Motivación

Hemos visto que si R es anillo de característica 0 y F es grupo formal de dim 1 sobre R, entonces

$\log_F(X) \in R \otimes \mathbb{Q}[[X]]$ y $\log_F : F \to \mathbb{G}_a$ es isomorfismo ("estricto" $\log_F(X) = X + \dots$)

definido sobre $R \otimes \mathbb{Q}$ ← se pierde la "integridad"

pero en general no es isomorf sobre R

¿Cómo podemos construir y describir todos los grupos formales sobre R módulo isomorf / isomorf estricto sobre R?

§7. Ecuación Funcional – Lema de Integridad

Ingredientes K anillo, $A \subseteq K$ subanillo

$\sigma: K \to K$ homo. de anillos t.q. $\sigma(A) \subseteq A$

$\mathfrak{a} \subseteq A$ ideal, $p \in \mathbb{N}$ primo con $p \in \mathfrak{a}$, $q = p^\ell$ ($\ell \in \mathbb{N}$)

t.q. $\sigma(x) \equiv x^q \bmod \mathfrak{a}$ $\forall x \in A$

$s_1, s_2, \ldots \in K$ t.q. $s_i \mathfrak{a} \subseteq A$

Obs: $\sigma(x) \equiv x^q \bmod \mathfrak{a}$ $\forall x \in A \Rightarrow \sigma(\mathfrak{a}) \subseteq \mathfrak{a}$

También asumimos

(*) $\forall r \in \mathbb{N}, \forall b \in K$: $\mathfrak{a}^r \cdot b \subseteq \mathfrak{a} \Rightarrow \mathfrak{a}^r \sigma(b) \subseteq \mathfrak{a}$

Obs: Si $\mathfrak{a} = cA$ con $c \in A$ y además $\sigma(c) = uc$ con $u \in A^\times$, entonces (*) se cumple pues

$$\mathfrak{a}^r \sigma(b) = c^r A \sigma(b) = \sigma(c)^r A \sigma(b) = \sigma(\underbrace{c^r b}_{\in \mathfrak{a}^r b \subseteq \mathfrak{a}}) A \subseteq \sigma(\mathfrak{a}) A \subseteq \mathfrak{a} A = \mathfrak{a}$$

Ejemplos (de Ingredientes) (1) $K = \mathbb{Q}$, $A = \mathbb{Z}$, $\sigma = id: K \to K$

$\mathfrak{a} = p\mathbb{Z}$, $q = p$ ($\forall x \in \mathbb{Z}: x \equiv x^p \bmod p\mathbb{Z}$)

$s_1, s_2, \ldots \in \frac{1}{p}\mathbb{Z} \subseteq \mathbb{Q}$. (*) se cumple ✓

(2) Recordar $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \notin p\mathbb{Z} \right\} \subseteq \mathbb{Q}$ anillo local con ideal maximal $p\mathbb{Z}_{(p)}$ y $\mathbb{Z}_{(p)} / p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p$

$A = \mathbb{Z}_{(p)}[V_1, V_2, \ldots; W_1, W_2, \ldots]$, $K = A \otimes \mathbb{Q}$

$$\sigma\left(b(V_1, V_2, \ldots; W_1, W_2, \ldots)\right) = b(V_1^p, V_2^p, \ldots; W_1^p, W_2^p, \ldots)$$

$\mathfrak{a} = pA$, $q = p$

$s_1, s_2, \ldots \in \frac{1}{p}A$. Notar que $\sigma\left(\sum_{I,J} c_{I,J} V^I W^J\right) = \sum_{I,J} c_{I,J} V^{pI} W^{pJ}$

$\equiv \sum_{I,J} c_{I,J}^p V^{pI} W^{pJ} \bmod \mathfrak{a}$

$\equiv \left(\sum_{I,J} c_{I,J} V^I W^J\right) \bmod \mathfrak{a}$

(*) se cumple pues $\sigma(p) = p$.

(3) K cuerpo local con cuerpo residual k finito

A = anillo de enteros de K

$p = \mathrm{car}(k)$, $q = p$, $\mathfrak{a}$ = ideal maximal de A

$\sigma: K \to K$ único endomorfismo t.q. $\sigma(x) \equiv x^p \bmod \mathfrak{a}$ $\forall x \in A$

(Endomorfismo de Frobenius)

$s_1, s_2, \ldots \in \frac{1}{\pi}A$ donde π es uniformizante de A ($\pi A = \mathfrak{a}$)

(*) se cumple pues $\sigma: A \to A$ es endomorfismo luego $\sigma(\pi) = u\pi$ con $u \in A^\times$

Procedimiento Dado homo. de anillos $\phi: A_1 \longrightarrow A_2$

definimos $\phi_*: A_1[\![X]\!] \longrightarrow A_2[\![X]\!]$

$$\sum_{i=0}^{\infty} a_i X^i \longmapsto \sum_{i=0}^{\infty} \phi(a_i) X^i$$

Dada $g(X) = \sum_{i=1}^{\infty} b_i X^i \in A[\![X]\!]$ y los "ingredientes" anteriores,

definimos $f_g(X) = \sum_{i=1}^{\infty} d_i X^i \in A[\![X]\!]$ a través de la siguiente recurrencia/ec. funcional

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

Observar que si $n = q^r m$ con $r \in \mathbb{N}_0$ y $m \in \mathbb{N}$ con $q \nmid m$

entonces $$d_n = \begin{cases} b_n + s_1 \sigma(d_{n/q}) + s_2 \sigma^2(d_{n/q^2}) + \dots + s_r \sigma^r(d_{n/q^r}) & \text{si } r \geq 1 \\ b_n & \text{si } r = 0. \end{cases}$$

Así la ec. funcional determina de manera única los coeficientes d_n

y por ende la serie $f_g(X) \in X K[\![X]\!]$.

Ejemplos ① Tomando $A = \mathbb{Z}_{(p)}$, $K = \mathbb{Q}$, $\sigma = id: K \longrightarrow K$, $q = p$

$\Pi = p\mathbb{Z}_{(p)}$, $s_1 = \frac{1}{p}$, $s_i = 0$ para $i \geq 2$.

y $g(X) = X$, obtenemos

$d_1 = b_1 = 1$, $d_p = 0 + \frac{1}{p} d_1 = \frac{1}{p}$

$d_{p^2} = 0 + \frac{1}{p} d_p = \frac{1}{p^2}$

$\vdots$

$d_{p^r} = 0 + \frac{1}{p} d_{p^{r-1}} = \frac{1}{p^r}$ para $r \geq 1$

Y si $m \in \mathbb{N}$, $m > 1$ con $p \nmid m$ obtenemos

$d_m = b_m = 0$

$d_{pm} = 0 + \frac{1}{p} d_m = 0$

$d_{p^2 m} = 0 + \frac{1}{p} d_{p m} = 0$

$\vdots$

$d_{p^r m} = 0 + \frac{1}{p} d_{p^{r-1} m} = 0$ para $r \geq 1$

Luego $f_g(X) = X + \frac{1}{p} X^p + \frac{1}{p^2} X^{p^2} + \dots = \sum_{i=0}^{\infty} \frac{1}{p^i} X^{p^i} =: H(X)$

(2) Otra vez $A = \mathbb{Z}_{(p)}$, $K = \mathbb{Q}$, $\sigma = id : K \to K$, $q = p$, $a = p\mathbb{Z}_{(p)}$

$S_1 = \frac{1}{p}$, $s_i = 0$ para $i \geq 2$

Escoger $g(X) = \begin{cases} \sum_{\substack{n \geq 1 \\ \text{impar}}} \frac{1}{n}(X^n - X^{2n}) & \text{si } p = 2 \\ \sum_{\substack{n \geq 1 \\ p \nmid n}} \frac{(-1)^{n+1}}{n} X^n & \text{si } p \geq 3 \end{cases}$

Entonces, para $p = 2$ obtenemos $d_1 = b_1 = 1$

$d_2 = b_2 + \frac{1}{2} d_1 = -1 + \frac{1}{2} = \frac{-1}{2}$

$d_4 = b_4 + \frac{1}{2} d_2 = 0 - \frac{1}{4} = \frac{-1}{4}$

$\vdots$

$d_{2^r} = b_{2^r} + \frac{1}{2} d_{2^{r-1}} = -\frac{1}{2^r}$ para $r \geq 2$

y para $m \geq 3$ impar tenemos:

$d_m = b_m = \frac{1}{m}$

$d_{2m} = b_{2m} + \frac{1}{2} b_m = -\frac{1}{m} + \frac{1}{2}\frac{1}{m} = \frac{-1}{2m}$

$d_{4m} = b_{4m} + \frac{1}{2} b_{2m} = \frac{1}{2}\frac{-1}{2m} = \frac{-1}{4m}$

$\vdots$

$d_{2^r m} = b_{2^r m} + \frac{1}{2} d_{2^{r-1} m} = 0 + \frac{1}{2}\left(\frac{-1}{2^{r-1} m}\right) = \frac{-1}{2^r m}$ para $r \geq 2$

Por lo tanto $f_g(X) = \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} X^m = \log(1+X)$

Para $p \geq 3$ tenemos $d_1 = b_1 = 1$

$d_p = b_p + \frac{1}{p} d_1 = 0 + \frac{1}{p}$

$d_{p^2} = b_{p^2} + \frac{1}{p} d_p = \frac{1}{p^2}$ ... $d_{p^r} = \frac{1}{p^r}$ para $r \geq 2$

y para $m > 1$, $p \nmid m$ tenemos

$d_m = b_m = \frac{(-1)^{m+1}}{m}$

$d_{mp} = b_{mp} + \frac{1}{p} d_m = 0 + \frac{1}{p}\frac{(-1)^{m+1}}{m} = \frac{(-1)^{mp+1}}{mp}$

$\vdots$

$d_{mp^r} = 0 + \frac{1}{p} d_{mp^{r-1}} = \frac{1}{p}\frac{(-1)^{mp^{r-1}+1}}{mp^{r-1}} = \frac{(-1)^{mp^r+1}}{mp^r}$

Por lo tanto $f_g(X) = \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} X^m = \log(1+X)$

¡Igual que antes!

Lema de ecuación funcional

Sean $A, K, \sigma, \pi, p, q, s_1, s_2, \dots$ ingredientes,

Sean $g(X) = \sum_{i=1}^{\infty} b_i X^i$, $\tilde{g}(X) = \sum_{i=1}^{\infty} \tilde{b}_i X^i \in A[[X]]$

tal que $b_1 \in A^\times$ (sólo para $g(X)$). Entonces

i) La serie $F_g(X,Y) := f_g^{-1}(f_g(X) + f_g(Y))$ está en $A[[X,Y]]$

ii) $f_g^{-1}(f_{\tilde{g}}(X)) \in A[[X]]$

iii) Si $h(X) = \sum_{n=1}^{\infty} c_n X^n \in A[[X]]$, entonces $\exists\, \hat{h}(X) = \sum_{n=1}^{\infty} \hat{c}_n X^n \in A[[X]]$

tal que $f_g(h(X)) = f_{\hat{h}}(X)$.

iv) Si $\alpha(X) \in A[[X]]$ y $\beta(X) \in K[[X]]$, $r \in \mathbb{N}$ entonces

$\alpha(X) \equiv \beta(X) \bmod \pi^r[[X]] \iff f_g(\alpha(X)) \equiv f_g(\beta(X)) \bmod \pi^r[[X]]$

Notación: Sean $f, \tilde{f} \in XK[[X]]$, $g, \tilde{g} \in XA[[X]]$ tales que:

$$f(X) = g(X) + \sum_{i=1}^{\infty} s_i \sigma_*^i (f)(X^{q^i}) \quad \text{y} \quad \tilde{f}(X) = \tilde{g}(X) + \sum_{i=1}^{\infty} s_i \sigma_*^i (\tilde{f})(X^{q^i})$$

Entonces decimos que f y $\tilde{f}$ satisfacen el mismo tipo de ecuación funcional (mismos $A, \sigma, p, q, s_1, s_2, \dots$ pero quizás $g \neq \tilde{g}$)

Prop: Suponga $f, \tilde{f} \in XK[[X]]$ tales que $f(X) \equiv \tilde{f}(X) \equiv X \bmod \deg 2$ y $f, \tilde{f}$ satisfacen ecuaciones funcionales. Podemos definir

$$F(X,Y) = f^{-1}(f(X) + f(Y)), \quad \tilde{F}(X,Y) = \tilde{f}^{-1}(\tilde{f}(X) + \tilde{f}(Y))$$

Entonces: $\exists\, h : F \to \tilde{F}$ isomorfismo "estricto" definido sobre A $\iff$ $f, \tilde{f}$ satisfacen el mismo tipo de ec. funcional

(i.e. $h \in XA[[X]]$ y $h(X) \equiv X \bmod \deg 2$)

Dem: Escribamos $f = f_g$, $\tilde{f} = f_{\tilde{g}}$ obtenidas vía ecuaciones funcionales (quizás de distinto tipo)

($\Rightarrow$) Si $\exists\, h : F \xrightarrow{F_g} \tilde{F} \xrightarrow{F_{\tilde{g}}}$ isomorfismo estricto, entonces como también

$f = f_g : F_g \longrightarrow \mathbb{G}_a$, $\tilde{f} = f_{\tilde{g}} : F_{\tilde{g}} \to \mathbb{G}_a$ isomorfismos estrictos, obtenemos:

$\tilde{f} \circ h \circ f^{-1} : \mathbb{G}_a \longrightarrow \mathbb{G}_a$ isomorfismo estricto. Pero $\mathrm{Aut}_K(\mathbb{G}_a) = \{uX : u \in K^\times\}$

por lo tanto $\tilde{f} \circ h \circ f^{-1}(X) = X$. Luego $\tilde{f} \circ h = f$. Por iii) tenemos

$\exists\, \hat{h} \in XA[[X]] : f = \tilde{f} \circ h = f_{\tilde{g}} \circ h = f_{\hat{h}}$ donde $f_{\hat{h}}$ satisface mismo tipo de ec funcional que $f_{\tilde{g}}$

Por lo tanto f y $\tilde{f}$ satisfacen mismo tipo de ecuación funcional.

($\Leftarrow$) Si f y $\tilde{f}$ satisfacen el mismo tipo de ec funcional,

entonces por ii) $h := f_{\tilde{g}}^{-1}(f_g(X)) = \tilde{f}^{-1} \circ f(X) \in A[[X]]$ y se verifica que $h: F \to \tilde{F}$ es isom. estricto definido sobre A.

$$\left(\tilde{F}(h(X), h(Y)) = h(F(X,Y)) \right) \Leftrightarrow \tilde{f}^{-1}(\tilde{f} \circ h(X) + \tilde{f} \circ h(Y)) = h(f^{-1}(f(X)+f(Y)))$$
$$\Leftrightarrow f^{-1}(f(X)+f(Y)) = h(f^{-1}(f(X)+f(Y)))$$
$$\Leftrightarrow f(X)+f(Y) = f(f^{-1}(f(X)+f(Y)))$$

Aplicaciones (1) Recordar que si $A = \mathbb{Z}_{(p)}$, $K = \mathbb{Q}$, $\sigma = id_K$, $q = p$, $a = p\mathbb{Z}_{(p)}$, $s_1 = \frac{1}{p}$, $s_i = 0$ $\forall i \neq 2$

Entonces $H(X) := \sum_{i=0}^{\infty} \frac{1}{p^i} X^{p^i} = f_g(X)$ donde $g(X) = X$.

y $L(X) := \log(1+X) := \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} X^m = f_{\tilde{g}}(X)$ donde $\tilde{g}(X) = \begin{cases} \sum_{\substack{n \geq 1 \\ \text{impar}}} \frac{1}{n}(X^n - X^{2n}) & \text{si } p=2 \\ \sum_{\substack{n \geq 1 \\ p \nmid n}} \frac{(-1)^{n+1}}{n} X^n & \text{si } p \geq 3 \end{cases}$

Como $L^{-1}(X) = \exp(X) - 1 = \sum_{n=1}^{\infty} \frac{X^n}{n!}$ concluimos:

$$\exp(H(X)) = L^{-1}(H(X)) + 1 = f_{\tilde{g}}^{-1}(f_g(X)) + 1 \in \mathbb{Z}_{(p)}[[X]]$$

$\Rightarrow \exp(H(X)) \in \mathbb{Z}_{(p)}[[X]]$ (Hasse) por ii) del Lema de ec. funcional

Más generalmente, podemos probar:

Prop: Si $d(X) = \sum_{i=0}^{\infty} d_i X^{p^i} \in \mathbb{Q}[[X]]$ y $\exp(d(X)) = \sum_{n=0}^{\infty} c_n X^n$

entonces: $c_n \in \mathbb{Z}_{(p)}$ $\forall n \in \mathbb{N}_0$ $\Leftrightarrow$ $\exists\, b_0, b_1, \ldots \in \mathbb{Z}_{(p)}$ t.q. $d_0 = b_0$ y $d_i = \frac{1}{p} d_{i-1} + b_i$ $\forall i \geq 1$

Dem: ($\Leftarrow$) $d(X) = f_{\hat{g}}(X)$ donde $\hat{g}(X) := \sum_{i=0}^{\infty} b_i X^{p^i} \in \mathbb{Z}_{(p)}[[X]]$

luego $\exp(d(X)) = L^{-1}(d(X)) + 1 = f_{\tilde{g}}^{-1}(f_{\hat{g}}(X)) + 1 \in \mathbb{Z}_{(p)}[[X]]$ por ii) del Lema de ec funcional

($\Rightarrow$) Si $\exp(d(X)) \in \mathbb{Z}_{(p)}[[X]]$ entonces

$$d(X) = L(\exp(d(X)) - 1) = f_{\tilde{g}}(\underbrace{\exp(d(X)) - 1}_{h(X)}) = f_{\hat{h}}$$

para algún $\hat{h}(X) \in X\mathbb{Z}_{(p)}[[X]]$ por iii) del Lema de ec. funcional.

Si escribimos $\hat{h}(X) = \sum_{i=0}^{\infty} b_i X^{p^i} + \sum_{\substack{j \geq 1 \\ j \neq p^i, i \geq 0}} e_j X^j \in \mathbb{Z}_{(p)}[[X]]$

vemos que $d_i = b_i + \frac{1}{p} d_{i-1}$ si $i \geq 1$, $d_0 = b_0$ // (De hecho $e_j = 0$ $\forall j$)

(2) Lema de integralidad de Dwork

- Bernard Dwork (1923 - 1998) Matemático estadounidense. Demostró la primera parte de las conjeturas de Weil (la función zeta de var. proy. suave sobre cuerpo finito es función racional)

Sea T = completación de $\mathbb{Q}_p^{ur}$, $\mathcal{O}_T/\mathfrak{m}_T \simeq \overline{\mathbb{F}_p}$, $\mathfrak{m}_T = p\mathcal{O}_T$

$\sigma \in Gal(T/\mathbb{Q}_p)$ aut. de Frobenius ($\sigma = Frob \in Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$)

Sea $h(X) = 1 + a_1 X + a_2 X + \ldots \in T[[X]]$

Entonces: $h(X) \in \mathcal{O}_T[[X]] \iff \dfrac{\sigma_* h(X^p)}{h(X)^p} \in 1 + X\mathfrak{m}_T[[X]]$

Dem: Escoger $K = T$, $A = \mathcal{O}_T$, $a = p\mathcal{O}_T = \mathfrak{m}_T$, σ = aut. de Frob. en $Gal(T/\mathbb{Q}_p)$

$s_1 = \frac{1}{p}$, $s_i = 0 \ \forall i \geq 2$

Notar que $K \supseteq \mathbb{Q}$, $A \supseteq \mathbb{Z}_{(p)}$, $a \supseteq p\mathbb{Z}_{(p)}$, $\sigma|_{\mathbb{Q}} = id_{\mathbb{Q}}$

luego $L(X) = \log(1+X) = f_{\tilde{g}}(X)$ con $\tilde{g}(X) \in X\mathbb{Z}_p[[X]] \subseteq X\mathcal{O}_T[[X]]$ (↑ Como antes)

Si $h(X) \in \mathcal{O}_T[[X]]$ entonces

$$\log(h(X)) = L(h(X) - 1) = f_{\tilde{g}}\Big(\sum_{i=1}^{\infty} a_i X^i\Big) = f_{\hat{h}} \quad \text{para algún } \hat{h} \in X\mathcal{O}_T[[X]]$$

($\sum a_i X^i \in \mathcal{O}_T[[X]]$ por iii)

Luego $\log(h(X)) = \hat{h}(X) + \frac{1}{p}\sigma_* \log(h(X^p)) = \hat{h}(X) + \frac{1}{p}\log(\sigma_* h(X^p))$

y así

$$\log(h(X)) - \frac{1}{p}\cdot\log(\sigma_* h(X^p)) \in X\mathcal{O}_T[[X]] \quad / \cdot(-p)$$

$$\iff -p\log(h(X)) + \log(\sigma_* h(X^p)) \in Xp\mathcal{O}_T[[X]]$$

$$\iff \log\left(\frac{\sigma_* h(X^p)}{h(X)^p}\right) \in Xp\mathcal{O}_T[[X]]$$

$$\iff f_{\tilde{g}}\left(\frac{\sigma_* h(X^p)}{h(X)^p} - 1\right) \equiv 0 = f_{\tilde{g}}(0) \mod p\mathcal{O}_T[[X]]$$

$$\iff \frac{\sigma_* h(X^p)}{h(X)^p} - 1 \equiv 0 \mod p\mathcal{O}_T[[X]]$$

$$\iff \frac{\sigma_* h(X^p)}{h(X)^p} \in 1 + Xp\mathcal{O}_T[[X]]$$

Recíprocamente, si $\dfrac{\sigma_* h(X^p)}{h(X)^p} \in 1 + Xp\mathcal{O}_T[[X]]$ concluimos que $\log(h(X)) = f_{\hat{h}}$ y por lo tanto

$$h(X) - 1 = f_{\tilde{g}}^{-1}(f_{\hat{h}}) \in \mathcal{O}_T[[X]] \quad \text{por ii)}$$

$$\Rightarrow h(X) \in \mathcal{O}_T[[X]] \ //$$

(3) Construcción de algunos grupos formales

Tomar $A = \mathbb{Z}[V_1, V_2, \ldots; T_1, T_2, \ldots] =: \mathbb{Z}[V,T]$, $K = \mathbb{Q}(V;T]$

$\sigma : K \to K$ $\mathbb{Q}$-homomorfismo con $\sigma(T_i) = T_i^p$, $\sigma(V_j) = T_j^p$ $\forall i,j$

$q = p$, $a = pA$, $s_i = \frac{1}{p} V_i$ $(i \in \mathbb{N})$.

Escogiendo $g(X) = X$, $\tilde{g}(X) = X + \sum_{i=1}^{\infty} T_i X^{p^i}$

obtenemos $f_V := f_g$, $f_{V,T} := f_{\tilde{g}}$

Se tiene $f_V(X) = X + \sum_{i=1}^{\infty} \frac{V_i}{p} f_V^{(p^i)}(X^{p^i})$ donde $f^{(p^i)} := \sigma^i_*(f)$

$$f_{V,T}(X) = X + \sum_{i=1}^{\infty} T_i X^{p^i} + \sum_{i=1}^{\infty} \frac{V_i}{p} f_{V,T}^{(p^i)}(X^{p^i})$$

Obs: $f_V \in (\mathbb{Q}[V])(\!(X)\!)$, $f_{V,0} = f_V$.

$$f_V(X) = \sum_{i=0}^{\infty} a_i(V) X^{p^i}$$

$a_0(V) = 1$, $a_1(V) = \frac{1}{p} V_1$,

$a_2(V) = \frac{1}{p^2} V_1 V_1^p + \frac{1}{p} V_2$,

$a_3(V) = \frac{1}{p^3} V_1 V_1^p V_1^{p^2} + \frac{1}{p^2} V_1 V_2^p + \frac{1}{p^2} V_2 V_1^{p^2} + \frac{1}{p} V_3$

$\vdots$

$$f_{V,T}(X) = \sum_{i=0}^{\infty} a_i(V,T) X^{p^i}$$

$a_0(V,T) = 1$, $a_1(V,T) = \frac{1}{p} V_1 + T_1$

$a_2(V,T) = \frac{1}{p^2} V_1 V_1^p + \frac{1}{p} V_2 + \frac{1}{p} V_1 T_1^p + T_2$

Definir $F_V(X,Y) := F_g(X,Y) = f_V^{-1}(f_V(X) + f_V(Y)) \in (\mathbb{Z}[V])(\!(X,Y)\!)$

$F_{V,T}(X,Y) := F_{\tilde{g}}(X,Y) = f_{V,T}^{-1}(f_{V,T}(X) + f_{V,T}(Y)) \in (\mathbb{Z}[V,T])(\!(X,Y)\!)$

$\alpha_{V,T}(X) := f_{V,T}^{-1}(f_V(X)) \in (\mathbb{Z}[V,T])[\![X]\!]$.

$\alpha_{V,T} : F_V \to F_{V,T}$ isomorf. estricto def. sobre $\mathbb{Z}[V,T]$

Se puede demostrar

Teorema Sea A una $\mathbb{Z}_{(p)}$-álgebra. Todo $F(X,Y)$ grupo formal conmutativo de dim 1 es estrictamente isomorfo a $\sigma_* F_V(X,Y)$ para algún $\sigma : \mathbb{Z}[V] \to A$ homo. de anillos.

Dem del lema de ec. funcional

Trabajaremos en $K[[X,Y]]$. Si $G,H \in K[[X,Y]]$ escribimos

$G \equiv H \mod (\mathfrak{a}^r, \deg m)$ si $G - H = \sum_{i,j\geq 0} b_{ij} X^i Y^j$ con $b_{ij} \in \mathfrak{a}^r$ si $i+j < m$

Además $\mathfrak{a}^0 := A$.

Lema 1: Escribamos $f_q(X) = \sum_{n=1}^{\infty} a_n X^n$ y $n = q^r m$, $q \nmid m$. $r \in \mathbb{N}_0$. Entonces $a_n \mathfrak{a}^r \subseteq A$.

Dem: Por inducción en $r \in \mathbb{N}_0$. Para $r=0$ tenemos $a_n = b_n$ donde $g(X) = \sum_{m=1}^{\infty} b_m X^m \in A[[X]]$, luego $a_n \in A$ y así $a_n \mathfrak{a}^0 \subseteq A$.

Sup $a_n \mathfrak{a}^i \subseteq A$ $\forall n = q^i m$ con $i < r$, $q \nmid m$. Si $\ell = q^r \cdot m$, $q \nmid m$

Entonces $a_\ell = a_{q^r m} = b_{q^r m} + s_1 \sigma(a_{q^{r-1} m}) + s_2 \sigma^2(a_{q^{r-2} m}) + \dots + s_r \sigma^r(a_m)$

($b_{q^r m} \in A$)

$a_{q^i m}\, \mathfrak{a}^i \subseteq A$ $\forall i \in \{0,\dots,r-1\}$ $\Rightarrow$ $a_{q^i m}\, \mathfrak{a}^r \subseteq \mathfrak{a}$ $\forall i \in \{0,\dots,r-1\}$

(hipótesis inductiva) $\Rightarrow$ $\sigma^j(a_{q^i m})\, \mathfrak{a}^r \subseteq \mathfrak{a}$ $\forall i \in \{0,\dots,r-1\}$ $\forall j \in \mathbb{N}_0$

$\Rightarrow$ $s_j \sigma^j(a_{q^i m})\, \mathfrak{a}^r \subseteq s_j \mathfrak{a} \subseteq A$ $\forall i \in \{0,\dots,r-1\}$, $\forall j \in \mathbb{N}_0$

Por lo tanto $a_\ell\, \mathfrak{a}^r \in A$ //

Lema 2: Sean $G(X,Y) \in A[[X,Y]]$, $n = q^r m$, $\ell > 0$. Entonces

$$G(X,Y)^{n q^\ell} \equiv \left((\sigma_*^\ell G)(X^{q^\ell}, Y^{q^\ell}) \right)^n \mod \mathfrak{a}^{r+1}$$

Dem: Recordar $\sigma(x) \equiv x^q \mod \mathfrak{a}$ $\forall x \in A$ y $p \in \mathfrak{a}$ ($\Rightarrow (x+y)^p \equiv x^p + y^p \mod \mathfrak{a}$ $\forall x,y \in A$)

luego $G(X,Y)^{q^\ell} \equiv (\sigma_*^\ell G)(X^{q^\ell}, Y^{q^\ell}) \mod \mathfrak{a}$

Elevando a q obtenemos:

$$G(X,Y)^{q^{\ell+1}} \equiv (\sigma_*^\ell G)(X^{q^\ell}, Y^{q^\ell})^q \mod \underbrace{\binom{q}{1}}_{\subseteq \mathfrak{a}^2} \mathfrak{a} + \binom{q}{2} \mathfrak{a}^2 + \dots + \binom{q}{q} \mathfrak{a}^q$$

luego $G(X,Y)^{q^{\ell+1}} \equiv (\sigma_*^\ell G)(X^{q^\ell}, Y^{q^\ell})^q \mod \mathfrak{a}^2$. Repitiendo el proceso obtenemos $G(X,Y)^{q^{\ell+r}} \equiv (\sigma_*^\ell G)(X^{q^\ell}, Y^{q^\ell})^{q^r} \mod \mathfrak{a}^{r+1}$.

Elevando a m obtenemos

$$G(X,Y)^{n q^\ell} \equiv \left((\sigma_*^\ell G)(X^{q^\ell}, Y^{q^\ell}) \right)^n \mod \mathfrak{a}^{r+1}$$ //

Dem de i): Escribamos $F(X,Y) = F_g(X,Y)$, $f(x) = f_g(x)$.

$F(X,Y) = \sum_{i=1}^{\infty} F_i(X,Y)$, $F_i(X,Y)$ homog. de grado i

Basta probar que $F_i(X,Y) \in A[X,Y]$ $\forall i \geq 1$.

Para $i=1$ observar $f(x) = b_1 X + \dots$, $f^{-1}(x) = b_1^{-1} X + \dots$ luego

$F_1(X,Y) = X+Y \in A[X,Y]$. Suponga $F_1, F_2, \dots, F_{n-1} \in A[X,Y]$

Para $r \geq 2$ tenemos:

$$F(X,Y)^r \equiv (F_1 + F_2 + \dots + F_{n-1})^r \mod \deg n+1$$

Usando Lema 2 con $G = F_1 + F_2 + \dots + F_{n-1}$ obtenemos para $n = q^r m$, $q \nmid m$, $i > 0$

$$\text{(*)} \quad F(X,Y)^{q^{in}} \equiv G^{q^{in}} \equiv \left(\sigma_*^i G(X^{q^i}, Y^{q^i})\right)^m \equiv \left(\sigma_*^i F(X^{q^i}, Y^{q^i})\right)^m \mod (\mathfrak{a}^{r+1}, \deg n+1)$$

Por otro lado, por def de F tenemos $f(F(X,Y)) = f(X) + f(Y)$, luego

$$\sigma_*^i f\left(\sigma_*^i F(X,Y)\right) = \sigma_*^i f(X) + \sigma_*^i f(Y)$$

Ahora, como $f(x) = g(x) + \sum_{n=1}^{\infty} s_n \sigma_*^n f(X^{q^n})$, sustituyendo X por F obtenemos

$$f(F(X,Y)) = g(F(X,Y)) + \sum_{i=1}^{\infty} s_n \sigma_*^i f(F(X,Y)^{q^i})$$

$$= g(F(X,Y)) + \sum_{i=1}^{\infty} s_i \sum_{n=1}^{\infty} \sigma^i(a_n) F(X,Y)^{q^{in}}$$

donde $f(x) = \sum_{n=1}^{\infty} a_n x^n$. De (*) tenemos, para $n = q^r m$

$$s_i \sigma^i(a_m) F(X,Y)^{q^{in}} \equiv s_i \sigma^i(a_m) \left(\sigma_*^i F(X^{q^i}, Y^{q^i})\right)^m \mod \left(s_i \sigma^i(a_m) \mathfrak{a}^{r+1}, \deg n+1\right)$$

pero $a_m \mathfrak{a}^r \in A$ (Lema 1) $\Rightarrow$ $\sigma^i(a_m) \mathfrak{a}^r \subseteq A$

$\Rightarrow$ $\sigma^i(a_m) \mathfrak{a}^{r+1} \subseteq \mathfrak{a}$

$\Rightarrow$ $s_i \sigma^i(a_m) \mathfrak{a}^{r+1} \in A$

luego la congruencia vale mod $(A, \deg n+1)$. Por lo tanto

$$f(F(X,Y)) \equiv g(F(X,Y)) + \sum_{i=1}^{\infty} s_i \underbrace{\sum_{n=1}^{\infty} \sigma^i(a_n) \left(\sigma_*^i F(X^{q^i}, Y^{q^i})\right)^n}_{\sigma_*^i f\left(\sigma_*^i F(X^{q^i}, Y^{q^i})\right) = \sigma_*^i f(X^{q^i}) + \sigma_*^i f(Y^{q^i})} \mod (A, \deg n+1)$$

$$\equiv g(F(X,Y)) + \underbrace{\sum_{i=1}^{\infty} s_i \sigma_*^i f(X^{q^i})}_{= f(X) - g(X)} + \underbrace{\sum_{i=1}^{\infty} s_i \sigma_*^i f(Y^{q^i})}_{= f(Y) - g(Y)}$$

$$\equiv g(F(X,Y)) + \underbrace{f(X) + f(Y) - g(X) - g(Y)}_{} \mod (A, \deg n+1)$$

$$\equiv g(F(X,Y)) + f(F(X,Y)) + 0 \mod (A, \deg n+1) \text{ pues } g \in A[[X]]$$

Como $g(F(X,Y)) \equiv b_1 F_n(X,Y) \mod (A, \deg n+1)$, concluimos

$b_1 F_n(X,Y) \equiv 0 \mod (A, \deg n+1)$, luego $b_1 F_n(X,Y) \in A[X,Y]$. como $b_1 \in A^\times$, obtenemos $F_n(X,Y) \in A[X,Y]$. Esto prueba i)

ii) usa las mismas ideas (ejercicio)

Dem de iii): Sea $\hat{f} := f(h(X))$. Como $h(X) \in A[[X]]$

$$\hat{f}(X) - \sum_{i=1}^{\infty} s_i \sigma_*^i \hat{f}(X^{q^i}) = f(h(X)) - \sum_{i=1}^{\infty} s_i \sigma_*^i f(\sigma_*^i h(X^{q^i}))$$

$$= f(h(X)) - \sum_{i=1}^{\infty} s_i \sum_{n=1}^{\infty} \sigma^i(a_n) \left(\sigma_*^i h(X^{q^i})\right)^n$$

$$\equiv f(h(X)) - \sum_{i=1}^{\infty} s_i \sum_{n=1}^{\infty} \sigma^i(a_n) \left(h(X)^{q^i}\right)^n \quad \text{mod } A$$

pues $\sigma_*^i h(X^{q^i}) \equiv h(X)^{q^i} \bmod \mathfrak{a}$, $\left(\sigma_*^i h(X^{q^i})\right)^n \equiv \left(h(X)^{q^i}\right)^n \bmod \mathfrak{a}^{r+s}$ si $n = q^r m, q \nmid m$

y $a_n \mathfrak{a}^r \subseteq A \Rightarrow a_n \mathfrak{a}^{r+1} \subseteq \mathfrak{a}$

(Lema 1) $\Rightarrow \sigma^i(a_n)\mathfrak{a}^{r+1} \subseteq \mathfrak{a}$

$\Rightarrow s_i \sigma^i(a_n)\mathfrak{a}^{r+1} \subseteq A$

Esto implica $\hat{f}(X) - \sum_{i=1}^{\infty} s_i \sigma_*^i \hat{f}(X^{q^i}) \equiv f(h(X)) - \sum_{i=1}^{\infty} s_i \sigma_*^i \left(f(h(X)^{q^i})\right) \bmod A$

$\equiv g(h(X)) \equiv 0 \quad \text{mod } A$

Por lo tanto $\hat{f} = f_{\hat{h}}$ con $\hat{h}(X) = \hat{f}(X) - \sum_{i=1}^{\infty} s_i \sigma_*^i \hat{f}(X^{q^i}) \in A[[X]]$ //

Dem de iv): ($\Rightarrow$) Sup $\alpha \in A[[X]]$, $\beta(X) = \alpha(X) + \gamma(X)$ con $\gamma(X) \in \mathfrak{a}^r A[[X]]$. Entonces $\beta(X)^{q^i} \equiv \alpha(X)^{q^i} \bmod \mathfrak{a}^{r+i}$ $\forall i \geq 0$.

y $\beta(X)^m \equiv \alpha(X)^m \bmod \mathfrak{a}^{r+i}$ $\forall n = q^i m, q \nmid m$. Luego $a_n \beta(X)^n \equiv a_n \alpha(X)^n \bmod \mathfrak{a}^r$

pues $a_n \mathfrak{a}^i \subseteq A$ (Lema 1). Así $f(\beta(X)) \equiv f(\alpha(X)) \bmod \mathfrak{a}^r$

($\Leftarrow$) Afirmamos: $\alpha(X) \equiv 0 \bmod \mathfrak{a}^r \Rightarrow f^{-1}(\alpha(X)) \equiv 0 \bmod \mathfrak{a}^r$

En efecto, si $\gamma(X) := f^{-1}(\alpha(X))$ entonces $\alpha(X) = f(\gamma(X))$.

Tenemos $\gamma(X) \equiv b_1^{-1}\alpha(X) \equiv 0 \bmod (\mathfrak{a}^r, \deg 2)$. Supongamos hemos probado $\gamma(X) \equiv 0 \bmod (\mathfrak{a}^r, \deg n)$. Entonces

$$\alpha(X) \equiv f(\gamma(X)) = g(\gamma(X)) + \sum_{i=1}^{\infty} s_i \sigma_*^i f(\gamma(X)^{q^i}) \bmod (\mathfrak{a}^r, \deg n+1)$$

Pero $\gamma(X)^{q^i} \equiv 0 \bmod (\mathfrak{a}^{r+i}, \deg n+1)$, luego $a_m \gamma(X)^{q^i m} \equiv 0 \bmod (\mathfrak{a}^{r+i}, \deg n+1)$ $\forall m \geq 1, i \geq 1$

y así $s_i \sigma^i(a_m) \gamma(X)^{q^i m} \equiv 0 \bmod (\mathfrak{a}^{r+i-1}, \deg n+1)$ $\forall i \geq 1$

Esto implica $0 \equiv g(\gamma(X)) + 0 \bmod (\mathfrak{a}^r, \deg n+1)$

Como $g(X)$ es invertible en $A[[X]]$ obtenemos $\gamma(X) \equiv 0 \bmod (\mathfrak{a}^r, \deg n+1)$

Esto implica la afirmación por inducción en n.

Supongo $f(\alpha(x)) \equiv f(\beta(x)) \mod a^r$. Sea

$\delta(x) := f^{-1}(f(\beta(x)) - f(\alpha(x)))$. Por la afirmación tenemos

$\delta(x) \equiv 0 \mod a^r$. Como $f(\delta(x)) + f(\alpha(x)) = f(\beta(x))$ tenemos

$$\beta(x) = f^{-1}(f(\delta(x)) + f(\alpha(x))) = F(\delta(x), \alpha(x))$$
$$\equiv F(0, \alpha(x)) \mod a^r$$
$$\equiv \alpha(x) \mod a^r \quad //$$

Comentarios Finales

(1) Al parecer el Lema de Ec. Funcional es de (Michiel) Hazewinkel ← Matemático holandés (1943, 79 años)
Fue estudiante de Frans Oort y Albert Menalda

Ref: "On formal groups, the functional equation lemma and some of its applications" Astérisque 63, 1979

(2) Motivación original: Si R es anillo sin torsión y $F(X,Y)$. Es gpo formal sobre R, entonces $f(x) = \log_F(x) \in R \otimes \mathbb{Q}[[X]]$.

ya $F(X,Y) = f^{-1}(f(x) + f(Y))$

¿Si partimos con $f(x) \in R \otimes \mathbb{Q}[[X]]$, cuándo $F(X,Y) = f^{-1}(f(x)+f(Y))$ está en $R[[X,Y]]$? Esta es una cuestión de integralidad.

Ejemplo trivial: Si $f \in R[[X]]$, $f(x) \equiv uX + \cdots$, $u \in A^\times$ entonces $F(X,Y) = f^{-1}(f(x) + f(Y)) \in R[[X,Y]]$. Este es el caso trivial de la ec. funcional con $a = A = K$, $\sigma = id$, $s_i = 0 \ \forall i$.
$(f_a = g \in A[[X]]^\times)$