MATH 254A: LOCAL FIELDS II

BRIAN OSSERMAN

1. Completions

We wanted to prove the following proposition:

Proposition 1.1. *We have:*

(i) $K_{\mathfrak{p}}$ *is the field of fractions of* $\hat{\mathscr{O}}_{K,\mathfrak{p}}$.
(ii) $\hat{\mathscr{O}}_{K,\mathfrak{p}}$ *is the subset of elements of* $K_{\mathfrak{p}}$ *with absolute value at most* 1.
(iii) $\hat{\mathscr{O}}_{K,\mathfrak{p}}$ *is also the completion of* $\mathscr{O}_{K,\mathfrak{p}}$ *with respect to the metric* $d_{\mathfrak{p}}(\cdot,\cdot)$ *induced by* $||\cdot||_{\mathfrak{p}}$.
(iv) $\hat{\mathscr{O}}_{K,\mathfrak{p}}$ *is the inverse limit of* $\mathscr{O}_K/\mathfrak{p}^n$ *over* $n \in \mathbb{N}$.

Proof. The main content is actually in (iii), which is equivalent to the statement that $\mathscr{O}_K$ is dense in $\mathscr{O}_{K,\mathfrak{p}}$ under the metric $d_{\mathfrak{p}}$. For this, we need to use the fact that $\mathscr{O}_K/\mathfrak{p}^n \xrightarrow{\sim} \mathscr{O}_{K,\mathfrak{p}}/\mathfrak{p}^n$ for all n, which we have used before, but never justified. We certainly get a map induced by $\mathscr{O}_K \hookrightarrow \mathscr{O}_{K,\mathfrak{p}}$, and the injectivity is easy to check, so we need to check surjectivity. Given $\frac{x}{s} \in \mathscr{O}_{K,\mathfrak{p}}$, with $x, s \in \mathscr{O}_K$, and $s \notin \mathfrak{p}$, we want to show that there exists $y \in \mathscr{O}_K$ with $ys \equiv x \pmod{\mathfrak{p}^n}$; it clearly suffices to see that s is a unit in $\mathscr{O}_K/\mathfrak{p}^n$. Since the latter is a finite ring, there exist $i < j$ with $s^i = s^j$ modulo $\mathfrak{p}^n$, so $s^i(1 - s^{j-i}) \in \mathfrak{p}^n$. Since $s \notin \mathfrak{p}$, by unique factorization into prime ideals, we find $(1 - s^{j-i}) \in \mathfrak{p}^n$, and s is a unit modulo $\mathfrak{p}^n$, as desired. We thus obtain the isomorphism $\mathscr{O}_K/\mathfrak{p}^n \xrightarrow{\sim} \mathscr{O}_{K,\mathfrak{p}}/\mathfrak{p}^n$.

It then follows easily that $\mathscr{O}_K$ is dense in $\mathscr{O}_{K,\mathfrak{p}}$: given $\frac{x}{s} \in \mathscr{O}_{K,\mathfrak{p}}$, for each n we can find $y_n \in \mathscr{O}_K$ such that $y_n \equiv \frac{x}{s} \pmod{\mathfrak{p}^n}$, which then gives a sequence in $\mathscr{O}_K$ converging to $\frac{x}{s}$. This completes the proof of (iii).

We then see (ii) because $\mathscr{O}_{K,\mathfrak{p}}$ is nearly defined to be the subset of K with absolute value at most 1; certainly, we have $||z||_{\mathfrak{p}} \leqslant 1$ for any $z \in \mathscr{O}_{K,\mathfrak{p}}$. Conversely, given $\frac{x}{y} \in K^*$ with $||\frac{x}{y}||_{\mathfrak{p}} \leqslant 1$, we claim we can write $\frac{x}{y} = \frac{x'}{s}$ with $s \notin \mathfrak{p}$. Indeed, let t be a generator of $\mathfrak{p}$ in $\mathscr{O}_{K,\mathfrak{p}}$, which we know is a DVR. Then we can write $x = t^e \frac{s_x}{s'_x}$, $y = t^{e'} \frac{s_y}{s'_y}$, with $s_x, s'_x, s_y, s'_y \notin \mathfrak{p}$, and $e \geqslant e'$ since $||\frac{x}{y}||_{\mathfrak{p}} \leqslant 1$. Thus $\frac{x}{y} = \frac{t^{e-e'} s_x s'_y}{s'_x s_y} \in \mathscr{O}_{K,\mathfrak{p}}$, as desired. It remains to see that this description is maintained under completion. But here we observe that $||\cdot||_{\mathfrak{p}}$ takes on discrete values away from 0, so any sequence in K converging to a point with $||\cdot||_{\mathfrak{p}} \leqslant 1$ must, after a finite number of terms, have every element with $||\cdot||_{\mathfrak{p}} \leqslant 1$, and hence contained in $\mathscr{O}_{K,\mathfrak{p}}$.

(i) then follows easily from (ii), as we see that for any $z \in K$, either $z \in \hat{\mathscr{O}}_{K,\mathfrak{p}}$ or $1/z$ is.

Finally, (iv) follows easily from the definition of $\hat{\mathscr{O}}_{K,\mathfrak{p}}$, just as in the case of $\mathbb{Z}_p$. □

Algebraic Geometry Remark 1.2. The rings $\hat{\mathscr{O}}_{K,\mathfrak{p}}$ are thus completions of local rings of rings of integers, in the sense used in algebraic geometry. As a result, they are closely analogous to rings of power series, and exhibit much of the same behavior.

2. Generality

For our purposes, a **local field** is $\mathbb{R}$, $\mathbb{C}$, or $K_{\mathfrak{p}}$ for some number field K and prime ideal $\mathfrak{p} \subset \mathscr{O}_K$. We say that the first category is **Archimedian**, while the second category is **non-Archimedian** (the terminology arises from the fact that for the second class, we have $||z_1 + z_2|| \leqslant \max\{||z_1||, ||z_2||\}$.

This definition of local field may seem rather ad-hoc, but from the proper point of view, it is quite natural. Indeed, we have the following basic theorem:

Theorem 2.1. *Let K be a number field. Then every absolute value $||\cdot||$ on K is equivalent to either $|\cdot| \circ \sigma$ for some $\sigma : K \to \mathbb{C}$, or $||\cdot||_{\mathfrak{p}}$ for some $\mathfrak{p} \subset \mathscr{O}_K$.*

Here, an absolute value $||\cdot|| : K \to \mathbb{R}_{\geqslant 0}$ is defined to be any map satisfying:

(i) $||z|| = 0$ *if and only if* $z = 0$*;*
(ii) $||z_1 z_2|| = ||z_1|| \cdot ||z_2||$*;*
(iii) $||z_1 + z_2|| \leqslant ||z_1|| + ||z_2||$.

The equivalence condition for absolute values is that the associated metric $d(z_1, z_2) := ||z_1 - z_2||$ induce the same topology on K.

Since this result is stated only for context, we do not give the proof; see [1, Thm. 4.4.1].

We denote the set of absolute values described in the theorem by M_K. Thus, every completion of K with respect to an absolute value arises as the completion with respect to an element of M_K, which is one of the local fields we have discussed. This is reflected by the following basic fact:

Proposition 2.2. *Given $z \in K^*$, we have the identity:*

$$\prod_{||\cdot|| \in M_K} ||z|| = 1.$$

Proof. We first treat the case $z \in \mathscr{O}_K$ (and still non-zero). We then have that $||z||_{\mathfrak{p}} = 1$ for all but finitely many $\mathfrak{p}$, so the product makes sense. Indeed, if we write $(z) = \prod_i \mathfrak{p}_i^{e_i}$, we see that $||z||_{\mathfrak{p}_i} = N(\mathfrak{p}_i)^{-e_i}$, so

$$\prod_{\mathfrak{p}} ||z||_{\mathfrak{p}} \frac{1}{N((z))} = \frac{1}{|N_{K/\mathbb{Q}}(z)|}.$$

On the other hand, $\prod_{\sigma_i} |\sigma_i(z)| = |N_{K/\mathbb{Q}}(z)|$, and since every absolute value in M_K is one of these two possibilities, we get the desired identity. The statement for all $z \in K^*$ then follows by the multiplicativity of all $||\cdot|| \in M_K$. □

Finally, we remark that the class of local fields itself is represented by a rather natural condition:

Theorem 2.3. *Let K be a topological field complete with respect to some absolute value, and locally compact. Then if K has characteristic 0, it is a local field in our sense.*

In fact, one typically defines a local field by this condition; the case of characteristic p is closely analogous, and every field K of characteristic p satisfying the conditions of the theorem is of the form $\mathbb{F}_{p^e}((t))$, with the absolute value $||z|| = 2^{-\operatorname{ord}_t z}$ for any $2 \in \mathbb{R}_{>1}$.

In any case, in order to study roots of polynomials over K, we see that it is rather natural to study roots over each $K_{\mathfrak{p}}$.

3. Hensel's lemma

There are many variations on Hensel's lemma, considering factorization rather than roots of polynomials, or multiple polynomials in multiple variables. We give the version given in [2], a variation on Newton's method for finding roots of real polynomials and then conclude a corollary for multivariate polynomials.

Theorem 3.1. *Let $f(x) \in \mathscr{O}_K[x]$, and $x_0 \in \mathscr{O}_K$ such that $||f(x_0)||_{\mathfrak{p}} < ||f'(x_0)^2||_{\mathfrak{p}}$. Then the sequence determined by $x_i = x_{i-1} - \frac{f(x_{i-1})}{f'(x_{i-1})}$ converges to a root of $f(x)$ in $\hat{\mathscr{O}}_{K,\mathfrak{p}}$, which agrees with x_0 modulo $\mathfrak{p}$.*

We wil prove the theorem next time, but first note the following more general corollary.

Corollary 3.2. *Let $f(x_1, \dots, x_n)$ be a polynomial with coefficients in $\mathscr{O}_K$, and suppose that $(y_1, \dots, y_n) \in \mathscr{O}_K^n$ is such that*

$$||f(y_1, \dots, y_n)||_{\mathfrak{p}} < ||\frac{\partial f}{\partial x_i}(y_1, \dots, y_n)^2||_{\mathfrak{p}}$$

for some i. Then there exists $y_i' \in \hat{\mathscr{O}}_{K,\mathfrak{p}}$ such that $(y_1, \dots, y_i', \dots, y_n)$ is a root of f.

Proof. Indeed, we may substitute y_j for x_j for all $j \neq i$, and treat f as a polynomial in the single variable x_i. The statement then follows directly from the previous theorem. □

References

1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, 1966.
2. Serge Lang, *Algebraic number theory*, second ed., Springer-Verlag, 1994.