Witt Vectors, Lifting Problems and Moduli Spaces of Curves

Andrew Kobin (akobin@ucsc.edu)

Begonia

Poppy

Characteristic 0 vs. Characteristic p

Characteristic 0

$1 + 1 + 1 + \cdots$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p,$ etc. are infinite

$(x+y)^n =$ 

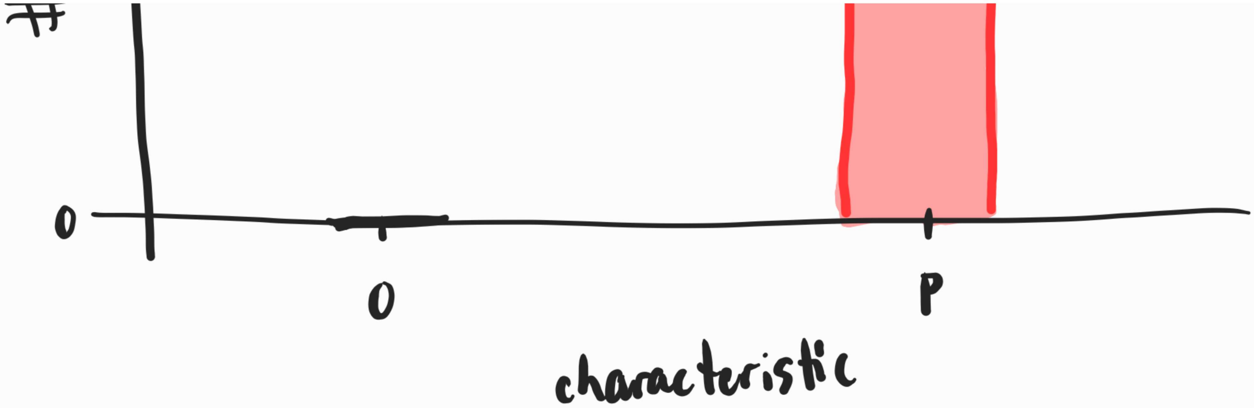
Characteristic p

$\underbrace{1 + 1 + \cdots 1}_{p} = 0$

there are finite fields! $|\mathbb{F}_q| = q$

$(x+y)^p = x^p + y^p$

Number of Riemann Hypotheses Proven



$\pi_1^{\text{ét}}(\mathbb{A}^1) = \{1\}$ $\pi_1^{\text{ét}}(\mathbb{A}^1) =$ ¯_(ツ)_/¯

Witt Vectors

Motivation: recall that the ring of p-adic integers are defined by $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

(a_n)

Want to think of $(a_n) \in \mathbb{Z}_p$ as a "p-adic power series"

$$\sum_{n=0}^{\infty} a_n p^n .$$

Problem: addition and multiplication are <u>not</u> just power series addition and multiplication.

e.g. $\ldots + (p-1)p^n + a_{n+1}p^{n+1} + \ldots$

$$+ \quad \cdots + 1p^n \Big/ + b_{n+1}p^{n+1} + \cdots$$
$$\overline{\qquad\qquad p^{n+1} \qquad\qquad}$$

$$= \quad \cdots \quad 0p^n + (a_{n+1} + b_{n+1} + \underline{\underline{1}})p^{n+1} \cdots$$

Elegant solution: endow the space of sequences (a_n) with a new ring structure $\rightsquigarrow$ Witt vectors.

$\boxed{\text{Def}}$ (ish) Let A be any commutative ring. The **ring of Witt vectors** over A, $\mathbb{W}(A)$, is the set

$$\mathbb{W}(A) = \{(a_0, a_1, a_2, \dots) \mid a_n \in A\}$$

together with addition and multiplication

$$(\underline{a_0, a_1, \dots}) + (\underline{b_0, b_1, \dots}) = (\underline{S_0(a_0, b_0)}, \underline{S_1(a_0, a_1, b_0, b_1)}, \dots)$$

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (P_0\underline{(a_0, b_0)}, P_1\underline{(a_0, a_1, b_0, b_1)}, \dots)$$

for certain symmetric polynomials

$$S_i = X_i + Y_i + \dots$$

$$P_i = X_i Y_i + \dots$$

e.g. $S_0 = X_0 + Y_0$

$$S_1 = X_1 + Y_1 + \frac{1}{p}\left(X_0^p + Y_0^p - (X_0 + Y_0)^p\right)$$

etc.

Better def? $\mathbb{W}(A)$ can be given its ring structure by establishing

$$\mathbb{W}(A) \longleftrightarrow (1+tA[[t]], \cdot)$$

$$(a_n) \longmapsto \prod_{n=1}^{\infty} (1-\tilde{a}_n t^n)$$

addition:

$$\left(\sum b_n t^n\right)\left(\sum c_n t^n\right)$$

multiplication:

$$(1-bt)\cdot(1-ct) = (1-bct)$$

For our purposes, the following facts will be enough to understand $\mathbb{W}(A)$:

(1) For any A, $\mathbb{W}(A)$ is a ring of characteristic 0.

(2) $\mathbb{W}(\mathbb{F}_p) \cong \mathbb{Z}_p$ as rings

$$(a_n) \longmapsto (a_n)$$

(3) If k is a field of char. p, the Frobenius

$$\begin{aligned} k &\longrightarrow k \\ x &\longmapsto x^p \end{aligned}$$

extends to a ring map

$$F : \mathbb{W}(k) \longrightarrow \mathbb{W}(k)$$

$$(a_0, a_1, \dots) \longmapsto \underline{(a_0^p, a_1^p, \dots)}$$

(4) $\mathbb{W}$ is a functor

$$\mathrm{Alg}_k \longrightarrow \mathrm{CommRing}$$
$$A \longmapsto \mathbb{W}(A).$$

Therefore we have defined an <u>affine</u> <u>ring</u> <u>scheme</u> $\mathbb{W}$.

(5) $\mathbb{W} \cong \varprojlim \mathbb{W}_n$ where

$$\mathbb{W}_n(A) = \{(a_0, a_1, \dots, a_{n-1})\}$$

$$\mathbb{W}_{n+1} \longrightarrow \mathbb{W}_n$$
$$(a_0, \dots, a_n) \longmapsto (a_0, \dots, a_{n-1})$$

e.g. $\mathbb{W}_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$.

e.g. $W(\mathbb{F}_p) \cong \mathbb{Z}_p$

Punchline: $\mathbb{W}$ provides a way of lifting rings in char. $p > 0$ to rings in char. 0.

Of course this extends much further, allowing us to lift:

- λ-ring structures
- field extensions
- varieties, schemes, stacks and morphisms between them

Lifting Field Extensions

Recall from Galois theory that a cyclic degree n Galois extension is of the form

$$L = K[x]/(x^n - f), \quad f \in K^\times.$$

$\mu_n \in K$

Kummer Theory:

$$\left\{\begin{matrix}\text{cyclic deg.} \\ n \text{ extensions}\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} K^\times / K^{\times n}$$

$$L = K(\sqrt[n]{f}) \longleftarrow\!\shortmid \; f$$

However, this fails in char. $p > 0$.

Instead, every deg. p Galois ext. is of the form

$$L = K[x]/(x^p - x - f), \quad f \in K.$$

Artin–Schreier Theory:

$$\left\{ \begin{matrix} \text{cyclic deg. } p \\ \text{extensions} \end{matrix} \right\} \overset{1:1}{\longleftrightarrow} K/\wp(K)$$

$\wp(K) = \{a^p - a\}$

$$L = K(\wp^{-1}(f)) \longleftarrow\!\shortmid f$$

Further complication: classifying these extensions up to isomorphism requires finer invariants.

$\mathbb{F}_q((t))$, ~~$\mathbb{Q}_p$~~

$\boxed{\text{Ex}}$ If K is a local field of char. p with valuation v, then there is an invariant called the ramification jump, e.g. for $L = K(\wp^{-1}(\alpha))$,

$x^p - x - \alpha$

jump $= -v(\alpha)$

Takeaway: cyclic $\mathbb{Z}/p\mathbb{Z}$-extensions are governed by $K/\wp(K) = \mathbb{W}_1(K)/\wp(\mathbb{W}_1(K))$.

$$\wp : \mathbb{W}(k) \longrightarrow \mathbb{W}(k)$$
$$a \longmapsto Fa - a$$
$$(a_i) \longmapsto (a_i^p) - (a_i)$$

For cyclic $\mathbb{Z}/p^n\mathbb{Z}$-extensions, we have:

Theorem (Artin–Schreier–Witt)

For a field K of characteristic $p > 0$ and any $n \geq 1$,

$$\left\{ \begin{matrix} \text{cyclic } \mathbb{Z}/p^n\mathbb{Z}\text{-ext's} \\ L/K \end{matrix} \right\} \xleftrightarrow{1:1} \mathbb{W}_n(K)/\wp\,\mathbb{W}_n(K)$$

$$L = K(\wp^{-1}(\underline{a})) \longleftarrow\!\!\mapsto \underline{a} = (a_0, \dots, a_{n-1}).$$

Application: can construct extensions of $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$ by lifting towers of cyclic extensions $\dots \supseteq K_n \supseteq \dots \supseteq K_1 \supseteq \mathbb{F}_p$.

Lifting Curves: Garuti's Compactification

Let $\varphi : Y \longrightarrow X$ be a Galois cover of curves over a field k of characteristic $p > 0$, with group

$$G = \mathrm{Gal}(Y/X) \cong \mathbb{Z}/p^n\mathbb{Z}.$$