Recall that:
- We want to classify complete dvrs. This is done by first splitting according to characteristics: 
  \((0,0), (p,p), (0,p)\).
- Equal case \((0,0)\) and \((p,p)\): we saw these are just \(k[[T]]\), \(k\) residue field.
- Case \((0,p)\): based on absolute ramification index \(e = v(p)\).
- We assume the residue field \(k\) is perfect.

Claim: There's an equivalence of categories

\[
\begin{cases}
\text{absolutely unramified complete dvrs} \\
\text{of characteristic } (0,p) \\
\text{with perfect residue field}
\end{cases} \rightarrow \begin{cases}
\text{perfect fields} \\
\text{of characteristic } p
\end{cases}
\]

with the inverse functor given by some \(k \mapsto W(k)\).

This will clarify the total picture: Any complete dvr of char. \((0,p)\) with residue field \(k\), is a totally ramified extension of \(W(k)\), of degree \(e = v(p)\).

The claim is proved by passing to more general objects:

A **p-ring**: a ring \(A\), with topology induced by a system of ideals \(a_1 \supset a_2 \supset \cdots\) satisfying \(a_n \cdot a_m \subset a_{nm}\), that is complete and Hausdorff, i.e.

\[
A \cong \lim_{\leftarrow n} A/a_n, \quad \bigcap_n a_n = 0,
\]

and \(A/a_1\) is a perfect ring of characteristic \(p\).

A **strict p-ring**: A p-ring with \(a_n = p^n A\), and \(p\) not a zero divisor. Essentially, when \(p\) is a “uniformizer” (without quotes if \(A/a_1\) is a field).

A perfect ring of characteristic \(p\) is one in which \(x \mapsto x^p\) is an automorphism.

Claim: There's an equivalence of categories

\[
\begin{cases}
\text{strict p-rings} \\
\text{with perfect residue ring}
\end{cases} \rightarrow \begin{cases}
\text{perfect rings} \\
\text{of characteristic } p
\end{cases}
\]

The previous claim follows from this, because:

abs. unramified complete dvr of char. \((0,p)\) with residue field \(k = \text{strict p-ring with residue field } k\)
Example 9.1. A complete dvr $A$ with characteristic $(0, p)$ is a $p$-ring. If the maximal ideal $m$ is $pA$, it is also strict, for instance $A = \mathbb{Z}_p$, or $\mathbb{Z}_p[\sqrt{-1}]$ if $p \equiv 3 \text{ (mod 4)}$. The ring $\mathbb{Z}_5[\sqrt{5}]$ is a $p$-ring, but not a strict one. $\mathbb{F}_p[[T]]$ is not a $p$-ring.

Example 9.2. $\mathbb{Z}_p[[T]]$ with topology induced by the ideal $(p, T)$ is a $p$-ring that is not strict. Its residue ring $\mathbb{F}_p$ is a field, but it’s not a dvr. Its maximal ideal is not principal.

**Key facts:**

1. $p$-rings $A$ have Teichmüller representatives: a unique multiplicative section $\omega : k \to A$. Its image is all the elements that admit $p^n$th roots for all $n$.
2. In strict $p$-rings every element has a $p$-power series, i.e. is of the form
   \[ \sum_{n=0}^{\infty} \omega(\alpha_n)p^n, \]
   with $\alpha_n \in k$.

Suppose we have a commutative diagram

\[
\begin{array}{ccc}
A & \xrightarrow{\phi} & A' \\
\downarrow & & \downarrow \\
k & \xrightarrow{f} & k'
\end{array}
\]

where $A, A'$ are $p$-rings with residue rings $k, k'$.

**Observations:**

- $\phi$ must preserve $p^n$th powers, so it must preserve Teichmüller representatives, i.e.
  \[ \omega_A(f(\alpha)) = \phi(\omega_A(\alpha)). \]
- If $A$ is strict, $\phi$ is determined by $f$:
  \[ \phi(a) = \phi(\sum_{n=0}^{\infty} \omega_A(\alpha_n)p^n) = \sum_{n=0}^{\infty} \phi(\omega_A(\alpha_n))p^n = \sum_{n=0}^{\infty} \omega_A'(f(\alpha_n))p^n \] \hspace{1cm} (3)

We want to construct a strict $p$-ring for any perfect ring $k$. In fact we know that a strict $p$-ring is in bijection with $k[[T]]$ via

\[ \sum_{n=0}^{\infty} \alpha_n T^n \mapsto \sum_{n=0}^{\infty} \omega(\alpha_n)p^n \]

Need to know how to add, subtract, multiply the $p$-power series.

**Idea:** Construct some huge “free” strict $p$-rings to find universal formulas.

Let $X_1, X_2, \ldots, Y_1, Y_2, \ldots$ be variables. Put

\[ S = \mathbb{Z}[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}], \]

and consider the completion $\widehat{S}$ with respect to ideals $p^nS$. This is a strict $p$-ring with residue ring

\[ \overline{S} = \mathbb{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]. \]

We have two distinguished elements of $\widehat{S}$, they are

\[ x = \sum_{n=0}^{\infty} X_n p^n, \quad y = \sum_{n=0}^{\infty} Y_n p^n. \]
The $X_i$ and $Y_i$ are the coordinates of $x$ and $y$. Now $x \cdot y$ also has some coordinates:

$$x \cdot y = \sum_{n=0}^{\infty} \omega(P_n)p^n,$$

where $P_n = P_n(X_i, Y_i) \in \overline{S} = \mathbb{F}_p[X_p^{\infty}, Y_p^{\infty}]$. Similarly there are polynomials $Q_n$ and $R_n$ that provide coordinates for $x + y$ and $x - y$.

Given any $p$-ring $A$, with $a, b \in A$. Suppose

$$a = \sum_n \omega_A(\alpha_n)p^n, \quad b = \sum_n \omega_A(\beta_n)p^n$$

for some coordinates $\alpha_n, \beta_n$ via $\omega_A : k \to A$. Then there’s a map $S \to A$, sending $X_i, Y_i$ to $\omega_A(\alpha_i), \omega_A(\beta_i)$. It extends by continuity to $\varphi : \hat{S} \to A$, still sending $x, y$ to $a, b$. So we have $\varphi(X_i) = \omega_A(\alpha_i)$. Then

$$a \cdot b = \varphi(x \cdot y) = \varphi(\sum X_n p^n \cdot \sum Y_n p^n) = \varphi(\sum \omega(P_n(X_i, Y_i))p^n) = \sum \omega_A(P_n(\alpha_i, \beta_i))p^n$$

- This shows that on elements that have a $p$-power series expansion, multiplication, addition, subtraction are all given by the same formulas as in $\hat{S}$.
- It implies you can lift $f : k \to k'$ to $\varphi : A \to A'$ as long as $A$ is strict: we already know what the value of $\varphi$ has to be (determined by (3)), now we can verify it respects addition and multiplication.
- That implies the functor in the claim is fully faithful.
- It remains to show essential surjectivity: to construct strict $p$-rings for any perfect ring $k$ of char. $p$.

**Note:** if $A \to k$ is a strict $p$-ring and $f : k \to k'$ is surjective, we can construct $A'$ as a quotient:

$$a, b \in A, \quad a \sim b \iff f(\alpha_i) = f(\beta_i) \forall i.$$  

**Exercise.** Describe the kernel of $A \to A'$ a different way.

**Evident Fact:** Given any perfect ring $k$, there’s a surjective map from some $\mathbb{F}_p[X_n^{p^{\infty}}]$ to it, where $\alpha \in I, I$ some large indexing set. That is the residue ring of a strict $p$-ring like $\hat{S}$.

Then we are done. We have proven our claim.

**Theorem 9.1.**— For every perfect ring $k$ of characteristic $p$, there is a unique strict $p$-ring $A$ with residue ring $k$ (up to isomorphism). The functor $A \rightsquigarrow k$ from strict $p$-rings to perfect rings with char. $p$ is an equivalence of categories.

**Corollary 9.1.1.**— The map $A \to k$ from absolutely unramified complete dvrs of char. $(0, p)$ with residue field $k$ to $k$ is an equivalence of categories.

Some consequences:

Suppose $A$ is a complete dvr, of mixed characteristic, $K$ fraction field, $m$ maximal ideal, etc.

Suppose $L_1, L_2$ are unramified extensions of $K$, with integers $B_1, B_2$, residue fields $k_1, k_2$. Then

$$\text{Hom}_K(L_1, L_2) \cong \text{Hom}_A(B_1, B_2) \cong \text{Hom}_k(k_1, k_2).$$

In fact, only need $L_1$ to be unramified.
In particular,
\[ \text{Gal}(L_1/K) \cong \text{Gal}(k_1/k). \]

**Example 9.3.** Consider the extension \( \mathbb{F}_{5^3} \) of \( \mathbb{F}_5 \). It’s defined by any third degree monic irreducible polynomial, e.g. \( x^3 + 3x + 3 \). The strict \( p \)-ring corresponding to \( \mathbb{F}_5 \) is \( \mathbb{Z}_5 \). Put
\[ K = \mathbb{Q}_5[X]/(X^3 + 3X + 3). \]

The residue degree of \( K/\mathbb{Q}_p \) is \( f = 3 \). We have \( n = ef \) and \( n = 3 \), so \( e = 1 \). The ring of integers of \( K \) is the unique complete absolutely unramified dvr of characteristic 0 and residue field \( \mathbb{F}_p^3 \).

**Example 9.4.** To construct ramified extensions we use Eisenstein polynomials. Consider
\[ P(X) = X^3 - 5. \]
This is clearly irreducible over \( \mathbb{Q} \). It’s also irreducible over \( \mathbb{Q}_5 \), but not over \( \mathbb{F}_5 \): Hensel’s lemma doesn’t apply as it’s not separable over \( \mathbb{F}_5 \). Put
\[ L = \mathbb{Q}_5[X]/((X^3 - 5)) = \mathbb{Q}_5(\sqrt[3]{5}). \]
The residue field of \( L \) is evidently just \( \mathbb{F}_5 \). Then \( f = 1 \), so \( e = 3 \). \( L \) is a totally ramified extension of \( \mathbb{Q}_5 \).

Any totally ramified extension of \( \mathbb{Q}_p \) can be defined by an Eisenstein polynomial. The non-leading coefficients of such a polynomial must must lie in \( p\mathbb{Z}_p \), a compact open subset of \( \mathbb{Q}_p \). But recall from homework that two irreducible polynomials whose coefficients are close enough will define the same extension. This shows there are only finitely many ramified extensions of \( \mathbb{Q}_p \) of a given degree.

In fact any absolutely unramified complete dvr of characteristic \((0, p)\) will have only finitely many totally ramified extensions of a given degree \( n \). The argument is the same.