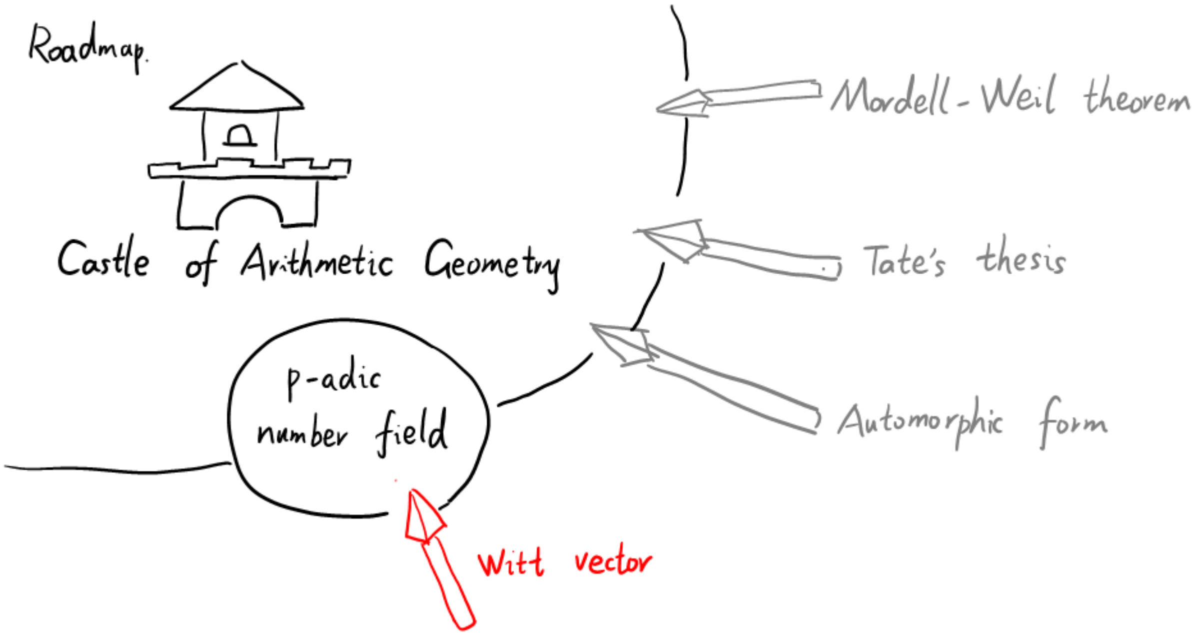
Eine Woche, ein Beispiel.

4.30 Witt vector

Roadmap.



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

Ref:
http://www.claymath.org/sites/default/files/brinon_witt.pdf
https://arxiv.org/pdf/1409.7445.pdf

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

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

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

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

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

[$[-]:\ \mathbb{F}_p \longrightarrow \mathbb{Z}_p$ s.t. ① $[ab]=[a][b]$ $\Rightarrow [a]^p=[a]$

② $\mathbb{F}_p \xrightarrow{[-]} \mathbb{Z}_p \xrightarrow{\pi} \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ is identity

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

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

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

$c_k \in \mathbb{Z}[a_0,\cdots a_k, b_0,\cdots b_k]$

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

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

$$c_0 = a_0+b_0$$

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

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

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

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

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

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

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

$$d_0 = a_0 b_0$$

$$d_1 = a_0 b_1 + a_1 b_0$$

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

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

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

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

Partial proof.

$k=0$: $[c_0] \equiv [a_0] + [b_0]$ mod p ①

$\Rightarrow c_0 = a_0 + b_0$ in $\mathbb{F}_p$

$k=1$: $[c_0] + [c_1]p \equiv [a_0] + [b_0] + ([a_1] + [b_1])p$ mod p^2

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

$\equiv [a_1] + [b_1] + \frac{1}{p}\{[a_0] + [b_0] - ([a_0] + [b_0])^p\}$ mod p^2 ②

[where ① $\Rightarrow [c_0] = [c_0]^p \equiv ([a_0] + [b_0])^p$ mod p^2]

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

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

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

$$\equiv [a_2] + [b_2] + \frac{1}{p}\left\{ \begin{array}{l} [a_1] + [b_1] - \left\{[a_1] + [b_1] + \frac{1}{p}\{[a_0] + [b_0] - ([a_0] + [b_0])^p\}\right\}^p \\ + \frac{1}{p}\{[a_0] + [b_0] - ([a_0] + [b_0])^{p^2}\} \end{array} \right\} \quad ③$$

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

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

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

It also applies to $\mathbb{Z}_p[\zeta_{q-1}]$. $q = p^d$, $d \in \mathbb{Z}_{\geq 0}$

[Verify: ① $\mathbb{F}_p[\zeta_{q-1}] = \mathbb{F}_q$

② $\mathcal{O}_K = \mathbb{Z}_p[\zeta_{q-1}]$

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

$K = \mathbb{Q}_p[\zeta_{q-1}] — \mathbb{Q}_p$

$\mathcal{O}_K = \mathbb{Z}_p[\zeta_{q-1}] — \mathbb{Z}_p$

$\mathcal{O}_K / p\mathcal{O}_K = \mathbb{F}_p[\zeta_{q-1}] = \mathbb{F}_q — \mathbb{F}_p$

$$\mathbb{Z}_p[\zeta_{q-1}] \ni x = \sum_{i=0}^{\infty} [a_i]^{p^{-i}} p^i \longleftrightarrow \{a_i\}_{i=0}^{\infty} \in \mathbb{F}_q^{\mathbb{N}}$$

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

$[-] : \mathbb{F}_q \longrightarrow \mathbb{Z}_p[\zeta_{q-1}]$ s.t ① $[ab] = [a][b]$ $\Rightarrow [a]^q = [a]$

② $\mathbb{F}_q \xrightarrow{[-]} \mathbb{Z}_p[\zeta_{q-1}] \xrightarrow{\pi} \mathbb{Z}_p[\zeta_{q-1}]/p\mathbb{Z}_p[\zeta_{q-1}] \cong \mathbb{F}_q$ is identity

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

$$(-)^{p^{-1}} : \begin{tikzcd} \mathbb{F}_q \arrow[r, shift left, "(-)^p"] \arrow[dr] & \mathbb{F}_q \arrow[l, shift left, "(-)^{p^{-1}}"] \arrow[dl] \\ & \mathbb{F}_p \end{tikzcd}$$

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

$$c_0 = a_0 + b_0$$

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

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

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

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

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

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

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

$$d_0 = a_0 b_0$$

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

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

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

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

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

These polynomial comes from some "generatering function".

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

let $X^{(N)} := \sum_{l \mid N} l X_l^{N/l}$ $N \in \mathbb{N}^+$. then

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

$X^{(1)} = X_1$

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

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

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

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

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

let $f_Z(t) = f_X(t)\, f_Y(t)$ $\Rightarrow Z^{(N)} = X^{(N)} + Y^{(N)}$

then
$$Z_1 = X_1 + Y_1$$
$$Z_2 = X_2 + Y_2 - X_1Y_1$$
$$Z_3 = X_3 + Y_3 + \frac{1}{3}\{X_1^3 + Y_1^3 - (X_1+Y_1)^3\}$$
$$Z_4 = X_4 + Y_4 + \frac{1}{2}\left\{X_2^2 + Y_2^2 - \{X_2+Y_2-X_1Y_1\}^2 + \frac{1}{2}\{X_1^4+Y_1^4-(X_1+Y_1)^4\}\right\}$$
$$Z_p = X_p + Y_p + \frac{1}{p}\{X_1^p + Y_1^p - (X_1+Y_1)^p\}$$
$$Z_{p^2} = X_{p^2} + Y_{p^2} + \frac{1}{p}\left[X_p^p + Y_p^p - \left\{X_p + Y_p + \frac{1}{p}\{X_1^p + Y_1^p - (X_1+Y_1)^p\}\right\}^p + \frac{1}{p}\{X_1^p + Y_1^p - (X_1+Y_1)^p\}\right]$$

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

then
$$V_1 = X_1Y_1$$
$$V_p = pX_pY_p + X_1^pY_p + X_pY_1^p$$
$$V_{p^2} = p^2X_{p^2}Y_{p^2} + p(X_p^pY_{p^2} + X_{p^2}Y_p^p) + X_1^{p^2}Y_{p^2} + X_p^pY_p^p + X_{p^2}Y_1^{p^2} + \frac{1}{p}\{X_1^{p^2}Y_p^p + X_p^pY_1^{p^2} - W_p^p\}$$

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

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

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

ring scheme structures are induced by the quotient map

$W_n = \operatorname{Spec} \mathbb{Z}[X_1, X_2, \cdots, X_n]$ n-truncated Witt scheme

$W_{\infty,p} = \operatorname{Spec} \mathbb{Z}[X_1, X_p, X_{p^2}, \cdots]$ p-typical Witt scheme

$W_{m,p} = \operatorname{Spec} \mathbb{Z}[X_1, X_p, X_{p^2}, \cdots X_{p^{m-1}}]$ m-truncated p-typical Witt scheme

denote $W_\cdot(S) := \operatorname{Hom}_{Sch}(S, W_\cdot) = \prod H^0(S, \mathcal{O}_S)$, $S \in Sch/\mathbb{Z}$

then $W_\cdot(S)$ has the ring structure

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

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

$$\{\text{alg extension}/\mathbb{F}_p\} \underset{\mathcal{O}_K/m\mathcal{O}_K \leftarrow\!\shortmid\, \mathcal{O}_K}{\overset{W_{\infty,p}}{\rightleftarrows}} \left\{\begin{matrix}\text{alg integral ring}/\mathbb{Z}_p \\ \text{unramified}\end{matrix}\right\} \underset{\mathcal{O}_K \leftarrow\!\shortmid\, K}{\overset{R \mapsto K(R)}{\rightleftarrows}} \{\text{unramified extension}/\mathbb{Q}_p\}$$

Non-commutative case: https://web.math.ku.dk/~larsh/papers/006/paper.pdf

[FingpSch, Ex 10.16] Let k be a perfect field, char $k \triangleq p > 0$.
$\exists!$ cpl DVR R with char $R = 0$, $m = \langle p \rangle$, $R/m \cong k$. $R = W_{\infty,p}(k)$