Hilbert Decomposition Theory

Recall that $B$ is a commutative ring with $1_R$, $G \subseteq \text{Aut}(B)$ is a profinite group acting continuously on $B$ endowed with the discrete topology, and $A = B^G$ is the point wise fixed subring of $B$. Then $B|A$ is an integral ring extension (WHY), hence $\text{Spec}(B) \to \text{Spec}(A)$ is surjective (WHY). Let $\mathcal{S}$ denote the set of finite subsets $\Sigma \subseteq B$ such that $G(\Sigma) = \Sigma$, and consider the partial ordering $\geq$ on $\mathcal{S}$ defined by $\Sigma'' \geq \Sigma' \iff \Sigma'' \supseteq \Sigma'$. Let $B_\Sigma := A[\Sigma] \subset B$ be viewed as an subextension of $B|A$, and consider the canonical projections

$$\pi : \text{Spec}(B) \xrightarrow{\rho_\Sigma} \text{Spec}(B_\Sigma) \xrightarrow{\sigma_\Sigma} \text{Spec}(A), \ q \mapsto q_\Sigma \mapsto p, \text{ and fibers } X_p \to X_{\Sigma, p} \to \{p\}$$

Finally, let $I_q \triangleleft D_q$ and $I_{q_S} \triangleleft D_{q_S}$ be the inertia/decomposition groups.

1) Prove the assertions from the class:
   a) $\forall \Sigma' \subset B$ finite $\exists \Sigma \in \mathcal{S}$ s.t. $\Sigma' \subset \Sigma$, hence $B = \cup_\Sigma B_\Sigma, \ q = \cup_\Sigma q_\Sigma$.
   b) $N_\Sigma := \{\sigma \in G | \sigma|_{B_\Sigma} = \text{id} \} \triangleleft G$ is an open normal subgroup in $G$.
   c) $G_\Sigma := G|_{B_\Sigma} \cong G/N_\Sigma$ canonically, and $G_\Sigma$ is finite and acts on $B_\Sigma$, and $B_\Sigma^{G_\Sigma} = A$.
   d) $(G_\Sigma)^\Sigma$ is a canonically a projective system, and $G = \varprojlim G_\Sigma$ canonically.

2) Complete the proofs of the assertions from the class:
   a) $D_q = \varprojlim_{\Sigma} D_{q_\Sigma}$, $I_q = \varprojlim_{\Sigma} I_{q_\Sigma}$, and $X_{\Sigma, p} \cong G_\Sigma/D_{q_\Sigma}$ as $G_\Sigma$-space, $X_p \cong G/D_q$ as $G$-space.
   b) $X_{\Sigma, p}$ are finite discrete spaces in the Zariski topology, $(X_\Sigma)^\Sigma$ is canonically a projective system, and $X_p = \varprojlim_{\Sigma} X_{\Sigma, p}$ as topological spaces endowed with the Zariski topology.
   c) The $G$ acts continuously on $X_p$, and $X_p \cong G/D_q$ as topological $G$-spaces.

3) Prove that for the ring extension $B|A$ the going down holds.

From now on, suppose that $B$ is an integrally closed domain, hence $A = B^G$ is integrally closed (WHY), and $K = \text{Quot}(A) \subseteq \text{Quot}(B) = L$ is a Galois extension with $G = \text{Gal}(L|K)$ (WHY). For subextensions $L'|K$ of $L|K$, set $B' = B \cap L'$, $q' := L' \cap q$. Thus if $G' = \text{Gal}(L|L')$, then $B' = B^{G'}$ is the integral closure of $A$ in $L'$.

4) Complete the proofs of the assertions from the class:
   a) $B^D | A$ is the minimal subextension $B'|A$ of $B|A$ such that $|X_{q'}| = 1$, and further one has: $\kappa(q^D) = \kappa(p)$, $q^D_{q'} = p B^D_{q'}$.
   b) $B^I | A$ is the maximal subextension $B'|A$ of $B|A$ such that $|X_{p'}| = 1$ and further satisfies: $\kappa(q^I) | \kappa(p)$ is the separable part of $\kappa(q) | \kappa(p)$, and $q^I_{q'} = p B^I_{q'}$.

Henselization

Recall the definition of the Henselization $A^h, m^h$ of a local ring $A, m$. Suppose that $A$ is an integrally closed domain, $K = \text{Quot}(A)$, and $A^s \subset K^s$ be the integral closure of $A$ in
a separable closure $K^s$ of $K$. Further, let $m^s \in X_m$ be a prime ideal of $A^s$ above $m$, and $K^D \subset K^s$ be the decomposition field of $m$ and $A^D \subset A^s$, $m^D \subset m^s$ be correspondingly defined. Finally, denote $m^h := m^D_v \subset A^D_v =: A^h$.

5) Study the proof of the following famous and very useful:

**Theorem.** $A^h, m^h$ be the Henselization of $A, m$.

**Hilbert Decomposition Theory for Valuations**

Let $O, m$ be the valuation ring/ideal of $K$, $L|K$ be a Galois extension, $G = \text{Gal}(L|K)$, and $\bar{O} \subset L$ be the integral closure of $O$ in $L$. Let $x_v$ be the set of prolongations $w|v$ of $v$ to $L$, and $X_m \subset \text{Spec}(\bar{O})$ be the fiber of $\text{Spec}(\bar{O}) \rightarrow \text{Spec}(O)$ above $m$.

6) Complete the proofs of the following assertions from the class:
   a) $X_v \rightarrow X_m$, $m_w \mapsto n_w := m_w \cap \bar{O}$ is a bijection.
   b) $D_{n_w} = \{\sigma \in G \mid w \circ \sigma = w\} = \{\sigma \in G \mid w(x) \geq 0 \Rightarrow w(\sigma x - x) \geq 0\}$
   c) $I_{n_w} = \{\sigma \in G \mid w(x) \geq 0 \Rightarrow w(\sigma x - x) > 0\}$

**Terminology/Notation:** Denoting by $I := I_w \triangleleft D := D_w \subset G$ the inertia/decomposition groups of $w$ in $G = \text{Gal}(L|K)$, the corresponding fixed fields $L^D \subset L^I$ are called the decomposition/inertia (sub)fields of $w$ in $L|K$ and/or $\text{Gal}(L|K)$. In particular, if $w|w^I|w^D|v$ are the corresponding prolongations of $v$, by Problem 4) above one has:

- $L^D$ is the minimal subextension $L'$ of $L$ such that $v' := w|L'$ satisfies $|X_{v'}| = 1$, and further one has: $\kappa(w^D) = \kappa(v)$, $m_{w^D} = m_vO_{w^D}$.
- $L^I$ is the maximal subextension $L'$ of $L$ such that $v' := w|L'$ satisfies $|X_{v'}| = 1$ and further: $\kappa(w')|\kappa(v)$ is separable, and $m_{w'} = m_vO_{w'}$.

**The ramification group**

In the previous notation, let $w \in X_v$ be fixed, $\kappa := \kappa(w) = O_w/m_w$ be the residue field of $w$, and $\mu_\kappa \leq \kappa^x$ be the group of roots of unity in $\kappa$. In particular, since $\mu_\kappa$ consists of separable elements over $\kappa(v)$, one has $\mu_\kappa \leq \kappa(w^I)$. Recall that in the above notation,

$$V_w := \{\sigma \in G \mid w(x) \geq 0 \Rightarrow w(\sigma x - x) > w(x)\}$$

is called the ramification group of $w|v$. The fixed field $L^v$ of $V := V_w$ in $L$ is called the ramification field of $w$ in $L$, and since $V \subset I$, one has: $\kappa(w')|\kappa(w^I)$ is purely inseparable (WHY).

7) Prove the following assertions (some from the class):
   a) If $w' := w \circ \sigma \in X_v$ for some $\sigma \in G$, then $V_{w'}$ and $V_w$ are conjugated under $\sigma$.
   b) $V_w \leq I_w$ is a normal subgroup in both $I_w$ and $D_w$.

**Functorial behavior.** Let $K'|K$ be a subextension of $L|K$, $G' := \text{Gal}(L|K')$, $v' := w|_{K'}$.

   c) One has:
- $V_{w|v'} = V_w \cap G'$.
- If $K'|K$ is Galois, one has an exact sequence: $1 \rightarrow V_{w|v'} \rightarrow V_w \rightarrow V_{w|v} \rightarrow 1$.  

The canonical pairing

8) Define $\psi : I_w \times L^\times \to \kappa^\times$, $(\sigma, x) \mapsto \sigma(x)/x \mod m_w$. Prove the following:
   a) $\psi$ is a well defined pairing of groups, and its image lies in $\mu \subset \kappa(w')$.
   b) One has $V_w \subset \ker(\psi)$ and $O_w^\times \cdot K^\times \subset \ker(\psi)$.

- Hence since $wL = L^\times/O_w^\times$, $vK = K^\times/O_v^\times$, one gets a canonical pairing of groups
  $I_w/V_w \times wL/vK \to \mu \subset \kappa(w')$

Finally, recalling that $wL/vK$ is an abelian torsion group (WHY), let $wL(p), wL' \subset wL$ be the preimages under $wL \to wL/vK$ of the $p^\infty$-torsion, respectively prime-to-$p$ torsion subgroups of $wL/vK$. Then $wL(p) + wL' = wL$ and $wL(p) \cap wL' = wK$ (WHY).

9) Study the proof of the following fundamental fact:

**Theorem.** In the above notation, the pairing $\psi$ gives rise to a perfect pairing

$$\overline{\psi} : I_w/V_w \times wL/wL(p) \to \mu$$

of the profinite group $I_w/V_w$ and the discrete torsion group $wL/wL(p)$. Further, recalling the ramification field $L'$ of $w$, setting $w' := w|_{L'}$, the following hold:

- $wL' = w' L'$, thus $I_w/V_w = I_w' = \text{Hom}(w' L'/vK, \mu_w)$ is the Pontryagin dual of $w' L'/vK$.
- $\kappa(w') = \kappa(w')$, the exact sequence $1 \to I_{w'} \to D_{w'} \to \text{Gal}(\kappa(w')|\kappa(v)) \to 1$ is split, and $\text{Gal}(\kappa(w')|\kappa(v))$ acts on $I_{w'} = \text{Hom}(w' L'/vK, \mu_w)$ canonically.
- For every finite subextension $L' | K$ of $L' | K$ and the restriction $w' := w|_{L'}$ one has: The ramification index $e(w'|v) := (v' L'/vK)$ is prime to $p$, $\kappa(w')|\kappa(v)$ is separable, and if $L' \subset L'$, the fundamental equality holds:

$$[L' : L''] = e(w'|w'') \cdot [\kappa(w') : \kappa(w'')]$$

**Terminology.** $L' | K$ is called the **tame subfield** of $L|K$ with respect to $w$.

**Question.** What should it mean that $v$ is tamely ramified in a subextension $L' | K$ of $L|K$?

10) Let $\mathcal{V}$ be a set of valuations of $K$, and $L|K$ be a Galois extension. Prove:

a) There exists a **unique maximal subextension** $L'|K$ of $L|K$ such that for all $v \in \mathcal{V}$ are tamely ramified in $L'|K$.

b) Moreover, $L'|K$ is a Galois extension.