Teorema de Serre-Tate

Sara Arias de Reyna

Institut für Experimentelle Mathematik
Universität Duisburg-Essen

24 de Setembre de 2012

Variedades Abelianas módulo p

Seminari de Teoria de Nombres de Barcelona 2012

Contents

Contents

Vectores de Witt

p primo

Vectores de Witt

p primo
A anillo de valoración discreta completo,

Vectores de Witt

p primo
A anillo de valoración discreta completo, $\mathrm{char}(A) = 0$,

Vectores de Witt

p primo
A anillo de valoración discreta completo, $\mathrm{char}(A) = 0$, $\pi \in A$ uniformizante

Vectores de Witt

p primo
A anillo de valoración discreta completo, $\mathrm{char}(A) = 0$, $\pi \in A$ uniformizante
k cuerpo residual de característica p.

Vectores de Witt

p primo
A anillo de valoración discreta completo, $\mathrm{char}(A) = 0$, $\pi \in A$ uniformizante
k cuerpo residual de característica p.

$\mathrm{proj} : A \to k$.

Vectores de Witt

p primo
A anillo de valoración discreta completo, $\mathrm{char}(A) = 0$, $\pi \in A$ uniformizante
k cuerpo residual de característica p.

$\mathrm{proj} : A \to k$.
Sea $f : k \to A$ una aplicación tal que $\mathrm{proj} \circ f = \mathrm{id}_k$.

Vectores de Witt

p primo
A anillo de valoración discreta completo, $\mathrm{char}(A) = 0$, $\pi \in A$ uniformizante
k cuerpo residual de característica p.

$\mathrm{proj} : A \to k$.
Sea $f : k \to A$ una aplicación tal que $\mathrm{proj} \circ f = \mathrm{id}_k$.

$$\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$$

Vectores de Witt

p primo
A anillo de valoración discreta completo, $\mathrm{char}(A) = 0$, $\pi \in A$ uniformizante
k cuerpo residual de característica p.

$$\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$$

Vectores de Witt

p primo
A anillo de valoración discreta completo, $\mathrm{char}(A) = 0$, $\pi \in A$ uniformizante
k cuerpo residual de característica p.

$$\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$$

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

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

para una familia de elementos $\{\lambda_i\}_{i\in\mathbb{N}} \subset k$.

Vectores de Witt

p primo
A anillo de valoración discreta completo, $\mathrm{char}(A) = 0$, $\pi \in A$ uniformizante
k cuerpo residual de característica p.

$$\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$$

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

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

para una familia de elementos $\{\lambda_i\}_{i\in\mathbb{N}} \subset k$.

Como conjunto, $A \simeq k^{\mathbb{N}}$.

Vectores de Witt

Como conjunto, $A \simeq k^{\mathbb{N}}$ a través de la aplicación $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$.

Vectores de Witt

Como conjunto, $A \simeq k^{\mathbb{N}}$ a través de la aplicación $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$.

Sean

$$\begin{cases} a = \sum_{i=0}^{\infty} f(\alpha_i)\pi^i \\ b = \sum_{i=0}^{\infty} f(\beta_i)\pi^i \end{cases} \Longrightarrow \begin{cases} a + b = \sum_{i=0}^{\infty} f(\gamma_i)\pi^i \\ a \cdot b = \sum_{i=0}^{\infty} f(\delta_i)\pi^i \end{cases}$$

Vectores de Witt

Como conjunto, $A \simeq k^{\mathbb{N}}$ a través de la aplicación $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$.

Sean

$$\begin{cases} a = \sum_{i=0}^{\infty} f(\alpha_i)\pi^i \\ b = \sum_{i=0}^{\infty} f(\beta_i)\pi^i \end{cases} \Longrightarrow \begin{cases} a + b = \sum_{i=0}^{\infty} f(\gamma_i)\pi^i \\ a \cdot b = \sum_{i=0}^{\infty} f(\delta_i)\pi^i \end{cases}$$

Podemos determinar $\{\gamma_i\}$ *y* $\{\delta_i\}$ *a partir de* $\{\alpha_i\}$ *y* $\{\beta_i\}$*?*

Vectores de Witt

k perfecto

Vectores de Witt

k perfecto

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.

Vectores de Witt

k perfecto

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.
- Sea $f : k \to A$ la aplicación de (1). se verifican:
  - $f(\alpha\beta) = f(\alpha)f(\beta)$

Vectores de Witt

k perfecto

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.
- Sea $f : k \to A$ la aplicación de (1). se verifican:
  - $f(\alpha\beta) = f(\alpha)f(\beta)$
  - Sea $a \in A$.

$$a \in f(k) \Leftrightarrow \forall n \in \mathbb{N}, a \text{ es una potencia } p^n\text{-ésima.}$$

Vectores de Witt

k perfecto

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.
- Sea $f : k \to A$ la aplicación de (1). se verifican:
  - $f(\alpha\beta) = f(\alpha)f(\beta)$
  - Sea $a \in A$.

$$a \in f(k) \Leftrightarrow \forall n \in \mathbb{N}, a \text{ es una potencia } p^n\text{-ésima.}$$

f es el *sistema de representantes multiplicativo* o *de Teichmüller*.

Vectores de Witt

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.
- Sea $f : k \to A$ la aplicación de (1). se verifican:
  - $f(\alpha\beta) = f(\alpha)f(\beta)$
  - Sea $a \in A$.

$$a \in f(k) \Leftrightarrow \forall n \in \mathbb{N}, a \text{ es una potencia } p^n\text{-ésima.}$$

f es el *sistema de representantes multiplicativo* o *de Teichmüller*.

Vectores de Witt

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.
- Sea $f : k \to A$ la aplicación de (1). se verifican:
  - $f(\alpha\beta) = f(\alpha)f(\beta)$
  - Sea $a \in A$.

$$a \in f(k) \Leftrightarrow \forall n \in \mathbb{N}, a \text{ es una potencia } p^n\text{-ésima.}$$

f es el *sistema de representantes multiplicativo* o *de Teichmüller*.

Vectores de Witt

A anillo tal que

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.
- Sea $f : k \to A$ la aplicación de (1). se verifican:
  - $f(\alpha\beta) = f(\alpha)f(\beta)$
  - Sea $a \in A$.

$$a \in f(k) \Leftrightarrow \forall n \in \mathbb{N}, a \text{ es una potencia } p^n\text{-ésima.}$$

f es el *sistema de representantes multiplicativo* o *de Teichmüller*.

Vectores de Witt

A anillo tal que

- completo y Hausdorff para la topología p-ádica
- $k = A/(p)$ anillo residual de característica p, perfecto
- $p \in A$ no divisor de cero

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.
- Sea $f : k \to A$ la aplicación de (1). se verifican:
  - $f(\alpha\beta) = f(\alpha)f(\beta)$
  - Sea $a \in A$.

$$a \in f(k) \Leftrightarrow \forall n \in \mathbb{N}, a \text{ es una potencia } p^n\text{-ésima.}$$

f es el *sistema de representantes multiplicativo* o *de Teichmüller*.

Vectores de Witt

A anillo tal que

- completo y Hausdorff para la topología p-ádica
- $k = A/(p)$ anillo residual de característica p, perfecto
- $p \in A$ no divisor de cero

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.
- Sea $f : k \to A$ la aplicación de (1). se verifican:
  - $f(\alpha\beta) = f(\alpha)f(\beta)$
  - Sea $a \in A$.

$$a \in f(k) \Leftrightarrow \forall n \in \mathbb{N}, a \text{ es una potencia } p^n\text{-ésima.}$$

f es el *sistema de representantes multiplicativo* o *de Teichmüller*.

Vectores de Witt

A anillo tal que

- completo y Hausdorff para la topología p-ádica
- $k = A/(p)$ anillo residual de característica p, $\lambda \mapsto \lambda^p$ es un automorfismo de k.
- $p \in A$ no divisor de cero

- Existe una única aplicación $f : k \to A$ tal que $\begin{tikzcd} A \arrow[r, bend left, "\mathrm{proj}"] & k \arrow[l, dotted, bend left, "f"] \end{tikzcd}$ y, para todo $\lambda \in k$, $f(\lambda^p) = f(\lambda)^p$.
- Sea $f : k \to A$ la aplicación de (1). se verifican:
  - $f(\alpha\beta) = f(\alpha)f(\beta)$
  - Sea $a \in A$.

$$a \in f(k) \Leftrightarrow \forall n \in \mathbb{N}, a \text{ es una potencia } p^n\text{-ésima.}$$

f es el *sistema de representantes multiplicativo* o *de Teichmüller*.

Vectores de Witt

A anillo tal que

- completo y Hausdorff para la topología p-ádica
- $k = A/(p)$ anillo residual de característica p, $\lambda \mapsto \lambda^p$ es un automorfismo de k.
- $p \in A$ no divisor de cero

Vectores de Witt

A anillo tal que

- completo y Hausdorff para la topología p-ádica
- $k = A/(p)$ anillo residual de característica p, $\lambda \mapsto \lambda^p$ es un automorfismo de k.
- $p \in A$ no divisor de cero

A es un *p-anillo estricto*

Vectores de Witt

- $X_0, X_1, \ldots, X_n, \ldots$; $Y_0, Y_1, \ldots, Y_n, \ldots$; familia de indeterminadas

Vectores de Witt

- $X_0, X_1, \ldots, X_n, \ldots$; $Y_0, Y_1, \ldots, Y_n, \ldots$; familia de indeterminadas
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$

Vectores de Witt

- $X_0, X_1, \ldots, X_n, \ldots$; $Y_0, Y_1, \ldots, Y_n, \ldots$; familia de indeterminadas
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- $\hat{S} =$ completación de S respecto a la topología p-ádica

Vectores de Witt

- $X_0, X_1, \ldots, X_n, \ldots$; $Y_0, Y_1, \ldots, Y_n, \ldots$; familia de indeterminadas
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- $\hat{S} =$ completación de S respecto a la topología p-ádica
- El anillo residual es $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$

Vectores de Witt

- $X_0, X_1, \ldots, X_n, \ldots$; $Y_0, Y_1, \ldots, Y_n, \ldots$; familia de indeterminadas
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- $\hat{S} =$ completación de S respecto a la topología p-ádica
- El anillo residual es $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo.

Vectores de Witt

- $X_0, X_1, \ldots, X_n, \ldots$; $Y_0, Y_1, \ldots, Y_n, \ldots$; familia de indeterminadas
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- $\hat{S} =$ completación de S respecto a la topología p-ádica
- El anillo residual es $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo.

Sean $x = \sum_{i=0}^{\infty} X_i p^i$, $y = \sum_{i=0}^{\infty} Y_i p^i$

Vectores de Witt

- $X_0, X_1, \ldots, X_n, \ldots$; $Y_0, Y_1, \ldots, Y_n, \ldots$; familia de indeterminadas
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- $\hat{S}$ = completación de S respecto a la topología p-ádica
- El anillo residual es $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo.

Sean $x = \sum_{i=0}^{\infty} X_i p^i$, $y = \sum_{i=0}^{\infty} Y_i p^i$

Existen unos únicos $Q_i^+, Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$ tales que

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

Vectores de Witt

- A p-anillo estricto

Vectores de Witt

- A p-anillo estricto
- $f : k \to A$ sistema de representantes multiplicativo

Vectores de Witt

- A p-anillo estricto
- $f : k \to A$ sistema de representantes multiplicativo

Lemma

Sean $\{\alpha_i\}_{i\in\mathbb{N}}$, $\{\beta_i\}_{i\in\mathbb{N}} \subset k^{\mathbb{N}}$. Se verifican

$$\left(\sum_{i=0}^{\infty} f(\alpha_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(\beta_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+(\alpha_0, \alpha_1, \ldots; \beta_0, \beta_1, \ldots))p^i$$

$$\left(\sum_{i=0}^{\infty} f(\alpha_i)p^i\right) \cdot \left(\sum_{i=0}^{\infty} f(\beta_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^\times(\alpha_0, \alpha_1, \ldots; \beta_0, \beta_1, \ldots))p^i$$

Vectores de Witt

Teorema

Sea k un anillo perfecto de característica p. Existe un único p- anillo estricto con anillo residual k.

Vectores de Witt

Teorema

Sea k un anillo perfecto de característica p. Existe un único p- anillo estricto con anillo residual k.

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.

Vectores de Witt

Podemos determinar $Q_i^+, Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$*?*

Vectores de Witt

Podemos determinar $Q_i^+, Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$*?*

- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$,

Vectores de Witt

Podemos determinar $Q_i^+, Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$*?*

- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$,

Vectores de Witt

Podemos determinar $Q_i^+, Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$*?*

- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$

Vectores de Witt

Podemos determinar $Q_i^+, Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$*?*

- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo.

Vectores de Witt

Podemos determinar $Q_i^+, Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$*?*

- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo. $f(X_i) = X_i$, $f(Y_j) = Y_j$.

Vectores de Witt

Podemos determinar $Q_i^+, Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$*?*

- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo. $f(X_i) = X_i$, $f(Y_j) = Y_j$.
- Sean $x = \sum_{i=0}^{\infty} f(X_i)p^i$, $y = \sum_{i=0}^{\infty} f(Y_i)p^i$.

Vectores de Witt

Podemos determinar $Q_i^+, Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$*?*

- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo. $f(X_i) = X_i$, $f(Y_j) = Y_j$.
- Sean $x = \sum_{i=0}^{\infty} f(X_i)p^i$, $y = \sum_{i=0}^{\infty} f(Y_i)p^i$.

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

Vectores de Witt

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

Vectores de Witt

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

$$f(X_0) + f(Y_0) = f(Q_0^+) \pmod{p}$$

Vectores de Witt

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

$$f(X_0) + f(Y_0) = f(Q_0^+) \pmod{p} \Rightarrow Q_0^+ = X_0 + Y_0$$

Vectores de Witt

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

$$f(X_0) + f(Y_0) = f(Q_0^+) \pmod{p} \Rightarrow Q_0^+ = X_0 + Y_0$$

$$(f(X_0) + pf(X_1)) + (f(Y_0) + pf(Y_1))) = f(Q_0^+) + pf(Q_1^+) \pmod{p^2}$$

Vectores de Witt

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

$$f(X_0) + f(Y_0) = f(Q_0^+) \pmod{p} \Rightarrow Q_0^+ = X_0 + Y_0$$

$$(f(X_0) + pf(X_1)) + (f(Y_0) + pf(Y_1))) = f(Q_0^+) + pf(Q_1^+) \pmod{p^2}$$

Vectores de Witt

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

$$f(X_0) + f(Y_0) = f(Q_0^+) \pmod{p} \Rightarrow Q_0^+ = X_0 + Y_0$$

$$(f(X_0) + pf(X_1)) + (f(Y_0) + pf(Y_1))) = f(Q_0^+) + pf(Q_1^+) \pmod{p^2}$$

$$f(Q_0^+) = f(X_0 + Y_0) = f((X_0 + Y_0)^{1/p})^p = f(X_0^{1/p} + Y_0^{1/p})^p$$

Vectores de Witt

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

$$f(X_0) + f(Y_0) = f(Q_0^+) \pmod{p} \Rightarrow Q_0^+ = X_0 + Y_0$$

$$(f(X_0) + pf(X_1)) + (f(Y_0) + pf(Y_1))) = f(Q_0^+) + pf(Q_1^+) \pmod{p^2}$$

$$f(Q_0^+) = f(X_0 + Y_0) = f((X_0 + Y_0)^{1/p})^p = f(X_0^{1/p} + Y_0^{1/p})^p$$

Pero $f(X_0^{1/p} + Y_0^{1/p}) \equiv f(X_0^{1/p}) + f(Y_0^{1/p}) \pmod{p}$

Vectores de Witt

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

$$f(X_0) + f(Y_0) = f(Q_0^+) \pmod{p} \Rightarrow Q_0^+ = X_0 + Y_0$$

$$(f(X_0) + pf(X_1)) + (f(Y_0) + pf(Y_1))) = f(Q_0^+) + pf(Q_1^+) \pmod{p^2}$$

$$f(Q_0^+) = f(X_0 + Y_0) = f((X_0 + Y_0)^{1/p})^p = f(X_0^{1/p} + Y_0^{1/p})^p$$

Pero $f(X_0^{1/p} + Y_0^{1/p}) \equiv f(X_0^{1/p}) + f(Y_0^{1/p}) \pmod{p} \Rightarrow$

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

Vectores de Witt

$$\left(\sum_{i=0}^{\infty} f(X_i)p^i\right) + \left(\sum_{i=0}^{\infty} f(Y_i)p^i\right) = \sum_{i=0}^{\infty} f(Q_i^+)p^i$$

$$f(X_0) + f(Y_0) = f(Q_0^+) \pmod{p} \Rightarrow Q_0^+ = X_0 + Y_0$$

$$(f(X_0) + pf(X_1)) + (f(Y_0) + pf(Y_1))) = f(Q_0^+) + pf(Q_1^+) \pmod{p^2}$$

$$f(Q_0^+) = f(X_0 + Y_0) = f((X_0 + Y_0)^{1/p})^p = f(X_0^{1/p} + Y_0^{1/p})^p$$

Pero $f(X_0^{1/p} + Y_0^{1/p}) \equiv f(X_0^{1/p}) + f(Y_0^{1/p}) \pmod{p} \Rightarrow$

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

Vectores de Witt

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

Vectores de Witt

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

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

Vectores de Witt

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

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

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

Vectores de Witt

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

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

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

$$\dots$$

Vectores de Witt

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

Vectores de Witt

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

Llamemos $\tilde{X}_0 := f(X_0^{1/p})$, $\tilde{Y}_0 := f(Y_0^{1/p})$, $\tilde{X}_1 := f(X_1)$, $\tilde{Y}_1 := f(Y_1)$.

Vectores de Witt

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

Llamemos $\tilde{X}_0 := f(X_0^{1/p})$, $\tilde{Y}_0 := f(Y_0^{1/p})$, $\tilde{X}_1 := f(X_1)$, $\tilde{Y}_1 := f(Y_1)$.

$$\left(\tilde{X}_0^p + p\tilde{X}_1\right) + \left(\tilde{Y}_0^p + p\tilde{Y}_1\right) = (\tilde{X}_0 + \tilde{Y}_0)^p + pf(Q_1^+) \pmod{p^2}$$

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \ldots, X_n, \ldots)$ sucesión de indeterminadas.

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

$$W_0(\mathbf{X}) = X_0$$

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

$$W_0(\mathbf{X}) = X_0$$
$$W_1(\mathbf{X}) = X_0^p + pX_1$$

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

$$W_0(\mathbf{X}) = X_0$$
$$W_1(\mathbf{X}) = X_0^p + pX_1$$
$$W_2(\mathbf{X}) = X_0^{p^2} + pX_1^p + p^2X_2$$

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

$$
\begin{aligned}
W_0(\mathbf{X}) &= X_0 \\
W_1(\mathbf{X}) &= X_0^p + pX_1 \\
W_2(\mathbf{X}) &= X_0^{p^2} + pX_1^p + p^2 X_2 \\
&\dots
\end{aligned}
$$

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

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

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

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

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

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

Polinomios de Witt

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

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

Polinomios de Witt

Notemos que podemos despejar X_n en función de $W_0, \dots, W_n$ en $\mathbb{Z}[\frac{1}{p}]$:

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

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

Polinomios de Witt

Notemos que podemos despejar X_n en función de $W_0, \dots, W_n$ en $\mathbb{Z}[\frac{1}{p}]$:

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

$$
\begin{aligned}
X_0 &= W_0 \\
X_1 &= \frac{1}{p}(W_1 - W_0^p) \\
W_2(\mathbf{X}) &= X_0^{p^2} + pX_1^p + p^2 X_2 \\
&\dots \\
W_n(\mathbf{X}) &= X_0^{p^n} + pX_1^{p^{n-1}} + p^2 X_2^{p^{n-2}} + \dots + p^{n-1} X_{n-1}^p + p^n X_n \\
&\dots
\end{aligned}
$$

Polinomios de Witt

Notemos que podemos despejar X_n en función de $W_0, \dots, W_n$ en $\mathbb{Z}[\frac{1}{p}]$:

Vectores de Witt

- $\mathbf{X} = (X_0, X_1, \dots, X_n, \dots)$ sucesión de indeterminadas.

$$
\begin{aligned}
X_0 &= W_0 \\
X_1 &= \frac{1}{p}(W_1 - W_0^p) \\
X_2 &= \frac{1}{p^2}(W_2 - W_0^{p^2} - p(W_1 - pW_0^p)) \\
&\dots \\
W_n(\mathbf{X}) &= X_0^{p^n} + pX_1^{p^{n-1}} + p^2X_2^{p^{n-2}} + \dots + p^{n-1}X_{n-1}^p + p^nX_n \\
&\dots
\end{aligned}
$$

Polinomios de Witt

Notemos que podemos despejar X_n en función de $W_0, \dots, W_n$ en $\mathbb{Z}[\frac{1}{p}]$:

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$
  (por ejemplo, $\Phi(X, Y) = X + Y$ o $\Phi(X, Y) = X \cdot Y$)

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$
  (por ejemplo, $\Phi(X, Y) = X + Y$ o $\Phi(X, Y) = X \cdot Y$)

Lema

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

$$W_n(\varphi_0, \varphi_1, \varphi_2, \dots) = \Phi(W_n(\mathbf{X}), W_n(\mathbf{Y}))$$

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$
  (por ejemplo, $\Phi(X, Y) = X + Y$ o $\Phi(X, Y) = X \cdot Y$)

Lema

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

$$W_n(\varphi_0, \varphi_1, \varphi_2, \dots) = \Phi(W_n(\mathbf{X}), W_n(\mathbf{Y}))$$

$$W_0(\varphi_0) = \Phi(X_0, Y_0)$$

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$
  (por ejemplo, $\Phi(X, Y) = X + Y$ o $\Phi(X, Y) = X \cdot Y$)

Lema

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

$$W_n(\varphi_0, \varphi_1, \varphi_2, \dots) = \Phi(W_n(\mathbf{X}), W_n(\mathbf{Y}))$$

$$\varphi_0 = W_0(\varphi_0) = \Phi(X_0, Y_0)$$

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$
  (por ejemplo, $\Phi(X, Y) = X + Y$ o $\Phi(X, Y) = X \cdot Y$)

Lema

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

$$W_n(\varphi_0, \varphi_1, \varphi_2, \dots) = \Phi(W_n(\mathbf{X}), W_n(\mathbf{Y}))$$

$$\varphi_0 = W_0(\varphi_0) = \Phi(X_0, Y_0)$$

$$W_1(\varphi_0, \varphi_1) = \Phi(W_1(X_0, X_1), W_1(Y_0, Y_1)) =$$

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$
  (por ejemplo, $\Phi(X, Y) = X + Y$ o $\Phi(X, Y) = X \cdot Y$)

Lema

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

$$W_n(\varphi_0, \varphi_1, \varphi_2, \dots) = \Phi(W_n(\mathbf{X}), W_n(\mathbf{Y}))$$

$$\varphi_0 = W_0(\varphi_0) = \Phi(X_0, Y_0)$$

$$W_1(\varphi_0, \varphi_1) = \Phi(W_1(X_0, X_1), W_1(Y_0, Y_1)) = \Phi(X_0^p + pX_1, Y_0^p + pY_1)$$

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$
  (por ejemplo, $\Phi(X, Y) = X + Y$ o $\Phi(X, Y) = X \cdot Y$)

Lema

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

$$W_n(\varphi_0, \varphi_1, \varphi_2, \dots) = \Phi(W_n(\mathbf{X}), W_n(\mathbf{Y}))$$

$$\varphi_0 = W_0(\varphi_0) = \Phi(X_0, Y_0)$$

$$p\varphi_1 + \varphi_0^p = W_1(\varphi_0, \varphi_1) = \Phi(W_1(X_0, X_1), W_1(Y_0, Y_1)) = \Phi(X_0^p + pX_1, Y_0^p + pY_1)$$

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$
  (por ejemplo, $\Phi(X, Y) = X + Y$ o $\Phi(X, Y) = X \cdot Y$)

Lema

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

$$W_n(\varphi_0, \varphi_1, \varphi_2, \dots) = \Phi(W_n(\mathbf{X}), W_n(\mathbf{Y}))$$

$$\varphi_0 = W_0(\varphi_0) = \Phi(X_0, Y_0)$$

$$\varphi_1 = \frac{1}{p}\left(\Phi(X_0^p + pX_1, Y_0^p + pY_1) - \varphi_0^p\right)$$

Vectores de Witt

- Sea $\Phi(X, Y) \in \mathbb{Z}[X, Y]$
  (por ejemplo, $\Phi(X, Y) = X + Y$ o $\Phi(X, Y) = X \cdot Y$)

Lema

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

$$W_n(\varphi_0, \varphi_1, \varphi_2, \dots) = \Phi(W_n(\mathbf{X}), W_n(\mathbf{Y}))$$

$$\varphi_0 = W_0(\varphi_0) = \Phi(X_0, Y_0)$$

$$\varphi_1 = \frac{1}{p}\left(\Phi(X_0^p + pX_1, Y_0^p + pY_1) - \varphi_0^p\right)$$

Los coeficientes están en $\mathbb{Z}$ (y no sólo en $\mathbb{Z}[\frac{1}{p}]$!!)

Vectores de Witt

$\Phi(X, Y) := X + Y$

Vectores de Witt

$\Phi(X, Y) := X + Y$ (resp. $X \cdot Y$),

Vectores de Witt

$\Phi(X, Y) := X + Y$ (resp. $X \cdot Y$), sea $S_n := \varphi_n$

Vectores de Witt

$\Phi(X, Y) := X + Y$ (resp. $X \cdot Y$), sea $S_n := \varphi_n$ (resp. $P_n := \varphi_n$)

Vectores de Witt

$\Phi(X, Y) := X + Y$ (resp. $X \cdot Y$), sea $S_n := \varphi_n$ (resp. $P_n := \varphi_n$)

A un anillo conmutativo;

Vectores de Witt

$\Phi(X, Y) := X + Y$ (resp. $X \cdot Y$), sea $S_n := \varphi_n$ (resp. $P_n := \varphi_n$)

A un anillo conmutativo; $A^{\mathbb{N}} = A \times A \times \cdots$.

Vectores de Witt

$\Phi(X, Y) := X + Y$ (resp. $X \cdot Y$), sea $S_n := \varphi_n$ (resp. $P_n := \varphi_n$)

A un anillo conmutativo; $A^{\mathbb{N}} = A \times A \times \cdots$.

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

Vectores de Witt

$\Phi(X, Y) := X + Y$ (resp. $X \cdot Y$), sea $S_n := \varphi_n$ (resp. $P_n := \varphi_n$)

A un anillo conmutativo; $A^{\mathbb{N}} = A \times A \times \cdots$.

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

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

Vectores de Witt

$\Phi(X, Y) := X + Y$ (resp. $X \cdot Y$), sea $S_n := \varphi_n$ (resp. $P_n := \varphi_n$)

A un anillo conmutativo; $A^{\mathbb{N}} = A \times A \times \cdots$.

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

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

Proposición

$W(A) := (A^{\mathbb{N}}, \oplus, \otimes)$ es un anillo conmutativo.

Vectores de Witt

$\Phi(X, Y) := X + Y$ (resp. $X \cdot Y$), sea $S_n := \varphi_n$ (resp. $P_n := \varphi_n$)

A un anillo conmutativo; $A^{\mathbb{N}} = A \times A \times \cdots$.

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

Proposición

$W(A) := (A^{\mathbb{N}}, \oplus, \otimes)$ es un anillo conmutativo.

La aplicación $W_* : W(A) \to A^{\mathbb{N}}$

$$(a_n)_n \mapsto (W_n(a_0, a_1, \ldots))_n$$

es un homomorfismo de anillos (isom. si p es invertible en A)

Vectores de Witt

- $\mathbf{X} := (X_0, X_1, \dots); \mathbf{Y} := (Y_0, Y_1, \dots);$

Vectores de Witt

- $\mathbf{X} := (X_0, X_1, \dots); \mathbf{Y} := (Y_0, Y_1, \dots);$
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}],$

Vectores de Witt

- $\mathbf{X} := (X_0, X_1, \dots); \mathbf{Y} := (Y_0, Y_1, \dots);$
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}], \hat{S},$

Vectores de Witt

- $\mathbf{X} := (X_0, X_1, \dots); \mathbf{Y} := (Y_0, Y_1, \dots);$
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$.

Vectores de Witt

- $\mathbf{X} := (X_0, X_1, \dots); \mathbf{Y} := (Y_0, Y_1, \dots);$
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$.
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo.

Vectores de Witt

- $\mathbf{X} := (X_0, X_1, \dots)$; $\mathbf{Y} := (Y_0, Y_1, \dots)$;
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$.
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo.

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

Vectores de Witt

- $\mathbf{X} := (X_0, X_1, \dots)$; $\mathbf{Y} := (Y_0, Y_1, \dots)$;
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$.
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo.

Sean $x = \sum_{i=0}^{\infty} X_i p^i$, $y = \sum_{i=0}^{\infty} Y_i p^i$. Existen unos únicos Q_i^+, $Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$ tales que

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

Vectores de Witt

- $\mathbf{X} := (X_0, X_1, \dots)$; $\mathbf{Y} := (Y_0, Y_1, \dots)$;
- $S = \mathbb{Z}[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$, $\hat{S}$, $\mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$.
- Sea $f : \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}] \to \hat{S}$ sistema de representantes multiplicativo.

Sean $x = \sum_{i=0}^{\infty} X_i p^i$, $y = \sum_{i=0}^{\infty} Y_i p^i$. Existen unos únicos Q_i^+, $Q_i^\times \in \mathbb{F}_p[\{X_i^{p^{-n}}, Y_i^{p^{-n}} : i \in \mathbb{N}, n \in \mathbb{N}\}]$ tales que

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

$$Q_i^+ = S_i(X_0^{p^{-i}}, X_1^{p^{-i+1}}, \dots, X_{i-1}^{p^{-1}}, X_i; Y_0^{p^{-i}}, Y_1^{p^{-i+1}}, \dots, Y_{i-1}^{p^{-1}}, Y_i)$$
$$Q_i^\times = P_i(X_0^{p^{-i}}, X_1^{p^{-i+1}}, \dots, X_{i-1}^{p^{-1}}, X_i; Y_0^{p^{-i}}, Y_1^{p^{-i+1}}, \dots, Y_{i-1}^{p^{-1}}, Y_i)$$

Vectores de Witt

Podríamos haber definido . . . ?

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo;

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo;

$$\tilde{\oplus} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^+(a_0, a_1, \dots; b_0, b_1, \dots))_n$$

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo;

$$\tilde{\oplus} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{+}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$
$$\tilde{\otimes} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{\times}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo;

$$\tilde{\oplus} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{+}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$
$$\tilde{\otimes} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{\times}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$

$$\tilde{W}(A) := (A^{\mathbb{N}}, \tilde{\oplus}, \tilde{\otimes})?$$

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo;

$$\tilde{\oplus} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{+}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$
$$\tilde{\otimes} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{\times}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$

$$\tilde{W}(A) := (A^{\mathbb{N}}, \tilde{\oplus}, \tilde{\otimes})?$$

Sí!

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo;

$$\tilde{\oplus} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{+}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$
$$\tilde{\otimes} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{\times}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$

$$\tilde{W}(A) := (A^{\mathbb{N}}, \tilde{\oplus}, \tilde{\otimes})?$$

Sí!

Pero tendríamos que trabajar con potencias negativas de las variables!

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo; A perfecto.

$$\tilde{\oplus} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{+}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$
$$\tilde{\otimes} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$(a_n)_n, (b_n)_n \mapsto (Q_n^{\times}(a_0, a_1, \dots; b_0, b_1, \dots))_n$$

$$\tilde{W}(A) := (A^{\mathbb{N}}, \tilde{\oplus}, \tilde{\otimes})?$$

Sí!

Pero tendríamos que trabajar con potencias negativas de las variables!

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo; A perfecto.

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo; A perfecto.

- $W(A) := (A^{\mathbb{N}}, \oplus, \otimes)$
- $\tilde{W}(A) := (A^{\mathbb{N}}, \tilde{\oplus}, \tilde{\otimes})$

Vectores de Witt

Podríamos haber definido . . . ?

A un anillo conmutativo; A perfecto.

- $W(A) := (A^{\mathbb{N}}, \oplus, \otimes)$
- $\tilde{W}(A) := (A^{\mathbb{N}}, \tilde{\oplus}, \tilde{\otimes})$

Lema

La aplicación

$$\Psi : \tilde{W}(A) \to W(A)$$

$$(a_0, a_1, a_2, \dots) \mapsto (a_0, a_1^p, a_2^{p^2}, \dots)$$

es un isomorfismo.

Vectores de Witt

A un anillo conmutativo, $N \in \mathbb{N}$.

Vectores de Witt

A un anillo conmutativo, $N \in \mathbb{N}$.

$$\oplus : A^N \times A^N \to A^N$$
$$(a_n)_{n=0}^N, (b_n)_{n=0}^N \mapsto (S_n(a_0, \ldots, a_N; b_0, \ldots, b_N))_{n=0}^N$$

Vectores de Witt

A un anillo conmutativo, $N \in \mathbb{N}$.

$$\oplus : A^N \times A^N \to A^N$$
$$(a_n)_{n=0}^N, (b_n)_{n=0}^N \mapsto (S_n(a_0, \ldots, a_N; b_0, \ldots, b_N))_{n=0}^N$$
$$\otimes : A^N \times A^N \to A^N$$
$$(a_n)_{n=0}^N, (b_n)_{n=0}^N \mapsto (P_n(a_0, \ldots, a_N; b_0, \ldots, b_N))_{n=0}^N$$

Vectores de Witt

A un anillo conmutativo, $N \in \mathbb{N}$.

$$\begin{aligned} \oplus : A^N \times A^N &\to A^N \\ (a_n)_{n=0}^N, (b_n)_{n=0}^N &\mapsto (S_n(a_0, \ldots, a_N; b_0, \ldots, b_N))_{n=0}^N \\ \otimes : A^N \times A^N &\to A^N \\ (a_n)_{n=0}^N, (b_n)_{n=0}^N &\mapsto (P_n(a_0, \ldots, a_N; b_0, \ldots, b_N))_{n=0}^N \end{aligned}$$

- $W(A)_N := (A^n, \oplus, \otimes)$ es un anillo conmutativo.

Vectores de Witt

A un anillo conmutativo, $N \in \mathbb{N}$.

$$\begin{aligned} \oplus : A^N \times A^N &\to A^N \\ (a_n)_{n=0}^N, (b_n)_{n=0}^N &\mapsto (S_n(a_0, \ldots, a_N; b_0, \ldots, b_N))_{n=0}^N \\ \otimes : A^N \times A^N &\to A^N \\ (a_n)_{n=0}^N, (b_n)_{n=0}^N &\mapsto (P_n(a_0, \ldots, a_N; b_0, \ldots, b_N))_{n=0}^N \end{aligned}$$

- $W(A)_N := (A^n, \oplus, \otimes)$ es un anillo conmutativo.
- Tenemos una aplicación cociente $W(A) \to W(A)_N$

Vectores de Witt

A un anillo conmutativo, $N \in \mathbb{N}$.

$$\oplus : A^N \times A^N \to A^N$$
$$(a_n)_{n=0}^N, (b_n)_{n=0}^N \mapsto (S_n(a_0, \ldots, a_N; b_0, \ldots, b_N))_{n=0}^N$$
$$\otimes : A^N \times A^N \to A^N$$
$$(a_n)_{n=0}^N, (b_n)_{n=0}^N \mapsto (P_n(a_0, \ldots, a_N; b_0, \ldots, b_N))_{n=0}^N$$

- $W(A)_N := (A^n, \oplus, \otimes)$ es un anillo conmutativo.
- Tenemos una aplicación cociente $W(A) \to W(A)_N$
- $$W(A) = \varprojlim_N W(A)_N$$

Vectores de Witt

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

Vectores de Witt

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

Verschiebung,

Vectores de Witt

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

Verschiebung, Traslación

Vectores de Witt

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

Verschiebung, Traslación

$$\begin{tikzcd} W(A) \arrow[r, "V"] \arrow[d, "w_*"] & W(A) \arrow[d, "w_*"] \\ A^{\mathbb{N}} \arrow[r, "?"] & A^{\mathbb{N}} \end{tikzcd}$$

Vectores de Witt

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

Verschiebung, Traslación

$$\begin{tikzcd} W(A) \arrow[r, "V"] \arrow[d, "w_*"] & W(A) \arrow[d, "w_*"] \\ A^{\mathbb{N}} \arrow[r, "?"] & A^{\mathbb{N}} \end{tikzcd}$$

$$(w_0, w_1, \dots, w_n, \dots) \mapsto (0, pw_0, pw_1, \dots)$$

Vectores de Witt

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

Verschiebung, Traslación

$$\begin{tikzcd} W(A) \arrow[r, "V"] \arrow[d, "w_*"] & W(A) \arrow[d, "w_*"] \\ A^{\mathbb{N}} \arrow[r, "?"] & A^{\mathbb{N}} \end{tikzcd}$$

$$(w_0, w_1, \dots, w_n, \dots) \mapsto (0, pw_0, pw_1, \dots)$$

Luego $V : W(A) \to W(A)$ es aditiva.

Vectores de Witt

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

Verschiebung, Traslación

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

Vectores de Witt

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

Verschiebung, Traslación

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

$$0 \to W_r(A) \to W_{N+r}(A) \to W_N(A) \to 0$$

Vectores de Witt

$$F : W(A) \to W(A)$$
$$(a_0, a_1, a_2, \dots) \mapsto (a_0^p, a_1^p, a_2^p \dots)$$

Vectores de Witt

$$F : W(A) \to W(A)$$
$$(a_0, a_1, a_2, \dots) \mapsto (a_0^p, a_1^p, a_2^p \dots)$$

Frobenius

Vectores de Witt

$$F : W(A) \to W(A)$$
$$(a_0, a_1, a_2, \dots) \mapsto (a_0^p, a_1^p, a_2^p \dots)$$

Frobenius

$$\begin{tikzcd} W(A) \arrow[r, "F"] \arrow[d, "w_*"] & W(A) \arrow[d, "w_*"] \\ A \arrow[r, "\psi"] & A \end{tikzcd}$$

Vectores de Witt

$$F : W(A) \to W(A)$$
$$(a_0, a_1, a_2, \dots) \mapsto (a_0^p, a_1^p, a_2^p \dots)$$

Frobenius

$$\begin{tikzcd} W(A) \arrow[r, "F"] \arrow[d, "w_*"] & W(A) \arrow[d, "w_*"] \\ A \arrow[r, "\psi"] & A \end{tikzcd}$$

$$(W_0(a_0), W_1(a_0, a_1), W_2(a_0, a_1, a_2), \dots) = (W_0(a_0^p), W_1(a_0^p, a_1^p), W_2(a_0^p, a_1^p, a_2^p), \dots)$$

Vectores de Witt

$$F : W(A) \to W(A)$$
$$(a_0, a_1, a_2, \dots) \mapsto (a_0^p, a_1^p, a_2^p \dots)$$

Frobenius

$$\begin{tikzcd} W(A) \arrow[r, "F"] \arrow[d, "W_*"] & W(A) \arrow[d, "W_*"] \\ A \arrow[r, "\psi"] & A \end{tikzcd}$$

$$(W_0(a_0), W_1(a_0, a_1), W_2(a_0, a_1, a_2), \dots) = (W_0(a_0^p), W_1(a_0^p, a_1^p), W_2(a_0^p, a_1^p, a_2^p), \dots)$$

$$(\psi \circ W_*)(a_0, a_1, a_2, \dots) = (W_1(a_0, 0), W_2(a_0, a_1, 0), W_3(a_0, a_1, a_2, 0), \dots)$$

Vectores de Witt

- Supongamos que k es un anillo perfecto de característica p.

Vectores de Witt

- Supongamos que k es un anillo perfecto de característica p.
- $\tilde{W}(k)$; $f : k \to \tilde{W}(k)$ sistema de representantes multiplicativo

Vectores de Witt

- Supongamos que k es un anillo perfecto de característica p.
- $\tilde{W}(k)$; $f : k \to \tilde{W}(k)$ sistema de representantes multiplicativo
- $\varphi : k \to k$ es un homomorfismo

Vectores de Witt

- Supongamos que k es un anillo perfecto de característica p.
- $\tilde{W}(k)$; $f : k \to \tilde{W}(k)$ sistema de representantes multiplicativo
- $\varphi : k \to k$ es un homomorfismo (por ejemplo $\varphi : \alpha \mapsto \alpha^p$)

Vectores de Witt

- Supongamos que k es un anillo perfecto de característica p.
- $\tilde{W}(k)$; $f : k \to \tilde{W}(k)$ sistema de representantes multiplicativo
- $\varphi : k \to k$ es un homomorfismo (por ejemplo $\varphi : \alpha \mapsto \alpha^p$)

$$\begin{tikzcd} \tilde{W}(k) \arrow[r, "\Phi"] \arrow[d] & \tilde{W}(k) \arrow[d] \\ k \arrow[r, "\varphi"] & k \end{tikzcd}$$

Vectores de Witt

- Supongamos que k es un anillo perfecto de característica p.
- $\tilde{W}(k)$; $f : k \to \tilde{W}(k)$ sistema de representantes multiplicativo
- $\varphi : k \to k$ es un homomorfismo (por ejemplo $\varphi : \alpha \mapsto \alpha^p$)

$$\begin{tikzcd} \tilde{W}(k) \arrow[r, "\Phi"] \arrow[d] & \tilde{W}(k) \arrow[d] \\ k \arrow[r, "\varphi"] & k \end{tikzcd}$$

$$\Phi : \sum_{i=0}^{\infty} f(\alpha_i)p^i \mapsto \sum_{i=0}^{\infty} f(\varphi(\alpha_i))p^i.$$

Vectores de Witt

- Supongamos que k es un anillo perfecto de característica p.
- $\tilde{W}(k)$; $f : k \to \tilde{W}(k)$ sistema de representantes multiplicativo
- $\varphi : k \to k$ es un homomorfismo (por ejemplo $\varphi : \alpha \mapsto \alpha^p$)

$$\begin{tikzcd} \tilde{W}(k) \arrow[r, "\Phi"] \arrow[d] & \tilde{W}(k) \arrow[d] \\ k \arrow[r, "\varphi"] & k \end{tikzcd} \qquad \begin{tikzcd} W(k) \arrow[r, "\Phi'"] \arrow[d] & W(k) \arrow[d] \\ k \arrow[r, "\varphi"] & k \end{tikzcd}$$

$$\Phi : \sum_{i=0}^{\infty} f(\alpha_i)p^i \mapsto \sum_{i=0}^{\infty} f(\varphi(\alpha_i))p^i.$$

Vectores de Witt

$$\Phi(\sum_{i=0}^{\infty} f(\alpha_i)p^i + \sum_{i=0}^{\infty} f(\beta_i)p^i) =$$

Vectores de Witt

$$\Phi(\sum_{i=0}^{\infty} f(\alpha_i)p^i + \sum_{i=0}^{\infty} f(\beta_i)p^i) = \Phi(\sum_{i=0}^{\infty} f(Q_i^+(\alpha,\beta))p^i) =$$

Vectores de Witt

$$\Phi(\sum_{i=0}^{\infty} f(\alpha_i)p^i + \sum_{i=0}^{\infty} f(\beta_i)p^i) = \Phi(\sum_{i=0}^{\infty} f(Q_i^+(\alpha,\beta))p^i) =$$

$$= \sum_{i=0}^{\infty} f(\varphi(Q_i^+(\alpha,\beta)))p^i$$

Vectores de Witt

$$\Phi(\sum_{i=0}^{\infty} f(\alpha_i)p^i + \sum_{i=0}^{\infty} f(\beta_i)p^i) = \Phi(\sum_{i=0}^{\infty} f(Q_i^+(\alpha,\beta))p^i) =$$

$$= \sum_{i=0}^{\infty} f(\varphi(Q_i^+(\alpha,\beta)))p^i = \sum_{i=0}^{\infty} f(Q_i^+(\varphi(\alpha),\varphi(\beta)))p^i =$$

Vectores de Witt

$$\Phi(\sum_{i=0}^{\infty} f(\alpha_i)p^i + \sum_{i=0}^{\infty} f(\beta_i)p^i) = \Phi(\sum_{i=0}^{\infty} f(Q_i^+(\alpha,\beta))p^i) =$$

$$= \sum_{i=0}^{\infty} f(\varphi(Q_i^+(\alpha,\beta)))p^i = \sum_{i=0}^{\infty} f(Q_i^+(\varphi(\alpha),\varphi(\beta)))p^i =$$

$$\Phi(\sum_{i=0}^{\infty} f(\alpha_i)p^i) + \Phi(\sum_{i=0}^{\infty} f(\beta_i)p^i)$$

Vectores de Witt

$$\Phi(\sum_{i=0}^{\infty} f(\alpha_i)p^i + \sum_{i=0}^{\infty} f(\beta_i)p^i) = \Phi(\sum_{i=0}^{\infty} f(Q_i^+(\alpha,\beta))p^i) =$$

$$= \sum_{i=0}^{\infty} f(\varphi(Q_i^+(\alpha,\beta)))p^i = \sum_{i=0}^{\infty} f(Q_i^+(\varphi(\alpha),\varphi(\beta)))p^i =$$

$$\Phi(\sum_{i=0}^{\infty} f(\alpha_i)p^i) + \Phi(\sum_{i=0}^{\infty} f(\beta_i)p^i)$$

$$\Phi\left(\left(\sum_{i=0}^{\infty} f(\alpha_i)p^i\right)\cdot\left(\sum_{i=0}^{\infty} f(\beta_i)p^i\right)\right) = \Phi\left(\sum_{i=0}^{\infty} f(\alpha_i)p^i\right)\cdot\Phi\left(\sum_{i=0}^{\infty} f(\beta_i)p^i\right)$$

Vectores de Witt

$$V \circ F = F \circ V$$

Vectores de Witt

$$V \circ F = F \circ V = p$$

Vectores de Witt

$$V \circ F = F \circ V = p$$

Verschiebung in $\tilde{W}(k)$

Vectores de Witt

$$V \circ F = F \circ V = p$$

Verschiebung in $\tilde{W}(k)$

$$\begin{tikzcd} \tilde{W}(k) \arrow[r] \arrow[d] & \tilde{W}(k) \arrow[d] \\ W(k) \arrow[r, "V"] & W(k) \end{tikzcd}$$

Vectores de Witt

$$V \circ F = F \circ V = p$$

Verschiebung in $\tilde{W}(k)$

$$\begin{tikzcd} \tilde{W}(k) \arrow[r] \arrow[d] & \tilde{W}(k) \arrow[d] \\ W(k) \arrow[r, "V"] & W(k) \end{tikzcd}$$

$$(a_0, a_1, a_2, \dots) \mapsto (a_0, a_1^p, a_2^{p^2}, \dots)$$
$$\mapsto (0, a_0, a_1^p, a_2^{p^2}, \dots) \mapsto (0, a_0^{-p}, a_1^{-p}, a_2^{-p}, \dots)$$

Vectores de Witt

$$V \circ F = F \circ V = p$$

Verschiebung in $\tilde{W}(k)$

$$\begin{tikzcd} \tilde{W}(k) \arrow[r] \arrow[d] & \tilde{W}(k) \arrow[d] \\ W(k) \arrow[r, "V"] & W(k) \end{tikzcd}$$

$$V : \tilde{W}(k) \to \tilde{W}(k)$$

$$(a_0, a_1, a_2, \dots) \mapsto (0, a_0^{-p}, a_1^{-p}, a_2^{-p}, \dots)$$

Vectores de Witt

$$V \circ F = F \circ V = p$$

Verschiebung in $\tilde{W}(k)$

$$\begin{tikzcd} \tilde{W}(k) \arrow[r] \arrow[d] & \tilde{W}(k) \arrow[d] \\ W(k) \arrow[r, "V"] & W(k) \end{tikzcd}$$

$$V : \tilde{W}(k) \to \tilde{W}(k)$$

$$(a_0, a_1, a_2, \dots) \mapsto (0, a_0^{-p}, a_1^{-p}, a_2^{-p}, \dots)$$

$$(V \circ F)(\sum_{i=0}^{\infty} f(a_i)p^i) = (F \circ V)(\sum_{i=0}^{\infty} f(a_i)p^i) = \sum_{i=0}^{\infty} f(a_i)p^{i+1} = p\sum_{i=0}^{\infty} f(a_i)p^i$$

Contents

Esquemas en grupos finitos de Witt

Esquema asociado a W_N?

Esquemas en grupos finitos de Witt

Esquema asociado a W_N?

Definición

$$\mathcal{W}_N := \operatorname{Spec} W_N$$

Esquemas en grupos finitos de Witt

Esquema asociado a W_N?

Definición

$$\cancel{\mathcal{W}_N := \operatorname{Spec} W_N}$$

Esquemas en grupos finitos de Witt

Esquemas en grupos finitos de Witt

$X \to S$ esquema sobre S.

Esquemas en grupos finitos de Witt

$X \to S$ esquema sobre S.

Sea $T \to S$ otro esquema sobre S.

Esquemas en grupos finitos de Witt

$X \to S$ 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 conjuto de morfismos de S-esquemas $\{t : T \to X\}$

Esquemas en grupos finitos de Witt

$X \to S$ 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 conjuto de morfismos de S-esquemas $\{t : T \to X\}$

Son equivalentes:

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

Esquemas en grupos finitos de Witt

$X \to S$ 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 conjuto de morfismos de S-esquemas $\{t : T \to X\}$

Son equivalentes:

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

$$\begin{tikzcd} T_1 \arrow[rr] \arrow[dr] & & T_2 \arrow[dl] \\ & S & \end{tikzcd}$$

Esquemas en grupos finitos de Witt

$X \to S$ 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 conjuto de morfismos de S-esquemas $\{t : T \to X\}$

Son equivalentes:

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

$$\begin{tikzcd} T_1 \arrow[rr] \arrow[dr] & & T_2 \arrow[dl] \\ & S & \end{tikzcd} \quad \rightsquigarrow X(T_2) \to X(T_1)$$

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Para darle una estructura de grupo:

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Para darle una estructura de grupo: sea $T \to \mathrm{Spec} k$ otro esquema afín

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Para darle una estructura de grupo: sea $T \to \mathrm{Spec} k$ otro esquema afín

$$(\mathbb{A}_k^N)(T) = \{T \to \mathbb{A}_k^N \text{ morfismo}\}$$

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Para darle una estructura de grupo: sea $T \to \mathrm{Spec} k$ otro esquema afín

$$(\mathbb{A}_k^N)(T) = \{T \to \mathbb{A}_k^N \text{ morfismo}\} \simeq \\ \{k[X_1, \ldots, X_N] \to \Gamma(T, \mathcal{O}_T) \text{ morfismo}\}$$

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Para darle una estructura de grupo: sea $T \to \mathrm{Spec} k$ otro esquema afín

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

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Para darle una estructura de grupo: sea $T \to \mathrm{Spec} k$ otro esquema afín

$$(\mathbb{A}_k^N)(T) = \{(t_1, \ldots, t_N) \in \Gamma(T, \mathcal{O}_T)^N\}$$

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Para darle una estructura de grupo: sea $T \to \mathrm{Spec} k$ otro esquema afín

$$(\mathbb{A}_k^N)(T) = \{(t_1, \ldots, t_N) \in \Gamma(T, \mathcal{O}_T)^N\}$$

Consideremos el morfismo $\oplus$ dado por

$$\begin{aligned} \oplus : \Gamma(T, \mathcal{O}_T)^N \times \Gamma(T, \mathcal{O}_T)^N &\to \Gamma(T, \mathcal{O}_T)^N \\ (a_n)_{n=0}^N, (b_n)_{n=0}^N &\mapsto (a_0 + b_0, \ldots, a_N + b_N)_{n=0}^N \end{aligned}$$

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Para darle una estructura de grupo: sea $T \to \mathrm{Spec} k$ otro esquema afín

$$(\mathbb{A}_k^N)(T) = \{(t_1, \ldots, t_N) \in \Gamma(T, \mathcal{O}_T)^N\}$$

Consideremos el morfismo $\oplus$ dado por

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

Esquemas en grupos finitos de Witt

- k cuerpo perfecto $\mathrm{char}(k) = p$
- $\mathbb{A}_k^N := \mathrm{Spec} k[X_1, \ldots, X_N]$ como esquema

Para darle una estructura de grupo: sea $T \to \mathrm{Spec} k$ otro esquema afín

$$(\mathbb{A}_k^N)(T) = \{(t_1, \ldots, t_N) \in \Gamma(T, \mathcal{O}_T)^N\}$$

Consideremos el morfismo $\oplus$ dado por

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

Definición

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

Esquemas en grupos finitos de Witt

$$F : \mathcal{W}_N \to \mathcal{W}_N$$
$$V : \mathcal{W}_N \to \mathcal{W}_{N+1}$$

Esquemas en grupos finitos de Witt

$$F : \mathcal{W}_N \to \mathcal{W}_N$$
$$V : \mathcal{W}_N \to \mathcal{W}_{N+1}$$

Sean X/S, Y/S dos esquemas en grupos.
Son equivalentes:

- Dar un morfismo de S-esquemas en grupos $X \to Y$.
- Para todo esquema afín $T \to S$, dar un morfismo de grupos $X(T) \to Y(T)$, "funtorialmente en T".

Esquemas en grupos finitos de Witt

$$F : \mathcal{W}_N \to \mathcal{W}_N$$
$$V : \mathcal{W}_N \to \mathcal{W}_{N+1}$$

Sean X/S, Y/S dos esquemas en grupos.
Son equivalentes:

- Dar un morfismo de S-esquemas en grupos $X \to Y$.
- Para todo esquema afín $T \to S$, dar un morfismo de grupos $X(T) \to Y(T)$, "funtorialmente en T".

$$(\mathbb{A}_k^N)(T) = \{(t_1, \ldots, t_N) \in \Gamma(T, \mathcal{O}_T)^N\}$$

Esquemas en grupos finitos de Witt

$$F : \mathcal{W}_N \to \mathcal{W}_N$$
$$V : \mathcal{W}_N \to \mathcal{W}_{N+1}$$

Sean X/S, Y/S dos esquemas en grupos.
Son equivalentes:

- Dar un morfismo de S-esquemas en grupos $X \to Y$.
- Para todo esquema afín $T \to S$, dar un morfismo de grupos $X(T) \to Y(T)$, "funtorialmente en T".

$$(\mathbb{A}_k^N)(T) = \{(t_1, \ldots, t_N) \in \Gamma(T, \mathcal{O}_T)^N\}$$

- $V : (t_1, \ldots, t_N) \mapsto (0, t_1, \ldots, t_N)$
- $F : (t_1, \ldots, t_N) \mapsto (t_1^p, \ldots, t_n^p)$.

Esquemas en grupos finitos de Witt

$$F : \mathcal{W}_N \to \mathcal{W}_N$$
$$V : \mathcal{W}_N \to \mathcal{W}_{N+1}$$

Esquemas en grupos finitos de Witt

$$F : \mathcal{W}_N \to \mathcal{W}_N$$
$$V : \mathcal{W}_N \to \mathcal{W}_{N+1}$$

$$V \circ F = F \circ V = [p]$$

Esquemas en grupos finitos de Witt

$$F : \mathcal{W}_N \to \mathcal{W}_N$$
$$V : \mathcal{W}_N \to \mathcal{W}_{N+1}$$

$$V \circ F = F \circ V = [p]$$

$$0 \longrightarrow \mathcal{W}_r(A) \longrightarrow \mathcal{W}_{N+r}(A) \longrightarrow \mathcal{W}_N(A) \longrightarrow 0$$

Esquemas en grupos finitos de Witt

$$F : \mathcal{W}_N \to \mathcal{W}_N$$
$$V : \mathcal{W}_N \to \mathcal{W}_{N+1}$$

$$V \circ F = F \circ V = [p]$$

$$0 \longrightarrow \mathcal{W}_r(A) \longrightarrow \mathcal{W}_{N+r}(A) \longrightarrow \mathcal{W}_N(A) \longrightarrow 0$$

Como $S_0(X, Y) = X + Y$, $\mathcal{W}_1 \simeq \mathbb{A}^1_k$; por tanto para todo N, $\mathcal{W}_N$ es una "extensión múltiple" de $\mathbb{A}^1_k$

Esquemas en grupos finitos de Witt

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

Esquemas en grupos finitos de Witt

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

Teorema

- Para cada esquema en grupos finito de tipo local-local X existen N, m, r tales que X se sumerge en $(W_N^m)^r$.

Esquemas en grupos finitos de Witt

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

Teorema

- Para cada esquema en grupos finito de tipo local-local X existen N, m, r tales que X se sumerge en $(W_N^m)^r$.
- Existe un pairing no degenerado $W_N^m \times W_m^N \to \mathbb{G}_m(k)$

Esquemas en grupos finitos de Witt

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

Teorema

- Para cada esquema en grupos finito de tipo local-local X existen N, m, r tales que X se sumerge en $(W_N^m)^r$.
- Existe un pairing no degenerado $W_N^m \times W_m^N \to \mathbb{G}_m(k)$

$$\rightsquigarrow W_N^m \simeq (W_m^N)^*$$

Contents

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano,

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano, k cuerpo residual,

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano, k cuerpo residual, $\mathrm{char}(k) = p$.

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano, k cuerpo residual, $\mathrm{char}(k) = p$.
Sea X_0/k un esquema en grupos

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano, k cuerpo residual, $\mathrm{char}(k) = p$.
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 $X \times_R k \to X_0$ de esquemas en grupos sobre k.

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano, k cuerpo residual, $\mathrm{char}(k) = p$.
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 $X \times_R k \to X_0$ de esquemas en grupos sobre k.

A_0/k variedad abeliana

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano, k cuerpo residual, $\mathrm{char}(k) = p$.
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 $X \times_R k \to X_0$ de esquemas en grupos sobre k.

A_0/k variedad abeliana, $A_0(p)$ grupo p-divisible asociado.

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano, k cuerpo residual, $\mathrm{char}(k) = p$.
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 $X \times_R k \to X_0$ de esquemas en grupos sobre k.

A_0/k variedad abeliana, $A_0(p)$ 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.

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano, k cuerpo residual, $\mathrm{char}(k) = p$.
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 $X \times_R k \to X_0$ de esquemas en grupos sobre k.

A_0/k variedad abeliana, $A_0(p)$ 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* de $A_0(p)$ a R es una sucesión de esquemas en grupos $\tilde{A}_{p^n}$ a R, planos, levantamientos de $A_0[p^n]$, y una familia de inyecciones $\tilde{A}_{p^n} \hookrightarrow \tilde{A}_{p^{n+1}}$ que levantan las inclusiones canónicas $A_0[p^n] \hookrightarrow A_0[p^{n+1}]$

Teorema de Serre-Tate

R anillo local, $\mathrm{char} R = 0$, Artiniano, k cuerpo residual, $\mathrm{char}(k) = p$.
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 $X \times_R k \to X_0$ de esquemas en grupos sobre k.

A_0/k variedad abeliana, $A_0(p)$ grupo p-divisible asociado.

Teorema (Serre, Tate)

Existe una equivalencia de categorías entre:

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

Teorema de Serre-Tate

- k cuerpo perfecto, $R = W(k)$, $n \in \mathbb{N}$.

Teorema de Serre-Tate

- k cuerpo perfecto, $R = W(k)$, $n \in \mathbb{N}$.
- $\mu_{p^n}(k) = \mathrm{Spec}\left(k[T]/(T^{p^n} - 1)\right)$.

Teorema de Serre-Tate

- k cuerpo perfecto, $R = W(k)$, $n \in \mathbb{N}$.
- $\mu_{p^n}(k) = \mathrm{Spec}\left(k[T]/(T^{p^n} - 1)\right)$.

Levantamiento natural de $\mu_{p^n}(k)$ a R?

Teorema de Serre-Tate

- k cuerpo perfecto, $R = W(k)$, $n \in \mathbb{N}$.
- $\mu_{p^n}(k) = \mathrm{Spec}\left(k[T]/(T^{p^n} - 1)\right)$.

Levantamiento natural de $\mu_{p^n}(k)$ a R?

$$\mu_{p^n}(R) = \mathrm{Spec}\left(R[T]/(T^{p^n} - 1)\right)$$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana.

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana.

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

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana.

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

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana.

$$A_0[p^n] \simeq \qquad G_{e,l} \quad \times \quad G_{l,e} \quad \times \quad G_{l,l}$$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana.

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

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana.

$$A_0[p^n] \simeq \qquad (\mathbb{Z}/p^n\mathbb{Z})^r \times \mu_{p^n}(k)^s \times G_{l,l}$$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s \times G_{l,l}$$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s \times G_{l,l}$$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

$$A_0 \rightsquigarrow (A_0, (\tilde{A}_{p^n})_n)$$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

$$A_0 \rightsquigarrow (A_0, (\tilde{A}_{p^n})_n)$$

Podemos aplicar la equivalencia de categorías para $R = W(k)/(p)^N$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

$$A_0 \rightsquigarrow (A_0, (\tilde{A}_{p^n})_n) \rightsquigarrow A_N$$

Podemos aplicar la equivalencia de categorías para $R = W(k)/(p)^N$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

$$A_0 \rightsquigarrow (A_0, (\tilde{A}_{p^n})_n) \rightsquigarrow A_N$$

Podemos aplicar la equivalencia de categorías para $R = W(k)/(p)^N$ para cada N

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

$$A_0 \rightsquigarrow (A_0, (\tilde{A}_{p^n})_n) \rightsquigarrow A_N \rightsquigarrow \varprojlim_N A_N$$

Podemos aplicar la equivalencia de categorías para $R = W(k)/(p)^N$ para cada N

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

$$A_0 \rightsquigarrow (A_0, (\tilde{A}_{p^n})_n) \rightsquigarrow A_N \rightsquigarrow \varprojlim_N A_N$$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

$$A_0 \rightsquigarrow (A_0, (\tilde{A}_{p^n})_n) \rightsquigarrow A_N \rightsquigarrow \varprojlim_N A_N := A$$

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

$$A_0 \rightsquigarrow (A_0, (\tilde{A}_{p^n})_n) \rightsquigarrow A_N \rightsquigarrow \varprojlim_N A_N := A$$

A es un esquema en grupos "formal" sobre $W(k)$.

Teorema de Serre-Tate

k cuerpo perfecto, $W(k)$, $n \in \mathbb{N}$.
A_0/k variedad abeliana ordinaria.

$$A_0[p^n] \simeq \qquad (\mu_{p^n}(k)^r)^* \times \mu_{p^n}(k)^s$$

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

$$A_0 \rightsquigarrow (A_0, (\tilde{A}_{p^n})_n) \rightsquigarrow A_N \rightsquigarrow \varprojlim_N A_N := A$$

A es un esquema en grupos "formal" sobre $W(k)$.
A es un esquema en grupos sobre $W(k)$.

Teorema de Serre-Tate

Teorema (Serre, Tate)

Sea k cuerpo perfecto y A_0/k una variedad abeliana ordinaria. Existe un *levantamiento canónico* de A_0 a una variedad abeliana $A/W(k)$.

Teorema de Serre-Tate

Teorema (Serre, Tate)

Sea k cuerpo perfecto y A_0/k una variedad abeliana ordinaria. Existe un *levantamiento canónico* de A_0 a una variedad abeliana $A/W(k)$.

Sea k cuerpo perfecto, 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.

Teorema de Serre-Tate

Teorema (Serre, Tate)

Sea k cuerpo perfecto y A_0/k una variedad abeliana ordinaria. Existe un *levantamiento canónico* de A_0 a una variedad abeliana $A/W(k)$.

Sea k cuerpo perfecto, 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.

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.

Teorema de Serre-Tate

Sara Arias de Reyna

Institut für Experimentelle Mathematik
Universität Duisburg-Essen

24 de Setembre de 2012

STNB 2012

Barcelona