Notes on Local Fields

1 Review: Galois theory

Let L/K be an algebraic extension. It is called:

- **normal**, if every polynomial $f \in K[T]$ with a root in L splits in L, $\iff$ L is the splitting field of a bunch of polynomials over K;
- **separable**, if for every element in L, its minimal polynomial over K has no multiple roots in its splitting field;
- **Galois**, if it is normal and separable, i.e., L is the splitting field of a bunch of *inseperable* polynomial over K. We put $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$.

Remark. 1. For a finite *normal* extension L/K, $|\mathrm{Aut}_K(L)| \leq [L : K]$, where the equality holds $\iff$ L/K is separable, i.e. Galois. This is because a K-automorphism of $L = K[T]/(f)$ just maps a root of f to another.

2. Normality is NOT transitive. As an example, take $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

Now let L/K be a Galois extension. Equip $\mathrm{Gal}(L/K)$ with the following **Krull topology**: $\forall \sigma \in \mathrm{Gal}(L/K)$, a basis of nbhd is given by

$$\sigma\,\mathrm{Gal}(L/F), \quad F/K < \infty \text{ \& Galois}.$$

This topology is the discrete topology when L/K finite, and is profinite when L/K infinite, whence

$$\mathrm{Gal}(L/K) \simeq \varprojlim_{F/K<\infty \text{ \& Galois}} \mathrm{Gal}(F/K).$$

The Galois theory says that the intermediate fields of L/K corresponds to the closed subgroups of $\mathrm{Gal}(L/K)$ bijectively and $\mathrm{Gal}(L/K)$-equivariantly.

- $\to$: For an intermediate field F, it gives $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$. Note that L/F is Glaois, but F/K is NOT always Galois. The Galois group acts on $\{\text{intermediate field of } L/K\}$ by $(\sigma, F) \mapsto \sigma F = \sigma(F)$.
- $\leftarrow$: For a subgroup $H < G$, it fixes a subfield $L^H \subset L$. The Galois group act on $\{H : H < \mathrm{Gal}(L/K)\}$ by conjugation, i.e., $(\sigma, H) \mapsto \sigma H \sigma^{-1}$.

In particular,

- Galois extensions correspond to normal closed subgroups,
- Finite extensions correspond to open subgroups.

2 DVR and Dedeking domains

2.1 Simple Extensions

Let A be a local ring with $(\mathfrak{m}, k)$, $f \in A[X]$ a monic polynomial of deg n. We consider the extension $A \to B_f := A[X]/f$.

Let $\overline{f}$ be the image of f in $k[X] \simeq A[X]/\mathfrak{m}$ with decomposition

$$\overline{f} = \prod_i \overline{g_i}^{e_i},\ g_i \in A[X],\ \overline{g_i} \in k[X] \text{ irreducible.}$$

and

$$\overline{B_f} := B_f/\mathfrak{m}B_f \simeq A[X]/(\mathfrak{m}, f) \simeq k[X]/(\overline{f}).$$

Lemma 2.1. $\mathfrak{m}_i := (\mathfrak{m},\ g_i \bmod f) \subset B_f$ are all the distinct maximal ideals of B_f.

Proof. Denote $\pi : B_f \to \overline{B_f}$. We have $B_f/\mathfrak{m}_i \simeq \overline{B_f}/(\overline{g_i})$, so $\mathfrak{m}_i$'s are maximal. Note that $\mathfrak{m}_i = \pi^{-1}(\overline{g}_i)$.

Take $\mathfrak{n} \in \operatorname{Spm} B_f$. If $\mathfrak{n} \supset \mathfrak{m}$, then $\mathfrak{n} = \pi^{-1}\pi\mathfrak{n}$, and goes to a maximal ideal in $\overline{B_f}$ (because $\overline{B_f}/\pi\mathfrak{n} \simeq B_f/\mathfrak{n}$), so $\mathfrak{n} = \pi^{-1}(\overline{g}_i) = \mathfrak{m}_i$.

So assume that $\mathfrak{m} \not\subset \mathfrak{n}$, then $\mathfrak{n} + \mathfrak{m}B_f = B_f$. (In this case $\mathfrak{n}/(\mathfrak{n} \cap \mathfrak{m}) \simeq \overline{B_f}$ as B_f-module, and thus $\pi^{-1}\pi\mathfrak{n} = B_f$.) Therefore

$$\frac{B_f}{\mathfrak{n}} = \frac{\mathfrak{n} + \mathfrak{m}B_f}{\mathfrak{n}} \simeq \frac{\mathfrak{m}B_f}{\mathfrak{n}}.$$

Since A is local and B_f is a f.g. A-mod, by Nakayama's lemma, we see $\mathfrak{n} = B_f$. Contradiction. $\square$

Now take A to be a DVR with $\mathfrak{m} = (\varpi)$ and $K = \operatorname{Frac} A$. Put $L := K[X]/(f)$. We give two cases where B_f is a DVR.

Unramified case

Let $\overline{f} \in k[X]$ be irreducible. Then B_f is a DVR with maximal ideal $\mathfrak{m}B_f$.

Corollary 2.1. $f \in A[X]$ is also irreducible, so L is a field. Moreover, B_f is the integral closure of A in L, and L/K is unramified if $\overline{f}$ is separable.

Proof. $L = K[X]/f \simeq (A[X]/f) \otimes_A K = B_f \otimes_A K$. As B_f is a domain, L is a field and $L = \operatorname{Frac} B_f$. It left to prove that B_f is integrally closed, ??????? $\square$

Totally ramified case

Let $f \in A[X]$ be an **Eisenstein polynomial**, i.e.,

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0,\ a_i \in \mathfrak{m},\ a_0 \notin \mathfrak{m}^2.$$

Proposition 2.1. B_f is a DVR, with maximal ideal generated by image of X and residue field k.

Proof. Let x be the image of X in B_f. We have $\overline{f} = X^n$, so B_f is a local ring with maximal ideal $(\mathfrak{m}, x)$. Observe that $a_0 \in \mathfrak{m} \setminus \mathfrak{m}^2$, hence it uniformizes $\mathfrak{m} \subset A$, and $-a_0 \bmod f = x^n + \cdots + (a_1 \bmod f)x$, we have $(\mathfrak{m}, x) = (x)$. $\square$

Similarly, we have f irreducible and L is a field with B_f the integral closure of A in L.