Even More on Valued Fields

(featuring Hensel's lemma)

Siyan Daniel Li-Huerta

September 22, 2020

Let F be a field complete with respect to a discretely valued norm $|\cdot|$. Let e be the smallest value > 1 that $|\cdot|$ takes, let v be the normalized valuation, and let π be a uniformizer.

Proposition

The natural map $\mathcal{O} \to \varprojlim_m \mathcal{O}/\pi^m\mathcal{O}$ is an isomorphism of topological rings.

Proof.

The kernel is $\bigcap_{m=1}^{\infty} \pi^m\mathcal{O} = \{0\}$, so the map is injective. For surjectivity, let $(y_m)_{m=1}^{\infty}$ be in $\varprojlim_m \mathcal{O}/\pi^m\mathcal{O}$, and choose representatives $\widetilde{y}_m$ of y_m in $\mathcal{O}$. For $m' \geq m \geq N$, we have $\widetilde{y}_m \equiv y_N \equiv \widetilde{y}_{m'} \mod \pi^N$, so $\{\widetilde{y}_m\}_{m=1}^{\infty}$ is a Cauchy sequence in $\mathcal{O}$. By completeness, it has a limit y in $\mathcal{O}$. For sufficiently large M, we have $y \equiv y_M \mod \pi^M$, so y maps to $(y_m)_{m=1}^{\infty}$.

To check that the map is continuous and open, it suffices to check that it preserves neighborhoods of 0. The image of $\{x \in \mathcal{O} \mid |x| \leq 1/e^N\}$ is the intersection of $\varprojlim_m \mathcal{O}/\pi^m\mathcal{O}$ with $(\prod_{m=N+1}^{\infty} \mathcal{O}/\pi^m\mathcal{O}) \times \{0\}^N$, and as N varies, both of these sets form a basis of neighborhoods of 0. $\square$

Let's generalize p-adic expansions to F. Let R be a set of representatives of $\mathcal{O}/\pi\mathcal{O}$ that contains 0.

Example

As $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$, here we can take $R = \{0, 1, \ldots, p-1\}$.

Proposition

Nonzero elements of F can be uniquely written as

$$a_N\pi^N + a_{N+1}\pi^{N+1} + \cdots ,$$

where N is an integer, the $a_N, a_{N+1}, \ldots$ lie in R, and $a_N \neq 0$.

Proof.

Let x be in $F^\times$, and set $N = v(x)$. Then x/π^N lies in $\mathcal{O}^\times$, so its image in $\mathcal{O}/\pi\mathcal{O}$ is nonzero. Thus $x/\pi^N - a_N = \pi y$ for a unique nonzero a_N in R and y in $\mathcal{O}$. If $y = 0$, we're done. Otherwise, we've only found the leading digit of x. Replace x with y and repeat this process to find the next digit. $\square$

Definition

Let $f = c_0 + c_1 t + \cdots + c_d t^d$ be in $F[t]$. The *Gauss norm* of f, denoted by $|f|$, is $\max\{|c_0|, \ldots, |c_d|\}$. We say f is *primitive* if $|f| = 1$.

The following lemma is extraordinarily useful. Recall that $\mathfrak{m} = \pi\mathcal{O}$ is the unique maximal ideal of $\mathcal{O}$. We call $\kappa = \mathcal{O}/\mathfrak{m}$ the *residue field*.

Lemma (Hensel)

Let f in $\mathcal{O}[t]$ be primitive. If $f \equiv gh \mod \pi$ for some relatively prime g and h in $\kappa[t]$, then there exist $\widetilde{g}$ and $\widetilde{h}$ in $\mathcal{O}[t]$ such that $\widetilde{g} \equiv g \mod \pi$, $\widetilde{h} \equiv h \mod \pi$, $\deg \widetilde{g} = \deg g$, and $f = \widetilde{g}\widetilde{h}$.

Example

Consider $f = t^2 + 5$ in $\mathbb{Z}_7[t]$. Then $f \equiv (t-3)(t-4) \mod 7$, so there exist $\widetilde{g}$ and $\widetilde{h}$ in $\mathbb{Z}_7[t]$ such that $\widetilde{g} \equiv t - 3 \mod 7$, $\widetilde{h} \equiv t - 4 \mod 7$, and $\deg \widetilde{g} = \deg g = 1$. Therefore we must have $\deg \widetilde{h} = 1$, and we see the leading coefficients of $\widetilde{g}$ and $\widetilde{h}$ lie in $\mathbb{Z}_7^\times$. This yields two square roots of -5 in $\mathbb{Z}_7$, which are representatives of 3 and 4 in $\mathbb{F}_7$. Indeed, one can check that their first two digits are $3 + 2 \cdot 7 + \cdots$ and $4 + 4 \cdot 7 + \cdots$.

Lemma (Hensel)

Let f in $\mathcal{O}[t]$ be primitive. If $f \equiv gh \mod \pi$ for some relatively prime g and h in $\kappa[t]$, then there exist $\widetilde{g}$ and $\widetilde{h}$ in $\mathcal{O}[t]$ such that $\widetilde{g} \equiv g \mod \pi$, $\widetilde{h} \equiv h \mod \pi$, $\deg \widetilde{g} = \deg g$, and $f = \widetilde{g}\widetilde{h}$.

Proof.

Write $d = \deg f$ and $n = \deg g$. So $\deg h \leq d - n$. Choose representatives g_0 and h_0 in $\mathcal{O}[t]$ of g and h such that $\deg g_0 = n$ and $\deg h_0 \leq d - n$. As g and h are relatively prime, we can find a and b in $\mathcal{O}[t]$ such that $ag + bh \equiv 1 \mod \pi$.

By inducting on m, we will find in $\mathcal{O}[t]$ elements $p_1, p_2, \ldots$ of degree $\leq n - 1$ and elements $q_1, q_2, \ldots$ of degree $\leq d - n$ such that

$$g_{m-1} = g_0 + p_1\pi + \cdots + p_{m-1}\pi^{m-1}, \; h_{m-1} = h_0 + q_1\pi + \cdots + q_{m-1}\pi^{m-1}$$

satisfy $f \equiv g_{m-1}h_{m-1} \mod \pi^m$. Note the $\{g_m\}_{m=1}^{\infty}$ and $\{h_m\}_{m=1}^{\infty}$ are Cauchy sequences. Thus they have limits $\widetilde{g}$ and $\widetilde{h}$, which fulfill the desired properties.

Lemma (Hensel)

Let f in $\mathcal{O}[t]$ be primitive. If $f \equiv gh \mod \pi$ for some relatively prime g and h in $\kappa[t]$, then there exist $\widetilde{g}$ and $\widetilde{h}$ in $\mathcal{O}[t]$ such that $\widetilde{g} \equiv g \mod \pi$, $\widetilde{h} \equiv h \mod \pi$, $\deg \widetilde{g} = \deg g$, and $f = \widetilde{g}\widetilde{h}$.

Proof (continued).

The $m = 1$ case holds by assumption. Assuming we found satisfactory $p_1, \ldots, p_{m-1}$ and $q_1, \ldots, q_{m-1}$, we want to choose p_m and q_m such that

$$\begin{aligned} f \equiv g_m h_m = (g_{m-1} + p_m\pi^m)(h_{m-1} + q_m\pi^m) \mod \pi^{m+1} &\iff \\ f - g_{m-1}h_{m-1} \equiv (g_{m-1}q_m + h_{m-1}p_m)\pi^m \mod \pi^{m+1} &\iff \\ f_m \equiv g_{m-1}q_m + h_{m-1}p_m \equiv g_0 q_m + h_0 p_m \mod \pi, & \end{aligned}$$

where $f_m = \pi^{-m}(f - g_{m-1}h_{m-1})$ lies in $\mathcal{O}[t]$. Note that $\deg f_m \leq d$. Because $1 \equiv ag_0 + bh_0 \mod \pi$, we have $f_m \equiv g_0 af_m + h_0 bf_m \mod \pi$. So $q_m = af_m$ and $p_m = bf_m$ look good, except their degrees might be too big.

Lemma (Hensel)

Let f in $\mathcal{O}[t]$ be primitive. If $f \equiv gh \mod \pi$ for some relatively prime g and h in $\kappa[t]$, then there exist $\widetilde{g}$ and $\widetilde{h}$ in $\mathcal{O}[t]$ such that $\widetilde{g} \equiv g \mod \pi$, $\widetilde{h} \equiv h \mod \pi$, $\deg \widetilde{g} = \deg g$, and $f = \widetilde{g}\widetilde{h}$.

Proof (continued).

What do we do instead? First, note that $g_0 \equiv g \mod \pi$ and $\deg g_0 = \deg g$, so the leading coefficient of g_0 lies in $\mathcal{O}^\times$. Thus polynomial division yields $bf_m = qg_0 + p_m$ for some q and p_m in $\mathcal{O}[t]$ with $\deg p_m \leq n-1$. Now we have

$$f_m \equiv g_0 af_m + h_0 bf_m = g_0(af_m + h_0 q) + h_0 p_m \mod \pi.$$

Let q_m be the element in $\mathcal{O}[t]$ obtained from removing every term in $af_m + h_0 q$ divisible by π. Then its degree can be checked mod π, and we still have $f_m \equiv g_0 q_m + h_0 p_m \mod \pi$. Since $\deg f_m \leq d$, $\deg h_0 p_m \leq (d-n) + (n-1) = d-1$, and $\deg g_0 = n$, we must have $\deg q_m \leq d - n$. □

Example

Consider $f = t^{p-1} - 1$ in $\mathbb{Z}_p[t]$. Then $f \equiv \prod_{i=1}^{p-1}(t-i) \mod p$, so repeatedly applying Hensel's lemma shows that f completely factors into degree 1 elements of $\mathbb{Z}_p[t]$ with leading coefficients in $\mathbb{Z}_p^\times$. Hence $\mathbb{Z}_p$ contains all $(p-1)$-th roots of unity, and $R = \{x \in \mathbb{Z}_p^\times \mid x^{p-1} = 1\} \cup \{0\}$ forms a set of representatives of $\mathbb{F}_p$ that's closed under multiplication. These are called *Teichmüller representatives*.

Corollary

Let $f = c_0 + \cdots + c_d t^d$ in $F[t]$ be irreducible, and suppose $c_d c_0 \neq 0$. Then $|f| = \max\{|c_0|, |c_d|\}$.

Proof.

By replacing f with a scalar multiple, we may assume $|f| = 1$ and f hence lies in $\mathcal{O}[t]$. Let r be the smallest such that $|c_r| = 1$. Then $f \equiv t^r(c_r + \cdots + c_d t^{d-r}) \mod \pi$, where $c_r \not\equiv 0 \mod \pi$. If $\max\{|c_0|, |c_d|\} < 1$, then we must have $1 \leq r \leq d-1$. Hensel's lemma then provides a nontrivial factorization of f, which cannot exist. $\square$

Corollary

Let E/F be a finite extension of degree d. Then $|\cdot|' = |\operatorname{Nm}_{E/F} \cdot|^{1/d}$ yields an extension of $|\cdot|$ to an absolute value on E, and it is the unique extension up to isomorphism.

Proof.

Write $\mathcal{O}'$ for the integral closure of $\mathcal{O}_F$ in E. For nonzero x in E, its characteristic polynomial over F is a power of its minimal polynomial $f = c_0 + \cdots + t^m$ over F. Thus $\operatorname{Nm}_{E/F} x = \pm c_0^{d/m}$. If x lies in $\mathcal{O}'$, then c_0 and hence $\operatorname{Nm}_{E/F} x$ lies in $\mathcal{O}_F$. Conversely, if $\operatorname{Nm}_{E/F} x$ lies in $\mathcal{O}_F$, then the previous lemma shows $|f| = \max\{|c_0|, |1|\} = 1$. Thus f lies in $\mathcal{O}_F[t]$, so x lies in $\mathcal{O}'$.

When x is in F, we have $\operatorname{Nm}_{E/F} x = x^d$, so $|\cdot|'$ extends $|\cdot|$. Let's show $|\cdot|'$ is a norm. Evidently $|x|' = 0$ if and only if $x = 0$, and $|\cdot|'$ also commutes with multiplication. As for the strong triangle inequality, let x and y be in $E^\times$, and say $|x|' \leq |y|'$ without loss of generality. Then $|x + y|' \leq \max\{|x|', |y|'\}$ is equivalent to $|x/y + 1|' \leq \max\{|x/y|', 1\} = 1$.

Corollary

Let E/F be a finite extension of degree d. Then $|\cdot|' = |\operatorname{Nm}_{E/F} \cdot|^{1/d}$ yields an extension of $|\cdot|$ to an absolute value on E, and it is the unique extension up to isomorphism.

Proof (continued).

Since $|x/y|' \leq 1$, then we have $|\operatorname{Nm}_{E/F}(x/y)| \leq 1$, i.e. $\operatorname{Nm}_{E/F}(x/y)$ lies in $\mathcal{O}_F$. Hence x/y lies in $\mathcal{O}'$. Because $\mathcal{O}'$ is a subring, so does $x/y + 1$, which implies $|\operatorname{Nm}_{E/F}(x/y+1)| \leq 1$ and hence $|x/y+1|' \leq 1$, as desired. So $|\cdot|'$ is a nonarchimedean norm on E, and its valuation ring is $\mathcal{O}'$. Write $\mathfrak{m}'$ for its maximal ideal.

For uniqueness, let $|\cdot|''$ be another norm on E extending $|\cdot|$. Then $|\cdot|''$ must be nontrivial and nonarchimedean. Write $\mathcal{O}''$ and $\mathfrak{m}''$ for its valuation ring and maximal ideal. If we had some x in $\mathcal{O}' \smallsetminus \mathcal{O}''$, then the coefficients $c_0, \dots, c_{m-1}$ of its minimal polynomial lie in $\mathcal{O}_F$ and hence $\mathcal{O}''$. Yet x^{-1} must lie in $\mathfrak{m}''$, so $1 = -c_{m-1}x^{-1} - \cdots - c_0 x^{-m}$ does too, which is false. Therefore $\mathcal{O}' \subseteq \mathcal{O}''$, so $|x|'' > 1$ implies $|x|' > 1$. Taking inverses shows that $|x|'' < 1$ implies $|x|' < 1$, so $|\cdot|''$ and $|\cdot|'$ are isomorphic. □