El teorema de Serre-Tate.

23 de Enero - 27 de Enero de 2012

Sara Arias de Reyna
26è Seminari de Teoria de Nombres de Barcelona

0.1 Introducción

En este capítulo introduciremos el anillo de vectores de Witt, siguiendo la excelente exposición del Capítulo II de [6]. Esta exposición no pretende ser completa, y en muchos casos no se explicitarán los detalles de las demostraciones (que, por otra parte, están desarrollados en [6]). A continuación introduciremos los esquemas en grupos finitos de Witt, para concluir enunciando el Teorema de Serre–Tate del levantamiento canónico al anillo de vectores de Witt de una variedad abeliana ordinaria definida sobre un cuerpo finito. Las referencias principales sobre este resultado son [5] y [1].

0.2 Vectores de Witt

Sea A un anillo de valoración discreta completo, de característica 0. Fijemos un uniformizante $\pi \in A$, y denotemos por k al cuerpo residual de A. Supongamos que k es un cuerpo de característica $p > 0$. Consideremos la aplicación $\mathrm{proj} : A \to k$. Escojamos una aplicación $f : k \to A$ (no necesariamente un homomorfismo) tal que $\mathrm{proj} \circ f = \mathrm{id}_k$.

0.2.1 Proposición. *Cada elemento $a \in A$ se escribe de forma única como una serie de potencias (convergente)*

$$\sum_{n=0}^{\infty} f(\lambda_i)\pi^i, \tag{0.2.1}$$

donde $\{\lambda_i\}_{i\in\mathbb{Z}_{\geq 0}}$ es una familia de elementos de k. Recíprocamente, toda serie de la forma (0.2.1) *converge a un elemento de A.*

Demostración. Sea $a \in A$. Notemos que

$$\begin{aligned}\mathrm{proj}(a - f(\mathrm{proj}(a))) &= \mathrm{proj}(a) - (\mathrm{proj} \circ f)(\mathrm{proj}(a)) \\ &= \mathrm{proj}(a) - \mathrm{proj}(a) = 0,\end{aligned}$$

por tanto $a - f(\mathrm{proj}(a))) \in (\pi)$, digamos $a = f(\mathrm{proj}(a))) + \pi a_1$ para cierto $a_1 \in A$. Podemos volver a aplicar este proceso a a_1, y escribir

$a_1 = f(\mathrm{proj}(a_1))) + \pi a_2$ para cierto $a_2 \in A$. Reiterando este proceso, obtenemos una sucesión de elementos $A_n := \sum_{i=0}^{n} f(\mathrm{proj}(a_i))\pi^i$ tal que $a - A_n \in (\pi)^{n+1}$. Esta sucesión converge a a, dando lugar a la expresión (0.2.1), donde $\lambda_i = \mathrm{proj}(a_i)$. La unicidad de la familia $\{\lambda_i\}_{i\in\mathbb{Z}_{\geq 0}}$ puede comprobarse fácilmente por inducción en i. La última afirmación del enunciado de la proposición es una consecuencia directa de la completitud de A. □

De este modo, cada elección de una aplicación $f : k \to A$ tal que $\mathrm{proj} \circ f = \mathrm{id}_k$ da lugar a una identificación $A \sim k^{\mathbb{Z}_{\geq 0}}$, donde a cada elemento a se le asocia la familia $\{\lambda_i\}_{i\in\mathbb{Z}_{\geq 0}}$ descrita en la Proposición 0.2.1. Naturalmente, la identificación $A \sim k^{\mathbb{Z}_{\geq 0}}$ es una biyección entre conjuntos, pero no tiene en cuenta la estructura algebraica de cada uno de ellos.

Supongamos que el cuerpo k es perfecto. Entre todas las posibles elecciones de $f : k \to A$, hay una que es particularmente adecuada, tal como veremos en la Proposición 0.2.5. Antes de enunciar esta proposición, sin embargo, nos situaremos en un contexto más general.

0.2.2 Definición Sea Λ un anillo de característica p. Diremos que Λ es *perfecto* si el endomorfismo $\phi : x \in \Lambda \mapsto x^p \in \Lambda$ es un isomorfismo.

0.2.3 Definición Diremos que un anillo A es *p-estricto* si se verifican las siguientes condiciones:

- A es completo y Hausdorff respecto de la topología p-ádica.
- El anillo $\Lambda := A/(p)$ tiene característica p y es perfecto.
- El elemento $p \in A$ no es un divisor de cero.

En particular, si A es un anillo de valoración discreta completo tal que su cuerpo residual es un cuerpo finito de característica p, entonces A es p-estricto. Notemos además que la Proposición 0.2.1 continúa siendo válida en este contexto; es decir, se verifica el siguiente resultado.

0.2.4 Proposición. *Sea A un anillo p-estricto y sea $\Lambda := A/(p)$. Sea $f : \Lambda \to A$ una aplicación tal que* $\mathrm{proj} \circ f = \mathrm{id}_\Lambda$, *donde* proj :

$A \to A/(p) = \Lambda$ es la proyección natural. Cada elemento $a \in A$ se escribe de forma única como una serie de potencias (convergente)

$$\sum_{n=0}^{\infty} f(\lambda_i)p^i, \tag{0.2.2}$$

donde $\{\lambda_i\}_{i\in\mathbb{Z}_{\geq 0}}$ es una familia de elementos de Λ. Recíprocamente, toda serie de la forma (0.2.2) *converge a un elemento de A.*

Mediante la Proposición 0.2.4, cada elección de una sección $f : \Lambda \to A$ proporciona una biyección $A \sim \Lambda^{\mathbb{Z}_{\geq 0}}$.

0.2.5 Proposición. *Sea A un anillo p-estricto, $\Lambda = A/(p)$.*

(1) Existe una única aplicación $f : \Lambda \to A$ tal que $\mathrm{proj} \circ f = \mathrm{id}_\Lambda$ y, para todo $\lambda \in \Lambda$, $f(\lambda^p) = f(\lambda)^p$.

(2) Sea $f : \Lambda \to A$ la aplicación de (1). Se verifican:

- *Para todo $\alpha, \beta \in \Lambda$, $f(\alpha\beta) = f(\alpha)f(\beta)$.*
- *Sea $a \in A$. Son equivalentes:*
  - *$a \in f(\Lambda)$*
  - *Para todo $n \in \mathbb{N}$, existe $b_n \in A$ tal que $a = (b_n)^{p^n}$*

0.2.6 Ejemplo. Sea $A = \mathbb{Z}_p$, completo respecto de la topología p-ádica, con cuerpo residual $\mathbb{F}_p$. Sea ζ_{p-1} una raíz primitiva $(p-1)$-ésima de la unidad, y sea $\alpha \in \mathbb{F}_p$ su proyección en $\mathbb{F}_p$. La aplicación $f : \mathbb{F}_p \to \mathbb{Z}_p$ definida por:

$$\begin{cases} 0 \mapsto 0 \\ \alpha^i \mapsto \zeta^i \text{ para todo } i = 1, \ldots, p-1 \end{cases}$$

satisface las condiciones de la Proposición 0.2.5.

Antes de proceder a la demostración, veamos un lema simple que será utilizado en varios puntos de la misma.

0.2.7 Lema. *Sea A un anillo p-estricto. Si $a - b \in (p)$, entonces para todo $n \in \mathbb{N}$, $a^{p^n} - b^{p^n} \in (p)^{n+1}$.*

Demostración. Procederemos por inducción en $n \in \mathbb{Z}_{\geq 0}$; para $n = 0$ es claro. Supongamos que se verifica para un cierto índice n. Entonces tenemos que

$$a^{p^{n+1}} - b^{p^{n+1}} = \underbrace{(a^{p^n} - b^{p^n})}_{\in (p)^{n+1}} \cdot \underbrace{(a^{p^n(p-1)} b^{p^n} + a^{p^n(p-2)} b^{2p^n} + \cdots + a^{p^n} b^{p^n(p-1)})}_{\in (p)},$$

donde en el segundo término hemos usado que $a^i b^j \equiv a^{i+j} \pmod{p}$ para cualesquiera exponentes $i, j \in \mathbb{N}$, luego los p sumandos del término de la derecha son todos congruentes a un mismo valor módulo p. $\square$

Demostración. [Demostración de la Proposición 0.2.5] Sea $\lambda \in \Lambda$. Como Λ es un anillo perfecto, existe un único elemento $\lambda' \in \Lambda$ tal que $(\lambda')^p = \lambda$; lo denotaremos por $\lambda^{\frac{1}{p}}$. De esta forma, podemos considerar la sucesión $\{\lambda^{\frac{1}{p^n}} : n \in \mathbb{N}\} \subset \Lambda$. Para cada $n \in \mathbb{N}$, denotemos por $L_n(\lambda) = \{a \in A : \text{proj}(a) = \lambda^{\frac{1}{p^n}}\}$ y $U_n(\lambda) = \{a^{p^n} : a \in L_n(\lambda)\}$. De esta forma tenemos una sucesión decreciente de conjuntos no vacíos

$$U_0(\lambda) \supset U_1(\lambda) \supset U_2(\lambda) \supset \cdots$$

Para cada $n \in \mathbb{N}$, escojamos $a_n \in U_n(\lambda)$. El Lema 0.2.7 muestra que la sucesión $\{a_n\} \subset A$ es de Cauchy. Puesto que A es completo, tenemos que la sucesión $\{a_n\}_n$ converge a un cierto elemento $a \in A$. Es fácil ver que el límite a sólo depende de λ y no de la sucesión $\{a_n\}_n$ escogida. Definamos pues $f(\lambda) := a$. Veamos que la aplicación f así definida cumple las propiedades enunciadas en (1).

Sea $\lambda \in \Lambda$ un elemento cualquiera, y sea $\{a_n\}_n \in A$ una sucesión que converge a $a = f(\lambda)$ y tal que $a_n \in U_n(\lambda)$ para todo $n \in \mathbb{N}$. Existe un $m \in \mathbb{N}$ tal que, para todo $n \geq m$, $a_n - a \in (p)$. Es decir, $\text{proj}(a_n) = \text{proj}(a)$. Pero como $a_n \in U_n(\lambda)$, la proyección de a_n en $A/(p)$ es precisamente λ, por tanto $\text{proj}(f(\lambda)) = \lambda$.

Sea $\mu = \lambda^p$. Consideremos una sucesión $\{a_n\}_n$ tal que $a_n \in U_n(\lambda)$ para todo $n \in \mathbb{N}$. Para cada n, tenemos que $a_n = b_n^{p^n}$ para un cierto $b_n \in L_n(\lambda)$, es decir, tal que $\text{proj}(b_n) = \lambda^{\frac{1}{p^n}}$. Observemos que

$a_n^p \in U_{n+1}(\mu)$; en efecto, $a_n^p = (b_n)^{p^{n+1}}$ y $\mathrm{proj}(b_n) = \lambda^{\frac{1}{p^n}} = (\lambda^p)^{\frac{1}{p^{n+1}}}$. Por tanto, $f(\mu)$ es el límite de $\{a_n^p\}_n$, es decir, $a^p = f(\lambda^p)$.

Supongamos ahora que tenemos otra aplicación $g : \Lambda \to A$ tal que $\mathrm{proj} \circ g = \mathrm{id}_\Lambda$ y, para todo $\lambda \in \Lambda$, $g(\lambda^p) = g(\lambda)^p$. Entonces, para todo $\lambda \in \Lambda$,

$$\mathrm{proj}(f(\lambda) - g(\lambda)) = (\mathrm{proj} \circ f)(\lambda) - (\mathrm{proj} \circ g)(\lambda) = \lambda - \lambda = 0.$$

Es decir, $f(\lambda) - g(\lambda) \in (p)$. Por tanto se verifica que, para todo $n \in \mathbb{N}$, $f(\lambda)^{p^n} - g(\lambda)^{p^n} \in (p)^{n+1}$ (Lema 0.2.7). Así pues, para todo $\lambda \in \Lambda$, $f(\lambda^{p^n}) - g(\lambda^{p^n}) \in (p)^{n+1}$.

Tomemos ahora un elemento $\mu \in \Lambda$ cualquiera. Como A es Hausdorff para la topología p-ádica, para probar que $f(\mu) = g(\mu)$ basta ver que, para todo $n \in \mathbb{N}$, $f(\mu) - g(\mu) \in (p)^{n+1}$. Sea pues $n \in \mathbb{N}$. Como Λ es perfecto, existe $\lambda \in \Lambda$ tal que $\mu = \lambda^{p^n}$. Así pues $f(\mu) - g(\mu) = f(\lambda^{p^n}) - g(\lambda^{p^n}) \in (p)^{n+1}$, como queríamos probar.

Sea pues $f : \Lambda \to A$ la aplicación de (1). Veamos ahora que se cumple la parte (2) de la proposición. La multiplicatividad de f se sigue directamente de la construcción descrita arriba: sean $\alpha, \beta \in \Lambda$, y $\{a_n\}_n, \{b_n\}_n$ dos sucesiones de elementos de A tales que, para todo $n \in \mathbb{N}$, $a_n \in U_n(\alpha)$ y $b_n \in U_n(\beta)$. Entonces es fácil ver que $a_n b_n \in U_n(\alpha\beta)$, y el límite de la sucesión $\{a_n b_n\}_n$ coincide con el producto de los límites de las sucesiones $\{a_n\}_n$ y $\{b_n\}_n$.

Por último, vamos a describir la imagen de f. Supongamos primero que $a \in \mathrm{Im}(f)$, digamos $a = f(\lambda)$ para cierto $\lambda \in \Lambda$. Sea $b_n = f(\lambda^{\frac{1}{p^n}})$. Entonces $(b_n)^{p^n} = (f(\lambda^{\frac{1}{p^n}}))^{p^n} = f(\lambda) = a$. Recíprocamente, sea $a \in A$ tal que, para todo $n \in \mathbb{N}$, a es una potencia p^n-ésima, digamos $a = b_n^{p^n}$. Sean α y β_n las proyecciones de a y b_n en $A/(p)$. Tenemos entonces que $\alpha = \beta_n^{p^n}$, por tanto $f(\alpha) = f(\beta_n^{p^n}) = f(\beta_n)^{p^n}$. Como $f(\beta_n) - b_n \in (p)$, tenemos por el Lema 0.2.7 que $f(\beta_n)^{p^n} - b_n^{p^n} \in (p)^{n+1}$, es decir, $f(\alpha) - a \in (p)^{n+1}$. Como A es Hausdorff para la topología p-ádica, podemos concluir que $f(\alpha) = a$, y por tanto $a \in \mathrm{Im}(f)$. □

0.2.8 Definición Sea A un anillo p-estricto con anillo residual Λ. La aplicación $f : \Lambda \to A$ descrita en la Proposición 0.2.5 se denomina *sistema de representantes multiplicativo* o *de Teichmüller*.

Sean $\mathbf{X} := X_0, X_1, \ldots, X_n, \ldots$ e $\mathbf{Y} := Y_0, Y_1, \ldots, Y_n, \ldots$ dos familias de indeterminadas. Consideremos el anillo

$$S := \mathbb{Z}[\{X_i^{\frac{1}{p^n}} : i \in \mathbb{Z}_{\geq 0}, n \in \mathbb{N}\} \cup \{Y_i^{\frac{1}{p^n}} : i \in \mathbb{Z}_{\geq 0}, n \in \mathbb{N}\}].$$

S no es completo respecto de la topología p-ádica; consideremos su completado $\hat{S}$. El anillo residual $\hat{S}/(p)$ coincide con

$$\Lambda := \mathbb{F}_p[\{X_i^{\frac{1}{p^n}} : i \in \mathbb{Z}_{\geq 0}, n \in \mathbb{N}\} \cup \{Y_i^{\frac{1}{p^n}} : i \in \mathbb{Z}_{\geq 0}, n \in \mathbb{N}\}].$$

Se comprueba fácilmente que $\hat{S}$ es un anillo p-estricto. Podemos por tanto consider su sistema de representantes multiplicativo

$$f : \Lambda \to \hat{S}.$$

Consideremos los elementos $x = \sum_{i=0}^{\infty} X_i p^i$, $y = \sum_{i=0}^{\infty} Y_i p^i$.

0.2.9 Lema. *Existen unos únicos $Q_i^+, Q_i^\times \in \Lambda$ tales que*

$$\begin{cases} x + y = \sum_{i=0}^{\infty} f(Q_i^+) p^i \\ x \cdot y = \sum_{i=0}^{\infty} f(Q_i^\times) p^i \end{cases}$$

Demostración. El resultado es un corolario de la Proposición 0.2.4, aplicada al anillo $A = \hat{S}$ y al sistema de representantes multiplicativo $f : \Lambda \to \hat{S}$. □

0.2.10 Ejemplo. Veamos cómo calcular explícitamente los polinomios $Q_0^+, Q_1^+, \cdots \in \Lambda$.

Partimos de la igualdad

$$x + y = \sum_{i=0}^{\infty} f(Q_i^+) p^i.$$

Si consideramos la igualdad anterior módulo p, obtenemos

$$f(X_0) + f(Y_0) \equiv f(Q_0^+) \pmod{p}, \tag{0.2.3}$$

por tanto, aplicando proj en ambos lados y teniendo en cuenta que $\mathrm{proj} \circ f = \mathrm{id}$, obtenemos que $Q_0^+ = X_0 + Y_0$.

Consideremos ahora la igualdad módulo p^2; tenemos

$$(f(X_0)+pf(X_1))+(f(Y_0)+pf(Y_1))=f(Q_0^+)+pf(Q_1^+) \quad (0.2.4)$$

La ecuación (0.2.3) nos dice cuánto vale $f(Q_0^+)$ modulo p, pero ahora estamos interesados en su valor módulo p^2. Ahora bien,

$$f(Q_0^+)=f(X_0+Y_0)=f((X_0+Y_0)^{\frac{1}{p}})^p=f(X_0^{\frac{1}{p}}+Y_0^{\frac{1}{p}})^p,$$

donde en la primera igualdad hemos sustituido Q_0^+ por su valor, en la segunda igualdad utilizamos que Λ es perfecto y f commuta con las potencias de p, y en la tercera igualdad utilizamos que la característica de Λ es p.

Por otra parte, tenemos que $(\mathrm{proj}\circ f)(X_0^{\frac{1}{p}}+Y_0^{\frac{1}{p}})=\mathrm{proj}(f(X_0^{\frac{1}{p}})+f(Y_0^{\frac{1}{p}}))$, luego $f(X_0^{\frac{1}{p}}+Y_0^{\frac{1}{p}})\equiv f(X_0^{\frac{1}{p}})+f(Y_0^{\frac{1}{p}}) \pmod p$, y por tanto el Lema 0.2.7 implica que

$$(f(X_0^{\frac{1}{p}}+Y_0^{\frac{1}{p}}))^p\equiv(f(X_0^{\frac{1}{p}})+f(Y_0^{\frac{1}{p}}))^p \pmod{p^2}.$$

Podemos por tanto sustituir $f(Q_0^+)$ por $(f(X_0^{\frac{1}{p}})+f(Y_0^{\frac{1}{p}}))^p$ en la ecuación (0.2.4) y obtenemos

$$(f(X_0)+pf(X_1))+(f(Y_0)+pf(Y_1)))= (f(X_0^{\frac{1}{p}})+f(Y_0^{\frac{1}{p}}))^p+pf(Q_1^+) \pmod{p^2}, \quad (0.2.5)$$

de donde podemos despejar

$$f(Q_1^+)=f(X_1)+f(Y_1)-\sum_{j=1}^{p-1}\binom{p}{j}f(X_0^{\frac{j}{p}})f(Y_0^{\frac{p-j}{p}}) \pmod p,$$

por tanto

$$Q_1^+=X_1+Y_1-\sum_{j=1}^{p-1}\binom{p}{j}X_0^{\frac{j}{p}}Y_0^{\frac{p-j}{p}} \pmod p,$$

De este modo podemos ir obteniendo explícitamente los polinomios Q_i^+.

Sean $X_0' = f(X_0)^{\frac{1}{p}}$, $Y_0' = f(Y_0)^{\frac{1}{p}}$, $X_1' = f(X_1)$ y $Y_1' = f(Y_1)$. Observemos que la ecuación (0.2.5) puede escribirse en función de las variables X_0', Y_0', X_1', Y_1' como

$$((X_0')^p + pX_1') + ((Y_0')^p + pY_1')) = (X_0' + Y_0')^p + pf(Q_1^+) \pmod{p^2},$$

En la Definición 0.2.15 veremos que el polinomio $(X_0')^p + pX_1'$ es el primero de una serie de polinomios que juegan un papel importante en la definición de los vectores de Witt.

En general, podemos obtener expresiones

$$\begin{aligned} Q_i^+ &= \tilde{S}_i(X_0^{p^{-i}}, X_1^{p^{-i+1}}, \dots, X_{i-1}^{p^{-1}}, X_i; Y_0^{p^{-i}}, Y_1^{p^{-i+1}}, \dots, Y_{i-1}^{p^{-1}}, Y_i) \\ Q_i^\times &= \tilde{P}_i(X_0^{p^{-i}}, X_1^{p^{-i+1}}, \dots, X_{i-1}^{p^{-1}}, X_i; Y_0^{p^{-i}}, Y_1^{p^{-i+1}}, \dots, Y_{i-1}^{p^{-1}}, Y_i) \end{aligned} \tag{0.2.6}$$

para los polinomios Q_i^+ y $Q_i^\times$, donde $\tilde{S}_i$, $\tilde{P}_i$ son polinomios con coeficientes en $\mathbb{F}_p$.

Las expresiones (0.2.6) para Q_i^+ y $Q_i^\times$ nos permiten dotar al conjunto $\Lambda^{\mathbb{Z}_{\geq 0}}$ de una estructura de anillo conmutativo del modo siguiente:

0.2.11 Definición Sea Λ un anillo conmutativo perfecto. Definamos las siguientes aplicaciones:

$$\begin{aligned} &\tilde{\oplus} : \Lambda^{\mathbb{N}} \times \Lambda^{\mathbb{N}} \to \Lambda^{\mathbb{N}} \\ &(\alpha_n)_n, (\beta_n)_n \mapsto (Q_n^+(\alpha_0, \alpha_1, \dots; \beta_0, \beta_1, \dots))_n \end{aligned}$$

$$\begin{aligned} &\tilde{\otimes} : \Lambda^{\mathbb{N}} \times \Lambda^{\mathbb{N}} \to \Lambda^{\mathbb{N}} \\ &(\alpha_n)_n, (\beta_n)_n \mapsto (Q_n^\times(\alpha_0, \alpha_1, \dots; \beta_0, \beta_1, \dots))_n \end{aligned}$$

El conjunto $\Lambda^{\mathbb{N}}$, dotado de las operaciones $\tilde{\oplus}$, $\tilde{\otimes}$ es un anillo conmutativo, que denotaremos $\tilde{W}(\Lambda)$.

0.2.12 Nota.

- Notemos que, si A es un anillo p-estricto con anillo residual Λ y $f : \Lambda \to A$ es el sistema de representantes multiplicativo, la biyección $A \sim \tilde{W}(\Lambda)$ dada por $a = \sum_i f(\alpha_i)p^i \mapsto (\alpha_i)_i$ es un isomorfismo de anillos.
- En la Definición 0.2.11 necesitamos la hipótesis Λ perfecto, ya que en las expresiones de Q_i^+ y $Q_i^\times$ aparecen potencias fraccionarias en p (ver (0.2.6)).

Utilizando esta construcción, puede demostrarse el siguiente teorema.

0.2.13 Teorema. *Sea Λ un anillo perfecto de característica p. Existe un único p-anillo estricto con anillo residual Λ.*

Demostración. Véase el Teorema 5 del § 5, Capítulo II de [6].□

En particular, se tiene el siguiente resultado (cf. Teorema 3 del §5, Capítulo II de [6]).

0.2.14 Teorema. *Sea k un cuerpo perfecto de característica p. Existe un único anillo de valoración discreta completo y absolutamente no-ramificado con cuerpo residual k.*

Hemos visto como, dado un anillo p-estricto A con anillo residual Λ, dotando a $\Lambda^{\mathbb{N}}$ de una estructura adecuada, la biyección $\Lambda^{\mathbb{N}} \simeq A$ da lugar a un isomorfismo de anillos. El siguiente objetivo es generalizar la definición de $\tilde{W}(\Lambda)$ a anillos que no sean necesariamente perfectos. Para esto, introducimos los polinomios de Witt.

0.2.15 Definición Sea $\mathbf{X} = (X_0, X_1, X_2, \dots)$ una sucesión de indeterminadas. Los polinomios

$$
\begin{aligned}
W_0(\mathbf{X}) &= X_0 \\
W_1(\mathbf{X}) &= X_0^p + pX_1 \\
W_2(\mathbf{X}) &= X_0^{p^2} + pX_1^p + p^2X_2 \\
&\cdots \\
W_n(\mathbf{X}) &= X_0^{p^n} + pX_1^{p^{n-1}} + p^2X_2^{p^{n-2}} + \cdots + p^{n-1}X_{n-1}^p + p^nX_n \\
&\cdots
\end{aligned}
$$

se denominan *polinomios de Witt.*

0.2.16 Nota. Notemos que, para cada $n \in \mathbb{N}$, podemos despejar X_n en función de $W_0, \dots, W_n$ en $\mathbb{Z}[\frac{1}{p}]$.

$$\begin{aligned} X_0 &= W_0 \\ X_1 &= \frac{1}{p}(W_1 - W_0^p) \\ X_2 &= \frac{1}{p^2}(W_2 - W_0^{p^2} - p(W_1 - pW_0^p)) \\ &\dots \end{aligned}$$

La importancia de estos polinomios radica en la siguiente proposición.

0.2.17 Proposición. *Sea $\Phi(X,Y) \in \mathbb{Z}[X,Y]$. Existe una única sucesión de elementos $\varphi_m(\mathbf{X},\mathbf{Y}) \in \mathbb{Z}[\mathbf{X},\mathbf{Y}]$ tal que, para todo $n \in \mathbb{N}$,*

$$W_n(\varphi_0(\mathbf{X},\mathbf{Y}), \varphi_1(\mathbf{X},\mathbf{Y}), \dots) = \Phi(W_n(\mathbf{X}), W_n(\mathbf{Y})). \tag{0.2.7}$$

Demostración. Ver Teorema 6 del Capítulo II de [6]. Nótese que la existencia y unicidad de elementos $\varphi_m(\mathbf{X},\mathbf{Y}) \in \mathbb{Z}[\frac{1}{p}][\mathbf{X},\mathbf{Y}]$ verificando la ecuación (0.2.7) es fácil de ver, en vista de la Nota 0.2.16; sin embargo, probar que los coeficientes de φ_m son de hecho números enteros es más laborioso. □

0.2.18 Definición Consideremos $\Phi(X,Y) = X+Y \in \mathbb{Z}[X,Y]$ (resp. $\Phi(X,Y) = X \cdot Y \in \mathbb{Z}[X,Y]$). Definimos $S_n := \varphi_n \in \mathbb{Z}[\mathbf{X},\mathbf{Y}]$ (resp. $P_n := \varphi_n \in \mathbb{Z}[\mathbf{X},\mathbf{Y}]$).

0.2.19 Definición Sea A un anillo conmutativo. Definamos las siguientes aplicaciones:

$$\begin{aligned} \oplus : A^{\mathbb{N}} \times A^{\mathbb{N}} &\to A^{\mathbb{N}} \\ (a_n)_n, (b_n)_n &\mapsto (S_n(a_0, a_1, \dots; b_0, b_1, \dots))_n \end{aligned}$$

$$\begin{aligned} \otimes : A^{\mathbb{N}} \times A^{\mathbb{N}} &\to A^{\mathbb{N}} \\ (a_n)_n, (b_n)_n &\mapsto (P_n(a_0, a_1, \dots; b_0, b_1, \dots))_n \end{aligned}$$

El conjunto $A^{\mathbb{N}}$, dotado de las operaciones $\oplus$, $\otimes$ es una anillo conmutativo, que denominaremos *anillo de vectores de Witt con coeficientes en* A y denotaremos $W(A)$.

0.2.20 Lema. *Sea A un anillo conmutativo. La aplicación*

$$\begin{aligned} W_* : W(A) &\to A^{\mathbb{N}} \\ (a_n)_n &\mapsto (W_n(a_0, a_1, \dots))_n \end{aligned}$$

es un homomorfismo de anillos (isom. si p es invertible en A), donde en $A^{\mathbb{N}}$ consideramos la estructura de anillo dada por la suma y el producto coordenada a coordenada.

Demostración. Las relaciones $W_*((a_n)_n \oplus (b_n)_n) = W_*((a_n)_n) + W_*((b_n)_n)$ y $W_*((a_n)_n \otimes (b_n)_n) = W_*((a_n)_n) \cdot W_*((b_n)_n)$ se siguen directamente de la Proposición 0.2.17 y de la definición de $\oplus$ y $\otimes$. Por otra parte, si p es invertible en A, podemos definir la aplicación inversa debido a la Nota 0.2.16. □

Veamos ahora que las definiciones 0.2.11 y 0.2.19 son esencialmente equivalentes cuando el anillo A es perfecto.

0.2.21 Proposición. *Sea A un anillo conmutativo perfecto. La aplicación*

$$\begin{aligned} \Psi : \tilde{W}(A) &\to W(A) \\ (a_0, a_1, a_2, \dots) &\mapsto (a_0, a_1^p, a_2^{p^2}, \dots) \end{aligned}$$

es un isomorfismo de anillos.

Demostración. La demostración puede realizarse por inducción, siguiendo un procedimiento similar al descrito en el Ejemplo 0.2.10. El lector interesado en los detalles de la prueba puede consultar el Teorema 1.5 de [4]. □

0.2.22 Nota. Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$. De la Nota 0.2.16 puede deducirse, por inducción en n, que el polinomio $\varphi_i(X, Y)$ de la Proposición 0.2.17 depende tan sólo de las i primeras variables $X_0, \dots, X_i$, $Y_0, \dots, Y_i$.

Sea $N \in \mathbb{N}$, A un anillo conmutativo. El comentario anterior permite definir las aplicaciones

$$\begin{aligned} &\oplus_N : A^N \times A^N \to A^N \\ &(a_n)_{n=1}^N, (b_n)_{n=1}^N \mapsto (S_n(a_0, \dots, a_n; b_0, b_1, \dots, b_n))_{n=1}^N \\ &\otimes_N : A^N \times A^N \to A^N \\ &(a_n)_{n=1}^N, (b_n)_{n=1}^N \mapsto (P_n(a_0, \dots, a_n; b_0, \dots, b_n))_{n=1}^N \end{aligned} \tag{0.2.8}$$

donde S_n, P_n son los polinomios de la Definición 0.2.18.

$(A^N, \otimes_N, \oplus_N)$ es un anillo conmutativo.

0.2.23 Definición Sea $N \in \mathbb{N}$, A un anillo conmutativo. Se define el *anillo de los vectores de Witt de longitud N* como el conjunto A^N, dotado de las operaciones $\oplus_N$ y $\otimes_N$ definidas por las expresiones (0.2.8).

0.2.24 Nota. Puede comprobarse que

$$W(A) = \varprojlim_N W_N(A).$$

A continuación vamos a definir dos operadores fundamentales sobre vectores de Witt: el Verschiebung (traslación) y el Frobenius. Sin embargo, antes veremos unos lemas auxiliares que nos permitirán estudiar el comportamiento de una aplicación respecto de la estructura de anillo de los vectores de Witt.

Sea $\varphi : A \to B$ una aplicación, y definamos una aplicación entre $W(A)$ y $W(B)$ del modo siguiente:

$$\begin{aligned} &\Phi : W(A) \to W(B) \\ &(a_0, a_1, \dots) \mapsto (\varphi(a_0), \varphi(a_1), \dots). \end{aligned}$$

0.2.25 Lema. *1. Si φ es inyectiva, Φ es inyectiva; si φ es sobreyectiva, Φ es sobreyectiva.*

2. Si φ es un homomorfismo de anillos, Φ es también un homomorfismo de anillos.

Demostración.

1. Supongamos primero que φ es inyectiva, y sean $\mathbf{a} = (a_0, a_1, \dots)$, $\mathbf{d} = (d_0, d_1, \dots) \in W(A)$ tales que $\Phi(\mathbf{a}) = \Phi(\mathbf{d})$. Por definición, esto significa que

$$(\varphi(a_0), \varphi(a_1), \dots) = (\varphi(d_0), \varphi(d_1), \dots).$$

   Como φ es inyectiva, obtenemos que $\mathbf{a} = \mathbf{d}$.

   Supongamos ahora que φ es sobreyectiva, y fijemos un elemento $\mathbf{b} = (b_0, b_1, \dots) \in W(B)$. Para cada $i = 0, 1, \dots$, escojamos a_i tal que $\varphi(a_i) = b_i$, y definamos $\mathbf{a} = (a_0, a_1, \dots) \in W(A)$. Este elemento satisface que $\Phi(\mathbf{a}) = \mathbf{b}$.

2. Sean $\mathbf{a} = (a_0, a_1, \dots), \mathbf{d} = (d_0, d_1, \dots) \in W(A)$. Entonces

$$\begin{aligned}\Phi(\oplus(\mathbf{a}, \mathbf{d})) &= \Phi(S_0(a_0; d_0), S_1(a_0, a_1; d_0, d_1), \dots) \\ &= (\varphi(S_0(a_0; d_0)), \varphi(S_1(a_0, a_1; d_0, d_1)), \dots)\end{aligned}$$

   Como φ es un homomorfismo, la expresión anterior coincide con:

$$\begin{aligned}&(S_0(\varphi(a_0); \varphi(d_0)), S_1(\varphi(a_0), \varphi(a_1); \varphi(d_0), \varphi(d_1)), \dots) \\ &\qquad = \oplus(\Phi(\mathbf{a}), \Phi(\mathbf{d})).\end{aligned}$$

   Análogamente se prueba que $\Phi(\otimes(\mathbf{a}, \mathbf{d})) = \otimes(\Phi(\mathbf{a}), \Phi(\mathbf{d}))$.

□

0.2.26 Definición Sea A un anillo conmutativo de característica p. Definimos el operador *Frobenius*

$$\begin{aligned}F : W(A) &\to W(A) \\ (a_0, a_1, a_2, \dots) &\mapsto (a_0^p, a_1^p, a_2^p, \dots)\end{aligned}$$

0.2.27 Nota. Sea A como en la definición 0.2.26, y consideremos la aplicación $\varphi : A \to A$ definida por $a \mapsto a^p$. Como A tiene característica p, φ es un homomorfismo de anillos, y por el Lema 0.2.25 deducimos que el operador F es un homomorfismo de anillos.

0.2.28 Definición Sea A un anillo conmutativo. Definimos el operador *Verschiebung*

$$V : W(A) \to W(A)$$
$$(a_0, a_1, a_2, \dots) \mapsto (0, a_0, a_1, \dots)$$

0.2.29 Nota. En este caso no podemos estudiar la relación entre V y la estructura de anillo de $W(A)$ mediante el Lema 0.2.25. Sin embargo, recordemos que tenemos una aplicación $W_* : W(A) \to A^{\mathbb{N}}$ (cf. Lema 0.2.20). Podemos dar una aplicación que cierre el diagrama?

$$\begin{array}{ccc} W(A) & \xrightarrow{V} & W(A) \\ {\scriptstyle W_*}\downarrow & & \downarrow{\scriptstyle W_*} \\ A^{\mathbb{N}} & \xrightarrow{?} & A^{\mathbb{N}} \end{array}$$

Sea $(w_0, w_1, \dots) \in A^{\mathbb{N}}$, y supongamos que existe $(a_0, \dots, a_n) \in W(A)$ tal que $W_*(a_0, a_1, \dots) = (w_0, w_1, \dots)$ (si p no es invertible en A, puede que no exista una tal tupla). Tenemos entonces que

$$W_* \circ V(a_0, a_1, \dots) = W_*(0, a_0, a_1, \dots) = (0, pw_0, pw_1, \dots).$$

Por tanto una aplicación que cierra el diagrama es $(w_0, w_1, \dots) \mapsto (0, pw_0, pw_1, \dots)$. En particular, podemos observar que es una aplicación aditiva (pero no multiplicativa). En el caso en que p sea invertible en A, tenemos que W_* es un isomorfismo, y por tanto $V : W(A) \to W(A)$ es un operador aditivo (¡pero no es multiplicativo!)

0.2.30 Lema. *Sean $A \subset B$ anillos, y sea $\Psi : W(B) \to W(B)$ una aplicación aditiva. Entonces la aplicación $W(A) \to W(A)$ inducida por Ψ es también aditiva.*

Demostración. Como la inclusión $A \to B$ es inyectiva, por el Lema 0.2.25 obtenemos que la inclusión natural $A^{\mathbb{N}} \subset B^{\mathbb{N}}$ es de hecho una inclusión de anillos $W(A) \to W(B)$, y podemos considerar la restricción de Ψ a $W(A)$. Como Ψ es aditiva, esta restricción también lo es. □

0.2.31 Lema. *Sean A, B anillos, $\varphi : A \to B$ un homomorfismo sobreyectivo, $\Phi : W(A) \to W(B)$ el morfismo (sobreyectivo) inducido por φ. Sean Ψ_A, Ψ_B dos aplicaciones que hacen el siguiente diagrama conmutativo:*

$$\begin{array}{ccc} W(A) & \xrightarrow{\Psi_A} & W(A) \\ {\scriptstyle\Phi}\downarrow & & \downarrow{\scriptstyle\Phi} \\ W(B) & \xrightarrow{\Psi_B} & W(B) \end{array}$$

Supongamos que $\Psi_A : W(A) \to W(A)$ una aplicación aditiva. Entonces la aplicación $\Psi_B : W(B) \to W(B)$ es también aditiva.

Demostración. Dados $\mathbf{b} = (b_0, b_1, \dots), \mathbf{d} = (d_0, d_1, \dots) \in W(B)$, existen $\mathbf{a} = (a_0, a_1, \dots), \mathbf{c} = (c_0, c_1, \dots) \in W(A)$ tal que $\Phi(\mathbf{a}) = \mathbf{b}$ y $\Phi(\mathbf{d}) = \mathbf{c}$. Tenemos entonces que

$$\begin{aligned} &\Psi_B(\oplus(\mathbf{b}, \mathbf{c})) = \Psi_B(\oplus(\Phi(\mathbf{a}), \Phi(\mathbf{d})) = \Psi_B(\Phi(\oplus(\mathbf{a}, \mathbf{d}))) \\ &= \Phi(\Psi_A(\oplus(\mathbf{a}, \mathbf{d}))) = \Phi(\oplus(\Psi_A(\mathbf{a}), \Psi(\mathbf{d}))) = \oplus(\Phi(\Psi_A(\mathbf{a})), \Phi(\Psi_A(\mathbf{d}))) \\ &= \oplus(\Psi_B(\Phi(\mathbf{a})), \Psi_B(\Phi(\mathbf{d}))) = \oplus(\Psi_B(\mathbf{b}), \Psi_B(\mathbf{c})). \end{aligned}$$

□

0.2.32 Lema. *Sea A un anillo conmutativo. El operador*

$$V : W(A) \to W(A)$$

es aditivo.

Demostración. Sea $\{T_\alpha\}_\alpha$ una familia de variables. Consideremos primero el anillo $A = \mathbb{Z}[\frac{1}{p}][\{T_\alpha\}_\alpha]$. Como p es invertible en este anillo, la Nota 0.2.29 muestra que el operador Verschiebung $V : W(A) \to W(A)$ es aditivo. Como $\mathbb{Z}[\{T_\alpha\}_\alpha]$ es un subanillo de A, el Lema 0.2.30 muestra que el operador Verschiebung $V : W(\mathbb{Z}[\{T_\alpha\}_\alpha]) \to W(\mathbb{Z}[\{T_\alpha\}_\alpha])$ es también aditivo. Finalmente, el Lema 0.2.31 muestra que, si A es un cociente del anillo $\mathbb{Z}[\{T_\alpha\}_\alpha]$, entonces el operador $V : W(A) \to W(A)$ es también aditivo. Pero cualquier anillo puede escribirse como cociente de $\mathbb{Z}[\{T_\alpha\}_\alpha]$; por tanto el lema es cierto para cualquier anillo A. □

Sea $N \in \mathbb{N}$, y denotemos por V^N la composición de V consigo mismo N veces. Observemos que se tiene la sucesión exacta

$$0 \longrightarrow W(A) \xrightarrow{V^N} W(A) \longrightarrow W_N(A) \longrightarrow 0 \tag{0.2.9}$$

El operador Verschiebung no lleva $W_r(A)$ en $W_r(A)$. Sin embargo, podemos definir $V : W_r(A) \to W_{r+1}(A)$. Podemos restringir la sucesión exacta (0.2.9) a $W_r(A)$ y obtenemos

$$0 \longrightarrow W_r(A) \xrightarrow{V^N} W_{r+N}(A) \longrightarrow W_N(A) \longrightarrow 0. \tag{0.2.10}$$

0.2.33 Nota. Sea A un anillo de característica p. Tenemos entonces definidos los dos operadores $V : W(A) \to W(A)$ y $F : W(A) \to W(A)$. Directamente a partir de su definición podemos ver que conmutan entre sí, es decir, $F \circ V = V \circ F$. Podemos calcular esta composición?

Supongamos primero que A es un anillo perfecto. Tenemos entonces el anillo $\tilde{W}(A)$, dotado de las operaciones $\tilde{\oplus}, \tilde{\otimes}$ (véase la Definición 0.2.11), y el isomorfismo $\Psi : \tilde{W}(A) \to W(A)$ (Proposición 0.2.21). Vamos a estudiar la cuestión primero en $\tilde{W}(A)$. Sean $\tilde{V}$ y $\tilde{F}$ las aplicaciones tales que los diagramas siguientes son conmutativos:

$$\begin{array}{ccc} \tilde{W}(A) & \xrightarrow{\tilde{V}} & \tilde{W}(A) \\ \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \Psi} \\ W(A) & \xrightarrow{V} & W(A) \end{array} \qquad \begin{array}{ccc} \tilde{W}(A) & \xrightarrow{\tilde{F}} & \tilde{W}(A) \\ \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \Psi} \\ W(A) & \xrightarrow{F} & W(A) \end{array}$$

Se comprueba fácilmente que

$$\tilde{V}(a_0, a_1, a_2, \dots) = (0, a_0^{-p}, a_1^{-p}, \dots)$$
$$\tilde{F}(a_0, a_1, a_2, \dots) = (a_0^p, a_1^p, a_2^p, \dots).$$

Por tanto $(\tilde{F} \circ \tilde{V})(a_0, a_1, a_2, \dots) = (0, a_0, a_1, \dots)$. Podemos escribir esta aplicación de otra forma. Sea $f : A \to \tilde{W}(A)$ un sistema de representantes de Teichmüller. Tenemos entonces que $(a_0, a_1, \dots) \in$

$\tilde{W}(A)$ puede escribirse como $\sum_{i=0}^{\infty} f(a_i)p^i$. Por tanto,

$$(\tilde{F} \circ \tilde{V})(a_0, a_1, a_2, \dots) = (\tilde{F} \circ \tilde{V}) \left(\sum_{i=0}^{\infty} f(a_i)p^i \right)$$
$$= \sum_{i=0}^{\infty} f(a_i)p^{i+1} = p \cdot \left(\sum_{i=0}^{\infty} f(a_i)p^i \right).$$

Por tanto, $\tilde{F} \circ \tilde{V} = \tilde{V} \circ \tilde{F} = p \cdot \mathrm{Id}$.

0.2.34 Proposición. *Sea A un anillo conmutativo de característica p. $F \circ V = V \circ F : W(A) \to W(A)$ es la multiplicación por p.*

Demostración. Todo anillo conmutativo de característica p es un subanillo de un anillo perfecto de característica p; por tanto, basta probar la proposición cuando A es perfecto. En la Nota 0.2.33 hemos probado que $\tilde{F} \circ \tilde{V} = p \cdot \mathrm{Id}$. Mediante el isomorfismo Ψ podemos transladar esta igualdad a $W(A)$. □

0.3 Esquemas en grupos de Witt

Comenzamos esta sección recordando algunos aspectos de los esquemas en grupos. El lector que no esté familiarizado con este tema puede consultar el Capítulo 3, §11 de [2].

Fijemos $X \to S$ un esquema sobre S. Sea $T \to S$ otro esquema sobre S. Se define el *conjunto de puntos de X con valores en T*, $X(T)$, como el conjunto de morfismos de S-esquemas $\{t : T \to X\}$.

Utilizaremos a menudo el siguiente principio:

Son equivalentes:

- Dar a X una estructura de S-esquema en grupos.
- Para todo esquema afín $T \to S$, dar a $X(T)$ una estructura de grupo, "funtorialmente en T".

De forma más precisa, la expresión "funtorialmente en T" significa que, dados dos S esquemas T_1, T_2 y un morfismo de S-esquemas $t : T_1 \to T_2$, éste induce de forma natural un morfismo de grupos $X(T_2) \to X(T_1)$.

En lo sucesivo, k denotará un cuerpo perfecto de característica p. Sea $N \in \mathbb{N}$, y consideremos el esquema

$$\mathbb{A}_N := \text{Spec } k[X_1, ..., X_N].$$

Vamos a dotar a $\mathbb{A}_N$ de una estructura de esquema en grupos sobre k. Para esto, consideremos un esquema afín $T \to k$. Tenemos entonces que

$$\begin{aligned}(\mathbb{A}_N)(T) &= \{T \to \mathbb{A}_N \text{ morfismo}\} \\ &\simeq \{k[X_1, \ldots, X_N] \to \Gamma(T, \mathcal{O}_T) \text{ morfismo}\} \\ &\simeq \{(t_1, \ldots, t_N) \in \Gamma(T, \mathcal{O}_T)^N\}\end{aligned}$$

Luego es suficiente dotar a $\Gamma(T, \mathcal{O}_T)^N$ de estructura de grupo. Para cada T, $\Gamma(T, \mathcal{O}_T)$ es un anillo; en particular, es un grupo abeliano con la suma, luego $\Gamma(T, \mathcal{O}_T)^N$ tiene de forma natural la estructura de grupo dada por la suma coordenada a coordenada. Sin embargo, a nosotros nos interesa dotar a $\Gamma(T, \mathcal{O}_T)^N$ de otra estructura de grupo; concretamente,

$$\begin{aligned}\oplus_N : \Gamma(T, \mathcal{O}_T)^N \times \Gamma(T, \mathcal{O}_T)^N &\to \Gamma(T, \mathcal{O}_T)^N \\ (a_n)_{n=1}^N, (b_n)_{n=1}^N &\mapsto (S_n(a_0, \ldots, a_n; b_0, \ldots, b_n))_{n=0}^N\end{aligned}$$

0.3.1 Definición Sea $N \in \mathbb{N}$. Definimos el *esquema en grupos finitos de Witt* como

$$\mathcal{W}_N := (\mathbb{A}^N, \oplus_N).$$

A continuación, veremos que el operador $F : W_N(A) \to W_N(A)$ y el operador $V : W_N(A) \to W_{N+1}(A)$ (cf. Definiciones 0.2.26 y 0.2.28) inducen morfismos de esquemas en grupos

$$\begin{aligned}F &: \mathcal{W}_N \to \mathcal{W}_N \\ V &: \mathcal{W}_N \to \mathcal{W}_{N+1}.\end{aligned}$$

Recordemos que, si $\mathcal{A}$ y $\mathcal{B}$ son dos esquemas en grupos afines, definir un morfismo $\varphi : \mathcal{A} \to \mathcal{B}$ de esquemas en grupos es equivalente a dar, para cada esquema en grupos afín T, un morfismo de grupos $\mathcal{A}(T) \to \mathcal{B}(T)$, "funtorialmente en T". Recordemos, además, que $\mathcal{W}_N(T) \sim \{(t_0, \ldots, t_N)\} \in \Gamma(T, \mathcal{O}(T))^N$.

0.3.2 Definición Sea T un esquema en grupos afín.

- Definimos el morfismos de esquemas en grupos $F : \mathcal{W}_N \to \mathcal{W}_N$ mediante la regla $F : (t_0, t_1, \ldots, t_N) \mapsto (t_0^p, t_1^p, \ldots, t_N^p)$.
- Definimos el morfismos de esquemas en grupos $V : \mathcal{W}_N \to \mathcal{W}_{N+1}$ mediante la regla $V : (t_0, t_1, \ldots, t_N) \mapsto (0, t_0, t_1, \ldots, t_N)$.

A continuación recogemos una serie de resultados esenciales sobre esquemas en grupos finitos de Witt. Para un estudio con más profundidad, el lector puede consultar [3].

0.3.3 Proposición. *Sean $N, r \in \mathbb{N}$. Se tiene una sucesión exacta*

$$0 \longrightarrow \mathcal{W}_r \xrightarrow{V^N} \mathcal{W}_{N+r} \longrightarrow \mathcal{W}_N \longrightarrow 0.$$

Demostración. Véase § 22, Lección 9 de [3]. □

0.3.4 Nota. Consideremos el esquema en grupos afín definido como $\mathbb{A}^1_k := \text{Spec } k[X_1]$, con la suma inducida por la suma habitual del anillo $k[X_1]$. Recordemos que $S_0(X, Y) = X + Y$. Por tanto, los esquemas en grupos $\mathbb{A}^1_k$ y $\mathcal{W}_1$ coinciden. La existencia de la sucesión exacta de la Proposición 0.3.3 prueba que todo $\mathcal{W}_N$ es una "extensión múltiple" de $\mathbb{A}^1_k$.

0.3.5 Definición Sean $N, m \in \mathbb{N}$. Definimos

$$\mathcal{W}_N^m := \ker(F^m : \mathcal{W}_N \to \mathcal{W}_N),$$

donde F es la composición del operador Frobenius consigo mismo m veces.

La siguiente proposición ilustra la importancia de los esquemas en grupos finitos de Witt.

0.3.6 Proposición. *Para cada esquema en grupos finito X de tipo local-local existen $N, m, r \in \mathbb{N}$ tales que $X \hookrightarrow (\mathcal{W}_N^m)^r$.*

Demostración. Véase la Proposición 22.5 de la Lección 9 de [3]. □

Finalmente, comentamos el comportamiento de los esquemas en grupos finitos de Witt respecto a la dualidad de Cartier.

0.3.7 Proposición. *Existe un pairing no degenerado*

$$\mathcal{W}_N^m \times \mathcal{W}_m^N \to \mathbb{G}_m(k).$$

Demostración. Véase el Teorema 25.3 de la Lección 11 de [3]. La construcción del pairing utiliza la exponencial de Artin-Hasse. □

0.3.8 Corolario. *El pairing de la Proposición 0.3.7 induce un isomorfismo*

$$\mathcal{W}_N^m \simeq (\mathcal{W}_m^N)^*,$$

donde * denota el dual de Cartier.

0.4 El teorema de Serre-Tate

En las secciones anteriores hemos reunido el material necesario para enunciar el Teorema de Serre-Tate del levantamiento canónico al anillo de vectores de Witt de una variedad abeliana ordinaria definida sobre un cuerpo finito. Comenzamos fijando la notación.

En esta sección, R denota un anillo local de característica 0, k su cuerpo residual, que supondremos de característica $p > 0$.

0.4.1 Definición Sea X_0/k un esquema en grupos. Un *levantamiento* de X_0 a R es un esquema en grupos X/R, junto con un isomorfismo $X \otimes_R k \to X_0$ de esquemas en grupos sobre k.

0.4.2 Definición Sea A_0 una variedad abeliana, y denotemos por $A_0(p)$ el grupo p-divisible asociado.

- Un *levantamiento de la variedad abeliana* A_0 a R es un esquema abeliano A/R, levantamiento de A_0 a R.
- Un *levantamiento del grupo p-divisible* $A_0(p)$ a R es una sucesión de esquemas en grupos A_{p^n} a R, planos, levantamientos de $A_0[p^n]$, y una familia de inyecciones $A_{p^n} \to A_{p^{n+1}}$ que levantan las inclusiones canónicas $A_0[p^n] \to A_0[p^{n+1}]$.

0.4.3 Ejemplo. Sea $n \in \mathbb{N}$. Supongamos que el cuerpo k es perfecto, y sea $R = W(k)$.

1. Consideremos el esquema

$$\mu_{p^n,k} := \text{Spec } k[T]/(T^p - 1).$$

Definimos una estructura de esquema en grupos del modo siguiente: sea T un esquema afín sobre Spec k, digamos $T =$ Spec S. Observemos que

$$\begin{aligned}\mu_{p^n,k}(T) = \{f : T \to \mu_{p^n,k} \text{ morfismo}\} = \\ \{f : k[T]/(T^p - 1) \to S \text{ morfismo de anillos }\} \\ \simeq \{s \in S : s^p - 1 = 0\}.\end{aligned}$$

Es decir, los puntos de μ_{p^n} con valores en T se corresponden con las raíces p-ésimas de la unidad contenidas en S. Este conjunto es de forma natural un grupo, con el producto.

Cómo podemos levantar este esquema en grupos a R? Consideremos el esquema

$$\mu_{p^n,R} := \text{Spec } R[T]/(T^p - 1).$$

Se comprueba que el morfismo

$$R[T]/(T^p - 1) \times_R k \to k[T]/(T^p - 1)$$

es un isomorfismo, que induce un morfismo de esquemas en grupos sobre k

$$\text{Spec } R[T]/(T^p - 1) \times_{\text{Spec } R} \text{Spec } k \to k[T]/(T^p - 1).$$

2. Consideremos ahora el esquema en grupos

$$\alpha_{p^n,k} := \text{Spec } k[T]/(T^p),$$

donde la operación de grupo viene dada del modo siguiente: sea T un esquema afín sobre Spec k, digamos $T = \text{Spec } S$. Tenemos que

$$\begin{aligned}\alpha_{p^n,k}(T) = \{f : T \to \alpha_{p^n,k} \text{ morfismo}\} = \\ \{f : k[T]/(T^p) \to S \text{ morfismo de anillos }\} \\ \simeq \{s \in S : s^p = 0\}.\end{aligned}$$

Dotamos a este conjunto de estructura de grupo con la suma.

Observemos que, como esquema, $\alpha_{p^n,k} = \text{Spec } k[T]/(T^p) \simeq \text{Spec } k[T]/(T^p - 1) = \mu_{p^n,k}$. Sin embargo, las estructuras de grupo son diferentes. Puede probarse que, como esquemas en grupos, $\alpha_{p^n,k}$ y $\mu_{p^n,k}$ no son isomorfos (cf. §5 of [3]).

Intentemos levantar este esquema en grupos a R. Análogamente al caso anterior, el morfismo $R[T]/(T^p) \times_R k \to k[T]/(T^p)$ es un isomorfismo, que induce un morfismo de esquemas sobre k,

$$\text{Spec } R[T]/(T^p) \times_{\text{Spec } R} \text{Spec } k \to k[T]/(T^p).$$

Sin embargo, no podemos dotar a Spec $R[T]/(T^p)$ de esquema en grupos utilizando la suma, ya que, como R tiene característica cero, el conjunto de puntos

$$(R[T]/(T^p))\,(T) \simeq \{s \in S : s^p = 0\}$$

no es un grupo con la suma (pues si $a, b \in S$ satisfacen que $a^p = 0$ y $b^p = 0$, puede ocurrir que $(a+b)^p \neq 0$, es decir, puede ocurrir que el conjunto $\alpha_{p^n,k}(T)$ no sea cerrado para la suma).

Enunciamos a continuación un resultado (cf. Teorema 4, §5 de [5]; Lema (3.2), capítulo V de [1]).

0.4.4 Teorema. (Serre-Tate) *Supongamos que el anillo R es Artiniano. Existe una equivalencia de categorías entre:*

- *Esquemas abelianos A sobre R.*
- *Pares $(A_0, \{\tilde{A}_{p^n}\}_n)$ de esquemas abelianos A_0 sobre k y levantamientos de $A_0(p)$ a R.*

En otras palabras, un esquema abeliano sobre R queda unívocamente definido por su grupo p-divisible y su proyección sobre k. Veremos a continuación cómo obtener el Teorema del levantamiento canónico de Serre y Tate a partir de este resultado.

En lo sucesivo, k denotará un cuerpo perfecto de característica p. Sea A_0/k un esquema abeliano. Tenemos entonces la siguiente descomposición del esquema en grupos correspondiente a los puntos de p^n-torsión

$$A_0[p^n] \simeq G_{r,r} \times G_{r,l} \times G_{l,r} \times G_{l,l},$$

donde $G_{r,r}$ es un esquema en grupos reducido cuyo dual es reducido, $G_{r,l}$ es un esquema en grupos reducido cuyo dual es local, $G_{l,r}$ es un esquema en grupos local cuyo dual es reducido, y $G_{l,l}$ es un esquema en grupos local cuyo dual es local (cf. capítulo III, §14, p. 136 de [2]).

Ahora bien, podemos especificar más la estructura de algunos de los factores.

0.4.5 Lema. *Sea k un cuerpo de característica $p > 0$ y A_0/k una variedad abeliana. Se verifican:*

- *Para todo $n \in \mathbb{N}$, $A_0[p^n]$ no tiene parte reducida-reducida.*
- *Existe un número natural s tal que, para todo $n \in \mathbb{N}$,*

$$\begin{cases} G_{r,l} \simeq (\mathbb{Z}/n\mathbb{Z})^s \\ G_{l,r} \simeq \mu_{p^n}^s, \end{cases}$$

  donde $\mathbb{Z}/n\mathbb{Z}$ denota el esquema en grupos constantemente igual al grupo cíclico de n elementos.

Demostración. Véase el capítulo III, §15, p. 146 de [2]. □

El número s que aparece en el lema 0.4.5 se denomina el p-rango de A_0/k. Ahora bien, hemos visto en el Ejemplo 0.4.3 que μ_{p^n} admite un levantamiento canónico. Más aún, puede comprobarse que el dual de Cartier de $(\mathbb{Z}/n\mathbb{Z})$ es μ_{p^n} (cf. Ejemplo (2) del §14, Capítulo III, p. 136 de [2]), luego un levantamiento canónico de $(\mathbb{Z}/n\mathbb{Z})$ es el dual de Cartier del levantamiento canónico de μ_{p^n}. En definitiva, el único obstáculo para obtener un levantamiento canónico de $A_0[p^n]$ es la parte local-local.

0.4.6 Definición Sea k un cuerpo de característica $p > 0$, y sea A_0/k una variedad abeliana. Diremos que es *ordinaria* si para todo número natural n (equivalentemente, para un n), el esquema en grupos $A_0[p^n]$ no tiene parte local-local.

Por tanto, si A_0/k es una variedad abeliana ordinaria, tenemos que $A_0[p^n]$ tiene un levantamiento canónico a cualquier anillo local Artiniano R cuyo cuerpo residual sea k. Podemos reinterpretar el Teorema 0.4.4 en el caso ordinario como sigue: un esquema abeliano A/R queda unívocamente definido por su reducción $A \otimes_R k$ sobre k. El teorema del levantamiento canónico de Serre-Tate puede enunciarse como sigue:

0.4.7 Teorema. (Serre-Tate) *Sea k un cuerpo perfecto de característica $p > 0$ y A_0/k una variedad abeliana ordinaria. Existe un levantamiento canónico de A_0 a una variedad abeliana $A/W(k)$.*

Demostración. Sea $s \in \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$,

$$A_0[p^n] \simeq (\mathbb{Z}/n\mathbb{Z})^s \times \mu_{p^n}^s$$

Sea $N \in \mathbb{N}$. Consideremos el esquema en grupos sobre el anillo Artiniano $R := W(k)/(p^N)$ definido como

$$\tilde{A}_{p^n} := (\mu_{p^n}(R)^s)^* \times \mu_{p^n}(R)^s$$

La pareja $(A_0, (\tilde{A}_{p^n}))_n$ satisface una de las condiciones equivalentes del Teorema 0.4.4; por tanto podemos asociarle un esquema abeliano A_N/R_N. Consideremos ahora el límite

$$A := \varinjlim_N A_N.$$

Este objeto es, en principio, simplemente un límite directo de esquemas, es decir, un esquema formal. Pero puede comprobarse (cf. [5], p. 84; Teorema 3.3 del capítulo V de [1]) que, de hecho, es un esquema abeliano, definido sobre el anillo de los vectores de Witt. □

El levantamiento canónico tiene buenas propiedades funtoriales. No entraremos en más detalles en esta exposición; simplemente enunciamos dos resultados (cf. Teorema 3.3 y Corolario 3.4 del capítulo V de [1])

0.4.8 Proposición. *Sea k un cuerpo perfecto de característica $p > 0$, A_0/k una variedad abeliana ordinaria y $A/W(k)$ el levantamiento canónico. La aplicación*

$$\mathrm{End}_{W(k)}(A) \to \mathrm{End}_k(A_0)$$

es biyectiva.

0.4.9 Proposición. *Sean A_0 , B_0 variedades abelianas ordinarias sobre k, A, B sus levantamientos canónicos. La aplicación*

$$\mathrm{Hom}_{W(k)}(A, B) \to \mathrm{Hom}_k(A_0, B_0)$$

es biyectiva.

Bibliografia

[1] Messing, William. *The Crystals Associated to Barsotti-Tate Groups: with Applications to Abelian Schemes*. Lecture Notes in Mathematics **264**, Springer-Verlag, (1972).

[2] Mumford, David. *Abelian Varieties*. Tata Institute of Fundamental Research Studies in Mathematics, Bombay. Oxford University Press (1974).

[3] Pink, Richard. *Finite group schemes*. Lecture course in WS 2004/05 Disponible online en
`http://www.math.ethz.ch/ pink/ftp/.../TitleContents.pdf`

[4] Rabinoff, Joseph. *The theory of Witt vectors*. Disponible online en `http://math.stanford.edu/rabinoff/misc/witt.pdf`

[5] Serre, Jean-Pierre. "Groupes p-divisibles (dáprès J. Tate)". *Séminaire Bourbaki*, 19e année, 1966/67, n. **318**.

[6] Serre, Jean-Pierre *Local fields*. Graduate Texts in Mathematics, **67**. Springer-Verlag, New York-Berlin, (1979).