $\bar{k}$, entonces $X_K \in \underline{\widehat{\mathrm{Sch}}}_K$ y $X_{\bar{k}} \in \underline{\widehat{\mathrm{Sch}}}_{\bar{k}}$ se denominan, respectivamente, las *fibras genérica* y *especial* de $X \in \underline{\widehat{\mathrm{Sch}}}_k$.

Nota 1.4. *Relación con los esquemas formales usuales de* [38]. 1. Los esquemas formales considerados anteriormente, adecuados para contextualizar a los grupos formales, son un caso especial de los esquemas formales usuales, introducidos en [38] ([21], $\mathrm{VII_B}$, §1.2 denomina a los primeros *variedades formales* para distinguirlos de los esquemas formales de [38], pero aquí tomamos la terminología de [25]). Respecto a estos recuérdese que un *esquema formal* es un espacio topológicamente anillado que localmente es un *esquema formal afín*. Éstos últimos se definen como los espacios topológicamente anillados isomorfos a los espectros formales $\mathrm{Spf}(k) := \mathrm{Spec}(k/I)$, siendo k un anillo I-ádico ($k = \varprojlim k/I^n$), con el haz estructural límite inverso de los haces estructurales de los esquemas afines $\mathrm{Spec}(A/I^n)$. Ver [38], Chap. I §§10.1-10.4. Denotamos por $\underline{\widehat{\mathrm{Sch}}}\mathrm{EGA}$ la categoría de estos esquemas formales.

Esta construcción de $\mathrm{Spf}(k)$ se puede trasladar de anillos I-ádicos a anillos seudo-compactos ([21], $\mathrm{VII_B}$, 1.1). Si k es seudo-compacto se define $\mathrm{Spf}(k) \in \underline{\widehat{\mathrm{Sch}}}\mathrm{EGA}$ (ahora no necesariamente afín, ver la nota 2) como el espacio anillado formado por el espacio espectro formal $\mathrm{Spf}(k)$ (ahora el del comienzo de esta subsección) con el haz estructural que, para $E \subset \mathrm{Spf}(A)$, tiene a $\prod_{\mathfrak{m}\in E} k_{\mathfrak{m}}$ como espacio de secciones. Por la nota 1.1 se tiene que si k es seudo-compacto local, entonces $\mathrm{Spf}(k) \in \underline{\widehat{\mathrm{Sch}}}\mathrm{EGAafín}$. Por lo tanto, en general, $\mathrm{Spf}(k) \in \underline{\widehat{\mathrm{Sch}}}\mathrm{EGA}$ ([21], $\mathrm{VII_B}$, 0.1.2(d)). Así, si $A \in \underline{\mathrm{PRO}}_k$, entonces $\mathrm{Spf}(A) \in \underline{\widehat{\mathrm{Sch}}}_k\mathrm{EGA}$, y se tiene un funtor

$$\mathrm{Spf}\colon \underline{\mathrm{PRO}}_k^{\mathrm{op}} \rightarrowtail \underline{\widehat{\mathrm{Sch}}}_k\mathrm{EGA},$$

fiel y pleno ([21], Proposition $\mathrm{VII_B}$.1.1). Entonces, con la proposición 1.1, se tiene

$$\underline{\widehat{\mathrm{Sch}}}_k \overset{\mathrm{Spf}}{\simeq} \underline{\mathrm{PRO}}_k^{\mathrm{op}} \overset{\mathrm{Spf}}{\rightarrowtail} \underline{\widehat{\mathrm{Sch}}}_k\mathrm{EGA},$$

de forma que $\underline{\widehat{\mathrm{Sch}}}_k$ *puede verse como una subcategoría plena de* $\underline{\widehat{\mathrm{Sch}}}_k\mathrm{EGA}$, y se identifican $\mathrm{Spf}(A)$, el funtorial y el de esta nota. Si $X \cong \mathrm{Spf}(A) \in \underline{\widehat{\mathrm{Sch}}}_k \subset \underline{\widehat{\mathrm{Sch}}}_k\mathrm{EGA}$, $A \in \underline{\mathrm{PRO}}_k$, es un esquema formal, entonces $A \cong \Gamma(X, \mathcal{O}_X)$, y se dice que A es el *álgebra afín* de X (aunque X no fuese afín).

2. *Para una k-álgebra A se tiene $A \in \underline{\mathrm{PRO}}_k \cap \underline{k\text{-álg}I\text{-ádica}}$ si y solo si $A \in \underline{k\text{-álg}I\text{-ádica}}$ y $\log_k A/I < \infty$, si y solo si $r(A)$ es abierto, si y solo si el espacio discreto* $\mathrm{Spf}(A)$ *es finito (ie, compacto), si y solo si* $\mathrm{Spf}(A) \in \underline{\widehat{\mathrm{Sch}}}_k \cap \underline{\widehat{\mathrm{Sch}}\mathrm{EGAafín}}$ ([21] $\mathrm{VII_B}$ 0.1.2(c)).

En cualquier caso, sea A una k-álgebra profiní o bien sea A una k-álgebra I-ádica, $\mathrm{Spf}(A)$ define un funtor

$$\mathrm{Spf}(A) := \mathrm{Hom}_{\underline{\mathrm{Top}k\text{-álg}}}(A, -)\colon \underline{\mathrm{Top}k\text{-álg}} \to \underline{\mathrm{Set}}.$$

3. Consideremos la *completación formal* $X|_{X'} \in \widehat{\underline{\mathrm{Sch}_k \mathrm{EGA}}} = (X', \mathcal{O}_{X|_{X'}})$ *de un* k*-esquema* (ordinario) X *a lo largo de un subesquema cerrado* ([38], Chap. I §10.8). En el caso afín $X = \mathrm{Spec}(A)$ y $X' = \mathrm{Spec}(A/I)$, entonces $X|_{X'} = \mathrm{Spf}(\hat{A}_I) = \varinjlim \mathrm{Spec}(A/I^n) = \mathrm{Spec}(A/I)$, denotando $\hat{A}_I = \varprojlim A/I^n$. Así $X|_{X'} \in \widehat{\underline{\mathrm{Sch}_k \mathrm{EGAafín}}}$. En particular, para X cualquiera, si X' está en un subesquema afín de X, eg, si X un punto cerrado. Se tiene $X|_{X'} \in \widehat{\underline{\mathrm{Sch}_k}}$ (afín) si y solo si $\mathrm{long}_k A/I < \infty$.

Ejemplo 1.1. (De esquemas formales). Se obtienen por completación de ejemplos usuales de esquemas afines ordinarios.

1. El espacio afín $\mathbb{A}^d_k := \mathrm{Spec}\, k[\mathbf{X}]$ (d variables). Se denota $\mathbb{G}_a := \mathbb{A}^1_k$, el llamado *grupo aditivo*. Así se tiene $\mathbb{G}^d_a = \mathbb{A}^d_k$.

Sea $A = k[[\mathbf{X}]] = \widehat{k[\mathbf{X}]}_I \in \underline{\mathrm{PRO}_k} \cap \underline{k\text{-álg}I\text{-ádica}}$, para k local de maximal $\mathfrak{m}$, e $I = \mathfrak{m} + \mathbf{X}k[[\mathbf{X}]]$ (puede ser $d = \infty$). Así (ahora $d < \infty$) $\mathbb{A}^d_k := \mathbb{A}^d_k|_0 = \mathrm{Spf}(k[[\mathbf{X}]]) \in \widehat{\mathrm{Sch}_k} \cap \widehat{\underline{\mathrm{SchEGAafín}}}$, es la completación formal del espacio afín $\mathbb{A}^d_k$ a lo largo del origen $0 = \mathrm{Spec}(k[\mathbf{X}]/I) = \mathrm{Spec}(\bar{k})$ (nota 1.4.3). En particular $\mathbb{G}_a = \hat{\mathbb{G}}_a$.

2. El *grupo multiplicativo* $\mathbb{G}_m := \mathrm{Spec}\, k\big[X, X^{-1}\big]$. Sobre $\mathbb{G}_m$ volveremos en el ejemplo 1.2.

Un k-módulo profiní M se dice *topológicamente libre* si es isomorfo a algún k^I (con la topología producto). Se dice que M es *topológicamente plano* si verifica cualquiera de las siguientes condiciones equivalentes (ver [25], Chap. I §3.5)

(i) M es objeto proyectivo en $\underline{k\text{-Mod.profiní}}$.
(ii) M es topológicamente libre localmente.
(iii) El funtor $-\hat{\otimes}_k M\colon \underline{k\text{-Mod.profiní}} \to \underline{k\text{-Mod.profiní}}$ es exacto.

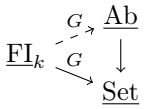
Es inmediato que si M es k-módulo de tipo finito, entonces estas nociones equivalen a "k-módulo libre" y a "k-módulo plano", respectivamente. La k-álgebra $k[[\mathbf{X}]]$ del ejemplo 1.1.1 es topológicamente libre. Si k es noetheriano, entonces un k-módulo topológicamente libre es plano.

Proposición 1.2 ([21] $\mathrm{VII}_\mathrm{B}(1.3.1)$)**.** *Un morfismo en* $\widehat{\underline{\mathrm{Sch}_k}}$ sobreyectivo (la aplicación entre los conjuntos subyacentes es sobreyectiva) *y topológicamente plano*[14] *es un coigualador.* □

Nota 1.5. En $\underline{\mathrm{Sch}_k}$ es elemental que un morfismo es sobreyectivo si y solo si su homomorfismo de álgebras afines es fielmente plano.

1.1.2. *Grupos formales* ([21], [25]). Sea k como en (1.1.1). Un k*-grupo formal* (aquí *se supondrá siempre conmutativo*) es un objeto grupo abeliano de la categoría $\widehat{\underline{\mathrm{Sch}_k}}$ de k-esquemas formales. Es decir, un k-grupo formal es un esquema formal $G \in \widehat{\underline{\mathrm{Sch}_k}}$ para el cual existe un levantamiento

[14] Un k-esquema formal se dice *topológicamente plano* si su álgebra afín es topológicamente plana como k-módulo. Un morfismo $f\colon X \to Y$ en $\widehat{\underline{\mathrm{Sch}_k}}$ se dice topológicamente plano si $X \in \widehat{\underline{\mathrm{Sch}_Y}}$ es topológicamente plano. (Ver las notas 1.2 y 1.3.1).



($\underline{\mathrm{Ab}}$ denota la categoría de grupos abelianos usuales). Denotemos $\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$ la categoría de k-grupos formales (conmutativos). Se utilizará también la notación

$$\mathrm{Hom}_k(G, G') := \mathrm{Hom}_{\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k}(G, G').$$

Los k-grupos formales están representados por lo que denominamos *k-álgebras de Hopf formales* (*con antípodo*, que corresponde al inverso en el grupo formal), las cuales forman una categoría, $\underline{k\text{-}\widehat{\mathrm{Hopf}}}$, cuyos objetos son $A \in \underline{\mathrm{PRO}}_k$ junto con una comultiplicación $\Delta\colon A \to A\hat{\otimes}_k A$, un antípodo $i\colon A \to A$ y una aumentación $\varepsilon\colon A \to k$, todos morfismos en la categoría $\underline{\mathrm{PRO}}_k$, y con axiomas análogos a los de una k-álgebra de Hopf ordinaria. Mediante la aumentación se tiene $A = k \oplus A^+$ en la categoría $\underline{k\text{-Mod}}$, donde $A^+ := \ker\varepsilon$ es el llamado *ideal aumentación*.

Proposición 1.3 ([25], Chap. I §5.2)**.** *La equivalencia de la* proposición 1.1 *induce una equivalencia de categorías*

$$\mathrm{Spf}\colon \underline{k\text{-}\widehat{\mathrm{Hopf}}}^{\mathrm{op}} \;\simeq\; \mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k. \qquad \square$$

Observando la nota 1.3.2 se tiene $\mathrm{Gr}\underline{\mathrm{Sch}}_k\underline{\text{finito}} \subset \mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$ ($\mathrm{Gr}\underline{\mathrm{Sch}}_k$ denota la categoría de esquemas afines en grupos).

Nota 1.6. 1. Sea $G = \mathrm{Spf}(A) \in \mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$. En este caso el funtor de la nota 1.4.2 se levanta a un funtor

$$G := \mathrm{Hom}_{\mathrm{Top}\underline{k\text{-álg}}}(A, -)\colon \underline{k\text{-álg.compl.linealT}_2} \to \underline{\mathrm{Ab}}$$

(puesto que $-\hat{\otimes}_k-$ es el coproducto en la categoría de la izquierda), extendiendo al funtor $G\colon \underline{\mathrm{FI}}_k \to \underline{\mathrm{Ab}}$. Así, si R es una k-álgebra completa lineal Hausdorff, entonces la operación del grupo $G(R) = \mathrm{Hom}_{\mathrm{Top}\underline{k\text{-álg}}}(A, R)$ se denota

$$x +_G y := \binom{x}{y}\Delta\colon A \to R,\ x, y \in G(R).$$

En el caso $X = \mathrm{Spf}(B) \in \widehat{\underline{\mathrm{Sch}}}_k$, se tiene que $G(B) := \mathrm{Hom}_{\mathrm{Top}\underline{k\text{-álg}}}(A, B) \cong \mathrm{Hom}_{\widehat{\underline{\mathrm{Sch}}}_k}(X, G) \in \underline{\mathrm{Ab}}$ (lema de Yoneda), y las operaciones de este grupo se denotan como sigue

$$f +_G g := m(f, g)\colon X \to G$$

si $f, g\colon X \to G$, donde $m\colon G \times G \to G$ denota aquí la multiplicación del objeto grupo G. Se utiliza la notación $[n]_G = n1_G := 1_G +_G \overset{n)}{\cdots} +_G 1_G$.

Las operaciones $x +_G y$ y $f +_G g$ son obviamente compatibles, ie, para $f, g\colon X \to G$ se tiene

$$(f +_G g)_R = f_R +_G g_R\colon X(R) \to G(R).$$

En particular $([n]_G)_R$ $(= (n1_G)_R) = n1_{G(R)}\colon G(R) \to G(R)$.

2. Sea $f\colon G = \mathrm{Spf}(A) \to G' = \mathrm{Spf}(B)$ un morfismo en $\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$. Entonces $(\ker f)(R) := \ker(G(R) \to G'(R))$, $R \in \underline{\mathrm{FI}}_k$, *es el núcleo de* f *en* $\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$, y $\ker f = \mathrm{Spf}(A/f^*B^+)$. Por lo tanto $0 \to (\ker f)(R) \to G(R) \to G'(R)$ es exacta para $R \in \underline{\mathrm{PRO}}_k$. Se utiliza la notación $G[n] := \ker([n]_G : G \to G) = \mathrm{Spf}(A/(n1_A)A^+)$. Se tiene $G[n]\,(R) = (0\colon n)_{G(R)}$ (ver el final de la nota 1).

La proposición 1.2 se utiliza en el siguiente

Teorema 1.1 ([21], $\mathrm{VII_B}$ (1.3.1) y 2.4)**.** *Sea* $0 \to G' \to G \to G'' \to 0$ *una sucesión en* $\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$.

(a) *Si* G' *es topológicamente plano, entonces la sucesión es exacta corta* (ie, $G' = \ker(G \to G'')$ y $G'' = \mathrm{coker}(G' \to G)$) *si y solo si* $G' = \ker(G \to G'')$ *y* $G \to G''$ *es sobreyectivo y topológicamente plano.*

(b) *Si la sucesión es de* $\mathrm{Gr}\underline{\mathrm{Sch}}_k\underline{\text{finito}}$*, entonces es exacta corta si y solo si* $G' = \ker(G \to G'')$ *y* $G \to G''$ *es fielmente plano* (ie, sobreyectivo, ver la nota 1.5). □

Teorema 1.2 ([21] $\mathrm{VII_B}$ (2.4.2), [25], Proposition I.6.5)**.** *Si* k *es un cuerpo, entonces las categorías* $\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$ *y* $\mathrm{Gr}\underline{\mathrm{Sch}}_k$ *son abelianas.* □

Proposición 1.4. *Para un morfismo de* k*-grupos formales* $f\colon G = \mathrm{Spf}(A) \to G' = \mathrm{Spf}(B)$ *son equivalentes*

(i) f *es un conúcleo de núcleo finito.*

(ii) f *es sobreyectivo, topológicamente plano, y* $k \to A/f^*B^+$ *es finita plana.*

(iii) f *es sobreyectivo, topológicamente plano, y* $k \to A/f^*B^+$ *es finita.*

(iv) f *es sobreyectivo y* $f^*\colon B \to A$ *es finita plana.*

Si B *es local* (ie, si G' es conexo, ver más adelante), *entonces* $\mathrm{Spf}(B) = *$, *y así* f *es siempre sobreyectivo. Si* B *es local noetheriana, entonces "plano" puede ser sustituido por "libre".*

Un morfismo verificando las condiciones anteriores se dice una *isogenia.*

Demostración. Las últimas afirmaciones son obvias, así como (iii)⇔(iv). Para (i)⇔(ii) usar el teorema 1.1. Para (iv)⇒(ii), que el álgebra $k \to A/f^*B^+$ es plana se sigue de que $A/f^*B^+ = A \otimes_B k$ y de que $B \to A$ es plana. □

Supongamos ahora cualquiera de las dos situaciones siguientes: k es un cuerpo o G es un k-esquema en grupos finito (y k como al comienzo). En cualquier caso se define el *dual de Cartier* de $G = \mathrm{Spf}(A)$ de la forma:

$$G^D := \mathrm{Spf}(A^*), \text{ siendo } A^* := \mathrm{Hom}_{\mathrm{Top}\underline{k\text{-álg}}}(A, k).$$

Este funtor establece equivalencias de categorías, respectivamente,

$$\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k^{\mathrm{op}} \overset{(-)^D}{\simeq} \mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k \quad \text{y} \quad \mathrm{Gr}\underline{\mathrm{Sch}}_k\underline{\text{finito}}^{\mathrm{op}} \overset{(-)^D}{\simeq} \mathrm{Gr}\underline{\mathrm{Sch}}_k\underline{\text{finito}}.$$

(Ver [25], Chap. I, §§5.4 y 5.5).

En lo que sigue se supondrá que k *es local (completo) y que su cuerpo residual* $\bar{k} = k/\mathfrak{m}$ *es perfecto.* Un k-grupo formal $G = \mathrm{Spf}(A)$ se dice *étale* si es topológicamente plano y si $A = \Pi A_i$, A_i k-álgebra finita étale (formalmente lisa

y no ramificada, equivalentemente, plana (libre) y residualmente separable). G se dice *conexo* si A es un anillo local. Es decir, si A es no factorizable (ver la nota 1.1). En particular se tiene la noción de k-esquema en grupos finito conexo.

Proposición 1.5 ([25], Chap. I §§7.2 y 7.3, [21] VII$_{\mathrm{B}}$ 2.5.1, 2.5.2)**.** (a) *El funtor $G \mapsto G_{\bar{k}}$ induce una equivalencia*

$$\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k\underline{\text{ét.top.plano}} \;\simeq\; \mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_{\bar{k}}\underline{\text{ét}}.$$

Además, si G es topológicamente plano y $G_{\bar{k}}$ es étale, entonces G está determinado por $G_{\bar{k}}$, y G es étale.

(b) *Sea $G = \mathrm{Spf}(A)$ un k-grupo formal topológicamente plano. Se tiene una sucesión exacta*

$$0 \to G^0 \to G \to G^{et} \to 0,$$

donde $G^{et}(B) := G(B/rB)$, $B \in \underline{\mathrm{FI}}_k$, y donde G^0 se define como el núcleo de $G \to G^{et}$ en $\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$ (ie, $G^0(B) := \ker(G(B) \to G^{et}(B)$, nota 1.6.2). *Así $G^0 =: \mathrm{Spf}(A^0)$ es un k-grupo formal topológicamente plano, donde $A^0 = A_{\epsilon^{-1}(\mathfrak{m})}$ es la componente local de A en el único maximal (abierto) de A que contiene a A^+. En particular G^0 es conexo, la* componente conexa *de G. Se tiene $(G^{et})_{\bar{k}} = (G_{\bar{k}})^{et} = \mathrm{Spf}(A_{\bar{k}}/rA_{\bar{k}})$, $A_{\bar{k}} = A/\mathfrak{m}A$. Así G^{et} es étale y se denomina el* cociente étale *de G.*

(c) *En el caso $k = \bar{k}$ la sucesión $0 \to G^0 \to G \to G^{et} \to 0$ escinde canónicamente. Así $A \cong A^{et}\hat{\otimes}_k A^0$, $G = G^0 \times_k G^{et}$ y $G^{et} = \mathrm{Spf}(A/rA)$* (la exactitud en (b) se sigue de la de este caso). □

Teorema 1.3 ([73], §§6.4, 11.4 y 14.4; [63], §3; [67], p. 160)**.** *Sea ahora k, además, noetheriano*

(a) *Si G es un k-esquema en grupos finito conexo, entonces $|G|$ es 1 si* $\mathrm{char}\,\bar{k} = 0$ *ó una potencia de* $\mathrm{char}\,\bar{k}$ *en otro caso.*

(b) *El funtor $G \mapsto G(\overline{\bar{k}})$* (aquí $\overline{\bar{k}}$ denota la clausura algebraica del cuerpo residual $\bar{k}$ y $G_{\bar{k}}$ es el grupo de Galois absoluto de $\bar{k}$[15]) *establece una equivalencia de categorías que conserva el orden $|\ |$*

$$\mathrm{Gr}\underline{\mathrm{Sch}}_k\underline{\text{ét.finito}} \;\simeq\; G_{\bar{k}}\text{-}\underline{\mathrm{Mod.discr.finito}}$$ □

Nota 1.7. Si $G = \mathrm{Spec}(A)$ es un k-esquema en grupos, entonces $\hat{G}^0 = G|_0$, ie, la componente conexa de la completación formal de G, coincide con la completación formal de G a lo largo de 0 (usando la proposición 1.5(b) ambos grupos formales están representados por $\hat{A}_{\epsilon^{-1}(\mathfrak{m})}$, siendo $\hat{A}$ la completación profiní).

Sea $f\colon G = \mathrm{Spf}(A) \to G' = \mathrm{Spf}(B)$ un morfismo de k-grupos formales. Se define

$$\deg(f) := \mathrm{rango}_B A \ (= \mathrm{rango}_k A/f^*B^+).$$

Así, si $\ker f$ es finito, entonces $\deg(f) = |\ker f|$. En particular, si $G[n]$ es finito, entonces $\deg [n]_G = |G[n]| = \mathrm{rango}_k\ A/(n1_A)A^+$ (ver la nota 1.6.2).

[15] Es el grupo fundamental étale del anillo k.

Proposición 1.6. *Sea G un k-esquema en grupos finito y p un número primo. Si $[p^n]_G = 0$ para $n >> 0$, entonces $|G|$ es una potencia de p.*

Demostración. [20], Corollaire de p. 40 lo hace si k es cuerpo. Nuestro caso se reduce al "caso cuerpo" usando la fibra genérica (si k fuese dominio) o la fibra especial, teniendo en cuenta que $|G|$ se conserva en extensión de escalares. □

Un k-grupo formal $G = \mathrm{Spf}(A)$ se dice *liso* si A es "*formalmente lisa*" sobre k, en el sentido de que $G(B) \twoheadrightarrow G(B/I)$ es sobreyectiva para cada k-álgebra finí B y cada ideal I de B tal que $I^2 = 0$ ([25], Chap. I, §9.6).

Teorema 1.4. *Sea $G = \mathrm{Spf}(A)$ un k-grupo formal. Se tiene*

(a) *Si G es liso, entonces es topológicamente plano.*

(b) *Si G es topológicamente plano, entonces son equivalentes*

(i) *G es liso.*

(ii) *$(G_{\bar{k}})^0 = (G^0)_{\bar{k}}$ es liso.*

(iii) *G^0 es liso.*

(iv) $A^0 \cong k[[\mathbf{X}]]$ (posiblemente infinitas variables y con la estructura $\underline{\mathrm{PRO}}_k$ como en el ejemplo 1.1.1).

Demostración. Es consecuencia de [25], Chap. I, Théorème 1, ver [25], Chap. I §9.7. □

Nota 1.8. Si $X = \mathrm{Spf}(A) \in \widehat{\mathrm{Sch}}_k\underline{\mathrm{EGAafín}}$, se dice que X es *formalmente liso* si A es una k-álgebra formalmente lisa ([52], §2.4). Así, si $G \in \mathrm{Gr}\widehat{\mathrm{Sch}}_k$ es afín y formalmente liso (como objeto de $\widehat{\mathrm{Sch}}_k\underline{\mathrm{EGA}}$), entonces es liso como k-grupo formal.

Los morfismos formalmente lisos de esquemas formales están implícitos en [34] y [35]. Ver [52], §2.4 y [4], §2. Usando el teorema 1.4 y [35], Théorème (17.5.1) y Proposition (17.5.3), *si la dimensión de G* (ver abajo) *es finita se tiene que G es formalmente liso en $\widehat{\mathrm{Sch}}_k\underline{\mathrm{EGAafín}}$ si y solo si es liso como grupo formal.*

Los grupos formales lisos se definen en [20] como los espectros formales de anillos de series de potencias formales (ver el teorema 1.4). Otros autores definen directamente "G liso" mediante (iv) del teorema 1.4. Pero este teorema (original de [25]) permite enmarcar la lisitud para grupos formales dentro de la lisitud formal de la Geometría Algebraica de EGA IV.

Sea $G = \mathrm{Spf}(A)$ un k-grupo formal. Se definen el *espacio cotangente y el espacio tangente* de G con valores en $B \in \underline{\mathrm{PRO}}_k$, respectivamente como sigue ([25], Chap. I, §1.8)

$$t^*_G(B) := A^+/Cl(A^{+2})\hat{\otimes}_k B \in \mathrm{Top}\underline{B\text{-Mod}}$$

$$t_G(B) := \mathrm{Hom}_{\mathrm{Top}\underline{k\text{-Mod}}}(A^+/Cl(A^{+2}), B) \in \mathrm{Top}\underline{B\text{-Mod}}.$$

Sean $\widehat{\Omega}_{A|k} := \widehat{\Omega_{A|k}}$ el A-módulo de *diferenciales continuas* de $A|k$ y $\Omega_k(G) := \ker \widehat{\Omega}_\partial$ el módulo de *diferenciales invariantes*, donde

$$\partial\colon A \to A\hat{\otimes}_k A \tag{1.1}$$

está dada por $\partial(a) := 1\otimes a - \Delta(a) + a\otimes 1$ (se entiende $\widehat{\Omega_\partial} = \widehat{\Omega}_{1\otimes -} - \widehat{\Omega}_\Delta + \widehat{\Omega}_{-\otimes 1}$).

Proposición 1.7 ([25], Chap. I §§8.2 y 8.5)**.** *En la situación anterior se tiene un diagrama conmutativo de A-módulos*

$$\begin{array}{ccc} \Omega_k(G) & \rightarrowtail & A\hat{\otimes}_k\Omega_k(G) \\ \cong\,\big\downarrow & \searrow & \big\downarrow\cong \\ t^*_G(k) & \rightarrowtail & (t^*_G(A)) = A\hat{\otimes}_k t^*_G(k) \underset{\eta^*}{\cong} \widehat{\Omega}_{A|k} \end{array}$$

donde η^* está inducida por el automorfismo $\eta\colon G\times G \to G\times G$ dado por $\eta(x,y) := (x, x -_G y)$, $x, y\colon A \to B$, $B \in \underline{\mathrm{FI}}_k$. □

Se define la *dimensión* de un k-grupo formal liso G como sigue ([25], Chap. I, §9.6)

$$\dim G := \dim G_{\bar{k}} := \dim_{\bar{k}}\, t^*_{G_{\bar{k}}}(\bar{k}).$$

Por el teorema 1.4 se tiene $G^0 = \mathrm{Spf}(k[[\mathbf{X}]])$ y $G^0_{\bar{k}} = \mathrm{Spf}(\bar{k}[[\mathbf{X}]])$. Así

$$\dim G = \dim G^0 = \text{nº de variables en } k[[\mathbf{X}]]\ (\leq \infty) \tag{1.2}$$

Si $k = \bar{k}$ (perfecto de característica p) y φ es el Fröbenius (absoluto) de k, para $G = \mathrm{Spf}(A) \in \mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$ considérese la k-álgebra $(k \xrightarrow{\varphi^{-1}} k \to A) =: A^{(p)}$, de anillo subyacente A, de forma que así el Fröbenius de A sea un homomorfismo de k-álgebras $F_A\colon A^{(p)} \to A$, $F_A(a) = a^p$. Así F_A es un morfismo en $\underline{k\text{-}\widehat{\mathrm{Hopf}}}$, y por lo tanto

$$F_G := \mathrm{Spf}(F_A)\colon G \to G^{(p)} := \mathrm{Spf}(A^{(p)})$$

es un morfismo en $\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$, llamado *morfismo de Fröbenius* de G. Sea $V_G\colon G^{(p)} \to G$ el obtenido de F_G por dualidad de Cartier, y $V_A\colon A \to A^{(p)}$ su correspondiente (ver [25], Chap. I, §§7.4 y 7.5). Sea F^n_G, $n \geq 0$, la composición

$$G \xrightarrow{F_G} G^{(p)} \xrightarrow{F_{G^{(p)}}} (G^{(p)})^{(p)} =: G^{(p^2)} \to \cdots \to G^{(p^n)} := (G^{(p^{n-1})})^{(p)}.$$

Así, teniendo en cuenta la nota 1.6.2, claramente

$$\ker F^n_G = \mathrm{Spf}(A/Cl(A^{+p^n})). \tag{1.3}$$

Proposición 1.8. *En la situación anterior se tiene*

(a) $V_G F_G = p1_G$, $F_G V_G = p1_{G^{(p)}}$ ([25], Chap. I §§7.4 y 7.5).

(b) $G^0 = \varinjlim \ker F^n_G$ (de (1.3) y de la proposición 1.5, ver [25], Chap. I §7.4).

(c) *Si G es liso, entonces* $\dim G < \infty$ *si y solo si* $\ker F_G$ *es un esquema en grupos finito* (de (1.3)). *En este caso* $|\ker F^n_G| = p^{nd}$. ([25], Chap. I §9.6).

(d) *G es liso si y solo si F_A es inyectiva* ([25], Chap. I, Théorème 1 y §9.6) *si y solo si F_G es epimorfismo* (por la proposición 1.3) *si y solo si F_G es conúcleo* (por el teorema 1.2) *si y solo si F_G es sobreyectivo y topológicamente plano* (por el teorema 1.1). *Por* (a)*, esto se tiene, en particular, si $p1_G$ es epimorfismo.*

(e) *$p1_G$ es isogenia si y solo si F_G y V_G son isogenias* (inmediato de lo anterior). □

1.1.3. *Grupos de Lie formales* ([41], [63]). Supongamos ahora que k es *local noetheriano completo*. Se define *grupo de Lie formal* sobre k como un k-grupo formal liso, conexo y de dimensión finita. Así, si G es un grupo de Lie formal, entonces (teorema 1.4) se tiene

$$G = \mathrm{Spf}(k[[X_1, \ldots, X_d]]),\ d = \dim G < \infty$$

(ver (1.2)), y entonces $k[[\mathbf{X}]] := k[[X_1, \ldots, X_d]] \in \underline{k\text{-}\widehat{\mathrm{Hopf}}}$. Por lo tanto dar una estructura de grupo de Lie formal sobre k, ie, dar una comultiplicación

$$\Delta\colon k[[\mathbf{X}]] \to k[[\mathbf{X}]]\,\hat{\otimes}_k k[[\mathbf{X}]] = k[[\mathbf{X}, \mathbf{Y}]]$$

con los axiomas de k-álgebra de Hopf formal (1.1.2), equivale a dar una familia de series de potencias formales $F(\mathbf{X}, \mathbf{Y}) \in k[[\mathbf{X}, \mathbf{Y}]]^d$ en $2d$ variables ($F_i := \Delta(X_i)$) verificando

$$F(\mathbf{X}, F(\mathbf{Y}, \mathbf{Z})) = F(F(\mathbf{X}, \mathbf{Y}), \mathbf{Z}) \text{ (asociativa)}$$
$$F(0, \mathbf{X}) = F(\mathbf{X}, 0) = \mathbf{X} \text{ (neutro)}$$
$$F(\mathbf{X}, \mathbf{Y}) = F(\mathbf{Y}, \mathbf{X}) \text{ (conmutativa)}.$$

Se deduce la ley del inverso, así como que $F(\mathbf{X}, \mathbf{Y}) = \mathbf{X} + \mathbf{Y}$ (mód deg 2). Una tal familia se denomina *ley de grupo formal* sobre k. En otros términos

Proposición 1.9. *Se tiene una equivalencia*

$$\underline{\mathrm{FLG}}_k \ \simeq\ \underline{\mathrm{FGL}}_k$$

entre las categorías de grupos de Lie formales y de leyes de grupo formal. □

Bajo la equivalencia de la proposición 1.9 se sigue que un morfismo $f\colon F \to F'$ en $\underline{\mathrm{FGL}}_k$ resulta ser una familia $f(\mathbf{X}) \in k[[\mathbf{X}]]_0^{d'}$ ($d' = \dim F'$) tal que $fF(\mathbf{X}, \mathbf{Y}) = F'(f(\mathbf{X}), f(\mathbf{Y}))$. Se tiene $[n]_F(\mathbf{X}) = n1_F = \mathbf{X} +_F \overset{n)}{\cdots} +_F \mathbf{X}$, $n \geq 0$.

Ejemplo 1.2. 1. Los esquemas en grupos ordinarios aditivo y multiplicativo $\mathbb{G}_a$ y $\mathbb{G}_m$ (ejemplo 1.1), vistos como funtores, son $\mathbb{G}_a(R) = R$, $\mathbb{G}_m(R) = \mathcal{U}(R)$ (unidades de R), $R \in \underline{k\text{-álg}}$. Como leyes de grupo formal son $\mathbb{G}_a = \mathrm{Spec}\ k[X]$, $\mathbb{G}_a = X + Y \in k[X, Y]$, y $\mathbb{G}_m = \mathrm{Spec}\ k[X]$, $\mathbb{G}_m = X + Y + XY = (1 + X)(1 + Y) - 1 \in k[X, Y]$. Por completación formal a lo largo de 0 se tiene

$$\mathbb{G}_a := \hat{\mathbb{G}}_a^0 = \mathrm{Spf}\ k[[X]]\,,\ \mathbb{G}_a = X + Y \in k[[X, Y]]$$
$$\mathbb{G}_m := \hat{\mathbb{G}}_m^0 = \mathrm{Spf}\ k[[X]]\,,\ \mathbb{G}_m = X + Y + XY \in k[[X, Y]]\,.$$

Como funtores formales se tiene $\hat{\mathbb{G}}_a(R) = R$, $\mathbb{G}_a(R) = r(R)$, $R \in \underline{\mathrm{FI}}_k$, y

$$\mathbb{G}_a(B) = \mathfrak{n},\ \mathbb{G}_m(B) = 1 + \mathfrak{n},\ \text{para } B = (B, \mathfrak{n}) \in \underline{\mathrm{FI}}_k\underline{\text{local}}.$$

Para $F \in \underline{\mathrm{FGL}}_k$ se tiene $\mathrm{Hom}_k(F, \mathbb{G}_a) = \ker \partial \subset k[[\mathbf{X}]]_0$, siendo ∂ la de (1.1).

2. Raíces de la unidad: $\mu_n := \ker [n]_{\mathbb{G}_m} = \mathbb{G}_m[n] = \mathrm{Spec}\, k[X]/(X^n - 1)$ es un esquema en grupos finito de orden n.

3. Sea X es un *k-esquema abeliano* d-dimensional (sobre esquemas abelianos ver [57], §V.20), y $X|_0 = \mathrm{Spf}(\hat{A})$ (A es el anillo local de X en 0) la completación formal de X a lo largo de 0 (nota 1.4.3). La multiplicación de X induce en $\hat{A}$ una comultiplicación, y así $X|_0$ es un grupo de Lie formal (teorema 1.4). Por lo tanto $X|_0$ es una ley de grupo formal (proposición 1.9). Esto es análogo, ahora

con series de potencias formales, al origen histórico de las leyes de grupo formal con series de potencias convergentes en un entorno del origen de un grupo de Lie clásico.

Proposición 1.10 ([41], Proposition 18.3.11)**.** *Si k es de distinta característica, entonces $\underline{\mathrm{FGL}}_k \to \underline{\mathrm{FGL}}_{\bar{k}}$ es un funtor fiel.* □

Vamos a considerar a continuación la altura de una ley de grupo formal. Como referencia seguir [41], §§(18.3.1)-(18.3.10) y (28.2). Sea ahora $k = \bar{k}$ un cuerpo perfecto de característica p, y $F \in \underline{\mathrm{FGL}}_k$. Se dice que F es de *altura finita* si $[p]_F : k[[\mathbf{X}]] \to k[[\mathbf{X}]]$ es finito. En este caso es libre (ver, eg, [54], Theorem 23.1), y así se tiene (proposición 1.4)

$$F \text{ es de altura finita si y solo si } [p]_F : F \to F \text{ es isogenia.}$$

El teorema 1.3(a), o también la proposición 1.6, dan que $\deg [p]_F$ es una potencia de p. Se define la *altura* $\mathrm{ht}(F)$ de F de la forma

$$\deg [p]_F =: p^{\mathrm{ht}(F)}.$$

Nota 1.9. (a) De la definición y de la proposición 1.8(a) y (c) se sigue que

$$\dim F \leq \mathrm{ht}(F).$$

(b) Lo que precede valdría para infinitas variables.

En el caso $d = \dim F = 1$, $\mathrm{ht}(F)$ tiene la siguiente interpretación. Sea $f(X)\colon F \to F'$ un morfismo en $\underline{\mathrm{FGL}}_k$. Así $f(X) \equiv 0$ (mód deg 1). Si $f(X) \equiv 0$ (mód deg 2), entonces $f(X) = 0$ ó $f(X) = g(X^{p^n})$ para alguna serie $g \not\equiv 0$ (mód deg 2), [41], §18.3. Se define

$$\mathrm{ht}(f(X)) := \infty \text{ o } h,$$

siendo h máximo para $f(X) = g(X^{p^h})$. Puesto que $[p]_F \equiv pX \equiv 0 \pmod{\deg 2}$, está definida $\mathrm{ht}\,[p]_F$.

Proposición 1.11. *Si $d = 1$, entonces $\mathrm{ht}(F) = \mathrm{ht}\,[p]_F$.*

Demostración. $[p]_F(X) = X^{p^h} u$, $u \in \mathcal{U}(k\left[\left[X^{p^h}\right]\right])$ ($h := \mathrm{ht}\,[p]_F$). Así

$$k[[[p]_F(X)]] = k\left[\left[X^{p^h}\right]\right] \subset k[[X]]\,. \qquad \square$$

Nota 1.10. Para $d \geq 1$ se tiene también $[p]_F = 0$ ó $[p]_F = g(\mathbf{X}^{p^n}) = A_1\mathbf{X}^{p^n} + \cdots$, $A_1 = J([p]_F) \neq 0$ (jacobiano). El mismo argumento que en la proposición 1.11 en cada variable da, eg, $d = 2$, $k[[Y]]\left[\left[a_{11}X^{p^n} + \cdots\right]\right] = k[[Y]]\left[\left[X^{p^n}u\right]\right]$, donde $u \in \mathcal{U}(k\left[\left[X^{p^n}, Y^{p^n}\right]\right])$ si $a_{11} \neq 0$. Pero a_{11} puede ser 0, y así, en general

$$\mathrm{rango}(k[[Y]]\left[\left[X^{p^n}u\right]\right] \subset k[[X,Y]]) \geq p^n, \text{ incluso } \infty.$$

Para cada variable X_i hay un tal n_i. Se ha probado (otra vez) $\dim F \leq \mathrm{ht}(F)$.

Sea ahora de nuevo k un anillo local noetheriano completo de característica 0 y cuerpo residual $\bar{k}$ perfecto de característica $p > 0$. Para $F \in \underline{\mathrm{FGL}}_k$ se define

la *altura* de F como

$$\mathrm{ht}(F) := \mathrm{ht}(F_{\bar{k}}) \ (\geq \dim F).$$

Así del caso residual se obtiene

Proposición 1.12. *En la situación anterior se tiene*

$$\mathrm{ht}(F) < \infty \text{ si y solo si } [p]_F : F \to F \text{ es isogenia.}$$

En este caso $\deg [p]_F = p^{\mathrm{ht}(F)}$. □

1.2. Grupos p-divisibles (o de Barsotti-Tate)

Los grupos p-divisibles constituyen una clase especial de grupos formales cuya importancia se debe en buena parte a que están asociados de forma natural a las variedades y esquemas abelianos. Fueron utilizados (en Geometría Algebraica aritmética) en [67] en teoría Hodge p-ádica, y por Grothendieck y Fontaine en un primer paso hacia los teoremas de comparación de períodos p-ádicos para esquemas propios y lisos (ver la introducción a §2.1). Han sido utilizados también por Faltings (1983) al probar la conjetura de Mordell (1922). Además, como ya se apuntó y a diferencia de otros grupos formales, tienen una teoría de dualidad. Grothendieck en [36] los denominó de "Barsotti-Tate" puesto que el término "p-divisible" vale para cualquier objeto grupo en una categoría, y no muestra su relación con la Geometría Algebraica.

Los grupos p-divisibles con estructura de módulo formal van a ser la base sobre la que vamos a establecer la teoría de períodos π-ádicos y las fórmulas explícitas buscadas.

1.2.1. Sea ahora k un *anillo conmutativo* (*local noetheriano completo* cuando estén involucrados grupos formales) y *fijemos en toda la sección un número primo* p. Sea G un esquema en grupos (respectivamente un grupo formal) sobre k. Se define la *p-torsión* de G como

$$G[p^\infty] := \underset{\rightarrow}{\cup} G[p^n] = \varinjlim G[p^n] = \mathrm{Spec}(A) \text{ o } \mathrm{Spf}(A),$$

siendo $A = \varprojlim A_n$, $G[p^n] := \mathrm{Spec}(A_n)$ (o $\mathrm{Spf}(A_n)$).

Si $G[p^\infty] = G$ se dice que G es un *esquema p-grupo* (o un *p-grupo formal*) sobre k. Es inmediato que esto equivale a que $G(R)$ es p-grupo ordinario para cada k-álgebra (o k-álgebra finí) R.

Sea h un entero ≥ 0. Un grupo *p-divisible* sobre k de *altura* h (ver [67], §2.1) es un sistema inductivo $G = (G_n, i_n),\ n \geq 0$, tal que

(a) G_n es un k-esquema en grupos finito y $|G_n| = p^{hn}$.

(b) Para cada $n \geq 0$ es exacta la sucesión $0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{[p^n]_{G_{n+1}}} G_{n+1}$ (es decir, $G_n = G_{n+1}[p^n]$).

Denotemos $\underline{p\text{-div}}_k$ la categoría de grupos p-divisibles sobre k.

Nota 1.11. 1. Sea ahora, en general, $G = (G_n)$ un sistema inductivo cualquiera de grupos formales $G_n = \mathrm{Spf}(A_n)$. Vamos a denotar también

$$G := \varinjlim G_n = \mathrm{Spf}(A),\ \ A := \varprojlim A_n.$$

Sea G un k-esquema en grupos (no necesariamente afín) o un k-grupo formal y considérese el sistema inductivo

$$G(p) := (G[p^n]).$$

En el caso de que los $G[p^n]$ sean finitos se tiene $G[p^n] = \mathrm{Spec}(A_n) = \mathrm{Spf}(A_n)$. Así, se tiene también $G(p) := \varinjlim G[p^n] = \mathrm{Spf}(A)$. Para la p-torsión $G[p^\infty] = \mathrm{Spec}(A)$ ó $\mathrm{Spf}(A)$, se tiene $G[p^\infty] = G(p)$ en el caso formal.

2. $G(p)$ es un grupo p-divisible si y solo si existe $h \geq 0$ tal que $|G[p^n]\,| = p^{hn}$. Esto ocurre al menos en los siguientes casos

(a) Si $G = \mathbb{G}_m$. Así $\mathbb{G}_m(p) = (\mu_{p^n})$, $|\mu_{p^n}| = p^n$, $h = 1$.

(b) Si G es un k-esquema abeliano d-dimensional. Entonces $|G[m]\,| = m^{2d}$, $h = 2d$. Además $G[m]$ es étale si m no es divisible por ninguna característica residual de k (ver [57], §V.20.7). Se sigue que $G(p)$ es un grupo p-divisible sobre k de altura $2d$ (ver el ejemplo 1.3(d)).

(c) Si $[p]_G : G \to G$ es isogenia. En efecto, $|G[p]\,| = p^h$ por la proposición 1.6. Se sigue que $|G[p^n]\,| = p^{hn}$ como se ve en el diagrama

$$\begin{array}{ccccc} G[p] & \rightarrowtail & G\big[p^{n+1}\big] & \xrightarrow{p} & G[p^n] \longrightarrow 0 \\ \big\downarrow & \blacksquare & \big\downarrow & \blacksquare & \big\downarrow \\ G & \xrightarrow[p]{} & G & \xrightarrow[p^n]{} & G \end{array}$$

3. (Ver [67], §2.1). Para $n, m \geq 0$ se tiene $|G_{m+n}| = |G_m| \cdot |G_n|$ por (a) de la definición de grupo p-divisible, y así una sucesión exacta

$$0 \to G_m \xrightarrow{i_{mn}} G_{m+n} \xrightarrow{j_{mn}} G_n \to 0,$$

donde i_{mn} se obtiene de los $i_n : G_n \to G_{n+1}$ ((b) de la definición de p-divisible) por iteración y j_{mn} es el único morfismo tal que es conmutativo el triángulo

$$\begin{array}{ccc} & G_n & \\ {\scriptstyle j_{mn}}\swarrow & & \searrow{\scriptstyle i_{nm}} \\ G_{m+n} & \xrightarrow[[p^m]_G]{} & G_{m+n} \end{array}$$

Proposición 1.13. *La definición de grupo p-divisible sobre k equivale a la siguiente: un p-grupo formal G sobre k tal que $[p]_G : G \to G$ es isogenia.*

Demostración. [20], p. 45 (para k cuerpo) y [63], p. 61. Para G como en el enunciado se tiene que $G(p)$ es p-divisible usando la nota 1.11.2(c). Además este $G(p)$ da el grupo G de partida (en la notación de la nota 1.11.1) ya que éste es p-grupo. Recíprocamente, si $G = (G_n)$ es p-divisible, sea $G = \varinjlim G_n = \varinjlim G[p^n]$, que es un p-grupo formal (ver la nota 1.3.4). Que $[p]_G : G \to G$ es un conúcleo se sigue de que $([p]_G : G \to G) = \varinjlim(j_n : G_{n+1} \to G_n)$ y de la nota 1.11.3. (Para esta segunda parte ver también la demostración directa de [39], (2.2.2)). □

Nota 1.12. Un grupo p-divisible es topológicamente plano, ie, si $G = \mathrm{Spf}(A)$, entonces $A \cong k^I$ en k-Mod.profiní (ver el argumento de [67], p. 163).

Proposición 1.14. (a) *Si $k \to k'$ es un homomorfismo local de anillos locales noetherianos completos y $G \in \underline{p\text{-div}}_k$, entonces $G_{k'} \in \underline{p\text{-div}}_{k'}$.*

(b) *Si $0 \to G' \to G \to G'' \to 0$ es una sucesión exacta de grupos formales y si G' y $G \in \underline{p\text{-div}}_k$, entonces $G'' \in \underline{p\text{-div}}_k$. Y también, si G' y $G'' \in \underline{p\text{-div}}_k$, entonces $G \in \underline{p\text{-div}}_k$.*

(c) *Sea $G = (G_n) \in \underline{p\text{-div}}_k$. Denotemos $G^0 := (G_n^0)$ y $G^{et} := (G_n^{et})$. Entonces $G^0, G^{et} \in \underline{p\text{-div}}_k$. Además G^0 y G^{et} son la componente conexa y el cociente étale de G, ahora como grupo formal (ie, son compatibles con la equivalencia de la* proposición 1.13*).*

Demostración. (b) Ver [56], §I.2.4. (c) Que G^0 y $G^{et} \in \underline{p\text{-div}}_k$ es obvio de las definiciones. El resto basta probarlo para el cociente étale, ie, $\varinjlim G_n^{et} = G^{et}$, lo que también se sigue de las definiciones. □

1.2.2. Un resultado fundamental se refiere a la relación de los grupos p-divisibles con los grupos de Lie formales. Supongamos ahora que k es *local noetheriano completo de cuerpo residual $\bar{k}$ de característica $p > 0$.*

Teorema 1.5 (Serre-Tate)**.** *El funtor $G \mapsto G(p)$ establece una equivalencia de categorías*

$$\underline{\mathrm{FLG}}_k\underline{\mathrm{ht} < \infty} \;\simeq\; \underline{p\text{-div}}_k\underline{\mathrm{conexo}}.$$

Su inverso es $G = (G_n) \mapsto G = \varinjlim G_n$ (notación de la nota 1.11.1)*.*

Demostración. [67], Proposition 1 (esbozo), o [56], Theorem (2.1.8). □

Nota 1.13. 1. La demostración del teorema 1.5 puede ser obtenida también sobre la base de [25], Chap. I, Théorème 1. Sea $G \in \underline{\mathrm{FLG}}_k\underline{\mathrm{ht} < \infty}$ y $G(p) = (G[p^n])$ (nota 1.11.1 y 1.11.2(c)). Así $G(p)$ es p-divisible por la nota 1.11.2(c). Además $G[p^n]$ es conexo al serlo G. Por lo tanto $G(p)$ es conexo.

Se tiene $\mathrm{Spf}(k[[\mathbf{X}]]) = G = \varinjlim G[p^n] = \varinjlim \mathrm{Spec}(k[[\mathbf{X}]]/(p^n)^*(\mathbf{X}))$ (nota 1.6.2), y así $k[[\mathbf{X}]] \cong \varprojlim k[[\mathbf{X}]]/(p^n)^*(\mathbf{X})$. Se deduce que el funtor $G \mapsto G(p)$ es fiel y pleno.

Sea ahora $G = (G_n) \in \underline{p\text{-div}}_k\underline{\mathrm{conexo}}$ y el grupo formal $G = \varinjlim G_n$ (notación de la nota 1.11.1). Así G es conexo (proposición 1.14(c)). Ahora el teorema 1.4 da (además de la versión original en leyes de grupo formal de este teorema 1.5) una reducción inmediata al caso $k = \bar{k}$. Bastaría pues probar que "$G_{\bar{k}}$ es liso" (en este caso, que la altura es finita se sigue de que $[p]_G : G \to G$ es isogenia (proposición 1.13) y de la proposición 1.12, y así $\dim G < \infty$ por la nota 1.9). Esto se sigue de la proposición 1.8.(d).

Para la demostración del teorema 1.5 ver también [64], Theorem 70.

2. Nótese que las alturas a uno y otro lado de la equivalencia del teorema 1.5 coinciden ya que $p^{\mathrm{ht}(G)} = |G[p]|$ (proposición 1.12) $= p^h$ ((a) de la definición de grupo p-divisible).

Corolario 1.1. (a) *Si $G \in \underline{\mathrm{FLG}}_k\underline{\mathrm{ht} < \infty}$, entonces G es un p-grupo formal.*

(b) *$G \in \underline{p\text{-div}}_k$ si y solo si $G \in p\text{-Gr}\underline{\widehat{\mathrm{Sch}}_k}\underline{\mathrm{liso}}$ tal que $G_{\bar{k}} \in \underline{p\text{-div}}_{\bar{k}}$. En particular, en $\underline{p\text{-div}}_k$ está definida la dimensión y es finita.*

Demostración. (a) Se sigue del teorema 1.5 y de la proposición 1.13.

(b) Si $G \in \underline{p\text{-div}}_k$, entonces G es topológicamente plano (nota 1.12). Al ser G^0 liso (por el teorema 1.5) se tiene que G es liso por el teorema 1.4. Recíprocamente, por el teorema 1.5 se sigue que G^0 es p-divisible sobre k puesto que $\operatorname{ht} G^0 \leq \operatorname{ht} G_{\bar{k}}$ (la proposición 1.12 y la nota 1.13.2) $< \infty$. Por la proposición 1.14(b) basta probar que $G^{et} \in \underline{p\text{-div}}_k$. Esto se sigue de la proposición 1.5(a). (Ver también [25], p. 186). □

Se va a extender la dualidad de Cartier para esquemas en grupos finitos (1.1.2) a grupos p-divisibles. Sea $G = (G_n) \in \underline{p\text{-div}}_k$ y la factorización única $i_n j_n = [p]_G$ (nota 1.11.3). Se define el *dual de Cartier*: $G^D := (G_n^D, j_n^D) \in \underline{p\text{-div}}_k$.

Proposición 1.15 ([67], Proposition 3)**.** *Para $G \in \underline{p\text{-div}}_k$ se tiene*

$$\dim G + \dim G^D = \operatorname{ht}(G) = \operatorname{ht}(G^D).$$

(Se tiene así, de nuevo, $\dim G \leq \operatorname{ht}(G)$). □

Ejemplo 1.3. (a) El grupo multiplicativo $\mathbb{G}_m = \mathbb{G}_m(p) = (\mu_{p^n})$ es un grupo p-divisible conexo sobre k de altura y dimensión 1. Su dual $\mathbb{G}_m^D = \mathbb{Q}_p/\mathbb{Z}_p$ es un grupo p-divisible étale de altura 1 y dimensión 0. (Ver la nota 1.11.2(a)).

(b) El grupo aditivo $\mathbb{G}_a$ es un grupo de Lie formal, pero *no es p-divisible sobre k* ya que, en la fibra especial, $[p]_{\mathbb{G}_a} : \mathbb{G}_a \to \mathbb{G}_a$ es 0 (al ser $p\bar{k} = 0$). Se sigue que $\operatorname{ht}(\mathbb{G}_a) = \infty$.

(c) Grupos p-divisibles étale. (En este ejemplo p no denota necesariamente $\operatorname{char} \bar{k}$). Para un grupo p-divisible $G = (G_n)$ sobre k de altura h se tiene: G es étale si y solo si $G_n(\bar{k}) \cong (\mathbb{Z}/p^n\mathbb{Z})^h$(en $G_{\bar{k}}$-$\underline{\text{Mod}}$) si y solo si $G_n \cong (\mathbb{Z}/p^n\mathbb{Z})^h$ si y solo si $G_n \in \underline{\text{Ab}}$ (esto se sigue del teorema 1.3(b), y de la definición de grupo p-divisible, ver [60], Example 1 y [63], §6, Example (1)). En este caso $G = \varinjlim G_n = (\mathbb{Q}_p/\mathbb{Z}_p)^h$. El grupo $\mathbb{G}_m^D$ es el caso $h = 1$. (Son los conexos los grupos p-divisibles difíciles de describir, teorema 1.5).

Nótese que si $p \neq \operatorname{char} \bar{k}$, entonces cada grupo p-divisible sobre k es étale por el teorema 1.3(a). En particular, si X es un k-esquema abeliano, entonces $X(p)$ es étale, como también se sigue de la nota 1.11.2(b).

(d) Ejemplo motivante, procedente de la Geometría Algebraica ([67], p. 166). Si X es un k-esquema abeliano d-dimensional, entonces $X(p)$ es un grupo p-divisible sobre k de altura $2d$ y dimensión d (nota 1.11.2(b), y para $\dim X(p) = d$ se usa la proposición 1.15, ver también [63], p. 64). Además $X(p)^0 = X|_0$, ie, la componente conexa de $X(p)$ (visto éste como p-grupo formal, la nota 1.11.1 y la proposición 1.13) es la completación formal de X a lo largo de 0 (ver el ejemplo 1.2.3), y es un grupo p-divisible sobre k de altura entre d y $2d$. (Ver también la nota 1.7).

Nota 1.14. Si G es p-divisible sobre k, entonces $\operatorname{Hom}_k(G, \mathbb{G}_a) = 0$. En efecto, en el caso de igual característica, para $f\colon G \to \mathbb{G}_a$ se tiene $f[p]_G = [p]_{\mathbb{G}_a} f = 0f = 0$, y $[p]_G$ es isogenia (uso del teorema 1.5). En el caso de distinta característica se obtiene del resultado para $G_{\bar{k}}$ usando la proposición 1.10.

1.2.3. *Grupo de puntos* ([67]). Sea K un *cuerpo completo discreto* (valor absoluto discreto) *de cuerpo residual* $\bar{k} = k/\pi k$ *de característica* $p > 0$. Sea $C := \widehat{\bar{K}}$ la completación de la clausura algebraica $\bar{K}$ de K, que es un cuerpo algebraicamente cerrado (aunque puede no ser discreto). Para un subcuerpo L de C, denotamos $\mathcal{O}_L$ su anillo de enteros y $\mathfrak{m}_L$ su ideal maximal.

Sea $G \in \mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$ y denotemos $d = \dim G$ si G fuese liso. Para cada $R \in \underline{k\text{-álg.compl.linealT}_2}$ se tiene el grupo de puntos $G(R) \in \underline{\mathrm{Ab}}$ (ver la nota 1.6.1). Así, para cualquier extensión algebraica $L|K$ está definido

$$G(\mathcal{O}_L) := \varinjlim G(\mathcal{O}_E),\ E|K \text{ subextensión finita de } L|K. \tag{1.4}$$

(Nótese que $\mathcal{O}_E$ es profiní, pero $\mathcal{O}_L$ no es completo). Sin embargo los grupos $G(\mathcal{O}_E)$ no son "geométricos" (puntos) en el sentido de que no viven en el espacio afín E^d, tal como sí ocurre en el caso de leyes de grupo formal.

Consideremos el caso $G \in \underline{\mathrm{FGL}}_k$. En este caso, para $R \in \underline{k\text{-álg.compl.linealT}_2}$ se tiene la inclusión

$$G(R) = \mathrm{Hom}_{\mathrm{Top}\underline{k\text{-álg}}}(k[[\mathbf{X}]], R) \subset R^d. \tag{1.5}$$

Así $G(R)$ se identifica en R^d al dominio de convergencia de todo $k[[\mathbf{X}]]$. Éste es el dominio de convergencia en R^d de todo $\underline{\mathrm{FGL}}_k$, en el cual G define una estructura de grupo

$$x +_G y := G(x, y) = \binom{x}{y} G,\ x, y \in G(R). \tag{1.6}$$

siendo esta última la operación que G define en (1.5) (ver la nota 1.6.1). Así *ambas construcciones* (1.5), (1.6) *del grupo* (de puntos) $G(R)$ *se identifican*. De hecho en el caso de que R sea una k-álgebra J-ádica se tiene

$$G(J) := G(R) = (J^d, +_G) \in \underline{\mathrm{Ab}} \tag{1.7}$$

(tomando como ideal de definición $J = r(R) = \{\text{elementos topológicamente nilpotentes de } R\}$). Un caso especialmente interesante de (1.7) va a ser el de la nota 2.9. En particular, para $L|K$ algebraica, y para la completación $\hat{L}(\subset C)$ se tiene

$$\begin{aligned} &G(\mathfrak{m}_{\hat{L}}) = G(\mathfrak{m}_{\hat{L}}^d, +_G) \\ &G(\mathfrak{m}_L) := G(\mathcal{O}_L) = \varinjlim G(\mathcal{O}_E) = \varinjlim (\mathfrak{m}_E^d, +_G) = (\mathfrak{m}_L^d, +_G) \end{aligned}$$

Así, aún no siendo L completo, la definición (1.4) es consistente con la de (1.7): $G(\mathfrak{m}_L) = G(\mathfrak{m}_{\hat{L}}) \cap L = G(\mathfrak{m}_C) \cap L$.

Sea $f\colon G \to G'$ un morfismo en $\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_k$ tal que $G \in \underline{\mathrm{FGL}}_k$. Aunque $\ker f$ no es una ley de grupo formal (se pierde la lisitud), se tienen sucesiones exactas (ver la nota 1.6.2)

$$\begin{aligned} &0 \to (\ker f)(\mathfrak{m}_L) \to G(\mathfrak{m}_L)(= \mathfrak{m}_L^d) \to G'(\mathfrak{m}_L) \\ &0 \to (\ker f)(\mathfrak{m}_{\hat{L}}) \to G(\mathfrak{m}_{\hat{L}})(= \mathfrak{m}_{\hat{L}}^d) \to G'(\mathfrak{m}_{\hat{L}}) \end{aligned} \tag{1.8}$$

Pero un grupo p-divisible $G = \varinjlim G_n = \mathrm{Spf}(A)$, $G_n = \mathrm{Spec}(A_n)$, $A = \varprojlim A_n$ puede no ser conexo, ie, no ser ley de grupo formal. Así, en cualquier caso, se

define (como en (1.1.1)), y se tiene

$$G(\mathcal{O}_{\hat{L}}) := \mathrm{Hom}_{\mathrm{Top}\underline{k\text{-álg}}}(A, \mathcal{O}_{\hat{L}}) = \varprojlim_i \varinjlim_n \mathrm{Hom}_{\underline{k\text{-álg}}}(A_n, \mathcal{O}_{\hat{L}}/\pi^i\mathcal{O}_{\hat{L}})$$
$$= \varprojlim_i \varinjlim_n G_n(\mathcal{O}_{\hat{L}}/\pi^i\mathcal{O}_{\hat{L}}) = \varprojlim_i G(\mathcal{O}_{\hat{L}}/\pi^i\mathcal{O}_{\hat{L}}).$$

Es claramente un $\mathbb{Z}_p$-módulo y se denomina *grupo de puntos de G con valores en $\hat{L}$*. Nótese que *esta definición de $G(\mathcal{O}_{\hat{L}^i})$ es consistente con las* (1.5) y (1.7). Respecto a la torsión, puesto que $G_n(\mathcal{O}_{\hat{L}}) = (0\colon p^n)_{G(\mathcal{O}_{\hat{L}})}$ (nota 1.6.2), se tiene

$$t\,(G(\mathcal{O}_{\hat{L}})) = \varinjlim G_n(\mathcal{O}_{\hat{L}}). \tag{1.9}$$

Si G es étale, entonces $G(\mathcal{O}_{\hat{L}})$ es un grupo de torsión (al ser $G_n(\mathcal{O}_{\hat{L}}/\pi^{i+1}\mathcal{O}_{\hat{L}}) \cong G_n(\mathcal{O}_{\hat{L}}/\pi^i\mathcal{O}_{\hat{L}})$). Si G es conexo, entonces $A = k[[\mathbf{X}]]$, y así el $G(\mathcal{O}_{\hat{L}})$ actual es un caso de (1.7) (como ya se había observado).

Proposición 1.16 ([67], Proposition 4)**.** *Si $\bar{k}$ es perfecto y $G \in \underline{p\text{-div}}_k$, entonces $G \twoheadrightarrow G^{et}$ tiene una sección, y así $G = \mathrm{Spf}(A^{et}[[\mathbf{X}]])$, denotando $G^{et} =: \mathrm{Spf}(A^{et})$. Se tiene entonces que*

$$0 \to G^0(\mathcal{O}_{\hat{L}}) \to G(\mathcal{O}_{\hat{L}}) \to G^{et}(\mathcal{O}_{\hat{L}}) \to 0.$$

es exacta. Se sigue que $G(\mathcal{O}_C)$ es un grupo divisible.

Demostración. Se apoya en la proposición 1.5(c). Detalles del levantamiento $G = \mathrm{Spf}(A^{et}[[\mathbf{X}]])$ pueden verse en [39], §4. Ver también [63], p. 68. □

1.2.4. *El (co-)módulo de Tate* ([67], pp. 168 y 169).

Proposición 1.17. *Sea H un subgrupo finito de $G \in \underline{p\text{-div}}_k$. Entonces*

$$H(\mathcal{O}_C) = H(\mathcal{O}_L) = H(L) \text{ para } L >> K \text{ (finita).}$$

En particular, si $G \in \underline{\mathrm{FGL}}_k$, entonces $H(\mathcal{O}_C) = H(\mathcal{O}_L) \subset (\mathfrak{m}_L^d, +_G)$ (ver (1.7) y (1.8))*, y así las componentes (en $\mathfrak{m}_L^d$) de los elementos de $H(\mathcal{O}_C)$ son enteras sobre k (algebraicas sobre K, ie, $K(H(\mathcal{O}_C))$ es finita sobre K).*

Demostración. Denotando por B el álgebra afín de H, para $y \in H(\mathcal{O}_C) = \mathrm{Hom}_{\underline{k\text{-álg}}}(B, \mathcal{O}_C)$ se tiene que el álgebra $k \to B \to y(B)$ es finita y, por lo tanto, entera. Se sigue, para $L := K(y(B),\ y \in H(\mathcal{O}_C))$, finita sobre K, que $H(\mathcal{O}_C) = H(\mathcal{O}_L) = H(L)$ (la última igualdad usando de nuevo que $k \to B$ es entera). □

Supongamos ahora que $\mathrm{char}\, K = 0$ *y que $\bar{k}$ es perfecto*, y sea $G = \varinjlim G_n$ un grupo p-divisible sobre k de altura h. De esta forma se tiene una función logaritmo, $\log\colon G(\mathcal{O}_{\hat{L}}) \to t_G(\hat{L})$, que es sobreyectiva para $\hat{L} = C$ (por la proposición 1.16), y que induce un isomorfismo de $\hat{L}$-espacios vectoriales

$$\log\colon G(\mathcal{O}_{\hat{L}}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong t_G(\hat{L})\ (\cong \hat{L}^d,\ d = \dim G).$$

Además, $G \times_k K$ es étale por el teorema 1.3(a). Usando ahora el ejemplo 1.3(c) para K y la proposición 1.17, se tiene un isomorfismo canónico

$$G_n(\mathcal{O}_{\hat{L}}) \cong (\mathbb{Z}/p^n\mathbb{Z})^h \in G_K\text{-}\underline{\mathrm{Mod.discr}} \tag{1.10}$$

para $L >> K$ (dependiendo de n), donde $G_K := G(\bar{K}/K)$ es el grupo de Galois absoluto de K.

Se definen el *comódulo y el módulo de Tate*, respectivamente, como

$$\Phi(G) := \varinjlim G_n(\bar{K}) \text{ respecto a } i_n \colon G_n \to G_{n+1}$$
$$T(G) := \varprojlim G_n(\bar{K}) \text{ respecto a } j_n \colon G_{n+1} \to G_n.$$

Por la proposición 1.17 se tiene

$$G[p^n] := G[p^n](\mathcal{O}_C) = (0 \colon p^n)_{G(\mathcal{O}_C)} = G_n(\mathcal{O}_C) = G_n(\bar{K}).$$

Por lo tanto de (1.10) se sigue que

$$\Phi(G) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h \quad \text{y} \quad T(G) \cong \mathbb{Z}_p^h \tag{1.11}$$

Así $\Phi(G)$ es un grupo p-divisible étale. Además G_K actúa (de forma obvia, la categoría TopG_K-Mod es (co)completa) continuamente sobre ellos, para la topología discreta de $\Phi(G)$ (límite de espacios discretos $\mathbb{Z}/p^n\mathbb{Z}$) y la p-ádica de $T(G)$ (que coincide con la topología producto de la de $\mathbb{Z}_p$). Ie, $\Phi(G)$ *y* $T(G)$ *son representaciones* $\mathbb{Z}_p$*-ádicas de* G_K (sobre éstas ver (2.1.1), más adelante). Usando además (1.9), se tiene

$$\Phi(G) = t\,(G(\mathfrak{m}_C)) = t(\mathfrak{m}_C^d, +_G),$$

la última igualdad si G es conexo. En este caso $K(\Phi(G)) \subset \bar{K}$, de nuevo por la proposición 1.17. Si G es étale, entonces $G(\mathfrak{m}_C) = \Phi(G) = G$ y $T(G) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, G)$.

Ejemplo 1.4. Si $G = \mathbb{G}_m$, entonces $\Phi(\mathbb{G}_m) = \varinjlim \mu_{p^n} = \mu_{p^\infty}$ y $T(\mathbb{G}_m) = \varprojlim \mu_{p^n} = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) =: \mathbb{Z}_p(1)$ $(\cong \mathbb{Z}_p)$ (ver el ejemplo 1.3(a)). Así

$$\mathbb{Z}_p(1) = \left\{\epsilon = (\epsilon_n),\ \epsilon_n \in \mathcal{O}_C,\ \epsilon_0 = 1,\ \epsilon_{n+1}^p = \epsilon_n\right\} = Cl < \epsilon >,$$

la última igualdad si ϵ_1 es una raíz primitiva p-ésima de la unidad. En este caso se dice que ϵ es un *sistema coherente de raíces* p^n*-ésimas de la unidad*.

Nota 1.15. 1. Sea ahora k un anillo local noetheriano completo cualquiera. Sea X un k-esquema abeliano de dimensión d. Para m no divisible por $\mathrm{char}\,\bar{k}$ se tiene que $X[m]$ es étale (nota 1.11.2(b)), y así $|X[m](\bar{\bar{k}})| = m^{2d}$ por el teorema 1.3(b). Puesto que esto vale para $m'|m$ se sigue que $X[m](\bar{\bar{k}}) \cong (\mathbb{Z}/m\mathbb{Z})^{2d}$. Por lo tanto, para el ℓ*-módulo de Tate* de X, $T_\ell(X) := \varprojlim X[\ell^n](\bar{\bar{k}})$, ℓ primo $\neq \mathrm{char}\,\bar{k}$, se tiene $T_\ell(X) \cong \mathbb{Z}_\ell^{2d}$.

Para K ahora como antes de esta nota y $\ell = p$, puesto que $X[m]_K = X_K[m]$, se tiene: $X[m](\bar{K}) = X_K[m](\bar{K}) \cong (\mathbb{Z}/m\mathbb{Z})^{2d}$. Así $T_p(X) := \varprojlim X[m](\bar{K}) = T_p(X_K) = T(X(p)) \cong \mathbb{Z}_p^{2d}$. *Los* $T_\ell(X)$ *(*ℓ *cualquier primo) son representaciones* $\mathbb{Z}_\ell$*-ádicas de* G_K.

2. Si G es un grupo p-divisible sobre un cuerpo K de altura h, y si $p \neq \mathrm{char}\,K$, entonces se tiene análogamente el módulo de Tate $T(G) \cong \mathbb{Z}_p^h$. También, si X es una K-variedad abeliana, entonces $T_p(X) = T(X(p))$.

3. La proposición 1.16 y el logaritmo son el punto de partida para el resultado principal de [67] (su Theorem 4), que establece un funtor fiel y pleno

$$K \times_k - \colon \underline{p\text{-div}}_k \rightarrowtail \underline{p\text{-div}}_K.$$

Puesto que se tiene una equivalencia $T(-)\colon \underline{p\text{-div}}_K \simeq \underline{\mathrm{Rep}_{\mathbb{Z}_p}(G_K)\text{libre}}$ (por el teorema 1.3(a) cada grupo p-divisible sobre K es étale, y entonces la equivalencia se sigue, por paso al límite, de la del teorema 1.3(b), teniendo en cuenta el ejemplo 1.3.(c), o (1.10)) *se tiene un funtor fiel y pleno*

$$T(-)\colon \underline{p\text{-div}}_k \rightarrowtail \underline{\mathrm{Rep}_{\mathbb{Z}_p}(G_K)\text{libre}}.$$

En particular, *cualquiera de los objetos* $T(G)$, $\Phi(G)$ y $K\times_k G$ *determina* G (salvo isomorfismo).

1.3. Teoría de Dieudonné

Fue Dieudonné el primero en ver y realizar la descripción/parametrización de las leyes de grupo formal sobre un cuerpo perfecto de característica p mediante objetos algebraicos del álgebra semilineal.

La teoría de Dieudonné surgió como una variante en característica p de la teoría de Lie que asocia a un esquema en grupos en característica 0 su álgebra de Lie, que es un objeto lineal que describe el esquema en grupos. En el caso de característica p lo paralelo al álgebra de Lie es el llamado *módulo de Dieudonné*, o mejor en su versión contravariante [5], reformulada en [25], Chaps. II y III, que vamos a exponer someramente a continuación.

Los módulos de Dieudonné allanaron el camino a los cristales de Dieudonné (cf. §1.5), y jugaron un papel en la demostración de Wiles del último Teorema de Fermat.

1.3.1. Sea pues $\bar{k}$ un *cuerpo perfecto de característica* p y $W(\bar{k})$ su anillo de vectores de Witt ([61], Chap. II, §6). El homomorfismo canónico $W(\bar{k})\twoheadrightarrow\bar{k}$ tiene una sección multiplicativa, el *representante de Teichmüller*, $[-]:\bar{k}\to W(\bar{k})$, $[a]:=(a,0,0,\ldots)$.

Se trata de asociar a un objeto "geométrico" sobre $\bar{k}$ (en característica p), el grupo formal, un objeto algebraico sobre $W(\bar{k})$ (en característica 0, lo que podría ser visto como el germen de la cohomología cristalina).

El Fröbenius (absoluto) φ de $\bar{k}$ tiene un único levantamiento continuo

$$\varphi\colon W(\bar{k})\to W(\bar{k}),\ \underline{a}^{\varphi}=(a_0,a_1,\ldots)^{\varphi}:=(a_o^p,a_1^p,\ldots).$$

Por otra parte se tiene el homomorfismo aditivo, llamado *Verschiebung* (o decalage)

$$V\colon W(\bar{k})\to W(\bar{k}),\ V\underline{a}=V(a_0,a_1,\ldots)=(0,a_0,a_1,\ldots).$$

Las propiedades de φ y V se sistematizan mediante la construcción del llamado *anillo de Dieudonné* ([25], Chap. II §2.2)

$$D_{\bar{k}}:=W(\bar{k})[\underline{F},\underline{V}]\,,$$

anillo de polinomios no conmutativos, dado por las relaciones $\underline{F}\,\underline{V}=\underline{V}\,\underline{F}=p$, $\underline{F}\,\underline{a}=\underline{a}^{\varphi}\underline{F}$ y $\underline{a}\,\underline{V}=\underline{V}\,\underline{a}^{\varphi}$. Así "$W(\bar{k})$ es un $D_{\bar{k}}$-módulo (izquierda)" (mediante las aplicaciones φ y V). En general se tiene

(a) Si $M\in D_{\bar{k}}\text{-}\underline{\mathrm{Mod}}$, entonces $M\in W(\bar{k})[\underline{F}]\text{-}\underline{\mathrm{Mod}}$ y $\underline{F}M\supset pM$.

(b) Si $M \in W(\bar{k})[\underline{F}]\text{-}\underline{\text{Mod}}$, $\underline{F}\colon M \rightarrowtail M$ es inyectiva y $\underline{F}M \supset pM$, entonces $M \in D_{\bar{k}}\text{-}\underline{\text{Mod}}$.

(c) $M \in D_{\bar{k}}\text{-}\underline{\text{Mod}}$, $W(\bar{k})$-libre de tipo finito si y solo si $M \in W(\bar{k})[\underline{F}]\,\underline{\text{-Mod}}$, $W(\bar{k})$-libre de tipo finito, $\underline{F}\colon M \to M$ es inyectiva y $\underline{F}M \supset pM$.

La construcción en [25] del módulo de Dieudonné de un $\bar{k}$-grupo formal está basada en la de los covectores de Witt. Para un anillo R se define

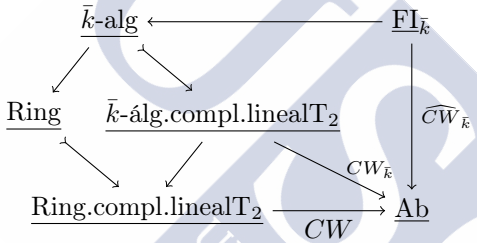
$$CW(R) := \{(\ldots, a_{-1}, a_0) \in R^{\mathbb{N}}, \text{ tales que el ideal generado por } \ldots, a_{-r-1}, a_{-r} \text{ es nilpotente para } r >> 0\}$$

Proposición 1.18 ([25], Proposition II.1.4)**.** *$CW(R)$ tiene una estructura natural de grupo abeliano topológico.* □

Si ahora R es un anillo topológico lineal completo Hausdorff, entonces la construcción anterior se extiende de la forma

$$CW(R) := \varprojlim CW(R/I). \tag{1.12}$$

Se tiene el siguiente diagrama funtorial (uso de la proposición 1.18)



Así $\widehat{CW}_{\bar{k}}$ es la completación formal del $\bar{k}$-funtor $CW_{\bar{k}}$. Se denominan, respectivamente, (los funtores) *grupo formal, y grupo, de los covectores de Witt.*

Proposición 1.19. *$\widehat{CW}_{\bar{k}}\colon \underline{\text{FI}}_{\bar{k}} \to \underline{\text{Ab}}$ es un p-grupo formal liso. Está representado por la completación profiní $\widehat{B^0_{\bar{k}}}$ de $\mathbb{Z}^0[[\mathbf{X}]] \hat{\otimes} k$, donde*

$$\mathbb{Z}^0[[\mathbf{X}]] = \varprojlim \mathbb{Z}[\ldots, X_{-1}, X_0]/(\ldots, X_{r+1}, X_r)^s.$$

El isomorfismo $\widehat{CW}_{\bar{k}}(R) \cong \text{Hom}_{\underline{\text{PRO}}_{\bar{k}}}(\widehat{B^0_{\bar{k}}}, R)$, $R \in \underline{\text{FI}}_{\bar{k}}$, está dado por

$$\underline{a} \in \widehat{CW}_{\bar{k}}(R) \leftrightarrow [X_{-n} \mapsto a_{-n} \in R] = \underline{a} \in \text{Hom}_{\underline{\text{PRO}}_{\bar{k}}}(\widehat{B^0_{\bar{k}}}, R).$$

Demostración. Que es grupo formal, representado como se indica, está probado en [25], Chap. II §4.2. Claramente conserva epimorfismos, y así es liso. Que es p-grupo formal se sigue de la proposición 1.20, a continuación. □

Si ahora R es una $\bar{k}$-álgebra, entonces se definen los homomorfismos continuos

$$\varphi\colon CW(R) \to CW(R),\ (\ldots, a_{-1}, a_0)^{\varphi} := (\ldots, a^p_{-1}, a^p_0)$$
$$V\colon CW(R) \to CW(R),\ V(\ldots, a_{-1}, a_0) := \ldots, a_{-2}, a_{-1}).$$

Nota 1.16. $\varphi, V\colon \widehat{CW}_{\bar{k}}(R) = \text{Hom}_{\underline{\text{PRO}}_{\bar{k}}}(\widehat{B^0_{\bar{k}}}, R) \to \text{Hom}_{\underline{\text{PRO}}_{\bar{k}}}(\widehat{B^0_{\bar{k}}}, R) = \widehat{CW}_{\bar{k}}(R)$ están inducidos por $F_{\widehat{B^0_{\bar{k}}}}$, $V_{\widehat{B^0_{\bar{k}}}}\colon \widehat{B^0_{\bar{k}}} \to \widehat{B^0_{\bar{k}}}$ de (1.1.2) [25], Chap. II §4.3, Remarque 1. Así, para $\underline{a} \in \widehat{CW}_{\bar{k}}(R)$, se tiene $(\ldots, a_{-2}, a_{-1}) = V\underline{a} = \text{Spf}(V_{\widehat{B^0_{\bar{k}}}})_R(\underline{a}) = \text{Spf}(\widehat{B^0_{\bar{k}}})(V_R)(\underline{a}) = (\ldots, V_R(a_{-1}), V_R(a_0))$.

Proposición 1.20. (a) *Si R es una $\bar{k}$-álgebra, entonces $CW(R)$ es un $D_{\bar{k}}$-módulo topológico* ($D_{\bar{k}}$ con la topología p-ádica) *de p-torsión. Así $\widehat{CW}_{\bar{k}}$ es p-grupo formal.*

(b) *Si R es una $\bar{k}$-álgebra profiní, entonces $\widehat{CW}_{\bar{k}}(R)$ es un $D_{\bar{k}}$-módulo topológico $W(\bar{k})[\underline{F}]$-módulo topológico lineal y $W(\bar{k})$-módulo* proartiniano (límite inverso de $W(\bar{k})$-módulos artinianos).

Demostración. (a) Ver [25], Proposition II.2.2 y §III.1.1. (b) Ver [25], Proposition II.4.1.(i). □

Las acciones de las variables $\underline{F}$ y $\underline{V}$ de $D_{\bar{k}}$ sobre $CW(R)$ (o $\widehat{CW}_{\bar{k}}(R)$) se denotarán también $\underline{F}$ y $\underline{V}$, o bien φ y V.

1.3.2. *El módulo de Dieudonné.* Sea $G = \mathrm{Spf}(A) \in \mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_{\bar{k}}$. Considerando la proposición 1.19 y el lema de Yoneda se tiene

$$\widehat{CW}_{\bar{k}}(A) = \mathrm{Hom}_{\widehat{\underline{\mathrm{Sch}}}_{\bar{k}}}(G, \widehat{CW}_{\bar{k}}),$$

que es un $D_{\bar{k}}$-módulo (como en la proposición 1.20). En [25], Chap. III §1.2, se define el *módulo de Dieudonné* de G de la forma

$$\underline{M}(G) := \mathrm{Hom}_{\bar{k}}(G, \widehat{CW}_{\bar{k}}),$$

y se tiene

$$\underline{M}(G) = \{\, \underline{a} \in \widehat{CW}_{\bar{k}}(A),\ \partial(\underline{a}) = \underline{a}\hat{\otimes}1 - \Delta(\underline{a}) + 1\hat{\otimes}\underline{a} = 0 \,\} \tag{1.13}$$

(∂ es la de (1.1)). Así $\underline{M}(G)$ es un sub$D_{\bar{k}}$-módulo cerrado de $\widehat{CW}_{\bar{k}}(A)$.

Nota 1.17. $\underline{M}(G)$ esta constituído por covectores de Witt $\underline{a} = (\ldots, a_{-1}, a_0)$. Equivalentemente, por transformaciones naturales $\underline{a}\colon G \Rightarrow \widehat{CW}_{\bar{k}}$, $\underline{a}_R\colon G(R) \to \widehat{CW}_{\bar{k}}(R)$, $R \in \underline{\mathrm{FI}}_{\bar{k}}$.

Sea ahora G un p-grupo formal sobre $\bar{k}$. En este caso $\underline{M}(G) = \varprojlim \underline{M}\,(G[p^n]) = \varprojlim \underline{M}(G)/p^n\underline{M}(G)$.

Proposición 1.21. *Sea $G = \mathrm{Spf}(A) \in p\text{-}\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_{\bar{k}}$. La aplicación $\underline{a} = (\ldots, a_{-1}, a_0) \mapsto a_0$ induce un diagrama conmutativo de filas exactas en* Top$\underline{\bar{k}}$-Vect

$$\begin{array}{ccccccc}
0 & \longrightarrow & \ker V|_{\underline{M}(G)} & \longrightarrow & \underline{M}(G) & \xrightarrow{V} & \underline{M}(G) \\
 & & \cong\downarrow & & \downarrow & & \\
0 & \longrightarrow & t_{G^D}(\bar{k}) \cong \mathrm{Hom}_{\bar{k}}(G, \mathbb{G}_a) & \longrightarrow & A^+ & \xrightarrow{\partial} & A^+ \otimes_k A^+
\end{array}$$

Los isomorfismos son de $\bar{k}[\underline{F}]$-módulos topológicos.

Demostración. El isomorfismo $\mathrm{Hom}_{\bar{k}}(G, \mathbb{G}_a) \cong t_{G^D}(\bar{k})$, para cualquier $G \in \mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_{\bar{k}}$, está en [25], Chap. I §§8.6 y 8.7, así como la fila inferior. Que la aplicación del enunciado induce una k-lineal inyectiva continua $\underline{M}(G) \rightarrowtail A^+$ se sigue de la nota 1.18.2, más adelante. El otro isomorfismo es [25], Proposition III.3.2. □

Proposición 1.22 ([25], Proposition III.4.3)**.** *Sea* $G = \mathrm{Spf}(A) \in p\text{-}\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_{\bar{k}}$. *Se tiene una sucesión exacta de* $D_{\bar{k}}$*-módulos topológicos*

$$0 \to \underline{F}\,\underline{M}(G) \to \underline{M}(G) \xrightarrow{\eta_G} t_G^*(\bar{k}) \to 0,$$

donde $\eta_G(\ldots, a_{-1}, a_0) := \bar{a_0} \in A^+/Cl(A^{+2}) = t_G^*(\bar{k})$. □

El que sigue es (en versión de Fontaine) el resultado principal de la teoría de Dieudonné (donde son usadas las proposiciones 1.21 y 1.22)

Teorema 1.6 ([25], Théorème III.1)**.** *Se tienen equivalencias inversas de categorías*

$$p\text{-}\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_{\bar{k}} \underset{\underline{G}}{\overset{\underline{M}}{\rightleftarrows}} D_{\bar{k}}\text{-}\underline{\mathrm{Mod}}\, W(\bar{k})[\underline{F}]\,\text{-}\underline{\text{profiní}},$$

siendo $\underline{G}(M)(R) := \mathrm{Hom}_{\mathrm{Top}D_{\bar{k}}\text{-}\underline{\mathrm{Mod}}}(\underline{M}, \widehat{CW}_{\bar{k}}(R))$, $R \in \underline{\mathrm{FI}}_{\bar{k}}$. □

Corolario 1.2 ([25], Proposition III.1.2)**.** *Sea* $G \in p\text{-}\mathrm{Gr}\underline{\mathrm{Sch}}_{\bar{k}}\underline{\text{finito}}$. *Para* $R \in \underline{\bar{k}\text{-alg}}$ *se tiene*

$$G(R) \cong \mathrm{Hom}_{D_{\bar{k}}}(\underline{M}(G), CW(R)).$$ □

Nota 1.18. 1. El isomorfismo del corolario 1.2 se define de forma obvia

$$x \in G(R) \mapsto [\underline{a} \in \underline{M}(G) \mapsto \underline{a}_R(x) \in CW(R)]\,.$$

Este es el germen de la *paridad de períodos p-ádicos* de [25] (ver (2.2.1)), que enfrenta a $\underline{M}(G_{\bar{k}})$ y $T(G)$, para G p-divisible sobre k ($T(G)$ juega aquí el papel de la homología singular en la paridad de períodos complejos), ya que $T(G) = \varprojlim G[p^n](\mathfrak{m}_{\bar{K}})$ (ver (1.2.4)).

2. De la nota 1.16 y de (1.13) se sigue que cada $\underline{a} \in \underline{M}(G)$ es de la forma $\underline{a} = (\ldots, V_A^2(a_0), V_A(a_0), a_0)$, $a_0 \in A^+$ ([25], Proposition III.3.1).

Proposición 1.23 ([25], Proposition III.6.1)**.** *Sea* $G \in p\text{-}\mathrm{Gr}\widehat{\underline{\mathrm{Sch}}}_{\bar{k}}$. *Se tiene*

(a) G *es liso si y solo si* $\underline{F}\colon \underline{M}(G) \to \underline{M}(G)$ *es inyectiva.*

(b) G *es conexo si y solo si* $\underline{F}$ *es topológicamente nilpotente sobre* $\underline{M}(G)$ *(ie,* $\underline{M}(G) \in W(\bar{k})[[\underline{F}]]\text{-}\underline{\mathrm{Mod}}$*).*

(c) *Si* G *es liso, entonces* $\dim G < \infty$ *si y solo si* $\dim_{\bar{k}} \underline{M}(G)/\underline{F}\,\underline{M}(G) < \infty$. *En este caso estas dimensiones son iguales.*

(d) $G \in \underline{p\text{-div}}_{\bar{k}}$ *si y solo si* $\underline{M}(G)$ *es* $W(\bar{k})$*-libre. En este caso*

$$\dim G = \dim_{\bar{k}} \underline{M}(G)/\underline{F}\,\underline{M}(G) \le \mathrm{ht}(G) = \mathrm{rango}_{W(\bar{k})} \underline{M}(G) =$$
$$\dim_{\bar{k}} \underline{M}(G)/p\underline{M}(G) = \dim G + \dim_{\bar{k}} \underline{M}(G)/\underline{V}\,\underline{M}(G).$$

(Se obtiene otra vez $\dim G \le \mathrm{ht}(G)$, ahora vía el módulo de Dieudonné). □

1.4. Cohomología de de Rham formal y módulo de Dieudonné

Para formular la teoría de Grothendieck-Cartier-Messing-Fontaine (ver §1.5) vamos a establecer previamente la relación entre el módulo de Dieudonné y la cohomología de de Rham.

1.4.1. Sea K un *cuerpo completo discreto de característica* 0 *y cuerpo residual* $\bar{k} = k/\pi k$ *perfecto de característica* $p > 0$, y sea $K_0 := \mathrm{Frac}(W(\bar{k}))$.

En [25], Chap. II §5.4 se define una *k-álgebra especial local* como una k-álgebra A local profiní, formalmente lisa y de dimensión finita. De otra forma, isomorfa a $\mathcal{O}_L[[\mathbf{X}]]$ ($d < \infty$ variables) para alguna extensión finita no ramificada $L|K$. Se construye la k-álgebra de "funciones analíticas" asociada a A como la completación

$$\hat{A}^{an}_{K_0} := \varprojlim A_{K_0}/J_s,$$

de $A_{K_0} = A \otimes_{W(\bar{k})} K_0 = A \otimes_k K$, siendo J_s ($s \geq 0$) el k-submódulo de A_{K_0} definido por $J_s := \sum_{n=1}^{\infty} \pi^{-n+1}\mathfrak{m}_A^{ns}$. Así $\hat{A}^{an}_{K_0}$ es una K-álgebra topológica (pero la topología sólo es lineal viendo a $\hat{A}^{an}_{K_0}$ como k-módulo).

Si A es una k-álgebra especial local se define el k-submódulo cerrado $P(A)$ de $\hat{A}^{an}_{K_0}$ mediante el cuadrado cartesiano del diagrama

$$\begin{array}{ccccc} A & \rightarrowtail & \hat{A}^{an}_{K_0} & \longrightarrow & L[[\mathbf{X}]] \\ \downarrow{\scriptstyle d} & \searrow & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} \\ \widehat{\Omega}_{A|k} & \longrightarrow & \widehat{\Omega}_{\hat{K}^{an}_{K_0}|k} & \rightarrowtail & \widehat{\Omega}_{L[[\mathbf{X}]]|K} \end{array}$$

en el cual las aplicaciones superiores son inyectivas y continuas. Ver [25], Lemme II.5.3 y Chap. II §5.5. En particular, para $A = k[[\mathbf{X}]]$, se tiene una inclusión continua $\widehat{k[[\mathbf{X}]]}^{an}_{K_0} \subset K[[\mathbf{X}]]$. En este caso se obtiene ([25], Chap. II §5.1)

$$P(k[[\mathbf{X}]]) = \{\lambda(\mathbf{X}) \in K[[\mathbf{X}]]\,,\ \partial\lambda/\partial X_i \in k[[\mathbf{X}]] \text{ para todo } i\}\,. \tag{1.14}$$

Proposición 1.24 ([25], Propositions II.5.4 et II.5.5)**.** *Sea A una k-álgebra especial local.*

(a) *Se tiene una aplicación $W(\bar{k})$-lineal continua*

$$\hat{w}_A \colon CW(A) \to P(A)$$

dada por $\hat{w}_A(\underline{a}) := \sum p^n a_{-n}^{p^n}$.

(b) *En el caso absolutamente no ramificado $K = K_0$, se tiene un diagrama conmutativo*

$$\begin{array}{ccc} CW(A) & \xrightarrow{\hat{w}_A} & P(A) \\ \downarrow & & \downarrow \\ \widehat{CW}_{\bar{k}}(A_{\bar{k}}) & \underset{w_A}{\cong} & P(A)/pA \end{array}$$

Por lo tanto $P(A)/pA$ es un $D_{\bar{k}}$-módulo topológico. La acción de $\underline{F}$ (inducida vía w_A de la de $\widehat{CW}_{\bar{k}}(A_{\bar{k}})$) sobre $P(W(\bar{k})[[\mathbf{X}]])/pW(\bar{k})[[\mathbf{X}]]$ es $\underline{F}\lambda(\mathbf{X}) = \lambda^{\varphi}(\mathbf{X}^p)$ (coherente con el Fröbenius $\lambda(\mathbf{X})^p = \lambda^{\varphi}(\mathbf{X}^p)$ en $\bar{k}[[\mathbf{X}]]$). □

Para extender la proposición 1.24 al caso ramificado, en [25], Chap. IV §§2 y 3 se procede como sigue. Ante todo se construye un funtor apropiado

$$M \in D_{\bar{k}}\text{-}\underline{\mathrm{Mod}} \mapsto M_k \in k\text{-}\underline{\mathrm{Mod}}.$$

Este funtor verifica

(a) $k \otimes_{W(\bar{k})} M \to M_k$ induce un isomorfismo $K \otimes_{W(\bar{k})} M \cong K \otimes_k M_k$
(b) Si $M \cong W(\bar{k})^r$, entonces $M_k/t(M_k) \cong k^r$
(c) $M_{W(\bar{k})} = M$

Sea A una k-álgebra especial local y $P'(A)$ el k-submódulo (va a ser cerrado) de $P(A)$ generado por los $p^{-n}(\pi\alpha)^{p^n}$, $\alpha \in A$, $n \geq 0$. Se tiene que $\pi A \subset P'(A) \subset \pi^\nu A$, siendo $\nu := \min_{n\geq 0}\{p^n - ne\} = \{1, p-e, \ldots\}$ (así $\nu = 1$ si y solo si $e \leq p-1$).

Proposición 1.25 ([25], Proposition IV.3.2)**.** *Para una k-álgebra especial local A la aplicación $W(\bar{k})$-lineal $\hat{w}_A$* (definida en la proposición 1.24(a)) *induce un isomorfismo*

$$w_A\colon \left(\widehat{CW}_{\bar{k}}(A_{\bar{k}})\right)_k \cong P(A)/P'(A). \qquad \square$$

1.4.2. *Cohomología de de Rham formal* [47]. Sea ahora k un anillo conmutativo. Si X es un k-esquema (ordinario) se define la cohomología de de Rham de X como la hipercohomología

$$H^n_{dR}(X) := \mathbb{H}(X, \Omega^*_{X|k}) \in k\text{-}\underline{\mathrm{Mod}},$$

donde $\Omega_{X|k}$ es el haz de diferenciales de X sobre k y $\Omega^*_{X|k} := (\wedge^k \Omega_{X|k})$ es el complejo de de Rham de X sobre k, con la diferencial exterior d.

Análogamente, si k es un anillo local noetheriano completo y X es un k-esquema formal EGA se tiene el haz de diferenciales continuas $\widehat{\Omega}_{X|k}$ (de modo paralelo a $\Omega_{X|k}$) así como la *cohomología de de Rham* (formal) de X sobre k

$$H^n_{dR}(X) := \mathbb{H}^n(X, \widehat{\Omega}^*_{X|k}) \in k\text{-}\underline{\mathrm{Mod}}.$$

En el caso $X = \mathrm{Spf}(A)$, $A \in \underline{\mathrm{PRO}}_k$ se tiene $H^n_{dR}(X) = H^n_{dR}(A) := H^n(\widehat{\Omega}^*_{A|k})$.

En el caso de esquemas ordinarios se tiene la siguiente descripción $H^1_{dR}(X) \cong$ Formas de segunda especie/Formas exactas. Y si X es una K-variedad abeliana, entonces se verifican los *teoremas del cuadrado y del cubo*, mediante los cuales cualquier estructura de grupo en X da propiedades para las formas de segunda especie. Pero en el caso formal no se tiene nada de esto.

Así, ahora para k *como en* (1.4.1) y $G = \mathrm{Spf}(k[[\mathbf{X}]]) \in \underline{\mathrm{FLG}}_k$, el teorema del cuadrado de variedades abelianas fuerza la noción de forma de segunda especie de G (ver más adelante), para que tal noción dé una cohomología de de Rham de G (como grupo formal) compatible con $X \in \underline{\mathrm{Var.abel}}_K \mapsto \chi(p) \in \underline{p\text{-div}}_k$ ($\chi_K = X$ y $\chi(p)$ el del ejemplo 1.3(d)).

Nótese que $H^1_{dR}(K[[\mathbf{X}]]) = 0$ (*lema de Poincaré formal*), y así se tiene un isomorfismo K-lineal

$$d\colon K[[\mathbf{X}]]_0 \cong \widehat{\Omega}^{\mathrm{Cl}}_{K[[\mathbf{X}]]|K}\ (1\text{-}\textit{formas cerradas})$$

Por la descripción de $P(k[[\mathbf{X}]])$ de (1.14) se tiene

$$\lambda \in P(k[[\mathbf{X}]])\ (\textit{integrales de } G) \text{ si y solo si } d\lambda = \omega \in \widehat{\Omega}_{k[[\mathbf{X}]]|k}.$$

La aplicación k-lineal $\partial\colon k[[\mathbf{X}]] \to k[[\mathbf{X}]]\,\hat{\otimes}_k k[[\mathbf{X}]]$ de (1.1) se extiende por continuidad

$$\partial\colon \widehat{k[[\mathbf{X}]]}^{an}_{K_0} \to \widehat{k[[\mathbf{X}]]}^{an}_{K_0} \hat{\otimes}_k \widehat{k[[\mathbf{X}]]}^{an}_{K_0}.$$

Para $H^1_{dR}(G) = \widehat{\Omega}^{\mathrm{Cl}}_{k[[\mathbf{X}]]|k}/dk[[\mathbf{X}]]$ (G el esquema formal subyacente), la diferencial exterior induce un isomorfismo de k-módulos ([47], Lemma 5.1.2)

$$P(k[[\mathbf{X}]])/k[[\mathbf{X}]] \cong \frac{P(k[[\mathbf{X}]]) \cap K[[\mathbf{X}]]_0}{k[[\mathbf{X}]] \cap K[[\mathbf{X}]]_0} \overset{d}{\cong} H^1_{dR}(G).$$

Las integrales de

$$\mathscr{L}_k(G) := P(k[[\mathbf{X}]]) \cap \ker \partial = P(k[[\mathbf{X}]]) \cap \mathrm{Hom}_K(G, \mathbb{G}_a) \subset K[[\mathbf{X}]]_0$$

(ver el ejemplo 1.2.1) se dicen de *integrales primera especie de G*. Las de

$$P(k[[\mathbf{X}]]) \cap \partial^{-1}(k[[\mathbf{X}]] \hat{\otimes}_k k[[\mathbf{X}]])$$

se dicen de *integrales segunda especie de G*. Pasando por la diferencial exterior se tienen las mismas nociones para formas diferenciales

Formas de primera especie de $G := d(\mathscr{L}_k(G)) \cong \mathscr{L}_k(G)$.

Formas de segunda especie de $G := d$(integrales de segunda especie de G).

Se define ahora la 1-*cohomología de de Rham* (formal) *de* G (éste ahora como grupo formal)

$$\begin{aligned} H^1_{dR}(G)_{kaz} :=& \frac{\text{Formas de segunda especie de } G}{dk[[\mathbf{X}]]} \\ \overset{d}{\cong}& \frac{(\text{Integrales de segunda especie de } G) \cap K[[\mathbf{X}]]_0}{k[[\mathbf{X}]] \cap K[[\mathbf{X}]]_0} \\ \cong& \frac{\text{Integrales de segunda especie de } G}{k[[\mathbf{X}]]} \end{aligned}$$

([47], Lemma 5.1.2). (En [47], p. 187 se denota $D(G|k)$. Aquí, para distinguirla de las otras H_{dR}, denotamos "kaz" por el autor). Se considera también en [47], p. 193, la 1-*cohomología de de Rham de G para un ideal I de k*. Todo es paralelo a lo anterior partiendo de la definición de integrales de segunda especie de G para I como las integrales de $P(k[[\mathbf{X}]]) \cap \partial^{-1}(I[[\mathbf{X}]] \hat{\otimes}_k I[[\mathbf{X}]])$, que denotamos aquí ($D_I(G|k)$ en [47])

$$\begin{aligned} H^1_{dR}(G;I)_{kaz} :=& \frac{\text{Formas de segunda especie de } G \text{ para } I}{dI[[\mathbf{X}]]} \\ \overset{d}{\cong}& \frac{(\text{Integrales de segunda especie de } G \text{ para } I) \cap K[[\mathbf{X}]]_0}{I[[\mathbf{X}]] \cap K[[\mathbf{X}]]_0} \\ \cong& \frac{\text{Integrales de segunda especie de } G \text{ para } I}{I[[\mathbf{X}]]} \end{aligned}$$

En el caso no ramificado $k = W(\bar{k})$, y para $I = pW(\bar{k})$, se tiene que

$$\begin{aligned} \mathbb{MH}_{W(\bar{k})[[\mathbf{X}]]}(G_{\bar{k}}) :=& \frac{\text{Integrales de segunda especie de } G \text{ para } pW(\bar{k})}{pW(\bar{k})[[\mathbf{X}]]} \\ \overset{d}{\cong}& H^1_{dR}(G; pW(\bar{k}))_{kaz} \end{aligned}$$

es exactamente el definido en [25], Chap. III §6.4.

1.4.3. *Cohomología de de Rham formal y módulo de Dieudonné.*

Proposición 1.26. *Supongamos $k = W(\bar{k})$. Para $G \in \underline{\mathrm{FLG}}_{W(\bar{k})}$ se tiene un diagrama conmutativo en* $\mathrm{Top}D_{\bar{k}}\text{-}\underline{\mathrm{Mod}}$

$$\begin{array}{ccccc}
 & & \underline{M}(G_{\bar{k}}) & \xrightarrow[w_G]{\cong} & \mathbb{MH}_{W(\bar{k})[[\mathbf{X}]]}(G_{\bar{k}}) \\
 & \swarrow & & \swarrow & \cong \searrow^{\frac{1}{p}d\underline{F}} \\
\widehat{CW}_{\bar{k}}(\bar{k}[[\mathbf{X}]]) & \xrightarrow[w_G]{\cong} & P(W(\bar{k})[[\mathbf{X}]])/pW(\bar{k})[[\mathbf{X}]] & & H^1_{dR}(G)_{kaz} \\
 & \searrow^{\cong} & \downarrow{\scriptstyle \frac{1}{p}\underline{F}}\ \cong & & \downarrow \\
 & & P(W(\bar{k})[[\mathbf{X}]])/W(\bar{k})[[\mathbf{X}]] & \overset{\cong}{\underset{d}{}} & H^1_{dR}(G)
\end{array}$$

Demostración. El isomorfismo ω_G inferior es el de la proposición 1.24(b). Los isomorfismos d y $\frac{1}{p}d\underline{F}$ son los de (1.4.2). El isomorfismo ω_G superior es [25], Proposition III.6.5. (Nótese que, al ser $\frac{1}{p}\underline{F}$ un isomorfismo, el isomorfismo ω_G inferior equivale al isomorfismo $\psi\colon \widehat{CW}_{\bar{k}}(\bar{k}[[\mathbf{X}]]) \cong H^1_{dR}(G)$ de [47], (5.5.3)). □

Nota 1.19. Con esta descripción el módulo de Dieudonné $\underline{M}(G_{\bar{k}})$ puede verse también constituido por integrales, así como por diferenciales. (Ver la nota 1.17).

La proposición 1.26 puede ser extendida al caso ramificado como sigue. Para $G = \mathrm{Spf}(k[[\mathbf{X}]]) \in \underline{\mathrm{FLG}}_k$ se define ahora ([25], Chap. IV §4.1)

$$\mathbb{MH}_k(G) := \frac{P(k[[\mathbf{X}]]) \cap \partial^{-1}(P'(k[[\mathbf{X}]] \hat{\otimes}_k k[[\mathbf{X}]])}{P'(k[[\mathbf{X}]])}.$$

Proposición 1.27 ([25], Proposition IV.4.1)**.** *En la situación previa se tiene un diagrama conmutativo de k-módulos topológicos* (donde el isomorfismo w_G inferior es el de la proposición 1.25)

$$\begin{array}{ccc}
\underline{M}(G_{\bar{k}})_k & \overset{\cong}{\underset{w_G}{}} & \mathbb{MH}_k(G) \\
\downarrow & & \downarrow \\
\left(\widehat{CW}_{\bar{k}}(\bar{k}[[\mathbf{X}]])\right)_k & \overset{\cong}{\underset{w_G}{}} & P(k[[\mathbf{X}]])/P'(k[[\mathbf{X}]])
\end{array}$$

□

Nota 1.20. Por claridad y para simplificar hemos supuesto en esta sección el *caso local* de las k-álgebras especiales (ie, el caso conexo). Pero los resultados son válidos para k-álgebras especiales generales y para *p-grupos formales lisos de dimensión finita sobre k*, como puede observarse en las citas a [25] de esta sección.

1.5. Teoría de Grothendieck-Cartier-Messing-Fontaine

"Se trata de levantar de característica p a característica 0 el teorema 1.6, para un anillo k como en (1.4.1). La idea original para la clasificación de los grupos p-divisibles sobre tal k fue de Grothendieck, quien vio que ésta podría

realizarse *mediante un par*, el formado por el módulo de Dieudonné $\underline{M}(G_{\bar{k}})$ y por un submódulo de cierta extensión de escalares adecuada de $\underline{M}(G_{\bar{k}})$ [un *iso-F-cristal* de Grothendieck, que va a dar la filtración de Hodge, ver la proposición 2.6]. Los primeros resultados fueron enunciados por Cartier (ver [14]) y por Grothendieck en [36] y [37], mediante curvas típicas (teoría covariante) y cristales de Dieudonné (teoría contravariante), respectivamente. Los trabajos de Grothendieck fueron retomados en [56] y después en [55]" (de [25], p. 14).

Esta línea es equivalente a la de [25], Chap. IV (ver [25], Chap. V §3), que es la que vamos a exponer someramente.

1.5.1. Sea k *como en* (1.4.1) y $G = \mathrm{Spf}(A)$ un p-grupo formal liso de dimensión finita d sobre k (ver la nota 1.20). Considérese la aplicación k-lineal compuesta

$$\rho(G)\colon \mathscr{L}_k(G) \to \mathbb{MH}_k(G) \overset{\omega_G}{\cong} \underline{M}(G_{\bar{k}})_k$$

(el último isomorfismo es el de la proposición 1.27).

Proposición 1.28 ([25], Proposition IV.4.2)**.** *En la situación anterior*

(a) *Se tiene un isomorfismo $\bar{k}$-lineal (d dimensional)*

$$\mathscr{L}_k(G)/\pi\mathscr{L}_k(G) \cong \underline{M}(G_{\bar{k}})/\underline{F}\,\underline{M}(G_{\bar{k}}).$$

(b) *El k-módulo $\mathscr{L}_k(G)$ es libre de rango d* (uso de la proposición 1.23(c)). □

Corolario 1.3. *La diferencial exterior $d\colon A \to \widehat{\Omega}_{A|k}$ induce un isomorfismo de k-módulos, dentro de la composición* (donde η^* es el isomorfismo de la proposición 1.7)

$$t^*_G(k) \overset{\eta^*}{\cong} \Omega_k(G) \overset{d}{\cong} \mathscr{L}_k(G) \xrightarrow{\rho(G)} \underline{M}(G_{\bar{k}})_k.$$

Por lo tanto el módulo de diferenciales invariantes $\Omega_k(G)$ está constituido por las formas de primera especie de G.

Demostración. Está bien definida $d\colon \mathscr{L}_k(G) \rightarrowtail \Omega_k(G)$. Por la proposición 1.28(b) estamos reducidos a

$$\mathscr{L}_k(G)/\pi\mathscr{L}_k(G) \cong \underline{M}(G_{\bar{k}})/\underline{F}\,\underline{M}(G_{\bar{k}}) (\text{proposición 1.28(a)}) \cong$$

$$t^*_{G_{\bar{k}}}(\bar{k}) (\text{proposición 1.22}) \cong \Omega_{\bar{k}}(G_{\bar{k}}) (\text{proposición 1.7}) \cong \Omega_k(G)/\pi\Omega_k(G). \quad \square$$

Así se tienen isomorfismos K-lineales (d-dimensionales)

$$t^*_G(K) \cong \Omega(G) := K \otimes_k \Omega_k(G) \overset{d}{\cong} K \otimes_k \mathscr{L}_k(G) \xrightarrow{1\otimes\rho(G)} K \otimes_{W(\bar{k})} \underline{M}(G_{\bar{k}}).$$

Proposición 1.29. (a) *G es p-divisible sobre k si y solo si (G es un p-grupo formal liso sobre k y) $\underline{M}(G_{\bar{k}}) \cong W(\bar{k})^{\mathrm{ht}(G)}$.*

(b) *Si $G = \mathrm{Spf}(A)$ es un grupo p-divisible sobre k, entonces $\rho(G)\colon \mathscr{L}_k(G) \rightarrowtail \underline{M}(G_{\bar{k}})_k$ es inyectiva.* (Se tiene así una prueba más de $d \leq \mathrm{ht}(G)$).

Demostración. (a) Se sigue del corolario 1.1 y de la proposición 1.23(d).

(b) (Ver [25], demostración de Proposition IV.5.1). Se ha de probar que $\mathscr{L}_k(G) \cap P'(A) = 0$. En otro caso sea $\lambda \neq 0 \in P'(A)$ tal que $\Delta\lambda = \lambda\hat{\otimes}1 + 1\hat{\otimes}\lambda$. Sea r máximo para que $\lambda_1 = \pi^{-r}\lambda \in A - \pi A$. Entonces $\bar{\lambda}_1 \neq 0$ en $A_{\bar{k}}$ y define un homomorfismo no nulo $\bar{k}[[\mathbf{X}]] \to A_{\bar{k}}$, de donde $\mathrm{Hom}_{\bar{k}}(G_{\bar{k}}, \mathbb{G}_a) \neq 0$. Esto contradice a que G es p-divisible (nota 1.14). □

1.5.2. *Clasificación.* Sea e $(= [K:K_0])$ el índice de ramificación absoluto de K. Considérese la categoría $\underline{\mathrm{SH}}_k$ (*sistemas Honda*), introducida en [25], Chap. IV §5.1, cuyos objetos son pares (L, M) donde M es un $D_{\bar{k}}$-módulo $W(\bar{k})$-libre de tipo finito (ver (1.3.1)) y L es un k-submódulo libre de M_k tal que $L/\pi L \cong M/\underline{F}\,M$. Sea $\underline{\mathrm{SH}}_k\underline{\mathrm{topNil}}$ la subcategoría plena de objetos $(L, M) \in \underline{\mathrm{SH}}_k$ tales que $\underline{F}$ es topológicamente nilpotente sobre M.

Teorema 1.7 ([25], Proposition IV.1.6, Remarque IV.4.8 y Proposition IV.5.1)**.** *Considérese el funtor*

$$LM_k\colon \underline{p\text{-div}}_k^{\mathrm{op}} \to \underline{\mathrm{SH}}_k$$

dado por $LM_k(G) := (\mathscr{L}_k(G), \underline{M}(G_{\bar{k}}))$. *Se tiene*

(a) $e < p-1$ *si y solo si* $LM_k\colon \underline{p\text{-div}}_k^{\mathrm{op}} \simeq \underline{\mathrm{SH}}_k$.

(b) *Para* $e \le p-1$ *se tiene* $LM_k\colon \underline{p\text{-div}}_k^{\mathrm{op}}\underline{\mathrm{conexo}} \simeq \underline{\mathrm{SH}}_k\underline{\mathrm{topNil}}$. □

Nota 1.21. Para el teorema 1.7, se usa en [25] el hecho de que si G es p-divisible sobre k, entonces $G^0 = \mathrm{Spf}(k[[\mathbf{X}]])$ (la proposición 1.14(c) y el teorema 1.4). Las proposiciones 1.28 y 1.29 son usadas para que LM_k tome valores en $\underline{\mathrm{SH}}_k$.

Sea ahora $\varphi\underline{\mathrm{MF}}_K$ la categoría de los llamados *φ-módulos (de Dieudonné) filtrados* sobre K, cuyos objetos son triples (D^i, D, φ), donde D es un K_0-espacio vectorial de dimensión finita, $\varphi\colon D \to D$ es una aplicación φ-semilineal biyectiva (y así $D \in K_0[\underline{F}]$, éste definido paralelamente a $W(\bar{k})[\underline{F}]$ de (1.3.1)[16]) y D^i, $i \in \mathbb{Z}$, es una K-filtración de $K \otimes_{K_0} D$ tal que $\sum D^i = K \otimes_{K_0} D$ e $\cap D^i = 0$. Ver [27], §5.1 y [31], §8.1. Para $D = (D^i, D, \varphi) \in \varphi\underline{\mathrm{MF}}_K$ se usará la notación

$$\mathrm{Fil}^i D := D^i,$$

(y también $D = (K \otimes_{K_0} D, D)$, sobreentendiendo la filtración en $K \otimes_{K_0} D$). Sea $\varphi\underline{\mathrm{MF}}_K^2$ la subcategoría plena de $\varphi\underline{\mathrm{MF}}_K$ de objetos con filtración de longitud 2.

Teorema 1.8. (a) *El funtor*

$$LM_K\colon (\underline{p\text{-div}}_k/\mathrm{isg})^{\mathrm{op}} \to \varphi\underline{\mathrm{MF}}_K^2$$

dado por $LM_K(G) := (K \otimes_k \mathscr{L}_k(G), K_0 \otimes_{W(\bar{k})} \underline{M}(G_{\bar{k}}))$ *es fiel y pleno* (donde "/isg" significa "salvo isogenia"[17], ver [36], §5).

(b) *Si* $e \le p-1$, *entonces se tiene una equivalencia de categorías*

$$LM_K\colon (\underline{p\text{-div}}_k/\mathrm{isg})^{\mathrm{op}} \ \simeq$$
$$\left\{D \in \varphi\underline{\mathrm{MF}}_K^2,\ \textit{existe un retículo } M \textit{ de } D \textit{ tal que } (M \cap D^1, M) \in \underline{\mathrm{SH}}_k\right\}$$

Demostración. Que es fiel y pleno está en [25], Proposition IV.5.2. Lo de la imagen esencial de LM_K se sigue del teorema 1.7 (ver también el argumento de la proposición 2.4, más adelante). □

[16] Abuso de notación para las φ's precedentes, pero ahora ya se tiene $\varphi = \underline{F}\colon D \to D$.

[17] $\mathrm{Hom}_{k/\mathrm{isg}}(G, G') := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{Hom}_k(G, G')$. Esta terminología se debe a que, para un morfismo $f\colon G \to G'$ en $\underline{p\text{-div}}_k$, son equivalentes: (i) $f_{\bar{k}}$ es una isogenia; (ii) $\underline{M}(f_{\bar{k}})$ es inyectiva y $ht(G) = ht(G')$; (iii) $K_0 \otimes_{W(\bar{k})} \underline{M}(f_{\bar{k}})$ es un isomorfismo; (iv) f es un isomorfismo en $\underline{p\text{-div}}_k/\mathrm{isg}$. (Uso del teorema 1.6, de la proposición 1.23(d) y del teorema 1.8).

Grothendieck, además, conjetura la descripción de la imagen esencial del funtor LM_K. En [26], (5.2.5), se conjeturó que esta imagen era la categoría $\varphi\underline{\mathrm{MF}}^2_K\underline{\mathrm{wAd}}$, de los módulos *débilmente admisibles*. Esta última conjetura fue resuelta en algunos casos como sigue (pero sobre esto volveremos en (2.2.2))

Teorema 1.9 ([49], Théorème 2.1; [50], Théorème 2.1)**.** *Si $d = 1$ ó $e \leq p-1$* (poca ramificación, basándose en el teorema 1.8)*, entonces*

$$LM_K\colon (\underline{p\text{-div}}_k/\mathrm{isg})^{\mathrm{op}} \;\simeq\; \varphi\underline{\mathrm{MF}}^2_K\underline{\mathrm{wAd}}. \qquad \square$$

1.6. Módulos formales. Teoría Honda

1.6.1. En términos no muy precisos un módulo formal es una ley de grupo formal sobre un anillo A sobre el cual actúa un subanillo B de A, dado. Aparecen en [53] para dar una construcción explícita de la teoría de cuerpos de clases local.

En términos rigurosos sea ahora K *como en* (1.4.1) *pero ahora con la notación* $k = A/\pi A$. Sea E una extensión finita de $\mathbb{Q}_p$ contenida en K y denótese B el anillo de enteros de E. Denótese $er := [E\colon\mathbb{Q}_p]$ y $q = p^r := |\bar{B}|$, de forma que así e es el índice de ramificación absoluto de E.

Un *B-módulo formal definido sobre A*, o simplemente un *BA-módulo formal*, es una ley de grupo formal F sobre A junto con un homomorfismo de anillos (nótese que $\underline{\mathrm{FGL}}_A$ es una categoría aditiva)

$$B \to \mathrm{End}_A(F)$$

tal que se tiene la igualdad $(B \to \mathrm{End}_A(F) \xrightarrow{J} A^{d\times d}) = (B \to A^{d\times d})$, donde $d = \dim F$, $B \to A^{d\times d}$ es el homomorfismo estructural y J la aplicación matriz jacobiana evaluada en 0 (ver [41], (21.1.2)). Para $B \to \mathrm{End}_A(F)$ se utiliza la notación

$$[a]_F = [a]_F(\mathbf{X})\colon F \to F \quad \text{y} \quad F[a] := \ker [a]_F\,,\ a \in B$$

(coherente con la ya usada para $a = n \geq 0$, ver la nota 1.6.2). Se denota $\underline{\mathrm{FML}}_{BA}$ la categoría de BA-módulos formales.

Casos interesantes de módulos formales surgen con las construcciones de grupos formales dadas por Honda en [43], que pasamos a exponer someramente.

Teorema 1.10 ([43], Theorem 1)**.** *Para cada $F \in \underline{\mathrm{FGL}}_A$ existe un único $\lambda(\mathbf{X}) \in K[[\mathbf{X}]]^d$ ($d = \dim F$) tal que*

(i) $\lambda(\mathbf{X}) \equiv \mathbf{X}$ (mód deg 2)

(ii) $F(\mathbf{X},\mathbf{Y}) = \lambda^{-1}(\lambda(\mathbf{X}) + \lambda(\mathbf{Y}))$ $\square$

En otros términos, existe un único $\lambda(\mathbf{X}) \in \mathrm{Hom}_K(F,\mathbb{G}_a)^d$ ($= \mathrm{Hom}_K(F,\mathbb{G}_a^d)$) tal que $\lambda(\mathbf{X}) \equiv \mathbf{X}$ (mód deg 2). Tal $\lambda(\mathbf{X})$ se llama el (vector) *logaritmo* (o *transformador*) de F, que denotamos $\lambda_F(\mathbf{X})$. Así $\lambda_F(\mathbf{X})\colon F \cong \mathbb{G}_a^d$ (sobre K). En particular $\lambda_{\mathbb{G}_a} = X$.

Corolario 1.4 ([43], §3.2)**.** *$F \overset{\sim}{\equiv} G$ en $\underline{\mathrm{FGL}}_A$* (isomorfismo fuerte, ie, un isomorfismo $f(\mathbf{X})$ tal que $f(\mathbf{X}) \equiv \mathbf{X}$ (mód deg 2)) *si y solo si $\lambda_G^{-1}\lambda_F \in A[[\mathbf{X}]]_0^d$. En este caso $\lambda_G^{-1}\lambda_F\colon F \overset{\sim}{\equiv} G$.* $\square$

Nota 1.22. 1. Se tiene un isomorfismo canónico $\mathrm{Hom}_K(F,\mathbb{G}_a)\cong K^d$, y que λ_F *es una* K*-base de* $\mathrm{Hom}_K(F,\mathbb{G}_a)$. En efecto, el argumento usado para probar el teorema 1.10 prueba también que la aplicación lineal $f(\mathbf{X})=a_1X_1+\cdots+a_dX_d+$ *sup* $\in \mathrm{Hom}_K(F,\mathbb{G}_a)\mapsto(a_1,\dots,a_d)\in K^d$ es biyectiva. Así $K\otimes_A\mathscr{L}_A(F)=\mathrm{Hom}_K(F,\mathbb{G}_a)$.

Puesto que $\lambda_F\subset P(A[[\mathbf{X}]])$ (eg, para $d=1$, $\lambda_F(X)=\sum_{k=1}^{\infty}\frac{c_i}{i}X^i$, $c_i\in A$, $c_1=1$, y ahora uso de (1.14)) y que la imagen de $\mathscr{L}_A(F)$ por el isomorfismo anterior está contenida en A^d, se sigue que λ_F *es una* A*-base de* $\mathscr{L}_A(F)$. Así se obtiene de nuevo la proposición 1.28(b) para este caso. En [25], Chap. V §2.5, se muestra el recíproco.

2. $F\in\underline{\mathrm{FGL}}_A$ admite una (necesariamente única) estructura de BA-módulo formal si y solo si $\lambda_F^{-1}(a\lambda_F(\mathbf{X}))\in A[[\mathbf{X}]]^d$ para todo $a\in B$. Esta estructura debe ser $[a]_F(\mathbf{X}):=\lambda_F^{-1}(a\lambda_F(\mathbf{X}))$, $a\in B$.

3. Así *los* BA*-módulos formales pueden ser vistos como una subclase (dependiente de* B*) de la categoría* $\underline{\mathrm{FGL}}_A$, más que como leyes de grupo formal sobre A con estructura adicional. Para $B=\mathbb{Z}_p$ se tiene $\underline{\mathrm{FGL}}_A=\underline{\mathrm{FML}}_{\mathbb{Z}_pA}$.

La interpretación de la altura dada en (1.1.3) para $d=1$ (ver la proposición 1.11) se puede trasladar ahora a Bk-módulos formales (definición análoga a la de BA-módulos formales). Sea así F un Bk-módulo formal y $d=1$. Entonces $[\pi]_F(X)=0$ ó $g(X^{q^h})$, $g\not\equiv 0$ (mód deg 2), h máximo. En este caso se define la B*-altura* de F mediante $\mathrm{ht}_B(F):=\infty$ o h. Así

$$\deg[\pi]_F=q^{\mathrm{ht}_B(F)}\quad\text{y}\quad \mathrm{ht}(F)=[E:\mathbb{Q}_p]\,\mathrm{ht}_B(F).$$

Por lo tanto, ahora en el caso $F\in\underline{\mathrm{FML}}_{BA}$ (y $d\geq 1$), se define la B*-altura* de F como sigue

$$\mathrm{ht}_B(F):=\mathrm{ht}(B)/[E:\mathbb{Q}_p]\,.$$

Proposición 1.30 ([41], (21.8.2); [19], Proposition 1)**.** *En la situación anterior* $\mathrm{ht}_B(F)\in\{\infty\}\cup\mathbb{N}$. *Además* $\deg[\pi]_F=q^{ht_B(F)}$. □

1.6.2. *Caso relativamente no ramificado.* Supongamos ahora además que $K|E$ *es no ramificada* (ie, $\pi\in E$). Así $A=W(k)[\pi]$ ([51], Proposition I.23) $=B[W(k)]=B\otimes_{W(B/\pi B)}W(k)$ y $K=EK_0=E\otimes_{E_0}K_0$ (en $E\otimes_{E_0}K_0\twoheadrightarrow EK_0$ ambos tienen la misma K_0-dimensión, o el mismo $W(k)$-rango en el caso de los anillos).

Denotemos φ el Fröbenius relativo de $K|E$. Éste se extiende a $K[[\mathbf{X}]]$ mediante $\varphi\lambda(\mathbf{X})=\lambda^{\varphi}(\mathbf{X}^q)$ (ver la proposición 1.24). Así $K[[\mathbf{X}]]$ se convierte en un $A[\underline{F}]$-módulo topológico ($A[\underline{F}]$ definido análogamente a $W(k)[\underline{F}]$ de (1.3.1), pero ahora con este Fröbenius φ, siendo así $A[\underline{F}]$ relativo a $K|E$, ver también D_k^A en (1.6.3)).

Consideremos ahora los anillos de series de potencias formales no conmutativas $A[[\underline{F}]]$ y $K[[\underline{F}]]$ (definidos análogamente a $A[\underline{F}]$). Sea $\lambda\in K[[\mathbf{X}]]_0^d$ (d variables), $\lambda\equiv 0$ (mód deg 1), y sea $u=\sum_{i=0}^{\infty}C_i\underline{F}^i\in K[[\underline{F}]]^{d\times d}$ ($C_i\in K^{d\times d}$). Se define

$$u*\lambda:=\sum_{i=0}^{\infty}C_i\lambda^{\varphi^i}(\mathbf{X}^{q^i})\in K[[\mathbf{X}]]_0^d$$

(ie, $u * \lambda$ está inducido por la acción del Fröbenius φ antes citada, $\underline{F} * \lambda := \varphi\lambda(\mathbf{X}) = \lambda^{\varphi}(\mathbf{X}^q)$).

Sean $P \in \mathrm{GL}_d(A)$, y $u \in A[[\underline{F}]]^{d\times d}$, *especial* en el sentido de que $u \equiv \pi I_d$ (mód deg 1). Se dice que $\lambda \in K[[\mathbf{X}]]_0^d$ es *tipo* $(P;u)$ si

$$\lambda \equiv P\mathbf{X} \text{ (mód deg 2)} \quad \text{y} \quad u * \lambda \equiv 0 \ (\pi).$$

λ se dice *tipo* u si es tipo $(I_d;u)$.

Proposición 1.31 ([43], p. 221 y Proposition 2.5)**.** *Sea $(P;u)$ un tipo especial, y así $u\pi^{-1} \in K[[\mathbf{X}]]^{d\times d}$ tiene inversa $u^{-1}\pi = I_d + B_1\underline{F} + \cdots$. Se tiene*

(a) $h := u^{-1}\pi * \mathbf{X} = \mathbf{X} + B_1\mathbf{X}^q + B_2\mathbf{X}^{q^2} + \cdots$ *es tipo u.*

(b) $\lambda \in K[[\mathbf{X}]]_0^d$ *es tipo $(P;u)$ si y solo si $\lambda = (u^{-1}\pi * \mathbf{X})\psi$ para algún $\psi \in A[[\mathbf{X}]]_0^d$ tal que $\psi \equiv P\mathbf{X}$* (mód deg 2).

En particular cada tipo $(P;u)$ lo es de algún $\lambda \in K[[\mathbf{X}]]_0^d$. □

Teorema 1.11 ([43], Theorem 2)**.** *Sean λ, μ, P, Q y u como antes*

(a) *Si λ es tipo $(P;u)$, entonces $F := \lambda^{-1}(\lambda(\mathbf{X}) + \lambda(\mathbf{Y})) \in \underline{\mathrm{FGL}}_A$.*

(b) *Si λ es tipo $(P;u)$ y μ es tipo $(Q;u)$, entonces $F \cong G$ (siendo F y G los construidos para λ y μ como en* (a)*).*

(c) *En la situación de* (b)*, λ y μ son tipo $(P;u)$ si y solo si $F \overset{\sim}{\equiv} G$* (para "⇐" usar el corolario 1.4 y la proposición 1.31(b)). □

Nota 1.23. En la situación del teorema 1.11.(a) se tiene (según la proposición 1.31) $\lambda = h\psi$, y así $\psi\colon F \cong H$ $(:= h^{-1}(h(\mathbf{X})+h(\mathbf{Y})))$ y $\lambda = P\lambda_F$. En particular λ es tipo u si y solo si $\lambda = \lambda_F$.

Un *grupo formal Honda* sobre A (relativo a B) es una ley de grupo formal sobre A construida como en el teorema 1.11.(a) a partir de un λ tipo u. Ie, una tal ley F para la que existe u especial tal que λ_F es tipo u (ver la nota 1.23). Denotamos $\underline{\mathrm{HDA}}_{BA}$ la subcategoría plena de $\underline{\mathrm{FGL}}_A$ formada por los grupos formales Honda sobre A (rel. B).

Proposición 1.32 ([43], Corollary to Theorem 3)**.** *Sea F un grupo formal Honda sobre A, y sea λ_F tipo u. Se tiene un isomorfismo de anillos*

$$A^{d\times d} \cap (u^{-1}A[[\underline{F}]]^{d\times d}\, u) \cong \mathrm{End}_A(F) \quad (d = \dim F)$$

dado por $C \mapsto \lambda_F^{-1}(C\lambda_F)$. □

Corolario 1.5. *Cada grupo formal Honda sobre A (relativo a B) es un BA-módulo formal.*

Demostración. De la proposición 1.32 y de la nota 1.22.2. □

El recíproco se probó en [18] para $d = 1$, y en [19], Remarque 3(a) en el caso general

Proposición 1.33. *Los grupos formales Honda sobre A (relativos a B) son exactamente las leyes de grupo formal sobre A que admiten una estructura de BA-módulo formal (ie, $\underline{\mathrm{HDA}}_{BA} = \underline{\mathrm{FML}}_{BA}$).* □

En el caso $d = 1$ se tiene un resultado de clasificación más preciso

Proposición 1.34. *Supongamos $d = 1$. Las clases de isomorfismo fuerte de grupos formales Honda sobre A de B-altura h ($h < \infty$) son biyectivas con elementos especiales $u = \pi - \sum_{i=1}^{h} a_i \underline{F}^i$, $a_1, \dots, a_{h-1} \in \pi A$, $a_h \notin \pi A$. La biyección está inducida por $\lambda_F = u^{-1}\pi * X$* (ver la proposición 1.31.(a)). *Un tal tipo u para F se dice su* tipo canónico.

Demostración. En el caso no ramificado $E = \mathbb{Q}_p$ es [43], Proposition 3.5. En el caso relativamente no ramificado es [18], Theorem 3.3.1, ó [41], Theorem 21.8.9 (aunque en este último el autor indica que la demostración es exactamente la del caso no ramificado). □

Nota 1.24. 1. Aunque la definición de la categoría $\underline{\mathrm{HDA}}_{BA}$ es relativa a la elección del uniformizante π, la proposición 1.33 muestra que $\underline{\mathrm{HDA}}_{BA} = \underline{\mathrm{FML}}_{BA}$, y esta última categoría es un absoluto (no depende de π). Pero, si $d = 1$, para cada π se tiene una parametrización de $\underline{\mathrm{HDA}}_{BA}$ por los tipos canónicos (proposición 1.34). Si se hace cambio de uniformizante $\pi' = \epsilon\pi$, $\epsilon \notin \pi A$, entonces, para un elemento u especial para π, se tiene que ϵu es especial para π', y si λ es tipo u, entonces λ es tipo ϵu.

Si $d = 1$, y $u' = \pi' - \sum_{i=1}^{h} a_i \underline{F}^i$, $a_i \in \pi A$ ($i < h$), $a_h \notin \pi A$, es el tipo canónico para π' de una clase de isomorfismo fuerte de $\underline{\mathrm{HDA}}_{BA}^{1h}$ (dimensión 1 y B-altura h), esta clase tendrá como tipo canónico para π a $u = \epsilon^{-1}u'$.

2. *Módulos de Lubin-Tate*. En la situación de la proposición 1.34 consideremos el elemento especial $u = \pi - a\underline{F}$, $a \notin \pi A$ (para π). Es tipo canónico de una clase de isomorfismo fuerte de $\underline{\mathrm{HDA}}_{BA}^{11}$, cuyos elementos se denominan *módulos de Lubin-Tate para π relativos*. Denotemos esta clase $\mathrm{rel}\underline{\mathrm{LT}}_{\pi,a}$, y $\mathrm{rel}\underline{\mathrm{LT}}_{\pi} := \mathrm{rel}\underline{\mathrm{LT}}_{\pi,1}$. Se tiene $\mathrm{rel}\underline{\mathrm{LT}}_{\pi,a} = \mathrm{rel}\underline{\mathrm{LT}}_{\epsilon\pi,\epsilon a}$, para $\epsilon \notin \pi A$, y

$$\underline{\mathrm{HDA}}_{BA}^{11} = \bigsqcup_{\pi \text{ uniformizante de } A} \mathrm{rel}\underline{\mathrm{LT}}_{\pi}.$$

Los módulos de Lubin-Tate relativos fueron introducidos en [62] para extender a ellos la reciprocidad de [74]. El caso $K = E$ da los *módulos de Lubin-Tate* (absolutos) introducidos en [53]. Así $\underline{\mathrm{FML}}_A^{11} = \bigsqcup \underline{\mathrm{LT}}_{\pi}$, π uniformizante de A.

Se tienen así casos especiales interesantes de módulos formales, así como construcciones y parametrizaciones de los mismos (teoría Honda).

1.6.3. *Resultados de Decauwert.* La teoría Honda no ramificada (caso $E = \mathbb{Q}_p$ de (1.6.2)) de clasificación de grupos formales se corresponde con la de Grothendieck y otros (cf §1.5), que utiliza el módulo de Dieudonné. Ver [25], Chap. V §2.

La correspondiente relativización a módulos formales fue realizada en [40] y [41] para característica p y teoría covariante de curvas típicas de Cartier (ver [41], §§29 y E.4). Para la teoría contravariante, vía el módulo de Dieudonné, tal relativización fue realizada en [19], y tanto para característica p como para característica 0. Es lo que pasamos a exponer.

Sean pues $(K, A, k = A/\pi A)$ y E como en (1.6.2). Denotemos $\underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$ la categoría de BA-módulos formales que son p-divisibles sobre A, ie, de altura finita (ver el teorema 1.5). Sea $F \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$ y denótese $d = \dim F$ y

$h_B = \mathrm{ht}_B(F)$. Así $F = \mathrm{Spf}(A[[\mathbf{X}]])$, con comultiplicación extendida $\Delta\colon K[[\mathbf{X}]] \to K[[\mathbf{X}]][\,\hat\otimes_A K[[\mathbf{X}]]$ ($\Delta(\mathbf{X}) = F(\mathbf{X},\mathbf{Y})$).

En el caso absolutamente no ramificado (ie, $E = \mathbb{Q}_p$, y así $A = W(k)$), la proposición 1.26 daba una interpretación diferencial del módulo de Dieudonné de la fibra especial de una ley de grupo formal. Inspirándose en esto, en el caso relativamente no ramificado, Decauwert en [19], p. 1414, introduce lo que aquí llamamos el *módulo de Dieudonné de F relativo a E*, como el cociente

$$M^E(F) := \frac{P(A[[\mathbf{X}]]) \cap \partial^{-1}(\pi(A[[\mathbf{X}]]\,\hat\otimes_A A[[\mathbf{X}]])) \cap K[[\mathbf{X}]]_F}{\pi A[[\mathbf{X}]]}$$

siendo ∂ como en (1.1) y $K[[\mathbf{X}]]_F := \{\lambda \in K[[\mathbf{X}]]\,,\, \lambda([a]_F(\mathbf{X})) - a\lambda(\mathbf{X}) \in A[[\mathbf{X}]],\ a \in B\}$. También con $A[[\mathbf{X}]]_0$ en lugar de $A[[\mathbf{X}]]$ (como en (1.4.2)).

Esta es la relativización correcta del clásico módulo de Dieudonné en el sentido de que es el involucrado en la relativización de Decauwert [19] a módulos formales (los teoremas 1.12 y 1.13 que siguen) de los teoremas de clasificación de grupos p-divisibles (teoremas 1.6 y 1.7). Pero antes se va a definir el *anillo de Dieudonné sobre A* (implícito en [19], ver también [41]). Éste es el anillo de polinomios no conmutativos

$$D_k^A := A[\underline{F}, \underline{V}]\,,$$

con las relaciones $\underline{F}\,\underline{V} = \underline{V}\,\underline{F} = \pi$, $\underline{F}a = a^\varphi \underline{F}$, $a\underline{V} = \underline{V}a^\varphi$, $a \in A$ (es relativo a $A|B$, y en el caso absolutamente no ramificado se obtiene el clásico D_k de (1.3.1)).

Denotemos $\underline{\mathrm{SH}}_A^E$ la categoría cuyos objetos son pares (L, M), donde M es un D_k^A-módulo A-libre de tipo finito, y L es un A-submódulo de M tal que $L/\pi L \cong M/\underline{F}M$ (relativiza a $\underline{\mathrm{SH}}_A$ de (1.5.2)). Sea $\underline{\mathrm{SH}}_A^E\underline{\mathrm{topNil}}$ la subcategoría plena de $\underline{\mathrm{SH}}_A^E$ de objetos (L, M) tales que $\underline{F}$ es topológicamente nilpotente sobre M, ie, $M \in A[[\underline{F}]]\,\underline{\text{-Mod}}$.

Teorema 1.12 ([19], Théorème 1)**.** (a) *El funtor M^E define una equivalencia entre la categoría $\underline{\mathrm{FML}}_{Bk}^{\mathrm{op}}$ y la subcategoría de $D_k^A\,\underline{\text{-Mod}}$ de objetos M sobre los que $\underline{F}$ es topológicamente nilpotente e inyectiva, y $\dim_k(M/\underline{F}M) < \infty$.*

(b) *En particular, M^E define una equivalencia entre $\underline{\mathrm{FML}}_{Bk}\underline{p\text{-div}}_k^{\mathrm{op}}$ y la subcategoría de $D_k^A\,\underline{\text{-Mod}}$ de objetos M sobre los que $\underline{F}$ es topológicamente nilpotente, con A libre de tipo finito y $\dim_k(M/\underline{F}M) < \infty$.* □

Teorema 1.13 ([19], Proposition 2 y Théorème 2)**.** *Se tiene una equivalencia de categorías*

$$LM_A^E\colon \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A^{\mathrm{op}} \ \simeq\ \underline{\mathrm{SH}}_A^E\underline{\mathrm{topNil}},$$

donde $LM_A^E(F) := (\mathscr{L}_A(F), M^E(F))$. Además

$$d = \mathrm{rank}_A \mathscr{L}_A(F) = \dim_k \mathscr{L}_A(F)/\pi\mathscr{L}_A(F) = \dim_k M^E(F)/\underline{F}M^E(F) \le$$
$$h_B = \mathrm{rank}_A M^E(F) = \dim_k M^E(F)/\pi M^E(F) = d + \dim_k M^E(F)/\underline{V}M^E(F).$$ □

Nota 1.25. El teorema 1.12 extiende a módulos formales el teorema 1.6 para leyes de grupo formal (proposición 1.23). El teorema 1.13 extiende a módulos formales el teorema 1.7(b) para $e = 1$. En lo de los A-rangos está implícito el uso de las proposiciones 1.23(d), 1.28(b), 1.29(a) y 1.30.

Capítulo 2

Períodos π-ádicos de módulos formales p-divisibles

2.1. Representaciones p-ádicas y anillos de períodos de Fontaine

Ya hemos visto cómo los grupos p-divisibles están clasificados, por un lado, mediante representaciones p-ádicas de G_K (K como en (2.1.1), ver la nota 1.15.3), y por otro mediante categorías del álgebra semilineal (teoremas 1.7 y 1.8). La teoría de períodos p-ádicos es una etapa más avanzada sobre esos tipos de objetos que parametrizan a los grupos formales (y a las variedades p-ádicas), y así enfrenta al módulo de Dieudonné $\underline{M}(F)$ contra el módulo de Tate $T(F)$ de un grupo p-divisible F sobre A.

La teoría clásica de períodos complejos para esquemas propios y lisos sobre $\mathbb{C}$ compara la cohomología de de Rham con la homología singular. En [67], Corollary 2 al Theorem 3, se probó que la representación p-ádica $V(F)$ (también $V_p(X)$, de un A-esquema abeliano X) es de Hodge-Tate (germen de la teoría de Hodge p-ádica). Apoyándose en esto y en teoría de Dieudonné, Grothendieck en [36] vio que podía ser establecida una teoría p-ádica, paralela a la de períodos complejos, para grupos p-divisibles y para esquemas p-ádicos propios y lisos (germen de la teoría de períodos p-ádicos), lo que hizo en grado 1 al probar que la cohomología de de Rham y la étale se determinan mutuamente. Para ello se apoyó en el caso de grupos p-divisibles y conjeturó el caso de grado superior para esquemas, y en su forma explícita. Este es su problema del "funtor misterioso" y es lo que constituye el objeto de la *teoría de los períodos p-ádicos*. Es decir, establecer isomorfismos explícitos de comparación entre la cohomología de de Rham y la étale (ésta última juega el papel de la homología singular del caso complejo, y que en grado 1 da el módulo de Tate de los grupos p-divisibles, teniéndose así la teoría de períodos p-ádicos para estos últimos).

El primer paso, decisivo, para la resolución de esta conjetura de Grothendieck

lo dio Fontaine. Para ello (y también para la clasificación de representaciones p-ádicas, como veremos) construyó en [27] los llamados *anillos de períodos* (que juegan el papel que $\mathbb{C}$ juega en los períodos complejos). Luego demostró el isomorfismo de períodos p-ádicos para grupos p-divisibles ([25], Théorème V.1 y [27], Théorème 6.2), obtiendo así el caso de grado 1 de la citada conjetura y de forma explícita para esquemas (ver la nota 2.3). Los grupos p-divisibles fueron así usados como intermediarios. Además en [27], Appendice, se establecieron de forma rigurosa y explícita las *conjeturas de Hodge-Tate, de de Rham y cristalina* de comparación de períodos p-ádicos para esquemas propios y lisos (resueltas parcialmente en [32] y definitivamente en [23]). La teoría de períodos p-ádicos para esquemas (y para grupos p-divisibles), y sus conjeturas, estaban establecidas.

Una vez que las teorías de Dieudonné, Grothendieck, Messing, Fontaine,... de clasificación de grupos p-divisibles fueron relativizadas a módulos formales (cf. (1.6.3)), apoyándonos en esto último, en este capítulo vamos también a relativizar a módulos formales la teoría de períodos p-ádicos para grupos p-divisibles, y así como a deducir algunas consecuencias, todo en orden a su aplicación a las fórmulas explícitas buscadas.

2.1.1. *Caso absoluto.* Sea K un *cuerpo completo discreto de característica* 0 *y cuerpo residual* $k = A/\pi A$ *perfecto de característica* p. Sea $G_K := G(\bar{K}/K)$ el grupo de Galois absoluto de K.

Denotemos $\underline{\mathrm{Rep}}(G_K)^\infty$ ($\underline{\mathrm{Rep}}(G_K)$) la categoría de *representaciones p-ádicas* de G_K, cuyos objetos son $\mathbb{Q}_p$-espacios vectoriales (respectivamente, de dimensión finita) V con una acción lineal y continua de G_K, la continuidad para los $\mathbb{Q}_p[G_K]$-submódulos de V de dimensión finita. En el caso de dimensión finita de V la continuidad equivale a la de $G_K \to \mathrm{GL}(V)$, éste con la topología relativa de la producto (para la cual es localmente compacto y totalmente desconexo).

Análogamente, $\underline{\mathrm{Rep}}_{\mathbb{Z}_p}(G_K)^\infty$ ($\underline{\mathrm{Rep}}_{\mathbb{Z}_p}(G_K)$), la categoría de *representaciones $\mathbb{Z}_p$-ádicas de G_K*, es la análoga a la anterior pero ahora para $\mathbb{Z}_p$-módulos (de tipo finito). Si $V \in \underline{\mathrm{Rep}}_{\mathbb{Z}_p}(G_K)$, entonces $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} V \in \underline{\mathrm{Rep}}(G_K)$.

Como ejemplos originales y motivantes de representaciones p-ádicas procedentes de la Geometría Algebraica se tienen los ya mencionados antes, $T(F) \in \underline{\mathrm{Rep}}_{\mathbb{Z}_p}(G_K)$ y $V(F) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T(F) \in \underline{\mathrm{Rep}}(G_K)$, para un grupo p-divisible F sobre A (ver (1.2.4)), los módulos de Tate de los A-esquemas (y K-variedades) abelianos sobre cuerpos locales (ver la nota 1.15.1), así como la cohomología étale de los esquemas propios y lisos sobre A.

Fue Taniyama en [66] el primero que definió e investigó las representaciones p-ádicas, en especial los "módulos de Tate" (sin pasar al límite inverso) de una variedad abeliana sobre un cuerpo de números algebraicos. Como representaciones p-ádicas, los módulos de Tate de una variedad abeliana (ver la nota 1.15.1) fueron usados por Faltings (1983) para probar la conjetura de Mordell (1922). Además proporcionan el *criterio de Néron-Ogg-Shafarevic* sobre *buena reducción* en primos para variedades abelianas sobre cuerpos de números, [10] y [57], §IV.3 (ie, los "factores de Euler" de la función de Hasse-Weil, la involucrada en la

conjetura de Birch y Swinnerton-Dyer (1963)). Esto abundó en la importancia de los módulos de Tate, y en general de las representaciones p-ádicas.

El problema de la clasificación de estas p-representaciones de G_K es doble (lo cual sería objeto de la *teoría de Hodge p-ádica*, contrapartida a la compleja). Por un lado no se dispone de una descripción "explícita" de G_K. Por lo tanto sería conveniente clasificar aquéllas mediante categorías del álgebra semilineal de naturaleza "puramente algebraica", en el sentido de que sus objetos estén desprovistos de (o que en ellos no intervenga el) grupo G_K. Por otro lado se trata de caracterizar ciertas clases de representaciones (cristalinas, semi-estables,...) en términos explícitos de sus correspondientes objetos algebraicos (sobre esto ver la nota 2.2, más adelante). Lo primero fue realizado en [25], [26], [27], [28], [29] y [30], y dio lugar (junto con las mencionadas conjeturas de comparación de períodos p-ádicos) a la construcción de los ya mencionados anillos de períodos de Fontaine.

En [25], Chap. V §1.4 (ver también [27], §2.1) se introduce el siguiente anillo

$$\mathcal{R} := \varprojlim \mathcal{O}_{\bar{K}}/p\mathcal{O}_{\bar{K}}, \text{ límite inverso respecto a } (-)^p \colon C \to C$$

(C es el introducido en (1.2.3)). Así $\mathcal{R}$, como conjunto, se puede identificar como $\mathcal{R} = \varprojlim \mathcal{O}_C$. Las operaciones de $\mathcal{R}$ inducen en tal identificación las siguientes, denotando $(x^{(n)}) \in \mathcal{R}$, $x^{(n)} \in \mathcal{O}_C$,

$$(x^{(n)}) \cdot (y^{(n)}) = (x^{(n)}y^{(n)})$$
$$(x^{(n)}) + (y^{(n)}) = (\lim_{m\to\infty} (x^{(n+m)} + y^{(n+m)})^{p^m}).$$

Así $\mathcal{R}$ es un anillo de valoración (no discreta) completo perfecto de característica p, $\mathfrak{m}_{\mathcal{R}} := \varprojlim \mathfrak{m}_C$ es su ideal maximal y $\bar{k} = \mathcal{R}/\mathfrak{m}_{\mathcal{R}} = \mathcal{O}_C/\mathfrak{m}_C$ es su cuerpo residual. La valoración de $\mathcal{R}$ es $v((x^{(n)})) := v(x^{(0)})$, siendo esta última v la valoración de C.

Considérese el *homomorfismo continuo y sobreyectivo de K-álgebras*

$$\theta \colon W_K(\mathcal{R}) := K \otimes_{W(k)} W(\mathcal{R}) \twoheadrightarrow C$$

($W(\mathcal{R})$ es el anillo de vectores de Witt de $\mathcal{R}$), *definido por* $\theta(\sum_{n>>-\infty} \pi^n[x_n]) := \sum_{n>>-\infty} \pi^n x_n^{(0)}$), *independiente de la elección de* π, *y de núcleo principal* $W_K^1(\mathcal{R})$ $:= K \otimes_{W(k)} W^1(\mathcal{R})$ (donde $W^1(\mathcal{R})$ es el núcleo de $\theta \colon W(\mathcal{R}) \twoheadrightarrow \mathcal{O}_C$, para $A = W(k)$, ie, $\theta(\sum_{n\geq 0} p^n[x_n]) := \sum_{n\geq 0} p^n x_n^{(0)}$) ([27], Proposition 2.4).

Se extiende θ a la correspondiente completación

$$\begin{array}{ccccc} tW_K(\mathcal{R}) = W_K^1(\mathcal{R}) & \rightarrowtail & W_K(\mathcal{R}) & \xrightarrow{\theta} & C \\ \downarrow & & \downarrow & & \| \\ tB_{dR}^+ = \ker\theta & \rightarrowtail & B_{dR}^+ := \varprojlim W_K(\mathcal{R})/W_K^1(\mathcal{R})^n & \xrightarrow{\theta} & C. \end{array}$$

Así es inmediato que B_{dR}^+ *es un anillo de valoración discreta completo de igual característica* 0 *y de cuerpo residual* C.

Nota 2.1. Se tiene un monomorfismo canónico $\log[-]$ (ver [27], Remarque 2.16(c) y [29], (1.5.4)) dentro de

$$\mathbb{Z}_p(1) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) \subset \mathrm{Hom}(\mathbb{Q}_p, \mu_{p^\infty})$$
$$\subset \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, 1 + \mathfrak{m}_C) = 1 + \mathfrak{m}_{\mathcal{R}} \overset{\log[-]}{\rightarrowtail} B_{dR}^+$$

Denótese A_{cris} la p-completación de la capa de potencias divididas de $W(\mathcal{R})$ respecto al núcleo $W^1(\mathcal{R})$ (sobre potencias divididas ver [8] o [9]). Se tiene que

$$\mathbb{Z}_p(1) \subset A_{cris} \subset B_{dR}^+$$

mediante el homomorfismo de la nota 2.1. Ver [29], (2.3.4) y (4.1.1).

Si $0 \neq t \in \mathbb{Z}_p(1)$, entonces t *es un uniformizante de* B_{dR}^+ ($t = \log[\epsilon]$, $\epsilon \in \mathbb{Z}_p(1)$, ver la nota 2.1). Ver [27], Proposition 2.17 ó [29], (1.5.4). El cuerpo de fracciones (*cuerpo de períodos p-ádicos*)

$$B_{dR} := B_{dR}^+[1/t]$$

está, por lo tanto, filtrado por $t^i B_{dR}^+$, $i \in \mathbb{Z}$. Así B_{dR} filtra a A_{cris}, como también filtra a los subanillos que incluimos a continuación

$$B_{cris}^+ := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} A_{cris} = K_0 \otimes_{W(k)} A_{cris} = A_{cris}[1/p] = \cup A_{cris}/p^i A_{cris}$$
$$B_{cris} := B_{cris}^+[1/t] = A_{cris}[1/t] = \cup B_{cris}^+/t^i B_{cris}^+ = \cup A_{cris}/t^i A_{cris}$$

(Ver [27] y [29]). También, extendiendo escalares a A (ver [31], §§2 y 7, y [16], §2), se tienen

$$A_{cris,A} := A \otimes_{W(k)} A_{cris} = A_{cris}[\pi]$$
$$B_{cris,A}^+ := A_{cris,A}[1/p] = A_{cris}[1/\pi] = K \otimes_{K_0} B_{cris}^+ = K \otimes_{W(k)} A_{cris}$$
$$= K \otimes_A A_{cris,A}$$
$$B_{cris,A} := A_{cris,A}[1/t] = K \otimes_{K_0} B_{cris} = B_{cris}[1/\pi]\,.$$

Está claro que G_K actúa con continuidad sobre $\mathcal{R}$, $W(\mathcal{R})$, $W_K(\mathcal{R})$ y B_{dR}, y todos los subanillos previos son G_K-estables.

El Fröbenius absoluto de $\mathcal{R}$, junto con el de K_0, se extiende a un Fröbenius φ de B_{cris} por funtorialidad y continuidad, y poniendo $\varphi(1/t) := 1/pt$ (ver [27], §4.11). Se tiene que tanto B_{cris}^+ como B_{cris} son objetos de cada una de las categorías $\varphi\underline{\mathrm{MF}}_K^\infty$ (definida como $\varphi\underline{\mathrm{MF}}_K$ de (1.5.2) pero permitiendo dimensión infinita) y $\underline{\mathrm{Rep}}(G_K)^\infty$. (Ver [27], §4.11). Esta construcción permite definir los funtores

$$\underline{\mathrm{Rep}}(G_K)^{\mathrm{op}} \underset{V_{cris}^*}{\overset{D_{cris}^*}{\rightleftarrows}} \varphi\underline{\mathrm{MF}}_K,$$

mediante $D_{cris}^*(V) := \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V, B_{cris})$ y $V_{cris}^*(D) := \mathrm{Hom}_{\varphi\underline{\mathrm{MF}}_K}(D, B_{cris})$. La acción de G_K está inducida por la de B_{cris}, y la filtración en $K \otimes_{K_0} D_{cris}^*(V) \subset \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V, B_{dR})$ está inducida por la de B_{dR}. *En el caso* $K = K_0$ *esta filtración coincide con la inducida por la de* B_{cris}. Ver [26], §3.1 y [27], §5.

Nota 2.2. 1. Para $V \in \underline{\mathrm{Rep}}(G_K)$ se tiene la desigualdad

$$\dim_{K_0} D_{cris}^*(V) \leq \dim_{\mathbb{Q}_p} V.$$

La demostración de esto comenzó con un lema de Serre-Tate (ver [59]) y fue realizada en [27], Proposition 1.6(i), Proposition 3.6 y en §5.1 (ver también [30], Proposition 1.42). Si hay igualdad la representación V se dice *cristalina*. En este caso V es de Hodge-Tate, y los *pesos de Hodge-Tate* de V son los $i \in \mathbb{Z}$

para los cuales $\mathrm{Fil}^i(K \otimes_{K_0} D^*_{cris}(V))/(\mathrm{Fil}^{i+1}K \otimes_{K_0} D^*_{cris}(V)) \neq 0$. (Ver [27], Proposition 1.6, §§3.7 y 5.1).

Se tienen equivalencias inversas

$$\underline{\mathrm{Rep}}_{cris}(G_K)^{\mathrm{op}} \underset{V^*_{cris}}{\overset{D^*_{cris}}{\rightleftarrows}} D^*_{cris}(\underline{\mathrm{Rep}}_{cris}(G_K)) =: \varphi\underline{\mathrm{MF}}_K\underline{\mathrm{Ad}}$$

(módulos filtrados *admisibles*), [27], Théorème 5.2.

2. En [27], §5.3 se conjeturó que la imagen esencial del funtor D^*_{cris} restringido a las representaciones cristalinas, ie, que la clase de los módulos filtrados admisibles, era exactamente la de los módulos filtrados *débilmente admisibles* (involucrados en el teorema 1.9), siendo éstos los definidos en términos explícitos de los ingredientes del módulo filtrado, e introducidos en [26]. La conjetura fue resuelta en [31], Théorème 8.4, para $e = 1$ y longitud menor que p. Este resultado fue generalizado parcialmente en [31], §§8.12 y 8.13 al caso relativamente no ramificado. (Ver también la nota 2.6, más adelante).

3. La situación de las notas 1 y 2 puede ser extendida a clases más amplias de p-representaciones de G_K, como las *semi-estables*, si en lugar de B_{cris} se considera otro anillo de períodos B_{st} (ver [29]). Los correspondientes objetos algebraicos son los (φ, N)-*módulos*, que forman una categoría $\varphi\underline{\mathrm{MF}}^N_K$, quedando ahora la conjetura de Fontaine de la nota 2 como sigue $\varphi\underline{\mathrm{MF}}^N_K\underline{\mathrm{Ad}} = \varphi\underline{\mathrm{MF}}^N_K\underline{\mathrm{wAd}}$ (ver [30]).

2.1.2. *El complejo de Herr y Tavares Ribeiro y la cohomología de Galois.* En [28] se consideró una categoría de objetos algebraicos más general, la de los (φ, Γ)-módulos, que permitió parametrizar toda la clase de representaciones $\mathbb{Z}_p$-ádicas (p-ádicas) de G_K. Es en esta subsección donde, además, vamos a resumir las herramientas cohomológicas usadas en [68] para el cálculo de las fórmulas explícitas. Para detalles ver [68], §§1.4 y 1.5, [28] y [42].

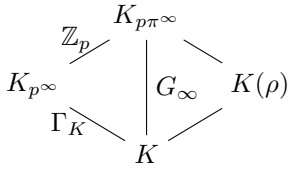
Sea Γ un grupo topológico y $\varphi\colon S \to S$ un morfismo de Γ-anillos topológicos lineales. Un (φ, Γ)-*módulo sobre* S es un S-módulo M con una acción semilineal de φ (ie, $M \in S[\underline{F}]\text{-}\underline{\mathrm{Mod}}$) y otra acción semilineal de Γ que conmuta con la primera. Un (φ, Γ)-*módulo étale* es un (φ, Γ)-módulo de tipo finito sobre S tal que φM genera M como S-módulo y la acción de Γ es continua (al ser M un S-módulo de tipo finito no hay ambigüedad sobre la topología de M, ie, la lineal coincide con la inducida vía la topología producto de la de S).

Sea K *como en* (2.1.1). La categoría $\underline{\mathrm{Rep}}_{\mathbb{Z}_p}(G_K)$ resulta ser equivalente a la categoría $\varphi\Gamma\text{-}\underline{\mathrm{Mod}}_S\underline{\text{ét}}$, de (φ, Γ)-módulos étale sobre cierto anillo S y sobre cierto grupo Γ. Ver [28], §3.4. Esto es suficiente para aplicar el método de [7] a las fórmulas explícitas para $F = \mathbb{G}_m$. Pero, para extender este método a $F \in \underline{p\text{-div}}_A$, en [68] se extiende la equivalencia de categorías de [28], de Γ_K al *caso metaabeliano* de G_∞, como pasamos a exponer.

Sea $\varepsilon = (\zeta_{p^n})$ un sistema coherente de raíces p^n-ésimas de 1 (ie, $Cl <\varepsilon>= \mathbb{Z}_p(1)$, ver el ejemplo 1.4). Sea $\rho = \rho_\pi := (\pi_{p^n})$ un sistema coherente de raíces p^n-ésimas de π. Denotemos

$$K_{p^\infty} := K(\varepsilon) \quad \text{y} \quad K_{p\pi^\infty} := K_{p^\infty}(\rho) = K(\varepsilon, \rho).$$

Se tiene un diagrama de extensiones de cuerpos (con las indicaciones y notaciones para sus grupos de Galois)



Así $G_\infty = \mathbb{Z}_p \rtimes \Gamma_K$, producto semidirecto de dos pro-p-grupos procíclicos, y así $G_\infty = Cl <\tau, \gamma>$ (denotando sus generadores topológicos por τ y γ).

Teorema 2.1 ([68], Theorem 1.3)**.** *Se tienen equivalencias inversas*

$$\underline{\mathrm{Rep}}_{\mathbb{Z}_p}(G_K) \underset{\tilde{V}_\pi}{\overset{\tilde{D}_\pi}{\rightleftarrows}} \varphi G_\infty\text{-}\underline{\mathrm{Mod}}_{\mathrm{S}}\underline{\text{ét}} \ (\mathrm{S} := W(\mathrm{Frac}(\mathcal{R}))^{G_{K_{p\pi^\infty}}}),$$

donde los funtores se denotan $\tilde{D}_\pi(V) := (V \otimes_{\mathbb{Z}_p} W(\mathrm{Frac}(\mathcal{R})))^{G_{K_{p\pi^\infty}}}$ *y* $\tilde{V}_\pi(M) := (M \otimes_S W(\mathrm{Frac}(\mathcal{R})))^{\varphi=1}$. □

La *cohomología de Galois continua* $H^n(\Gamma, A)$, $n \geq 0$, siendo Γ un grupo topológico y A un Γ módulo topológico, se define usando la resolución estándard (ver [58], §II.3). Así, para $V \in \underline{\mathrm{Rep}}_{\mathbb{Z}_p}(G_K)$ (K como en (2.1.1)) se tiene

$$H^n(\ /K, V) := H^n(\mathrm{Hom}_{\mathrm{Top}}(G_K^m, V)),\ n \geq 0$$

(G_K^m denota el complejo de cocadenas no homogéneo).

Consideremos el *carácter ciclotómico* $\chi\colon G_K \to \mathcal{U}(\mathbb{Z}_p)$, definido como la composición de los homomorfismos canónicos $G_K \to \mathrm{Aut}(\mu_{p^\infty}) \cong \mathcal{U}(\mathbb{Z}_p)$. Así $\zeta_{p^n}^{\chi(\sigma)} = \zeta_{p^n}^{\sigma}$, $\sigma \in G_K$. Se tiene también la aplicación $\psi\colon G_K \to \mathbb{Z}_p$ determinada por $\zeta_{p^n}^{\psi(\sigma)} = \pi_{p^n}^{\sigma-1}$.

Supongamos $p > 2$. De esta forma se puede tomar $G_\infty = Cl <\tau, \gamma>$ tal que $\gamma\tau\gamma^{-1} = \tau^{\chi(\gamma)}$ (ver [68], §1.1). Se eligen γ y τ tales que $\psi(\tau) = 1$, ie, $\rho^\tau = \rho\epsilon$.

El complejo de Herr [42] para el caso Γ_K fue adaptado en [68], (1.5.1) al caso metaabeliano de G_∞ como sigue. Para $M \in \varphi G_\infty\text{-}\underline{\mathrm{Mod}}_{\mathrm{S}}\underline{\text{ét}}$ (como en el teorema 2.1) se construye un complejo (que aquí denominamos el *complejo de Herr y Tavares Ribeiro*)

$$C_{\varphi\gamma\tau}(M)\colon 0 \to M \xrightarrow{\alpha} M^3 \xrightarrow{\beta} M^3 \xrightarrow{\eta} M \to 0,$$

adecuado para tener el siguiente

Teorema 2.2 ([68], Theorem 1.5)**.** *Para* $V \in \underline{\mathrm{Rep}}_{\mathbb{Z}_p}(G_K)$ *se tiene*

(a) $H^n C_{\varphi\gamma\tau}(\tilde{D}_\pi(V)) \cong H^n(\ /K, V)$, $n \geq 0$.

(b) *En grado* 1, *explícitamente, sea* $(x, y, z) \in Z^1(C_{\varphi\gamma\tau}(\tilde{D}_\pi(V)))$, *y sea* $b \in V \otimes_{\mathbb{Z}_p} W(\mathrm{Frac}(\mathcal{R}))$ *tal que* $b^{\varphi-1} = x$. *Entonces, mediantes el isomorfismo de* (a), *corresponde a* (x, y, z) *el cociclo*

$$c\colon \sigma \mapsto c\sigma := -b^{\sigma-1} + \gamma^n \frac{\tau^m - 1}{\tau - 1} z + \frac{\gamma^n - 1}{\gamma - 1} y,\ \textit{si}\ \sigma|_{G_\infty} = \gamma^n \tau^m. \qquad \square$$

2.1.3. *Caso relativamente no ramificado.* Sean ahora K *como en* (2.1.1) y E *como en* (1.6.2). El Fröbenius (absoluto) de $\mathcal{R}$, junto con el Fröbenius (relativo) φ de $K|E$, se extiende a un Fröbenius φ de $B_{cris,A}$ (para E) por funtorialidad y continuidad, y poniendo $\varphi(1/t) = 1/pt$ (ver (2.1.1) y [31], §7.16).

Consideremos la categoría $\underline{\mathrm{Rep}}_E(G_K)^\infty$ ($\underline{\mathrm{Rep}}_E(G_K)$) de *$E$-representaciones de G_K*, cuyos objetos son E-espacios vectoriales (de dimensión finita) V con una acción lineal y continua de G_K, la continuidad para $E[G_K]$-submódulos de V de dimensión finita.

Sea también $\varphi\underline{\mathrm{MF}}^\infty_{KE}$ ($\varphi\underline{\mathrm{MF}}_{KE}$, $\varphi\underline{\mathrm{MF}}^2_{KE}$) la categoría de los llamados *φ-módulos filtrados sobre K relativos a E* (φ el de $K|E$), cuyos objetos son triples $(\Delta^i, \Delta, \varphi)$, donde Δ es un K-espacio vectorial, $\varphi\colon \Delta \to \Delta$ es una aplicación φ-semilineal biyectiva (y así $\Delta \in K[\underline{F}]\text{-}\underline{\mathrm{Mod}}$) y Δ^i, $i \in \mathbb{Z}$, es una K-filtración de Δ (respectivamente $\dim_K \Delta < \infty$, Δ^i de longitud 2) tal que $\sum \Delta^i = \Delta$ y $\cap \Delta^i = 0$ (ver [31], §7.1). Si se "olvida" E, en lugar de $\varphi\underline{\mathrm{MF}}_{KE}$, se tiene la categoría $\varphi\underline{\mathrm{MF}}_K$ de (1.5.2).

Análogamente, se define la categoría $\underline{\mathrm{Rep}}_B(G_K)^\infty$ ($\underline{\mathrm{Rep}}_B(G_K)$) de *$B$-representaciones de G_K*. Éstas son B-módulos (de tipo finito) M con una G_K-acción lineal y continua. La continuidad es para la topología π-ádica de los $B[G_K]$-submódulos de M de tipo finito sobre B, la cual, al ser éstos de tipo finito, coincide con la inducida por la topología producto de la de B.

Se tiene que tanto $B^+_{cris,A}$ como $B_{cris,A}$ son objetos de cada una de las categorías $\varphi\underline{\mathrm{MF}}^\infty_{KE}$ (por tener aquellos un Fröbenius, como se acaba de mostrar) y $\underline{\mathrm{Rep}}_E(G_K)^\infty$ (ver [27], §4.11). Como en el caso absoluto, en [31] se definen y estudian los funtores

$$\underline{\mathrm{Rep}}_E(G_K)^{\mathrm{op}} \underset{V^*_{cris,A}}{\overset{D^*_{cris,A}}{\rightleftarrows}} \varphi\underline{\mathrm{MF}}_{KE},$$

$D^*_{cris,A}(V) := \mathrm{Hom}_{E[G_K]}(V, B_{cris,A})$ y $V^*_{cris,A}(\Delta) := \mathrm{Hom}_{\varphi\underline{\mathrm{MF}}_{KE}}(\Delta, B_{cris,A})$. La acción de G_K está inducida por la de $B_{cris,A}$. *La filtración en $D^*_{cris,A}(V)$, inducida por la de* $\mathrm{Hom}_{E[G_K]}(V, B_{dR})$, *coincide en este caso con la inducida por la de $B_{cris,A}$* (ver la nota 2.7.3).

2.2. Períodos π-ádicos de módulos formales p-divisibles

Incluimos en esta sección los resultados de períodos π-ádicos, relativización a módulos formales de la teoría de períodos p-ádicos de grupos p-divisibles, los cuales, junto con la relativización de la clasificación de los mismos, realizada en [19] (ver (1.6.3)), van a constituir la base que nos permitirá adaptar directamente los métodos de [2] y [68] a las fórmulas explícitas.

2.2.1. *El isomorfismo de comparación de períodos π-ádicos para módulos formales.* Este isomorfismo es la relativización a módulos formales del isomorfismo de períodos p-ádicos para grupos p-divisibles, siendo éste último el resultado principal de [27] (su teorema 6.2). Éste es el análogo para grupos formales a los isomorfismos de períodos p-ádicos para esquemas propios y lisos, conjeturados

en [27], Appendice (ver [44], que incluye una nota histórica), teniendo en cuenta para el primero la relación entre $LM_K(F)$ y la cohomología de de Rham de F (ver la proposición 2.6, más adelante). Recordemos ante todo brevemente los términos del caso de grupos formales.

Sea K *como en* (2.1.1) y $F \in \underline{p\text{-div}}_A$. La paridad de períodos p-ádicos de [25] parte de la paridad (tautológica, es decir, de la propia definición de $\underline{M}(F_k)$)

$$\underline{M}(F_k) \times F(S) \to \widehat{CW}_k(S), \quad (\underline{a}, x) \mapsto \underline{a}_S(x) \ (S \in \underline{k\text{-álg}})$$

(ver la nota 1.18). Puesto que $T(F) = \varprojlim F[p^s]$ se obtiene así por paso al límite la paridad de períodos p-ádicos

$$\underline{M}(F_k) \times T(F) \to A_{cris}.$$

En [25], Proposition V.1.5, se prueba que esta paridad induce (si $e < p-1$) el $\mathbb{Z}_p$-isomorfismo

$$T(F) \cong \mathrm{Hom}_{\mathrm{D}_k\text{-}\underline{\mathrm{Mod}A\text{-fil}}}(\underline{M}(F_k), A_{cris}), \tag{2.1}$$

y, a su vez (sin restricción), el siguiente $\mathbb{Q}_p$-isomorfismo ([25], Théorème V.1)

$$V(F) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T(F) \cong \mathrm{Hom}_{\varphi\underline{\mathrm{MF}}_K}(LM_K(F), B^+_{cris}).$$

(Para $u \in \mathrm{Hom}_{D_k}(\underline{M}(F_k), A_{cris})$, "$A$-filtrado" significa aquí que $u_K(K \otimes_k \mathscr{L}_A(F)) \subset \mathrm{Fil}^1 B^+_{cris}$, ie, que $u_K \in \mathrm{Hom}_{\varphi\underline{\mathrm{MF}}_K}(LM_K(F), B^+_{cris})$). Por lo tanto se tiene un morfismo natural

$$\eta_F \colon LM_K(F) \to D^*_{cris} V(F)$$

en la categoría $\varphi\underline{\mathrm{MF}}_K$, que llamaremos el *morfismo de comparación de períodos p-ádicos* (para F). Es decir, se tiene una transformación natural η entre los funtores

$$\begin{array}{ccc} & \xrightarrow{V(-)} & \underline{\mathrm{Rep}}(G_K) \\ \underline{p\text{-div}}_A & & \Big\downarrow D^*_{cris} \\ & \xrightarrow[LM_K]{} & \varphi\underline{\mathrm{MF}}_K \end{array}$$

En particular se tiene la *paridad de períodos p-ádicos* (filtrada, para F)

$$(K \otimes_{W(k)} \underline{M}(F_k)) \times T(F) \to B^+_{cris,A}.$$

Teorema 2.3 ([27], Théorème 6.2, isomorfismo de comparación de períodos p-ádicos de grupos p-divisibles)**.** *Sea F un grupo p-divisible sobre A. Se tiene un isomorfismo natural*

$$\eta_F \colon LM_K(F) \cong D^*_{cris} V(F)$$

en la categoría $\varphi\underline{\mathrm{MF}}_K$. En particular $V(F)$ es cristalina. □

Nota 2.3. Del teorema 2.3 se deduce, en particular, un caso de grado 1 y de forma explícita, decisivo, de la *conjetura cristalina* (usando los grupos p-divisibles como puente). En efecto, si X es un esquema abeliano sobre A, entonces $H^1_{cris}(X_K/K) \cong LM_K(X(p))$ en $\varphi\underline{\mathrm{MF}}_K$ (ver [9]). Por otra parte $H^1_{et}(X_{\bar{K}}, \mathbb{Q}_p) \cong V(X(p))^* = V_p(X)^*$. Por lo tanto del teorema 2.3 se obtiene: $H^1_{cris}(X_K/K) \cong D_{cris}(H^1_{et}(X_{\bar{K}}, \mathbb{Q}_p)$ en $\varphi\underline{\mathrm{MF}}_K$. Pero nótese que, cuando [27], la conjetura cristalina para variedades abelianas era ya un teorema en todos los grados y sin recurrir a los grupos p-divisibles (ver [27], A.12, y [32]).

Volvamos ahora, y *para lo que resta de este capítulo*, al *caso relativamente no ramificado* de (2.1.3), y sea así $F \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$, $d = \dim F$, $h_B = \mathrm{ht}_B(F)$ (como en (1.6.3)). Como en el caso absoluto, F tiene asociados dos objetos algebraicos. Por un lado el módulo de Dieudonné relativo $M^E(F)$, y por otro el módulo de Tate $T(F)$, que en este caso relativo va a resultar una B-representación de G_K.

Denotamos $F[\pi^s] := F[\pi^s](\mathfrak{m}_C)$. Se tiene así $T(F) = \varprojlim F[p^s] = \varprojlim F[\pi^s]$ ($p = u\pi^e$, u unidad de A, el último límite inverso es para $[\pi]_F$) $\in \underline{\mathrm{Rep}}_B(G_K)$. Por lo tanto $V(F) \in \underline{\mathrm{Rep}}_E(G_K)$.

Proposición 2.1. *En la situación anterior se tiene*

$$F[\pi^s] \cong (B/\pi^s B)^{h_B}, \quad T(F) \cong B^{h_B} \quad y \quad V(F) \cong E^{h_B}.$$

Demostración. En cuanto al primer isomorfismo (del que se siguen los otros dos, como en (1.11)), los casos $s = 1$ y $s = te$, $t \geq 1$, se reducen fácilmente a (1.10). Luego utilizar la sucesión exacta $0 \to F[\pi^s] \to F[\pi^{te}] = F[p^t] \to F[\pi^{te-s}] \to 0$ inductivamente desde $te - s = 1$. (Para una demostración π-ádica, ie, sin reducir a (1.10), para dimensión 1, ver [22], Proposition 1). □

Consideremos el funtor

$$LM_K^E \colon \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A^{\mathrm{op}} \to \varphi\underline{\mathrm{MF}}_{KE}$$

dado por $LM_K^E(F) := (K \otimes_A \mathscr{L}_A(F), K \otimes_A M^E(F))$ (que relativiza a LM_K del teorema 1.8 y que se obtiene por extensión de escalares del funtor relativo LM_A^E del teorema 1.13). Respecto a su imagen esencial volveremos en (2.2.2) (tal como ya habíamos anunciado para LM_K).

Teorema 2.4 (Isomorfismo de comparación de períodos π-ádicos de módulos formales p-divisibles)**.** *Sea $F \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-}div}_A$. El isomorfismo η_F del* teorema 2.3 *induce un isomorfismo natural*

$$\eta_F \colon LM_K^E(F) \cong D^*_{cris,A}V(F).$$

en la categoría $\varphi\underline{\mathrm{MF}}_{KE}$. En particular se tiene

$$\dim_K D^*_{cris,A}V(F) = h_B \quad y \quad \dim_K \mathrm{Fil}^1 D^*_{cris,A}V(F) = d \quad (\mathrm{Fil}^2 D^*_{cris,A}V(F) = 0).$$

Demostración. La afirmación sobre las dimensiones es una parte de la proposición 2.4, más adelante (así, en último término, de la "parte dimensional" del teorema 1.13), una vez que el isomorfismo del presente teorema haya sido probado.

Ante todo nótese que se tiene una relación $M^E(F) \leftharpoonup \underline{M}(F_k)$. Es la inducida por el siguiente diagrama (conmutativo por las definiciones)

$$\begin{array}{ccccc}
 & & M^E(F) & \rightarrowtail & P(A[[\mathbf{X}]]/\pi A[[\mathbf{X}]]) \\
 & \nearrow & \downarrow & \searrow & \downarrow \\
\mathscr{L}_A(F) & & \underline{M}(F_k) & \rightarrowtail & P(W(k)[[\mathbf{X}]])/pW(k)[[\mathbf{X}]] \\
 & \searrow & \downarrow & \nearrow & \downarrow \\
 & & \underline{M}(F_k)_A & \rightarrowtail & P(A[[\mathbf{X}]]/P'(A[[\mathbf{X}]])
\end{array}$$

(donde el morfismo $\underline{M}(F_k)_A \rightarrowtail P(A[[\mathbf{X}]])/P'(A[[\mathbf{X}]])$ es el de la proposición 1.27). La relación anterior induce la siguiente $K \otimes_A M^E(F) \rightharpoonup K \otimes_{W(k)} \underline{M}(F_k)$, y ésta, a su vez, un K-isomorfismo

$$K \otimes_A M^E(F) \cong \left\{\alpha \in K \otimes_{W(k)} \underline{M}(F_k),\ a\alpha = \alpha a\ \forall a \in B\right\} \tag{2.2}$$

(ver [19], Remarque 3(c)). La acción a la derecha de B sobre $\underline{M}(F_k)$ es la inducida por funtorialidad de la de B sobre F[18].

Se obtiene así una aplicación inyectiva canónica

$$K \otimes_A M^E(F) \rightarrowtail K \otimes_{W(k)} \underline{M}(F_k) \tag{2.3}$$

en la categoría de K-espacios vectoriales filtrados, como consecuencia del argumento que precede y de la parte que involucra a $\mathscr{L}_A(F)$ del anterior diagrama. Se tiene un diagrama conmutativo de K-espacios vectoriales

$$\begin{array}{ccc} K \otimes_A M^E(F) & \overset{\eta_F}{\dashrightarrow} & D^*_{cris,A}V(F) = \mathrm{Hom}_{E[G_K]}(V(F), B_{cris,A}) \\ \downarrow & & \downarrow \\ K \otimes_{W(k)} \underline{M}(F_k) & \underset{\eta_F}{\overset{\cong}{\longrightarrow}} & K \otimes_{K_0} D^*_{cris}V(F) \cong \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V(F), B_{cris,A}) \end{array}$$

El isomorfismo inferior es el del teorema 2.3. La aplicación η_F superior está bien definida. Es decir, para la η_F inferior, $\eta_F(d)$ pasa de ser $\mathbb{Q}_p$-lineal a E-lineal cuando $d \in K \otimes_A M^E(F)$ como consecuencia del isomorfismo (2.2). Puesto que el isomorfismo inferior es filtrado y por (2.3), se sigue que la η_F superior también es filtrada. Además ésta η_F superior conmuta con la acción de $\underline{F}$ puesto que esta acción está inducida por φ, que sobre $K_0[[\mathbf{X}]]$ es φ_0^r (donde φ_0 denota aquí el Fröbenius de $K_0|\mathbb{Q}_p$) y puesto que $\eta_F \colon K_0 \otimes_{W(k)} \underline{M}(F_k) \cong D^*_{cris}V(F)$ conmuta con $\underline{F}$ (por el teorema 2.3). Así la η_F superior es un morfismo en $\varphi\underline{\mathrm{MF}}_{KE}$. Por lo tanto sólo resta probar que este morfismo es biyectivo sobre las filtraciones

$$\begin{aligned} \eta_F(\mathrm{Fil}^i LM^E_K(F)) &= \eta_F((K \otimes_A M^E(F)) \cap \mathrm{Fil}^i LM_K(F)) \text{ (uso de (2.3))} \\ &= \eta_F(K \otimes_A M^E(F)) \cap \mathrm{Fil}^i D^*_{dR}V(F) \text{ (teorema 2.3)} \\ &= D^*_{cris,A}V(F) \cap \mathrm{Fil}^i D^*_{dR}V(F) \ (=: \mathrm{Fil}^i D^*_{cris,A}V(F)). \end{aligned}$$

La última igualdad se deduce de la siguiente desigualdad general

$$\dim_K D^*_{cris,A}(V) \leq \dim_E V$$

para cualquier $V \in \underline{\mathrm{Rep}}_E(G_K)$. Esta desigualdad se obtiene trasladando mutatis mutandis la demostración clásica de la misma para el caso absoluto (ver la nota 2.2.1), sin más que cambiar $\mathbb{Q}_p, B_{cris}, D^*_{cris}$, etc por $E, B_{cris,A}, D^*_{cris,A}$, etc, respectivamente. (Una demostración directa y unificada de la desigualdad mencionada, que incluye a nuestro caso, puede verse también en [12], §1.5). □

Nota 2.4. 1. En la demostración del teorema 2.4 están implícitas las relaciones entre los funtores LM_A y LM^E_A y entre LM_K y LM^E_K. La primera está implícita también en [19] al relativizar la clasificación de grupos p-divisibles (teorema 1.7) a módulos formales (teorema 1.13, ver la nota 1.25).

[18] Nótese que en [41], para la teoría covariante, la B-acción se define así. En cualquier caso esta acción se puede extender a una de $A = B \otimes_{W(\bar{B})} W(k)$

2. Nótese en lo anterior que el módulo de Dieudonné relativo, introducido en [19], no sólo es el adecuado para la clasificación que dan los teoremas relativos 1.12 y 1.13 (para lo cual fue construido específicamente), sino que (como en el caso absoluto) resultó adecuado también para la teoría de períodos π-ádicos.

2.2.2. *La categoría $\varphi\underline{\mathrm{MF}}^{ff2\oplus}_{AB}$. La imagen esencial del funtor LM^E_K.* Tanto para dar una descripción de esa imagen esencial (ver la nota 2.6.1, más adelante) como para derivar del teorema 2.4 su versión reticular (teorema 2.5), es necesario considerar la categoría $\varphi\underline{\mathrm{MF}}^{ff2}_{AB}$, introducida en [31], §§1.1, 1.5 y 9.7, aunque allí para "longitud finita" (e involucrada en el caso de grupos formales en [2], así como [1], [3] y [12], donde sus objetos se denominan "módulos de Fontaine-Laffaille").

En nuestro caso los objetos de $\varphi\underline{\mathrm{MF}}^{ff2}_{AB}$ son triples (M^1, M, φ) donde M es aquí un A-módulo libre de tipo finito (ff), $\varphi\colon M \to M$ es una aplicación φ-semilineal (ie, M es un $A[\underline{F}]$-módulo) y M^1 es un A-submódulo de M tal que $\varphi M^1 \subset \pi M$ y $M = \varphi M + (\varphi/\pi)M^1$. Denótese $\varphi\underline{\mathrm{MF}}^{ff2\oplus}_{AB}$ la subcategoría plena (propia, como se ve fácilmente) de la anterior cuyos objetos verifican que M^1 es un sumando directo de M. Para compararla con la categoría $\underline{\mathrm{SH}}^E_A$ (cf. (1.6.3)) probaremos el siguiente

Lema 2.1. *Para $(L, M) \in \underline{\mathrm{SH}}^E_A$ se tiene que tanto L como $\underline{V}L$ son sumandos directos de M.*

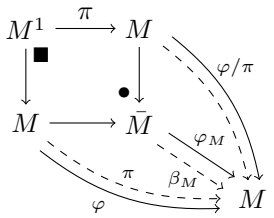
Demostración. Puesto que cualquier matriz sobre un dominio principal diagonaliza por equivalencia, se puede suponer que $(L, M) = (\pi^{s_1}A \times \cdots \times \pi^{s_d}A, A^n)$, $s_i \geq 0$. Pero $\underline{F}A^n \supset \pi A^n$, y así $\underline{F}A^n \cap L = \pi L$, lo que fuerza a que $s_1 = \cdots = s_d = 0$. Sea pues $(A^d, A^n) \in \underline{\mathrm{SH}}^E_A$. Si $\underline{V}A^d$ no fuese sumando directo, entonces alguna de las primeras d columnas de $\underline{V}$, digamos $\underline{V}(1, 0, \ldots, 0)$, debe ser divisible por π. Por lo tanto $(\pi, 0, \ldots, 0) = \underline{F}\,\underline{V}(1, 0, \ldots, 0)$ da que $(1, 0, \ldots, 0) \in \underline{V}A^n \cap A^d = \pi A^d$. Contradicción. □

Proposición 2.2. *Se tienen equivalencias inversas de categorías*

$$\underline{\mathrm{SH}}^E_A \underset{H}{\overset{I}{\rightleftarrows}} \varphi\underline{\mathrm{MF}}^{ff2\oplus}_{AB}$$

dadas por $H(M^1, M, \varphi) := ((\varphi/\pi)M^1, M)$ e $I(L, M) := (\underline{V}L, M, \varphi)$ ($\varphi := \underline{F}\colon M \to M$).

Demostración. Nótese que $\underline{V}L$ es un sumando directo de M por el lema 2.1. Para $(M^1, M, \varphi) \in \varphi\underline{\mathrm{MF}}^{ff2\oplus}_{AB}$ considérese el diagrama que sigue, en el cual $\bar{M}$ está definido mediante el cuadrado cocartesiano (y bicartesiano)



Se va a adaptar a nuestro caso ("libre de tipo finito") la demostración dada para "longitud finita" en [31], §§9.7 y 9.10. Todo transcurre paralelo excepto que, para la construcción del funtor H, es necesario tener que φ_M es un isomorfismo. Puesto que A es un dominio principal basta probar que $\bar{M}$ es A-isomorfo a M. Al ser M^1 un sumando directo de M se tiene una sucesión exacta

$$0 \to M^1 \xrightarrow{\theta} M^1 \oplus N \oplus M^1 \to \bar{M} \to 0,\ \theta(x) = (x, 0, -\pi x),$$

lo que claramente da que $\bar{M}$ es un A-módulo libre del mismo rango que M. □

Nota 2.5. De la demostración de la proposición 2.2 se sigue que tanto $\underline{\mathrm{SH}}_A^E$ como $\varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus}$ son subcategorías plenas de la categoría D_k^A-$\underline{\mathrm{Mod.}}A$-$\underline{\mathrm{fil}}^{ff2}$, de los D_k^A-módulos con una A-filtración de longitud 2 y A-libres de tipo finito. Para $(M^1, M, \varphi) \in \varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus}$ se toma $\underline{V} := \beta_\pi \varphi_\pi^{-1}$.

Proposición 2.3. *Para enteros $h \geq d \geq 1$ denótense $\underline{\mathrm{SH}}_A^{Edh}$ y $\varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus dh}$ las respectivas subcategorías de $\underline{\mathrm{SH}}_A^E$ y de $\varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus}$ de objetos cuyos A-rangos son h y d. Se tiene*

(a) *La igualdad $h = d$ es equivalente a que $\underline{\mathrm{SH}}_A^{Edh}\underline{\mathrm{topNil}} = \varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus dh}\underline{\mathrm{topNil}}$, y, a su vez, a que exista $F \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-}div}_A$ tal que $LM_A^E(F) \in \varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus dh}$.*

(b) *$h > d$ es equivalente a que $(\underline{\mathrm{SH}}_A^{Edh}\underline{\mathrm{topNil}}) \cap (\varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus dh}\underline{\mathrm{topNil}}) = \varnothing$.*

Demostración. Si $h = d$, entonces, para $(M, M) \in \underline{\mathrm{SH}}_A^E$, obtenemos que $(\varphi/\pi)M \cong M$ puesto que $\underline{V}M$ es un sumando directo de M por el lema 2.1. Así $(M, M) \in \varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus}$. Recíprocamente, si $(M, M) \in \varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus}$, entonces $(\varphi/\pi)M$ es un sumando directo de M (ver la proposición 2.2). Se sigue, análogamente que $(M, M) \in \underline{\mathrm{SH}}_A^E$.

Sea ahora $h > d$. Si se tuviese que $(A^d, A^h) \in \underline{\mathrm{SH}}_A^E$ y que $\varphi A^d \subset \pi A^h$, entonces φ no podría ser topológicamente nilpotente. En efecto, de $A^h = \varphi A^h + A^d$ se obtiene que

$$(0, 0, \ldots, 1) \in < (p, 0, \ldots, 0), \ldots, (0, 0, \overset{d-1)}{\ldots}, 0, p, 0, \ldots, 0), (a_{1,d+1}, \ldots, a_{h',d+1}),$$
$$(1, 0, \ldots, 0), \ldots, (0, 0, \overset{d-1)}{\ldots}, 0, 1, 0, \ldots, 0) >_A .$$

Esto obliga a que a_{hh} sea una unidad de K, lo que impide que φ sea topológicamente nilpotente. Así se obtiene (b) y la segunda equivalencia de (a). □

Lema 2.2. *Sea A un dominio semihereditario y K su cuerpo de fracciones. Si M es un retículo de un K-espacio vectorial Δ de dimensión finita y L es un A-submódulo de M, entonces L es un sumando directo de M si (y sólo si) existe un K-subespacio W de Δ tal que $L = M \cap W$.*

Demostración. Puesto que $M/L \rightarrowtail \Delta/W$ es inyectiva, M/L es libre de torsión, y por lo tanto proyectivo sobre A. □

Proposición 2.4. *Se tiene una equivalencia de categorías*

$$LM_K^E\colon (\underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A/\mathrm{isg})^{\mathrm{op}} \simeq$$
$$\{\Delta \in \varphi\underline{\mathrm{MF}}_{\mathrm{KE}}^2,\ \textit{existe un retículo } M \textit{ de } \Delta \textit{ tal que } (M \cap \Delta^1,\ M) \in \underline{\mathrm{SH}}_A^E\underline{\mathrm{topNil}}\}$$

Las K-dimensiones en $LM_K^E(F)$ son d y h_B.

Demostración. Puesto que tenemos el teorema 1.13 es fácil trasladar el argumento, para $E = \mathbb{Q}_p$, de [25], Proposition IV.5.2, a nuestro caso de módulos formales. Así se tiene que LM_K^E es fiel y pleno. Que su imagen esencial es la indicada en el enunciado se sigue del teorema 1.13, de nuevo, y del lema 2.1, teniendo en cuenta que la igualdad $L = M \cap (K \otimes_A L)$ equivale a que L sea sumando directo de M (lema 2.2). □

Es fácil ahora extender a módulos formales la caracterización de [50], Théorème 2.1 de la imagen esencial del funtor LM_K (ver el teorema 1.9). Para ello tomamos la definición de φ-módulo filtrado sobre K relativo a E ($\varphi\underline{\mathrm{MF}}_{\mathrm{KE}}$) *débilmente admisible* de [31], §§7.3 y 7.4, así como su descripción dada en [31], Proposition 7.8 (ésta extiende de forma sencilla a la del caso $E = \mathbb{Q}_p$).

Proposición 2.5. *Se tiene una equivalencia de categorías*

$$LM_K^E\colon (\underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A/\mathrm{isg})^{\mathrm{op}} \ \simeq\ \varphi\underline{\mathrm{MF}}^2_{KE}\underline{\mathrm{wAd.topNil}}.$$

(La segunda categoría es la subcategoría plena de $\varphi\underline{\mathrm{MF}}^2_{KE}$ de los módulos débilmente admisibles sobre los cuales $\underline{F}$ es topológicamente nilpotente).

Demostración. Teniendo en cuenta la proposición 2.4 (así, como que, para un $A[\underline{F}]$-módulo M libre de tipo finito sobre A, la acción de $\underline{F}$ es topológicamente nilpotente si y solo si así es sobre $K \otimes_A M$) es suficiente probar que se tienen las inclusiones

$$\mathrm{Im}(LM_K^E) \subset \varphi\underline{\mathrm{MF}}^2_{KE}\underline{\mathrm{wAd.topNil}} \subset 2^{\mathrm{o}} \text{ miembro en la proposición 2.4.}$$

La primera inclusión es análoga a [49], Proposition 1.4. En cuanto a la segunda, trasládese la parte correspondiente de las demostraciones (para grupos formales) de [50], Théorème 2.1. □

Nota 2.6. 1. Se puede dar todavía otra caracterización de la imagen esencial de LM_K^E usando ahora la categoría $\varphi\underline{\mathrm{MF}}^{ff2}_{AB}$ (en lugar de $\underline{\mathrm{SH}}^E_A$ de la proposición 2.4). En efecto la subcategoría $\varphi\underline{\mathrm{MF}}^2_{KE}\underline{\mathrm{wAd}}$ coincide con la siguiente

$$\{\ \Delta \in \varphi\underline{\mathrm{MF}}^2_{KE},\ \text{existe un retículo } M \text{ de } \Delta \text{ tal que } (M \cap \Delta^1, M) \in \varphi\underline{\mathrm{MF}}^{ff2}_{AB}\ \}.$$

Además un retículo M de $\Delta \in \varphi\underline{\mathrm{MF}}^2_{KE}\underline{\mathrm{wAd}}$ verifica $(M \cap \Delta^1, M) \in \varphi\underline{\mathrm{MF}}^{ff2}_{AB}$ si y solo si $\varphi(M \cap \Delta^1) \subset \pi M$. Ver [31], Proposition 7.8.

2. En el caso absoluto (el de (1.5.1)) ya habíamos comentado las conjeturas de Fontaine sobre la imagen esencial de LM_K (al final de (1.5.2)), y sobre que "módulo filtrado admisible equivale a débilmente admisible" (nota 2.2). Estas conjeturas tienen una relación vía el teorema 2.3 (ver también la nota 3). Como aplicación de ese teorema, se sigue del teorema 1.9 que, si $d = 1$ ó $e \leq p-1$, entonces

(a) La imagen esencial de LM_K es $\varphi\underline{\mathrm{MF}}^2_K\underline{\mathrm{Ad}}$. Ie, $\varphi\underline{\mathrm{MF}}^2_K\underline{\mathrm{Ad}} = \varphi\underline{\mathrm{MF}}^2_K\underline{\mathrm{wAd}}$. Los grupos p-divisibles fueron usados como puente.

(b) La imagen esencial del funtor $V(-)\colon \underline{p\text{-div}}_A \to \underline{\mathrm{Rep}}(G_K)$ es la categoría de representaciones cristalinas de pesos Hodge-Tate entre 0 y 1 (uso otra vez del teorema 2.3).

3. La conjetura de Fontaine "$\varphi\underline{\mathrm{MF}}_K\underline{\mathrm{Ad}} = \varphi\underline{\mathrm{MF}}_K\underline{\mathrm{wAd}}$" (nota 2.2) ha sido resuelta en [17]. Las restricciones sobre la ramificación para la parametrización de los grupos p-divisibles (ver el teorema 1.7) y las de la nota 2(b) han sido eliminadas en trabajos más recientes de Breuil y Kisin: Los grupos p-divisibles sobre A resultan clasificados mediante objetos adecuados del álgebra semilineal sobre los anillos $W(k)[[t]]$ y la capa de potencias divididas de $W(k)[t]$ respecto al ideal generado por el polinomio de Eisenstein de $K|K_0$ (el *anillo de Breuil*). Ver detalles en [11], o en el survey [12], §III.12. De esta clasificación, [11], Théorème 5.3.2, da la imagen esencial de $V(-)\colon \underline{p\text{-div}}_A \to \underline{\mathrm{Rep}}(G_K)$, como en la nota 2(b), sin restricciones. Usando ahora esto, junto con [49], Proposition 1.4, [27], Théorème 6.2 (aquí el teorema 2.3) y "$\varphi\underline{\mathrm{MF}}_K\underline{\mathrm{Ad}} = \varphi\underline{\mathrm{MF}}_K\underline{\mathrm{wAd}}$" (antes citado), se sigue que la imagen esencial de LM_K es $\varphi\underline{\mathrm{MF}}^2_K\underline{\mathrm{wAd}}$, ie, la conjetura de [26] (y la de Grothendieck) ha sido resuelta ([11], Corollaire 5.3.3).

2.2.3. *Morfismo de comparación reticular de períodos π-ádicos de módulos formales p-divisibles.* Vamos ahora a derivar del teorema de comparación de períodos π-ádicos vectorial (teorema 2.4) su versión reticular. El primer miembro del isomorfismo de ese teorema contiene el retículo $LM^E_A(F)$ (que involucra a $M^E(F)$). En su segundo miembro (involucrando a $T(F)$ y a $A_{cris,A}$) lo apropiado es el siguiente *retículo* de períodos π-ádicos

$$D^*_{cris,A}(F) := \mathrm{Hom}_{B[G_K]}(T(F), A_{cris,A}) \in A[\underline{F}]\,\underline{\text{-Mod}A\text{-fil}},$$

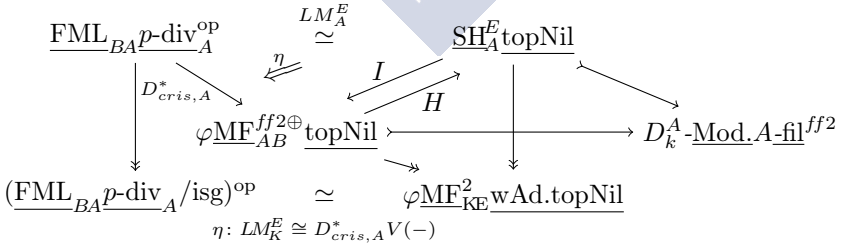
donde el Fröbenius y la filtración están inducidos por los de $A_{cris,A}$ (para $E = \mathbb{Q}_p$ ver [2], §1.2). Téngase en cuenta que $\mathrm{Fil}^i A_{cris,A} := A_{cris,A} \cap t^i B^+_{dR} = A \otimes_{W(k)} \mathrm{Fil}^i A_{cris}$.

La categoría adecuada para el funtor $D^*_{cris,A}$, que se acaba de definir, en lugar de $\underline{\mathrm{SH}}^E_A$ (la del funtor LM^E_A), es ahora la categoría $\varphi\underline{\mathrm{MF}}^{ff2}_{AB}$ de (2.2.2).

Teorema 2.5. *Sea $F \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$. El isomorfismo del* teorema 2.4 *induce, por restricción, un monomorfismo natural* (reticular)

$$\eta_F\colon LM^E_A(F) \rightarrowtail D^*_{cris,A}(F)$$

en la categoría D^A_k-$\underline{\text{Mod } A\text{-fil}}$, dentro de un diagrama funtorial (conmutativo, excepto, obviamente, el "cuadrado que tiene I/H como diagonal")



Además

$$\mathrm{rango}_A D^*_{cris,A}(F) = h_B \quad y \quad \mathrm{rango}_A \mathrm{Fil}^1 D^*_{cris,A}(F) = d.$$

Demostración. Ante todo úsese la nota 2.5 para las dos inclusiones $\rightarrowtail$.

Se tiene $D^*_{cris,A}V(F) = \mathrm{Hom}_{E[G_K]}(V(F), B^+_{cris,A})$ (usando [27], §5.5) $\cong \mathrm{Hom}_{B[G_K]}(T(F), B^+_{cris,A}) \cong K \otimes_A \mathrm{Hom}_{B[G_K]}(T(F), A_{cris,A})$. Así $D^*_{cris,A}(F)$ es un retículo (completo) de $D^*_{cris,A}V(F)$. Además $\mathrm{Fil}^i D^*_{cris,A}(F) = D^*_{cris,A}(F) \cap \mathrm{Fil}^i D^*_{cris,A}V(F)$ (ver la observación que se hizo tras la definición de $D^*_{cris,A}$ en (2.1.3)) y, por lo tanto, $\mathrm{Fil}^i D^*_{cris,A}V(F) \cong K \otimes_A \mathrm{Fil}^i D^*_{cris,A}(F)$ (al ser K el cuerpo de fracciones de A). En consecuencia se tiene un isomorfismo $D^*_{cris,A}V(F) \cong K \otimes_A D^*_{cris,A}(F)$ en la categoría $\varphi\underline{\mathrm{MF}}_{KE}$. Ahora el teorema 2.4 da que $\mathrm{Fil}^i D^*_{cris,A}(F)$ tiene longitud 2 con A-rangos h_B y d.

La inclusión $\varphi\mathrm{Fil}^1 A_{cris} \subset pA_{cris}$ se sigue de $\varphi W^1(\mathcal{R}) \subset W^1(\mathcal{R}) + pW(\mathcal{R})$ (y ésta del hecho general del Fröbenius de un anillo de vectores de Witt $\varphi(\underline{a}) \equiv \underline{a}^p$ mód p, $\underline{a} \in W(\mathcal{R})$). Así $\varphi\mathrm{Fil}^1 A_{cris,A} \subset \pi A_{cris,A} + pA_{cris} = \pi A_{cris,A}$. Por lo tanto

$$\varphi\mathrm{Fil}^1 D^*_{cris,A}(F) \subset \pi D^*_{cris,A}(F). \tag{2.4}$$

Que $\mathrm{Fil}^1 D^*_{cris,A}(F)$ es un sumando directo de $D^*_{cris,A}(F)$ se sigue de la igualdad $\mathrm{Fil}^i D^*_{cris,A}(F) = D^*_{cris,A}(F) \cap \mathrm{Fil}^i D^*_{cris,A}V(F)$ y del lema 2.2.

El teorema 2.4, de nuevo, junto con la proposición 2.5, dan que $D^*_{cris,A}V(F) \in \varphi\underline{\mathrm{MF}}^2_{KE}\underline{\mathrm{wAd}}$. Ahora la nota 2.6.1 y (2.4) dan que $D^*_{cris,A}(F) \in \varphi\underline{\mathrm{MF}}^{ff2}_{AB}$. La nilpotencia topológica de $\underline{F}$ sobre $D^*_{cris,A}(F)$ se sigue con el mismo argumento que en la demostración de la proposición 2.5.

Para $(L, M) \in \underline{\mathrm{SH}}^E_A$ se tiene que $\underline{V}$: $(K \otimes_A L, K \otimes_A M) \to (K \otimes_A \underline{V}L, K \otimes_A M)$ es un morfismo en $\varphi\underline{\mathrm{MF}}_{KE}$ puesto que $\underline{V}\varphi = \varphi\underline{V}(= \pi)$. Además es isomorfismo puesto que lo es π. Por lo tanto el triángulo $\varphi\underline{\mathrm{MF}}_{AB}$, $\underline{\mathrm{SH}}^E_A$, $\varphi\underline{\mathrm{MF}}_{KE}$ es conmutativo.

Que los funtores que terminan en $\varphi\underline{\mathrm{MF}}^2_{KE}\underline{\mathrm{wAd.topNil}}$ son densos se sigue de las proposiciones 2.4 y 2.5 y de la nota 2.6.1. (Esto también puede deducirse de la proposición 2.5 y de la conmutatividad que se acaba de probar). □

Nota 2.7. 1. A diferencia de lo que ocurre en el caso vectorial (teorema 2.4), en el caso reticular el morfismo η_F del teorema 2.5 puede no ser isomorfismo. No lo es de hecho al menos cuando $h_B > d$, puesto que en esta situación la proposición 2.3 da que las subcategorías $\underline{\mathrm{SH}}^{Edh_B}_A\underline{\mathrm{topNil}}$ y $\varphi\underline{\mathrm{MF}}^{ff2\oplus dh_B}_{AB}\underline{\mathrm{topNil}}$, de D^A_k-$\underline{\mathrm{Mod}}$, son disjuntas. (Aunque son equivalentes (proposición 2.2), vistas como subcategorías de D^A_k-$\underline{\mathrm{Mod}}$, sus objetos son estructuralmente distintos.) Esto es coherente con el hecho de que [27], Théorème 6.2, haya sido obtenido del isomorfismo (2.1) y por un camino elaborado. Si tal η_F fuese isomorfismo, entonces éste ya hubiera dado directamente el isomorfismo de [27], Théorème 6.2.

2. La nilpotencia topológica involucrada en (2.2.2) y (2.2.3) (y en los teoremas 1.7, 1.12 y 1.13) se deriva en último término de que el grupo p-divisible subyacente es conexo (ver la proposición 1.23(b)).

3. La filtración adecuada en $D^*_{cris,A}(F)$ es la inducida por la de $A_{cris,A}$ (ver (2.3.1)). En la demostración del teorema 2.5 se muestra que aquella es compatible con la de $D^*_{cris,A}V(F)$, ya que se está en el caso relativamente no ramificado (ver tras la definición de $D^*_{cris,A}$ en (2.1.3)). En la situación absoluta

de (2.1.1) no se tendría esta compatibilidad de filtraciones, salvo en el caso absolutamente no ramificado (ver tras la definición de D^*_{cris} en (2.1.1)). De hecho esto último es la restricción impuesta en [2] y [68].

2.2.4. *Relación con la paridad de períodos p-ádicos explícita de* [16]. El isomorfismo del teorema 2.4 da una *paridad de períodos π-ádicos* (para $F \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$)

$$(K \otimes_A M^E(F)) \times T(F) \to B^+_{cris,A},$$

la cual es una $(K \times B)$-paridad filtrada (conserva la filtración), que además conserva el Fröbenius y la acción de G_K. Para establecer su relación con la paridad de períodos p-ádicos explícita de [16], Proposition 3.1, vamos a mostrar la descripción de $LM^E_K(F)$ en términos de la cohomología de de Rham.

Sea ahora $F \in \underline{p\text{-div}}_A\underline{\text{conexo}}$. Se tiene entonces un diagrama conmutativo

$$\begin{array}{ccccc} K \otimes_{W(k)} \underline{M}(F_k) & \hookleftarrow & A \otimes_{W(k)} \underline{M}(F_k) & \hookrightarrow & H^1_{dR}(F)_{kaz} \\ \cong\downarrow & & \downarrow & & \downarrow \\ K \otimes_A \underline{M}(F_k)_A & \hookleftarrow & \underline{M}(F_k)_A & \xrightarrow{\cong} & \mathbb{MH}_A(F) \end{array}$$

El isomorfismo izquierdo es el de (1.4.1)(a) y el derecho el de la proposición 1.27. La columna derecha (inducida por d^{-1}) y el homomorfismo $\underline{M}(F_k) \to H^1_{dR}(F)_{kaz}$[19] se obtienen como en el caso $A = W(k)$ de la proposición 1.26. Se sigue que la columna central es inyectiva. Por lo tanto lo es $A \otimes_{W(k)} \underline{M}(F_k) \rightarrowtail H^1_{dR}(F)_{kaz}$. Puesto que ambos A-módulos tienen el mismo rango $h = \mathrm{ht}(F)$ (para el rango de $H^1_{dR}(F)_{kaz}$ ver el *crucial resultado* [47], Theorem 5.3.3) este morfismo induce un K-isomorfismo $K \otimes_{W(k)} \underline{M}(F_k) \cong K \otimes_A H^1_{dR}(F)_{kaz} \cong H^1_{dR}(F)_{coz}$. El último isomorfismo es obvio de la definición de $H^1_{dR}(F)_{coz}$ de [16], §3, análoga a la de $H^1_{dR}(F)_{kaz}$ (ver (1.4.2)), pero ahora definiendo

$$K\text{-}\textit{Integrales de segunda especie de } F := \partial^{-1}(K[[\mathbf{X}]] \,\widehat{\otimes}_A K[[\mathbf{X}]]).$$

Por restricción aquel isomorfismo induce uno sobre K_0, $K_0 \otimes_{W(k)} \underline{M}(F_k) \cong H^1_{dR}(F)^{(0)}_{coz}$, donde $H^1_{dR}(F)^{(0)}_{coz} := \{w \in H^1_{dR}(F)_{coz},\ w \text{ tiene coeficientes en } K_0\}$ ([16], §3).

Proposición 2.6. *Los isomorfismos que se acaban de obtener inducen un isomorfismo d, dentro del siguiente triángulo conmutativo en la categoría* $\varphi\underline{\mathrm{MF}}_K$ (junto con la descripción de este último)

$$\begin{array}{ccc} LM_K(F) & \overset{d}{\cong} & H^1_{dR}(F)^{(0)}_{coz} \\ \eta_F \cong & & \cong \int_o w \\ D^*_{cris}V(F) & & \end{array} \qquad \begin{array}{ccc} \lambda \in K \otimes_{W(k)} \underline{M}(F_k) \subset K[[\mathbf{X}]]_0 & \hookrightarrow & d\lambda = w \in H^1_{dR}(F)_{coz} \\ & \searrow \qquad \nearrow & \\ \eta_F(\lambda) = l = [o \mapsto \int_o w] \in \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(T(F), B^+_{cris,A})^{20} & & \end{array}$$

[19] $\underline{M}(F_k) \to H^1_{dR}(F)_{kaz}$ involucra ahora a $\hat{w}_G$ de la proposición 1.24(a). En el caso $e < p-1$ (*poco ramificado*) $A \otimes_{W(k)} \underline{M}(F_k) \to H^1_{dR}(F)_{kaz}$ es isomorfismo ([13], Theorem 1.4).

[20] El módulo filtrado $H^1_{dR}(F)^{(0)}_{coz}$ da la "filtración de Hodge" de $H^1_{dR}(F)_{coz}$.

El morfismo derecho está dado por la integración p-ádica sobre grupos formales de Colmez ([16], Proposition 3.1, que da una descripción explícita de la paridad de períodos p-ádicos)

$$\int_o w := \lim_{s\to\infty} p^s \lambda(\hat{o}_s),$$

donde $o = (o_s) \in T(F) = \varprojlim F[p^s]$ *y* $\hat{o}_s \in F(W_A(\mathfrak{m}_{\mathcal{R}}))$, $\theta(\hat{o}_s) = o_s$. ($W_A(\mathcal{R}) := A\otimes_{W(k)}W(\mathcal{R})$ y $\theta\colon F(W_A(\mathfrak{m}_{\mathcal{R}})) \twoheadrightarrow F(\mathfrak{m}_C) \supset F[p^s](\mathfrak{m}_C)$, ver (1.8). Para $F(W_A(\mathfrak{m}_{\mathcal{R}}))$ ver la nota 2.9).

Demostración. Continuamos ahora el argumento que precede a esta proposición. La inclusión en $K[[\mathbf{X}]]_0$ es vía la proposición 1.26 (ver la nota 1.19). Las formas de primera especie $\Omega_A(F)$ dan la filtración de $H^1_{dR}(F)_{kaz}$. Luego se filtra a $H^1_{dR}(F)_{coz} = K\otimes_{K_0} H^1_{dR}(F)_{kaz}$ con el K-subespacio $\mathrm{Fil}^1 H^1_{dR}(F)_{coz} := \Omega(F) = K\otimes_A \Omega_A(F)$ (ver (1.4.2) y (1.5.1)). Así se tiene $H^1_{dR}(F)^{(0)}_{coz} := (\Omega(F), H^1_{dR}(F)^{(0)}_{coz}) \in \varphi\underline{\mathrm{MF}}_K$, y que el K-isomorfismo $d\colon K\otimes_{W(k)} \underline{M}(F_k) \cong H^1_{dR}(F)_{coz}$ es filtrado puesto que d induce un isomorfismo $K\otimes_A \mathscr{L}_A(F) \cong \Omega(F)$ (ver (1.5.1)). El isomorfismo $K_0\otimes_{W(k)} \underline{M}(F_k) \cong H^1_{dR}(F)^{(0)}_{coz}$ conmuta con la acción de $\underline{F}$ puesto que esta acción en ambos miembros está inducida por el isomorfismo $\underline{M}(F_k) \cong \mathrm{MH}_{W(k)[[\mathbf{X}]]}(F_k)$ de la proposición 1.26 (ver la proposición 1.24). Obtenemos así que $d\colon LM_K(F) \cong H^1_{dR}(F)^{(0)}_{coz}$ es un isomorfismo en $\varphi\underline{\mathrm{MF}}_K$.

Por conmutatividad el morfismo derecho del enunciado es isomorfismo. La conmutatividad se sigue de la igualdad de las integraciones p-ádicas de diferenciales de [16] y de [25]. (Tal igualdad se muestra, eg, en [13], p. 546.) □

Sea ahora $F \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$. Así se tiene un morfismo de K-espacios vectoriales filtrados $K\otimes_A M^E(F) \rightarrowtail K\otimes_{W(k)} \underline{M}(F_k)$ (ver la demostración del teorema 2.4). Denótese $H^1_{dR}(F)^E_{coz}$ el K-subespacio filtrado de $H^1_{dR}(F)_{coz}$ correspondiente a $K\otimes_A M^E(F)$ mediante el K-isomorfismo filtrado $K\otimes_{W(k)} \underline{M}(F_k) \cong H^1_{dR}(F)_{coz}$ de la proposición 2.6. Así $H^1_{dR}(F)^E_{coz} \in \varphi\underline{\mathrm{MF}}_{KE}$ y $\mathrm{Fil}^1 H^1_{dR}(F)^E_{coz} = \Omega(F)$.

Corolario 2.1. *Se tiene un triángulo conmutativo en la categoría* $\varphi\underline{\mathrm{MF}}_{KE}$

$$\begin{array}{ccc} LM^E_K(F) & \overset{d}{\cong} & H^1_{dR}(F)^E_{coz} \\ {\scriptstyle \eta_F\cong} & & {\scriptstyle \cong \int_o w} \\ & D^*_{cris,A}V(F) & \end{array}$$

(con descripción análoga a la de la proposición 2.6*).*

Demostración. Por restricción en la proposición 2.6 y uso del teorema 2.4. □

Nota 2.8. La descripción explícita de la paridad de períodos p-ádicos de [16] da ahora, por restricción, la siguiente descripción para la paridad de períodos π-ádicos ($d\lambda = w$)

$$\int_o w = \lim_{s\to\infty} \pi^s \lambda(\hat{o}_s),$$

donde $o = (o_s) \in T(F) = \varprojlim F[\pi^s]$ y $\hat{o}_s \in F(W_A(\mathfrak{m}_{\mathcal{R}}))$, $\theta(\hat{o}_s) = o_s$. De hecho $\lim_{s\to\infty} p^s\lambda(\hat{o}_s) = \lim_{s\to\infty} \pi^{es}\lambda(\hat{o}_{es}) = \lim_{s\to\infty} \pi^s\lambda(\hat{o}_s)$.

2.3. Sustitución del módulo formal

En la situación de (2.1.3) sea $F \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$, $d = \dim F$, $h_B = \mathrm{ht}_B(F)$. En secciones anteriores hemos obtenido los resultados y preparación cruciales y necesarios para que la extensión y adaptación a módulos formales de la idea y argumentos para el caso $E = \mathbb{Q}_p$ de [2], §§1.3-1.7 y 2.1 (y de [68], §§2.1 y 2.2), basados en la estructura de $D^*_{cris}(F)$, e involucrando la sustitución del grupo formal, esté preparada y pueda ser realizada. Por lo tanto en esta sección (y en el capítulo siguiente) vamos a mostrar someramente los ingredientes y el hilo de la citada adaptación.

2.3.1. El método de períodos π-ádicos a fórmulas explícitas, extensión y adaptación de [2] y de [68], usa, en lugar de la estructura de $LM^E_A(F) \in \underline{\mathrm{SH}}^E_A$ de (1.6.3), la de $D^*_{cris,A}(F) \in \varphi\underline{\mathrm{MF}}_{AB}$, sobre la cual informa el teorema 2.5.

Ese teorema 2.5 *se usa, en primer lugar, para comenzar eligiendo una A-base filtrada $(\underline{l}, \underline{m})$ de $D^*_{cris,A}(F)$. Así los cardinales son $|\underline{l}| = d$ y $|\underline{m}| = h_B - d$.*

Bajo los isomorfismos del corolario 2.1 denotemos también $(\underline{l}, \underline{m})$ el sistema de $LM^E_K(F)$ tal que $\eta_F(\underline{l}, \underline{m}) := (\underline{l}, \underline{m})$. Así se tiene

$$\underline{l}(o) = \textstyle\int_o d\,\underline{l} \in (B^+_{cris,A})^d \quad \text{y} \quad \underline{m}(o) = \textstyle\int_o d\,\underline{m} \in (B^+_{cris,A})^{h_B - d}.$$

En esta situación la demostración en el caso $E = \mathbb{Q}_p$ de [2], Lemma 1.5.1 es válida también en nuestro caso relativo puesto que $A_{cris,A}$ es también la p-completación (o π-completación) de la capa de potencias divididas de $W_A(\mathcal{R})$ respecto a $W^1_A(\mathcal{R})$. Así se tiene

Lema 2.3. *La serie $\underline{l} \in (K \otimes_A \mathscr{L}_A(F))^d = \mathrm{Hom}_K(F, \mathbb{G}_a)^d$* (ver la nota 1.22.1) *induce un $B[G_K]$-homomorfismo inyectivo continuo dentro de un diagrama*

$$\begin{array}{ccc} F(W^1_A(\mathfrak{m}_{\mathcal{R}})) & \rightarrowtail & (\mathrm{Fil}^1 A_{cris,A})^d \\ \downarrow & & \downarrow \\ F(W_A(\mathfrak{m}_{\mathcal{R}})) & \xrightarrow{\underline{l}} & (B^+_{cris,A})^d \end{array}$$

□

Corolario 2.2. $\underline{l}\colon F(\mathfrak{m}_{\mathcal{R}}) \to (B^+_{cris,A})^d$ mód $\pi W_A(\mathfrak{m}_{\mathcal{R}})$ *es inyectiva.*

Demostración. La demostración de [2], Corollary 1.5.1, sólo depende del hecho de que $\underline{l} \in \mathrm{Hom}_K(F, \mathbb{G}_a)^d$, y así se traslada aquí. □

Nota 2.9. Respecto al corolario 2.2, $F(\mathfrak{m}_{\mathcal{R}})$ está definido ya que se tiene $F(\mathfrak{m}_{\mathcal{R}}) = F(W_A(\mathfrak{m}_{\mathcal{R}})/\pi W_A(\mathfrak{m}_{\mathcal{R}}))$. En cuanto al lema 2.3 se tiene que $F(W(\mathfrak{m}_{\mathcal{R}}))$ *está definido*. En efecto, la topología natural del anillo de valoración discreta completo $W(\mathrm{Frac}(\mathcal{R}))$ es la p-ádica, y $W(\mathcal{R})$ es un p-anillo estricto ([59], Chap. II, Theorems 5 y 7). Pero *si se toma en $W(\mathcal{R})$ la topología* (más débil) *producto de las v-topologías de $\mathcal{R}$*, que también es la topología límite inverso de las topologías producto de $W_n(\mathcal{R}) \cong \mathcal{R}^n$ (para la cual $W(\mathcal{R})$ también es completo), entonces

(a) esta topología es J-ádica, $J = W(\mathfrak{m}_{\mathcal{R}}) + pW(\mathcal{R})$ (ver [27], §2.2, [68], §1.2), y así $W(\mathcal{R})$ está en el caso (1.7) de grupo de puntos (1.2.3).

(b) si $x \in W(\mathfrak{m}_{\mathcal{R}})$, entonces x es topológicamente nilpotente de $W(\mathcal{R})$ para aquella topología producto.

Puesto que $\theta(\pi^s 1_F(\hat{o}_s)) = \pi^s 1_F(o_s) = o_0 = 0$ ($\hat{o}_s$ como en la proposición 2.6) se sigue que $\pi^s 1_F(\hat{o}_s) \in F(W_A^1(\mathfrak{m}_{\mathcal{R}}))$. Al tratarse de un subconjunto cerrado la sucesión $\pi^s 1_F(\hat{o}_s)$ convergerá en $F(W_A^1(\mathfrak{m}_{\mathcal{R}}))$ si fuese de Cauchy. Esto se sigue (análogamente al caso $E = \mathbb{Q}_p$) de la nilpotencia topológica de $\pi 1_F$ sobre $F(W_A(\mathfrak{m}_{\mathcal{R}}))$, uniforme en $F(W_A^1(\mathfrak{m}_{\mathcal{R}}))$, lo cual se reduce a mismo hecho para $E = \mathbb{Q}_p$, y esto último es [68], Lemma 2.1.(2). Por lo tanto $\underline{l}(o) = \underline{l}\left(\lim_{s\to\infty} \pi^s 1_F(\hat{o}_s)\right)$ y $\underline{m}(o) = \underline{m}\left(\lim_{s\to\infty} \pi^s 1_F(\hat{o}_s)\right)$.

Lema 2.4. *La aplicación $j(o) := \lim_{s\to\infty} \pi^s 1_F(\hat{o}_s)$ sólo depende de o, y da lugar a un $B[G_K]$-homomorfismo continuo inyectivo dentro de un diagrama conmutativo filtrado*

$$\begin{array}{ccc} T(F) & \xrightarrow{(\underline{l},\underline{m})} & A_{cris,A}^{h_B} \\ & {\scriptstyle j}\searrow \quad \nearrow{\scriptstyle (\underline{l},\underline{m})} & \\ & F(W_A^1(\mathfrak{m}_{\mathcal{R}})) & \end{array}$$

Demostración. La discusión previa da la conmutatividad, viendo j como una relación. Que j es una aplicación, ie, que sólo depende de o, se sigue del lema 2.3 así como del hecho de que $\int_o w$ sólo depende de o ([16], Proposition 3.1). Además j es inyectiva puesto que lo es $(\underline{l},\underline{m})\colon T(F) \to A_{cris,A}^{h_B}$ al ser $(\underline{l},\underline{m})$ una A-base. □

2.3.2. Puesto que $D^*_{cris,A}(F) \in \varphi\underline{\mathrm{MF}}^{ff2\oplus}_{AB}\,\underline{\mathrm{topNil}}$ (*uso del* teorema 2.5, *de nuevo*) y como consecuencia de la estructura de los objetos de $\varphi\underline{\mathrm{MF}}^{ff2}_{AB}$, sea $\mathcal{E} \in \mathrm{GL}_{h_B}(A)$ la matriz tal que

$$\begin{pmatrix} \frac{\varphi}{\pi}\underline{l} \\ \varphi\underline{m} \end{pmatrix} = \mathcal{E}\begin{pmatrix} \underline{l} \\ \underline{m} \end{pmatrix}$$

y denótese $\mathcal{E}^{-1} =: \begin{pmatrix} A & B \\ C & D \end{pmatrix}$. Por la nilpotencia topológica de φ sobre $D^*_{cris,A}(F)$ la igualdad precedente puede ser reformulada en la forma (ver [2], §1.3)

$$\underline{l} = \sum_{u\geq 1} F_u \frac{\varphi^u \underline{l}}{\pi} \quad \text{y} \quad \underline{m} = \sum_{u\geq 1} F'_u \frac{\varphi^u \underline{l}}{\pi},$$

donde $F_1 = A,\ F_2 = B\varphi(C),\ F_u = B\left(\prod_{k=1}^{u-2}\varphi^k(D)\right)\varphi^{u-1}(C)$, y $F'_1 = C,\ F'_2 = D\varphi(C),\ F'_u = D\left(\prod_{k=1}^{u-2}\varphi^k(D)\right)\varphi^{u-1}(C),\ u \geq 3$. Se define la matriz (operador B-lineal)

$$\mathcal{A} := \sum_{u\geq 1} F_u \underline{F}^u \in A^{d\times d}\left[[\underline{F}]\right],$$

para que así $\underline{l}$ verifique la ecuación funcional

$$(I - \frac{\mathcal{A}}{\pi})\underline{l} = 0 \tag{2.5}$$

De esto se sigue que

$$\mathrm{Im}(\underline{l}) = ((\mathrm{Fil}^1 A_{cris,A})^d)^{\frac{\mathcal{A}}{\pi}-I=0} \quad \text{e} \quad \mathrm{Im}(j) = F(W_A^1(\mathfrak{m}_{\mathcal{R}}))^{(\frac{\mathcal{A}}{\pi}-I)\underline{l}=0}$$

El argumento de [2], Lemma 1.6.2, pero aquí usando la ecuación funcional (2.5) en lugar de la de allí, da también (teniendo en cuenta, además, el corolario 2.2) que $F(\mathfrak{m}_{\mathcal{R}})$ *es únicamente* π*-divisible* ("π-divisible" equivale a "p $(= \pi^e)$-divisible"). Por lo tanto, para cada $x \in F(\mathfrak{m}_{\mathcal{R}})$, existe un único $x_s \in F(\mathfrak{m}_{\mathcal{R}})$ para todo $s \geq 0$, tal que $[\pi^s]_F(x_s) = x$. Entonces, como en [2], Lemma 2.2.1, se tiene

Lema 2.5. (a) *Existe* $\delta(x) := \lim\limits_{s\to\infty} [\pi^s]_F(x_s) \in F(W_A(\mathfrak{m}_{\mathcal{R}}))$.

(b) *Esto define un* G_K*-morfismo*

$$\delta\colon F(\mathfrak{m}_{\mathcal{R}}) \to F(W_A(\mathfrak{m}_{\mathcal{R}}))^{(\mathcal{A}-\pi I)\underline{l}=0}$$

tal que $[x] \equiv \delta(x)$ mód $\pi W_A(\mathfrak{m}_{\mathcal{R}})$ *y* $\theta\delta(x) = \theta[x]$. □

Proposición 2.7. *Para la aplicación* $(\mathcal{A}-\pi I)\underline{l}\colon F(W_A(\mathfrak{m}_{\mathcal{R}}) \to (B^+_{cris,A})^d$ *se tiene*

(a) $(\mathcal{A}-\pi I)\underline{l}F(W_A(\mathfrak{m}_{\mathcal{R}})) = (\mathcal{A}-\pi I)\underline{l}F(W_A^1(\mathfrak{m}_{\mathcal{R}})) = (\mathcal{A}-\pi I)\underline{l}F(\pi W_A^1(\mathfrak{m}_{\mathcal{R}})) = \pi W_A(\mathfrak{m}_{\mathcal{R}})^d$.

(b) *La siguiente sucesión es exacta (donde* j *es la del* lema 2.4*)*

$$0 \to T(F) \xrightarrow{j} F(W_A^1(\mathfrak{m}_{\mathcal{R}})) \xrightarrow{(\frac{\mathcal{A}}{\pi}-I)\underline{l}} W_A(\mathfrak{m}_{\mathcal{R}})^d \to 0.$$

Demostración. Como en [2], Proposition 2.1, (b) se sigue de (a), y (a) se sigue del lema 2.5 junto con la expresión para $\mathrm{Im}(j)$ mostrada previamente. □

Nota 2.10. Sea ε un generador topológico de $T(\mathbb{G}_m) = \mathbb{Z}_p(1) \subset \mathcal{R}$ (ver el ejemplo 1.4), y denótese (como en [68], §1.2)

$$X := [\varepsilon] - 1 \in W^1(\mathfrak{m}_{\mathcal{R}}).$$

Como en [2], Remark 1.7.5, también ahora se tiene que el diagrama del lema 2.4 toma valores en el subanillo (filtrado) $W_A(\mathcal{R})\big[\big[X^{p-1}/p\big]\big]$ de $A_{cris,A}$.

2.3.3. A partir de ahora es conveniente (necesario, ver las notas 2.11 y 2.13, más adelante) cambiar el módulo formal F por otro $F_{\mathcal{A}}$ sobre el cual, usando el método y argumentos de [2] y [68], será ultimado el cálculo de las fórmulas explícitas buscadas.

Para la matriz $u := \pi I - \mathcal{A} \in K[[\underline{F}]]^{d\times d}$, que es especial, se denota

$$l_{\mathcal{A}}(\mathbf{X}) := u^{-1}\pi * \mathbf{X} = (I - \frac{\mathcal{A}}{\pi})^{-1}(\mathbf{X}) = \mathbf{X} + \sum_{m\geq 1} \frac{\mathcal{A}^m(\mathbf{X})}{\pi^m} \in K[[\mathbf{X}]]_0^d$$

(ver (1.6.2)). Así $l_{\mathcal{A}}$ es tipo u (proposición 1.31(a)). Su ecuación funcional es en este caso $(I - \frac{\mathcal{A}}{\pi})l_{\mathcal{A}} = \mathbf{X}$ (comparar con la de (2.5) para $\underline{l}$). Según el teorema 1.11 y la proposición 1.33 se sigue que

$$F_{\mathcal{A}}(\mathbf{X}, \mathbf{Y}) := l_{\mathcal{A}}^{-1}(l_{\mathcal{A}}(\mathbf{X}) + l_{\mathcal{A}}(\mathbf{Y})) \in \underline{\mathrm{FML}}_{BA}.$$

Pongamos también

$$m_{\mathcal{A}}(\mathbf{X}) := \sum_{m\geq 1} F'_m \frac{\varphi^m l_{\mathcal{A}}}{\pi} \in K[[\mathbf{X}]]_0^{h_B-d},$$

de tal forma que ahora se tiene

$$\begin{pmatrix} \frac{\varphi}{\pi} l_{\mathcal{A}} \\ \varphi m_{\mathcal{A}} \end{pmatrix} = \mathcal{E} \begin{pmatrix} \frac{\mathcal{A}}{\pi} l_{\mathcal{A}} \\ m_{\mathcal{A}} \end{pmatrix} \tag{2.6}$$

y un morfismo inyectivo

$$LM_K^E(F) \rightarrowtail LM_K^E(F_{\mathcal{A}})$$

en la categoría $\varphi\underline{\mathrm{MF}}_{KE}$, dado por $(\underline{l}, \underline{m}) \mapsto (l_{\mathcal{A}}, m_{\mathcal{A}})$, que es isomorfismo sobre Fil[1] ya que $\mathscr{L}_A(F_{\mathcal{A}}) =< l_{\mathcal{A}}(= \lambda_{F_{\mathcal{A}}}) >$, ver el teorema 1.10 y la nota 1.22.1. Por lo tanto aquel morfismo es isomorfismo si y solo si $h = h_{\mathcal{A}}$, las alturas de F y $F_{\mathcal{A}}$. En cuanto a la comparación de las alturas

Proposición 2.8. (a) $h \leq h_{\mathcal{A}}$.

(b) $h_B = d$ *si y solo si* $h_{B\mathcal{A}}$ $(:= h_{\mathcal{A}}/\,[E{:}\mathbb{Q}_p]) = d$.

(c) *Si* $d = 1$, *entonces* $\psi_1 := l_{\mathcal{A}}^{-1}\lambda_F \colon F \overset{\sim}{\equiv} F_{\mathcal{A}}$ *sobre* A. *En particular* $h = h_{\mathcal{A}}$.

Demostración. (a) Se sigue del morfismo inyectivo previo teniendo en cuenta la expresión para h_B del teorema 1.13.

(b) Puesto que $h \leq h_{\mathcal{A}}$ sólo resta el "sólo si". Puesto que ahora $\mathcal{E}^{-1} = A$, y así $u = \pi I - A\underline{F}$, es fácil adaptar el argumento para $d = 1$ de [43], demostración de Proposition 3.5, y obtener $[\pi]_{(F_{\mathcal{A}})_k}(\mathbf{X}) = \pi\mathbf{X} + A\mathbf{X}^q + \cdots$. Así rango $[\pi]_{(F_{\mathcal{A}})_k}(\mathbf{X}) = q^d$, y $h_{B\mathcal{A}} = d$ (ver (1.6.3)).

(c) Se tiene $\lambda_F = P^{-1}\underline{l}$, $P^{-1} \in \mathrm{GL}_d(A)$ (ver (2.3.4), más adelante). Entonces $u * \lambda_F = (uP^{-1}) * \underline{l} \equiv 0$ (mód π) si P conmutase con u, lo que ocurre si $d = 1$. Usar ahora el teorema 1.11. □

Mostraremos más adelante que $F \cong F_{\mathcal{A}}$. Pero desde ahora vamos a suponer solamente que $h_{\mathcal{A}} < \infty$ (ie, que también $F_{\mathcal{A}} \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$). Los isomorfismos del corolario 2.1 para $F_{\mathcal{A}}$ permiten definir ahora el sistema filtrado $(\hat{\underline{l}}, \hat{\underline{m}})$ en $D^*_{cris,A}V(F_{\mathcal{A}})$ como sigue

$$\begin{array}{ccccc} LM_K^E(F_{\mathcal{A}}) & \overset{d}{\cong} & H^1_{dR}(F_{\mathcal{A}})^E_{coz} & & (l_{\mathcal{A}}, m_{\mathcal{A}}) \longleftrightarrow (dl_{\mathcal{A}}, dm_{\mathcal{A}}) \\ {\scriptstyle \eta_{F_{\mathcal{A}}}}\cong & & \cong {\scriptstyle \int_o w} & & \nwarrow \quad \nearrow \\ D^*_{cris,A}V(F_{\mathcal{A}}) & & & & (\hat{\underline{l}}, \hat{\underline{m}}) := \eta_{F_{\mathcal{A}}}(l_{\mathcal{A}}, m_{\mathcal{A}}) \end{array}$$

Por lo tanto, para $o \in T(F_{\mathcal{A}})$, se tiene (ver la nota 2.8)

$$\hat{\underline{l}}(o) = \int_o dl_{\mathcal{A}} = \lim_{s\to\infty} \pi^s l_{\mathcal{A}}(\hat{o}_s) \in (B^+_{cris,A})^d$$

$$\hat{\underline{m}}(o) = \int_o dm_{\mathcal{A}} = \lim_{s\to\infty} \pi^s m_{\mathcal{A}}(\hat{o}_s) \in (B^+_{cris,A})^{h_B-d}.$$

Los resultados de (2.3.1) y (2.3.2) para F y $(\underline{l}, \underline{m})$ son válidos de forma análoga para $F_{\mathcal{A}}$, $(l_{\mathcal{A}}, m_{\mathcal{A}})$ y $(\hat{\underline{l}}, \hat{\underline{m}})$. Así, como en el lema 2.4 y en la nota 2.10, se tiene un diagrama conmutativo filtrado

$$\begin{array}{ccc} T(F_{\mathcal{A}}) & \xrightarrow{(\hat{\underline{l}},\hat{\underline{m}})} & W_A(\mathcal{R})\big[\big[X^{p-1}/p\big]\big]^{h_{B\mathcal{A}}} \\ \downarrow j & \nearrow_{(l_{\mathcal{A}},m_{\mathcal{A}})} & \\ F_{\mathcal{A}}(W_A^1(\mathfrak{m}_{\mathcal{R}})) & & \end{array}$$

así como la igualdad $\begin{pmatrix} \varphi\hat{\underline{l}} \\ \pi\hat{\underline{m}} \end{pmatrix} = \mathcal{E}\begin{pmatrix} \hat{\underline{l}} \\ \hat{\underline{m}} \end{pmatrix}$. Entonces $(\hat{\underline{l}},\hat{\underline{m}})$ está en $D^*_{cris,A}(F_{\mathcal{A}})$ (filtrado) y por lo tanto $(\underline{l},\underline{m}) \mapsto (\hat{\underline{l}},\hat{\underline{m}})$ induce un morfismo en $\varphi\underline{\mathrm{MF}}_{AB}$ inyectivo

$$D^*_{cris,A}(F) \rightarrowtail D^*_{cris,A}(F_{\mathcal{A}}). \tag{2.7}$$

Esta construcción de $(l_{\mathcal{A}}, m_{\mathcal{A}})$ da, además, como en [2], Lemma 1.7.6

Proposición 2.9. *Se tiene un homomorfismo*

$$l_{\mathcal{A}}\colon F_{\mathcal{A}}(W_A^1(\mathfrak{m}_{\mathcal{R}})) \rightarrowtail (W_A^1(\mathfrak{m}_{\mathcal{R}}) + \frac{X^{p-1}}{p}W_A(\mathcal{R})\big[\big[X^{p-1}/p\big]\big])^d. \qquad \square$$

Nota 2.11. Si se compara esta situación para $F_{\mathcal{A}}$ con la de F (comienzo de (2.3.1)) nótese que ahora $l_{\mathcal{A}} = \lambda_{F_{\mathcal{A}}}$, mientras que allí $< \underline{l} >_A = \mathrm{Fil}^1 D^*_{cris,A}(F) \supset \mathscr{L}_A(F) =< \lambda_F >_A$ (la inclusión vía η_F, ver al comienzo de (2.3.4)). Pero las fórmulas explícitas finales han de ser en términos de logaritmos. Otra diferencia entre ambas situaciones está en las ecuaciones funcionales de $F_{\mathcal{A}}$ y de F ((2.5) y la del comienzo de esta subsección para $l_{\mathcal{A}}$). De hecho la proposición 2.9, y el lema 2.6, más adelante (necesarios para las fórmulas explícitas, ver la sección 3.2) son para $F_{\mathcal{A}}$.

2.3.4. Teniendo en cuenta la nota 2.11 y siguiendo todavía a [2], §§1.3-1.5, buscamos un isomorfismo canónico $F \cong F_{\mathcal{A}}$ sobre A, de sustitución.

Puesto que $l_{\mathcal{A}}$ es de tipo $u = \pi I - \mathcal{A}$, y $u * \underline{l} \cong 0$ (mód π) por (2.5), para usar [43], Lemma 2.4 y Theorem 2, se necesita una matriz $P \in \mathrm{GL}_d(A)$ tal que $\underline{l} \equiv P\mathbf{X}$ (mód deg 2). Para ello, y también para simplificar, se va a ver como una inclusión el morfismo de comparación reticular del teorema 2.5. Así

$$\eta_F\colon \mathscr{L}_A(F) =< \lambda_F >_A \subset \mathrm{Fil}^1 D^*_{cris,A}(F) =< \underline{l} >_A,$$

y sea $P \in \mathrm{GL}_d(K)$ tal que $P\lambda_F = \underline{l}$ (así $P^{-1} \in A^{d\times d}$), de forma que $\underline{l} \equiv P\mathbf{X}$ (mód deg 2). Se tiene $\psi := l_{\mathcal{A}}^{-1}\underline{l}\colon F \cong F_{\mathcal{A}}$ sobre K.

Proposición 2.10. *Con la notación anterior las siguientes condiciones son equivalentes*

(i) $\psi\colon F \cong F_{\mathcal{A}}$ *es sobre* A

(ii) $P \in \mathrm{GL}_d(A)$

(iii) $\eta_F\colon \mathscr{L}_A(F) = \mathrm{Fil}^1 D^*_{cris,A}(F)$

(iv) $\underline{l}$ *es tipo* $(P;u)$

(v) $\psi\colon F \cong F_{\mathcal{A}}$ *es sobre* A, *y* $\psi_*\colon D^*_{cris,A}(F) \cong D^*_{cris,A}(F_{\mathcal{A}})$ *es el morfismo* (2.7). *En particular* $(\hat{\underline{l}},\hat{\underline{m}})$ *es una* A*-base de* $D^*_{cris,A}(F_{\mathcal{A}})$.

(vi) *Existe* $\chi\colon F \cong F_{\mathcal{A}}$ *sobre* A *tal que* $\chi_*\colon D^*_{cris,A}(F) \cong D^*_{cris,A}(F_{\mathcal{A}})$ *es el morfismo* (2.7).

Demostración. Las equivalencias (i)-(iv) se siguen de [43], Lemma 2.4. (vi) $\Leftrightarrow$ (v) es inmediata. (i) $\Rightarrow$ (v) En el K-isomorfismo $\psi_*\colon D^*_{cris,A}V(F) \cong D^*_{cris,A}V(F_{\mathcal{A}})$ se corresponden, por construcción, las K-bases filtradas $(\underline{l},\underline{m})$ y $(\hat{\underline{l}},\hat{\underline{m}})$. Puesto que $(\hat{\underline{l}},\hat{\underline{m}}) \subset D^*_{cris,A}(F)$ y $\psi_*\colon D^*_{cris,A}(F) \cong D^*_{cris,A}(F_{\mathcal{A}})$ es la restricción del anterior K-isomorfismo, ha de estar inducido por $(\underline{l},\underline{m}) \mapsto (\hat{\underline{l}},\hat{\underline{m}})$, ie, es el morfismo (2.7). □

Nota 2.12. 1. Recuérdese de la nota 2.7 que, cuando $h_B > d$, se tiene una inclusión propia

$$\eta_F\colon LM^E_A(F) \subsetneq D^*_{cris,A}(F).$$

Pero sobre Fil^1 todavía se podría tener igualdad, en cuyo caso las condiciones de la proposición 2.10 serían verdaderas.

2. En el caso $h_B = d$ y si P conmuta con $A(=\mathcal{E})$ (en particular para el caso Lubin-Tate relativo), se podría probar de forma paralela a la proposición 2.8(c) que $\psi_1 := l_{\mathcal{A}}^{-1}\lambda_F\colon F \stackrel{\sim}{\equiv} F_{\mathcal{A}}$ sobre A. Se sigue que $\hat{\underline{l}}$ es una A-base de $D^*_{cris,A}(F_{\mathcal{A}})$ y que el monomorfismo (2.7) es un isomorfismo (pero no está necesariamente inducido por ψ_1, por lo que esto es más débil que (vi) de la proposición 2.10). En el caso de la proposición 2.8(c), aunque $F \stackrel{\sim}{\equiv} F_{\mathcal{A}}$, no se tiene necesariamente que (2.7) es un isomorfismo. En cualquier caso, los resultados de [19] (aquí (1.6.3)) dan validez para el caso relativo de módulos formales al argumento de [2], §1.4 para el isomorfismo entre F y $F_{\mathcal{A}}$.

3. La condición (vi) de la proposición 2.10 es la versión para módulos formales de [2], Proposition 1.5.2, cuya adaptación a nuestro caso relativo es directa. En efecto, por lo que hemos expuesto en (1.6.1), (1.6.2) y (2.1.1), los argumentos generales allí mencionados para esa proposición son claramente válidos en el contexto relativo de módulos formales. Así, *podemos dar por verdaderas las condiciones equivalentes de la* proposición 2.10. Por lo tanto *vamos a suponer que* $F = F_{\mathcal{A}}$.

En cualquier caso nótese que para esto último incluso sería suficiente la condición más débil de que *el morfismo* (2.7) *es isomorfismo*. Ver la nota 2. También sería suficiente la condición más débil $F \stackrel{\sim}{\equiv} F_{\mathcal{A}}$ (ver de nuevo la nota 2). En efecto, los argumentos que siguen darían todavía una matriz de períodos π-ádicos (ver más abajo), que permitiría, como luego se mostrará en el capítulo 3, obtener una fórmula explícita para $F_{\mathcal{A}}$ (que se trasladaría a F).

Para la paridad de períodos π-ádicos (cf. (2.2.4)) se tiene la *paridad de períodos π-ádicos reticular*, la cual, por la nota 2.12.3 ($F = F_{\mathcal{A}}$) y usando la proposición 2.9, resulta como sigue

$$< , >\colon D^*_{cris,A}(F) \otimes_B T(F) \to W_A(\mathfrak{m}_{\mathcal{R}}) + \frac{X^{p-1}}{p}W_A(\mathcal{R})\left[\left[\frac{X^{p-1}}{p}\right]\right].$$

Está determinada por

$$< \hat{\underline{l}}, o >:= \hat{\underline{l}}(o) = \textstyle\int_o dl_{\mathcal{A}} \quad \text{y} \quad < \hat{\underline{m}}, o >:= \hat{\underline{m}}(o) = \textstyle\int_o dm_{\mathcal{A}}.$$

Análogamente al caso absolutamente no ramificado de [2], (1.5.3) y [68], p. 290, se define la *matriz de períodos π-ádicos* (para F) como la matriz de la

paridad reticular anterior respecto a la base $(\hat{\underline{l}}, \underline{\hat{m}})$ de $D^*_{cris,A}(F)$ (proposición 2.10 y nota 2.12.2 y 3) y una *B-base prefijada* $o = (o^1, \dots, o^{h_B})$ de $T(F)$ (uso de la proposición 2.1), ie

$$\mathcal{V} := \begin{pmatrix} < \hat{\underline{l}}, o^1 > & \dots & < \hat{\underline{l}}, o^{h_B} > \\ < \underline{\hat{m}}, o^1 > & \dots & < \underline{\hat{m}}, o^{h_B} > \end{pmatrix},$$

la cual pertenece a $\mathrm{GL}_{h_B}(\mathrm{Frac}(W_A(\mathcal{R})\big[\big[X^{p-1}/p\big]\big])) \cap W_A(\mathcal{R})\big[\big[X^{p-1}/p\big]\big]^{h_B \times h_B}$.

Sea $(o^1, \dots, o^{h_B}) := 1 \otimes (o^1, \dots, o^{h_B})$ la $A_{cris,A}$-base de $A_{cris,A} \otimes_B T(F)$, y U las coordenadas de $u \in A_{cris,A} \otimes_B T(F)$ en la base $(o^1, \dots, o^{h_B})\mathcal{V}^{-1}$. Es fácil comprobar que las coordenadas de $\varphi(u)$ en la misma base son

$$\mathcal{E}^{-1} \begin{pmatrix} I_d \varphi/\pi & 0 \\ 0 & I_{h_B - d} \varphi \end{pmatrix} U$$

Entonces usando (2.6), se tiene, como en [68], p. 291, el siguiente

Lema 2.6. $\begin{pmatrix} \mathcal{A}/\pi & 0 \\ 0 & I_{h_B - d} \end{pmatrix}$ *actúa como el Fröbenius (el inducido por el de* $A_{cris,A}$*) sobre* $D_{cris,A}(F) := (A_{cris,A} \otimes_B T(F))^{G_K}$. □

Nota 2.13. La matriz $\mathcal{V}$ y la base $(\hat{\underline{l}}, \underline{\hat{m}})$ van a jugar, a posteriori, un papel meramente intermediario. Al hacer $F = F_{\mathcal{A}}$ la base inicial $(\underline{l}, \underline{m})$ de LM^E_K se sustituye por la $(l_{\mathcal{A}}, m_{\mathcal{A}})$, canónica, con $l_{\mathcal{A}}$ logaritmo explícito. La intervención de esta última base, para las fórmulas explícitas, tendrá lugar desde que se pruebe la proposición 3.2. Ésta va a dar la matriz de períodos aproximada (uso de la correspondencia $(\hat{\underline{l}}, \underline{\hat{m}})$ y $(l_{\mathcal{A}}, m_{\mathcal{A}})$), en cuyos términos y los de $(l_{\mathcal{A}}, m_{\mathcal{A}})$ se van a obtener aquellas fórmulas.

Capítulo 3

Fórmulas explícitas para el símbolo de Hilbert

Los resultados de las secciones 1.6 y 2.2 sobre clasificación, rangos y períodos π-ádicos de módulos formales p-divisibles, junto con la adaptación hecha en la sección 2.3 de resultados de [2], dan todo el soporte y preparación cruciales para que podamos ahora mostrar brevemente (y ya sin demostraciones) cómo el método de [68] para las fórmulas explícitas del símbolo de Hilbert tiene validez más general: Puede ser adaptado y extendido directamente, del caso de grupos formales y no ramificación absoluta, al caso de módulos formales (ie, para no ramificación relativa).

3.1. El símbolo de Hilbert de un módulo formal

3.1.1. *En todo el capítulo continúan la situación y la notación del* capítulo 2.

La teoría de Kummer clásica (parte I, (1.2.1)) resulta ser el caso $\mathbb{G}_m$ de la teoría de Kummer para grupos formales introducida en [33], §IV.3. En el caso que estamos tratando aquí, ie, para $F \in \underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$, *fíjese un entero* $M > 0$. Se tiene una aplicación de Kummer y una teoría de Kummer relativa a la isogenia $\left[\pi^M\right]_F$ y a una *extensión algebraica* $L|K$ tal que $L \supset F\left[\pi^M\right]$ $(= F\left[\pi^M\right](\mathfrak{m}_C) \subset \mathfrak{m}_C^d$, ver (1.8)). La *aplicación de Kummer* es el morfismo de conexión de la cohomología de Galois de L para la sucesión exacta $0 \to F\left[\pi^M\right] \to F(\mathfrak{m}_{\bar{K}}) \xrightarrow{\left[\pi^M\right]_F} F(\mathfrak{m}_{\bar{K}}) \to 0$. Es decir, una aplicación

$$\kappa_F \colon F(\mathfrak{m}_L) \to H^1(\ /L, F\left[\pi^M\right]),$$

dada explícitamente por la construcción de la *teoría de Kummer*

$$(\ ,\ ]_F : G_L \times F(\mathfrak{m}_L) \to F\left[\pi^M\right], \tag{3.1}$$

donde $(\sigma, b\,]_F := \beta^\sigma -_F \beta = \kappa_F(b)(\sigma)$, $\beta \in F(\mathfrak{m}_L)$ tal que $\left[\pi^M\right]_F(\beta) = b$.

En [25], Chap. V §1.1 se define $U(F) := \varprojlim F(\mathfrak{m}_C)$, donde el límite inverso es para $[p]_F : F(\mathfrak{m}_C) \to F(\mathfrak{m}_C)$. En nuestro caso de módulos formales se tiene

(como para $T(F)$, ver (2.2.1))

$$U(F) = \varprojlim F(\mathfrak{m}_C),$$

ahora el límite inverso para $[\pi]_F$. De esta forma $U(F)$ pasa a ser un E-espacio vectorial. (Para $F(\mathfrak{m}_L)$ y $F(\mathfrak{m}_C)$ ver (1.2.3)).

Como en [68], (2.4.1), se define $R(F) = R(F)_L$ mediante el siguiente cuadrado cartesiano

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T(F) & \longrightarrow & R(F) & \to & F(\mathfrak{m}_L) & \longrightarrow & 0 \\ & & \| & & \downarrow & \blacksquare & \downarrow & & \\ 0 & \longrightarrow & T(F) & \longrightarrow & U(F) & \to & F(\mathfrak{m}_C) & \longrightarrow & 0 \end{array}$$

Para $\sigma \in G_L$ y $x = (x_s)_{s\geq 0} \in R(F)$ se define $(\sigma, x\,]_{R(F)} := (x_s^\sigma -_F x_s)_{s\geq 0}$, de forma que así se tiene un levantamiento de (3.1)

$$\begin{array}{ccc} G_L \times R(F) & \xrightarrow{(\ ,\ ]_{R(F)}} & T(F) = \varprojlim F[\pi^s] \\ {\scriptstyle 1\times(\ )_0}\downarrow & & \downarrow{\scriptstyle (\ )_M} \\ G_L \times F(\mathfrak{m}_C) & \xrightarrow{(\ ,\ ]_F} & F\big[\pi^M\big] \end{array}$$

En lo que sigue *se va a suponer que* $[L{:}\mathbb{Q}_p] < \infty$ (así $C = \mathbb{C}_p := \widehat{\overline{\mathbb{Q}}}_p$, los *complejos p-ádicos*). Por lo tanto ahora se puede usar teoría de cuerpos de clases local, y sea pues $\psi := (\ ,/L)\colon \dot{L} \to (G_L)_{ab}$ el símbolo de resto nórmico. Se define el *π^M-símbolo de Hilbert para el módulo formal F* como la composición

$$(\ ,\ )\colon \dot{L} \times F(\mathfrak{m}_L) \xrightarrow{\psi\times 1} (G_L)_{ab} \times F(\mathfrak{m}_L) \xrightarrow{(\ ,\ ]_F} F\big[\pi^M\big]\,.$$

Es decir, $(a,b)_F := (\psi(a), b]_F = \beta^{\psi(a)} -_F \beta = \kappa_F(b)(\psi(a))$, donde $\beta \in F(\mathfrak{m}_L)$ es tal que $\big[\pi^M\big]_F(\beta) = b$.

Nota 3.1. Este símbolo (que es relativización del considerado para $E = \mathbb{Q}_p$ en [2]) fue definido por primera vez para grupos formales en [74] en el caso de módulos de Lubin-Tate, y ya había sido propuesto en el caso general en [33].

El isomorfismo $\mathrm{inv}_L\colon H^2(\ /L) \cong \mathbb{Q}/\mathbb{Z}$ de teoría de cuerpos de clases local (cálculo del grupo de Brauer de un cuerpo local), [61], Chap. XIII, Proposition 6) da el siguiente (donde el último isomorfismo se sigue de que $F\big[\pi^M\big]$ es un $\mathbb{Z}/p^M\mathbb{Z}$-módulo)

$$\mathrm{inv}_L\colon H^2(\ /L, \mu_{p^M} \otimes F\big[\pi^M\big]) \cong H^2(\ /L, \mu_{p^M}) \otimes F\big[\pi^M\big] \cong \mu_{p^M} \otimes F\big[\pi^M\big] \cong F\big[\pi^M\big]$$

Proposición 3.1. *En la situación anterior se tiene la siguiente factorización para el símbolo de Hilbert de F*

$$\begin{array}{ccc} \dot{L} \times F(\mathfrak{m}_L) & \xrightarrow{\qquad\qquad (\ ,\ )_F \qquad\qquad} & F\big[\pi^M\big] \\ {\scriptstyle \kappa\times\kappa_F}\downarrow & & \mathrm{inv}_L \uparrow \cong \\ H^1(\ /L, \mu_{p^M}) \times H^1(\ /L, F\big[\pi^M\big]) & \xrightarrow{\cup} & H^2(\ /L, \mu_{p^M} \otimes F\big[\pi^M\big]) \end{array}$$

(κ denota la aplicación de Kummer clásica, *ie,* para $F = \mathbb{G}_m$, y $\cup$ el cup producto).

Demostración. Teniendo en cuenta el argumento previo la demostración es análoga a la del caso $E = \mathbb{Q}_p$ (ver [68], §0.6) y a la del caso $F = \mathbb{G}_m$ (ver [58], Proposition 7.2.13). □

3.1.2. En lo que sigue *volvemos a suponer que* $F = F_{\mathcal{A}}$ (ver la nota 2.12.3), y así podemos utilizar todo lo desarrollado en el capítulo 2. Imitando el método de [68], como consecuencia de la proposición 3.1, sólo resta el cálculo explícito de la aplicación de Kummer κ_F. En orden a clarificar todos los ingredientes involucrados en esa tarea, así como en la obtención de la fórmula final, vamos a reproducir someramente en esta subsección, y luego en la (3.2.1), lo de [68], (2.4.1) y (2.4.2), indicando cómo eso se puede adaptar a nuestro caso.

Se tiene un diagrama (conmutativo por construcción)

$$\begin{array}{ccccc} G_L\times F(\mathfrak{m}_{\mathcal{R}})_L & \xrightarrow{1\times\delta} & G_L\times F(W_A(\mathfrak{m}_{\mathcal{R}}))_L^{(\mathcal{A}-\pi I)l_{\mathcal{A}}=0} & \to & F(W_A^1(\mathfrak{m}_{\mathcal{R}}))^{(\mathcal{A}-\pi I)l_{\mathcal{A}}=0} \\ {\scriptstyle 1\times\iota}\downarrow & & & & \cong\uparrow{\scriptstyle j} \\ G_L\times R(F) & & \xrightarrow{\quad (\ ,\ )_{R(F)}\quad} & & T(F) \end{array}$$

La aplicación δ es la del lema 2.5, y el isomorfismo j es el de la proposición 2.7(b) (ambos ahora para $l_{\mathcal{A}}$). La paridad superior derecha está dada, simplemente, por $(\sigma-1)u$. Se denota $F(\mathfrak{m}_{\mathcal{R}})_L := F(\mathfrak{m}_{\mathcal{R}}) \cap \theta\,[\ ]^{-1}(L) = F(\mathfrak{m}_{\mathcal{R}}) \cap \theta\,[\ ]^{-1} F(\mathfrak{m}_L)$ (análogamente para $F(W_A(\mathfrak{m}_{\mathcal{R}}))_L$). Finalmente $\iota(\zeta) := (\theta\delta(\pi^{-s}1_F(\zeta)))_{s\geq 0} = (\theta\,[\pi^{-s}1_F(\zeta)])_{s\geq 0} \in R(F)$ (ver el lema 2.5(b)).

Trataremos ahora de expresar $(\sigma, (\pi^{-s}1_F(\zeta))\,]_{R(F)}$ (y así κ_F, ver (3.1.1)) en términos de períodos π-ádicos, ie, de la matriz $\boldsymbol{\mathcal{V}}$, de $l_{\mathcal{A}}$ y de $m_{\mathcal{A}}$.

Sea $X = [\varepsilon] - 1 \in W^1(\mathfrak{m}_{\mathcal{R}})$ (ver la nota 2.10), y sea $Y := [\rho] \in W(\mathfrak{m}_{\mathcal{R}})$, siendo $\rho := (\Pi_{p^n})$ un sistema coherente de raíces p^n-ésimas de un uniformizante Π de L (cf. (2.1.2)).

Nota 3.2. X e Y son topológicamente nilpotentes (ver la nota 2.9(b)) y algebraicamente independientes sobre A (ver [68], §1.2), y así $A[[X,Y]]$ *es un anillo de series de potencias formales, subanillo de* $W_A(\mathcal{R})$ (nota 2.9(a)). El Fröbenius de $W_A(\mathcal{R})$ induce en $A[[X,Y]]$ el siguiente (coherente con el de (1.6.2))

$$\varphi(X) = (1+X)^q - 1 \quad \text{y} \quad \varphi(Y) = Y^q$$

No es restrictivo suponer que L *es totalmente ramificada sobre* K. De esta forma $\mathfrak{m}_L = \Pi A[\Pi]$. Se tiene así que la restricción

$$\theta\colon F(YA[[Y]]) \twoheadrightarrow F(\mathfrak{m}_L) \tag{3.2}$$

es tal que $\theta(Y) = \Pi$, y es sobreyectiva. Sean pues $\zeta \in F(\mathfrak{m}_{\mathcal{R}})_L$ y $\beta \in F(YA[[Y]])$ tales que $\beta(\Pi)$(uso de la nota 3.2) $= \theta(\beta) = \theta\,[\zeta] = \iota(\zeta)_0 \in F(\mathfrak{m}_L)$. La conmutatividad del diagrama anterior significa ahora que, para cada $\sigma \in G_{Lp\Pi^\infty}$,

$$j(\sigma, \iota(\zeta)\,]_{R(F)} = (\sigma-1)(\delta(\zeta) -_F \beta) \tag{3.3}$$

Usando el lema 2.3 (ahora para $l_{\mathcal{A}}$) se tiene que

$$\Lambda := \boldsymbol{\mathcal{V}}^{-1} \begin{pmatrix} l_{\mathcal{A}}(\delta(\zeta) -_F \beta) \\ m_{\mathcal{A}}(\delta(\zeta) -_F \beta) \end{pmatrix} \in A_{cris,A}^{h_B}$$

puesto que $\theta(\delta(\zeta) -_F \beta) = \theta([\varepsilon] -_F \beta) = 0$ (θ conserva $+_F$). Así

$$\lambda := o\Lambda = o\boldsymbol{\mathcal{V}}^{-1} \begin{pmatrix} l_{\mathcal{A}}(\delta(\zeta) -_F \beta) \\ m_{\mathcal{A}}(\delta(\zeta) -_F \beta) \end{pmatrix} \in D_{cris,A}(F).$$

De esta forma (como en [68], (2.4.1)) de (3.3) se obtiene la

Proposición 3.2. *Con la notación anterior se verifica, para cada $\sigma \in G_{Lp\Pi^\infty}$,*

$$(\sigma, \iota(\zeta)]_{\mathcal{R}(F)} = (\sigma - 1)\lambda. \qquad \square$$

3.2. Fórmulas explícitas

3.2.1. Continuamos la línea indicada al comienzo de (3.1.2). Para calcular κ_F es suficiente calcular $\kappa_F \iota(\zeta)_0 \in H^1(\ /L, F\big[\pi^M\big])$ para cada $\zeta \in F(\mathfrak{m}_{\mathcal{R}})_L$. Esto se realiza del lado del complejo de Herr y Tavares Ribeiro $C_{\varphi\gamma\tau}(\tilde{D}_\Pi F\big[\pi^M\big])$ (cf. (2.1.2)). Así el teorema 2.2(a) da

$$H^1(\ /L, F\big[\pi^M\big]) \cong H^1 C_{\varphi\gamma\tau}(\tilde{D}_\Pi F\big[\pi^M\big]).$$

Ahora el teorema 2.2(b) dice que si $(x, y, z) \in Z^1 C_{\varphi\gamma\tau}(\tilde{D}_\Pi F\big[\pi^M\big])$ corresponde a $\kappa_F \iota(\zeta)_0$, entonces este último está representado en $H^1(\ /L, F\big[\pi^M\big])$ por un cociclo cuya restricción es

$$\sigma \in G_{Lp\Pi^\infty} \mapsto (\sigma - 1)(-b) \in F\big[\pi^M\big]\,,$$

siendo $b \in F\big[\pi^M\big] \otimes_B W_A(\mathrm{Frac}(\mathcal{R}))$ tal que $(\varphi - 1)b = x$. Por lo tanto la proposición 3.2 da que, para cada $\sigma \in G_{Lp\Pi^\infty}$, se tiene

$$(\sigma - 1)\lambda = (\sigma, \iota(\zeta)\,]_{R(F),M} = \kappa_F \iota(\zeta)_0(\sigma) = (\sigma - 1)(-b).$$

Entonces $x = (\varphi - 1)b = (\varphi - 1)(-\lambda) = o\boldsymbol{\mathcal{V}}^{-1} \begin{pmatrix} (\frac{\mathcal{A}}{\pi} - I) l_{\mathcal{A}}(\beta) \\ 0 \end{pmatrix} \in A_{cris,A} \otimes_B T(F)$, la última igualdad por el lema 2.6.

Pero se necesita construir x perteneciendo a $\tilde{D}_\Pi F\big[\pi^M\big]$ (ver la proposición 3.4, más adelante). Esto se hace construyendo una aproximación del anterior $x = (\varphi - 1)b$ tal que $(\sigma - 1)b \equiv (\sigma - 1)(-\lambda)$ mód π^M para cada $\sigma \in G_{Lp\Pi^\infty}$, lo cual, a su vez, se realiza aproximando la matriz $\boldsymbol{\mathcal{V}}$.

Obsérvese una muestra de $\boldsymbol{\mathcal{V}}$, eg, $\langle \hat{\underline{l}}, o^1 \rangle = \lim\limits_{s \to \infty} \pi^s l_{\mathcal{A}}(\hat{o}^1_s)$, $\hat{o}^1_s \in F(W_A(\mathfrak{m}_{\mathcal{R}}))$, $\theta(\hat{o}^1_s) = o^1_s$. Considérese la $B/\pi^M B$-base $(o^1_M, \ldots, o^{h_B}_M)$ de $F\big[\pi^M\big]$ (ver la proposición 2.1). Puesto que $F(\mathfrak{m}_L) \supset F\big[\pi^M\big]$ la aplicación (3.2) da algún $\hat{o}^i_M \in F(YA[[Y]])$ tal que $\theta(\hat{o}^i_M) = \hat{o}^i_M(\Pi) = o^i_M \in F\big[\pi^M\big]$. Así la siguiente matriz es una aproximación de $\boldsymbol{\mathcal{V}}$ módulo π^M (que va a resultar suficiente)

$$\boldsymbol{\mathcal{V}}_Y := \begin{pmatrix} \pi^M l_{\mathcal{A}}(\hat{o}^1_M) & \ldots & \pi^M l_{\mathcal{A}}(\hat{o}^{h_B}_M) \\ \pi^M m_{\mathcal{A}}(\hat{o}^1_M) & \ldots & \pi^M m_{\mathcal{A}}(\hat{o}^{h_B}_M) \end{pmatrix}.$$

Ésta se denomina la *matriz de períodos π-ádicos aproximada* (para F, que va a estar involucrada en las fórmulas explícitas finales, ver la nota 2.13). Por construcción sus coeficientes están en el subanillo cerrado $A[[Y]]\,[[Y^{ep}/p]]$ de la completación p-ádica de la capa de potencias divididas de $A[[Y]]$ respecto a $\ker(\theta\colon A[[Y]] \to \mathcal{O}_L)$ (contenida en $A_{cris,A}$). En efecto, el argumento de [2],

(3.4.1) y (3.4.2) vale en nuestro caso al estar suponiendo que $L|K$ es totalmente ramificada (ver (3.1.2)), y así $\ker\theta = g(Y)A[[Y]]$, denotando $g(t)$ el polinomio de Eisenstein de $L|K$.

Ahora la proposición 2.9 permite refinar aquel subanillo y mostrar cómo $\boldsymbol{\nu}_Y$ aproxima a $\boldsymbol{\nu}$, tal como se hace en el caso p-ádico en [2], (3.4.2).

El citado subanillo de coeficientes de $\boldsymbol{\nu}_Y$ es un caso de los anillos $G_{[b,a]}$, estudiados en el caso p-ádico en [68], §2.3. En nuestro caso π-ádico definimos, simplemente, para $a > b \geq 0$ en $\mathbb{R}$,

$$G_{[b,a],A} := A \otimes_{W(k)} G_{[b,a]} = W_A(\mathcal{R})\big[\big[Y^{ae}/p, p/Y^{be}\big]\big] \subset W_A(\mathrm{Frac}(\mathcal{R}))[1/p]$$
$$G_{Y,[b,a],A} := A \otimes_{W(k)} G_{Y,[b,a]} = A[[Y]]\,\big[\big[Y^{ae}/p, p/Y^{be}\big]\big]$$

Con esta notación $\boldsymbol{\nu}_Y$ tiene coeficientes en $G_{Y,[0,p],A} \subset A_{cris,A}$. Puesto que algunas propiedades de estos anillos son necesarias para la vía de [68] a las fórmulas explícitas, vamos a mostrar someramente cómo esas propiedades, para nuestro caso relativo, puede ser fácilmente reducidas a las del caso $E = \mathbb{Q}_p$ de [68], §2.3.

Así [68], Lemma 2.6, se traslada directamente a nuestro caso aplicando el funtor $A \otimes_{W(k)} -$, y teniendo en cuenta que "el producto tensorial por un módulo plano conserva intersecciones".

También [68], Lemma 2.8, se traslada fácilmente. Eg, "$G_{[b,a],A}$ es local" se reduce al caso absoluto como un caso particular de la siguiente

Proposición 3.3. *Sea k un anillo y A y B k-álgebras verificando*

(a) *A y B son locales*

(b) *$k \to A$ es entera*

(c) $\dim A = 0$, *ó* $\dim A = 1$, $\mathrm{char}\, A = 0$ *y $A \otimes_k B/\mathfrak{m}$ es de característica p para todo maximal $\mathfrak{m}$ (equivalentemente $B/\mathfrak{m}_B$ es de característica p).*

(d) *$A/\mathfrak{m}_A \otimes_k B/\mathfrak{m}_B$ es local.*

Entonces $A \otimes_k B$ es local. Si además, $A/\mathfrak{m}_A \otimes_k B/\mathfrak{m}_B$ es cuerpo, entonces

$$\mathfrak{m}_{A\otimes_k B} = \mathfrak{m}_A \otimes_k B + A \otimes_k \mathfrak{m}_B.$$

Demostración. Sea $\mathfrak{m}$ un maximal de $A \otimes_k B$. Si $\mathfrak{m} \cap A \neq \mathfrak{m}_A$, entonces $\mathfrak{m} \cap A = 0$, y así $A \rightarrowtail A \otimes_k B/\mathfrak{m}$ es inyectiva, en contradicción con la hipótesis sobre la característica. Por lo tanto $\mathfrak{m}_A \otimes_A B \subset J(A \otimes_k B)$.

Usando ahora el argumento de [65], Theorem (b) $\Rightarrow$ (a), se tiene también que $A \otimes_k \mathfrak{m}_B \subset J(A \otimes_k B)$ al ser $k \to A$ entera. Así, puesto que, por (d), $A \otimes_k B/(\mathfrak{m}_A \otimes_k B + A \otimes_k \mathfrak{m}_B)$ es local, se sigue que $A \otimes_k B$ es local. □

Finalmente, para trasladar [68], Lemma 2.10, la inclusión $\mathrm{Frac}(G_{Y,[b,a],A}) \subset G_{Y,[p-1,p-1),A}\,[1/p]$[21] se reduce al caso p-ádico observando que el segundo anillo contiene a $\mathrm{Frac}(A) = K = A\,[1/p]$. (De esto último se sigue que $\boldsymbol{\nu}_Y^{-1}$ tiene sus coeficientes en $G_{Y,[p-1,p-1),A}\,[1/p]$).

El cálculo en el caso p-ádico de una fórmula explícita para κ_F, y también para el símbolo de Hilbert, se apoya en un lema técnico ([68], Lemma 2.11) sobre los

[21] Los $G_{[b,a),A}$ y $G_{Y,[b,a),A}$ semiabiertos se definen paralelamente a los p-ádicos correspondientes ([68], §2.3).

coeficientes de $\boldsymbol{\mathcal{V}}_Y^{-1}$ (éstos son series de Laurent), así como de su parte principal, $\boldsymbol{\mathcal{V}}_Y^{(-1)}$, respecto a los anillos $G_{[b,a]}$. La versión π-ádica de este lema se reduce ahora directamente a la del caso absoluto teniendo en cuenta la proposición 2.9 y las observaciones que se acaban de hacer sobre los anillos $G_{[b,a],A}$ y $G_{Y,[b,a],A}$.

3.2.2. *Fórmulas explícitas.* Todo está ahora preparado para que los elaborados cálculos y argumentos de [68], (2.4.3), (2.4.4) y §2.5, funcionen en nuestro caso de módulos formales sin más y de forma paralela, y así que su traslación (que ya no vamos a reproducir aquí) sea directa. De este modo, [68], Proposition 2.14, vale sin más en el caso π-ádico

Proposición 3.4 (Cálculo explícito de κ_F)**.** *Denótese*

$$x := o\boldsymbol{\mathcal{V}}_Y^{(-1)} \begin{pmatrix} (\mathcal{A}/\pi - I) l_{\mathcal{A}}(\beta) \\ 0 \end{pmatrix} \in \tilde{D}_\Pi T(F)$$

Entonces existe $z \in \tilde{D}_\Pi T(F) \cap (T(F) \otimes_B W_A(\mathfrak{m}_{\mathcal{R}}))$*, único módulo* π^M*, tal que el cociclo* $(x, 0, z)$ *corresponde a* $\kappa_F \beta(\Pi) \in H^1(\ /L, F\big[\pi^M\big])$*. Además*

$$z \equiv XY\boldsymbol{\mathcal{V}}_Y^{(-1)} \frac{d}{dY} \begin{pmatrix} l_{\mathcal{A}}(\beta) \\ m_{\mathcal{A}}(\beta) \end{pmatrix} \text{ mód } XW_A(\mathfrak{m}_{\mathcal{R}}). \qquad \square$$

Teniendo en cuenta, además, las proposiciones 3.1 y 3.2, así como los cálculos explícitos de la aplicación de Kummer clásica κ (uso de la nota 3.2) y del cup producto $\cup$ efectuados en [68], §§1.6 y 1.7, la demostración de [68], Theorem 2.16 (fórmula explícita del símbolo de Hilbert en el caso absolutamente no ramificado) ya corre paralela sobre nuestro caso general de módulos formales

Teorema 3.1 (Fórmula explícita para el símbolo de Hilbert de un módulo formal)**.** *Sea* $\alpha \in \mathcal{U}(W(k)[[Y]]\,[1/Y])$ *y* $\beta \in F(YA[[Y]])$*. Las coordenadas del símbolo de Hilbert* $(\alpha(\Pi), \beta(\Pi))_F \in F\big[\pi^M\big]$ *en la* $B/\pi^M B$*-base* $(o_M^1, \ldots, o_M^{h_B})$ *de* $F\big[\pi^M\big]$ *son*

$$(\mathrm{S}\cdot\mathrm{res}_Y)\boldsymbol{\mathcal{V}}_Y^{-1}\left[\begin{pmatrix} (I - \frac{\mathcal{A}}{\pi}) l_{\mathcal{A}}(\beta) \\ 0 \end{pmatrix} d_{\log}\alpha(Y) - \mathscr{L}(\alpha) \frac{d}{dY} \begin{pmatrix} \frac{\mathcal{A}}{\pi} l_{\mathcal{A}}(\beta) \\ m_{\mathcal{A}}(\beta) \end{pmatrix}\right] \in B^{h_B} \ (\text{mód } \pi^M)$$

donde S *denota la traza de* $A|B$*,* res_Y *el residuo de una serie de Laurent y* $d_{\log}$ *la derivada logarítmica, y* $\mathscr{L}(\alpha) := \left(1 - \frac{\varphi}{p}\right) \log\, \alpha(Y) = \frac{1}{p} \log \frac{\alpha(Y)^p}{\alpha^\varphi(Y^p)} \in W(k)[[Y]]$ (aquí φ denota también el Fröbenius absoluto de $W(k)[[Y]]$). $\square$

Nota 3.3. 1. La fórmula explícita del teorema 3.1 puede ser expresada (obviamente) también como sigue

$$(S\cdot\mathrm{res}_Y)\boldsymbol{\mathcal{V}}_Y^{-1}\left[\left(I - \begin{pmatrix} \frac{\mathcal{A}}{\pi} \\ I \end{pmatrix}\right)\begin{pmatrix} l_{\mathcal{A}}(\beta) \\ m_{\mathcal{A}}(\beta) \end{pmatrix} d_{\log}\alpha(Y) - \frac{1}{p}\log\frac{\alpha(Y)^p}{\alpha^\varphi(Y^p)} \begin{pmatrix} \frac{\mathcal{A}}{\pi} \\ I \end{pmatrix} \frac{d}{dY} \begin{pmatrix} l_{\mathcal{A}}(\beta) \\ m_{\mathcal{A}}(\beta) \end{pmatrix}\right]$$

2. Se han unificado el contexto y las fórmulas explícitas de Abrashkin [2] y Tavares Ribeiro [68] con las de Vostokov y Demchenko [70] ($p > 2$), que ahora todas resultan particularizando la fórmula del teorema 3.1. En particular, para grupos de Lubin-Tate [69] y de Lubin-Tate relativos [70].

Lista de símbolos

$\mathrm{Spf}(k)$	espectro formal del anillo k	65
$r(k)$		66
$J(k)$	radical de Jacobson del anillo k	66
$\bar{k}$	cuerpo residual de un anillo local o un cuerpo local	66
$\underline{\mathrm{PRO}}_k$	categoría de k-álgebras profiní	66
$\underline{\mathrm{FI}}_k$	categoría de k-álgebras finí	66
long_k	longitud de un k-módulo	66
$\mathcal{C}^{\mathrm{op}}$	categoría dual de una categoría $\mathcal{C}$	66
$\rightarrowtail$	monomorfismo/funtor fiel y pleno	66
Top$k$-$\underline{\text{álg}}$	categoría de k-álgebras topológicas	66
$\widehat{\underline{\mathrm{Sch}}_k}$, $\widehat{\underline{\mathrm{Sch}}_Y}$	categoría de k-esquemas formales sobre k, Y	66
$\simeq$	equivalencia de categorías	67
f^*	morfismo en $\underline{\mathrm{PRO}}_k$ tal que $\mathrm{Spf}(f^*) = f$	67
k-$\underline{\text{álg}}$	categoría de k-álgebras	67
$\underline{\mathrm{Sch}}_k$	categoría de k-esquemas afines	67
k-$\underline{\text{alg.loc.libre.finita}}$	categoría de k-álgebras localmente libres finitas	67
$\underline{\mathrm{Sch}}_k\underline{\text{finito}}$	categoría de k-esquemas finitos	67
$\widehat{\underline{\mathrm{Sch}}_k}\underline{\text{finí}}$	objetos de $\widehat{\underline{\mathrm{Sch}}_k}$ de álgebra afín finí	67
k-$\underline{\text{alg.finita}}$	categoría de k-álgebras finitas	67
$\underline{\mathrm{Sch}}_k\underline{\text{alg.finita}}$	k-esquemas espectros de k-álgebras finitas	67
$\lvert\cdot\rvert$	orden de un k-esquema finito	67
$\hat{X}$	completación formal del esquema X	67
$X \times_k Y$	producto en la categoría $\widehat{\underline{\mathrm{Sch}}_k}$	67
$M \hat{\otimes}_k N$	producto tensorial completo	67
$X_{k'}$	extensión de escalares del k-esquema X a k'	67
$\widehat{\underline{\mathrm{Sch}}_k}\underline{\text{EGA}}$	categoría de los k-esquemas formales usuales de [38]	68
$\widehat{\underline{\mathrm{Sch}}_k}\underline{\text{EGAafín}}$	categoría de los k-esquemas formales afines (de [38])	68
k-$\underline{\text{álg}}I$-$\underline{\text{ádica}}$	categoría de las k-álgebras I-ádicas	68
$X\vert_{X'}$	completación del esquema X a lo largo de X'	69
$\mathbb{G}_a$, $\widehat{\mathbb{G}_a}$	grupo (esquema o formal) aditivo	69
$k[[\mathbf{X}]]$	anillo de series de potencias formales en varias variables	69
$\mathbb{G}_m$, $\widehat{\mathbb{G}_m}$	grupo (esquema o formal) multiplicativo	69

R-$\underline{\text{Mod}}$	categoría de módulos (izquierda) sobre un anillo R	69
$\text{Gr}\widehat{\underline{\text{Sch}}}_k$	categoría de los k-grupos formales	70
$\text{Hom}_k(G, G')$	morfismos en $\text{Gr}\widehat{\underline{\text{Sch}}}_k$	70
k-$\widehat{\underline{\text{Hopf}}}$	categoría de las k-álgebras de Hopf formales	70
$\overline{\Delta}$	comultiplicación de una k-álgebra de Hopf formal	70
ε	aumentación de una k-álgebra de Hopf formal	70
A^+	ideal aumentación de una k-álgebra de Hopf formal	70
$\text{Gr}\underline{\text{Sch}}_k\underline{\text{finito}}$	categoría de los k-esquemas finitos en grupos	70
k-$\underline{\text{álg.compl.lineal}}\text{T}_2$	categoría de las k-álgebras completas, lineales y Hausdorff	70
$x +_G y, f +_G g$	operación para el grupo formal G	70
$[n]_G = n1_G$		70
G^D	dual de Cartier de G	70
$G[n]$	núcleo de $[n]_G$	70
$\text{Gr}\widehat{\underline{\text{Sch}}}_{\bar{k}}\underline{\text{ét}}$	categoría de los $\bar{k}$-grupos formales étale	72
$\text{Gr}\widehat{\underline{\text{Sch}}}_k\underline{\text{ét.top.plano}}$	k-grupos formales topológicamente planos étale	72
G^0	componente conexa de G	72
G^{et}	cociente étale de G	72
$\overline{\bar{k}}$	clausura algebraica del cuerpo residual $\bar{k}$	72
G_K	grupo de Galois absoluto de un cuerpo K	72
$\text{Gr}\underline{\text{Sch}}_k\underline{\text{ét.finito}}$	categoría de los k-esquemas en grupos étale finitos	72
Γ-$\underline{\text{Mod.discr.(finito)}}$	categoría de los Γ-módulos discretos (finitos) sobre un grupo profinito Γ	72
deg(f)	grado de un morfismo de k-grupos formales f	72
$\twoheadrightarrow$	morfismo sobreyectivo/funtor denso	73
$t^*_G(B)$	espacio cotangente de G con valores en $B \in \underline{\text{PRO}}_k$	73
$t_G(B)$	espacio tangente de G con valores en $B \in \underline{\text{PRO}}_k$	73
Cl	clausura o adherencia topológica	73
$\text{Top}\underline{B}$-$\underline{\text{Mod}}$	categoría de los B-módulos topológicos	73
$\widehat{\Omega}_{A\|k}$, $(\widehat{\Omega}_{X\|k})$	módulo (haz) de diferenciales continuas de $A\|k$ (de un esquema formal $X\|k$)	73
$\Omega_k(G)$	módulo de diferenciales invariantes de G	73
∂		74
$\dim G$	dimensión del grupo formal G	74
$A^{(p)}$		74
F_G		74
V_G		74
V_A		74
$\underline{\text{FLG}}_k$	categoría de los k-grupos de Lie formales	75
$\underline{\text{FGL}}_k$	categoría de las leyes de grupo formal sobre k	75
$k[[\mathbf{X}]]_0$	series de potencias formales sin término constante	75
$\mathcal{U}(R)$	unidades de un anillo R	75
$\underline{\text{FI}}_k\underline{\text{local}}$	categoría de las k-álgebras finí locales	75

μ_n	grupo o esquema en grupos de raíces n-ésimas de 1	75
$\mathrm{ht}(F)$	altura del grupo formal F	76
$G[p^\infty]$	p-torsión de un grupo esquema (o formal) G sobre k	77
$\underline{p\text{-div}}_k$	categoría de los grupos p-divisibles sobre k	77
$\overline{G(p)}$		78
$\underline{\mathrm{FLG}}_k\underline{\mathrm{ht}<\infty}$	k-grupos de Lie formales de altura finita	79
$\underline{p\text{-div}}_k\underline{\text{conexo}}$	categoría de los grupos p-divisibles sobre k conexos	79
$p\text{-Gr}\widehat{\underline{\mathrm{Sch}}}_k\underline{\text{liso}}$	categoría de los p-grupos formales sobre k lisos	79
$\bar{K}$	clausura algebraica de un cuerpo K	81
$C := \hat{\bar{K}}$	completación de la clausura algebraica de K	81
π	uniformizante de un cuerpo completo discreto	81
$\mathcal{O}_L$	anillo de enteros de un cuerpo valorado L	81
$\mathfrak{m}_L$	ideal maximal de $\mathcal{O}_L$	81
$G(J) := G(R)$	grupo de puntos de un álgebra J-ádica	81
$\hat{L}$	completación de un cuerpo valorado L	81
$G(\mathfrak{m}_L) := G(\mathcal{O}_L)$		81
$G(\mathcal{O}_{\hat{L}})$	grupo de puntos de G con valores en $\hat{L}$	82
$G[p^n]{:=}G[p^n](\mathfrak{m}_C)$		83
$\Phi(G)$	comódulo de Tate del grupo p-divisible G sobre k	83
$T(G)$	módulo de Tate del grupo p-divisible sobre k G	83
$\mathbb{Z}_p(1)$	módulo de Tate del grupo multiplicativo $\mathbb{G}_m$	83
$< >, < >_A$	subgrupo, A-submódulo generado	83
$T_\ell(X)$	ℓ-módulo de Tate del k-esquema abeliano X	83
$W(-)$	anillo de vectores de Witt de un anillo	84
$[-]$	representante de Teichmüller	84
φ	levantamiento/extensión del Fröbenius de $\bar{k}$	84
V	Verschiebung o decalage	84
$D_{\bar{k}}$	anillo de Dieudonné	84
$\underline{F}$, $\underline{V}$	variables del anillo de Dieudonné $D_{\bar{k}}$	84
$CW(R)$	covectores de Witt de un anillo R	85
$\widehat{CW}_{\bar{k}}$	(funtor) grupo formal de los covectores de Witt	85
$\widehat{B^0_{\bar{k}}}$	completación profiní de $\mathbb{Z}^0[[\mathbf{X}]]\,\hat{\otimes}k$	85
$\underline{M}(G)$	módulo de Dieudonné del $\bar{k}$-grupo formal G	86
$p\text{-Gr}\widehat{\underline{\mathrm{Sch}}}_{\bar{k}}$	categoría de los p-grupos formales sobre $\bar{k}$	87
$p\text{-Gr}\underline{\mathrm{Sch}}_{\bar{k}}\underline{\text{finito}}$	categoría de los esquemas p-grupo sobre $\bar{k}$ finitos	87
$\mathrm{Frac}(-)$	cuerpo de fracciones de un dominio	88
K_0	cuerpo de fracciones de $W(\bar{k})$ (para K)	88
$\hat{A}^{an}_{K_0}$	álgebra de "funciones analíticas" de A	88
d	diferencial exterior del complejo de de Rham (formal)	88
$P(A)$		88
$\hat{w}_A$, w_A		88
M_k		88
$P'(A)$	k-submódulo de $P(A)$ generado por los $p^{-n}(\pi\alpha)^{p^n}$	89
$H^n_{dR}(X)$	cohomología de de Rham de un esquema (formal)	89

$\mathcal{R}$	anillo de Fontaine	101
$W_K(\mathcal{R})$	anillo de vectores de Witt de $\mathcal{R}$ con coeficientes en K	101
θ		101
$W_K^1(\mathcal{R})$	núcleo de θ	101
B_{dR}^+		101
A_{cris}		102
B_{dR}	cuerpo de períodos p-ádicos	102
B_{cris}^+		102
B_{cris}	anillo cristalino	102
$A_{cris,A}$		102
$B_{cris,A}^+$		102
$B_{cris,A}$		102
$\varphi\underline{\mathrm{MF}}_K^\infty$	φ-módulos filtrados de dimensión $\leq \infty$	102
$D_{cris}^*(V)$		102
$\underline{\mathrm{Rep}}_{cris}(G_K)$	categoría de representaciones p-ádicas cristalinas	103
$\varphi\underline{\mathrm{MF}}_K\underline{\mathrm{Ad}}$	categoría de los φ-módulos filtrados admisibles	103
$\varphi\Gamma$-$\underline{\mathrm{Mod}}_S\underline{\text{ét}}$	categoría de los (φ,Γ)-módulos étale sobre S	103
$\rho = (\pi_{p^n})$	sistema coherente de raíces p^n-ésimas de π	103
$K_{p^\infty} := K(\varepsilon)$		103
$K_{p\pi^\infty} := K(\varepsilon,\rho)$		103
G_∞	grupo de Galois $K_{p\pi^\infty}\vert K$	104
τ, γ	generadores topológicos de G_∞	104
$\tilde{D}_\pi(V)$		104
$\tilde{V}_\pi(V)$		104
$H^n(\Gamma, A)$	cohomología de Galois continua	104
χ	carácter ciclotómico	104
$C_{\varphi\gamma\tau}(M)$	complejo de Herr y Tavares Ribeiro de M	104
$\underline{\mathrm{Rep}}_E(G_K)^\infty$	categoría de E-representaciones de G_K	105
$\underline{\mathrm{Rep}}_E(G_K)$	E-representaciones de G_K de dimensión finita	105
$\varphi\underline{\mathrm{MF}}_{KE}^\infty$	categoría de φ-módulos filtrados relativos a E	105
$\varphi\underline{\mathrm{MF}}_{KE}$ ($\varphi\underline{\mathrm{MF}}_{KE}^2$)	φ-módulos filtrados sobre K relativos a E de dimensión finita (filtración de longitud 2)	105
$\underline{\mathrm{Rep}}_B(G_K)^\infty$	categoría de B-representaciones de G_K	105
$\underline{\mathrm{Rep}}_B(G_K)$	B-representaciones de G_K de tipo finito	105
$D_{cris,A}^*(V)$		105
η_F	morfismo de comparación para el grupo formal F	106
LM_K^E		107
$F\big[\pi^M\big] := F\big[\pi^M\big](\mathfrak{m}_C)$		107
$\varphi\underline{\mathrm{MF}}_{AB}^{ff2}$		109
$\varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus}$	objetos (M^1, M, φ) de $\varphi\underline{\mathrm{MF}}_{AB}^{ff2}$ donde M^1 es sumando directo	109
D_k^A-$\underline{\mathrm{Mod}}A$-$\underline{\mathrm{fil}}^{ff2}$	categoría de los D_k^A-módulos A-filtrados de longitud 2 y A-libres de tipo finito	110
$\underline{\mathrm{SH}}_A^{Edh}$	subcategoría de $\underline{\mathrm{SH}}_A^E$ de objetos de A-rangos d, h	110
$\varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus dh}$	objetos de $\varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus}$ de A-rangos d, h	110

$\varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus dh}\underline{\mathrm{topNil}}$	objetos de $\varphi\underline{\mathrm{MF}}_{AB}^{ff2\oplus dh}$ sobre los que $\underline{F}$ es topológicamente nilpotente	110
$\underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A/\mathrm{isg}$	objetos de $\underline{\mathrm{FML}}_{BA}\underline{p\text{-div}}_A$ "salvo isogenia"	110
$\varphi\underline{\mathrm{MF}}_{KE}^{2}\underline{\mathrm{wAd.topNil}}$	objetos débilmente admisibles de $\varphi\underline{\mathrm{MF}}_{KE}^{2}$ sobre los que $\underline{F}$ es topológicamente nilpotente	111
$D^*_{cris,A}(F)$		112
I, H		112
$H^1_{dR}(F)^{(0)}_{coz}$		114
$H^1_{dR}(F)_{coz}/H^1_{dR}(F)^E_{coz}$	1-cohomología de de Rham del grupo formal F (de Colmez)/relativa a E	114
$\int_o w$	integración p-ádica sobre grupos formales	114
$W_A(\mathcal{R})$	anillo de vectores de Witt con coeficientes en A	115
$(\underline{l},\underline{m})$	base filtrada de $D^*_{cris,A}(F)$	116
$j(o)$		117
$\mathcal{E}$		117
$\mathcal{A}$		117
δ		118
$X := [\varepsilon] - 1$		118
$F_{\mathcal{A}}$	módulo formal de sustitución de F	118
$(l_{\mathcal{A}},m_{\mathcal{A}})$	base filtrada de $LM^E_K(F_{\mathcal{A}})$	118
$h_{B\mathcal{A}}$	altura relativa del módulo formal $F_{\mathcal{A}}$	119
$(\underline{\hat{l}},\underline{\hat{m}})$	base filtrada de $D^*_{cris,A}(F_{\mathcal{A}})$	119
$\psi_1 := l_{\mathcal{A}}^{-1}\lambda_F$		119
$<\ ,\ >$	paridad de períodos π-ádicos reticular	121
$\boldsymbol{\mathcal{V}}$	matriz de períodos π-ádicos	122
$D_{cris,A}(F)$		122
κ_F	aplicación de Kummer del módulo formal F	123
$(\ ,\ ]_F$	paridad de la teoría de Kummer relativa a F	123
$(\ ,\ ]_{R(F)}$		124
$(\ ,\ )_F$	π^M-símbolo de Hilbert para el módulo formal F	124
inv_L		124
ι		125
$Y := [\rho]$		125
$\boldsymbol{\mathcal{V}}_Y$	matriz de períodos π-ádicos aproximada	126
$G_{[b,a],A}$		127
$G_{Y,[b,a],A}$		127

Bibliografía

[1] Abrashkin, V. (1990). *Ramification in étale cohomology*, Invent. Math., **101** (3), 631-640.

[2] Abrashkin, V. (1997). *Explicit formulas for the Hilbert symbol of a formal group over Witt vectors*, Izv. Ross. Akad. Nauk Ser. Mat., **61**(3), 3-56.

[3] Abrashkin, V. (2015). *Ramification estimate for Fontaine-Laffaille Galois modules*, J. Algebra, **427**, 319-328.

[4] Alonso-Tarrío, L., Jeremías-López, A. and Pérez-Rodríguez, M. (2007). *Infinitesimal lifting and Jacobi Criterion for smoothness on formal schemes*, Comm. Algebra 35, no. 4, 1341-1367.

[5] Barsotti, I. (1962). *Analytical methods for abelian varieties in positive characteristic*, Colloq. Théorie des Groupes Algébriques (Bruxelles), 77-85.

[6] Benois, D. (1997). *Périodes p-adiques et lois de réciprocité explicites*, J. Reine Angew. Math., **493**, 115-151.

[7] Benois, D. (2000). *On Iwasawa theory of crystalline representations*, Duke Math. J. 104, no. 2, 211-267.

[8] Berthelot, P. *Cohomologie cristalline des schémas de caractéristique* $p > 0$, Lecture Notes in Mathematics, vol. 407, Springer, 1974.

[9] Berthelot, P. and Ogus, A. *Notes on crystalline cohomology*, Princeton University Press, Princeton, N.J., 1978.

[10] Bosch, S., Lütkebohmert, W. and Raynaud, M. *Néron models*, Ergebnise der Mathematik und ihrer Grenzgebiete (3), 21, Springer, 1990.

[11] Breuil, C. (2000) *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. of Math. (2) 152, no. 2, 489-549.

[12] Brion, O. and Conrad, B. *CMI Summer school notes on p-adic Hodge theory (Preliminary version)*, online, 2009. `math.stanford.edu/~conrad/papers/notes.pdf`

[13] Candilera, M. and Cristante, V. (1995). *Periods and duality of p-adic Barsotti-Tate groups*, Ann. Scuola Norm. Sup. Pisa Cl. Sci., **22** (4), 545-593.

[14] Cartier, P. *Relévements des groupes formels commutatifs*, Séminaire Bourbaki, vol. 1968/69, Exposés 347-363, Exp. no. 359, 217-230, Lecture Notes in Mathematics, Springer, Berlin, 1971.

[15] Coates, J. and Wiles, A. (1977). *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39**, no. 3, pp. 223-251.

[16] Colmez, P. (1992). *Périodes p-adiques des variétés abéliennes*, Math. Ann. 292 (4), 629-644.

[17] Colmez, P. and Fontaine, J.-M. (2000). *Construction des représentations p-adiques semi-stables*, Invent. Math, **140** (1), 1-43.

[18] Cox, L.H. (1974). *Formal A-modules over p-adic integer rings*, Compositio Math 29, 287-308.

[19] Decauwert, J.-M. (1976). *Classification des A-modules formels*, C. R. Acad. Sci. Paris Sér. A-B, **282** (24), Aii, A1413-A1416.

[20] Demazure, M. *Lectures on p-divisible groups*, Lecture Notes in Mathematics, vol. 302, Springer, 1972.

[21] Demazure, M. and Grothendieck, A. *Schémas en groupes I.* (SGA3). *Propriétés générales des schémas en groupes. Séminaire de Géométrie Algébrique du Bois Marie* 1962-64, Lecture Notes in Mathematics, vol. 151, Springer, 1970. Revised and annotated edition. Soc. Math. de France, 2011.

[22] Demchenko, O. V. (2001). *Formal Honda groups: the arithmetic of the group of points*, Algebra i Analiz 12 (2000), no. 1, 132-149; English transl., St. Petersburg Math. J., **12**, no. 1, 101-115.

[23] Faltings, G. (1989). *Crystalline cohomology and p-adic Galois-representations*, Algebraic analysis, geometry and number theory, Johns Hopkins Univ. Press, Baltimore, MD, 25-80.

[24] Florez, J. *Explicit Reciprocity Laws for Higher Local Fields.* Thesis (Ph.D.)-City University of New York. 2016.

[25] Fontaine, J.-M. *Groupes p-divisibles sur le corps locaux*, Astérisque, no. 47-48, Société Mathématique de France, 1977.

[26] Fontaine, J.-M. (1979) *Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate*, Astérisque, no. 65, 3-80.

[27] Fontaine, J.-M. (1982). *Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; Construction d'un anneau de Barsotti-Tate*, Ann. of Math. (2) **115**, no. 3, 529-577.

[28] Fontaine, J.-M. (1990). *Représentations p-adiques des corps locaux I. The Grothendieck Festschrift , vol. II*, Progr. Math., 87, Boston, 249-309.

[29] Fontaine, J.-M. (1994). *Le corps des périodes p-adiques*, Astérisque, no. 223, 59-111.

[30] Fontaine, J.-M. (1994). *Représentations p-adiques semi-estables*, Astérisque, no. 223, 113-184.

[31] Fontaine, J.-M. and Laffaille, G. (1982). *Construction de représentations p-adiques*, Ann. Sci. École Norm. Sup., **15** (4), 547-608.

[32] Fontaine, J.-M. and Messing, W. (1987). *p-adic periods and p-adic étale cohomology*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., 67, Amer. Math. Soc., Providence, 179-207.

[33] Fröhlich, A. *Formal groups*, Lecture Notes in Mathematics, no. 74, Springer, 1968.

[34] Grothendieck, A. *Éléments de géométrie algébrique IV. Étude locale des schémas et des morphismes de schémas I*, Inst. Hautes Études Sci. Publ. Math., no. 20, 1964.

[35] Grothendieck, A. *Éléments de géométrie algébrique IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math., no. 32, 1967.

[36] Grotehndieck, A. (1970). *Groupes de Barsotti-Tate et cristaux*, Actes du Congrés International des Mathñematiciens, Tome 1, 431-436.

[37] Grothendieck, A. *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Séminaire de Mathématiques Supérieures, No. 45 (Été, 1970), Les Presses de l'Université de Montréal, Montreal, Que., 1974, 155 pp.

[38] Grothendieck, A. and Dieudonné, J.A. *Éléments de géométrie algébrique I. Fundamental Principles of Mathematical Sciences*, Springer, 1971.

[39] Haines, T. J. *Notes on Tate's p-divisible groups*, online. `http://www.math.umd.edu/~tjh/Tate_pdiv_notes.pdf`

[40] Hazewinkel, M. (1977). *Une théorie de Cartier-Dieudonné pour les A-modules formels*, C. R. Acad. Sci. Paris Sér. A-B, **284** (12), A655-A657.

[41] Hazewinkel, M. *Formal groups and applications*, Pure and Applied Mathematics, vol. 78, Academic Press, 1978.

[42] Herr, L. (1998). *Sur la cohomologie galoisienne des corps p-adiques*, Bull. Soc. Math. France, 126, no. 4, 563-600.

[43] Honda, T. (1970). *On the theory of commutative formal groups*, J. Math. Soc. Japan, 22, 213-246.

[44] Illusie, L. (1990). *Cohomologie de de Rham et cohomologie étale p-adique (d'après G. Faltings, J.-M. Fontaine et al.)*, Séminaire Bourbaki, vol. 1989/90, Astérisque no. 189-190, Exp. no. 726, 325-374.

[45] Kato, K. (1991). *The explicit reciprocity law and the cohomology of Fontaine-Messing*. Bull. Soc. Math. France 119, no. 4, 397-441.

[46] Kato, K. (1999). *Generalized explicit reciprocity laws. Algebraic number theory* (Hapcheon/Saga, 1996), Adv. Stud. Contemp. Math. 1, 57-126.

[47] Katz, N. M. (1981). *Crystalline cohomology, Dieudonné modules, and Jacobi sums*, Automorphic forms representation theory and arithmetic (Bombay, 1979), Tata Inst. Fund. Res. Studies in Math, 10, 165-246.

[48] Kolyvagin, V. A. (1979). *Formal groups and the norm residue symbol.* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 43, no. 5, 1054-1120, 1198.

[49] Laffaille, G. (1979). *Construction de groupes p-divisibles. Le cas de dimension 1*, Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. III, Astérisque, no. 65, Soc. Math. France, Paris, 103-123.

[50] Laffaille, G. (1980). *Groupes p-divisibles et modules filtrés: le cas peu ramifié*, Bull. Soc. Math. France, **108** (2), 187-206.

[51] Lang, S. *Algebraic number theory*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970.

[52] Lipman, J., Nayak, S. and Sastry, P. (2005). *Pseudofunctorial behavoir of Cousin complexes on formal schemes. Variance and duality for Cousin complexes on formal schemes*, Contemp. Math., no. 375, 3-133.

[53] Lubin, J. and Tate, J. (1965). *Formal complex multiplication in local fields*, Ann. of Math., 81, no. 2, 380-387.

[54] Matsumura, H. *Commutative ring theory*, Cambridge Univ. Press, 1986.

[55] Mazur, B. and Messing, W. *Universial extension and one dimensional crystalline cohomology*, Lecture Notes in Mathematics, vol. 370, Springer, 1974.
[56] Messing, W. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, vol. 264, Springer, 1972.
[57] Milne, J.S. (1986). *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 103-150.
[58] Neukirch, J. and Schmidt, A. and Wingberg, W. *Cohomology of number fields*, Springer, 1999.
[59] Serre, J.-P. (1967). *Sur les groupes de Galois attachés aux groupes p-divisibles*, Proc. Conf. Local Fields (Driebergen, 1966), 118-131.
[60] Serre, J.-P. (1967). *Groupes p-divisibles (d'après J. Tate)*, Séminaire Bourbaki 1966/67, Exposé 318, Société Mathématique de France, 1995.
[61] Serre, J.-P. *Local fields*, Graduate Texts in Mathematics, 67, Springer-Verlag, New York-Berlin, 1979.
[62] de Shalit, E. (1985). *Relative Lubin-Tate groups*, Proc. Amer. Math. Soc. 95, no. 1, 1-4.
[63] Shatz, S. S. (1986). *Group schemes, formal groups, and p-divisible groups*, Arithmetic geometry (Storrs, Conn. 1984), 29-78.
[64] Stix, J. *A course on finite flat group schemes and p-divisible groups*, online, 2009. `www.uni-frankfurt.de/52288632/Stix_finflat_Grpschemes.pdf`
[65] Sweedler, M. E. (1975). *When is the tensor product of algebras local?*, Proc. Amer. Math. Soc., **48**, 8-10.
[66] Taniyama, Y. (1957). *L-functions of number fields and zeta functions of abelian varieties*, J. Math. Soc. Japan, 9, 330-366.
[67] Tate, J.-T. (1967). *p-divisible groups*, Proc. Conf. Local Fields (Driebergen, 1966), 158-183.
[68] Tavares Ribeiro, F. (2011). *An explicit formula for the Hilbert symbol of a formal group*, Ann. Inst. Fourier, **61**(1), 261-318.
[69] Vostokov, S. V. (1979). *Normed pairing in formal modules*, Izv. Akad. Nauk SSSR Ser. Mat. **43**, no. 4, 765-794.
[70] Vostokov, S. V. and Demchenko, O. V. (1998). *Explicit form of the Hilbert pairing for relative formal Lubin-Tate groups*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 227 (1995), 41-44; English transl., J. Math. Sci. (New York), **89**, no. 2, 1105-1107.
[71] Vostokov, S. V. and Demchenko, O. V. (2003). *An explicit formula for the Hilbert pairing of formal Honda groups*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 272 (2000), 86-128; English transl., J. Math. Sci. (N. Y.), **116**, 2926-2952.
[72] Vostokov, S. V. and Lorents, F. (2003). *An explicit formula for the Hilbert symbol for Honda groups in a multidimensional local field.* Mat. Sb. 194, no. 2, 3-36; translation in Sb. Math. 194, no. 1-2, 165-197
[73] Waterhouse, W. C. *Introduction to affine group schemes*, Graduate Texts in Mathematics, 66, Springer, 1979.
[74] Wiles, A. (1978). *Higher explicit reciprocity laws*, Ann. Math., **107**(2), 235-254.

Índice alfabético

Esta tesis consta de dos partes bien diferenciadas e independientes, pero dentro de un campo común, el de las leyes de reciprocidad de la Teoría de Números. La primera versa sobre leyes de reciprocidad particulares, con fórmulas en términos de coordenadas/parámetros de los argumentos, mientras que la segunda lo hace sobre leyes de reciprocidad explícitas con fórmulas analíticas, sobre grupos formales p-divisibles y con el método de períodos p-ádicos, en el marco del 9º Problema de Hilbert. Se tratan así dos facetas diferentes de las varias que tiene el campo de las leyes de reciprocidad. Los métodos en cada una de ellas son pues muy diferentes.