

Eine Woche, ein Beispiel.

4.30 Witt vector

Roadmap.



Castle of Arithmetic Geometry

p -adic
number field

Witt vector

Mordell-Weil theorem

Tate's thesis

Automorphic form

<https://mathoverflow.net/questions/306046/how-to-visualize-a-witt-vector>

Begin: An analog between $K[[t]]$ and \mathbb{Z}_p .

	$K[[t]]$	\mathbb{Z}_p
element	$x = \sum_{i=0}^{\infty} a_i t^i \leftrightarrow \{a_i\}_{i=0}^{\infty} \in K^{\mathbb{N}}$	$x = \sum_{i=0}^{\infty} a_i p^i \leftrightarrow \{a_i\}_{i=0}^{\infty} \in \{0, 1, \dots, p-1\}^{\mathbb{N}}$
addition	$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (c_0, c_1, \dots)$ $c_k = a_k + b_k$	$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (c_0, c_1, \dots)$ $c_k = ?$
multiplication	$(a_0, a_1, \dots)(b_0, b_1, \dots) = (d_0, d_1, \dots)$ $d_k = \sum_{i=0}^k a_i b_{k-i}$	$(a_0, a_1, \dots)(b_0, b_1, \dots) = (d_0, d_1, \dots)$ $d_k = ?$

$\{0, 1, \dots, p-1\}$: not closed under addition and multiplication.

? Can we express c_k as a polynomial of $a_0, a_1, \dots, b_0, b_1, \dots$? No. ☹️

improvement: replace $\{0, 1, \dots, p-1\}^{\mathbb{N}}$ by $\{[0], [1], \dots, [p-1]\}^{\mathbb{N}}$

$$\left[\begin{array}{l} [-]: \mathbb{F}_p \rightarrow \mathbb{Z}_p \text{ s.t. } \textcircled{1} [ab] = [a][b] \Rightarrow [a]^p = [a] \\ \textcircled{2} \mathbb{F}_p \xrightarrow{[-]} \mathbb{Z}_p \xrightarrow{\pi} \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p \text{ is identity} \end{array} \right]$$

$[-]$ is called the Teichmüller lift of \mathbb{F}_p .

Now $\{[0], [1], \dots, [p-1]\}$ is closed under multiplication, and

$$\mathbb{Z}_p \ni x = \sum_{i=0}^{\infty} [a_i] p^i \leftrightarrow \{a_i\}_{i=0}^{\infty} \in \mathbb{F}_p^{\mathbb{N}}$$

induces the natural algebraic ring structure on $\mathbb{F}_p^{\mathbb{N}}$:

$$(a_0, a_1, a_2, a_3, \dots) + (b_0, b_1, b_2, b_3, \dots) = (c_0, c_1, c_2, c_3, \dots)$$

$$c_0 = a_0 + b_0$$

$$c_1 = a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - c_0^p)$$

$$= a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - (a_0 + b_0)^p)$$

$$c_2 = a_2 + b_2 + \frac{1}{p} \left\{ a_1^p + b_1^p - c_1^p + \frac{1}{p} \{ a_0^{p^2} + b_0^{p^2} - c_0^{p^2} \} \right\}$$

$$= a_2 + b_2 + \frac{1}{p} \left\{ a_1^p + b_1^p - \left\{ a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - (a_0 + b_0)^p) \right\}^p + \frac{1}{p} \{ a_0^{p^2} + b_0^{p^2} - (a_0 + b_0)^{p^2} \} \right\}$$

$$c_3 = a_3 + b_3 + \frac{1}{p} \left\{ a_2^p + b_2^p - c_2^p + \frac{1}{p} \{ a_1^{p^2} + b_1^{p^2} - c_1^{p^2} + \frac{1}{p} \{ a_0^{p^3} + b_0^{p^3} - c_0^{p^3} \} \} \right\}$$

$$= a_3 + b_3 + \frac{1}{p} \left\{ a_2^p + b_2^p - \left\{ a_2 + b_2 + \frac{1}{p} \left\{ a_1^p + b_1^p - \left\{ a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - (a_0 + b_0)^p) \right\}^p + \frac{1}{p} \{ a_0^{p^2} + b_0^{p^2} - (a_0 + b_0)^{p^2} \} \right\}^p + \frac{1}{p} \{ a_1^{p^2} + b_1^{p^2} - \left\{ a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - (a_0 + b_0)^p) \right\}^p + \frac{1}{p} \{ a_0^{p^3} + b_0^{p^3} - (a_0 + b_0)^{p^3} \} \right\}^p \right\}$$

$$(a_0, a_1, a_2, a_3, \dots) \times (b_0, b_1, b_2, b_3, \dots) = (d_0, d_1, d_2, d_3, \dots)$$

$$d_0 = a_0 b_0$$

$$d_1 = a_0 b_1 + a_1 b_0$$

$$d_2 = \sum_{i=0}^2 a_i b_{2-i} + \frac{1}{p} \left\{ \sum_{i=0}^1 (a_i b_{1-i})^p - d_1^p \right\}$$

$$= \sum_{i=0}^2 a_i b_{2-i} + \frac{1}{p} \left\{ \sum_{i=0}^1 (a_i b_{1-i})^p - (a_0 b_1 + a_1 b_0)^p \right\}$$

$$d_3 = \sum_{i=0}^3 a_i b_{3-i} + \frac{1}{p} \left\{ \sum_{i=0}^2 (a_i b_{2-i})^p - d_2^p + \frac{1}{p} \left\{ \sum_{i=0}^1 (a_i b_{1-i})^{p^2} - d_1^{p^2} \right\} \right\}$$

$$= \sum_{i=0}^3 a_i b_{3-i} + \frac{1}{p} \left\{ \sum_{i=0}^2 (a_i b_{2-i})^p - \left\{ \sum_{i=0}^2 a_i b_{2-i} + \frac{1}{p} \left\{ \sum_{i=0}^1 (a_i b_{1-i})^p - (a_0 b_1 + a_1 b_0)^p \right\} \right\}^p + \frac{1}{p} \left\{ \sum_{i=0}^1 (a_i b_{1-i})^{p^2} - (a_0 b_1 + a_1 b_0)^{p^2} \right\} \right\}$$

Partial proof.

$$k=0: [c_0] \equiv [a_0] + [b_0]$$

$$\Rightarrow c_0 = a_0 + b_0$$

$$\text{mod } p \quad \textcircled{1}$$

$$\text{in } \mathbb{F}_p$$

$$k=1: [c_0] + [c_1]p \equiv [a_0] + [b_0] + ([a_1] + [b_1])p$$

$$\Rightarrow [c_1] \equiv [a_1] + [b_1] + \frac{1}{p} \{ [a_0] + [b_0] - [c_0] \}$$

$$\text{mod } p^2$$

$$\equiv [a_1] + [b_1] + \frac{1}{p} \{ [a_0] + [b_0] - ([a_0] + [b_0])^p \}$$

$$\text{mod } p^2 \quad \textcircled{2}$$

$$\left[\text{where } \textcircled{1} \Rightarrow [c_0] = [c_0]^p \equiv ([a_0] + [b_0])^p \right]$$

$$\text{mod } p^2$$

$$\Rightarrow c_1 = a_1 + b_1 + \frac{1}{p} \{ a_0^p + b_0^p - (a_0 + b_0)^p \}$$

$$k=2: [c_0] + [c_1]p + [c_2]p^2 \equiv [a_0] + [b_0] + ([a_1] + [b_1])p + ([a_2] + [b_2])p^2 \text{ mod } p^3$$

$$\Rightarrow [c_2] \equiv [a_2] + [b_2] + \frac{1}{p} \left\{ [a_1] + [b_1] - [c_1] + \frac{1}{p} \{ [a_0] + [b_0] - [c_0] \} \right\} \text{ mod } p^3$$

$$\equiv [a_2] + [b_2] + \frac{1}{p} \left\{ [a_1] + [b_1] - \left\{ [a_1] + [b_1] + \frac{1}{p} \{ [a_0] + [b_0] - ([a_0] + [b_0])^p \} \right\}^p + \frac{1}{p} \{ [a_0] + [b_0] - ([a_0] + [b_0])^p \} \right\} \text{ mod } p^3 \quad \textcircled{3}$$

$$\left[\text{where } \textcircled{1} \Rightarrow [c_0] = [c_0]^{p^2} \equiv ([a_0] + [b_0])^{p^2} \text{ mod } p^3 \right]$$

$$\textcircled{2} \Rightarrow [c_1] = [c_1]^p \equiv \left\{ [a_1] + [b_1] + \frac{1}{p} \{ [a_0] + [b_0] - ([a_0] + [b_0])^p \} \right\}^p \text{ mod } p^3$$

$$\Rightarrow c_2 = a_2 + b_2 + \frac{1}{p} \left\{ a_1^p + b_1^p - \left\{ a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - (a_0 + b_0)^p) \right\}^p + \frac{1}{p} \{ a_0^{p^2} + b_0^{p^2} - (a_0 + b_0)^{p^2} \} \right\}$$

It also applies to $\mathbb{Z}_p[\{q_i\}]$: $q = p^d, d \in \mathbb{Z}_{\geq 0}$

$$\text{Verify: } \textcircled{1} \mathbb{F}_p[\{q_i\}] = \mathbb{F}_q$$

$$\textcircled{2} \mathcal{O}_K = \mathbb{Z}_p[\{q_i\}]$$

$\textcircled{3} K/\mathbb{Q}_p$ is the unique unramified extension of degree d

$$K = \mathbb{Q}_p[\{q_i\}] \longrightarrow \mathbb{Q}_p$$

$$\mathcal{O}_K = \mathbb{Z}_p[\{q_i\}] \longrightarrow \mathbb{Z}_p$$

$$\mathcal{O}_K/\mathfrak{p} \mathcal{O}_K = \mathbb{F}_p[\{q_i\}] = \mathbb{F}_q \longrightarrow \mathbb{F}_p$$

$$\mathbb{Z}_p[\{q_i\}] \ni x = \sum_{i=0}^{\infty} [a_i] p^i \longleftrightarrow \{a_i\}_{i=0}^{\infty} \in \mathbb{F}_q^{\mathbb{N}}$$

induces the natural algebraic ring structure on $\mathbb{F}_p^{\mathbb{N}}$: $c_K \in \mathbb{Z}[a_0, \dots, a_k, b_0, \dots, b_k]$

$$\left[\begin{array}{l} [-]: \mathbb{F}_q \rightarrow \mathbb{Z}_p[\xi_{q-1}] \text{ s.t. } \textcircled{1} [ab] = [a][b] \Rightarrow [a]^q = [a] \\ \textcircled{2} \mathbb{F}_q \xrightarrow{[-]} \mathbb{Z}_p[\xi_{q-1}] \xrightarrow{\pi} \mathbb{Z}_p[\xi_{q-1}]/_p \mathbb{Z}_p[\xi_{q-1}] \cong \mathbb{F}_q \text{ is identity} \end{array} \right] \left[\begin{array}{l} (-)^{p^i}: \mathbb{F}_q \xrightarrow{(-)^p} \mathbb{F}_q \\ \downarrow \mathbb{F}_p \end{array} \right]$$

$[-]$ is called the Teichmüller lift of \mathbb{F}_q

$$(a_0, a_1, a_2, a_3, \dots) + (b_0, b_1, b_2, b_3, \dots) = (c_0, c_1, c_2, c_3, \dots)$$

$$c_0 = a_0 + b_0$$

$$c_1 = a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - c_0^p)$$

$$= a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - (a_0 + b_0)^p)$$

$$c_2 = a_2 + b_2 + \frac{1}{p} \left\{ a_1^p + b_1^p - c_1^p + \frac{1}{p} \{ a_0^{p^2} + b_0^{p^2} - c_0^{p^2} \} \right\}$$

$$= a_2 + b_2 + \frac{1}{p} \left\{ a_1^p + b_1^p - \left\{ a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - (a_0 + b_0)^p) \right\}^p + \frac{1}{p} \{ a_0^{p^2} + b_0^{p^2} - (a_0 + b_0)^{p^2} \} \right\}$$

$$c_3 = a_3 + b_3 + \frac{1}{p} \left\{ a_2^p + b_2^p - c_2^p + \frac{1}{p} \left\{ a_1^{p^2} + b_1^{p^2} - c_1^{p^2} + \frac{1}{p} \{ a_0^{p^3} + b_0^{p^3} - c_0^{p^3} \} \right\} \right\}$$

$$= a_3 + b_3 + \frac{1}{p} \left\{ a_2^p + b_2^p - \left\{ a_2 + b_2 + \frac{1}{p} \left\{ a_1^p + b_1^p - \left\{ a_1 + b_1 + \frac{1}{p} (a_0^p + b_0^p - (a_0 + b_0)^p) \right\}^p + \frac{1}{p} \{ a_0^{p^2} + b_0^{p^2} - (a_0 + b_0)^{p^2} \} \right\}^p + \frac{1}{p} \{ a_0^{p^3} + b_0^{p^3} - (a_0 + b_0)^{p^3} \} \right\} \right\}$$

$$(a_0, a_1, a_2, a_3, \dots) \times (b_0, b_1, b_2, b_3, \dots) = (d_0, d_1, d_2, d_3, \dots)$$

$$d_0 = a_0 b_0$$

$$d_1 = a_0^p b_1 + a_1 b_0^p$$

$$d_2 = \sum_{i=0}^2 a_i^{p^i} b_{2-i}^{p^i} + \frac{1}{p} \left\{ \sum_{i=0}^2 (a_i^{p^i} b_{1-i}^{p^i})^p - d_1^p \right\}$$

$$= \sum_{i=0}^2 a_i^{p^i} b_{2-i}^{p^i} + \frac{1}{p} \left\{ \sum_{i=0}^2 (a_i^{p^i} b_{1-i}^{p^i})^p - (a_0^p b_1 + a_1 b_0^p)^p \right\}$$

$$d_3 = \sum_{i=0}^3 a_i^{p^i} b_{3-i}^{p^i} + \frac{1}{p} \left\{ \sum_{i=0}^3 (a_i^{p^i} b_{2-i}^{p^i})^p - d_2^p + \frac{1}{p} \left\{ \sum_{i=0}^2 (a_i^{p^i} b_{1-i}^{p^i})^{p^2} - d_1^{p^2} \right\} \right\}$$

$$= \sum_{i=0}^3 a_i^{p^i} b_{3-i}^{p^i} + \frac{1}{p} \left\{ \sum_{i=0}^3 (a_i^{p^i} b_{2-i}^{p^i})^p - \left\{ \sum_{i=0}^2 a_i^{p^i} b_{2-i}^{p^i} + \frac{1}{p} \left\{ \sum_{i=0}^2 (a_i^{p^i} b_{1-i}^{p^i})^p - (a_0^p b_1 + a_1 b_0^p)^p \right\}^p + \frac{1}{p} \left\{ \sum_{i=0}^2 (a_i^{p^i} b_{1-i}^{p^i})^{p^2} - (a_0^p b_1 + a_1 b_0^p)^{p^2} \right\} \right\} \right\}$$

These polynomial comes from some "generating function".

$$f_X(t) := \prod_{k=1}^{\infty} (1 - X_k t^k) \in \mathbb{Z}[X_1, X_2, \dots][[t]]$$

$$\text{let } X^{(N)} := \sum_{i \in \mathbb{N}} i X_i^{N/i} \quad N \in \mathbb{N}^+ \text{ then}$$

$$f_X(t) = \exp \left(- \sum_{N=1}^{\infty} \frac{1}{N} X^{(N)} t^N \right)$$

$$X^{(1)} = X_1$$

$$X^{(2)} = X_1^2 + 2X_2$$

$$X^{(3)} = X_1^3 + 3X_2 X_1 + 3X_3$$

$$X^{(4)} = X_1^4 + 2X_2^2 + 4X_2 X_1 + 6X_4$$

$$X^{(5)} = X_1^5 + 5X_2 X_1^2 + 5X_3 X_1 + 5X_5$$

$$X^{(6)} = X_1^6 + 2X_2^3 + 3X_2^2 X_1 + 6X_3 X_1^2 + 6X_4 X_1 + 6X_6$$

let $f_z(t) = f_x(t) f_y(t) \Rightarrow Z^{(N)} = X^{(N)} + Y^{(N)}$

then

$$\begin{aligned} Z_1 &= X_1 + Y_1 \\ Z_2 &= X_2 + Y_2 - X_1 Y_1 \\ Z_3 &= X_3 + Y_3 + \frac{1}{2} \{X_1^2 + Y_1^2 - (X_1 + Y_1)^2\} \\ Z_4 &= X_4 + Y_4 + \frac{1}{2} \left\{ X_2^2 + Y_2^2 - \{X_2 + Y_2 - X_1 Y_1\}^2 \right. \\ &\quad \left. + \frac{1}{2} \{X_1^2 + Y_1^2 - (X_1 + Y_1)^2\} \right\} \\ Z_p &= X_p + Y_p + \frac{1}{p} \{X_1^p + Y_1^p - (X_1 + Y_1)^p\} \\ Z_{p^2} &= X_{p^2} + Y_{p^2} + \frac{1}{p} \left\{ X_p^p + Y_p^p - \{X_p + Y_p + \frac{1}{p} \{X_1^p + Y_1^p - (X_1 + Y_1)^p\}\}^p \right. \\ &\quad \left. + \frac{1}{p} \{X_1^p + Y_1^p - (X_1 + Y_1)^p\} \right\} \end{aligned}$$

let $f_v(t) = \exp(-\sum_{N=1}^{\infty} \frac{1}{N} X^{(N)} Y^{(N)} t^N) \Rightarrow V^{(N)} = X^{(N)} Y^{(N)}$

then

$$\begin{aligned} V_1 &= X_1 Y_1 \\ V_p &= p X_p Y_p + X_1^p Y_1 + X_p Y_1^p \\ V_{p^2} &= p^2 X_{p^2} Y_{p^2} + p (X_p^p Y_p + X_{p^2} Y_p^p) + X_1^{p^2} Y_{p^2} + X_p^p Y_p^p + X_{p^2} Y_1^p \\ &\quad + \frac{1}{p} \{X_1^{p^2} Y_1^p + X_p^p Y_{p^2} - W_p^p\} \end{aligned}$$

This makes $\text{Spec } \mathbb{Z}[X_1, X_2, \dots]$ the structure of ring scheme.

where

$$\begin{aligned} +: \quad \mathbb{Z}[Z_1, Z_2, \dots] &\longrightarrow \mathbb{Z}[X_1, X_2, \dots] \otimes_{\mathbb{Z}} \mathbb{Z}[Y_1, Y_2, \dots] \\ Z_n &\longmapsto Z_n(X_1, \dots, X_n, Y_1, \dots, Y_n) \\ \times: \quad \mathbb{Z}[V_1, V_2, \dots] &\longrightarrow \mathbb{Z}[X_1, X_2, \dots] \otimes_{\mathbb{Z}} \mathbb{Z}[Y_1, Y_2, \dots] \\ V_n &\longmapsto V_n(X_1, \dots, X_n, Y_1, \dots, Y_n) \end{aligned}$$

denote $W_{\infty} = \text{Spec } \mathbb{Z}[X_1, X_2, \dots]$ universal Witt scheme

ring scheme structures $\left\{ \begin{aligned} W_n &= \text{Spec } \mathbb{Z}[X_1, X_2, \dots, X_n] && n\text{-truncated Witt scheme} \\ W_{\infty, p} &= \text{Spec } \mathbb{Z}[X_1, X_p, X_{p^2}, \dots] && p\text{-typical Witt scheme} \\ W_{m, p} &= \text{Spec } \mathbb{Z}[X_1, X_p, X_{p^2}, \dots, X_{p^{m-1}}] && m\text{-truncated } p\text{-typical Witt scheme} \end{aligned} \right.$

are induced by the quotient map

denote $W(S) := \text{Hom}_{\Sigma_{\text{ch}}} (S, W) = \prod H^0(S, \mathcal{O}_S)$, $S \in \text{Sch}/\mathbb{Z}$

then $W(S)$ has the ring structure

E.g. $W_{\infty, p}(\mathbb{F}_p) = \mathbb{F}_p^{\mathbb{N}} \cong \mathbb{Z}_p$

$W_{\infty, p}(\mathbb{F}_q) = \mathbb{F}_q^{\mathbb{N}} \cong \mathbb{Z}_p[\zeta_{q-1}]$

$$\left\{ \text{finite extension } \mathbb{F}_p \right\} \xrightleftharpoons[W_{\infty, p}]{\text{alg integral ring } / \mathbb{Z}_p} \left\{ \text{unramified} \right\} \xrightleftharpoons[\mathbb{Q}_k \leftarrow K]{R \mapsto K(R)} \left\{ \text{unramified extension } / \mathbb{Q}_p \right\}$$

$\mathbb{Q}_k / \mathbb{Q}_k \leftarrow \mathbb{Q}_k$