Leyes de grupo formal de Lubin-Tate

José Cuevas Barrientos

1. Preliminares

1.1. Leyes de grupos formales.

Definición 1.1: Una ***ley de grupo formal (unidimensional)*** (o simplemente ***grupo formal*** en otros textos) es un par (A, F), donde A es un dominio[1] y $F \in A[[x, y]]$ es una serie formal de potencias tal que:

1. $F(x, 0) = x$ y $F(0, y) = y$.
2. $F(x, F(y, z)) = F(F(x, y), z)$ (asociatividad).

Si F además satisface que $F(x, y) = F(y, x)$, entonces se dice que (A, F) es una ley de grupo formal conmutativo.

De no haber ambigüedad sobre los signos diremos a secas que F es una ley de grupo formal sobre A.

Definición 1.2: Sea A un dominio y sean F, G dos leyes de grupo formal sobre A. Un ***homomorfismo de leyes de grupo formal*** $\alpha \colon F \to G$ es una serie formal de potencias $\alpha(t) \in A[[t]]$ tal que

$$F(\alpha(x), \alpha(y)) = \alpha(G(x, y)).$$

Se denota por $\operatorname{Hom}_A(F, G)$ a los homomorfismos de leyes de grupo formal desde F a G. Un homomorfismo α se dice un ***isomorfismo*** si existe otro homomorfismo $\beta \colon G \to F$ tal que

$$\alpha(\beta(t)) = \beta(\alpha(t)) = t,$$

en cuyo caso, β se dice la ***inversa*** de α. Un isomorfismo α se dice ***estricto*** si $\alpha(x) \equiv x \pmod{\deg 2}$.

1.2. Cuerpos métricos.

Definición 1.3: Un ***cuerpo métrico*** es un par $(K, |\,|)$ donde K es un cuerpo y $|\,| \colon K \to \mathbb{R}_{\geq 0}$ es una función valor absoluto, i.e., una función que satisface:

1. $|x| \geq 0$ y $|x| = 0$ syss $x = 0$.
2. $|x|\,|y| = |xy|$.

Fecha: 26 de octubre de 2022.

[1] Un anillo unitario conmuativo .

3. $|x+y| \leq |x| + |y|$ (desigualdad triangular).

Un cuerpo métrico es ***ultramétrico*** si además satisface:

4. $|x+y| \leq \max\{|x|, |y|\}$ (desigualdad ultramétrica).

Un cuerpo métrico es ***completo*** si lo es con respecto a la métrica, i.e., si todas las sucesiones de Cauchy convergen.

Un cuerpo métrico se dice ***de valuación discreta*** si el grupo multiplicativo

$$\{|a| : a \in K^\times\} \subseteq \mathbb{R}^\times$$

es un subespacio discreto (con la topología usual sobre $\mathbb{R}$).

Ejemplo. Sea ν_p la valuación p-ádica sobre $\mathbb{Z}$, vale decir, la función tal que $\nu_p(a) = n$ si $p^n \mid a$ pero $p^{n+1} \nmid a$. Ésta se extiende a $\mathbb{Q}$ definiendo $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$. Finalmente, la función

$$\left|\frac{a}{b}\right|_p := p^{-\nu_p(a/b)}$$

es un valor absoluto ultramétrico sobre $\mathbb{Q}$, llamado el valor absoluto p-ádico.

Si K es un cuerpo ultramétrico, entonces tiene asociado un anillo y un ideal:

$$\mathfrak{o} := \{a \in K : |a| \leq 1\}, \qquad \mathfrak{m} := \{a \in K : |a| < 1\}.$$

Proposición 1.4: $(\mathfrak{o}, \mathfrak{m})$ es un anillo local (cfr. [**3,** pág. 155]), que llamamos el ***anillo de valuación*** de K.

Como es local, tiene asociado un cuerpo $k := \mathfrak{o}/\mathfrak{m}$ el cual llamamos el ***cuerpo de residuos (de clases)*** de K.

Teorema 1.5: El anillo $(\mathfrak{o}, \mathfrak{m}, k)$ es un dominio de valuación discreta (i.e., $\mathfrak{m}$ es principal) syss K es un cuerpo ultramétrico de valuación discreta (cfr. [**1,** pág. 42]).

Definición 1.6: Si $(A, \mathfrak{m})$ es un dominio de valuación discreta, un elemento $\pi \in A$ tal que $\mathfrak{m} = (\pi)$ se dice un ***uniformizador***.

Teorema 1.7: Si K es un cuerpo métrico, entonces existe un único cuerpo métrico completo L que le contiene y tal que K es denso en L. Éste cuerpo L es único salvo K-isomorfismos isométricos (cfr. [**1,** pág. 24])

Definición 1.8: Al cuerpo del teorema anterior le decimos la ***compleción*** de K y se denota $\hat{K}$.

Ejemplo. $\mathbb{Q}_p$ es por definición la compleción de $(\mathbb{Q}, |\,|_p)$ y sus elementos se dicen ***números p-ádicos***. Una extensión finita de $\mathbb{Q}_p$ se dice así mismo un «cuerpo p-ádico».

Teorema 1.9: Sea K un cuerpo ultramétrico no-trivial, son equivalentes:

1. K es localmente compacto (como espacio topológico).
2. K es completo, de valuación discreta y su cuerpo de residuos es finito.

DEMOSTRACIÓN: Cfr. [**1,** pág. 46]. □

Definición 1.10: Un ***cuerpo local*** K es un cuerpo métrico localmente compacto.

Queda implícito que al declarar «sea K un cuerpo local» lo tomamos junto a una elección de valor absoluto.

Corolario 1.10.1: Todo cuerpo p-ádico $K/\mathbb{Q}_p$ y toda extensión finita $K/\mathbb{F}_p((t))$ son cuerpos locales. En ambos casos, su cuerpo de residuos k es una extensión finita de $\mathbb{F}_p$.

Uno puede inclusive probar que los cuerpos locales de característica 0 son $\mathbb{R}$ y $\mathbb{C}$ (arquimedianos), y los cuerpos p-ádicos (ultramétricos). En característica prima $p > 0$ aparecen extensiones finitas del cuerpo de series formales $\mathbb{F}_p((t))$.

Definición 1.11: Sea p un número primo y sea $K := \mathbb{Q}_p$ o $K := \mathbb{F}_p((t))$. Dada una extensión finita separable L/K de grado n, llamamos su ***índice de ramificación*** y su ***grado de inercia*** a

$$e := [L^\times : K^\times], \qquad f := [\Bbbk_L : \mathbb{F}_p].$$

Teorema 1.12: Si L/K es una extensión finita separable entre cuerpos locales de grado n, entonces $ef = n$ (cfr. [**1,** pág. 125]).

Definición 1.13: Una extensión finita separable de cuerpos locales L/K se dice ***no ramificada*** si $e = 1$ (o si $f = n$).

Teorema 1.14: Sea K un cuerpo local. Existe una única extensión algebraica K^{nr}/K tal que para toda extensión finita separable L/K no ramificada se cumple que $L \subseteq K^{\mathrm{nr}}$ (cfr. [**1,** pág. 123]).

(Evidentemente, en el teorema anterior se asumen de antemano inclusiones de L y K^{nr} en una clausura algebraica o separable de K.)

1.3. La ecuación funcional y lema de integridad.

Definición 1.15: Los ***ingredientes*** para una ecuación funcional son:

- K/A una extensión de anillos (K no es necesariamente un cuerpo).
- $\sigma\colon K \to K$ un endomorfismo de K tal que $\sigma[A] \subseteq A$.
- $\mathfrak{a} \trianglelefteq A$ es un ideal.
- p es un número primo con $p \in \mathfrak{a}$ y q es una potencia de p tal que para todo $a \in A$ se cumple que $\sigma(a) \equiv a^q \pmod{\mathfrak{a}}$.
- $s_1, s_2, s_3, \ldots$ es una sucesión de elementos de K tales que $s_i\mathfrak{a} \subseteq A$.

Además, exigimos que

$$\forall r \in \mathbb{N}, b \in K \quad \mathfrak{a}^r b \subseteq \mathfrak{a} \implies \mathfrak{a}^r \sigma(b) \subseteq \mathfrak{a}.$$

Nótese que la última condición se satisface si $\mathfrak{a} = (c)$ y $\sigma(c) = uc$ con $u \in A^\times$.

Ejemplo. Sea K un cuerpo local ultramétrico cuyo cuerpo de residuos k tiene $q < \infty$ elementos. Sea $p := \operatorname{car} k$, sea $A := \mathfrak{o}$ el anillo de valuación de K, $\mathfrak{a} := \mathfrak{m}$ su ideal maximal y sea σ el único endomorfismo (de Frobenius) tal que $\sigma(a) \equiv a^q \pmod{\mathfrak{m}}$ (cfr. [**1,** pág. 148]). Si π es un uniformizador de $\mathfrak{o}$, entonces con $s_i \in \pi^{-1}\mathfrak{o}$ se tienen ejemplos de ingredientes.

Proposición 1.16 (ecuación funcional): Dados unos ingredientes y una serie de potencias $g(x) \in A[[x]]$ sin término constante, entonces existe una única serie $f_g \in A[[x]]$ tal que

$$f_g(x) = g(x) + \sum_{i=1}^{\infty} s_i \sigma_*^i f(x^{q^i}),$$

donde $\sigma_*^i f_g$ significa aplicar i veces el endomorfismo a los coeficientes de f_g.

Definición 1.17: Fijando los ingredientes $A, K, \mathfrak{a}$. Decimos que dos series de potencias $f(x), \bar{f}(x)$ que vengan de ecuaciones funcionales son ***del mismo tipo*** si los ingredientes restantes $p, q, \sigma, (s_n)_n$ son los mismos en ambos casos.

Lema 1.18 (de integridad): Sean $A, K, \sigma, \mathfrak{a}, p, q, s_n$ ingredientes y sean $g(x) = \sum_{i=1}^{\infty} b_i x^i, \bar{g}(x) = \sum_{i=1}^{\infty} \bar{b}_i x^i \in A[[x]]$ series de potencias con $b_1 \in A^\times$. Entonces:

1. $F(x,y) := f_g^{-1}\big(f_g(x) + f_g(y)\big) \in A[[x]]$.
2. $f_g^{-1}\big(f_{\bar{g}}(x)\big) \in A[[x]]$.
3. Dado $h(x) = \sum_{i=1}^{\infty} c_i x_i \in A[[x]]$ existe una serie de potencias $\hat{h}(x) \in A[[x]]$ tal que $f_g(h(x)) = f_{\hat{h}}(x)$.
4. Sean $\alpha(x) \in A[[x]]$, $\beta(x) \in K[[x]]$ con $r \in \mathbb{N}_{\neq 0}$ se cumple:

$$\alpha(x) \equiv \beta(x) \pmod{\mathfrak{a}^r A[[x]]} \iff f_g\big(\alpha(x)\big) \equiv f_g\big(\beta(x)\big) \pmod{\mathfrak{a}^r A[[x]]}.$$

Corolario 1.18.1: Sean $f(x), \bar{f}(x)$ series que satisfagan ecuaciones funcionales. Los grupos formales $F(x,y) := f^{-1}(f(x) + f(y))$ y $\bar{F}(x,y) := \bar{f}^{-1}(\bar{f}(x) + \bar{f}(y))$ son estrictamente isomorfos syss f y $\bar{f}$ son del mismo tipo.

2. Las leyes de grupo formal de Lubin-Tate

Sea K un cuerpo local ultramétrico. Sea π un uniformizador de su anillo de valuación $(\mathfrak{o}, \mathfrak{m})$. Denotamos por $\mathscr{E}_\pi$ el conjunto de todas las series de potencias $e(x) \in \mathfrak{o}[[x]]$ tales que

$$e(x) \equiv \pi x \pmod{\deg 2}, \qquad e(x) \equiv x^q \pmod{\pi}.$$

Por ejemplo, $\pi x + x^q \in \mathscr{E}_\pi$.

Lema 2.1: Sean $e(x), \bar{e}(x) \in \mathscr{E}_\pi$, y sea $L(\boldsymbol{x}) := L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i$ una forma lineal. Existe una única serie formal $\phi(\boldsymbol{x}) \in \mathfrak{o}[[\boldsymbol{x}]]$ tal que:

1. $\phi(\boldsymbol{x}) \equiv L(\boldsymbol{x}) \pmod{\deg 2}$.
2. $e\big(\phi(\boldsymbol{x})\big) = \phi\big(\bar{e}(x_1), \dots, \bar{e}(x_n)\big)$.

Demostración: Iremos construyendo aproximaciones de ϕ por recursión y un argumento inductivo nos dará unicidad en cada paso. Definamos $\phi_1(\boldsymbol{x}) := L(\boldsymbol{x})$ y supongamos que tenemos $\phi_r(\boldsymbol{x})$ de grado r de modo que:

$$e\big(\phi_r(\boldsymbol{x})\big) \equiv \phi_r\big(\bar{e}(x_1), \dots, \bar{e}(x_n)\big) \pmod{\deg(r+1)}.$$

Así, definamos

$$\phi_{r+1}(\boldsymbol{x}) := \phi_r(\boldsymbol{x}) + E_{r+1}(\boldsymbol{x}),$$

donde $E_{r+1}(\boldsymbol{x})$ es un polinomio homogéneo de grado $r+1$ sin fijar.

Sea $D_{r+1}(\boldsymbol{x})$ el único polinomio homogéneo de grado $r+1$ tal que

$$e\big(\phi_r(\boldsymbol{x})\big) \equiv \phi_r\big(\bar{e}(x_1), \dots, \bar{e}(x_n)\big) + D_{r+1}(\boldsymbol{x}) \pmod{\deg(r+2)},$$

notamos que

$$\begin{aligned} \phi_{r+1}\big(\bar{e}(x_1), \dots, \bar{e}(x_n)\big) &\equiv \phi_r\big(\bar{e}(x_1), \dots, \bar{e}(x_n)\big) + \pi^{r+1} E_{r+1}(\boldsymbol{x}) \\ e\big(\phi_{r+1}(\boldsymbol{x})\big) &\equiv e(\phi_r(\boldsymbol{x})) + \pi E_{r+1}(\boldsymbol{x}) \pmod{\deg(r+2)}. \end{aligned}$$

Así pues, definiremos:

$$E_{r+1}(\boldsymbol{x}) := \frac{D_{r+1}(\boldsymbol{x})}{\pi^{r+1} - \pi}.$$

Ahora bien, como $-1 \in \mathfrak{o}^\times$, entonces $\pi^r - 1 \in \mathfrak{o}^\times$, por lo que, para ver que E está en $\mathfrak{o}$, simplemente hay que comprobar que $D_{r+1}(\boldsymbol{x}) \equiv 0 \pmod{\pi}$. Para ello, recuerde que $e(x) \equiv \bar{e}(x) \equiv x^q \pmod{\pi}$ y que $a^q \equiv a \pmod{\pi}$ puesto que $a^{q-1} \equiv 1 \pmod{\pi}$ si $a \not\equiv 0$ por Lagrange. Así que

$$\begin{aligned} \phi_r(\bar{e}(x_1), \dots, \bar{e}(x_n)) \equiv \phi_r(x_1^q, \dots, x_n^q) &\equiv \big(\phi_r(x_1, \dots, x_n)\big)^q \\ &\equiv e\big(\phi_r(\boldsymbol{x})\big) \pmod{\pi}, \end{aligned}$$

de modo que su resta, que es D_{r+1}, es nula módulo π.

Finalmente definimos $\phi(\boldsymbol{x}) \equiv \phi_r(\boldsymbol{x}) \pmod{\deg(r+1)}$ para todo r y, como dijimos, la unicidad sale de la unicidad de los ϕ_r's. □

Ésto nos permite construir varias series formales:

Teorema 2.2 (Lubin-Tate): Para todo $e(x), \bar{e}(x) \in \mathscr{E}_\pi$ y todo $a \in \mathfrak{o}$ definamos las series de potencias $F_e(x,y)$ y $[a]_{e,\bar{e}}(x)$ como las únicas que satisfacen:

$$F_e(x,y) \equiv x + y, \qquad [a]_{e,\bar{e}}(x) \equiv ax \pmod{\deg 2}$$
$$e(F_e(x,y)) = F_e(e(x), e(y)), \qquad e([a]_{e,\bar{e}}(x)) = [a]_{e,\bar{e}}(\bar{e}(x)).$$

Denotamos $[a]_e(x) := [a]_{e,e}(x)$. Se cumple lo siguiente:

1. $F_e(x,y)$ es una ley de grupo formal conmutativo.
2. $[a]_e(x)$ es un endomorfismo de $F_e(x,y)$ para todo $a \in \mathfrak{o}$.
3. $[\pi]_e(x) = e(x)$.
4. $[1]_{\bar{e},e} \colon F_e \to F_{\bar{e}}$ es un isomorfismo estricto.
5. $[a]_e([b]_e(x)) = [ab]_e(x)$.
6. $F_e([a]_e(x), [b]_e(x)) = [a+b]_e(x)$.
7. $[1]_{\bar{e},e}([a]_e(x)) = [a]_{\bar{e}}([1]_{\bar{e},e}(x))$.

Demostración: Veamos que $F_e(x,y)$ satisface asociatividad. Definamos $G(x,y,z) := F_e(F_e(x,y),z)$ y $H(x,y,z) = F_e(x, F_e(y,z))$ y notemos que

$$G(x,y,z) \equiv x + y + z \equiv H(x,y,z) \pmod{\deg 2}$$
$$e(G(x,y,z)) = G(e(x), e(y), e(z)), \qquad e(H(x,y,z)) = H(e(x), e(y), e(z)).$$

Así pues, el lema anterior asegura que $G = H$. El resto son similares y, por ende, quedan de ejercicio. □

Recuerde que $\operatorname{End}(F_e)$ es un anillo, donde la suma es la suma coordenada a coordenada y el producto es la composición. Luego se tiene:

Corolario 2.2.1: La aplicación

$$\mathfrak{o} \longrightarrow \operatorname{End}(F_e), \qquad a \longmapsto [a]_e$$

es un monomorfismo de anillos.

Demostración: Basta ver que es una función por el inciso 2 del teorema anterior, respeta suma por 6 y respeta productos por 5. □

Observación 2.2.2: El corolario anterior diría que F_e es el análogo de un «$\mathfrak{o}$-módulo», no obstante, por definición una «ley de grupo formal» es meramente «una ley formal» y carece de puntos para ser un grupo. Esto puede, no obstante, repararse; tome los elementos del maximal $\mathfrak{m}$ y, para ellos, la serie $F_e(-,-)$ convergerá; ahora $F_e(\mathfrak{m})$ *es* un grupo abeliano y es un $\mathfrak{o}$-módulo.

Proposición 2.3: Fijando los intgredientes K, $A := \mathfrak{o}$, $\mathfrak{a} := (\pi)$, $p := \operatorname{car} k$, $q := |k|$, $\sigma = \mathrm{Id}_K$, $s_1 = \pi^{-1}$ y $0 = s_2 = s_3 = \cdots$, se satisface que las leyes de grupo formal de Lubin-Tate están en biyección con las leyes de grupo formal obtenidas a partir del lema de integridad variando el $g(x)$ obtenido por

$$g(x) \longmapsto f_g^{-1}(\pi f_g(x)) \in \mathscr{E}_\pi.$$

Demostración: Primero probaremos la contención «$\subseteq$»: que toda ley de grupo formal de Lubin-Tate viene del lema de integridad. Con $g(x) := x$ se obtiene la serie:

$$f(x) = x + \pi^{-1} f(x^q),$$

definamos:

$$F(x,y) := f^{-1}\big(f(x) + f(y)\big), \qquad [\pi]_F(x) := f^{-1}(\pi f(x)).$$

Nótese que $F \in A[[x,y]]$ por el inciso 1 del lema de integridad, mientras que como $\pi f(x)$ satisface la siguiente ecuación funcional:

$$\pi f(x) = \pi x + \pi^{-1}(\pi f(x^q)),$$

vemos que por el inciso 2 se tiene que $[\pi]_F \in A[[x]]$.

Afirmamos que $[\pi]_F(x) \equiv x^q \pmod{\pi}$: para ello nótese que $f(x) = x + c_q x^q + \cdots$ y $f^{-1}(x) = x + d_q x^q + \cdots$, de modo que

$$\begin{aligned}
[\pi]_F(x) &= (\pi f(x)) + d_q(\pi f(x))^q + \cdots \\
&\equiv \pi x + f(x^q) + d_q(\pi x + f(x^q))^q \pmod{\deg(q+1)} \\
&\equiv f(x^q) + d_q(f(x^q))^q \pmod{\pi} \\
&= x^q + \pi^{-1} f(x^{q^2}) + d_q(x^q + \pi^{-1} f(x^{q^2}))^q \\
&\equiv x^q \pmod{\pi, \deg(q+1)}.
\end{aligned}$$

Ahora, por inducción, supongamos que tenemos probada la relación para $\deg = m-1$. Para probar el caso inductivo, empleamos el inciso 4 del lema de integridad para notar que

$$f([\pi]_F(x)) = [\pi]_F(x) + \pi^{-1} f([\pi]_F(x)^q) \equiv [\pi]_F(x) + \pi^{-1} f(x^{q^2}) \pmod{\pi, \deg m}$$
$$f([\pi]_F(x)) = \pi f(x) = \pi x + f(x^q) = \pi x + x^q + \pi^{-1} f(x^{q^2})$$

de modo que $f([\pi]_F(x)) \equiv f(x^q) \pmod{\pi}$ y luego $[\pi]_F(x) \equiv x^q \pmod{\pi}$ como se quería probar.

En consecuencia, $[\pi]_F(x) \in \mathscr{E}_\pi$, luego definiendo $e(x) := [\pi]_F(x)$ se tiene que $F(x,y) = F_e(x,y)$. Sea $F_{\bar e}(x,y)$ otra ley de grupo formal de Lubin-Tate, entonces por el inciso 4 se cumple que $[1]_{\bar e,e} \colon F_e \to F_{\bar e}$ es un isomorfismo estricto, vale decir,

$$\begin{aligned}
F_{\bar e}(x,y) &= [1]_{\bar e,e}^{-1}\big(F_e([1]_{\bar e,e}(x), [1]_{\bar e,e}(y))\big) \\
&= [1]_{\bar e,e}^{-1} f^{-1}(f([1]_{\bar e,e}(x)) + f([1]_{\bar e,e}(y))) = \bar f^{-1}(\bar f(x) + \bar f(y)),
\end{aligned}$$

donde $\bar{f}(x) := f\big([1]_{\bar{e},e}(x)\big)$. Como $f, \bar{f}$ determinan leyes de grupo formal estrictamente isomorfos, entonces provienen de ecuaciones funcionales del mismo tipo.

Ahora probamos «$\supseteq$»: dada una ley de grupo formal obtenida a partir de una ecuación funcional aplicada a un $g(x)$, la misma demostración prueba que $e(x) := f_g^{-1}(\pi f_g(x)) \in \mathscr{E}_\pi$, de modo que induce una ley de grupo formal de Lubin-Tate $F_e(x,y)$ que es la única tal que $e(F_e(x,y)) = F_e(e(x), e(y))$ y notamos que $F_g(x,y) := f_g^{-1}(f_g(x) + f_g(y))$ también satisface dicha condición. $\square$

Sea K un cuerpo p-ádico, luego podemos tomar dos uniformizadores $\pi, \bar{\pi}$ de su anillo de valuación $\mathfrak{o}$ y existe un invertible $u \in \mathfrak{o}^\times$ tal que $\bar{\pi} = u\pi$. Consideremos su extensión no ramificada maximal K^{nr} y su compleción $\hat{K}^{\mathrm{nr}}$ así como su anillo de valuación $\hat{\mathfrak{o}}^{\mathrm{nr}}$. Luego sea la única extensión continua σ del K-automorfismo de Frobenius sobre K_{nr} y sea $\varepsilon \in \hat{\mathfrak{o}}^{\mathrm{nr}}$ el único elemento tal que $\sigma(\varepsilon) = u\varepsilon$ (cfr. [**2,** pág. 48], Rmk. 8.3.15 (ii)).

Proposición 2.4: Sean $e(x) \in \mathscr{E}_\pi$, $\bar{e}(x) \in \mathscr{E}_{\bar{\pi}}$. Existe una serie de potencias $\alpha(x) \in \hat{\mathfrak{o}}_{\mathrm{nr}}$ tal que para todo $a \in \mathfrak{o}$ se cumple:

$$\alpha(x) \equiv \varepsilon x \pmod{\deg 2}, \qquad \sigma_*\alpha(x) = \alpha([u]_e(x))$$
$$\alpha(F_e(x,y)) = F_{\bar{e}}(\alpha(x), \alpha(y)), \qquad \alpha([a]_e(x)) = [a]_{\bar{e}}(\alpha(x)).$$

Demostración: Por la proposición anterior, y los incisos 4 y 6 del teorema de Lubin-Tate, podemos suponer que

$$F(x,y) = f^{-1}\big(f(x) + f(y)\big), \qquad \bar{F}(x,y) = \bar{f}^{-1}\big(\bar{f}(x) + \bar{f}(y)\big)$$

donde $f, \bar{f}$ satisfacen las ecuaciones funcionales

$$f(x) = x + \pi^{-1} f(x^q), \qquad \bar{f}(x) = x + \bar{\pi}^{-1}\bar{f}(x^q).$$

Ahora bien, podemos considerar los nuevos ingredientes $K = \hat{K}_{\mathrm{nr}}$, $A = \hat{\mathfrak{o}}_{\mathrm{nr}}$, $\mathfrak{a} = \bar{\pi}A$, σ la extensión continua del automorfismo de Frobenius, $s_1 = \bar{\pi}^{-1}$, $0 = s_2 = s_3 = \cdots$; y tomar a la serie de potencias $g(x) = x$ y notar que $\varepsilon f(x)$ satisface una ecuación funcional con éstos ingredientes:

$$\begin{aligned}\varepsilon f(x) &= \varepsilon x + \varepsilon\pi^{-1} f(x) = \varepsilon x + \varepsilon u \bar{\pi}^{-1} f(x)\\ &= \varepsilon x + \bar{\pi}^{-1}\sigma(\varepsilon) f(x) = \varepsilon x + \bar{\pi}^{-1}\sigma_*(\varepsilon f)(x),\end{aligned}$$

de modo que $\bar{f}(x)$ y $\varepsilon f(x)$ satisfacen el mismo tipo de ecuación funcional (sobre $\hat{\mathfrak{o}}_{\mathrm{nr}}$), luego definimos $\alpha(x) := \bar{f}^{-1}(\varepsilon f(x)) \in \hat{\mathfrak{o}}_{\mathrm{nr}}[x]$ por el lema de integridad. Basta recordar que $[a]_e(x) = f^{-1}(af(x))$ para concluir todas las afirmaciones del enunciado, exceptuando que $\sigma_*\alpha(x) = \alpha([u]_e(x))$ lo que sale de que

$$\begin{aligned}\sigma_*\alpha(x) &= \bar{f}^{-1}(\sigma_*(\varepsilon f)(x)) = \bar{f}^{-1}(\varepsilon u f(x))\\ &= \bar{f}^{-1}\big(\varepsilon f([u]_e(x))\big) = \alpha([u]_e(x)).\end{aligned}$$

$\square$

Referencias

1. Cassels, J. W. S. *Local Fields* (Cambridge University Press, 1986).
2. Hazewinkel, M. *Formal groups and applications* (Academic Press, 1978).
3. Nagata, M. *Theory of Commutative Fields Translations in Mathematical Monographies* **125** (American Mathematical Society, 1967).

Correo electrónico: josecuevasbtos@uc.cl
URL: josecuevas.xyz