Algebraic Number Theory part III, Michaelmas 2012: notes

Review of basic properties of number fields

Lecture 1

(Algebraic) Number Field = finite extension $K/\mathbb{Q}$, degree $n = [K:\mathbb{Q}]$. Its *ring of integers* is

$$\mathfrak{o}_K = \{\text{algebraic integers of } K\} = \{x \in K \mid \text{min. poly of } x \text{ is in } \mathbb{Z}[X]\}$$

One shows (using the discriminant) that $\mathfrak{o}_K \simeq \mathbb{Z}^n$ as a $\mathbb{Z}$-module. *Algebra:* $\mathfrak{o}_K$ is a *Dedekind domain*. Recall that for an integral domain R with FoF F, TFAE:

i) R is Noetherian, is integrally closed in F, and every non-0 prime ideal of R is maximal.

ii) Every non-0 ideal of R has a unique factorisation as a product of prime ideals.

(It's easy to see that $\mathfrak{o}_K$ satisfies (i).)

A *fractional ideal* of R is a finitely-generated non-0 R-submodule of F. Equivalently, is is xR for some $x \in F^*$. Then {fractional ideals} is an abelian group under multiplication, and (ii) implies that is is freely generated by the set of non-0 prime ideals

$$I = \prod P^{v_P(I)}, \quad \text{where } v_P(I) \in \mathbb{Z} \text{ and } v_P(I) = 0 \text{ for all but finitely many } P.$$

If I, $J \subset R$ are ideals, then

$$v_P(I+J) = \min(v_P(I), v_P(J)), \quad v_P(I \cap J) = \max(v_P(I), v_P(J)), \quad I + J = R \implies I \cap J = IJ$$

and the Chinese Remainder Theorem then implies

$$R/I \xrightarrow{\sim} \prod R/P^{v_P(I)}.$$

The *class group*: $Cl(R) = \{\text{fractional ideals}\}/\{\text{principal ideals } xR\}$. Then:

Theorem. *$Cl(\mathfrak{o}_K)$ is finite.*

This needs more than just algebra (for an arbitrary Dedekind domain R, $Cl(R)$ can be infinite).

Archimedean analysis: There are exactly $n = [K:\mathbb{Q}]$ distinct embeddings $\sigma_i \colon K \hookrightarrow \mathbb{C}$: can write then as r_1 real and r_2 pairs of complex conjugate embeddings, where $n = r_1 + 2r_2$:

$$\sigma_1, \dots \sigma_{r_1} \colon K \hookrightarrow \mathbb{R}, \quad \sigma_{r_1+1} = \overline{\sigma}_{r_1+r_2+1}, \dots, \sigma_{r_1+r_2} = \overline{\sigma}_n \colon K \hookrightarrow \mathbb{C}.$$

If $(x_1, \dots, x_n)$ is a $\mathbb{Q}$-basis for K then $\det(\sigma_i(x_j)) \neq 0$. In particular, if $\mathfrak{o}_K = \sum \mathbb{Z}x_i$ then $d_K = \det(\sigma_i(x_j))^2 \in \mathbb{Z} \setminus 0$, the *discriminant* of K. Then

$$\sigma = (\sigma_1, \dots, \sigma_{r_1+r_2} \colon K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$$

and $\sigma(\mathfrak{o}_K)$ is a *lattice* (discrete subgroup of rank n).

One aspect of modern algebraic number theory is to regard the prime ideals P and the complex embeddings σ_i as analogous objects. From this viewpoint, primes correspond to embedding of K into topological fields other than $\mathbb{C}$, so-called nonarchimedean fields. Begin by looking at these.

1 Valuations and absolute values

Definition. A (rank 1) valuation of K is a non-trivial homomorphism $v\colon K^* \to \mathbb{R}$ s.t.:

$$\text{for all } x, \in K \text{ with } y \neq -x, \qquad v(x+y) \geq \min(v(x), v(y)). \qquad \text{(V)}$$

Remark. By convention we extend v to all of K by setting $v(0) = +\infty$, so that (with the obvious arithmetic in $\mathbb{R} \cup \{+\infty\}$) (V) holds for all $x, y \in K$. Some people don't require $v(K^*) \neq \{0\}$ (so allow the "trivial valuation").

Examples. (i) p-adic valuation: $v_p\colon \mathbb{Q}^* \to \mathbb{R}$, $v_p(p^n a/b) = n$ if $(p, ab) = 1$.

(ii) K a number field, $0 \neq P \subset \mathfrak{o}_K$ a prime ideal. Then define, for $0 \neq x \in K^*$, $v_P(x)$ to be the exponent of P in the factorisation of the fractional ideal $x\mathfrak{o}_K$. Obviously a homomorpism. To see that (V) holds, let $x, y \in K$. Multiplying by suitable $z \in \mathfrak{o}_K$, may assume WLOG $x, y \in \mathfrak{o}_K$. In this case $v_P(x) = n \iff x \in P^n \setminus P^{n+1}$ and (V) is then obvious.

(iii) K = field of meromorphic functions on $\mathbb{C}$. Then $v(f) = \mathrm{ord}_{z=0} f(z)$ is a valuation of K.

Definition. A valuation v of K is *discrete* is $v(K^*) \subset \mathbb{R}$ is a discrete subgroup; it then equals $r\mathbb{Z}$ for some $r > 0$. A discrete valuation v is *normalised* if $v(K^*) = \mathbb{Z}$.

All the previous examples are normalised discrete valuations. We will come across important examples when $v(K^*) = \mathbb{Q}$.

Remark. There are other (rank > 1) valuations of fields. We shall not consider them.

If v is a valuation of F, and $\alpha > 0$, then αv is obviously also a valuation. We say v, αv are *equivalent* valuations.

Proposition 1.1. *Let v be a valuation on K. Then if $v(x) \neq v(y)$, $v(x+y) = \min(v(x), v(y))$.*

Proof. WLOG $v(x) < v(y) = v(-y)$, so $v(x) = v((x+y)-y) \geq \min(v(x+y), v(y))$, hence $v(x) \geq v(x+y) \geq \min(v(x), v(y)) = v(x)$. □

Lecture 2

Definition. Let K be a field, $R \subset K$ a proper subring. We say that R is a *valuation ring* of K is $x \in K \setminus R \implies x^{-1} \in R$.

Remark. Definition implies that if $x, y \in R \setminus 0 \implies$ at least one of x/y, y/x is in R. Obviously then $\mathrm{Frac}(R) = K$.

Theorem 1.2. *Let R be a valuation ring of K. Then*

i) R is a local ring with maximal ideal $\mathfrak{m} = R \setminus R^*$.

ii) R is integrally closed.

iii) Every finitely generated ideal of R is principal; in particularly R is Noetherian (every ideal is f.g.) iff R is a PID.

Recall what these mean: a ring R is *local* if it has exactly one maximal ideal. A domain R is *integrally closed* if $x \in \mathrm{Frac}(R)$, $a_0, \ldots, a_{n-1} \in R$ with $x^n + \sum a_i x^i = 0$ implies $x \in R$.

Proof. i) Let $\mathfrak{m} = R \setminus R^*$. Trivially $x \in \mathfrak{m}$, $y \in R \implies xy \in \mathfrak{m}$. If $x, y \in \mathfrak{m} \setminus 0$ then WLOG $z = y/x \in R$, hence $x + y = x(1+z) \in \mathfrak{m}$. So $\mathfrak{m}$ is an ideal. Since $R \setminus \mathfrak{m} = R^*$, every proper ideal of R is contained in $\mathfrak{m}$, hence $\mathfrak{m}$ is the unique maximal ideal of R.

ii) Let $x \in K^*$ be integral over R, say

$$x^n + \sum_{i=0}^{n-1} a_i x^i = 0, \qquad a_i \in R.$$

If $x^{-1} \notin R$ then $x \in R$ and we are finished. Otherwise, $x^{-1} \in R$ and

$$x^{-1}\Big(-\sum_{i=0}^{n-1} a_i (x^{-1})^{n-i-1}\Big) = 1$$

so $x^{-1} \in R^*$, hence $x \in R$.

iii) If x, $y \in R$ are nonzero then

$$xR + yR = \begin{cases} xR & \text{if } y/x \in R \\ yR & \text{if } x/y \in R \end{cases}$$

□

Theorem 1.3. *(i) Let K be a field, v a valuation on K. Define*

$$R_v = \{x \in K \mid v(x) \geq 0\}, \qquad \mathfrak{m}_v = \{x \in K \mid v(x) > 0\}.$$

Then R_v is a valuation ring with maximal ideal $\mathfrak{m}$, and v induces an isomorphism $K^*/R_v^* \xrightarrow{\sim} v(K^*) \subset \mathbb{R}$.

(ii) R_v is a maximal proper subring of K, and depends only on the equivalence class of v.

(iii) If v, v' are valuations of K and $R_v \subset R_{v'}$ then $R_v = R_{v'}$ and v, v' are equivalent. In particular, for any valuation ring R of K there is at most one equivalence class of valuations v with $R_v = R$.

Examples to bear in mind is

$$\mathbb{Z}_{(p)} = \Big\{\frac{x}{y} \;\Big|\; x, y \in \mathbb{Z},\ (p, y) = 1\Big\} \subset \mathbb{Q}$$

the valuation ring of the p-adic valuation v_p, and more generally

$$\mathfrak{o}_{K,P} = \Big\{\frac{x}{y}\Big| x, y \in \mathfrak{o}_K,\ y \notin P\Big\} \subset K$$

the valuation ring of the P-adic valuation of a number field K.

Proof. i) By definition of a valuation, R_v is a ring, and $R_v \neq K$ since v is nontrivial. Also $x \notin R_v \implies v(x) < 0 \implies v(x^{-1}) > 0 \implies x^{-1} \in R$. So R_v is a valuation ring of K, its nonunits are obviously $\mathfrak{m}$, and $\ker(v) = R_v^*$.

ii) Let $x \in K \setminus R_v$. Then $v(x) < 0$, so for any $y \in K$, there exists $n \in \mathbb{Z}$ with $v(y) \geq nv(x)$. Then $y/x^n \in R$, so $y \in R[x]$ i.e. $R[x] = K$, so R is maximal. Obviously if v and v' are quivalent, $R_v = R_{v'}$.

iii) By ii) we get $R_{v'} = R_v$ (hence $\mathfrak{m}_v = \mathfrak{m}_{v'}$). Therefore for any $x, y \in K$

$$v(x) \geq v(y) \iff x/y \in R_v \iff v'(x) \geq v'(y).$$

Let $0 \neq \pi \in \mathfrak{m}_v$. Then for any $p/q \in \mathbb{Q}$, $q > 0$,

$$\frac{v(x)}{v(\pi)} \geq \frac{p}{q} \iff v(x^q) \geq v(\pi^p) \iff x^q \pi^{-p} \in R_v$$

and the same for v', hence $v(x)/v(\pi) = v'(x)/v'(\pi)$, and so v, v' are equivalent. $\square$

Remark. Conversely, any valuation ring of a field which is maximal is some R_v (see example sheet). (To get all valuation rings we need to consider valuations of higher rank.)

Definition. A *discrete valuation ring* or DVR is the valuation ring of a discrete valuation on some field.

Proposition 1.4. *A domain is a DVR $\iff$ it is a PID with a unique nonzero prime ideal.*

Proof. Let R be a PID with ! prime ideal πR, $\mathrm{Frac}(R) = K$. For $0 \neq x \in R$ define $v(x) = n \in \mathbb{N}$ with $xR = \pi^n R$; for $0 \neq x/y \in K^*$ set $v(x/y) = v(x) - v(y)$ — easy to see that v is a DV on K with valuation ring R.

Lecture 3

Conversely, let R_v be a DVR. As $v(K^*)$ is discrete, there exists $x \in I$ with $v(x)$ minimal, and then $I = xR$. So R_v is Noetherian, hence a PID by Theorem 1.2(iii), and in a PID, maximal ideals are the same as non-0 prime ideals. $\square$

Lemma 1.5. *(R, π) a DVR. Then for every m, $n \geq 0$, have R-module isomorphism*

$$\pi^m \colon R/\pi^n R \xrightarrow{\sim} \pi^m R/\pi^{m+n} R.$$

Proof. Obvious for any ring R and $\pi \in R$ which is not a zero-divisor. $\square$

Theorem 1.6. *Any valuation on $\mathbb{Q}$ is equivalent to some v_p. Any valuation on a number field K is equivalent to some v_P.*

Proof. Let $\mathfrak{o}_K$ be the ring of integers of K, v a valuation of K. Then as R_v is integrally closed, $R_v \supset \mathfrak{o}_K$. As $\mathrm{Frac}\,\mathfrak{o}_K = K$, v is nontrivial on $\mathfrak{o}_K$. Therefore $P = \mathfrak{m}_v \cap \mathfrak{o}_K$ is a non-zero prime ideal of $\mathfrak{o}_K$. Then $x \in \mathfrak{o}_K \setminus P \subset R_v \setminus \mathfrak{m}_v \implies v(x) = 0$, and so $R_v \supset \mathfrak{o}_{K,P}$. Then by Thm.1.3(iii), $R_v = \mathfrak{o}_{K,P}$ and v factors through $v_P \colon K^*/\mathfrak{o}_{K,P}^* \xrightarrow{\sim} \mathbb{Z}$. $\square$

Definition. K a field. A map $|-| : K \to \mathbb{R}_{\geq 0}$ is an *absolute value (AV)* if for all x, $y \in K$:

(AV1) $|x| = 0$ iff $x = 0$

(AV2) $|xy| = |x| \cdot |y|$

(AV3) $|x + y| \leq |x| + |y|$

(AV4) $\exists x \in K$ with $|x| \notin \{0, 1\}$.

If (AV3) can be replaced by

(AV3N) $|x + y| \leq \max(|x|, |y|)$

then it is said to be a *nonarchimedean* AV. If not, say it is *archimedean*.

Obvious archimedean AVs are usual (Euclidean) absolute value on $\mathbb{R}$, and modulus on $\mathbb{C}$.

Theorem 1.7. *Fix $\rho \in (0,1)$. Let v be a valuation on K. Then $|x|_v = \rho^{v(x)}$ is a nonarchimedean AV on K, and $v \to |-|_v$ is a bijection between valuations and NAAVs on K.*

Proof. Obvious from definitions. Recover v from $|-|_v$ by $v(x) = \log |x|_v / \log \rho$. □

For example, v_p on $\mathbb{Q}$ gives rise to the p-adic AV, usually normalised by taking $\rho = 1/p$:

$$|p^n u/v|_p := \frac{1}{p^n}, \quad (p, uv) = 1.$$

If $|-|$ is a non-arch. AV then so is $|-|^r$, any $r > 0$. We say $|-|$, $|-|^r$ are *equivalent* AVs.

Proposition 1.8. *Let $|-|$ be an AV on K. Then the function $d(x,y) = |x-y|$ is a metric on K, invariant under translation, for which the field operations are continuous. Equivalent AVs determine equivalent metrics.*

Proof. Follows instantly from the axioms. □

In particular, any AV on K makes K into a topological field, the topology only depending on the equivalence class of the AV.

It's convenient to weaken the definition of AV to replace (AV3) with

(AV3$'$) for some $\alpha \in (0,1]$, $|x+y|^\alpha \leq |x|^\alpha + |y|^\alpha$.

With this definition, the square of complex modulus is an AV on $\mathbb{C}$. If $|-|$ satisfies (AV3$'$) then $|-|^r$ satisfies (AV3), so this definition is not significantly different.

We've already classified NAAVs of $\mathbb{Q}$. For archimedean ones, one has:

Theorem 1.9 (Ostrowski's Theorem)**.** *Any archimedean AV of $\mathbb{Q}$ is equivalent to the Euclidean AV.*

Proof. Omitted. □

2 Completion

Let K be a field with an AV $|-|$, satisfying (AV3). Mimicing one of the usual constructions of $\mathbb{R}$ from $\mathbb{Q}$, we can enlarge K to a complete field:

Theorem 2.1. *There exists a field $\widehat{K}$ with an AV $|-|\hat{}$, together with an isometric embedding $\iota\colon K \hookrightarrow \widehat{K}$, such that:*

i) $\widehat{K}$ is complete w.r.t the metric given by $|-|\hat{}$;

ii) $\iota(K)$ is dense in $\widehat{K}$; and

iii) any isometric embedding $(K, |-|) \overset{(}{\longrightarrow} K', |-|')$ of K into a complete field factors uniquely through ι.

Proof. (Sketch) Let $R \subset K^{\mathbb{N}}$ be the set of Cauchy sequences in K, and $I \subset R$ be the subset of null sequences. It's easy to see that R is a ring, and I is an ideal. Moreover I is maximal: let $x = (x_n) \in R \setminus I$. As $x \notin I$, $|x_n|$ is bounded below by some $\epsilon > 0$ for all $n \geq N$ sufficiently large. Set $y_n = 1/x_n$ for $n \geq N$. Then

$$|y_n - y_m| = \frac{|x_m - x_n|}{|x_m x_n|} \leq \epsilon^{-2} |x_m - x_n|$$

so the sequence $y = (y_n)$ (where we define $y_n = 0$ if $n < N$) is Cauchy, and $xy \in 1 + I$. So R/I is a field, and easily check that it is complete with respect to the absolute value

$$|(x_n)_{n\in\mathbb{N}}| = \lim_{n\to\infty} |x_n|.$$

If $j\colon K \hookrightarrow K'$ is an embedding of K into a complete field as in (iii), then it defines a map $R \to K'$ by $(x_n) \mapsto \lim j(x_n)$, whose kernel is I. $\square$

If $K = \mathbb{Q}$ and $|-|$ is Euclidean AV then $\widehat{K} = \mathbb{R}$.

Lecture 4

If $K = \mathbb{Q}$ and $|-| = |-|_\infty$, Euclidean absolute value, then $\hat{K} = \mathbb{R}$.

Until the end of this section, we consider only non-archimedean valuations. Then it's clear that the extension $|-|\hat{}$ is also non-archimedean. We'll simply denote it $|-|$ if there is no confusion. Then if $|-| = |-|_v$ for some valuation v of K, we get an extension of v to a valuation of $\hat{K}$, which we'll also denote v.

Example: $K = \mathbb{Q}$, $|-| = |-|_p$ the p-adic absolute value. Then $\hat{K}$ is denoted $\mathbb{Q}_p$, the *field of p-adic numbers.* It's valuation ring is written $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\}$, the *ring of p-adic integers.*

Let's give a completely explicit description of $\mathbb{Q}_p$ and $\mathbb{Z}_p$.

Proposition 2.2. *Every element of $\mathbb{Z}_p$ has a unique representation as a series*

$$x = a_0 + a_1 p + \cdots = \sum_{n=0}^{\infty} a_n p^n, \qquad a_n \in \{0, 1, \ldots, p-1\}.$$

Every element of $\mathbb{Q}_p$ has a unique representation as a series

$$x = a_{-N} p^{-N} + a_{-N+1} p^{-N+1} + \cdots = \sum_{n=-N}^{\infty} a_n p^n, \qquad a_n \in \{0, 1, \ldots, p-1\}$$

for some N. In either case, $v_p(x) = \min\{n \mid a_n \neq 0\}$.

Proof. Let $x_n = \sum_{i\leq n} a_i p^i$. Then if $n > m$,

$$|x_n - x_m|_p = \left| \sum_{i=m}^{n-1} a_i p^i \right|_p \leq \max\{|a_i p^i|_p \mid m \geq i < n\} \leq p^{-m}$$

so (x_n) is Cauchy and the series converges. Conversely, suppose $x \in \mathbb{Z}_p$ and $n > 0$. Claim there exists a unique $y_n \in \mathbb{Z}$ with $0 \leq y_n < p^n$ and $|x - y_n|_p \leq p^{-n}$. In fact, as $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, there exists $a/b \in \mathbb{Q}$ with $|x - a/b|_p \leq p^{-n}$. As $|x|_p \leq 1$, the strict triangle equality (AV3N) implies $|a/b|_p \leq 1$, so WLOG $(p, b) = 1$. Choose $c \in \mathbb{Z}$ with $bc \equiv 1 \pmod{p^n}$. Then $v_p(bc) = 0$, i.e. $|bc|_p = 1$, so

$$|x - ac|_p \leq \max(|x - bcx|_p, |bcx - ac|) = \max(|x|_p |bc - 1|_p, |x - a/b|_p) \leq p^{-n}$$

Let $y_n \in \{0, 1, \ldots, p^n - 1\}$ be the unique element with $y \equiv ac \pmod{p^n}$. Then $y_n = y_{n+1} \pmod{p^n}$ and so there exists a unique sequence $(a_i) \in \{0, \ldots, p-1\}^{\mathbb{N}}$ such that for every $n > 0$,

$$y_n = \sum_{i=0}^{n-1} a_i p^i.$$

Thus every element of $\mathbb{Z}_p$ has a unique representation in the given form. As $\mathbb{Z}_p$ is the valuation ring of $\mathbb{Q}_p$ with respect to $|-|_p$, $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, so writing $x \in \mathbb{Q}_p$ as x/p^N with $x \in \mathbb{Z}_p$ gives the second part.

For the last, suppose $x = \sum_{n \geq 0} a_n p^n \in \mathbb{Z}_p$ with $0 \leq a_n < p$. Then $x = a_0 + py$, $y = \sum_{n \geq 1} a_n p^{n-1} \in \mathbb{Z}_p$, so $v_p(x) = 0 \iff v_p(a_0) = 0 \iff a_0 \neq 0$. The formula for $v_p(x)$, $x \in \mathbb{Q}_p$¡ follows at once. □

In other words, p-adic numbers may be represented as "backwards decimals" (in base p, of course!), and addition and multiplication can be carried out in the same way as for decimal expansion of real numbers.

A more sophisticated, and more general, way to see this uses the concept of *inverse limit*.

Let X_n ($n \in \mathbb{N}$) be a sequence of sets (or groups, rings or ...) and $\pi_n \colon X_n \to X_{n-1}$ a collections of maps (or homomorphisms) between them. We call the system (X_n, π_n) an *inverse system*. Its *inverse limit* is defined to be

$$\varprojlim (X_n, \pi_n) = \varprojlim X_n := \{(x_n)_n \mid \forall n,\ x_n \in X_n,\ \pi_n(x_n) = x_{n-1}\} \subset \prod_{n \in \mathbb{N}} X_n.$$

Typically we wil only be concerned with inverse systems in which the π_n are surjective. If X_n are groups (or rings, or ...) and π_n are homomorphisms, then $\varprojlim X_n$ is also a group (or ring...) under the obvious operations.

Remark. More generally, we may replace $\mathbb{N}$ with any partially-ordered set I in which every pair of elements has an upper bound. View I as a category, with one morphism $f_{ij} \colon i \to j$ whenever $i \geq j$. Fix a category $\mathcal{C}$ (sets, groups, rings...). A *projective system* in $\mathcal{C}$ is a functor $X \colon I \to \mathcal{C}$. So for each $i \in I$ we have an object $X(i)$, and for each pair i, j with $i \geq j$ a morphism $X_{ij} \colon X(i) \to X(j)$. If $\mathcal{C}$ is a concrete category (the objects are sets with some additional structure) we may form

$$\varprojlim X = \{(x_i)_{i \in I} \mid x_i \in X(i),\ X_{ij}(x_i) = x_i \text{ if } i \geq j\} \subset \prod_{i \in I} X_i.$$

Depending on $\mathcal{C}$, this may or may not be an object of $\mathcal{C}$ — if it is, we call it the *projective limit* of X.

Example: let $X_n = \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\pi_n} \mathbb{Z}/p^{n-1}\mathbb{Z}$, reduction modulo p^{n-1}. Then I claim that (at least as a set) $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is precisely $\mathbb{Z}_p$. This is clear from the proof of Proposition 2.2, using the standard bijection $\{0, 1, \ldots, p^n - 1\} \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Completion: let R be a ring, $I \subset R$ an ideal, I^n its n-th power (recall that the product of ideals I and J is

$$IJ = \{\text{finite sums } \sum x_n y_n \mid x_n \in I,\ y_n \in J\}$$

which is an ideal). The *I-adic completion* of R is

$$\widehat{R} = \varprojlim R/I^n$$

where the maps $\pi_n \colon R/I^n \to R/I^{n-1}$ are the obvious ones. Clearly $\widehat{R}$ is a ring, and there is a homomorphism $R \to \widehat{R}$ given by

$$(x \in R) \mapsto ((x_n = x + I^n)_n \in \varprojlim R/I^n)$$

whose kernel is $\bigcap_n I^n$.

Example: $R = k[T]$ polynomial ring over a field k, $I = (T)$. Then R/I^n is the ring of truncated polynomials $\{\sum_{0\le i<n} a_i T^i\}$, and it's easy to see that $\widehat{R}$ is the ring of formal power series

$$k[[T]] = \{\sum_{n\ge 0} a_n T^n\}.$$

Lecture 5

Last time: R ring, I ideal; I-adic completion $\widehat{R} = \varprojlim R/I^n$. We say R is *I-adically complete* if the natural map $R \to \widehat{R}$ is an isomorphism.

Topology on the inverse limit: let $X = \varprojlim X_n$, and let $pr_m \colon X \to X_m$ be the m-th component map: $(x_n) \mapsto x_m$. We define the *inverse limit* topology to be the smallest topology for which the maps pr_m are continuous (for the discrete topology on X_m). This means that the open sets of X are arbitrary unions of sets of the form

$$U_{m,a} = pr_m^{-1}(a).$$

Proposition 2.3. *(i) $\varprojlim X_n$ is totally disconnected.*

(ii) Suppose each X_n is finite. *Then $\varprojlim X_n$ is compact.*

Proof. (i) Let $x = (x_n)$, $y = (y_n) \in \varprojlim X_n$. Suppose $x \neq y$. Then for some m we have $x_m \neq y_m$, and then $\varprojlim X_n$ is the disjoint union of the open sets

$$U_{m,x_m} \qquad \text{and} \qquad (pr_n^{-1}(x_m))^c = \bigcup_{x_m \neq a \in X_m} U_{m,a}$$

with x belonging to the first and y to the second. So $\varprojlim X_n$ is totally disconnected.

(ii) Each X_n is compact for the discrete topology. Tychonoff's theorem (product of compact spaces with the product topology is compact) implies that $\prod X_n$ is compact. Then $\varprojlim X_n \subset \prod X_n$ is a closed subspace with the induced topology (check!) hence is compact. □

Theorem 2.4. *Let v be a valuation of K, R the valuation ring. Let $\hat{K}$ be the completion of K with respect to $|-|_v$, and $\hat{R}$ its valuation ring. Then for any $\pi \in R \setminus 0$ with $v(\pi) > 0$, there is a canonical topological isomorphism between $\hat{R}$ and $\varprojlim R/\pi^n R$.*

Proof. Let $(x_n) \in \varprojlim R/\pi^n R$. For each n choose $y_n \in R$ lifting x_n. Then if $n > m$, $y_n - y_m \in \pi^m R$ so $|y_n - y_m|_v \le |\pi|_v^m$. As $|\pi|_v < 1$, (y_n) is a Cauchy sequence, converging to a unique element $y \in \hat{K}$, and $|y| = \lim |y_n| \geq 0$, so $y \in \hat{R}/$ If (y'_n) is another set of liftings, converging to $y' \in \hat{R}$, then $|y'_n - y_n| \leq |\pi|^n$, so $(y'_n - y_n)$ is a null sequence and $y' = y$. This defines the map $\varprojlim R/\pi^n R \to \hat{R}$. which is easily checked to be a continuous homomorphism.

In the other direction, let (y_n) be a Cauchy sequence in K converging to some $y \in \hat{K}$ with $|y| \leq 1$. Then (see example sheet) $|y_n| = |y|$ for $n \geq N$ sufficiently large, in particular $y_n \in R'$ for $n \geq N$. Choose a subsequence (z_n) of (y_n) such that $|z_{n+1} - z_n| \leq |\pi|^n$. Then $z_{n+1} - z_n \in \pi^n R$, so $(z_n) \in \varprojlim R/\pi^n R$. Exercise to check this is the required continuous inverse. □

Hensel's lemma: origin of p-adic numbers:

Problem. Let $f \in \mathbb{Z}[T]$, and suppose $a \in \mathbb{Z}$ with $f(a) \equiv 0 \pmod{p^n}$, some $n > 0$. Can we find $b \in \mathbb{Z}$ with $b \equiv a \pmod{p^n}$ and $f(b) \equiv 0 \pmod{p^{n+1}}$?

Example: take $p = 2$, $f = T^2 + 1$, $a = 1$. Then even for $n = 1$ answer is no (-1 is not a square mod 4).

If we could do this for every n, this would give a sequence $x_n \in \mathbb{Z}$ such that $x_{n+1} \equiv x_n \pmod{p^n}$ and $f(x_n) \equiv 0 \pmod{p^n}$. Then the limit $x = \lim(x_n) \in \mathbb{Z}_p$ exists and is a root of f.

Theorem 2.5 (Hensel's Lemma)**.** *Let R be a complete DVR, uniformiser π. Suppose f, g_1, $h_1 \in R[T]$ with g_1 monic, $(\bar{g}_1, \bar{h}_1) = 1$ and $f \equiv g_1 h_1 \pmod{\pi}$. Then there exist unique g, $h \in R[T]$ with g monic such that $g \equiv g_1$, $h \equiv h_1 \pmod{\pi}$ and $f - gh$.*

(Here $\bar{g} \in k[T]$ denotes the reduction of g mod π.)

Corollary 2.6. *Let $f \in R[T]$ be monic. Suppose $a \in R$ with $f(a) \equiv 0 \not\equiv f'(a) \pmod{\pi}$. There there exists a unique $b \in R$ with $b \equiv a \pmod{\pi}$ and $f(b) = 0$.*

(Proof of corollary: write $f(T) = (T - a)h_1(T) + f(a)$, $h_1 \in R[T]$, $g_1 = T - a$ and apply Theorem.)

Proof. Let $N = \deg(f)$, $d = \deg(g_1)$. WLOG $\deg(h_1) \leq N - d$. Will inductively construct (g_n, h_n) in $R[T]$ such that g_n is monic of degree d, $\deg(h_n) \leq N - d$, $f \equiv g_n h_n \pmod{\pi^n}$ and $g_{n+1} \equiv g_n$, $h_{n+1} \equiv h_n \pmod{\pi^n}$, and such that at each stage, (g_n, h_n) is unique modulo π^n.

Granted this: by completeness of R, the sequences (g_n), (h_n) converge coefficient-by-coefficient to some g, $h \in R[T]$ and $f = gh$. By the uniqueness at each stage, any g, h satisfying the conditions of the theorem has $g \equiv g_n$, $h \equiv h_n \pmod{\pi^n}$ hence the solution is unique.

Lecture 6

Construction: suppose we have (g_n, h_n), so $f - g_n h_n = \pi^n q$ for some $q \in R[T]$, $\deg(q) \leq N$, and (g_n, h_n) unique mod π^n. Write

$$g_{n+1} = g_n + \pi^n u, \quad h_{n+1} = h_n + \pi^n v, \qquad \deg(u) \leq d - 1,\ \deg(v) \leq N - d.$$

Then

$$f \equiv g_{n+1} h_{n+1} \pmod{\pi^{n+1}} \qquad \Longleftrightarrow \qquad g_n v + h_n u \equiv q \pmod{\pi}.$$

So enough to show there exist unique $\bar{u}$, $\bar{v} \in k[T]$ with $\deg(\bar{u}) \leq d - 1$, $\deg(\bar{v}) \leq N - d$ and

$$\bar{g}_n \bar{u} + \bar{h}_n \bar{v} = \bar{q}. \qquad (*)$$

Now $(\bar{g}_n, \bar{h}_n) = (\bar{g}_1, \bar{h}_1) = 1$ in $k[T]$, so there exists a pair $(\bar{u}, \bar{v})$ satisfying $(*)$, and the pair is unique up to transformations $\bar{u} \mapsto \bar{u} + \bar{r}\bar{g}_1$, $\bar{v} \mapsto \bar{v} - \bar{r}\bar{h}_1$ with $\bar{r} \in k[T]$. So there is a unique choice of $\bar{r}$ for which $\deg(\bar{u}) \leq d - 1$, and $(*)$ then implies $\deg(\bar{v}) \leq N - d$. □

Before we pass on to extensions, one final remark (which could have come earlier):

Proposition 2.7. *Let R be a valuation ring, $\pi \in \mathfrak{m}_R \setminus R$, and $\hat{R} = \varprojlim R/\pi^n R$. Then the map $R/\pi^n R \to \hat{R}/\pi^n \hat{R}$ is an isomorphism.*

Proof. By Theorem 2.4, $\hat{R}$ is the valuation ring of the completion $\hat{K}$ of K, so $R \to \hat{R}$ is injective and $\pi^n \hat{R} = \{x \in \hat{K} \mid v(x) \geq nv(\pi)\}$. Therefore $\pi^n \hat{R} \cap R = \pi^n R$, so $R/\pi^n R \to \hat{R}/\pi^n \hat{R}$ is injective. As K is dense in $\hat{K}$, R is dense in $E\hat{R}$ and so for all $x \in \hat{R}$, there exists $y \in R$ with $x - y \in \pi^n \hat{R}$. Therefore the map is an isomorphism. □

Examples. Take $R = \mathbb{Z}_p$ (p odd), $f = T^{p-1} - 1$. Then $f \equiv (T-1)(T-2)\cdots(T-p+1)$, so Hensel's lemma says that for each $a \in \{1, \ldots, p-1\}$ there exists a unique $\hat{a} \in \mathbb{Z}_p$ with $\hat{a} \equiv a \pmod{p}$ and $(\hat{a})^{p-1} = 1$. So $\mathbb{Z}_p$ contains all $(p-1)$-st roots of 1.

More generally, let R be a complete DVR with finite residue field $\mathbb{F}_q$. Applying Hensel's lemma with $f = T^{q-1} - 1$ shows that R comtains all $(q-1)$-st roots of unity.