p: prime

$\Phi_n(X_0, X_1, \cdots, X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + p^2 X_2^{p^{n-2}} + \cdots + p^{n-1} X_{n-1}^{p} + p^n X_n$

$\Phi_0(X_0) = X_0$

$\Phi_1(X_0, X_1) = X_0^p + pX_1$ $\qquad$ $\Phi_{n-1}(X_0, \cdots, X_{n-1}) = X_0^{p^{n-1}} + pX_1^{p^{n-2}} + \cdots + p^{n-1} X_{n-1}$

$\Phi_2(X_0, X_1, X_2) = X_0^{p^2} + pX_1^p + p^2 X_2$

$$\Rightarrow \quad \Phi_n(X_0, X_1, \cdots, X_n) = \Phi_{n-1}(X_0^p, X_1^p, \cdots, X_{n-1}^p) + p^n X_n$$
$$= X_0^{p^n} + p\,\Phi_{n-1}(X_1, \cdots, X_n)$$

Lemma 1 $A = J_0 \supseteq J_1 \supseteq J_2 \supseteq \cdots$ decreasing sequence of ideals, $p \in J_1$

$J_n \cdot J_m \subseteq J_{n+m}$ $\forall m, n \in \mathbb{N}$

(1) $a_i \equiv b_i \pmod{J_m}$ for $i = 0, 1, \cdots, n$ $\Rightarrow$ $\Phi_i(a_0, \cdots, a_n) \equiv \Phi_i(b_1, \cdots, b_n) \pmod{J_{m+1}}$ for $i = 0, 1, \cdots, n$

(2) If $[p] : \bigoplus_{m \geq 0} J_m/J_{m+1} \longrightarrow \bigoplus_{m \geq 0} J_m/J_{m+1}$ is injective

($[p]$ is wt-1 homom.)

then: If $\Phi_i(a_0, \cdots, a_n) \equiv \Phi_i(b_0, b_1, \cdots, b_n) \pmod{J_{m+i}}$ for $i = 0, 1, \cdots, n$

then $a_i \equiv b_i \pmod{J_m}$ for $i = 0, 1, \cdots, n$.

pf of (1) Induction on n.

pf of (2) Induction on n.

W2

Lemma 2 A : ring, with p-adic filtration

$\sigma : A \to A$ ring homom. s.t. $\sigma(a) \equiv a^p \pmod{p}$ $\forall a \in A$

$a_0, \dots, a_{n-1} \in A$

Let $u_i = \Phi_i(a_0, \dots, a_i)$ for $i = 0, 1, \dots, n$

Given an element "u_n" $\in A$

$\exists a_n \in A$ s.t. $\Phi_n(a_0, \dots, a_{n-1}, a_n) = u_n$

$\iff u_n \equiv \sigma(u_{n-1}) \pmod{p^n A}$

Prop 3 : A : ring $\sigma : A \to A$ lifting of Frobenius

$$\Phi : A^{\mathbb{N}} \to \mathbb{A}^{\mathbb{N}}$$
$$(a_i)_{i \in \mathbb{N}} \mapsto (\Phi_i(a_0, \dots, a_i))_{i \in \mathbb{N}}$$

$(u_0, u_1, \dots) = (u_i)_{i \in \mathbb{N}} \in \mathrm{Im}(\Phi)$

$\iff u_n \equiv \sigma(u_{n-1}) \mod p^n \quad \forall n.$

$F : A^{\mathbb{N}} \to \mathbb{A}^{\mathbb{N}} \quad (b_0, b_1, b_2, \dots) \mapsto (b_1, b_2, \dots)$

$V : \mathbb{A}^{\mathbb{N}} \to \mathbb{A}^{\mathbb{N}} \quad (b_0, b_1, b_2, \dots) \mapsto (0, pa_0, pa_1, \dots)$

Properties of Witt vectors

Prop 4 $\underline{\Phi}: W(\cdot) \to \mathbb{A}^{\mathbb{N}}$ $\underline{a}=(a_0, a_1, \cdots, a_m, \cdots) \mapsto (\Phi_0(\underline{a}), \Phi_1(\underline{a}), \Phi_2(\underline{a}), \cdots)$

Have: $\underline{S}: W(\cdot) \times W(\cdot) \to W(\cdot)$ functorial maps

$\underline{P}: W(\cdot) \times W(\cdot) \to W(\cdot)$

$\underline{I}: W(\cdot) \times W(\cdot) \to W(\cdot)$

s.t. $\underline{\Phi}(\underline{S}(\underline{a},\underline{b})) = \underline{\Phi}(\underline{a}) + \underline{\Phi}(\underline{b})$

$\underline{\Phi}(\underline{P}(\underline{a},\underline{b})) = \underline{\Phi}(\underline{a}) \cdot \underline{\Phi}(\underline{b})$ $\forall \underline{a}, \underline{b}$

$\underline{\Phi}(\underline{I}(\underline{a})) = -\underline{\Phi}(\underline{a})$

so that $(\underline{W}, \underline{S}, \underline{P}, \underline{I})$ defines a functor from (Comm. Alg) to (Rings)

and $\underline{\Phi}: \underline{W} \to \mathbb{A}^{\mathbb{N}}$ is a natural transformation

In addition:

$\underline{\Phi} \circ F = f \circ \underline{\Phi}$ $F: W(\cdot) \to W(\cdot)$ ring endomorphisms

$\underline{\Phi} \circ V = v \circ \underline{\Phi}$ $V: W(\cdot) \to W(\cdot)$ endom of $(W(\cdot), +)$

Prop 5: (a) $F_A(V_A(\underline{a})) = p \cdot \underline{a}$ $\forall \underline{a} \in W(A)$ $\forall$ comm. ring A

(b) $V_A(a \cdot F_A(\underline{b})) = V_A(\underline{a}) \cdot \underline{b}$ $\forall \underline{a}, \underline{b} \in W(A)$

(c) $V_A(\underline{a}) \cdot V_A(\underline{b}) = p \cdot V_A(\underline{a} \cdot \underline{b})$ $\forall \underline{a}, \underline{b} \in W(A)$

(d) $V_A(F_A(\underline{b})) = V_A(1) \cdot \underline{b}$ $1 = (1,0,0,\cdots) \in W(A)$ $\forall \underline{b} \in W(A)$

$V_A(1) = (0,1,0,0,\cdots) \in W(A)$

(e) $F_A(\underline{a}) \equiv \underline{a}^p \mod p\, W(A)$ $\forall a \in W(A)$

Note: (e) is different from: The images of $F_A(\underline{a})$ and $(a_0^p, a_1^p, a_2^p, \cdots)$ in $W(A/pA)$ are equal.

Pf (b) check $V_B(\xi f_B(\eta)) = V_B(\xi) \cdot \eta$ $\forall \xi, \eta \in \mathbb{A}^{\mathbb{N}}(\mathbb{Z}[X_0, X_1, X_2, \cdots; Y_0, Y_1, Y_2, \cdots])$

$\|$ $\|$

$V_B(\xi_0 \eta_1, \xi_1 \eta_2, \cdots)$? $(0, p\xi_0\eta_1, p\xi_1\eta_2)$

yes

Pf of (c): $V(\underline{a})\cdot V(\underline{b}) = V_A\cdot(\underline{a}\cdot FV(\underline{b})) = V_A(\underline{a}\cdot p\underline{b}) = p\cdot V_A(\underline{a}\cdot\underline{b})$

($V(\underline{b})$ ↑ by (b); $V_A\cdot(\underline{a}\cdot FV(\underline{b}))$ ↑ by (a))

(d) $V_A(F_A(\underline{b})) = V_A(1\cdot F_A(\underline{b})) = V_A(1)\cdot\underline{b}$, $V_A(1) = (0,1,0,0,\dots)\in W(A)$

(e) Suffices to check:

$$f_B(\xi)\equiv \xi^p \pmod{p\,\underline{\Phi}_B(W(B))} \qquad \forall \xi\in \underline{\Phi}_B(W(B))$$

Have $\xi = (\xi_0,\xi_1,\dots)\in B^{\mathbb{N}}$, $\sigma(\xi_n)\equiv \xi_{n+1} \pmod{p^{n+1}B}$ $\forall n$

$f_B(\xi) = (\xi_1,\xi_2,\dots)$

$f_B(\xi)\equiv \xi^p \pmod{p\,\underline{\Phi}_B(W(B))}$ means:

$$\sigma\left(\xi_{n+1}-\xi_n^p\right)-\left(\xi_{n+2}-\xi_{n+1}^p\right)\equiv 0 \pmod{p^{n+2}B} \qquad \forall n$$

This congruence follows from the condition that $\sigma(\xi_n)-\xi_{n+1}\equiv 0 \pmod{p^{n+1}B}$ $\forall n$

QED

Def^n: $\tau_A: A\to W(A)$ $\quad a\mapsto (a,0,0,0,\dots)$ $\forall a\in A$

(Teichmüller map)

Prop 6: (a) $\tau(a\cdot b) = \tau(a)\cdot\tau(b)$ $\forall a\in A$ ($\tau_A: A\to W(A)$ is "multiplicative")

(b) $\tau(a)\cdot\underline{x} = (a^{p^n}x_n)_{n\in\mathbb{N}}$ $\forall a\in A$, $\forall \underline{x}=(x_0,x_1,x_2,\dots)\in W(A)$

(c) $(a_0,a_1,\dots) = \sum_{n\geq 0} V^n(\tau(a_n))$ $\forall a_0,a_1,\dots\in A$

(Exercise)

Def^n a) $\forall$ commutative ring A, $\forall n\in\mathbb{N}$

define the V-adic filtration $(V_m(A))_{m\geq 0}$ on $W(A)$ by:

$V_m(A) := V^m(W(A))$

Note: $V_m(\underline{a})\cdot\underline{b} = V_m(\underline{a}\cdot F^m(\underline{b}))$ $\forall a,b\in W(A)$

$\Rightarrow$ $V_m(A)$ is an ideal of $W(A)$

This filtration defines a topology on $W(A)$, called the V-adic topology

b) Define $\forall m\in\mathbb{N}_{\geq 1}$, $W_m(A) := W(A)/V^m(W(A))$

$$\{\underbrace{[(a_0,\dots,a_{m-1})}_{\|} : a_0,a_1,\dots,a_{m-1}\in A\}$$

$W_m(A)$ is a commutative ring.

Def^n a) Define $V_m^n : W_m(A) \longrightarrow W_{m+n}(A)$ $\quad \forall m \geq 1,\ \forall n \geq 0$

by

$$\begin{array}{ccc} W(A) & \xrightarrow{V^n} & W(A) \\ \downarrow \pi_m & & \downarrow \pi_{m+n} \\ W_m(A) & \xrightarrow[V_m^n]{} & W_{m+n}(A) \end{array}$$

b) Define $F_m^n : W_{m+n}(A) \longrightarrow W_m(A)$ $\quad \forall m \geq 1,\ \forall n \geq 0$

by

$$\begin{array}{ccc} W(A) & \xrightarrow{F^n} & W(A) \\ \pi_{m+n} \downarrow & & \downarrow \pi_m \\ W_{m+n}(A) & \xrightarrow[F_m^n]{} & W_m(A) \end{array}$$

Note $F(V_{m+1}(A)) \subseteq V_m(A)$

$\because\ F(V^{m+1}(\underline{a})) = p \cdot V^m(\underline{a}) \quad \forall \underline{a} \in W(A)$

Lemma: $V_1(A)^k = p^{k-1} V_1(A) \subseteq V^k(W(A)) \quad \forall k \geq 1$

$\left(V(\underline{a}) \cdot V(\underline{b}) = p\, V(\underline{a} \cdot \underline{b}) \quad \forall \underline{a}, \underline{b} \in W(A), \text{ by Prop 5 (c), plus induction} \right)$

Prop 7. Suppose that $p \cdot 1_A = 0$ in A

(a) $F\underline{a} = (a_n^p)_{n \in \mathbb{Z}} \quad \forall \underline{a} \in W(A)$

(b) $p \cdot \underline{a} = VF(\underline{a}) = FV(\underline{a}) = (0, a_0^p, a_1^p, \cdots) \quad \forall \underline{a} = (a_0, a_1, a_2, \cdots) \in W(A)$

(c) $V^m(\underline{a}) \cdot V^n(\underline{b}) = V^{m+n}\left(F^n(\underline{a}) \cdot F^m(\underline{b})\right) \quad \forall \underline{a}, \underline{b} \in W(A)$

Pf. (a) $\Leftrightarrow$ $F_n(\underline{X}) \equiv X_n^p \pmod p$ in $\mathbb{Z}[X_0, X_1, \cdots]$ $\quad \forall n$ $\quad F(\underline{X}) = (F_0(\underline{X}), F_1(\underline{X}), F_2(\underline{X}), \cdots) \in W(\mathbb{Z}[X_0, X_1, X_2, \cdots])$

This congruence is equivalent to:

$$\Phi_m(F(\underline{X})) \equiv \Phi_m(X_0^p, X_1^p, X_2^p, \cdots) \pmod{p^{m+1}\mathbb{Z}[X_0, X_1, X_2, \cdots]} \quad \forall m$$

$\|$

$$\Phi_{m+1}(\underline{X}) = \Phi_m(X_0^p, X_1^p, \cdots, X_m^p) + p^{m+1} X_{m+1}$$

(b) follows from (a).

(c) $V^m(\underline{a}) \cdot V^n(\underline{b}) = V^m(\underline{a} \cdot F^m V^n(\underline{b})) = V^m(\underline{a} \cdot V^n F^m(\underline{b})) = V^m\left(V^n(F^n(\underline{a}) \cdot F^m(\underline{b}))\right)$

$FV = VF$

$= V^{m+n}(F^n(\underline{a}) \cdot F^m(\underline{b}))$

Prop 8 (1) The $V_1(A)$-adic topology on $W(A)$ is finer than the p-adic topology on $W(A)$ ($\Leftrightarrow V_1(A)^k \subseteq p^{k-1} W(A) \quad \forall k \geq 1$)

(2) Suppose that $p \cdot 1_A = 0$ in A.

(2a) The $V_1(A)$-adic topology on $W(A)$ coincides with the p-adic topology on $W(A)$.

(2b) The p-adic topology on $W(A)$ is finer than the V-adic topology on $W(A)$.

(2c) $W(A)$ is complete and separated w.r.t. the p-adic topology

pf (2a): $p^k W(A) \subseteq V_1(A)^k \subseteq p^{k-1} W(A)$

(2b): $p^m W(A) \subseteq V^m(W(A))$

Prop 9. Suppose that A is perfect of characteristic $p>0$, i.e. $p \cdot 1_A = 0$ and $Fr_p : A \xrightarrow{\sim} A$.

(a) $\forall \underline{a} = (a_0, a_1, \dots, a_n, \dots) \in W(A)$, $\underline{a} = \sum_{n \geq 0} p^n \tau(a_n^{p^{-n}})$

(b) The three topologies on $W(A)$ coincide: p-adic, V-adic, $V_1(A)$-adic

In particular, $V_n(A) = p^n W(A) = (V_1(A))^n \quad \forall n \geq 1$

(c) $W(A)/_p W(A) \xrightarrow{\sim} A$

Prop 10 Suppose that A is a perfect field of characteristic $p>0$. Then $W(A)$ is a discrete valuation ring with maximal ideal $p \cdot W(A)$ and residue field A.

(Exer)

Cohen 1

p-ring

Def 1 A <u>p-ring</u> is a commutative ring C such that $p \cdot C$ is a maximal ideal of C and C is complete and separated for the p-adic topology.

Prop 1 Let C be a p-ring (0) Every element of C is of the form $p^n \cdot u$, with $n \in \mathbb{N}$, $u \in C^\times$

(1) C is a local ring with maximal ideal pC

(2) Suppose $p \cdot 1_C$ is nilpotent. Let d = the smallest natural number s.t. $p^d \cdot 1_C = 0$
Then every ideal of C is of the form $p^k C$ for some k with $0 \le k \le d$.
Moreover $p^k C \neq p^\ell C$ $\forall\, k \neq \ell$, $1 \le k, \ell \le d$, and $\text{length}_C(C) = d$

(3) Suppose $p \cdot 1_C$ is not unipotent. Then C is a DVR of mixed characteristics $(0,p)$.
The ideals of C are of the form $p^n C$, $n \in \mathbb{N}$: $p^n C \neq p^m C$ if $n \neq m$. $\text{length}_C(C) = \infty$

pf: (0), (1): exercise $\because \bigcap_{n \in \mathbb{N}} p^n C = (0)$

(2) $C \supseteq pC \supseteq \cdots \supseteq p^{d-1}C \supseteq p^d C = (0)$.

Note: $p^i C \supsetneq p^{i+1} C$ for $i = 0, 1, \cdots d-1$. : If $p^i C = p^{i+1} C$ $i \le d-1$ $\Rightarrow$ $p^{d-1} C = p^{d-i-1} \cdot p^i C = p^{d-i-1} \cdot p^{i+1} C = p^d C = (0)$

Let I be an ideal of C, and let k be the smallest natural number s.t. $I \supseteq p^k C$.

Claim: $I = p^k C$: Given any $x \in I$, write $x = p^m u$, $u \in C^\times$ $\Rightarrow$ $p^m C \subseteq I \Rightarrow m \ge k$ $\Rightarrow x \in p^k C$

$\ell_C(C) = d$ $\because$ $p^i C / p^{i+1} C \cong C/pC$ as C-modules.

(3) Immediate from defn of DVR.

Remark: Prop 1 shows: p-rings which are domains = absolutely unramified complete dvr's

Will see: p-rings which are not domains = quotient rings of abs. unramified complete dvr's by $(\overline{p}^d)$, $d \in \mathbb{N}_{\ge 1}$

Prop 2 Let $u: C \to C'$ be a ring homom of p-rings, $\kappa_C = C/pC$, $\kappa_{C'} = C'/pC'$
$v: \kappa_C \to \kappa_{C'}$ induced by u.

(a) $\ell(C) \ge \ell(C')$; $\ell(C) = \ell(C')$ iff u is injective

(b) u is surjective iff $v: \kappa_C \xrightarrow{\sim} \kappa_{C'}$

(c) u is an isom iff $v: \kappa_C \xrightarrow{\sim} \kappa_{C'}$ and $\ell(C) = \ell(C')$

Note (a) + (b) $\Rightarrow$ (c) trivially

Pf (a) $p^{n-1}1_{C'} \neq 0 \Rightarrow p^{n-1}1_C \neq 0$ } $\Rightarrow \ell(C') \leq \ell(C)$
$\Leftrightarrow$ if u is injective and $\ell(C') = \ell(C)$ if u is injective

(b) : dévissage, $(p^n C)_{0 \leq n \leq d} \to (p^m C')_{0 \leq m \leq d'}$ $\quad d' = \ell(C') \leq \ell(C) = d$

Prop 3 $(C_m, \pi_{n,m} : C_m \to C_n)$ a projective system of p-rings indexed by $\mathbb{N}$ s.t. $\pi_{n,m} : C_m \twoheadrightarrow C_n \quad \forall\, m \geq n$.

Then $C := \varprojlim_m C_m$ is a p-ring, and $\pi_n : C \twoheadrightarrow C_m \ \forall m$ inducing an isom $\kappa_C \xrightarrow{\sim} \kappa_{C_m}$ (exer.)

Def^n Let (A, m_A) be a complete separated local ring (not nec. Noetherian) such that $\kappa_A := A/m_A$ is a field of characteristic $p > 0$.
A Cohen subring of A is a local subring $C \subseteq A$ which is a p-ring such that $A = m_A + C$; i.e. $C/m_A \cap C = C/pC \xrightarrow{\sim} A/m_A$
(κ_C = κ_C, κ_A = κ_A)

Example : C : a p-ring $\Rightarrow$ C is a Cohen subring of $C[\![X_1, \dots, X_n]\!]$

Theorem 4 (Existence of Cohen subring in complete local rings)
Let (A, m_A) be a complete separated local ring s.t. $\kappa = A/m_A \supseteq \mathbb{F}_p$.
Let $S \subseteq A$ be a subset of A s.t. $\pi : A \to \kappa$ induces a bijection $S \xrightarrow{\sim} \pi(S) \subseteq \kappa$ and $\pi(S)$ is a p-basis of κ.

(a) $\exists!$ Cohen subring $C \subseteq A$ containing S

(b) C is closed in A, and the m_A-adic topology of A induces the p-adic topology on C

(c) Every closed subring $A' \subseteq A$ such that $A' \supseteq S$ and $A' + m_A = A$ contains C

Will first prove Thm 4 when m_A is nilpotent. Then deduce the general case from this special case

Cohen 3

Pf of Thm 4.

Part I. Case when $m_A^{n+1} = (0)$, $n \in \mathbb{N}$

Let $B_n = \mathrm{Im}\left(\Phi_n : W_{n+1}(A) \longrightarrow A\right) \subseteq A$

$$[a_0, a_1, \cdots, a_n] \mapsto \sum_{i=0}^{n} p^i a_i^{p^{n-i}}$$

Define $C_n :=$ the subring generated by $S \cup B_n$.

Lemma 1 Let $A' \subseteq A$ be a subring of A s.t. $A' \supseteq S$. Then $A' \supseteq C_n \iff A' + m_A = A$

pf of Lemma 1: "$\Rightarrow$": $\pi(B_n) = \kappa^{p^n} \rightsquigarrow \pi(C_n) = \kappa^{p^n}[\pi(S)] = \kappa$

"$\Leftarrow$": Suppose $A' + m_A = A$ $\quad \forall a_0, a_1, \cdots, a_n \in A$, pick $a_0', a_1', \cdots, a_n' \in A'$ s.t. $a_i' \equiv a_i \ (m_A)$ $\forall i = 0, 1, \cdots, n$

$\rightsquigarrow \Phi_n(a_0, a_1, \cdots, a_n) \equiv \Phi_n(a_0', a_1', \cdots, a_n') \in A' \Rightarrow A' \supseteq B_n$ q.e.d.

(* they are $\equiv \pmod{m^{n+1}}$)

Let $\mathcal{C} = \{$ subrings $A' \subseteq A$ s.t. $A' \supseteq S$ and $A' + m_A = A\}$

$= \{$ subrings $A' \subseteq A$ s.t. $A' \supseteq S \cup B_n\}$ (Lemma 1) $\ni C_n =$ the unique minimal element in $\mathcal{C}$ $\quad (= C)$

Must show: pC is a maximal ideal of A

Lemma 2 $C \cap m_A = pC$ (Must show "$\subseteq$")

pf of Lemma 2: $C_n = C_{n+1} = C$ Consider monomials $Z_\alpha := \prod_{s \in S} s^{\alpha_s}$ $\quad \alpha = (\alpha_s)_{s \in S}$, $0 \le \alpha_s < p^{n+1}$ $\forall s$

Since $\Phi_{n+1}(a_0, a_1, \cdots, a_{n+1}) = a_0^{p^{n+1}} + p\,\Phi_n(a_1, \cdots, a_{n+1})$

$\rightsquigarrow$ Every element of B_{n+1} is of the form $a^{p^{n+1}} + p \cdot b$ with $a \in A$, $b \in B_n$

$\rightsquigarrow$ Every element $x \in C_{n+1}$ is of the form

$$x = \sum_{\alpha \in \Lambda} c_\alpha^{p^{n+1}} Z_\alpha + py, \quad c_\alpha \in A \ \forall \alpha \in \Lambda, \text{ and } y \in C_n = C$$

$\Lambda \leftarrow$ the set of all $(\alpha_s)_{s \in S}$ s.t. $0 \le \alpha_s < p^{n+1}$ $\forall s$

$\Rightarrow$ If $x \in C \cap m_A$, then $c_\alpha \in m_A$ $\forall \alpha \in \Lambda$, hence $c_\alpha^{p^{n+1}} = 0$ $\forall \alpha \in \Lambda$

In other words $x = py$ for some $y \in C$ q.e.d.

Back to Thm 4, under the assumption that $m_A^{n+1} = (0)$.

(b): trivial; (c) follows from Lemma 1.

For (a), suppose $C' \subseteq A$, $C' \supseteq S$, C': Cohen subring. Lemma 1 $\Rightarrow C' \supseteq C$ (inclusion of p-rings with the same residue field)

$\Rightarrow C' = C$.

Cohen 4

Proof of Thm 4, Part 2 = general case $\quad \pi_n : A \twoheadrightarrow A_n$

Let $A_n = A/\mathfrak{m}_A^{n+1}$ $\forall n \in \mathbb{N}$. Let C_n = the Cohen subring of A_n containing $\pi_n(S)$.

Let $\pi_{n,m} : A_m \twoheadrightarrow A_n$ $\forall m \geq n$ $\rightsquigarrow$ $\pi_{n,m}(C_m) = C_n$ $\forall m \geq n$ by Part 1

Let $C = \varprojlim_n C_n \subseteq A = \varprojlim_n A_n$

Easy to see: C is a Cohen subring of A

Check C is closed in A: Let $J_n = C \cap \mathfrak{m}_A^n$ $\quad \bigcap_{n\geq 1} J_n = (0)$ $\quad$ or $\quad \bigcap_{n\in\mathbb{N}} \mathfrak{m}_A^n = (0)$

Since every ideal of C is of the form $p^m C$, there is a function $t : \mathbb{N} \to \mathbb{N}$ s.t. $J_n = p^{t(n)} C$

Assertion (b) follows easily.

Assertion (c): Given $A' \subseteq A$ (closed subring), $A' \supseteq S$, and $A' + \mathfrak{m}_A = A$

Part 1 $\Rightarrow$ $\pi_n(A') \supseteq C_n$ $\forall n$ $\quad A' = \bigcap_{n\geq 1} \pi_n^{-1}(\pi_n(A'))$ since A' is closed

$\Rightarrow A' \supseteq \bigcap_{n\geq 1} \pi_n^{-1}(C_n) = C$ $\qquad$ QED

Prop 5. (Uniqueness of p-rings)

Let C and C' be p-rings with residue fields κ_C and $\kappa_{C'}$, $\pi_C : C \twoheadrightarrow \kappa_C$, $\pi_{C'} : C' \twoheadrightarrow \kappa_{C'}$. Let $v : \kappa_C \xrightarrow{\sim} \kappa_{C'}$

Let $(x_s)_{s\in S}$ be a family of elements of C s.t. $(\pi(x_s))_{s\in S}$ is a p-basis of κ_C

Let $(x'_s)_{s\in S}$ be a family of elements of C' s.t. $(\pi'(x'_s))_{s\in S}$ is a p-basis of $\kappa_{C'}$

Suppose that $v(\pi(x_s)) = \pi(x'_s)$ $\forall s \in S$ and $\ell(C) \geq \ell(C')$.

$\exists!$ homomorphism $u : C \to C'$ such that $u(x_s) = x'_s$ $\forall s$ and $\pi_{C'} \circ u = v \circ \pi_C$.

This homomorphism u is surjective; u is an isomorphism if $\ell(C) = \ell(C')$.

Pf: Let $\tilde{A} = C \times_\kappa C' = \{(a, a') \mid a \in A,\ a' \in A',\ v(\pi(a)) = \pi'(a')\}$, a complete local ring

$\cup \{(x_s, x'_s) \mid s \in S\}$

Apply Thm 5 $\rightsquigarrow$ get a Cohen subring $\tilde{C} \subseteq \tilde{A}$

Have $\ell(\tilde{C}) = \max(\ell(C), \ell(C'))$ (consider $p^n 1_{\tilde{A}}$)

$\rightsquigarrow \mathrm{pr}_1|_{\tilde{C}} : \tilde{C} \xrightarrow{\sim} C$ is an isom. $\rightsquigarrow$ define $u := \mathrm{pr}_2 \circ (\mathrm{pr}_1|_{\tilde{C}})^{-1} : C \to C'$

q.e.d.

Cohen 5

Prop 6 (Existence of p-rings)
Let $\kappa \supseteq \mathbb{F}_p$ be a field. Let $n \in \mathbb{N} \cup \{\infty\}$. There exists a p-ring whose residue field is isomorphic to κ

Pf: A Cohen subring C of $W(\kappa)$ is p-ring with $\ell(C) = \infty$.
(Recall that $(W(\kappa), m = V(W(\kappa))$ is a complete separated local ring. q.e.d.

Corollary 7 Let C be a p-ring with $\ell(C) =: n < \infty$. There exists a p-ring C' and an isomorphism $C'/p^n C' \xrightarrow{\sim} C$
(Immediate from Prop 6 and Prop 5)

Proposition 7 Let $\kappa \supseteq \mathbb{F}_p$ be a perfect field of characteristic $p>0$
Let C be a p-ring with $C/pC \xrightarrow{\alpha}_{\sim} \kappa$. Let $n = \ell(C) \in \mathbb{N} \cup \{\infty\}$.
There exists a isomorphism $C \to W_n(\kappa)$ which induces the isom. $C/pC \xrightarrow{\alpha}_{\sim} \kappa$.

Prop 8 Let A be a complete separated local ring whose residue field k is perfect of characteristic $p>0$. $\pi: A \twoheadrightarrow k$
(a) $\exists!$ ring homom $u: W(k) \to A$ such that $\pi(u(\underline{a})) = a_0$
(b) The homom u in (a) is continuous for $\forall \underline{a} = (a_0, a_1, \dots) \in W(k)$ the $pW(k)$-adic topology on $W(k)$, and $\mathrm{Im}(u) =$ the unique Cohen subring of A.

Prop 9 Let A be a complete separated local ring with perfect residue field $k \supseteq \mathbb{F}_p$. (a) The exists a unique multiplicative subset $S \subseteq A$ such that $\pi: A \twoheadrightarrow k$ induces a bijection $S \xrightarrow{\sim} k$
(b) An element $a \in A$ is in S iff $\forall n \in \mathbb{N}$, $\exists\, a_n \in A$ s.t. $a_n^{p^n} = a$.
(c) $S = \{ u(y, 0, 0, 0, \dots) \mid y \in k \}$, where $u: W(k) \to A$ is the ring homom in Prop 8.

Proof of Prop 9: Let $T = \{x \in A \mid \forall n \in \mathbb{N},\ \exists x_n \in A \text{ s.t. } x_n^{p^n} = x\}$

Uniqueness part of (a): $\forall$ multiplicativ (= multiplicatively closed) subset $S \subseteq A$ s.t.

$\pi|_S : S \xrightarrow{\sim} k$. Clearly $S \subseteq T$

Must show: $\pi|_T : T \to k$ is injective

Otherwise $\exists x, y \in T$ s.t. $x \neq y$ and $\pi(x) = \pi(y)$ $\forall n \in \mathbb{N}$, pick $x_n, y_n \in A$ $x_n^{p^n} = x$, $y_n^{p^n} = y$

$\leadsto$ $x_n \equiv y_n \pmod{\mathfrak{m}_A} \implies \underset{x}{x_n^{p^n}} \equiv \underset{y}{y_n^{p^n}} \pmod{\mathfrak{m}^{n+1}}$ $\forall n$ $\Rightarrow x = y$

existence: Have $u : W(k) \to A$

$S := \{u(y, 0, 0, \cdots) \mid y \in k\}$ is a multiplicative subset of A

and $\pi|_S : S \xrightarrow{\sim} k$. We have proved (a) – (c). QED

<u>Theorem 10</u> Let $(A, \mathfrak{m})$ be a complete Noetherian local ring with $k = A/\mathfrak{m}_A \supseteq \mathbb{F}_p, p > 0$.

Let C be a p-ring with $C/pC = k$ and $\ell(C) = \infty$. Let $m = \dim_k(\mathfrak{m}_A / \mathfrak{m}_A^2 + pA)$

(1) $\exists$ an ideal $\mathfrak{a} \subseteq C[[T_1, \cdots, T_m]]$ and a local isomorphism $C[[T_1, \cdots, T_m]]/\mathfrak{a} \xrightarrow{\sim} A$

(2) Let $d := \dim(A)$. Suppose that $p \cdot 1_A$ is not a zero divisor of A.

Then $\exists$ a subring $B \subseteq A$ such that $B \cong C[[T_1, \cdots, T_{d-1}]]$ and A is a finite A'-algebra

Pf: (1) Let C' = a Cohen subring of A. Know: $\exists$ surjective local homom $C \twoheadrightarrow C' \hookrightarrow A$ (composite u)

Let $\bar{t}_1, \cdots, \bar{t}_m$ be a k-basis of $\mathfrak{m}_A/(\mathfrak{m}_A^2 + pA)$, and pick $t_1, \cdots, t_m \in \mathfrak{m}$ s.t. $t_i \mapsto \bar{t}_i$ $\forall i$

$\leadsto$ $\exists$ a surjective ring homom $C[[T_1, \cdots, T_m]] \xrightarrow{v} A$ extending u s.t. $v(T_i) = t_i$ $\forall i$

(2) Assume: $p \cdot 1_A$ is not a zero divisor of A

$\leadsto$ $\exists$ elements $y_1, \cdots, y_{d-1} \in \mathfrak{m}$ such that $\dim(A/(p, y_1, \cdots, y_{d-1})) = 0$

$\leadsto$ get a ring homom $\alpha : C[[T_1, \cdots, T_{d-1}]] \to A$, $T_j \mapsto y_j$. α is finite by Nakayama's Lemma

$\Rightarrow$ α is injective (Consider $gr_\circ(C[[T_1, \cdots, T_{d-1}]]) \cong k[\omega, T_1, \cdots, T_{d-1}]$)

QED

Remark: Thm 10 is the case of mixed characteristics $(0, p)$ of Cohen's structure theorem.

(Existence of coeff. fields) Cohen 7

Prop. 11 Let $(A, \mathfrak{m})$ be a complete separated local ring, and assume A contains a subfield k_0.

(a) Suppose that $\mathrm{char}(k_0) = 0$. $\exists!$ subfield $k \subseteq A$ containing k_0 s.t. the composition $k \hookrightarrow A \twoheadrightarrow A/\mathfrak{m}$ is an isomorphism

(b) Suppose that $\mathrm{char}(k_0) = p > 0$. There is a subfield $K \subseteq A$ (i.e. K is a subring of A and K is a field) such that the composition $K \hookrightarrow A \twoheadrightarrow A/\mathfrak{m}$ is an isomorphism

Pf (a): Follows easily from Hensel's lemma

(b) Will prove a strong statement (b)':

(b)': If $(x_\lambda)_{\lambda \in \Lambda}$ is a p-basis of $\kappa_A = A/\mathfrak{m}_A$, then $\exists!$ a unique subfield K containing all x_λ's such that $K \hookrightarrow A \twoheadrightarrow A/\mathfrak{m}$ is $\cong$. This subfield K is a Cohen subring of A.

(Consequence of Thm 4) QED

Theorem 12 Let A be a complete Noetherian local ring which contains a field. Let $d = \dim(A)$, and let K be a coefficient field of A.

Let $m = \dim_K(\mathfrak{m}_A/\mathfrak{m}_A^2)$

(a) $\exists$ an ideal $\mathfrak{a} \subseteq K[\![T_1, \dots, T_m]\!]$ and an isom. $K[\![T_1, \dots, T_m]\!]/\mathfrak{a} \xrightarrow{\sim} A$

(b) $\exists$ a K-subalgebra $A' \subseteq A$ such that A is a finite A'-algebra and $A' \cong K[\![X_1, \dots, X_d]\!]$

(c) If the local ring $(A, \mathfrak{m}_A)$ is regular, i.e. $\dim_K(\mathfrak{m}_A/\mathfrak{m}_A^2) = \dim(A)$, then $\exists$ a K-isom. $K[\![X_1, \dots, X_d]\!] \xrightarrow{\sim} A$

(This follows from Prop. 12)

Remark: Cohen's structure theorem(s) is a deep/landmark theorem and has many applications, including the finiteness of derived normal models of complete Noetherian local rings and analytic unramifiedness of Nagata rings.