Remark 0.0.1. Let L/K be a Galois extension of fields, i.e. normal and separable. Let $\mathcal{I}$ be the set of finite Galois extensions of K contained in L and order this set by inclusion. Then for each pair $E, F \in \mathcal{I}$, we have $EF \in \mathcal{I}$. Thus

(1) $\mathcal{I}$ is directed.
(2) $L = \cup_{E \in \mathcal{I}} E$.

We can study inverse limits over this directed set. An element $\gamma = (\gamma_E) \in \prod_{E \in \mathcal{I}} \mathrm{Gal}(E/K)$ is contained in

$$\varprojlim_{E \in \mathcal{I}} \mathrm{Gal}(E/K)$$

if and only if $\gamma_F|_E = \gamma_E$ for $E \subset F \in \mathcal{I}$.

Lemma 0.0.2. The restriction maps induce an isomorphism of groups

$$\mathrm{Gal}(L/K) \to \varprojlim_{E \in \mathcal{I}} \mathrm{Gal}(E/K).$$

Remark 0.0.3. Given the discrete topology on each finite group $\mathrm{Gal}(E/K)$, the group $\mathrm{Gal}(L/K)$ is then a profinite group.

Lemma 0.0.4. There is a bijection between intermediate extensions $L/E/K$ and closed subgroups $H \subset \mathrm{Gal}(L/K)$ given by

$$E/K \mapsto \mathrm{Gal}(L/E)$$

and

$$H \mapsto L^H.$$

Moreover, the bijection induces bijections between

(1) finite extensions and open subgroups;
(2) finite Galois extensions and open normal subgroups;
(3) Galois extensions and closed normal subgroups.

Example 0.0.5. Let $K = \mathbb{F}_q$ with $q = p^f$. Let $\overline{K}$ be an algebraic closure of K with Galois group $G = \mathrm{Gal}(\overline{K}/K)$. For each $n \geq 1$, there exists a unique extension K_n of degree n of K contained in $\overline{K}$ (consider $x^{q^n} - x$). The extension K_n/K is a cyclic extension with Galois group

$$\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/n\mathbb{Z} = \langle \varphi_n \rangle,$$

where $\varphi_n = (x \mapsto x^q)$ is called the arithmetic Frobenius of $\mathrm{Gal}(K_n/K)$. Then

$$G \simeq \varprojlim_n \mathrm{Gal}(K_n/K) \simeq \varprojlim_n \mathbb{Z}/n\mathbb{Z} \simeq \widehat{\mathbb{Z}}.$$

Definition 0.0.6. Let p be a prime. Let X, Y, X_i, Y_i be indeterminates where $i \in \mathbb{N}$. Write $\underline{X} = (X_0, X_1, \dots)$ and $\underline{Y} = (Y_0, Y_1, \dots)$. The n-th Witt polynomial of $\underline{X}$ is

$$W_n(\underline{X}) = W_n(X_0, \dots, X_n) = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}.$$

Example 0.0.7.

$$\begin{aligned} W_0 &= X_0 \\ W_1 &= X_0^p + pX_1 \\ W_2 &= X_0^{p^2} + pX_1^p + p^2 X_2 \end{aligned}$$

Lemma 0.0.8. We have

$$X_n \in \mathbb{Z}[p^{-1}][W_0, \dots, W_n].$$

Lemma 0.0.9. Let $\Phi(X, Y) \in \mathbb{Z}[X, Y]$. There exists a unique sequence of polynomials $(\Phi_n)_{n \in \mathbb{N}}$

$$\Phi_n \in \mathbb{Z}[X_0, X_1, \dots, X_n, Y_0, Y_1, \dots, Y_n]$$

such that for every $n \in \mathbb{N}$,

$$\Phi(W_n(\underline{X}), W_n(\underline{Y})) = W_n(\Phi_0, \dots, \Phi_n).$$

The same result holds after replacing $\mathbb{Z}$ by $\mathbb{Z}_p$.

Proof. The equation

$$\Phi(W_n(\underline{X}), W_n(\underline{Y})) = W_n(\Phi_0, \dots, \Phi_n),$$

or equivalently,

$$\Phi(W_n(\underline{X}), W_n(\underline{Y})) = \sum_{i=0}^{n} p^i \Phi_i^{p^{n-i}}.$$

Hence, the polynomials $(\Phi_n)_{n\in\mathbb{Z}}$ exist and are unique, with coefficients in $\mathbb{Z}[p^{-1}]$. In other words,

$$\Phi_n \in \mathbb{Z}[p^{-1}][X_0, \dots, X_n, Y_0, \dots, Y_n]$$

is given inductively by the formula

$$\Phi_n = \frac{1}{p^n}\left(\Phi\left(\sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n} p^i Y_i^{p^{n-i}}\right) - \sum_{i=0}^{n-1} p^i \Phi_i^{p^{n-i}}\right).$$

Next, we use induction on $n \geq 0$ to show that the coefficients are integral. For $n = 0$, we have $\Phi_0 = \Phi(X_0, Y_0)$. For $n = 1$, we have

$$\begin{aligned} p\Phi_1 &= \Phi(X_0^p + pX_1, Y_0^p + pY_1) - \Phi(X_0, Y_0)^p \\ &\equiv \Phi(X_0^p, Y_0^p) - \Phi(X_0, Y_0)^p \mod p \\ &\equiv 0 \mod p. \end{aligned}$$

Hence the coefficients of Φ_1 are integers. For general $n \geq 1$, we argue as follows. We have

$$\begin{aligned} p^n\Phi_n(\underline{X}, \underline{Y}) &= \Phi\left(\sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n} p^i Y_i^{p^{n-i}}\right) - \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}} \\ &\equiv \Phi\left(\sum_{i=0}^{n-1} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n-1} p^i Y_i^{p^{n-i}}\right) - \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}} \mod p^n \\ &= \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}^p, \underline{Y}^p)^{p^{n-1-i}} - \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}} \mod p^n, \end{aligned}$$

where $\underline{X}^p$ and $\underline{Y}^p$ denote $(X_0^p, \dots)$ and $(Y_0^p, \dots)$ respectively. It remains to prove that

$$\Phi_i(\underline{X}^p, \underline{Y}^p)^{p^{n-i-1}} \equiv \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}} \mod p^{n-i},$$

which follows from a direct induction and the next lemma. □

Lemma 0.0.10. Let p be a prime. Let $a, b \in \mathbb{Z}$. Let $k \geq 1$. If $a \equiv b \bmod p^k$, then $a^p \equiv b^p \bmod p^{k+1}$.