ALGEBRAIC NUMBER THEORY

LECTURE 7 NOTES

Material covered: Local fields, Hensel's lemma.

Remark. The non-archimedean topology: Recall that if K is a field with a valuation $|\ |$, then it also is a metric space with $d(x,y) = |x-y|$. The topology has a basis of open neighborhoods given by $B(x,\epsilon) = \{y \in K \,|\, |x-y| < \epsilon\}$. If the valuation is nonarchimedean, then this metric space or topology is rather bizarre. For instance, the open balls don't have a unique center: in fact, if we take any $y \in B(x,\epsilon)$, then y is a center of the ball as well, i.e. $B(x,\epsilon) = B(y,\epsilon)$! To see this, use the strong triangle inequality

$$d(z,x) < \epsilon \text{ and } d(y,x) < \epsilon \Rightarrow d(z,x) < \epsilon$$

so that $B(x,\epsilon) \subset B(y,\epsilon)$ and similarly, $B(y,\epsilon) \subset B(x,\epsilon)$. Note that the set $D(x,\epsilon) = \{y \in K \,|\, |x-y| \leq \epsilon\}$ is a closed set, but it is not necessarily the closure of $B(x,\epsilon)$ (see the next remark).

Remark. If the norm is discrete as well as nonarchimedean, then things get even stranger. Suppose $|x| = c^{-v(x)}$ for some $c > 1$ and a normalized exponential valuation v. Then the set $B(x,\epsilon)$ can be identified with $\{y \in K \,|\, v(x-y) > -\log_c(\epsilon)\}$. Since the valuation is discrete and integer-valued, it's easy to see that $v(x-y) > -\log_c(\epsilon)$ is equivalent to $v(x-y) \geq \lfloor -\log_c(\epsilon) + 1 \rfloor = \delta$, say. Therefore $B(x,\epsilon) = D(x,\delta)$ is closed. Hence K is disconnected, and the same argument shows that any subspace of K containing more than one point is disconected. In other words, K is totally disconnected.

Proposition 1. *Let K be a field with a discrete valuation v, and $\mathfrak{o}$ its valuation ring, $\mathfrak{p}$ the maximal ideal. Let $\widehat{K}$ be the completion of K with respect to v and $\hat{\mathfrak{o}}, \hat{\mathfrak{p}}$ the valuation ring and maximal ideal of $\hat{v}$. Then $\hat{\mathfrak{o}}/\hat{\mathfrak{p}} \cong \mathfrak{o}/\mathfrak{p}$ (and in fact, $\hat{\mathfrak{o}}/\hat{\mathfrak{p}}^r \cong \mathfrak{o}/\mathfrak{p}^r$ for $r \geq 1$).*

Proof. We have a map $\mathfrak{o} \to \hat{\mathfrak{o}} \to \hat{\mathfrak{o}}/\hat{\mathfrak{p}}$ and the kernel of this composition consists of all elements x of $\mathfrak{o}$ which are in $\mathfrak{p}$, so those which have $\hat{v} = v(x) \geq 1$. In other words, the kernel is $\mathfrak{p}$. So $\mathfrak{o}/\mathfrak{p} \to \hat{\mathfrak{o}}/\hat{\mathfrak{p}}$ and we just need to see that the map is surjective. Let $0 \neq x \in \hat{\mathfrak{o}}$ be the (limit of) the sequence $\{a_n\}$ in K. Now because $1 \geq \lim_{n\to\infty} |a_n| = |a_m|$ for m large enough, it follows that the sequence a_n eventually lies in $\mathfrak{o}$. Now choose N large enough such that $v(a_n - a_N) \geq 1$ for $n \geq N$. Then $x = a_N + y$ where $y = \lim(a_n - a_N)$ lies in $\hat{\mathfrak{p}}$, by definition.

Therefore $\hat{\mathfrak{o}} = \mathfrak{o} + \hat{\mathfrak{p}}$ proving the surjectivity. A similar proof works for the more general statement. □

Example. If we start with $K = \mathbb{Q}$ with its p-adic valuation $v_p(x) =$ power of p dividing x, then the completion is called the *field of p-adic numbers* $\mathbb{Q}_p$. Any nonzero element $\mathbb{Q}_p$ can be written as an infinite convergent series $p^k(a_0 + a_1 p + a_2 p^2 + \dots)$, with $k \in \mathbb{Z}$ and $a_0, a_1, \dots \in \{0, 1, \dots, p-1\}$.

More generally, we have the following description.

Proposition 2. *Let $R \subset \mathfrak{o}$ be a system of representatives for $\kappa = \mathfrak{o}/\mathfrak{p}$, which is usually taken to include 0 for convenience. Then every $0 \neq x \in \hat{K}$ has a unique representation as a convergent series*

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \dots)$$

where $a_i \in R, a_0 \neq 0, m \in \mathbb{Z}$.

Proof. Since π is also a uniformizer of the DVR $\hat{\mathfrak{o}}$, let $x = \pi^m u$, where $u \in \hat{\mathfrak{o}}^*$. Since $\hat{\mathfrak{o}}/\hat{\mathfrak{p}} \cong \mathfrak{o}/\mathfrak{p}$, the class $u \mod \hat{\mathfrak{p}}$ has a unique representative $a_0 \in R, a_0 \neq 0$. So $u = a_0 + \pi b_1$, with $b_1 \in \hat{\mathfrak{o}}$. Assume by induction we have

$$u = a_0 + a_1\pi + a_2\pi^2 + \dots + a_{n-1}\pi^{n-1} + \pi^n b_n$$

with $b_n \in \hat{\mathfrak{o}}$, and let a_n be the representative in R of the residue class of $b_n \mod \hat{\mathfrak{p}}$ to continue. So we get $\sum a_i \pi^i$ which is easily seen to be convergent and unique. □

Remark. The valuation ring $\mathbb{Z}_p$ of $\mathbb{Q}_p$ can be thought of as the collection of all the $\mathbb{Z}/p^n\mathbb{Z}$ together. Any element of $\mathbb{Z}_p$ determines a compatible collection of elements of $\mathbb{Z}/p^n\mathbb{Z}$ and vice versa. In formal terminology, $\mathbb{Z}_p$ is the inverse limit of the $\mathbb{Z}/p^n\mathbb{Z}$. Note that, for instance, every prime $q \neq p$ is invertible in $\mathbb{Z}_p$; in fact, it is already invertible in the valuation ring of $\mathbb{Q}$ with respect to $|\ |_p$.

The completion $\hat{K}$ of K with respect to the discrete valuation v is a complete metric space. We say that a field K is a *complete discretely valued field* (or CDVF for short) if it is complete with respect to the discrete valuation specificied.

Exercise. Two valuations are equivalent iff they define the same topology on K.

Example. In $\mathbb{Q}_p$, a basis of neighborhoods of 0 is given by $p^n\mathbb{Z}_p, n \in \mathbb{Z}$. These get smaller as n increases.

Lemma 1. *Let K be a CDVF such that $\kappa = \mathfrak{o}/\mathfrak{p}$ is finite. Then $\mathfrak{o}$ is compact and K is locally compact.*

Proof. For a metric space, compactness is equivalent to sequential compactness. So let $\{a_n\}$ be a sequence in $\mathfrak{o}$. Write

$$a_n = a_{n0} + a_{n1}\pi + a_{n2}\pi^2 + \dots$$

for every n, where a_{ni} are elements of a system of representatives $R \subset \mathfrak{o}$ of κ, which is finite. Since the values taken by the sequence $\{a_{n0}\}_{n\geq q}$ lie in a finite set R, some value must be taken infinitely often, say by some subsequence $\{a'_n\}$ where $a'_n = a_{f(n)}$ for some increasing function n. Then looking at the values a'_{n1} we refine further to a sequence $\{a''_n\}$ and so on. It's clear that the sequence $\{a_n^{(n)}\}$ will converge, and it is a subsequence of the original sequence. □

Example. In particular, $\mathbb{Z}_p$ is compact and $\mathbb{Q}_p$ is locally compact.

Definition 1. *Let $K_\mathfrak{p}$ be the completion of a number field K with respect to the nonarchimedean valuation $v_\mathfrak{p}$ corresponding to a prime $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$. (Recall that $v_\mathfrak{p}(x)$ is the power of $\mathfrak{p}$ dividing the principal fractional ideal (x) if $0 \neq x \in K$.) These fields $K_\mathfrak{p}$ are called* ***nonarchimedean local fields****. The* ***archimedean local fields*** *are $\mathbb{R}$ and $\mathbb{C}$.*

Theorem 1 (Ostrowski)**.** *Let K be a field complete with respect to an archimedean valuation. Then K is isomorphic to $\mathbb{R}$ or $\mathbb{C}$, and the valuation is equivalent to the usual archimedean valuation.*

We will omit the proof of this theorem (see, for instance, Neukirch pg. 125).

Remark. Nonarchimedean local fields are always CDVFs. There are also some local fields in positive characteristic (namely the Laurent series $\mathbb{F}_q((t))$ over a finite field), but we will not discuss them in this course.

Example. There is no square root of -1 in $\mathbb{Q}$, but there is a square root in $\mathbb{Q}_5$ for instance, which we may see from

$$(-1)^{1/2} = (4-5)^{1/2} = 2(1-5/4)^{1/2} = 2\left(1 - \frac{1}{2}\cdot\frac{5}{4} + \binom{\frac{1}{2}}{2}\cdot\left(\frac{5}{4}\right)^2 + \dots\right)$$

which converges since $|5| < 1$ in $\mathbb{Q}_5$, and 2 is invertible.

The following lemma is extremely important in the study of CDVFs.

Theorem 2 (Hensel's lemma)**.** *Let $f(x) \in \mathfrak{o}[x]$ be a primitive polynomial, i.e. $f(x) \neq 0$ mod $\mathfrak{p}$. Suppose that the reduction $\overline{f}(x)$ of f mod $\mathfrak{p}$ factors as $\overline{h}(x)\overline{g}(x)$, into relatively prime polynomials $\overline{g}, \overline{h} \in \kappa[x]$. Then $f(x) = g(x)h(x)$ for some polynomials $g, h \in \mathfrak{o}[x]$ such that $\deg g = \deg \overline{g}$ and $g(x) \equiv \overline{g}(x)$ mod $\mathfrak{p}$, $h(x) \equiv \overline{h}(x)$ mod $\mathfrak{p}$.*

Proof. Let π be a uniformizer. Let $\deg f = d, \deg \overline{g} = m$. Then $\deg \overline{h} \leq d - m$ (this is because the degree of $\overline{f}$ might be smaller than degree of f, if the highest coefficient is divisible by π. We inductively construct polynomials g_n and h_n of degrees m and at most $d - m$ respectively, such that

- $g_{n+1} \equiv g_n \bmod \pi^{n+1}$
- $h_{n+1} \equiv h_n \bmod \pi^{n+1}$

- $f \equiv g_n h_n \bmod \pi^{n+1}$.

Then it will follow that g_n, h_n converge to polynomials g, h with the required degree constraints and reductions mod $\mathfrak{p}$, such that $f = gh$. Now, g_0 and h_0 can be taken to be lifts of $\overline{g}, \overline{h}$ of the same degrees. Note that by assumption, $ag_0 + bh_0 \equiv 1 \bmod \mathfrak{p}$ for some polynomials $a, b \in \mathfrak{o}[x]$. To do the inductive step, suppose we have already constructed $g_0, h_0, \ldots, g_n, h_n$ with the desired properties. Let $g_{n+1} = g_n + p_n \pi^{n+1}$, $h_{n+1} = h_n + q_n \pi^{n+1}$. The first two conditions are automatically satisfied, and the third condition for $n+1$ becomes

$$f - g_n h_n \equiv (g_n q_n + h_n p_n)\pi^{n+1} \bmod \pi^{n+2}$$

since the last term is $\pi^{2n+2} p_n q_n$ which is divisible by π^{n+2}. By the induction hypothesis, the LHS is divisible by π^{n+1}. Let $r_n = \pi^{-n-1}(f - g_n h_n)$. Then cancelling π^{n+1}, the third condition becomes

$$r_n \equiv g_n q_n + h_n p_n \bmod \pi \equiv g_0 q_n + h_0 p_n \bmod \pi.$$

Now we recall that $ag_0 + bh_0 \equiv 1 \bmod \pi$, so that $(ar_n)g_0 + (br_n)h_0 \equiv r_n \bmod \pi$. At this point we would just like to set $q_n = ar_n$ and $p_n = br_n$, but the problem is that the degrees might become too large if we do that. So the final trick is the following: noting that the highest coefficient of g_0 is a unit (because $\deg g_0 = \deg \overline{g}$), we can divide with remainder:

$$br_n = qg_0 + p_n$$

where $\deg p_n < deg g_0 = m$. Then we have

$$r_n \equiv ar_n g_0 + br_n h_0 \equiv ar_n g_0 + (qg_0 + p_n)h_0 = (ar_n + h_0 q)g_0 + p_n h_0 \bmod \pi.$$

Let q_n be the polynomial obtained from $ar_n + h_0 q$ by omitting all coefficients divisible by π. Then because

$$g_0 q_n + h_0 p_n \equiv r_n \bmod \pi$$

and $\deg r_n \leq d$ (follows from induction hypothesis), $\deg h_0 p_n \leq (d-m) + (m-1) = d-1$, and the fact that the highest coefficient of g_0 is a unit, forces $\deg q_n \leq d - m$. This completes the inductive step. □

Corollary 1. *Let $f(x) \in \mathfrak{o}[x]$ be such that $\overline{f}(x)$ has a root $\alpha \in \kappa$ with $\overline{f}'(\alpha) \neq 0$. Then $f(x)$ has a root $x_0 \in \mathfrak{o}$ which reduces to α mod $\mathfrak{p}$.*

Example. If $p \neq 2$ and $x^2 \equiv a \bmod p$ has a solution then a is a square in $\mathbb{Z}_p$.

Example. The polynomial $x^{p-1} - 1 \in \mathbb{F}_p[x]$ has $p-1$ distinct solutions. So all the $(p-1)$'st roots of unity exist in $\mathbb{Z}_p$.

Corollary 2. *Let K be a CDVF. Then for every* irreducible *polynomial*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$$

such that $a_0 a_n \neq 0$, we have that

$$|f| := \max\{|a_0|, |a_1|, \ldots, |a_n|\}$$

equals $\max(|a_0|, |a_n|)$. *In particular, if $a_n = 1$ and $a_0 \in \mathfrak{o}$, then $f \in \mathfrak{o}[x]$.*

Proof. After multiplying by an element of K we may assume w.lo.g. that $f \in \mathfrak{o}[x]$ and that $|f| = 1$, i.e. that one of $a_0, a_1, \ldots, a_n$ is a unit. Let a_r be the first among the $a_0, a_1, \ldots, a_n$ such that $|a_r| = 1$. Then

$$f(x) \equiv x^r(a_r + a_{r+1}x + \ldots a_n x^{n-r}) \bmod \mathfrak{p}.$$

If $\max(|a_0|, |a_n|) < 1$ then $0 < r < n$ and so f would factor in $\mathfrak{o}[x]$ by Hensel's lemma, contradicting irreducibility. □

Now let L/K be a finite (hence algebraic) extension of a CDVF K. Then we'll define a valuation on L which extends that on $K \hookrightarrow L$, and show that L is a CDVF with respect to it.

Theorem 3. *There is a unique extension of a discrete valuation $|\ |$ of K to any finite extension L/K, and it is given by $|\alpha| = \sqrt[n]{N_{L/K}(\alpha)}$, where L/K has degree n. The field L is complete with respect to this valuation.*

Proof. Let $\mathfrak{O}$ be the integral closure of $\mathfrak{o}$ in L. We claim $\mathfrak{O} = \{\alpha \in L \mid N_{L/K}(\alpha) \in \mathfrak{o}\}$. It's clear that $\alpha \in \mathfrak{O} \Rightarrow N_{L/K}(\alpha) \in \mathfrak{o}$, since $\mathfrak{o}$ is integrally closed (it's a PID).

Conversely, let $\alpha \in L$ and $N_{L/K}(\alpha) \in \mathfrak{o}$. Let

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$$

be the minimal polynomial of α. Then $N_{L/K}(\alpha) = \pm a_0^m \in \mathfrak{o}$ for $m = [L : K(\alpha)]$, so $a_0 \in \mathfrak{o}$ as well. By the irreducibility of $f(x)$, the lemma above implies $f(x) \in \mathfrak{o}[x]$, so that $\alpha \in \mathfrak{O}$.

Now for the function $|\alpha| = \sqrt[n]{N_{L/K}(\alpha)}$, it's clear that $\alpha = 0 \Leftrightarrow |\alpha| = 0$ and $|\alpha\beta| = |\alpha||\beta|$. To prove the stong triangle inequality $|\alpha + \beta| \leq \max(|\alpha|, |\beta|)$, it's enough after dividing by α or β to show

$$|\alpha| \leq 1 \rightarrow |\alpha + 1| \leq 1$$

But $|\alpha| \leq 1$ is equivalent to $\alpha \in \mathfrak{O}$ which implies $\alpha+1 \in \mathfrak{O}$ which gives $|\alpha+1| \leq 1$, so this is true as well. It's clear from $N_{L/K}(a) = a^n$ for $a \in K$ that the valuation extends that of K.

Uniqueness: suppose we have another valuation $|\ |'$ extending that of K. Then let $\mathfrak{O}, \mathfrak{O}'$ be the corresponding DVRs and $\mathfrak{B}, \mathfrak{B}'$ the associated maximal ideals. We will show that the valuations are equivalent, so one is a power of the other. Since they agree on K, they are equal.

Suppose $\alpha \in \mathfrak{O} \backslash \mathfrak{O}'$. Let

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$$

be the minimal polynomial of α over K. Then $a_{d-1}, \ldots, a_0 \in \mathfrak{o}$ by the above. Also $\alpha \notin \mathfrak{O}' \Rightarrow v'(\alpha) < 0 \Rightarrow \alpha^{-1} \in \mathfrak{B}'$. Then

$$1 = -a_{d-1}\alpha^{-1} \cdots - a_0(\alpha^{-1})^d \in \mathfrak{B}'$$

which is impossible. This shows that $\mathfrak{O} \subset \mathfrak{O}'$ or in other words $|x| \leq 1 \Rightarrow |x|' \leq 1$. The reverse implication must also be true: otherwise if $|x|' \leq 1$ and $|x| > 1$, then letting π' be a uniformizer for $\mathfrak{O}'$, we have that $y = 1/(\pi' + \pi'^2 x^e)$ has $|y| < 1$ for large enough e, but $|y|' > 1$. Therefore the valuations are equivalent.

Finally, to show that L is complete, notice that L is a finite dimensional vector space over L. Now we use the standard fact that for any field complete with respect to an absolute value, any two norms on a finite dimensional vector space over it are equivalent, i.e. they define the same topology, or equivalently, each norm is bounded by a fixed positive multiple of the other. So the above norm on L must be equivalent (in the topological sense) to the max norm, which is defined as follows: let $v_1, \ldots, v_n$ be a basis of L over K. The max norm of an element $x = \sum x_i v_i$ ($x_i \in K$), is just $\max\{|x_1|, \ldots, |x_n|\}$. Now it's clear that L is complete with respect to the max norm, since for any Cauchy sequence, each of the coordinates will define Cauchy sequences in K, which comverge because K is complete. So L is complete with respect to the other norm as well. $\square$

18.786 Topics in Algebraic Number Theory
Spring 2010