Lecture 5

Corollary 4.5: Let $f(X) = a_n X^n + \dots + a_0 \in K[X]$ with $a_0, a_n \neq 0$. If $f(X)$ is irreducible, then $|a_i| \leq \max(|a_0|, |a_n|)$ for all i.

Proof: Upon scaling, WMA $f(X) \in \mathcal{O}_K[X]$ with $\max_i(|a_i|) = 1$. Thus we need to show that $\max(|a_0|, |a_n|) = 1$. If not, let r be minimal s.t. $|a_r| = 1$; then $0 < r < n$. Thus we have

$$\bar{f}(X) = X^r(a_r + \dots + a_n X^{n-r}) \bmod \mathfrak{m}.$$

Then Theorem 4.5 implies $f(X) = g(X)h(X)$, with $0 < \deg g < n$ $\square$

§ Teichmüller lifts

$A = \{0, \dots, p-1\}$ coset reps for $\mathbb{F}_p = \mathbb{Z}_p / p\mathbb{Z}_p$ in $\mathbb{Z}_p$.

Is there a more natural choice?

Definition 5.1: A ring R of characteristic p is a **perfect ring** if the Frobenius $x \mapsto x^p$ is an automorphism of R. A field of char p is a perfect field if it is perfect as a ring.

Remark: Since char $R = p$, $(x+y)^p = x^p + y^p$, so Frobenius is ring hom.

Example: (i) $\mathbb{F}_{p^n}$ and $\overline{\mathbb{F}}_p$ are perfect fields.

(ii) $\mathbb{F}_p[t]$ is not perfect, $t \notin \mathrm{Im}(\mathrm{Frob})$.

(iii) $\mathbb{F}_p(t^{1/p^\infty}) := \mathbb{F}_p(t, t^{1/p}, t^{1/p^2}, \ldots)$ is a perfect field (perfection of $\mathbb{F}_p(t)$).

Fact: A field k is perfect iff any finite extension of k is separable.

Theorem 5.2: Let $(K, |\cdot|)$ be a complete discretely valued field s.t. $k := \mathcal{O}_K/m$ is a perfect field of char. p. Then there exists a unique map

$$[\ \ ] : k \longrightarrow \mathcal{O}_K$$

s.t. (i) $a \equiv [a] \bmod m \quad \forall a \in k$.

(ii) $[ab] \equiv [a][b] \quad \forall a, b \in k$.

Moreover if char $\mathcal{O}_K = p$, $[\ \ ]$ is a ring hom

Definition 5.3: The element $[a] \in \mathcal{O}_K$ constructed in Theorem 5.2 is called the Teichmüller lift of

Lemma 5.4: Let $(K, |\cdot|)$ be as in Theorem 5.2, and fix $\pi \in \mathcal{O}_K$ a uniformizer. Let $x, y \in \mathcal{O}_K$ s.t. $x \equiv y \bmod \pi^k \quad (k \geq 1)$.

then $x^p \equiv y^p \mod \pi^{k+1}$

Proof: Let $x = y + u\pi^k$, $u \in \mathcal{O}_K$. Then

$$x^p = \sum_{i=0}^{p} \binom{p}{i} y^i (u\pi^k)^{p-i}$$

$$(p>2) \quad = y^p + p u \pi^k y^{p-1} + \sum_{i=0}^{p-2} \binom{p}{i} y^i (u\pi^k)^{p-i}$$

Since $\mathcal{O}_K/\pi\mathcal{O}_K$ char. p, we have $p \in \pi\mathcal{O}_K$.

Thus $p u \pi^k y^{p-1} \in \pi^{k+1}\mathcal{O}_K$.

For $i = 0, \dots, p-2$, $(u\pi^k)^{p-i} \in \pi^{k+1}\mathcal{O}_K$

$\Rightarrow x^p \equiv y^p \mod \pi^{k+1}$. □

Proof of Theorem 5.2:

Let $a \in k$. For each $i \geq 0$ we choose a lift $y_i \in \mathcal{O}_K$ of a^{1/p^i}, and we define.

4 $$x_i := y_i^{p^i}$$

We claim that $(x_i)_{i=1}^{\infty}$ is a Cauchy sequence, and its limit $x_i \longrightarrow x$ is independent of the choice of y_i.

By construction

$$y_i \equiv y_{i+1}^p \mod \pi$$

By Lemma 5.4 and induction on k, we have $y_i^{p^k} \equiv y_{i+1}^{p^{k+1}} \mod \pi^{k+1}$,

and hence

$$x_i \equiv x_{i+1} \mod \pi^{i+1} \quad (\text{take } k=i).$$

$\Rightarrow |x_i - x_{i+1}| \to 0$.

$\Rightarrow (x_i)_{i=1}^{\infty}$ is Cauchy, so $x_i \to x \in \mathcal{O}_K$.

Suppose $(x_i')_{i=1}^{\infty}$ arises from another choice y_i' lifting $a^{\frac{1}{p^i}}$. Then x_i' is Cauchy, and $x_i' \to x' \in \mathcal{O}_K$.

Let $(x_i'')_{i=1}^{\infty} = \begin{cases} x_i & i \text{ even} \\ x_i' & i \text{ odd} \end{cases}$

Then x_i'' arises from lifting $y_i'' := \begin{cases} y_i & i \text{ even} \\ y_i' & i \text{ odd} \end{cases}$

Then x_i'' is Cauchy and $x_i'' \to x$, $x_i'' \to x'$

$\Rightarrow x = x'$, hence x is indep. of y_i.

We define $[a] = x$.

Then $x_i \equiv y_i^{p^i} \equiv (a^{\frac{1}{p^i}})^{p^i} \equiv a \bmod \pi$

$\Rightarrow x \equiv a \bmod \pi$ so (i) is satisfied.

We let $b \in k$ and we choose $u_i \in \mathcal{O}_K$ a lift of $b^{\frac{1}{p^i}}$; let $z_i := u_i^{p^i}$.

Then $\lim_{i\to\infty} z_i = [b]$.

Now $u_i y_i$ is a lift of $(ab)^{\frac{1}{p^i}}$, hence

$$[ab] = \lim_{i\to\infty} x_i z_i = \lim_{i\to\infty} x_i \lim_{i\to\infty} z_i$$
$$= [a][b].$$

$\Rightarrow$ (ii) is satisfied.

If char $K = p$, $y_i + u_i$ is a lift of

$a^{\frac{1}{p^i}} + b^{\frac{1}{p^i}} = (a+b)^{\frac{1}{p^i}}$

$a^{p} + b^{p} = (a+b)^{p}$

Then $[a+b] = \lim_{i\to\infty} (y_i + u_i)^{p^i}$

$= \lim_{i\to\infty} y_i^{p^i} + u_i^{p^i}$

$= \lim_{i\to\infty} x_i + z_i = [a] + [b]$.

b Easy to check that $[0] = 0$ and $[1] = 1$.

$\Rightarrow [\ ]$ is a ring hom.

Uniqueness: Let $\phi : k \to \mathcal{O}_K$ be another such map. Then for $a \in k$, $\phi(a^{\frac{1}{p^i}})$ is a lift of $a^{\frac{1}{p^i}}$; it follows that

$$[a] = \lim_{i\to\infty} \phi(a^{\frac{1}{p^i}})^{p^i} = \lim_{i\to\infty} \phi(a) = \phi(a).$$

□

Eg. $K = \mathbb{Q}_p \quad [\ ] : \mathbb{F}_p \to \mathbb{Z}_p$

$a \in \mathbb{F}_p^{\times} \quad [a]^{p-1} = [a^{p-1}] = [1] = 1$

$\Rightarrow [a]$ is a $(p-1)^{th}$-root of unity.

More generally

Lemma 5.6: $(K, |\cdot|)$ complete discretely valued field. If $k := \mathcal{O}_K/m \subseteq \overline{\mathbb{F}_p}$, $[a] \in \mathcal{O}_K^{\times}$ is a root of unity.

Proof: $a \in k \Rightarrow a \in \mathbb{F}_{p^n}$ some n

$$\Rightarrow [a]^{p^n - 1} = [a^{p^n-1}] = [1] = 1.$$

□

Theorem 5.7: Let $(K, |\cdot|)$ be a complete discretely valued field with char $k = p > 0$. Assume k is perfect. Then $K \cong k((t))$.

Proof: Since $K = \mathrm{Frac}(\mathcal{O}_K)$, it suffices to show $\mathcal{O}_K \cong k[[t]]$. Fix $\pi \in \mathcal{O}_K$ a uniformizer, let $[\ ] : k \to \mathcal{O}_K$ be the Teichmüller map and define

$$\varphi : k[[t]] \longrightarrow \mathcal{O}_K$$

$$\varphi\left(\sum_{i=0}^{\infty} a_i t^i\right) = \sum_{i=0}^{\infty} [a_i] \pi^i .$$

Then φ is a ring hom. since $[\ ]$ and it is bijection by Prop. 3.5 (ii).