Lecture 6-8.

§6 Witt vectors

Let A be a ring such that $R = A/pA$ is perfect, p is not a zero divisor in $\underline{A}$, and A is separated and complete w.r.t. p-adic topology. (In this case, A is called a <u>perfect p-ring</u>) For any $x \in R$, we may choose a sequence $\{x_{(i)}\} \subset R$ such that $x_{(0)} = x$, $x_{(i)}^p = x_{(i-1)}$. Lift these $x_{(i)}$ arbitrarily to $\hat{x}_{(i)} \in A$, define the <u>Teichmüller lift</u> of x to be

$$[x] := \lim_{n\to\infty} \widehat{x_{(n)}}^{\,p^n}$$

<u>Rmk</u>: (1). The limit exist & independent to the choice of $\{x_{(i)}\}$ since

$$(\hat{x}_{(n+m)})^{p^{n+m}} \equiv (\widehat{x_{(n)}})^{p^n} \mod p^n \quad \forall m \geqslant 0$$

(2). Teichmüller lift is only multiplicative. not additive.

For any $a \in A$, there exists a unique expression $a = \sum_{i\geq 0} p^i [x_i]$ for some $x_i \in R$.
(Just let $x_0 = a \bmod p$, $x_1 = \frac{a - [x_0]}{p} \bmod p$, induction).

<u>Universal formulas</u>

Now we focus on a "prototype" of perfect p-ring:

$$S = \mathbb{Z}_p[X_i^{-p^\infty}, Y_i^{-p^\infty}]_{i\geq 0} \quad \text{(Note that } S \text{ itself is not complete.)}$$

$$S/pS = \mathbb{F}_p[X_i^{-p^\infty}, Y_i^{-p^\infty}]_{i\geq 0} \qquad \text{we have } [X_i] = X_i,\ [Y_i] = Y_i.$$

Then $\sum_{i\geq 0} p^i X_i + \sum_{i\geq 0} p^i Y_i \in S$ has an expression $\sum_{i\geq 0} p^i [S_i]$, for some $S_i \in S/pS$

$(\sum_{i\geq 0} p^i X_i) \cdot (\sum_{i\geq 0} p^i Y_i) \in S$ " " " $\sum_{i\geq 0} p^i [P_i]$, " " $P_i \in S/pS$

It is easy to show by induction that $S_n, P_n \in \mathbb{F}_p[X_i^{-p^n}, Y_i^{-p^n}]_{i\leq n} \subseteq \mathbb{F}_p[X_i^{-p^\infty}, Y_i^{-p^\infty}]$

For any general perfect p-ring A, $a = \sum p^i [x_i]$ $b = \sum p^i [y_i]$, let $\pi: S \to A$ s.t.

$\pi(X_i)=[x_i]$, $\pi(Y_i)=[y_i]$. then

$$a+b=\sum p^i[x_i]+\sum p^i[y_i] = \sum p^i[S(x_i,y_i)]$$

$$a\cdot b = \left(\sum p^i[x_i]\right)\cdot\left(\sum p^i[y_i]\right) = \sum p^i[P(x_i,y_i)]$$

Thus $[S_i]$ and $[P_i]$ are called the "universal formulas" for $+$, $\times$.

<u>Construction of Witt vectors</u>

<u>Thm</u> If R is of characteristic p and perfect, then there exists a unique perfect p-ring $W(R)$, the <u>Witt vectors</u> with coefficients in R, s.t. $W(R)/pW(R)=R$.
and the construction is functorial (i.e. $\forall f: R\to R'$, f can lift to $W(f): W(R)\to W(R')$)

Pf: Construction of $W(R)$:

Starting from prototype: Given an index set J, let $S_J := \widehat{\mathbb{Z}_p[X_j^{-p^{\infty}}]}_{j\in J}$

$R_J := \mathbb{F}_p[X_j^{p^{-\infty}}]_{j\in J}$. Then $S_J/pS_J = R_J$, set $W(R_J)=S_J$.

In general, $\forall$ perfect ring R, $R=R_J/I$, where I is a perfect ideal ($I^p=I$). We define $W(I) := \{\sum_{i=0} p^i[x_i]\in S_J \mid x_i\in I\}\subseteq W(R_J)$.

We set $W(R) := W(R_J)/W(I)$. Then we have:

$$\begin{array}{ccc} W(R_J) & \xrightarrow{\bmod p} & R_J \\ \cup\!\mid & \circlearrowright & \cup\!\mid \\ W(I) & \twoheadrightarrow & I \end{array}$$

①. $W(R)/pW(R) = S_J/(pS_J+W(I)) = R_J/I = R$.

②. If $p\cdot x=0$ in $W(R)$, $p\cdot\hat{x}\in W(I)$ for some lift $\hat{x}\in W(\hat{R})$.
writing $\hat{x}=\sum p^i[x_i]$, $\underset{\in W(I)}{p\hat{x}=\sum p^{i+1}[x_i]} \Leftrightarrow x_i\in I \Leftrightarrow \hat{x}\in W(I)\Leftrightarrow x=0$ in $W(R)$.
$\therefore p$ is not a zero divisor.

③. Completeness: Follows from $W(R_J)$ is complete, $W(I)$ is closed under p-adic topology.

④. Separatedness: $\bigcap_{n\geq 0}(p^nS_J+W(I)) = W(I) \Rightarrow \bigcap p^n W(R)=\{0\}$.

⑤. Uniqueness: If there is a $W(R)'$. mapping $\sum p^i[x_i]\in W(R)$ to $\sum p^i[x_i]\in W(R)'$ gives a bijective ring homomorphism.

⑥. Functorality: $f: R\to R'$, define $W(f): \sum p^i[x_i]\mapsto \sum p^i[f(x_i)]$. is a ring homomorphism

$\square$

We define the Frobenius map φ on $W(R)$ given by $W(x \mapsto x^p)$, which is an automorphism.

<u>Thm</u> If R is perfect of char. p, A is complete for p-adic topology, then any ring map $f: R \to A/pA$ lifts to $W(f): W(R) \to A$.

Pf: The point is although A/pA is not perfect, we are not able to take p^n-th root in A/pA. We can always do this in R.

$\forall x \in R$, let $\{x_{(i)}\}$ be a sequence s.t. $x_{(0)} = x$, $x_{(i)}^p = x_{(i-1)}$

let $\hat{f}$ be any set-theoritical lift of f.

Define $W(f)([x]) := \lim\limits_{n\to\infty} \hat{f}(x_{(n)})^{p^n}$.

and $W(f)(\sum p^i [x_i]) := \sum p^i W(f)([x_i])$

$W(f)$ is additive: Let S_k be the universal formula $\in \mathbb{F}_p[X_i, Y_i]$.

Let $S_{k,(n)}(X_i^{p^{-n}}, Y_i^{p^{-n}}) \in \mathbb{F}_p[X_i^{p^{-n}}, Y_i^{p^{-n}}]$ s.t.

$S_{k,(0)}(X_i, Y_i) = S_k(X_i, Y_i)$, $(S_{k,(n)}(X_i^{p^{-n}}, Y_i^{p^{-n}}))^p = S_{k,(n-1)}(X_i^{p^{-(n-1)}}, Y_i^{p^{-(n-1)}})$

Let $\widehat{S_{k,(n)}}$ be arbitrary lift in $\mathbb{Z}_p[X_i^{p^{-n}}, Y_i^{p^{-n}}]$

Then in $\mathbb{Z}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]$, $\sum\limits_{k=0}^{n} p^k X_k + \sum\limits_{k=0}^{n} p^k Y_k \equiv \sum\limits_{k=0}^{n} S_{k,(n)}(X_i^{p^{-n}}, Y_i^{p^{-n}})^{p^n} \mod p^n$

$\therefore$ In A, $\sum\limits_{k=0}^{n} \hat{f}(x_{k,(n)})^{p^n} \cdot p^k + \sum\limits_{k=0}^{n} \hat{f}(y_{k,(n)})^{p^n} \cdot p^k \equiv \sum\limits_{k=0}^{n} S_{k(n)}(\hat{f}(x_{i,(n)}), \hat{f}(y_{i,(n)}))^{p^n} \mod p^n$

$\equiv \sum\limits_{k=0}^{n} \hat{f}(S_{k(n)}(x_{i,(n)}, y_{i,(n)}))^{p^n} \mod p^n$

$\downarrow$ $W(f)(\sum p^k [x_k]) + W(f)(\sum p^k [y_k])$

$\downarrow$ $W(f)(\sum p^k [S_k(x_i, y_i)])$

multiplicative is similar. $\square$

If A is complete for p-adic topology, let $\mathrm{Perf}(A/pA) := \varprojlim\limits_{x \mapsto x^p} A/pA$

Then $\mathrm{Perf}(A/pA)$ is perfect of char p. $(\cdots \to A/pA \xrightarrow{x \mapsto x^p} A/pA \xrightarrow{x \mapsto x^p} A/pA)$

$\forall x = (\cdots, x_2, x_1, x_0) \in \mathrm{Perf}(A/pA)$, the limit $\lim_{n\to\infty} \hat{x}_n^{p^n}$ convergence to a unique $x^{(0)}$ only depends on x.

Cor: The map $\theta: W(\mathrm{Perf}(A/pA)) \to A$ is a ring homomorphism.

$$\sum p^i [x_i] \longmapsto \sum p^i x_i^{(0)}$$

pf: follows immediately from previous thm.

§7. Galois cohomology.

We will not define the general Galois cohomology, instead we only focus on H^0 and H^1.

Let G, M be topological groups, M with a continuous G-action.

$H^0(G,M) := M^G$, $H^1(G,M) := \{\text{cocycles}\} \big/ \text{Cohomologous relation} = \dfrac{\{c: G\to M \mid c(gh) = c(g)\cdot g(c(h))\}}{c(g) \sim m^{-1} c(g) g(m) \quad \forall m \in M}$

Rmk: The cohomology class $[c]$ is trivial in $H^1(G,M)$ iff $c(g) = m^{-1} g(m)$ for some $m \in M$.

Long exact sequence Let R be a topological ring with continuous G action.

$0 \to X \to E \to Y \to 0$ is an exact sequence of R mods with G-action. then we have

$$0 \to X^G \to E^G \to Y^G \xrightarrow{\delta} H^1(G,X) \to H^1(G,E) \to H^1(G,Y)$$

δ is defined as: $\forall y \in Y^G$, $\exists e \in E$, image of e is y. $\delta(y)(g) = e - g(e) \in X$.

Restriction and inflation Let G, M be topological groups, H is a closed normal subgroup of G.

We have 2 maps:

$\mathrm{res}: H^1(G,M) \to H^1(H,M)$ $\qquad$ $\mathrm{infl}: H^1(G/H, M^H) \hookrightarrow H^1(G,M)$

$\mathrm{res}(c)(h) = c(h)$. $\qquad$ $\mathrm{infl}(c)(g) = c(\bar{g})$.

And there is a G-action on $H^1(H,M)$. $g(c)(h) := g(c(g^{-1}hg))$.

H acts trivially on it, so it's a G/H-action on $H^1(H,M)$.

(If $g \in H$, $g(c)(h) = g(\, c(g^{-1})\, g^{-1}(c(h))\, (g^{-1}h)(c(g))\,)$

$= \underbrace{g c(g^{-1})}_{= c(g)^{-1}} \cdot c(h) \cdot h(c(g)) \quad \Rightarrow \quad [g(c)] = [c]\,)$

Thm: G, M, H as above. Then $\exists$ an exact sequence

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{infl}} H^1(G,M) \xrightarrow{\text{res}} H^1(H,M)^{G/H}.$$

证: (1). $\text{res}(H^1(G,M)) \subseteq H^1(H,M)^{G/H}$

If $c \in H^1(G,M)$, $g \in G$. $g(\text{res}(c))(h) = g\,c(g^{-1}hg) = \underbrace{g\,c(g^{-1})}_{=\,c(g)^{-1}} \cdot c(h)\, h(c(g))$

$\Rightarrow [g(\text{res}(c))] = [\text{res}(c)]$, $[\text{res}(c)] \in H^1(H,M)^{G/H}$

(2). $\text{res}(c) = 0$ iff $c \in \text{infl}(H^1(G/H, M^H))$

"$\Leftarrow$" $\text{res} \circ \text{infl}(c)(h) = \text{infl}(c)(h) = c(\bar{1}) = 1$

"$\Rightarrow$" If $\text{res}(c) = 0$, the c is trivial on H. $\Rightarrow c(gh) = c(g)$ $c: G/H \to M$

and $h(c(g)) = \underbrace{c(h)^{-1}}_{=\,1} c(g) = c(g) \Rightarrow c(g) \in M^H$

$\therefore c \in \text{infl}(H^1(G/H, M^H))$.

Intepretation for $H^1(G, GL_d(R))$ and $H^1(G,M)$

1. Let R be a topological ring with continuous G action. X is a free R-mod of rank d with semilinear G-action. ($g(rx) = g(r)g(x)$, $r \in R, x \in X$) Let $e = \{e_1, \dots, e_d\}$ be a basis of X.

Then $\begin{matrix} G \to GL_d(R) \\ g \mapsto \text{Mat}_e(g) \end{matrix}$ is a cocycle. If e' is a different basis of X.

then $\text{Mat}_{e'}(g) = M^{-1}\,\text{Mat}_e(g)\,g(M)$. Thus we get a

$$H^1(G, GL_d(R)) \xleftrightarrow{1:1} \{\text{semilinear actions of } G \text{ on rank } d \text{ free } R\text{-mods}\}$$

2. Let M be a R-mod with semilinear G-action. E is an extension of R by M. $0 \to M \xrightarrow{\alpha} E \xrightarrow{\beta} R \to 0$

Choose $e \in E$ s.t. $\beta(e) = 1 \in R$ then $e - g(e) \in M$. $g \mapsto e - g(e)$ is a cocycle in M. different e' gives a cocycle different by $(e-e') - g(e-e')$, which is a coboundary.

$$\therefore H^1(G,M) \xleftrightarrow{1:1} \{\text{isom. class of extensions of } R \text{ by } M\}$$

Thm: If L/k is a finite Galois ext. $G = Gal(L/k)$, then

(1). $H^1(G, GL_d(L)) = \{1\}$

(2). $H^1(G, L) = \{0\}$

Pf: (1) For simplicity, assume L is an infinite field.

$\forall [U] \in H^1(G, GL_d(L))$, given $\alpha \in L$, define $P(\alpha) = \sum_{h \in G} U(h) \cdot h(\alpha) \in M_d(L)$

Then $U(g) \cdot g(P(\alpha)) = \sum_{h \in G} U(g)\, g(U(h))\, gh(\alpha) = \sum_{h \in G} U(gh)\, gh(\alpha) = P(\alpha)$.

So it suffices to find α s.t. $P(\alpha)$ is invertible, then $U(g) = P(\alpha)\, g(P(\alpha)^{-1}) \Rightarrow [U] = 1$.

Let $Q(X_g \mid g \in G) = \det\left(\sum_{g \in G} X_g U(g)\right)$. This polynomial is non-zero since $U(g)$ is invertible.

The following thm of Artin gives us $\exists \alpha \in L$ $Q(g\alpha)$ is not zero immediately.

Thm (Artin) Let L be an infinite field, $\sigma_1, \dots, \sigma_n$ are distinct elements of a finite group of automorphisms of L, Then $\sigma_1, \dots, \sigma_n$ are algebraically independent $/L$.

Pf: See [Lang, Algebra P_{311}].

(2). $\forall [f] \in H^1(G, L)$, define cocycle $U: g \mapsto \begin{pmatrix} 1 & f(g) \\ 0 & 1 \end{pmatrix}$, then $[U] \in H^1(G, GL_2(L))$

Now (1) tells us $\exists M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ s.t. $U(g) \cdot g(M) = M$ $\forall g$.

$$U(g) \cdot g(M) = \begin{pmatrix} g(a) + f(g)g(c) & g(b) + f(g)g(d) \\ g(c) & g(d) \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$\therefore$ $g(c) = c$, $g(d) = d$ $\forall g$. One of c, d is not zero.

Suppose $c \neq 0$, then $f(g) = \frac{a}{c} - g\left(\frac{a}{c}\right)$. $\Rightarrow [f]$ is trivial $\square$.

Cor: L/k is Galois extension (possibly infinite)

$G = Gal(L/k)$. L with discrete topology. If we only consider continuous cocycles, then $H^1(G, GL_d(L)) = \{1\}$. $H^1(G, L) = \{0\}$.

Pf: In both cases, a continuous cocycle must factors through some finite quotient $Gal(M/k)$. M/k is finite extension. Then apply the previous thm.

Prop Let A be a topological ring, $\pi \in A$ is a topological nilpotent element and π is not a zero-divisor. A is complete for p-adic topology. Let G be a group acting continuously on A with $\pi \in A^G$, and let $R = A/\pi A$. If $H^1(G, GL_d(R))$ and $H^1(G, R)$ are both trivial, ~~and $GL_d(A) \to GL_d(R)$ is surjective~~, then $H^1(G, GL_d(A))$ and $H^1(G, A)$ are both trivial.

Pf: If $[U] \in H^1(G, GL_d(A))$, $[\bar{U}] \in H^1(G, GL_d(R))$.

By triviality of $H^1(G, GL_d(R))$, and $GL_d(A) \to GL_d(R)$ surjects

$\exists M_0 \in GL_d(A)$ s.t. $M_0^{-1} U(g) g(M_0) \in Id + \pi M_d(A)$.

We proceed by induction. Suppose we have constructed $M_0, \cdots, M_{k-1}$ s.t.

$M_{k-1}^{-1} \cdots M_0^{-1} U(g) \cdot g(M_0 \cdots M_{k-1}) = Id + \pi^k C(g) \in Id + \pi^k M_d(A)$

Then $\bar{C}(g) \in H^1(G, M_d(R))$ (Since $Id + \pi^k C(gh) = (Id + \pi^k C(g))(Id + \pi^k g(C(h)))$)

$\Rightarrow \bar{C}(gh) = \bar{C}(g) + g(\bar{C}(h))$

If we write $M_k = Id + \pi^k R_k$.

$M_k^{-1} \cdots M_0^{-1} U(g) g(M_0 \cdots M_k) \equiv Id + \pi^k (R_k - g(R_k) + C(g)) \mod \pi^{k+1}$.

Thus the triviality of $H^1(G, R)$ allows us to find such R_k.

and let $M = \prod_{k=0}^{\infty} M_k \Rightarrow M^{-1} \cdot U(g) g(M) = Id$. This shows $H^1(G, GL_d(A))$ is trivial.

The proof of triviality of $H^1(G, A)$ is similar. $\square$

§8. The Dieudonné-Manin thm.

Ref: [Zink, Cartier theory of commutative formal groups, Chap VI]

Let k be a perfect field of char. p. $K = W(k)[\frac{1}{p}]$, $\sigma := W(x \mapsto x^p) : K \to K$ is called the absolute Frobenius. Since k is perfect, $\sigma^a(K) = K$ $\forall a \in \mathbb{Z}$.

Definition: A φ-module over K (D, φ) (or just D) is a finite dim'l K-vector space D with a bijective map $\varphi : D \to D$ that is σ^a-semilinear for some $a \in \mathbb{Z} \setminus \{0\}$.

Such a D is called <u>effective</u> if $\exists$ a $W(k)$ lattice $M \subseteq D$, s.t. $\varphi(M) \subseteq M$.

Now if M is a lattice of D, let $a_n = a_n(M)$ be the largest integer s.t. $\varphi^n(M) \subseteq p^{a_n} M$. Then $a_{n+m} \geq a_n + a_m$. Thus $\lim_{n\to\infty} \frac{a_n}{n}$ exists, and equals to $\lambda := \sup_n \frac{a_n}{n}$.

Rmk: (1). λ doesn't depend on M. $\forall M'$, $\exists e, f$ s.t. $p^e M \subseteq M'$, $p^f M' \subseteq M$.
$\Rightarrow a_n(M) - a_n(M')$ is bounded by a constant $C(e,f)$.
(2) $\lambda < \infty$. $\exists b$ s.t. $p^b M \subseteq \varphi(M)$. $\Rightarrow p^{bn} M \subseteq \varphi^n(M) \subseteq p^{a_n} M \Rightarrow \frac{a_n}{n} \leq b$.

Def: λ is called the <u>first slope</u> of the φ-module D.
Let $h = \dim_k(D)$, h is called the <u>height</u> of the φ-module D

Rmk: If $\varphi' = p^{-s}\varphi^r$, then $\lambda' = r\lambda - s$. λ depends on φ.

<u>Lemma 1</u>: If M is a lattice of D s.t. $\varphi^{h+1}(M) \subseteq p^{-1}M$, then $\exists M' \subseteq D$ s.t. $\varphi(M') \subseteq M'$.

Pf: Let $N = M + \varphi(M) + \cdots + \varphi^{h+1}(M)$. $\quad N_j = N + \varphi(N) + \cdots + \varphi^j(N)$
$$= M + \varphi(M) + \cdots + \varphi^{h+j+1}(M)$$
Then $N = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_{h+1} \subseteq p^{-1} N_0$.
Since $p^{-1}N_0/N_0$ is a k-vector space of dim h. N_i/N_0 is its subspace.
$\therefore \exists\, 0 \leq i \leq h$ s.t. $N_i = N_{i+1} \Rightarrow \varphi(N_i) \subseteq N_i$.

<u>Lemma 2</u>: If D is a φ-module,
(1). $\lambda \geq 0$ iff D is effective
(2). If $\lambda > 0$, then $\lambda \geq \frac{1}{h}$.

Pf: (1) "$\Leftarrow$" If D is effective, $\exists M$ s.t. $\varphi(M) \subseteq M$, then $a_n(M) \geq 0$ $\therefore \lambda \geq 0$.

"$\Rightarrow$" ① If $\lambda > 0$, then $a_n \geq 0$ for $n \gg 0$. $\therefore \exists M$, $\varphi^n(M) \subseteq M$

Let $M' = M + \varphi(M) + \cdots + \varphi^{n-1}(M) \Rightarrow \varphi(M') \subseteq M'$.

②. If $\lambda = 0$. Let $\varphi' = p \cdot \varphi^{h+1}$, then $\lambda' > 0$, by ①: $\exists M'$, $\varphi'(M') \subseteq M'$

i.e. $\varphi^{h+1}(M') \subseteq p^{-1}M'$. By Lemma 1, $\exists M$ s.t. $\varphi(M) \subseteq M$.

(2). If $\lambda > 0$, then φ is nilpotent on M/pM for any M s.t. $\varphi(M) \subseteq M$.

But $\dim_k(M/pM) = h$, φ is nilpotent $\Leftrightarrow \varphi^h = 0$ on M/pM $\Rightarrow \lambda \geq \frac{1}{h}$.

<u>Prop 3</u> If D is a φ-module, then its first slope $\lambda = \frac{s}{r}$ where $s, r \in \mathbb{Z}$, $1 \leq r \leq h$.

Pf: $\exists\, 1 \leq r \leq h$ s.t. $|r\lambda - s| \leq \frac{1}{h+1}$ (think $\mathbb{R}/\mathbb{Z}$ as a circle with $0, \lambda, 2\lambda, \cdots, h\lambda$ on it)

Set $\varphi' = p^{-s}\varphi^r \Rightarrow |\lambda'| \leq \frac{1}{h+1}$.

$\lambda' \geq \frac{1}{-(h+1)} \Rightarrow (D, p\cdot(\varphi')^{h+1})$ is effective $\underset{\text{Lem 1}}{\Rightarrow} (D, \varphi')$ is effective

$\Rightarrow \lambda' \geq 0$. But $\lambda' \leq \frac{1}{h+1} < \frac{1}{h}$ $\therefore \lambda' = 0$ by Lemma 2(2).

$\therefore \lambda = s/r$.

<u>Lemma 4</u>: If M is a $W(k)$-lattice of D. stable under φ, then $\exists!$ decomposition $M = M_0 \oplus M_{>0}$ s.t. $\varphi: M_0 \to M_0$ is bijective and $\varphi: M_{>0} \to M_{>0}$ is topologically nilpotent.

Pf: If $n \geq 1$, then M/p^nM is both Noetherian and Artinian

$\therefore \exists k>0$ s.t. $\bigcap_{j\geq 0} \mathrm{im}(\varphi^j) = \mathrm{im}(\varphi^k)$. $\bigcup_{j\geq 0} \ker(\varphi^j) = \ker(\varphi^k)$.

If $x \in M/p^nM$, $\exists y$ s.t. $\varphi^k(x) = \varphi^{2k}(y) \Rightarrow x = \underbrace{x - \varphi^k(y)}_{\in \ker\varphi^k} + \underbrace{\varphi^k(y)}_{\in \mathrm{im}\,\varphi^k}$.

So we may set $(M/p^nM)_0 = \mathrm{im}(\varphi^k)$

$(M/p^nM)_{>0} = \ker(\varphi^k)$. Then $M/p^nM = (M/p^nM)_0 \oplus (M/p^nM)_{\geq 0}$

This construction is compatible with projective limits

$\therefore$ We get a decomposition of $M = M_0 \oplus M_{\geq 0}$

Def If D is a φ-module, it is called <u>pure of slope $\lambda = \frac{s}{r}$</u>, with $s, r \in \mathbb{Z}$ if $\exists$ a lattice $M \subseteq D$, s.t. $p^{-s}\varphi^r|_M$ is a bijection.

<u>Rmk</u>: This implies D has first slope λ.

<u>Thm5</u>: If D is a φ-mod, $\exists$ rational numbers $\lambda_1 < \cdots < \lambda_k$ and a unique decomposition $D = \bigoplus_{i=1}^k D_{\lambda_i}$, where D_{λ_i} is pure of slope λ_i.

Pf: Let λ be the first slope of D, $\lambda = \frac{s}{r}$.

Set $\varphi' = p^{-s}\varphi^r$ then (D, φ') is effective.

By lemma 2, $\exists M$ that is φ' stable. Use lemma 4 to decompose M into $M_0 \oplus M_{>0}$ (both stable by φ'). $M_0 \neq 0$.

Tensoring with K we set $D_\lambda = M_0 \otimes K$ and $D_{>\lambda} = M_{>0} \otimes K$.

Now the thm follows by further decomposing $D_{>\lambda}$ until $M_{>0} = 0$.

Def Under the notation above, $\{\lambda_i\}$ are called the slopes of D.

Rmk: The first slope is the minimal slope of D.

Def: A φ-module over k (of char p) is a finite dimensional k-vector space V, with $\varphi: V \to V$ being a σ^a-semilinear map (where σ is the Frobenius map) for some $a \in \mathbb{Z} \setminus \{0\}$, and $\mathrm{Mat}(\varphi) \in GL_{\dim(V)}(k)$.

Thm 6. If k is separably closed of characteristic p, V is a φ-module over k, with $a \geq 1$, then

(1). V admits a basis of elements fixed by φ.

(2). $1-\varphi: V \to V$ is surjective.

Pf: Choose an arbitary $e_0 \in V$, let $e_i = \varphi^i(e_0)$, $d = \dim(\mathrm{span}\{e_i\})$

$\therefore$ We may write $e_d = a_0 e_0 + \cdots + a_{d-1} e_{d-1}$

The equation $\varphi(b_0 e_0 + \cdots + b_{d-1} e_{d-1}) = b_0 e_0 + \cdots + b_{d-1} e_{d-1}$ is equivalent to

$$\begin{cases} b_0 = b_{d-1}^q a_0 \quad (q = p^a) \\ b_i = b_{i-1}^q + b_{d-1}^q a_i, \quad 1 \leq i \leq d-1. \end{cases}$$

If we set $x = b_{d-1}$, then other b_j's are determined by x and a_i provided that $x = a_0^{q^{d-1}} x^{q^d} + \cdots + a_{d-1} x^q$. Note that $a_0^{q^{d-1}} x^{q^d - 1} + \cdots + a_{d-1} x^{q-1} = 0$ is a separable equation. Thus it has solutions in k, so we get a $v \neq 0$, $v \in V^{\varphi=1}$

We proceed by induction. Induction hypothesis of (1) $\Rightarrow$ V/kv admits a basis $\bar{v}_1, \ldots, \bar{v}_{n-1}$ fixed by φ. Suppose $\varphi(v_i) = v_i + \alpha_i v$. v_i is an arbitary lift of $\bar{v}_i$. Then let $u_i = v_i + \beta_i v$, $\varphi(u_i) = v_i + (\alpha_i + \beta_i^q) v = u_i + (\alpha_i + \beta_i^q - \beta_i) v$

Since $x^q - x + \alpha_i = 0$ is separable, we may find solutions $\beta_i \in k \Rightarrow \varphi(u_i) = u_i$.
So we get $\{v, u_1, \dots, u_{n-1}\}$ is a basis of V fixed by φ.
And $1-\varphi|_{ku}$ is surjective for any u fixed by φ, since $(1-\varphi)(\beta u) = (\beta - \beta^q)u$
and $\beta^q - \beta + \alpha = 0$ is solvable for any $\alpha \in k$. Since $\mathrm{span}\{V^{\varphi=1}\} = V$, $1-\varphi$ is surjective on V

<u>Def</u> If A is complete for p-adic topology, $A/pA = k$ as above, with a Frobenius σ lifting $x \mapsto x^p$, then a <u>φ-module over A</u> is a free A-module V of finite rank, with $\varphi: V \to V$, σ^a-semilinear for some $a \in \mathbb{Z}\setminus\{0\}$, s.t. $\mathrm{Mat}(\varphi)$ is in $GL_{\mathrm{rank}(V)}(A)$.

<u>Cor</u>: If V is a φ-module over A, $a \geq 1$, then
(1). V admits a basis of elements fixed by φ
(2). $1-\varphi: V \to V$ is surjective.

<u>Pf</u>: (1). by previous thm, $\exists v_1, \dots, v_n$ s.t. $\varphi(v_i) \equiv v_i \bmod p$. Suppose $\varphi(v_i) = v_i + pw_i$
We want to find z_i s.t. $\varphi(v_i + pz_i) \equiv v_i + pz_i \bmod p^2$. $\Leftrightarrow (1-\varphi)(z_i) \equiv w_i \bmod p$.
Such a z_i exists by (2) of previous thm. Proceed by induction we get $\tilde{v}_i$ s.t. $\varphi(\tilde{v}_i) = \tilde{v}_i$. The proof of (2) is similar.

<u>Rmk</u>: If k is algebraically closed (instead of separably closed), the above results are true for $\forall a \in \mathbb{Z}\setminus\{0\}$ (instead of $a \geq 1$).

Now let k be an algebraically closed field. $K = W(k)[\frac{1}{p}]$, $\lambda = \frac{s}{r} \in \mathbb{Q}_{\geq 0}$ with $s, r \geq 0$, $\gcd(s,r) = 1$.

<u>Def</u>: <u>E_λ, the elementary φ-module over K of slope λ</u>, is given by $E_\lambda = \bigoplus_{i=0}^{r-1} K e_i$

as a K-module, φ's action is given by

$$\begin{cases} \varphi(e_0) = e_1 \\ \quad \vdots \\ \varphi(e_{r-2}) = e_{r-1} \\ \varphi(e_{r-1}) = p^s e_0 \end{cases}$$

Prop 8: The φ-module E_λ is irreducible.

Pf: Suppose $D \subsetneqq E_\lambda$ is a sub-φ-module, thus stable under φ.
By thm 5, D is a direct sum of pure φ-mod. We may replace D by its pure submodule to assume D is pure of some slope d/h, $\dim D \geq h$.
Let $\varphi' = p^{-d}\varphi^h$, by cor 7(1) $\exists\, y \in D$, $y \neq 0$, $(1-\varphi')(y) = 0$. i.e. $\varphi^h(y) = p^d y$.
If $y = \sum_{i=0}^{r-1} y_i e_i$, $\varphi^{rh}(y) = p^{rd} y \Rightarrow p^{sh}(\sigma_a)^{rh}(y_i) = p^{rd} y_i \Rightarrow sh = rd$
$\therefore \frac{s}{r} = \frac{d}{h}$, but $\gcd(s,r) = 1$. $\dim D \geq h \geq r \Rightarrow D = E_\lambda$.
Therefore E_λ is irreducible.

Thm 9. If k is algebraically closed, $K = W(k)[1/p]$, D is a φ-module over K.
Then $\exists!$ decomposition $D = E_{\lambda_1}^{m_1} \oplus \cdots \oplus E_{\lambda_n}^{m_n}$, each m_λ only depends on D.

Pf: By thm 5, $D = \oplus D_{\lambda_i}$, D_{λ_i} pure of slope λ_i. So it suffices to show for any pure φ-module D of slope $\lambda = \frac{s}{r}$, $D = E_\lambda^m$, $m = \frac{\dim D}{r}$.
By cor 7 (applied to $p^{-s}\varphi^r$), there is a basis of D consisting elements in $D^{\varphi^r = p^s}$. Choose any $y \in D^{\varphi^r = p^s}$, we may define a map $E_\lambda \to D$.
$(a_0 + a_1\varphi + \cdots + a_{r-1}\varphi^{r-1})e_0 \mapsto (a_0 + a_1\varphi + \cdots + a_{r-1}\varphi^{r-1})y$. Since E_λ is irreducible,

The map is injective as long as $y \neq 0$.

Now if we have $y_1, \dots, y_k \in D^{\varphi^r = p^s}$, giving an injective map $E_\lambda^k \to D$, either it is already surjective, or we can take y_{k+1} outside its image in $D^{\varphi^r = p^s}$.

Then the map induced by $y_1, \dots, y_{k+1} : E_\lambda^{k+1} \to D$ is still injective.

Proceed by induction, we get $D \cong E_\lambda^m$. This finishes the proof.