Today: Initial theory of local fields

Notation:
- $R = \text{complete DVR}$
- $K = \text{fraction field of } R$
- $\pi = \text{a chosen generator of the maximal ideal of } R$
  ($\pi = \text{"the uniformizer"}$)
- $k = R/\pi R$, the residue field

Hensel's lemma: $0 \neq f \in R[x]$
- $\deg(f) = d$;
- $\overline{f}(x) = \text{image of } f \text{ in } k[x]$.
Assume that $\overline{f}(x) \neq 0$, and suppose we have a factorization
$\overline{f}(x) = u(x)v(x)$, $u,v \in k[x]$
$u \neq 0$, $\deg(u) = e \leq d$
$\gcd(u,v) = 1$
Then $\exists g,h \in R[x]$ with $f = gh$
$\deg g = e$, $\overline{g} = u$

This was proved last time. We also proved a corollary which we are not going to state again.
Theorem. Let $D$ be a finite dimensional division algebra over $K$. Let

$$A = \{ x \in D \mid \text{Norm}_{D/K}(x) \in \mathbb{R}^2 \}.$$ 

Then:

1. $x \in A \Rightarrow x$ is integral over $R$
2. $A$ is a subring of $D$ (and hence an $R$-subalgebra)
3. $\exists \pi_D \in A$ so that $\forall 0 \neq x \in A$ can be expressed uniquely as $x = \pi_D^{-m} u$ (can also interchange) ($m \geq 0$, $u \in A^*$$)$
4. Assume that the center of $D$ is a separable extension of $K$. Then $A$ is an $R$-order in $D$, and is therefore the unique maximal $R$-order in $D$.

We proved (0), (1) last time.

Proof of (2): Consider the composition

$$D^\times \xrightarrow{\text{Norm}} K^\times \xrightarrow{\text{val}} \mathbb{Z}$$

Its image is a nonzero subgroup of $\mathbb{Z}$. 

Proof of (3): 

We proved (0), (1) last time.

Proof of (2): Consider the composition

$$D^\times \xrightarrow{\text{Norm}} K^\times \xrightarrow{\text{val}} \mathbb{Z}$$

Its image is a nonzero subgroup of $\mathbb{Z}$.
hence is of the form $eZ$ for some $e \in \mathbb{N}$. Choose $\pi_D \in D^*$ with $\text{val} (\text{Norm} (\pi_D)) = e$. It is easy to check that it works.

**Proof of (3):** Let $w_1, \ldots, w_n$ be a $K$-basis for $D$. We may assume that $w_1, \ldots, w_n \in A$. Because $A$ is a subring of $D$, we have $A \subseteq Rw_1 + \ldots + Rw_n$, where $\{w_i\}$ is the dual basis of $\{w_i\}$ with respect to the "reduced trace form" $B(x, y) = L(x, y)$, where

$$
\begin{align*}
D & \xrightarrow{\text{tr}_{red}} \mathbb{Z} \\
\mathbb{Z} & \xrightarrow{\text{tr}_{z/K}} K \\
\mathbb{L} & \quad \quad \\
\text{and } \mathbb{Z} & \text{ is the center of } D.
\end{align*}
$$

[What is the reduced trace, $\text{tr}_{red}$?]

**Fact:** If $D$ is a finite dimensional central division algebra over a field $E$, there exists a unique linear functional $\text{tr}_{red} : D \rightarrow E$ with the property that $\text{tr}_{red}$ extends scalars to $E$ and identifying $D \otimes E = \text{Mat}_n(E)$ turns $\text{tr}_{red}$ into the usual trace of matrices, $\text{Mat}_n(E) \rightarrow E$. ]
Proof of (4): There exists \( e \in \mathbb{N} \) (the same as the one we used in (2)) such that \( P^e = A \pi \), where \( \pi \in R \) is the uniformizer. Now use the fact that \( A \) is a free \( R \)-module of finite rank, and \( A \) is \( p \)-adically complete \( \iff \) \( A \) is \( p^e \)-adically complete.

\[ 5.3 \] Notation: Let \( D, A, R, \) etc. be as above. Let \( e \in \mathbb{N} \) be as in the proof of part (2). Write \( k_D = A/p \), and \( f = \dim_k(k_D) \), which equals \([k_D:k]\) in case \( k_D \) is a field.

In order to avoid confusion, one sometimes writes \( e = e(D/K) \), \( f = f(D/K) \).

\[ 5.4 \] Proposition. Assume that the center of \( D \) is separable over \( K \). Then \( e(D/K) \cdot f(D/K) = \dim_K(D) \).

Proof: Let us write \( n = \dim_K(D) \).
Then \( A / \pi A \cong (R / \pi R)^n \) as \( R \)-modules. We have \( A \supset \pi A \supset \pi^2 A \supset \ldots \supset \pi^e A = \pi A \).

We have \( A / \pi_D A \cong \pi_D^r A / \pi_D^{r+1} A \) \( \forall r \in \mathbb{Z} \) as \( R \)-modules.

\[ \Rightarrow \quad \text{length}_R (A / \pi A) = e \cdot \text{length}_R (A / \pi_D A) = e \cdot t. \]

\[ \textbf{5.5.5. ASSUMPTION} \]

The residue field \( k = R / \pi R \) is always assumed to be perfect from now on.

Also, from now on, we consider the commutative case only; in other words, we work with \( L = \text{finite separable} \) extension of \( K \).

We write \( R_L = \text{integral closure of} \ R \text{ in} \ L \).

\( \pi_L = \text{a uniformizer in} \ R_L \)

\( k_L = R_L / \pi_L R_L \).
Def.: We say that the extension $L/K$ is unramified if $e(L/K) = 1$, equivalently, if $\pi = \pi_K$ already generates the maximal ideal of $R_L$.

Def.: We say $L/K$ is totally ramified if $f(L/K) = 1$, i.e., if $e(L/K) = [L:K]$.

Example 5.6. Let $f$ be a monic irreducible polynomial in $k[X]$ of degree $d$, and lift $f$ to a monic polynomial $f(x) \in R[X]$ (hence also of degree $d$). Then

(i) $f(x)$ is irreducible in $K[X]$;

(ii) $R[X]/(f(x)) \subset K[X]/(f(x))$ is the integral closure of $R$ in $K[X]/(f(x))$;

(iii) $E := K[X]/(f(x))$ is an unramified extension of $K$, and $k_E \cong k[X]/(f(x))$.

In fact, we will soon see that every finite unramified extension of $K$ can be obtained by a procedure of this type.

Proof of (i). This is standard.
Proof of (ii). Clearly, it suffices to show that $R[X]/(\xi(x))$ is a PID. Let us write $B = R[X]/(\xi(x)), \ E = K[X]/(\xi(x))$.

Then $B/\pi B = R[X]/(\xi, \pi) \cong K[X]/(\bar{\xi})$ is a field. So $\pi B$ is a maximal ideal of $B$.

We want to deduce that $B$ is a DVR.

If $m \subset B$ is any maximal ideal, then, as $B$ is integral over $R$, $m \cap R$ is a maximal ideal of $R \Rightarrow m \cap R = \pi R \Rightarrow \pi \in m \Rightarrow \pi B \subset m \Rightarrow m = \pi B$.

So $\pi B$ is the unique maximal ideal of $B$, and this is clearly enough. \hfill\Box

Proof of (iii). We already proved this in the course of proving (ii), because we have shown that $\pi B$ is the unique maximal ideal of $B$ ($\Rightarrow E/K$ is unramified), and we have also shown $k_E \cong K[X]/(\bar{\xi})$.

Q.E.D.
§5.8. We have a natural functor

\[
\begin{align*}
\{ \text{finite separable extensions of } K \} & \rightarrow \{ \text{finite extensions of } k \} \\
L & \rightarrow k_L
\end{align*}
\]

mappings are the \(K\)-algebra homomorphisms

Proposition 1: Let \(E\) be an unramified (finite) extension of \(K\), and \(L\) any finite separable extension of \(K\). Then the natural map (of finite sets)

\[
\text{Hom}_{K\text{-alg}} (E, L) \rightarrow \text{Hom}_{k\text{-alg}} (k_E, k_L)
\]

is a bijection.

Proof: Consider first the special case as before: \(E = k[X] / (f(x))\), where \(f(x)\) is amonic polynomial in \(R[X]\), and \(f(x)\) is irreducible in \(k[X]\). Then

\[
\text{Hom}_{K\text{-alg}} (E, L) = \{ x \in L \mid f(x) = 0 \} = \{ x \in R_L \mid f(x) = 0 \}
\]

We want to show that the obvious map

\[
\{ x \in R_L \mid f(x) = 0 \} \rightarrow \{ \beta \in k_L \mid f(\beta) = 0 \}
\]

is bijective. This is an easy exercise in using Hensel's lemma.
Next: let \( L/K \) be any unramified (finite separable) extension. Then \( k_L \) is a finite separable extension of \( k \), so we can write \( k_L = k[X]/(F(X)) \), where \( F(X) \in k[X] \) is monic and irreducible.

Construct \( E \) as before using this \( F(X) \). Then, by the previous part of the proof, we get a bijection \( \text{Hom}_{K-\text{alg}}(E, L) \cong \text{Hom}_{K-\text{alg}}(k_E, k_L) \).

But \( k_E \cong k_L \) over \( k \) by construction. This implies that there exists a \( K \)-algebra isomorphic to one of the "standard" ones, constructed in Example 5.6.

In turn, this implies the proposition in full generality.

\[ \text{Corollary (of the proof): Every finite unramified extension of } K \text{ is isomorphic to one of the "standard" ones, constructed in Example 5.6.} \]

\[ \text{Lemma: If } L \text{ is any finite separable extension of } K, \text{ then there} \]

\[ \text{is unique.} \]
exists an intermediate field \(K \subset E \subset L\), with \(E/K\) unramified and \(L/E\) totally \(K\) ramified. (Later we'll see \(E\) is unique.)

**Proof:** This is easy to prove using the same idea as the one used in the proof of Proposition 1 in §5.8.

\[\begin{array}{c}
\text{Corollary of Proposition 1. The functor} \\
\begin{cases}
\text{unramified} \\
\text{extensions of } K
\end{cases} 
\rightarrow 
\begin{cases}
\text{finite} \\
\text{extensions of } K
\end{cases} \\
L 
\rightarrow k_L
\end{array}\]

is an equivalence of categories.

\[\begin{array}{c}
\text{Properties of unramified extensions} \\
\text{in §§5.12.}
\end{array}\]

(1) Given a tower of finite separable extensions \(K \subset E \subset L\), we have \(L/K\) is unramified \(\Leftrightarrow\) \(E/K\) and \(L/E\) are unramified.

(2) Base change:
If $E/K$, $L/K$ are finite separable extensions and $E/K$ is unramified, then $LE/L$ is unramified.

(3) If $E_1/K$, $E_2/K$ are both unramified, then $E_1E_2/K$ is unramified.

Proof: (1) is straightforward.

(3) follows from (1) and (3).

For (2), we may assume $E = K[x]/(f(x))$, where $f(x) \in R[x]$ is monic and $\overline{f(x)} \in k[x]$ is irreducible. Clearly, $\overline{f(x)} \in k[x]$ is irreducible.

For (2), we may assume $E = L[x]/(g(x))$, where $g(x) \in R_L[x]$ is monic and irreducible.

Now $g(x)$ divides $f(x)$ implies $\overline{g(x)}$ divides $\overline{f(x)}$. Since $\overline{f(x)}$ divides $\overline{f(x)}$, $\overline{g(x)}$ has no repeated roots in $k_L$. Then $\overline{g(x)}$ is irreducible by Hensel's Lemma (otherwise we could factor $g(x)$).

So by Example 5.6, we are done.