The Theory of Witt-vectors

- **Main example: p-adic numbers**

Fix $p \in \mathbb{Z}$ prime; write $\forall\, x \in \mathbb{Q}^\times \quad x = p^n \cdot \frac{a}{b}$ with

$$p \nmid a, \quad p \nmid b.$$

Def $|x|_p := p^{-n}$ & $|0|_p := 0$ — p-adic abs value

Check: $\cdot\ |x|_p \geq 0 \quad \forall\, x \in \mathbb{Q}$

$\cdot\ |x|_p = 0 \iff x = 0$

$\cdot\ |xy|_p = |x|_p\,|y|_p$

$\cdot\ |x+y|_p \leq \max\{|x|_p, |y|_p\}$ — non-archimedean

Easy: $|x|_p \neq |y|_p \Rightarrow |x+y|_p = \max\{|x|_p, |y|_p\}$

Def
$$\mathbb{Q}_p = \frac{\{\text{Cauchy seq}^{\text{in}}\mathbb{Q} \text{ w.r.t } |\cdot|_p\}}{\{\text{null-seq wrt } |\cdot|_p\}}$$

i.e. the completion of $\mathbb{Q}$ wrt $|\cdot|_p$.

Prop If $(a_m) \not\to 0$ is Cauchy (wrt $|\cdot|_p$)
then $\exists\, N \in \mathbb{N}$ s.t. $|a_m|_p = |a_m|_p \quad \forall\, m, m \geq N$.

Pf
- $\forall\, \varepsilon > 0\ \exists\, N_\varepsilon > 0 \quad \forall\, m, n \geq N_\varepsilon \quad |a_m - a_n|_p < \varepsilon$
- $(a_m) \not\to 0 \Rightarrow \exists\, \varepsilon_0 > 0$ s.t. $\forall N \quad \exists\, m_0 > N$ s.t. $|a_{m_0}| \geq \varepsilon_0$

If $m > N_{\varepsilon_0} \Rightarrow |a_m|_p = |a_m - a_{m_0} + a_{m_0}|_p$

$$\leq \max\{\underbrace{|a_m - a_{m_0}|_p}_{<\varepsilon}, \underbrace{|a_{m_0}|_p}_{\geq \varepsilon}\}$$

$$= |a_{m_0}|_p$$

∎

Cor We can extend $|\cdot|_p$ to $\mathbb{Q}_p$.

Def p-adic integers $\mathbb{Z}_p := \{ x \in \mathbb{Q}_p : |x|_p \leq 1 \}$

- $\mathbb{Q}_p$ is a field, with ring of integers $\mathbb{Z}_p$.
- $\mathbb{Z}_p$ is a local ring with unique maximal ideal $p\mathbb{Z}_p = \{ |x|_p < 1 \}$

and $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p = \{ |x|_p = 1 \}$

Prop $\mathbb{Z}_p / p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

Pf Let $\alpha \in \mathbb{Z}_p$ represented by the Cauchy seq (a_m)

- by Prop: $|a_m|_p = |a_m|_p \quad \forall\, m, n \geq 0$
- $\alpha \in \mathbb{Z}_p \Rightarrow |a_m|_p \leq 1$

so that $a_m \equiv a_m \mod p$, $\equiv a \mod p$ is well-defined

So $\mathbb{Z}_p \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is surjective

and $\ker = p\mathbb{Z}_p$

Note that $\mathbb{Z} \hookrightarrow \mathbb{Z}_p \hookleftarrow$ char $\mathbb{Z}_p = 0$

$0 \to p\mathbb{Z} \to \mathbb{Z} \to \mathbb{F}_p \to 0 \hookleftarrow$ char $\mathbb{F}_p = p$

Hensel's lemma: Let $f \in \mathbb{Z}_p[x]$ and let $\bar{f} \in \mathbb{F}_p[x]$ be the reduction. If x_0 is a simple root of $\bar{f}$ in $\mathbb{F}_p$ ($x_0 \in \mathbb{F}_p$, $\bar{f}(x_0) = 0$, $\bar{f}'(x_0) \neq 0$)

$\Rightarrow \exists!\ a \in \mathbb{Z}_p$ st $f(a) = 0$

(Pf: Newton method and strong tri. ineq.)

(- So far we have been fairly analytic, let's be more algebraic.)

- Let (a_n) be a Cauchy seq wrt $(\cdot|_p)$ in $\mathbb{Z}$. The image (a_n) is ultimately constant in $\mathbb{Z}/p^n\mathbb{Z}$, say ξ_n.

- Under the projection $\pi_{n+1} : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$

we have $\xi_{n+1} \overset{\pi_{n+1}}{\longmapsto} \xi_n$

So $$\boxed{\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}} \overset{\text{set}}{=} \left\{ (\xi_0, \xi_1, \dots) \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} : \pi_{n+1}(\xi_{n+1}) = \xi_n \right\}$$

also $\mathbb{Z}_p \ni x = x_0 + x_1 p + x_2 p^2 + \dots$ with $x_i \in \{0, \dots, p-1\}$ — p-adic exp

- $\mathbb{Z}_p$ is a ring! But: how can we compute $x+y$, $x \cdot y$ using the p-adic exp?

(- Idea: choose better coefficients x_i in $\mathbb{Z}_p$ (instead of in $\mathbb{Z}$))

Teichmüller representatives of $\mathbb{F}_p^*$ ($\cup \{0\}$):

$x_0 \in \mathbb{F}_p^*$ lift via Hensel's lemma to a (unique) solution $\omega(x_0)$ of $X^{p-1} - 1 = 0$ in $\mathbb{Z}_p^\times$

$$\omega : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$$ T. character mult (not additive)

Eg $\bar{2} \in \mathbb{F}_5$: $\begin{cases} X \equiv 2 \mod 5 \\ X^{5-1} - 1 \mod 25 \end{cases} \rightsquigarrow \begin{cases} X \equiv 7 \mod 25 \\ X^{5-1} - 1 \mod 125 \end{cases}$

$\omega(\bar{2}) = (2, 7, 57, \dots)$ $\qquad$ $\downarrow$

$x \equiv 57 \mod 125$

Def R a commutative ring. A Witt vector over R is a sequence $(a_0, a_1, \dots)$ of elements of R.

$W(R) = \{\text{Witt vectors over } R\}$

$W(R) \leftrightarrow R^{\mathbb{N}}$ as sets

(Instead of using the product structure...)

Def The n-th Witt polynomial $w_n \in \mathbb{Z}[X_0, X_1, \dots]$ by

$$w_n := \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + p X_1^{p^{n-1}} + \dots + p^n X_n$$

Eg

$$w_0 = X_0$$
$$w_1 = X_0^p + p X_1$$
$$w_2 = X_0^p + p X_1^p + p^2 X_2$$

Thm For every polynomial $\Phi \in \mathbb{Z}[X;Y]$ there exists a unique sequence $(\varphi_0, \varphi_1, \dots)$ of elements of $\mathbb{Z}[X_0, X_1, \dots; Y_0, Y_1, \dots]$ s.t.

$$w_n(\varphi_0, \varphi_1, \dots) = \Phi(w_n(X_0, X_1, \dots); w_n(Y_0, Y_1, \dots)) \quad \forall n \geq 0$$

(Pf idea: you can "recover" the variable X_i using w_k with $k \leq i$. So define the φ_j inductively and then prove that have coeff in $\mathbb{Z}$)

Eg • $\Phi(X;Y) = X + Y$ "$\varphi_i = S_i$"

$$S_0 = X_0 + Y_0, \quad S_1 = X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}$$

• $\Phi(X;Y) = X \cdot Y$ "$\varphi_i = P_i$"

$$P_0 = X_0 \cdot Y_0, \quad P_1 = Y_0^p X_1 + X_0^p Y_1 + p X_1 Y_1$$

- Check: with this operations $W(R)$ is a (unital) commutative ring.

Examples

- If p is invertible in R, then the witt poly's give an iso between $W(R) \simeq R^{\mathbb{N}}$
- $W(\mathbb{F}_p) \cong \mathbb{Z}_p$ ($\mathbb{Z}_p$ is a strict p-ring with residue ring $\mathbb{F}_p$, hence it is unique up to iso)

(• Why Witt-vectors are awesome?)
Why they are better approach to p-adic int.?

The operations on $W(R)$ are polynomial equation with integer coefficients. So they are indep. of R. Moreover they are unique. So

$$
\begin{array}{ccc}
W : \underline{\text{Rng}} & \longrightarrow & \underline{\text{Rng}} \\
R & \longmapsto & W(R) \\
\big\downarrow & & \big\downarrow \\
S & \longmapsto & W(S)
\end{array}
$$

canonically.

Eg

$$
\begin{array}{cccc}
x & \mathbb{F}_q & \longmapsto & W(\mathbb{F}_q) \\
\big\downarrow & \big\downarrow F & & \big\downarrow W(F) \\
x^p & \mathbb{F}_q & \longmapsto & W(\mathbb{F}_q)
\end{array}
$$

hom. b/c char $\mathbb{F}_q = p$

induced hom [illegible] but in char 0