Contents

Let K we a number field of degree n over the rationals.

1 Introduction to the problem

2 Dual basis

Let $\omega_1, ..., \omega_n$ be a basis for K over k and choose n elements, $c_1, ..., c_n$, in k. We know that the $n \times n$ matrix, $\mathrm{Tr}\omega_i\omega_j$, is non-singular since

$$0 \neq \mathrm{disc}(\omega_1, ..., \omega_n) = |\mathrm{Tr}(\omega_i\omega_j)|^2$$

This means that there is a unique solution, $x_1, ..., x_n \in k$, to the n equations

$$\sum_{j=1}^{n} \mathrm{Tr}(\omega_i\omega_j)x_j = \frac{c_i}{n} \quad (i = 1, ..., n)$$

Let $\alpha = \sum_{j=1}^{n} x_j\omega_j$. Using rules of the trace, we get for any i that

$$c_i = \sum_{j=1}^{n} \mathrm{Tr}(x_j\omega_i\omega_j) = \mathrm{Tr}(\sum_{j=1}^{n} x_j\omega_i\omega_j) = \mathrm{Tr}(\alpha\omega_i)$$

Thus, we have demonstrated that for any choice of $c_1, ..., c_n \in k$, there is a unique $\alpha \in K$ such that $\mathrm{Tr}(\alpha\omega_i) = c_i$. Now choose $c_{ij} = \delta_{ij}$, where δ_{ij} is the Kronecker delta. For every $i = 1, ..., n$ we get a unique $\omega_i^* \in K$ such that $\mathrm{Tr}(\omega_i^*\omega_j) = c_{ij}$ for $j = 1, ..., n$. We call $\omega_1^*, ..., \omega_n^*$ the dual basis of $\omega_1, ..., \omega_n$. It is indeed a basis. Assume that

$$\sum_{i=1}^{n} x_i\omega_i^* = 0.$$

Multiplying by ω_j and taking the trace, we get

$$0 = \mathrm{Tr}(\sum_{i=1}^{n} x_i\omega_i^*\omega_j) = \sum_{i=1}^{n} x_i \mathrm{Tr}(\omega_i^*\omega_j) = x_j,$$

which shows that all the x_j's are zero. Thus, the ω_i^*'s are linearly independent and as there are n of them, they form a basis.

3 Formal power series

Let K be a field. By $K[[x]]$ we denote the set of all expressions of the form $\sum_{i=0}^{\infty} a_i x^i$, where the a_i belong to K is a commutative ring with addition defined in the the obvious way and multiplication defined as

$$(\sum_{i=0}^{\infty} a_i x^i)(\sum_{i=0}^{\infty} b_i x^i) = \sum_{i=0}^{\infty}(\sum_{j=0}^{i} a_j b_{i-j})x^i$$

Thus, multiplication is really just the process of expanding out brackets and collecting all like terms. Let us see what happens to the coefficients when multiplying many elements from $K[[x]]$. For elements $f \in K[[x]]$ we introduce the notation $[x^i]f$ to denote the ith coefficient of f. Suppose that we have a sequence $f_1, f_2, ... \in K[[x]]$ with each f_i having the form

$$f_i = \sum_{j=0}^{\infty} a_{ij}x^j$$

Define $P_{k,n} = \{a_{1h_1}...a_{nh_n} | h \in \mathbb{N}_0^n, |h| = k\}$, where we by $|h|$ mean the sum of the entries of $h \in \mathbb{N}_0^n$ and let $P_k = \bigcup_{n\in\mathbb{N}_0} P_{k,n}$. Let $g_n = \prod_{i=1}^{n} f_i$. We claim that $[x_k]g_n = \sum_{c\in P_{k,n}} c$; when expanding out the brackets in the product $\prod_{i=1}^{n} f_i$ one ends up with a bunch of terms of degree k and each such term corresponds exactly to an element in $P_{k,n}$. The process of collecting all of these terms is then just the number $[x_k]g_n$. Suppose that $f(x) = \sum_{i=0}^{\infty}$ and let us now consider the simpler case where each $f_i = f$. If $a_0 \neq 0$ then P_0 contains infinitely many non-zero elements since a_0^n is non-zero for all n, as a_0 is a unit, and $a_0^n \in P_{0,n}$. If on the other hand $a_0 = 0$ then $P_{k,n} = \emptyset$ for all $n > k$. As each $P_{k,n}$ is finite it therefore follows that P_k is finite for all $k \in \mathbb{N}_0$, and so we conclude that P_k contains only finitely many non-zero elements. This shows that if $f \in (x)$ and

$g \in K[[x]]$ where $g(x) = \sum_{i=0}^{\infty} a_i x^i$ we can define

$$g(f(x)) = \sum_{i=0}^{\infty} a_i f(x)^i$$

One way to think about this is that g induces a function $g : (x) \to K[[x]]$. Composition also makes sense if g is just a polynomial. In this case we can allow $f \in K[[x]]$. Observe that we can define the following elements in $K[[x]]$

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$
$$\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n}$$

These are of course just the usual power series for the logarithm and the exponential function. Defining $F(x) = \log(1+x)$ we have two induced functions $\exp : (x) \to K[[x]]$ and $F : (x) \to K[[x]]$. It is clear that $\exp(x) - 1 \in (x)$ and that $F(\exp(x) - 1) = \log(\exp(x)) = x$. Similarly $\exp(\log(1+x)) = 1 + x$.

(TALK ABOUT HOW THESE DEFINITION RELATE TO P-ADIC DEFINTIONS) (TODO) Next, see that exp f(u) = exp f(u), where f(u) is a p adic number, exp on the left hand side is the p adic exponential and exp on the right is the formal power series exponential function

The ring $K[[x]]$ is in fact a PID and a local ring, with maximal ideal (x). One might therefore wonder if this ring is the valuation ring of some valued field. It turns out that it is.

This ring has no zero divisors, so we can consider its field of fractions, which we will denote by $K((x))$. (THIS FIELD OCCURS AS THE COMPLETION OF K[[x]]) We now have a field extension $K((x))/K$, and hence we can think about which elements are algebraic over K. We have the following theorem

Proposition 3.1. *The completion of the rational functions $K(x)$ with respect to the valuation $v_{\mathfrak{p}}$, where $\mathfrak{p} = (x)$, is isomorphic to $K((x))$.*

Proof. □

Let $\omega : K((x)) \to \mathbb{Z} \cup \{\infty\}$ be defined by

$$\omega(\sum_{i=m}^{\infty} a_i x^i) = m$$

It is clear that that $\omega(fg) = \omega(f) + \omega(g)$ for all $f, g \in K((x))$ so ω is a homomorphism.

Theorem 3.1. *K is integrally closed in $K((x))$. Equivalently, any element*

Proof. Suppose that $f \in K((x))$ and suppose there is monic polynomial $g \in K[x]$ so that $g(f(x)) = 0$ and let us show that $f \in K$. Take $g \in K[[x]]$. Then we can write

$$g(x) = \sum_{i=0}^{n} a_i x^i$$

where the a_i are in K. Suppose first that $\omega(f) > 0$. Then the sequence $(\omega(f^i))$ is strictly increasing because ω is a homomorphism. so ha $\omega(g(f(x))) =$

$g(f(x)) = 0$

Consider first the special case where $f \in K[[x]]$. Suppose also that we have a non-zero polynomial $g \in K[x]$ of degree n

$$g(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$$

It is clear that if f has finite degree then the only way for $g(f(x))$ to be 0 is if $f \in K$. So suppose that f has infinite degree. Note that

$$g(f(x)) = \sum_{i=0}^{n} c_i f(x)^i$$

We want to show that if $g(f(x)) = 0$ then all the c_i are 0. In other words, $g(x) = 0$. Hence, if we can show that the powers $1, f, ..., f^n$ are linearly independent over K, we are done with this special case. So assume that

$$c_0 + ... + c_n f(x)^n = 0$$

Evaluating at $x = 0$ shows that $c_0 = 0$. Suppose $a_i x^i$ is the term of f with lowest degree, the existence of which is due to the fact that f has infinite degree. Differentiating f exactly i times gives us a polynomial $f^{(i)}$ with non-zero constant term - in other words, $f^{(i)}$ is a unit. Differentiating our original equation i times gives us

$$c_1 f^{(i)}(x) + ... + c_n (f(x)^{n-1})^{(i)} = 0$$

Multiplying this equation by $\frac{1}{f^{(i)}(x)}$ leaves us in a situation similar to the one we started with. Now we can evaluate in $x = 0$ and we get that $c_1 = 0$. Repeating this argument we get that all the c_i are 0. Now if $f \in K((x))$ we can write □

4 Forms and Modules

A form $F(x_1, ..., x_m)$ in m variables of degree k is a homogenous polynomial of degree k with coefficients in $\mathbb{Q}$. If it splits into linear factors in some extension, K, of $\mathbb{Q}$, then it is called decomposable and in this case K can in fact be chosen to be a number field [See Thm 1 p 79 Borevich]. The following proposition provides some examples of forms that are decomposable.

Proposition 4.1. *Any form, $F(x,y)$, in two variables is decomposable.*

Proof. Assume that F has degree m and notice that we can write $F(x,y) = y^m F(\frac{x}{y},1) = y^m G(\frac{x}{y})$ where G is in $\mathbb{Q}[t]$ having degree $r \leq m$. As G is just a polynomial we can factor it into linear terms over its splitting field, K,

$$G(t) = \prod_{i=1}^{r}(a_i t + b_i)$$

Now,

$$F(x,y) = y^m G(\frac{x}{y}) = y^m \prod_{i=1}^{r}(a_i \frac{x}{y} + b_i) = y^{m-r} \prod_{i=1}^{r}(a_i x + b_i y)$$

Thus, $F(x,y)$ is decomposable as it splits into linear factors over K.

□

We shall use this fact once we start looking at Thue's theorem.

A form F is called reducible if it can be written as a product of two forms of degree strictly larger than 0. Otherwise it is called irreducible. Two forms are called equivalent if one can be obtained from the other by a linear change of variables with coefficients in $\mathbb{Z}$. As an example,

$$u^2 + 3v^2 \text{ and } 7x^2 - 2xy + 4y^2$$

are equivalent since the second form can be obtained from the first by setting $u = 2x + y$ and $v = x - y$. Two forms being equivalent clearly defines an equivalence relation on the set of forms. Observe that if (x_0, y_0) is a solution to the second form above then (u_0, v_0), with $u_0 = 2x_0 + y_0$ and $v_0 = x_0 - y_0$, is a solution to the first form above. In general, if we have a solution to an equation like (**??**), then we immediately have a solution to all forms equivalent to F. Let us assume that K is a number field of degree n over $\mathbb{Q}$ and let $\mu_1, ..., \mu_k$ be elements in K. The set, M, consisting of all $\mathbb{Z}$-linear combinations of these is called a module in K and we will write $M = \{\mu_1, ..., \mu_k\}$ for this set. The μ_i's are called generators for the module and we can use them to construct a form; As K is in particular a finite separable extension of $\mathbb{Q}$, the primitive element theorem states that there is $\theta \in K$ so that $K = \mathbb{Q}(\theta)$. Let f be the minimal polynomial for θ over $\mathbb{Q}$. Adjoining all the roots of f to $\mathbb{Q}$, we get a field, N, which has finite degree, n, over $\mathbb{Q}$ and which is splitting field for the irreducible polynomial f. Hence N is a number field and is Galois over $\mathbb{Q}$. Let $G = \text{Gal}(N/\mathbb{Q})$ and $H = \text{Gal}(N/K)$. Now $n = [K : \mathbb{Q}] = [G : H]$ so we can find $\sigma_1, ..., \sigma_n$ so that $G = \cup_{i=1}^{n} \sigma_i H$ is a disjoint union. For $x_1, ..., x_k \in \mathbb{Z}$ we now set $F(x_1, ..., x_k) = N_{K/\mathbb{Q}}(x_1\mu_1 + ... + x_k\mu_k)$ and we observe that

$$\begin{aligned} F(x_1, ..., x_k) &= \prod_{i=1}^{n} \sigma_i(x_1\mu_1 + ... + x_k\mu_k) \\ &= \prod_{i=1}^{n} \left(x_1\sigma_i(\mu_1) + ... + x_k\sigma_i(\mu_k)\right) \end{aligned}$$

When expanding out the parentheses we see that F is a homogenous polynomial of degree n in the variables $x_1, ..., x_k$. Since the norm, $N_{K/\mathbb{Q}}$, sends elements in K to $\mathbb{Q}$ we know that $F(x_1, ..., x_n)$ is fixed by every single $\sigma \in G$ for all $x_1, ..., x_n \in \mathbb{Z}$. This implies that all the coefficients of F are fixed by every $\sigma \in G$, so they all belong to $\mathbb{Q}$. Therefore F is a form of degree n. A form like this is called a norm form and is said to be connected to the module M. Such forms are decomposable as they clearly factor into linear factors over N. In fact, all forms connected to M are equivalent. For if $\rho_1, ..., \rho_l$ is another set of generators for M, we get the norm form

$$G(y_1, ..., y_s) = N_{K/\mathbb{Q}}(y_1\rho_1 + ... + y_s\rho_l).$$

For every $j = 1, ..., l$ we can find integers $c_{j1}, ..., c_{jk}$ so that $\rho_j = \sum_{k=1}^{m} c_{jk}\mu_k$ since $\rho_j \in M$ and the μ_i generate M. We then have

$$\sum_{j=1}^{l} y_j\rho_j = \sum_{j=1}^{l} y_j \sum_{k=1}^{m} c_{jk}\mu_k = \sum_{k=1}^{m}(\sum_{j=1}^{l} c_{jk}y_j)\mu_k = \sum_{k=1}^{m} x_k\mu_k,$$

where $x_k = \sum_{j=1}^{l} c_{jk}y_j$ for $k = 1, ..., m$. Taking norms on both sides of the above equation, we see that the form F can be obtained from G by a linear change of variables with integer coefficients. In other words F and G are equivalent and we conclude that all forms connected to M are equivalent. If M contains a basis for the vector space $K/\mathbb{Q}$, then it is called a **full module**. Otherwise it is called a **nonfull module**. A form which is connected to a module is correspondingly called full or nonfull. By definition M is a finitely generated abelian group and by the structure theorem, M determines uniquely integers $r, s \geq 0$ and $d_1 \mid ... \mid d_s$, $d_i \geq 2$ such that

$$M \cong \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_s\mathbb{Z}$$

But M lives inside a field, which has no zero divisors, so M must be a torsion-free $\mathbb{Z}$-module, and so $s = 0$. Thus, $M \cong \mathbb{Z}^r$, which means that M is a free abelian group of rank r. The modules in K can therefore be thought of as finitely generated free abelian groups, which means that concepts such as rank and basis now make sense for modules. The full modules inside K are exactly the modules having rank n and the nonfull ones have rank strictly smaller than that.

5 Coefficient rings and orders

In the following we assume that K is an algebraic number field of degree n over $\mathbb{Q}$. An **order** in K is a full module in K which is also a ring with unity. We will now give a way of constructing such a ring. Given a full module M in K, we can consider an element α in K so that $\alpha M \subseteq M$. Such an element is called a **coefficient** of M, and the set of all of these is called the **coefficient ring** of M, which we will denote by $\mathfrak{O}_M$, or simply $\mathfrak{O}$, when it is clear from the context what is meant. It would be strange to call this object a ring, if it wasn't a ring, so let us check that it is. It is clear that $1 \in \mathfrak{D}$ since $1M \subseteq M$ and so $\mathfrak{D}$ is non-empty. Let now α, β in $\mathfrak{D}$ and take any element in x in M. We have $\alpha x, \beta x \in M$ so

$$(\alpha - \beta)x = \alpha x - \beta x \in M$$

Thus, $\alpha - \beta \in \mathfrak{D}$. Checking that we have closure under multiplication is similar and so by the subring criterion $\mathfrak{D}$ is a subring of K. In fact, $\mathfrak{D}$ is also a full module. To justify this, we must show that $\mathfrak{D}$ is a module and that it contains a basis for K as a vector space over $\mathbb{Q}$. If γ is any non-zero element of M, then $\gamma\mathfrak{D}$ is a group under addition and we have that $\gamma\mathfrak{D} \subseteq M$. Thus, $\gamma\mathfrak{D}$ is a free abelian group, since it is contained in the free abelian group M which means that it is a module in K. But then also $\mathfrak{D} = \gamma^{-1}\gamma\mathfrak{D}$ is a module. Let us show that $\mathfrak{D}$ is also full. Since M is full we can find inside it a basis, $\mu_1, ..., \mu_n \in M$, for K as a vector space over $\mathbb{Q}$ which is also a basis for M. (MAYBE JUSTIFY THIS) We need the following lemma

Lemma 5.1. *For any $\alpha \in K$ we have that $\alpha\mu_i$ is in M for all the μ_i if and only if α is in $\mathfrak{D}$.*

Proof. Take any $x \in M$ and write $x = \sum_{i=1}^{n} a_i\mu_i$ where the a_i are integers. Multiplying by α we get

$$\alpha x = \sum_{i=1}^{n} a_i(\alpha\mu_i)$$

So if the $\alpha\mu_i$ are all in M, this is just a finite sum of elements in M, meaning that the entire sum is in M. Hence, $\alpha M \subseteq M$. The other direction is clear. □

From this lemma it follows that if $\alpha \in K$ there exists an integer $c \neq 0$ so that $c\alpha \in \mathfrak{D}$. This is because we each μ_i can find a $\mathbb{Q}$-linear combination

$$\alpha\mu_i = \sum_{j=1}^{n} a_{ij}\mu_j,$$

since the μ_i constitute a basis for K over $\mathbb{Q}$. Choose now an integer, $c \neq 0$ so that ca_{ij} is an integer for all i, j. This implies that $c\alpha\mu_i$ is in M for all the μ_i which by (5.1) means that $c\alpha$ is in $\mathfrak{D}$. From this it is clear that we can pick an integer $b \neq 0$ so that we for all μ_i have that $c\mu_i$ is in $\mathfrak{D}$. The elements $c\mu_1, ..., c\mu_n$ is of course still is a basis for K over $\mathbb{Q}$ so $\mathfrak{D}$ is full. Hence $\mathfrak{D}$ is an order in K. In fact $\mathfrak{D}$ is contained in O_K, the ring of integers of K. Because if $\alpha \in \mathfrak{D}$ then we have $\mathbb{Z}[\alpha] \subseteq \mathfrak{D}$ so $\mathbb{Z}[\alpha]$ has rank smaller than or equal to n. Hence $\mathbb{Z}[\alpha]$ is in particular finitely generated and that is the same as saying that $\alpha \in O_K$. Let us summarize what we have found in the following proposition

Proposition 5.1. *The coefficient ring $\mathfrak{D}$ is an order of K and is a subring of the ring of integers of K.*

6 Only finitely many solutions up to associates

Theorem 6.1 (Dirichlet's unit theorem)**.** *Let $\mathfrak{O}$ be an order in some number field K of degree n and let r and $2s$ be the number of real and complex embeddings into $\mathbb{C}$, respectively. Then*

$$\mathfrak{O}^* = W \oplus V$$

where W is a finite cyclic group consisting of all roots of unity of $\mathfrak{O}$ and V is a free abelian group of rank $t = r + s - 1$.

Proof. Let O be the ring of algebraic integers in K. For the order O we know that the above theorem holds, so we get

$$O^* = W \oplus V$$

with W and V as above. Since $\mathfrak{O}$ is a subring of O we also have $\mathfrak{O}^* \subseteq O^*$. Hence,

$$\mathfrak{O}^* = W' \oplus V'$$

where $W' \trianglelefteq W$ is finite cyclic and $V' \trianglelefteq V$ is free abelian of rank $t' \leq t$. We wish to show two things; That W' does indeed consist of all roots of unity of $\mathfrak{O}$ and that $t' = t$. For the first claim, if we have any root of unity $\xi \in \mathfrak{O}$, then ξ has finite order so it cannot possibly belong to V'. Thus the only possibility is that ξ is in W'. For the second claim, consider the quotient of groups $O/\mathfrak{O}$. Both of these have rank n, so this quotient is finite, and so we know that $f := [O : \mathfrak{O}] < \infty$. Thus, if $x \in O$ then $\overline{fx} = 0$ in $O/\mathfrak{O}$ so $fx \in \mathfrak{O}$, so $fO \subseteq \mathfrak{O}$. Of course fO is also a free abelian group of rank n, so again $R = O/fO$ is finite. But fO is also an ideal of the ring O, so in fact R is a finite ring. Consider now any unit $\epsilon \in V$. Then ϵ is in O^*, so $\overline{\epsilon} \in R$ is also a unit, since ring maps preserve units. Set now $k = \#R^*$. Then $\overline{\epsilon^k} = \overline{1}$ and $\overline{\epsilon^{-k}} = \overline{(\epsilon^{-1})^k} = \overline{1}$. Together, these equalities give us

$$\epsilon^k = 1 + f\alpha$$
$$\epsilon^{-k} = 1 + f\beta$$

where $\alpha, \beta \in O$. But as we argued above, $f\alpha$ and $f\beta$ both belong to $\mathfrak{O}$ and so both ϵ^k and ϵ^{-k} belong to $\mathfrak{O}$ which means that $\epsilon^k \in \mathfrak{O}^*$. Thus, ϵ^k is either in W' or V' and the first option is impossible as that would imply that ϵ^k would be in W. Thus, ϵ^k is in V' so V/V' is finite meaning that $t' = t$. □

In particular the above proposition says that there are units $\epsilon_1, ..., \epsilon_t$ such that every element in V has a unique representation of the form $\epsilon_1^{u_1}...\epsilon_t^{u_t}$, where all the u_i belong to $\mathbb{Z}$. These units are called a fundamental system for $\mathfrak{O}$.

We say that two elements, α, β in a a full module M are **associated** if there is a unit $\epsilon \in \mathfrak{O}$ so that $\alpha = \epsilon\beta$. Note that when M is equal to its own coefficient ring, this concept is exactly the same as that of being associated in rings. Being associated elements in M defines an equivalence relation on M, and from now on we will denote this relation as $\sim$. Define now for some $c \in \mathbb{N}$ the subsets

$$M_c = \{\alpha \in M \mid N(\alpha) = c\}$$
$$\overline{M}_c = \{\alpha \in M \mid |N(\alpha)| = c\}$$

We are now ready to formulate the following theorem.

Theorem 6.2. *Let M be a full module of K. Then the quotient set $\overline{M}_c/\sim$ is finite for any $c \in \mathbb{N}$. In particular $M_c/\sim$ is finite.*

Proof. We first consider the special case where $M = \mathfrak{O}$. The ring $\mathfrak{O}$ is a full module so it is a free abelian group of rank n, hence isomorphic to $\mathbb{Z}^n$. Considering $\mathfrak{O}$ as an abelian group with respect to addition we get the isomorphisms

$$\mathfrak{O}/c\mathfrak{O} \cong \mathbb{Z}^n/c\mathbb{Z}^n \cong (\mathbb{Z}/c\mathbb{Z})^n$$

Now, $\mathbb{Z}/c\mathbb{Z}$ contains c elements, which means that

$$c^n = \#(\mathbb{Z}/c\mathbb{Z})^n = \#\mathfrak{O}/c\mathfrak{O}$$

Denote by $\bar{\alpha}$ as the image of the canonical projection of α in $\mathfrak{O}/c\mathfrak{O}$ and denote by $[\alpha]$ an equivalence class in $\overline{M}_c/\sim$, represented by $\alpha \in \overline{M}_c$. We show that there is a well-defined surjective function of sets

$$\phi : \overline{M}_c/c\mathfrak{O} \twoheadrightarrow \overline{M}_c/\sim,$$

given by $\phi(\bar{\alpha}) = [\alpha]$. Suppose $\bar{\alpha}, \bar{\beta}$ are in $\overline{M}_c/c\mathfrak{O}$ so that $\bar{\alpha} = \bar{\beta}$, where α, β are in $\overline{M}_c$, so $|N_{K/\mathbb{Q}}(\alpha)| = |N_{K/\mathbb{Q}}(\beta)| = c$. Let us show that $[\alpha] = [\beta]$ - in other words we show that α and β are associates. Since $M = \mathfrak{O}$ by assumption, we know that $\alpha, \beta \in \mathfrak{O}$ so $\overline{\alpha} = \overline{\beta}$ implies that

$$\alpha = \beta + c\gamma = \beta + |N_{K/\mathbb{Q}}(\beta)|\gamma,$$

for some γ in $\mathfrak{O}$. We claim that β divides $N_{K/\mathbb{Q}}(\beta)$ in $\mathfrak{O}$ - the reason for this is as follows. We know that β is an algebraic integer since it belongs to $\mathfrak{O}$, so its minimal polynomial $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_0$ has integer coefficients. Now $a_0 = -(\beta^m + a_{m-1}\beta^{m-1} + ... + a_1\beta)$ so $\beta \mid a_0$ in $\mathfrak{O}$ and therefore β also divides a_0^m, where $m = [K : \mathbb{Q}(\alpha)]$. By (8.2) we have $N_{K/\mathbb{Q}}(\beta) = \pm a_0^m$ and the claim follows. We therefore also know that β divides $|N_{K/\mathbb{Q}}(\beta)|$ in $\mathfrak{O}$. Hence, β divides α in $\mathfrak{O}$ and similarly α divides β in $\mathfrak{O}$. Thus, α and β are associates, showing that ϕ is well-defined. It is surjective simply because if $[\alpha] \in \overline{M}_c/\sim$, then α is in $\overline{M}_c$ so $\phi(\bar{\alpha}) = [\alpha]$. That ϕ is a surjection implies that $\#(\overline{M}_c/\sim) \leq \#\overline{M}_c/c\mathfrak{O}$, since each element in $\overline{M}_c/\sim$ has at least one preimage. Now the inclusion $\overline{M}_c/c\mathfrak{O} \subseteq \mathfrak{O}/c\mathfrak{O}$ implies that $\#(\overline{M}_c/\sim) \leq \#\overline{M}_c/c\mathfrak{O} \leq \#\mathfrak{O}/c\mathfrak{O} = c^n$. We will now prove the general statement. Suppose that M is a full module and that $\mathfrak{O}$ is the coefficient ring of M. Then $\overline{\mathfrak{O}}_c/\sim$ has finitely many elements. Take now a non-zero integer b so that $bM \subseteq \mathfrak{O}$. We then obtain injective maps

$$M \hookrightarrow bM \hookrightarrow \mathfrak{O},$$

where the first map is multiplication by b and the second one is inclusion. It is clear that if α and β are associated then also $b\alpha$ and $b\beta$ are associated. Hence we get the induced injective maps

$$(\overline{M}_c/\sim) \hookrightarrow (b\overline{M}_c/\sim) \hookrightarrow (\overline{\mathfrak{D}_c}/\sim)$$

Which means that

$$\#(\overline{M}_c/\sim) \leq \#(b\overline{M}_c/\sim) \leq \#(\overline{\mathfrak{D}_c}/\sim) \leq c^n$$

The last claim now follows since $M_c \subseteq \overline{M}_c$.

□

We now present a result that allows to find all the elements of M_c if we know the elements of $M_c/\sim$ and all the units with norm 1 in $\mathfrak{D}$.

Lemma 6.1. *Assume that the elements of $M_c/\sim$ are $[\gamma_1], ..., [\gamma_k]$ and that $\alpha \in M$. We then have that $\alpha \in M_c$ if and only if there is a uniquely determined i such that $\alpha = \epsilon\gamma_i$ where ϵ is a unit in $\mathfrak{D}$ with norm 1.*

Proof. If $\alpha \in M_c$ then, there is a unique γ_i such that $\alpha \in [\gamma_i]$. This means that $\alpha = \epsilon\gamma_i$ for some unit ϵ in $\mathfrak{D}$. But then

$$c = N(\alpha) = N(\epsilon\gamma_i) = N(\epsilon)N(\gamma_i) = N(\epsilon)c$$

So we must have that $N(\epsilon) = 1$. □

Note that an element $\epsilon \in \mathfrak{D}$ is a unit if and only if $N_{K/\mathbb{Q}}(\epsilon) = \pm 1$ simply because ϵ is an algebraic integer. In light of the above proposition we are now interested in figuring out when ϵ has norm 1. This is what the next theorem is about.

Lemma 6.2. *Let K be a number field of degree n over $\mathbb{Q}$. Suppose n is odd. Then the only roots of unity in O_K are ± 1 and we have $N(1) = 1$ and $N(-1) = -1$. On the other hand, if n is even, then all the roots of unity in O_K have norm 1.*

Proof. Let ζ be a primitive kth root of unity in O_K. To start with, let us suppose that n is odd. Then

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq K$$

Denote by φ Euler's totient function. We have $\varphi(k) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$, we have $\varphi(k) \mid n$. Thus, $\varphi(k)$ has to be odd. But this happens only when k is 1 or 2 so $\zeta = \pm 1$. We see that $N(-1) = (-1)^n = -1$ and the fact that $N(1) = 1$ is always true. Next, assume that n is even. We then clearly have $1 = N(1) = N(-1)$. Then any embedding $\sigma : K \hookrightarrow \mathbb{C}$ must send ζ to a primitive kth root of unity in $\mathbb{C}$. Suppose that $k \geq 3$. In this case $\sigma(\zeta)$ is an imaginary number and therefore

σ must be a complex embedding. Since σ is arbitrary we have $n = 2s$, where s is the number of pairs of complex conjugate embeddings. Thus,

$$N(\zeta) = \prod_{i=1}^{s} \sigma_i(\zeta)\overline{\sigma_i}(\zeta) = \prod_{i=1}^{s} |\sigma_i(\zeta)|^2 = 1$$

□

Theorem 6.3. *Let K be a number field of degree $n = 2s + r$ over the rationals and let $c \in \mathbb{Z}$. Assume further that M is a full module with ring of coefficients $\mathfrak{D}$ and set $t = r+s-1$. Then there exists a fundamental system of units $\epsilon_1, ..., \epsilon_t$ for $\mathfrak{D}$, and a finite number of elements $\gamma_1, ..., \gamma_k$ in M_c such that every $\alpha \in M_c$ can be written uniquely as*

$$\alpha = \gamma_i \epsilon_1^{u_1} ... \epsilon_t^{u_t}$$

for some γ_i and where $u_1, ..., u_t \in \mathbb{Z}$.

Proof. By Dirichlet's unit theorem, we know that we can find a fundamental system of units, $\epsilon_1, ..., \epsilon_t$, where $t = r + s - 1$ such that every element $\epsilon \in \mathfrak{D}^*$ can be written uniquely as

$$\epsilon = \zeta \epsilon_1^{u_1} ... \epsilon_t^{u_t}$$

where the u_i are integers and $\zeta \in \mathfrak{D}$ is a root of unity. Let us find the subgroup of $\mathfrak{D}^*$ containing only elements of norm 1. Suppose first that n is odd. Then we know from (6.2) that there are only two roots of unity, namely 1 and -1 and that $N(-1) = -1$. If need be, let us swap out all ϵ_i that have norm -1 with $-\epsilon_i$. This leaves us with a new system of fundamental units and they generate the subgroup of $\mathfrak{D}$ having norm 1. Suppose now n is even. Then by (6.2) all the roots of unity have norm 1, so if it happens that all the ϵ_i have norm 1, then all units of $\mathfrak{D}$ will have norm 1. So suppose that not all the ϵ_i have norm 1. We can without loss of generality assume that $1 = N(\epsilon_1) = ... = N(\epsilon_q)$ and $-1 = N(\epsilon_{q+1}) = ... = N(\epsilon_t)$, where $q < t$. Define $\mu_i = \epsilon_i$ for $i \in \{1, ..., q\}$ and $\mu_i = \epsilon_i \epsilon_t$ for $i \in \{q + 1, ..., t - 1\}$. We now have a new fundamental system of units, namely $\mu_1, ..., \mu_{t-1}, \epsilon_t$ and only the last unit, ϵ_t, has norm -1. By setting $\mu_t = \epsilon_t^2$, all units of norm 1 in $\mathfrak{D}$ can now be written as $\zeta \mu_1^{u_1} ... \mu_t^{u_t}$, where ζ is a root of unity in $\mathfrak{D}$.

Let now $[\gamma_1'], ..., [\gamma_l']$ be all the elements of $M_c/\sim$ and let $\alpha \in M_c$. By (6.1), there is a unique γ_i' and a unit $\epsilon \in \mathfrak{D}$ of norm 1 so that $\alpha = \gamma_i' \epsilon$. For odd n the statement in the proposition now follows once we set $\gamma_i = \gamma_i'$ and $k = l$. When n is even, we can consider all products $\zeta \gamma_i'$, where $\zeta \in \mathfrak{D}$ is a root of unity. There are only finitely many of these products, and we can denote them by $\gamma_1, ..., \gamma_k$. All of these belong to M_c since the roots of unity have norm 1 and the statement now follows for when n is even. □

Corollary 6.1. *There exists an independent system of units, $\epsilon_1, ..., \epsilon_t$ and a finite number of elements, $\gamma_1, ..., \gamma_k$ so that*

$$M_c = \{\gamma \epsilon_1^{u_1} ... \epsilon_t^{u_t}\}$$

so that

Consider for example the field $\mathbb{Q}(i)$. This field has degree 2 over $\mathbb{Q}$ and both embeddings into $\mathbb{C}$ are complex. Hence $r = 0$ so $t = 0$ so there are only finitely many elements in M_c. This holds in general for every imaginary quadratic field.

7 Fields with an absolute value

Definition 7.1 (Absolute value)**.** *Let K be a field. A function $|\cdot| : K \to \mathbb{R}$, is called an absolute value if it happens to satisfy the properties*

- $|x| \geq 0$ *for every $x \in K$. (Non-negativity)*
- $|x| = 0$ *if and only if $x = 0$. (Positive definiteness)*
- $|xy| = |x||y|$ *for every $x, y \in K$. (Multiplicativity)*
- $|x + y| \leq |x| + |y|$ *for every $x, y \in K$. (Triangle inequality)*

When the triangle inequality can be upgraded to the stronger condition

$$|x + y| \leq \max\{|x|, |y|\} \quad \textit{for every } x, y \in K,$$

the absolute value is said to be ***non-archimedean****. Otherwise it is called* ***archimedean****. If $|\cdot|$ is indeed an absolute value then the field K is called a valued field. A field with a non-archimedean absolute value is called a non-archimedean valued field and similarly a field with an archimedean absolute value is called an archimedean valued field.*

FIELD OF FRACTIONS We could easily have made this definition more general by allowing K to be any ring. In that case, absolute values would only exists on domains. For if we had x, y both non-zero so that $xy = 0$ then $|x|, |y|$ would also be non-zero but $0 = |0| = |xy|$. But $|x||y| \neq 0$, so $|\cdot|$ cannot be an absolute value. The usual absolute value on $\mathbb{R}$, which we will denote by $|\cdot|_\infty$, is an example of an archimedean absolute value, so $(\mathbb{R}, |\cdot|)$ is an example of a valued field. The function sending everything to 1 except for 0 which is sent to 0 is also an example of an absolute value, and it is called the trivial absolute value. Note that for an arbitrary absolute value we have for all $x \in K$ that

- If $x^n = 1$ then $|x| = 1$.
- $|x| = |-x|$

In particular, $1 = |1| = |-1|$ and if K is a finite field then $|\cdot|$ is the trivial absolute value, since every non-zero element in such a field has finite order.

Once we have an absolute value on field K, we can use it to define a metric, $d : K^2 \to \mathbb{R}$, by setting $d(x, y) = |x - y|$. As such, K can now be thought of as a metric space, and we therefore now have a topology on K, generated by d. We will also refer to this topology as the topology induced by $|\cdot|$. It might very well happen that two absolute values, $|\cdot|_1$ and $|\cdot|_2$, induce the same topology on K. In fact, all of these are equivalent

- $|\cdot|_1$ and $|\cdot|_2$ are equivalent
- $|x|_1 = |x|_2^s$ for all $x \in K$ for some $s > 0$
- $|x|_1 < 1 \iff |x|_2 < 1$
- If (x_n) is a sequence in K then $x_n \to a$ with respect to $|\cdot|_1$ if and only if $x_n \to a$ with respect to $|\cdot|_2$.

, which is again the same as saying that

$$|x|_1 < 1 \iff |x|_2 < 1$$

If one of these equivalent conditions are satisfied we say that the absolute values are equivalent. This defines an equivalence relation on the set of absolute values on K, and the equivalence classes are called places of K. The non-archimedian absolute values induce a topology that is quite different compared to what one perhaps might expect. For example, triangles are isosceles - that is to say, any triangle will always have two sides of the same length. (SAY THAT WE ARE WORKING WITH NON ARCHIMEDIAN FIELDS)

Proposition 7.1. *Suppose $x, y \in K$ and that $|x| \neq |y|$. Then $|x + y| = \max\{|x|, |y|\}$. In particular, all triangles are isosceles.*

Proof. Assume without loss of generality that $|x| > |y|$. Then we have

$$|x + y| \leq |x| = \max\{|x|, |y|\}$$

Also, $|x| = |(x + y) - y| \leq \max\{|x + y|, |y|\} = |x + y|$, since $|x| > |y|$. Thus, $|x| = |x+y|$. For the last claim suppose that $z \in K$ and consider the three sides $A = x - y$, $B = y - z$ and $C = x - z$ and suppose that two of these sides, say A and B have different length, that is, $|A| \neq |B|$. We clearly have that $A + B = C$ and so by what we have just shown we have that

$$|C| = |A + B| = \max\{|A|, |B|\}$$

But that means that C has the same length as A or B and we conclude that two sides in the triangle must have the same length. □

We also have the following lemma which does not hold for archimedian absolute values

Lemma 7.1. *Let $|\cdot|$ be a non-achimedian absolute value on a field K. Suppose (x_n) is a sequence in K. Define the sequence $y_n = x_{n+1} - x_n$. The following are equivalent*

1. *x_n is Cauchy.*
2. *$y_n \to 0$ for $n \to \infty$.*

Proof. A sequence being Cauchy clearly implies that y_n converges to 0. On the other hand let $N \in \mathbb{N}$ be so large that $|y_n| < \epsilon$ for all $n \geq N$. Suppose now $n > m > N$. We obtain

$$\begin{aligned}|x_n - x_m| &= |x_n - x_{n-1} + x_{n-1} - ... + x_{m+1} - x_m| \\ &= |y_n + y_{n-1} + ... + y_m| \leq \max\{|y_n|, ..., |y_m|\} < \epsilon\end{aligned}$$

□

This lemma can be really helpful in situations where the sequence (x_n) has the form $x_n = \sum_{i=1}^{n} z_n$, since in this case we can determine if (x_n) is cauchy simply by checking if z_n converges to 0. This is certainly not something we can do in the archimedian setting though. For example if $z_n = \frac{1}{n}$ then x_n is the harmonic series and we know that it diverges with respect to $|\cdot|_\infty$. However, z_n certainly converges to 0.

Proposition 7.2. *An absolute value $|\cdot|$ on a field K is uniformly continuous.*

Proof. Let $\epsilon > 0$ and pick $\delta = \epsilon$. For any $x, y \in K$ so that $|x - y| < \delta$ we have

$$||x| - |y||_\infty \leq |x - y| < \delta = \epsilon$$

where we have used the reverse triangle inequality. □

Uniformly continuous functions have the nice property that they preserve Cauchy sequences. This implies that if we have some Cauchy sequence, (x_n) in K, then $(|x_n|)$ is a Cauchy sequence in $\mathbb{R}$. We will use this fact later on.

Definition 7.2. *Let K, L be valued fields and suppose that $\phi : K \to L$ is a function. We say that ϕ preserves the absolute value if $|\phi(x)|_L = |x|_K$.*

It is worth pointing out that if ϕ is as above and is also a homomorphism, then ϕ is actually uniformly continuous. This is simply because we have for all $x, y \in K$ that

$$|\phi(x) - \phi(y)|_F = |\phi(x - y)|_F = |x - y|_K$$

We now turn to a notion that is closely related to non-archimedian absolute values - namely valuations.

Definition 7.3 (Valuation)**.** *A valuation on a field K is a function $v : K \to \mathbb{R} \cup \{\infty\}$ with the following properties*

1. *$v(x) = \infty$ if and only if $x = 0$.*
2. *$v(xy) = v(x) + v(y)$ for every $x, y \in K$.*
3. *$v(x + y) \geq \min\{v(x), v(y)\}$ for every $x, y \in K$.*

The symbol ∞ is just an element so that for all $x \in \mathbb{R}$ we have $\infty > x$, $\infty + x = x + \infty = \infty$ and $\infty + \infty = \infty$.

We stipulated above that valuations and absolute values have something to do with each other. Let us see why. Suppose we have access to a valuation, v on a field K. Then for any $q > 1$ we get what we will call a corresponding absolute value on K by setting $|x| = q^{-v(x)}$. This absolute value is in fact non-archimedean because of the third property in the definition above and all absolute values corresponding to v are equivalent. In other words, they all correspond to the same place. Because if we take $p, q > 1$ and suppose that $p > q$ then we get two absolute values $|x|_1 = p^{-v(x)}$ and $|x|_2 = q^{-v(x)}$. Setting $s = \log \frac{p}{q}$ we have $s > 0$ and we obtain $p = q^s$ and so

$$|x|_1 = |x|_2^s$$

We will say that two valuations v_1 and v_2 are equivalent if $v_1 = sv_2$ for some $s > 0$. In this case any absolute value corresponding to v_1 will be equivalent to any absolute value corresponding to v_2. Because if we have an arbitrary absolute value corresponding to v_1, that is to say, if we have $|x| = q^{-v_1(x)}$ for some $q > 1$ then we can write

$$|x| = q^{-v_1(x)} = q^{-sv_2(x)} = (q^s)^{-v_2(x)}$$

and as $q^s > 1$ it follows from the argument above that any absolute value corresponding to v_2 has to be equivalent to $|x|$. On the other hand, if we start with a non-archimedean absolute value, $|\cdot|$, on a field K then we can obtain a valuation v by fixing some $q > 1$ and setting $v(x) = -\frac{\log |x|}{\log q}$ for $x \in K^*$ and $v(0) = \infty$. We will call v a valuation corresponding to $|\cdot|$ and we see that there is a bijective correspondence between non-archimedean absolute values and valuations. As such, fields with non-archimedean absolute value and fields with a valuation are really the same objects and we can therefore freely choose to work with valuations or absolute values as we see fit. When working with valuations it is useful to have the following in mind. Assume that K is a valued field with non-archimedean absolute value $|\cdot|$ and v is a corresponding valuation. If $a \in K$ and (x_n) is a sequence in K, then x_n converges to a if and only if $v(x_n - a) \to \infty$. Let us now present different objects attached to a valuation. Some of these don't change when the valuation is swapped out with another equivalent one. The object we define now, the so-called value group, does not have this property though.

Definition 7.4. *Let v be a valuation on a field K. The group $\Gamma_v = v(K^*)$ is called the value group of v and if there is $s > 0$ so that $\Gamma_v = s\mathbb{Z}$ we say that v is discrete. If $s = 1$ then v is called normalized and in this case an element $\pi \in K$ so that $v(\pi) = 1$ is called a prime element.*

Definition 7.5 (Valuation ring)**.** *Let O be an integral domain with field of fractions K. If for all $x \in K$ we have that $x \in O$ or $x^{-1} \in O$ then O is called a valuation ring.*

A valuation ring O is a local ring and it has maximal ideal $\mathfrak{p} = \{x \in K \mid x^{-1} \notin O\}$ since the set $O \setminus \mathfrak{p}$ consists of all units of O. Hence $O/\mathfrak{p}$ is a field and it is called the residue field of O. Also, O is integrally closed; Suppose that $x \in K$ is integral over O. That is we have $x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$ where the a_i all belong to O. Assume now for contradiction that $x \notin O$. That means that $x^{-1} \in O$ and so we can solve for x in the equation above, meaning that $x \in O$, which is a contradiction. A valuation on a field can be used to construct a valuation ring.

Proposition 7.3. *Let K be a non-archimedian valued field with valuation v and a valuation corresponding to $|\cdot|$. Then*

$$O := \{x \in K \mid v(x) \geq 0\}$$

is a valuation ring and is called the valuation ring of K with respect to v. It has field of fractions K and it has unique maximal ideal

$$\mathfrak{p} = \{x \in K \mid v(x) > 0\}$$

Its units are

$$O^* = \{x \in K \mid v(x) = 0\}$$

If v is discrete, then the valuation ring is a PID. If v is normalized and $\pi \in O$ is a prime element then we have

- $K^* = \{\pi^k \mid k \in \mathbb{Z}\} \times O^*$
- $(\pi) = \mathfrak{p}$
- *The non-zero ideals of O are given by $\mathfrak{p}^n = \{x \in K : v(x) \geq n\}$ for $n \geq 0$*
- $O/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}$ *for $n \geq 0$*

Proof. Suppose that v is discrete and normalized. Let now $x \in K^*$. Then $v(x) = m \in \mathbb{Z}$, since $v(K^*) = \mathbb{Z}$ by assumption, and so $v(x\pi^{-m}) = v(x) - mv(\pi) = 0$ meaning that $x\pi^{-1} \in O^*$. Thus $x\pi^{-1} = u$ for some $u \in O^*$ which means that $K^* = (\pi) \times O^*$.

□

There is in fact another way of constructing the valuation ring. Suppose K is complete with respect to a discrete valuation. For each n we have the natural projection

$$O \xrightarrow{\pi_n} O/\mathfrak{p}^n.$$

We have the inclusions $\mathfrak{p} \supset \mathfrak{p}^2 \supset ...$, which implies that every element in $\mathfrak{p}^{n+1}$ is sent to zero under this map, giving us a commutative diagram

$$\begin{tikzcd} & O \arrow[dl, "\pi_n"'] \arrow[dr, "\pi_{n+1}"] & \\ O/\mathfrak{p}^n & & O/\mathfrak{p}^{n+1} \arrow[ll, "\lambda_n"'] \end{tikzcd}$$

Thus, we get a sequence of maps

$$O/\mathfrak{p} \xleftarrow{\lambda_1} O/\mathfrak{p}^2 \xleftarrow{\lambda_2} O/\mathfrak{p}^3 \xleftarrow{\lambda_3} \ldots$$

This leads us the following definition.

Definition 7.6. *The set*

$$\lim_{\leftarrow} O/\mathfrak{p}^n = \{(x_n) \in \prod_{n=1}^{\infty} O/\mathfrak{p}^n : \lambda_n(x_{n+1}) = x_n\}$$

is a subring of $\prod_{n=1}^{\infty} O/\mathfrak{p}^n$ and is called the projective limit of the system of rings $O/\mathfrak{p}^n$.

Because of the commutative diagram above we obtain a ring map

$$O \to \lim_{\leftarrow} O/\mathfrak{p}^n$$

which just sends an element in O to its respective equivalence class in the projective limit. Equipping each of the $O/\mathfrak{p}^n$ with the discrete topology, the projective limit becomes a closed subset of the product topology on $\prod_{n=1}^{\infty} O/\mathfrak{p}^n$. We have the following theorem

Theorem 7.1. *The map $O \to \lim_{\leftarrow} O/\mathfrak{p}^n$ is an isomorphism of rings and a homeomorphism.*

8 Completions of fields

Let $(K, |\cdot|)$ be a valued field. A Cauchy sequence in K is a sequence (x_n) in K so that for every $\epsilon > 0$ there exists an $N \in \mathbb{N}$ so that if $m, n \geq N$ then

$$|x_n - x_m| \leq \epsilon$$

A null sequence is a sequence in K converging to 0.

Definition 8.1. *We say that a metric space X with metric d is complete if every Cauchy sequence in X converges to an element in X with respect to d. A valued field $(K, |\cdot|)$ is called a complete field if it is complete as metric space with respect to $d(x, y) = |x - y|$.*

(Maybe we should say here that $\mathbb{Q}$ is dense in $\mathbb{R}$).

Recall that the closed sets in a metric space are characterized as the sets containing all their limit points. In a complete metric space we have the following characterization of closed sets.

Proposition 8.1. *Suppose X is a complete metric space. Then a subset $A \subseteq X$ is closed if and only if A is complete.*

Proof. Suppose first that A is closed and let (x_n) be any Cauchy sequence in A. Then this sequence converges to some point $a \in X$ since X is complete. But as A is closed in X that means by definition that $a \in A$. On the other hand, assume that A is complete and let (x_n) be a sequence in A converging to some element $a \in X$. But then (x_n) is in fact a Cauchy sequence, hence $a \in A$. □

Definition 8.2 (Completion)**.** *Suppose $(K, |\cdot|)$ is a valued field. A completion of K is a complete valued field $\hat{K}$ together with a homomorphism $\hat{\iota} : K \to \hat{K}$ preserving the absolute value, satisfying the following universal property; If L is any other complete valued field and $\iota : K \to L$ is a homomorphism preserving the absolute value, then there is a unique homomorphism $\phi : \hat{K} \to L$, which preserves the absolute value, making the following diagram commute*

$$\begin{tikzcd}
 & K \arrow[ld, "\hat{\iota}"'] \arrow[rd, "\iota"] & \\
\hat{K} \arrow[rr, dashed, "\exists!\phi"'] & & L
\end{tikzcd}$$

The map ϕ in the diagram above is actually uniformly continuous since it preserves absolute values and is a homomorphism. Note also that we talk about 'a' completion, insinuating that there are multiple different ones. This is true, but it turns out that they are all unique up to unique isomorphism. This is a quite strong statement - much stronger than just being unique up to isomorphism.

Proposition 8.2. *Suppose K is a valued field and that $(\hat{K}_1, \iota_1)$ and $(\hat{K}_2, \iota_2)$ are completions of K. Then there is a unique absolute value preserving isomorphism, $\phi : \hat{K}_1 \to \hat{K}_2$ so that $\phi \circ \iota_1 = \iota_2$. In other words, the completion of K is unique up to unique isomorphism.*

Proof. Let us invoke the universal property on both $\hat{K}_1$ and $\hat{K}_2$ to obtain the diagram

$$\begin{tikzcd}
 & K \arrow[ld, "\iota_1"'] \arrow[rd, "\iota_2"] & \\
\hat{K}_1 \arrow[rr, dashed, "\exists!\phi" description] & & \hat{K}_2 \arrow[ll, dashed, bend left, "\exists!\psi" description]
\end{tikzcd}$$

By definition both ϕ and ψ preserve the absolute value. Writing out the two commutativity conditions we get

$$\iota_1 = \psi \circ \iota_2$$
$$\iota_2 = \phi \circ \iota_1$$

Combining these we obtain

$$\iota_1 = \psi \circ (\phi \circ \iota_1) = (\psi \circ \phi) \circ \iota_1$$

So $\psi \circ \phi$ has to be the identity on $\hat{K}_1$ and similarly $\phi \circ \psi$ is the identity on $\hat{K}_2$, hence ϕ is an isomorphism and it is the only one satisfying the equation $\iota_2 = \phi \circ \iota_1$. □

Because of this proposition we will more often than not say ”the completion” rather than ”a completion”. So far we haven’t demonstrated that the completion actually exists. This will be our next goal. The process of constructing such an object is very similar to the idea of the concrete construction of, for example, the tensor product - construct a huge object that sort of does what you want, then sculpt it into the desired object by modding out by a suitable relation.

Theorem 8.1. *Let K be a valued field and R be the set of all Cauchy sequences of K. Then R is a ring and the set $\mathfrak{m}$ of all null sequences of R is a maximal ideal.*

Proof. The addition and multiplication operations on R are defined element wise and it is easily seen that the Cauchy property is preserved under these operations. Rules such as the distributive law are inherited directly from the ring structure on K, and so R is a ring. The set $\mathfrak{m}$ is non-empty, as it most certainly contains the constant sequence $(0, 0, 0, ...)$. It is also contained in R since every convergent sequence is a Cauchy sequence so in particular the null sequences are Cauchy. Furthermore the difference of two null sequences is again a null sequence and the product of any sequence by a null sequence is also a null sequence. Thus, $\mathfrak{m}$ is an ideal of R. Let us now show that it is a maximal ideal. Take a sequence $(x_n) \in R$ which is not also in $\mathfrak{m}$. Such an element exists since R contains, for example, the constant sequence $1 = (1, 1, 1, ...)$ which is clearly not a null sequence. We wish to show that the ideal $J = (x_n) + \mathfrak{m}$ contains 1, i.e, that this ideal is in fact the entire ring R. The sequence $|x_n|$ is a Cauchy sequence in $\mathbb{R}$ with respect to the usual absolute value. Hence there is an N so that if $n \geq N$ then $|x_n| \geq c > 0$. Thus we can define

$$y_n = \begin{cases} \frac{1}{x_n} & \text{if } n \leq N \\ 0 & \text{if } n > N \end{cases}$$

Let now $\epsilon > 0$ be given and choose M so that $|x_n - x_m| < c^2\epsilon$ whenever $n, m \geq M$. For $n, m \geq \max\{N, M\}$ we now have

$$|y_n - y_m| = |\frac{1}{x_n} - \frac{1}{x_m}| = |\frac{x_m - x_n}{x_n x_m}| \leq \frac{1}{c^2}|x_m - x_n| \leq \frac{c^2\epsilon}{c^2} = \epsilon$$

But that means that y_n belongs to R and so $x_n y_n$ is in J. Denote by 1 the identity in R, i.e, the constant sequence $(1, 1, 1, ...)$. We now have $1 - x_n y_n \in J$ and so 1 is in J. □

From this it follows that $\hat{K} = R/\mathfrak{m}$ is a field. Define now

$$\hat{\imath}(x) = (x, x, x, ...) + \mathfrak{m} \in \hat{K}$$

for $x \in K$. This map is a homomorphism of fields and it is certainly not the zero map, which implies that it is injective. We can therefore think of K as a subfield of $\hat{K}$.

let us first recall the following proposition

Proposition 8.3. *Suppose X and Y are topological spaces and that $f : A \to Y$ is map defined on a dense subset A of X. Then f extends uniquely to a continuous map $\tilde{f} : X \to Y$.*

Theorem 8.2 (Existence of completion)**.** *Suppose $(K, |\cdot|)$ is a valued field and let R the set of all Cauchy sequences of K with respect to $|\cdot|$ and $\mathfrak{m} \subseteq R$ the maximal ideal consitsting of all null sequences. The function $f : R \to \mathbb{R}$, given by*

$$(x_n) \mapsto \lim_{n\to\infty} |x_n|$$

descends to the function, $|\cdot|' : \hat{K} \to \mathbb{R}$ given by

$$|\overline{(x_n)}|' = f((x_n))$$

We have the following properties

- *($\hat{K}$, $|\cdot|'$) is a valued field*
- *The homomorphism $\hat{\imath}$ preserves the absolute value.*
- *K is dense in $\hat{K}$*
- *$\hat{K}$ is complete with respect to $|\cdot|'$*

Furthermore, the pair $(\hat{K}, \hat{\imath})$ is the completion of K.

Proof. Let us first show that f descends to a function on the quotient. First of all, if $(x_n) \in R$, then (x_n) is a Cauchy sequence in K. Hence $(|x_n|)$ is a Cauchy sequence in $\mathbb{R}$, hence it converges to an element in $\mathbb{R}$, since $\mathbb{R}$ is complete with respect to $|\cdot|_\infty$, which is shown in [**?**].

Hence the map f is well defined. Take now two elements x and y in $\hat{K}$ with $x = y$ and suppose they are represented by the Cauchy sequences (x_n) and (y_n) in K, respectively. By the reverse triangle inequality we have

$$||x_n| - |y_n||_\infty \leq |x_n - y_n|$$

But $x_n - y_n$ is a null sequence and hence the left hand side converges to 0. This means that $\lim_{n\to\infty}(|x_n| - |y_n|) = 0$ and therefore

$$\lim_{n\to\infty} |x_n| = \lim_{n\to\infty} |y_n|$$

This shows that the map f descends to the quotient as desired. Let us move on to justifying that $|\cdot|'$ is actually an absolute value on $\hat{K}$. This is essentially inherited from the absolute value on K. So let us just show that $|\cdot|'$ possesses the zero-detection property. Suppose $x = \overline{(x_n)} \in \hat{K}$ so that $|x|' = 0$. We have

$$0 = |x|' = \lim_{n\to\infty} |x_n|$$

But this just says that (x_n) is a null sequence so $x = 0$. On the other hand, if we already know that $x = 0$ then it is clear that x_n is a null sequence and therefore $|x|' = 0$. It is also easily seen that $|\cdot|'$ extends $|\cdot|$. For if $x \in K$ then

$$|x| = \lim_{n\to\infty} |x| = f(\hat{\iota}(x)) = |\overline{\hat{\iota}(x)}|'$$

Let us now show that K is dense in $\hat{K}$. What we mean by this is that the image of K under the $\hat{\iota}$ is dense in $\hat{K}$. Let $\epsilon > 0$, take $\lambda \in \hat{K}$ and consider the open ball $B(\lambda, \epsilon)$. Let us show that we can find a constant sequence inside of this ball. Let (x_n) be a Cauchy sequence representing λ and find $N \in \mathbb{N}$ so that $|x_n - x_m| < \epsilon/2$ for all $m, n \geq N$. Define now the constant sequence $y = \hat{\iota}(x_N)$. Using the definition of the absolute value on $\hat{K}$ we get

$$|\lambda - y|' = \lim_{n\to\infty} |x_n - x_N| \leq \epsilon/2 < \epsilon$$

This shows that $y \in B(\lambda, \epsilon)$ and we conclude that K is dense in $\hat{K}$. Now we are ready to show that $\hat{K}$ is complete with respect to $|\cdot|'$. To do this, suppose that we have a Cauchy sequence (λ_n) in $\hat{K}$. As we have just seen, K is dense in $\hat{K}$. So for every λ_i, we can find an element $y_i \in K$ so that $|\lambda_i - \hat{\iota}(y_i)|' < \frac{1}{i}$. This way we get a sequence $(\hat{\iota}(y_n))$ in $\hat{K}$ and we observe that

$$\lim_{n\to\infty} |\lambda_n - \hat{\iota}(y_n)|' = 0$$

So by (**??**), $(\hat{\iota}(y_n))$ is also Cauchy. But then also the sequence (y_n) in K is Cauchy since $|\cdot|'$ extends the absolute value on K. But that means that (y_n) represents an element in $\hat{K}$. Call this element λ and let us show that $\lim_{n\to\infty} \lambda_n = \lambda$. To do this, it suffices to show that $\lim_{n\to\infty} \tilde{y}_n = \lambda$. As (y_n) is Cauchy, we can find N so that if $n, m \geq N$ then $|y_n - y_m| < \epsilon/2$. For any $n \geq N$ we now have

$$|\tilde{y}_n - \lambda|' = \lim_{m\to\infty} |y_n - y_m| \leq \epsilon/2 < \epsilon$$

This shows that

$$\lim_{n\to\infty} |\tilde{y}_n - \lambda|' = 0$$

which shows that $\hat{K}$ is complete with respect to $|\cdot|'$. Moving on to the last statement, let us see why $(\hat{K}, \hat{\iota})$ is the completion of K. So let L be a complete valued field and $\iota : K \to L$ a homomorphism preserving the absolute value. Let us define a function $\phi : \hat{K} \to L$. Pick an element $\lambda \in \hat{K}$. Because $\hat{\iota}(K)$ is dense in $\hat{K}$, there is Cauchy sequence, (y_n), in $\hat{\iota}(K)$ that converges to λ. Hence there is a sequence (x_n) in K so that $(\hat{\iota}(x_n)) = (y_n)$ and as $\hat{\iota}$ preserves the absolute value the sequence (x_n) is also Cauchy. As ι preserves the absolute value, we now have a Cauchy sequence $(\iota(x_n))$ in L and the fact that L is complete ensures that it converges to an element, $\lambda' := \lim_{n\to\infty} \iota(x_n)$. By uniqueness of limits we therefore obtain a well defined map $\phi : \hat{K} \to L$ mapping the element λ to λ'. It preserves absolute values since we have for $x \in \hat{K}$ that

$$\begin{aligned} |\phi(x)|_L &= |\lim_{n\to\infty} \iota(x_n)|_L \\ &= \lim_{n\to\infty} |\iota(x_n)|_L \\ &= \lim_{n\to\infty} |x_n|_K \\ &= \lim_{n\to\infty} |\hat{\iota}(x_n)|_{\hat{K}} \\ &= |\lim_{n\to\infty} \hat{\iota}(x_n)|_{\hat{K}} = |x|_{\hat{K}} \end{aligned}$$

Therefore f is continuous and it satisfies $\phi \circ \hat{\iota} = \iota$. This means that it is in particular defined on the dense subset $\hat{\iota}(K)$ which makes it uniquely determined by (8.3). The map ϕ is also a ring map because the limit of the sum of two convergent sequences is the sum of the limits of the sequences and similarly for the product. Thus the pair $(\hat{K}, \hat{\iota})$ is the completion of K. □

Remark 8.1. *Because $|\cdot|'$ extends $|\cdot|$, we will, for ease of notation, simply denote $|\cdot|'$ by $|\cdot|$. Also, if we knew that $|\cdot|$ was non-archimedian then, as (8.4) spells out, the sequence $(|x_n|)$ would eventually become constant. Thus we would not have needed to invoke the fact that $\mathbb{R}$ is complete to conclude that $(|x_n|)$ converges.*

Proposition 8.4. *Let $(K, |\cdot|)$ be a non-archimedian valued field. If (x_n) is a Cauchy sequence which is not a null sequence, then there exists an N so that $|x_n| = |x_m|$ for all $m, n \geq N$. In other words, the sequence must eventually become constant.*

Proof. Since (x_n) does not converge to 0, there exists an $N_1 \in \mathbb{N}$ and $c > 0$ so that $|x_n| \geq c > 0$ for all $n \geq N_1$. As the sequence is Cauchy, we can find $N_2 \in \mathbb{N}$ so that $|x_n - x_m| < c$ for all $n, m \geq N_2$. Set now $N := \max\{N_1, N_2\}$ and suppose $n, m \geq N$. Then

$$|x_n - x_m| < c \leq \min\{|x_n|, |x_m|\}$$

This means that both $|x_n|$ and $|x_m|$ are different from $|x_n - x_m|$ and hence $|x_n| = |x_m|$ since triangles are isosceles by (7.1). □

Let $(K, |\cdot|)$ be a nonarchimedian valued field with $\hat{K}$ its completion and let v be a valuation on K corresponding to $|\cdot|$. We can extend the valuation on K to a valuation on $\hat{K}$; Let $x \in \hat{K}$ be represented by the Cauchy sequence (x_n) in K and suppose that $x = 0$. Then (x_n) converges to 0 and that means that $v(x_n) \to \infty$. On the other hand, if (x_n) does not converge to 0, then by what we showed above, the sequence $(|x_n|)$ must eventually become a non-zero constant and hence the sequence $(v(x_n))$ becomes constant at some point as well and therefore it converges. Hence we obtain a valuation, $\hat{v}$, on $\hat{K}$ by defining $\hat{v}(x_n) = \lim_{x\to\infty} v(x_n)$. Note that this shows that $\hat{v}$ and v have the same value group and in particular, if v is discrete then so is $\hat{v}$. We will sometimes speak about the completion with respect to a valuation v. By this we mean the completion of the field with respect to an absolute value corresponding to v.

Theorem 8.3 (Approximation theorem). *Suppose $|\cdot|_1, ..., |\cdot|_n$ are pairwise inequivalent absolute values on a field K and suppose that we have $(a_1, ..., a_n) \in K^n$. Then for any given $\epsilon > 0$ there is an $x \in K$ so that $|x - a_i| < \epsilon$ for all $i = 1, ..., n$.*

Lemma 8.1 (Hensel's Lemma). *Let K be a field with valuation and let O be its corresponding valuation ring and $\mathfrak{p}$ the unique maximal ideal of O. Denote by $\bar{\cdot}$ the canonical map $O[x] \twoheadrightarrow \kappa[x]$, where $\kappa = O/\mathfrak{p}$. Suppose that $f \in O[x]$ such that $\overline{f} \neq 0$ and that there are relatively prime polynomials $g_0, h_0 \in \kappa[x]$ so that $\overline{f} = g_0 h_0$. Then there are polynomials $g, h \in O[x]$ so that $f = gh$ with* $\deg(g) = \deg(g_0)$ *and $\overline{g} = g_0$ and $\overline{h} = h_0$*

Proof. MISSING □

Lemma 8.2. *(DOES THIS ONLY APPLY FOR CHARACTERIC 0?) Consider the field extension K/F and suppose that $\alpha \in K$ is algebraic over F. Write*

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a + a_0$$

for the minimal polynomial of α over F. Then $N_{F(\alpha)/F}(\alpha) = \pm a_0$. If K/F is finite then $N_{K/F}(\alpha) = \pm a_0^m$ where $m = [K : F(\alpha)]$

Proof. Denote by $\alpha_1, ..., \alpha_n$ the n conjugates of α. Then we can write

$$f(x) = (x - \alpha_1)...(x - \alpha_n),$$

and we see that

$$a_0 = \pm\alpha_1...\alpha_n = N_{F(\alpha)/F}(\alpha)$$

Now if K/F is finite and $m = [K : F(\alpha)]$ then

$$N_{K/F}(\alpha) = N_{F(\alpha)/F}(N_{K/F(\alpha)}(\alpha)) = N_{F/K}(\alpha^m) = N_{F/K}(\alpha)^m = \pm a_0^m$$

□

Theorem 8.4. *Suppose $(K, |\cdot|)$ is a complete valued nonarchimedian field and that L/K is a finite field extension of degree n. Then $|\cdot|$ can be extended in a unique way to a nonarchimedian absolute value on L given explicitly as*

$$|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}, \text{ for all } \alpha \in L \qquad (\star)$$

Furthermore $(L, |\cdot|)$ is complete.

Proof. Let us first make sure that the function $(\star)$ is actually well defined. For all $\alpha \in L$ we know that $N_{L/K}(\alpha) \in K$. Hence it makes sense to use the absolute value on K on it. After doing so we get a real number greater than or equal to 0, and so it makes sense to take the nth root of this number. Let us start with the existence part. Let o be the valuation ring of K and O the integral closure of o in L. To help us establish that $(\star)$ is an absolute value on L we will first show that

$$O = \{\alpha \in L \mid N_{L/K}(\alpha) \in o\}. \qquad (\triangle)$$

First, suppose that $\alpha \in O$. Then α is integral over o and hence so are all the conjugates of α. But then the product of all of the conjugates of α is also integral over o and this product is equal to $N_{L/K}(\alpha)$, which we know is an element of K. Since o is integrally closed in K it now follows that $N_{L/K}(\alpha)$ is in o. This shows one of the inclusions. Let us now show the other. So assume that $\alpha \in L^*$ and that $N_{L/K}(\alpha) \in o$. Since L/K is a finite extension, L is algebraic over K and therefore α is in particular algebraic over K. Hence we can consider its minimal polynomial, f, over K. Then by (8.2) we have that

$$N_{L/K}(\alpha) = \pm a_0^m$$

where $m = [L : F]$ and a_0 is the constant term of f. But that means that $a_0^m \in o$ so $|a_0|^m = |a_0^m| \leq 1$, so $|a_0| \leq 1$ so $a_0 \in o$. If we can show that $f \in o[x]$ we are done, as that would establish that α is integral over o meaning that $\alpha \in O$. For contradiction, let us assume that $f \notin o[x]$ and let $\mathfrak{p}$ be the maximal ideal of o. We have $a := \max\{|a_d|, |a_{d-1}|..., |a_0|\} > 1$, where $a_d = 1$, since at least one of the coefficients of f does not belong to o. We can now find the smallest i so that $|a_i| = a$. This implies that $a \neq 0$ and so we can now define $g(x) = \frac{1}{a} f = \frac{1}{a} x^d + ... + \frac{a_0}{a}$ which is clearly in $o[x]$ and $\overline{g}$ is non-zero in $o/\mathfrak{p}$, since the ith coefficient of g is $1 \notin \mathfrak{p}$. Now by the choice of i we now have that $|\frac{a_0}{a}| < 1$, ..., $|\frac{a_{i-1}}{a}| < 1$. Thus, $\frac{a_d}{a}, ..., \frac{a_{i+1}}{a}$ all belong to $\mathfrak{p}$ and therefore they are all zero in the quotient $o/\mathfrak{p}$. Hence the terms in g having degree $0, ..., i-1$ all vanish in $o/\mathfrak{p}[x]$ and so we get a factorization $\overline{g(x)} = x^i h(x)$ where $h \in o/\mathfrak{p}[x]$ and $x \nmid h(x)$. Hence x^i and h are coprime and so by Hensel's lemma we now get a factorization of g, so g is not irreducible. But this cannot be the case since f is irreducible. Hence we get a contradiction, and we conclude that we must have $f \in o[x]$. We have now established $(\triangle)$.

Let us now use this result to show that

$$O = \{\alpha \in L \mid |\alpha| \leq 1\}$$

So suppose $\alpha \in L$. We have that $|\alpha| \leq 1$ is the same as saying that $|N_{L/K}(\alpha)| \leq 1$ which is the same as saying that $N_{L/K}(\alpha)$ belongs to the valuation ring o which, by what we have just shown is the same as $\alpha \in O$. Note that this means that once we have shown that $(\star)$ is a nonarchimedian absolute value on L, we can conclude that its valuation ring is O. So let us show this. Let us first show that $(\star)$ satisfies the strong triangle inequality. Since O is a ring we know that if $\alpha \in O$ then also $\alpha + 1 \in O$. From what we just showed this immediately implies that if $|\alpha| \leq 1$ then $|\alpha+1| \leq 1$. From this we can now deduce the strong triangle inequality. Assume that $\alpha, \beta \in L$ and that $|\alpha| \leq |\beta|$. Note that if $\beta = 0$ then the strong triangle inequality is already satisfied, so suppose that $\beta \neq 0$. Then $|\beta| \neq 0$ and we have $\frac{\alpha}{\beta} \in L$ and $|\frac{\alpha}{\beta}| \leq 1$. Thus

$$|\frac{\alpha}{\beta}+1| \leq 1$$

and after multiplication by $|\beta|$ we are left with the inequality

$$|\alpha+\beta| \leq |\beta|$$

Because we assumed that $|\alpha| \leq |\beta|$ we have $|\beta| = \max\{|\alpha|, |\beta|\}$. We conclude that the strong triangle inequality is satisfied, namely $|\alpha+\beta| \leq \max\{|\alpha|, |\beta|\}$ for all $\alpha, \beta \in L$. We still have some things to check before we can conclude that $|\cdot|$ is an absolute value on L, but these are easier to do. Firstly if $\alpha \in L$ then we have $|N_{L/K}(\alpha)| = 0$ if and only if $N_{L/K}(\alpha) = 0$ if and only if $\alpha = 0$. The fact that $|\alpha\beta| = |\alpha||\beta|$ for all $\alpha, \beta \in L$ follows from the fact that all the functions involved in the right hand side of $(\star)$ are multiplicative. We conclude that $(\star)$ is an absolute value on L. It also extends the absolute value on K since if $\alpha \in K$ then $N_{L/K}(\alpha) = \alpha^n$.

Let us now move on to proving the uniqueness of $(\star)$. So let $|\cdot|'$ be another nonarchimedian absolute value on L which extends the absolute value on K. Denote by O' the valuation ring with respect to $|\cdot|'$ and let $\mathfrak{p}$ and $\mathfrak{p}'$ be the maximal ideal of O and O' respectively. Let us show that $O \subseteq O'$. Assume for contradiction that $\alpha \in O$ but $\alpha \notin O'$. Then $\alpha \neq 0$ and we have that $|\alpha|' > 1$ and thus $\alpha^{-1} \in O'$. Since $\alpha \notin O'$ then α^{-1} cannot be a unit of O' and hence α^{-1} belongs to $\mathfrak{p}'$. As $\alpha \in O$ and O is the integral closure of o in L, we can find an equation

$$\alpha^d + a_{d-1}\alpha^{d-1} + ... + a_0 = 0$$

where all the a_i belong to o. But o is contained in O' since if $x \in o$ then $x \in K$ so $|x|' = |x| \leq 1$. Hence all the a_i belong to O'. Multiplying the above equation by α^{-1} and moving things around we get

$$1 = -(a_{d-1}\alpha^{-1} + ... + a_0\alpha^{-d})$$

But each term $a_{d-i}\alpha^{-i}$ is in $\mathfrak{p}'$ since $a_{d-i} \in O'$ and $\alpha^{-i} \in \mathfrak{p}'$ combined with the fact that $\mathfrak{p}'$ is an ideal. But that means that $1 \in \mathfrak{p}'$ which is impossible. Hence $O \subseteq O'$. What this means is that if $|\alpha| \leq 1$ then $|\alpha|' \leq 1$ and this implies that $|\cdot|$ and $|\cdot|'$ are equivalent (TODO). But then there exists some fixed $s \geq 1$ so that $|x|' = |x|^s$ for all $x \in L$ and as $|\cdot|$ and $|\cdot|'$ are equal on K we must have $s = 1$. Hence $|x|' = |x|$, proving uniqueness.

We now only need to show that L is complete with respect to $|\cdot|$. Let $1, \beta_2, ..., \beta_n \in L$ be a basis for L over K. Then for any $z \in L$ there exists unique $x_1, ..., x_n \in K$ so that $z = x_1 + x_2\beta_2 + ... + x_n\beta_n$, and so we get a map, $\phi : L \to \mathbb{R}$ by sending z to $\max\{|x_1|, ..., |x_n|\}$. This defines a non-archimedian absolute value on L and L is complete with respect to it.

Observe that if $z \in K$ then we have $0 = x_2 = ... = x_n$, showing that ϕ extends the absolute value on K. Hence by the uniqueness property we have just shown we now have that $\phi = |\cdot|$ and therefore $(L, |\cdot|)$ is complete. □

Proposition 8.5. *Let (K, v) be a valued field and K_v the completion of K with respect to v. We have*

$$O_{\hat{v}}/\mathfrak{p}_{\hat{v}} \cong O_v/\mathfrak{p}_v$$

If v is discrete then for all $n \geq 1$ we have

$$O_{\hat{v}}/\mathfrak{p}_{\hat{v}}^n \cong O_v/\mathfrak{p}_v^n$$

Proof. □

Lemma 8.3. *Let K be a number field. The field of fractions of the ring of integers of K, O_K, is equal to K. In other words, every element of K can be written as $\frac{\alpha}{\beta}$ for some $\alpha, \beta \in O$, where $\beta \neq 0$.*

Proof. Let F be the field of fractions of O_K. Then $F \subseteq K$ as F is the smallest field containing O_K. For the other inclusion, suppose for contradiction that $[K : F] > 1$. Take then an element, x, which is in K but not in F. Next, find an integer d so that $d\alpha$ is an algebraic integer. What this means is that $d\alpha \in O_K$, and therefore $d\alpha \in F$. But then $\alpha \in F$, contrary to our initial assumption. Hence $[K : F] = 1$ and so $F = K$. □

Recall that for a commutative ring R with unity we can localize at any given prime ideal $\mathfrak{p} \subseteq R$ and obtain the local ring $R_\mathfrak{p} = \{\frac{\alpha}{\beta} \mid \alpha \in R, \beta \in R \setminus \mathfrak{p}\}$ with two elements $\frac{\alpha}{\beta}$ and $\frac{\alpha'}{\beta'}$ in $R_\mathfrak{p}$ being equal if an only if there exists an element $s \in R \setminus \mathfrak{p}$ so that $s\alpha\beta' = s\alpha'\beta$. The ring $R_\mathfrak{p}$ has unique maximal ideal $\mathfrak{M} = \{\frac{\alpha}{\beta} \mid \alpha \in \mathfrak{p}, \beta \in R \setminus \mathfrak{p}\}$ and the localization map is the homomorphism sending an element $r \in R$ to $\frac{r}{1} \in R_\mathfrak{p}$.

Lemma 8.4. $\mathrm{Frac}(R/\mathfrak{p})$ *is canonically isomorphic to $R_\mathfrak{p}/\mathfrak{M}$. In particular, if $\mathfrak{p}$ is a maximal ideal then $R/\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{M}$.*

Proof. Firstly, $R/\mathfrak{p}$ is an integral domain as $\mathfrak{p}$ is a prime, so it makes sense to take the field of fractions of this ring. Consider the composition of maps $R \hookrightarrow R_\mathfrak{p} \twoheadrightarrow R_\mathfrak{p}/\mathfrak{M}$, with the first one being the localization map and the second one the natural projection. Then $r \in R$ is sent to zero if and only if $\frac{r}{1} \in \mathfrak{M}$ which is equivalent to $r \in \mathfrak{p}$. Hence we get an induced injective homomorphism, ϕ

$$R/\mathfrak{p} \hookrightarrow R_\mathfrak{p}/\mathfrak{M}$$

which is given by $\phi(r + \mathfrak{p}) = \frac{r}{1} + \mathfrak{M}$. We know that $R_\mathfrak{p}/\mathfrak{M}$ is a field since $\mathfrak{M}$ is a maximal ideal, so it follows from the universal property for the field of fractions that there is a unique injective homomorphism $\sigma : \mathrm{Frac}(R/\mathfrak{p}) \to R_\mathfrak{p}/\mathfrak{M}$, extending ϕ, which is given by $\sigma(\frac{\alpha}{\beta}) = \phi(\alpha)\phi(\beta)^{-1}$. Let us show that this map is surjective. Suppose that $\frac{a}{b} + \mathfrak{M} \in R_{\mathfrak{p}}/\mathfrak{M}$ with $a \in R$ and $b \notin \mathfrak{p}$. Thus, $b + \mathfrak{p}$ is non-zero in $R/\mathfrak{p}$. We can now evaluate

$$\sigma(\frac{a+\mathfrak{p}}{b+\mathfrak{p}}) = \phi(a+\mathfrak{p})\phi(b+\mathfrak{p})^{-1} = (\frac{a}{1} + \mathfrak{M})(\frac{b}{1} + \mathfrak{M})^{-1} = \frac{a}{b} + \mathfrak{M}$$

For the last statement, suppose that $\mathfrak{p}$ is maximal. Then $R/\mathfrak{p}$ is a field, so it is isomorphic to its field of fractions. □

Proposition 8.6. *Let O be a Dedekind domain and K its field of fractions. For any prime $\mathfrak{p}$ of O there is a function, $v_{\mathfrak{p}} : O \to \mathbb{R} \cup \{\infty\}$ on O so that $v_{\mathfrak{p}}(0) = \infty$ and that*

$$\forall x \in O \setminus \{0\} : v_{\mathfrak{p}}(x) = m \iff (x) = \mathfrak{p}^m A,\ A \text{ an ideal of } O \text{ and } \mathfrak{p} \nmid A. \quad (1)$$

The function v extends to a discrete valuation on K, which we will also call $v_{\mathfrak{p}}$, which for $\frac{\alpha}{\beta} \in K$, $\alpha, \beta \in O$ and $\beta \neq 0$ is given by

$$v_{\mathfrak{p}}(\frac{\alpha}{\beta}) = v_{\mathfrak{p}}(\alpha) - v_{\mathfrak{p}}(\beta)$$

The valuation $v_{\mathfrak{p}}$ extends to the completion $K_{\mathfrak{p}}$ of K with respect to $v_{\mathfrak{p}}$ and is also denoted by $v_{\mathfrak{p}}$. Let O_{v_p} be the valuation ring of K and let $\mathfrak{P}_{v_{\mathfrak{p}}}$ be its unique maximal ideal. Similarly, let $O_{\mathfrak{p}}$ be the valuation ring of $K_{\mathfrak{p}}$ and $\hat{\mathfrak{p}}$ its unique maximal ideal. We have the following;

1. *The localization of O at $\mathfrak{p}$, that is, the ring*

   $$O_{(\mathfrak{p})} = \{\frac{\alpha}{\beta} \in K \mid \alpha \in O, \beta \notin \mathfrak{p}\} = \{\frac{\alpha}{\beta} \in K \mid \alpha \in O, v_{\mathfrak{p}}(\beta) = 0\}$$

   is the same ring as $O_{v_{\mathfrak{p}}}$.

2. *The natural inclusions*

   $$O \hookrightarrow O_{(\mathfrak{p})} \hookrightarrow O_{\mathfrak{p}},$$

   give rise to the equalities $\mathfrak{P}_{v_{\mathfrak{p}}} = \mathfrak{p}O_{(\mathfrak{p})}$ and $\hat{\mathfrak{p}} = \mathfrak{p}O_{\mathfrak{p}}$, as well as the isomorphisms

   $$O/\mathfrak{p} \cong O_{(\mathfrak{p})}/\mathfrak{P}_{v_{\mathfrak{p}}} \cong O_{\mathfrak{p}}/\hat{\mathfrak{p}}$$

In particular, $K_{\mathfrak{p}}$ is a local field if $O/\mathfrak{p}$ is finite.

Proof. The function $v_{\mathfrak{p}}$ on O with the mentioned property is well defined since we have unique factorization of prime ideals in Dedekind domains. Let us now see that the function $v_{\mathfrak{p}}$ we have defined on K is actually well defined. If $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}$ then $\alpha\beta' = \alpha'\beta \in O$ and applying $v_{\mathfrak{p}}$ on both sides and using that it takes multiplication to addition we obtain

$$v_{\mathfrak{p}}(\alpha) - v_{\mathfrak{p}}(\beta) = v_{\mathfrak{p}}(\alpha') - v_{\mathfrak{p}}(\beta')$$

which shows that it is well defined. If we can show that all the properties in (**??**) are satisfied for the restriction of $v_\mathfrak{p}$ to O, we are done, since the function $v_\mathfrak{p}$ will then directly inherit all of these properties. It is immediate that $v_\mathfrak{p}(x) = \infty$ if and only if $x = 0$. Let now $x, y \in O$ and suppose both x and y are non-zero. We then have $v_\mathfrak{p}(x) = m$ and $v_\mathfrak{p}(y) = n$ and we can write

$$(x) = \mathfrak{p}^m A, (y) = \mathfrak{p}^n B$$

Thus, $(xy) = (x)(y) = \mathfrak{p}^{m+n}AB$ and $\mathfrak{p} \nmid AB$, so $v_\mathfrak{p}(xy) = m + n$. For the last property, let $d = \min\{m, n\}$. Then

$$(x + y) \subseteq (x) + (y) = \mathfrak{p}^d(\mathfrak{p}^{m-d}A + \mathfrak{p}^{n-d}B)$$

From this we see that $\mathfrak{p}^d \mid (x + y)$ and so $d \leq v_\mathfrak{p}(x + y)$. Note that if either x or y are 0, then these two properties follow immediately. We conclude that $v_\mathfrak{p}$ is a valuation on K. It is discrete since it maps O into $\mathbb{N}_0 \cup \{\infty\}$ so it maps K into $\mathbb{Z} \cup \{\infty\}$. Because of (**??**) the valuation on $K_\mathfrak{p}$ is as well. For (2.), it is clear that we have the inclusion, $O_{(\mathfrak{p})} \subseteq O_{v_\mathfrak{p}}$. So let $\frac{x}{y} \in O_{v_\mathfrak{p}}$ with $x, y \in O$ and both x and y non-zero and let $u = v_\mathfrak{p}(x)$, $v = v_\mathfrak{p}(y)$. Since $v_\mathfrak{p}(\frac{x}{y}) \geq 0$ we have $u \geq v$. We can now write

$$xO = \mathfrak{p}^u A, \text{ and } yO = \mathfrak{p}^v B$$

where A, B are two ideals of O so that $\mathfrak{p} \nmid A$ and $\mathfrak{p} \nmid B$. This means that $\mathfrak{p} \not\supseteq B$, which implies that we can find $c \in B$ such that $c \notin \mathfrak{p}$. But then $v_\mathfrak{p}(c) = 0$ and hence we are done if we can show that there is $b \in O$ so that $xc = yb$ as that would imply that $\frac{x}{y} = \frac{b}{c}$. Now, $xc \in xO$ and also $xc \in B$, meaning that $xc \in xO \cdot B$. But,

$$xO \cdot B = \mathfrak{p}^u AB = \mathfrak{p}^{u-v}A\mathfrak{p}^v B = \mathfrak{p}^{u-v}A \cdot yO$$

So $xc \in \mathfrak{p}^{u-v}A \cdot yO$ which means that we can find $b \in \mathfrak{p}^{u-v}A$ such that $xc = by$. We conclude that $O_{v_\mathfrak{p}} = O_{(\mathfrak{p})}$. As for (3.), consider the natural inclusions

$$O \hookrightarrow O_{(\mathfrak{p})} \hookrightarrow O_\mathfrak{p},$$

Since O is a Dedekind domain, $\mathfrak{p}$ is in fact a maximal ideal so by (8.4) it follows that $O/\mathfrak{p} \cong O_{(\mathfrak{p})}/\mathfrak{P}_{v_\mathfrak{p}}$. The other isomorphism is just (8.5).

(((Apparently this valuation is always discrete? :OOOO)))

For the last claim, if K is discrete then by (1) in the proposition we know that the valuation on $K_\mathfrak{p}$ is also discrete. If furthermore $O/\mathfrak{p}$ is finite then so is the residue field $K_\mathfrak{p}/O_\mathfrak{p}$ because of the isomorphisms from (3). Hence $K_\mathfrak{p}$ is in this case a local field. □

Remark 8.2. *Note that we have shown that the localization of Dedekind domain at a prime is a local Dedekind domain. It can be shown that local Dedekind domains are PIDs which implies that $O_{(\mathfrak{p})}$ is in fact a discrete valuation ring.*

Let us now see some examples using this construction.

Example 8.1. *Let K be a number field and pick a prime $\mathfrak{p}$ of O_K. From (8.3) we know that $K = \mathrm{Frac}(O_K)$. Hence from the above proposition we obtain the so-called $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}} : K \to \mathbb{Z} \cup \{\infty\}$ which extends to a discrete valuation on the completion, $K_{\mathfrak{p}}$. The elements of $K_{\mathfrak{p}}$ and $O_{v_{\mathfrak{p}}}$ are called $\mathfrak{p}$-adic numbers and $\mathfrak{p}$-adic integers, respectively. We know that $O_K/\mathfrak{p}$ is finite so $K_{\mathfrak{p}}$ is a local field. In the special case where $K = \mathbb{Q}$ we have $\mathfrak{p} = (p)$ for some prime $p \in mbbZ$. We denote $K_{\mathfrak{p}}$ as $\mathbb{Q}_p$ and we call this ring the p-adic numbers. The ring $O_{v_{\mathfrak{p}}}$ is denoted by $\mathbb{Z}_p$ and called the p-adic integers.*

Lemma 8.5. *A PID is a Dedekind domain.*

Proof. Assume R is a PID. Then any ideal I of R is generated by a single element, so in particular it is finitely generated. Also, we know that if I is prime then it is in fact maximal. R is in particular a UFD and we claim that these are integrally closed. Let K be the field of fractions of R and suppose $\frac{a}{b} \in K$ with $a, b \in R$, $b \neq 0$ so that $\gcd(a, b) = 1$. Suppose that we have

$$(\frac{a}{b})^n + c_{n-1}(\frac{a}{b})^{n-1} + ... + c_1(\frac{a}{b}) + c_0 = 0$$

where the c_i are in R. Multiplying by b^n we get

$$a^n + c_{n-1}a^{n-1}b + ... + c_1ab^{n-1} + c_0b^n = 0$$

which shows that $b \mid a^n$ in R, meaning that $b \mid a$ in R. But since $\gcd(a, b) = 1$, b has to be a unit and therefore $\frac{a}{b} \in R$. We conclude that R is a Dedekind domain. □

Example 8.2. *Let F be a field. Then $O := F[x]$ is a PID hence a Dedekind domain. The ideal $\mathfrak{p} = (x)$ is a maximal ideal and so we get a valuation $v_{\mathfrak{p}}$ on $K := F(x)$ that extends to $K_{\mathfrak{p}}$. The field $K(x)$ is dense in $K((x))$, $K((x))$ is complete and the inclusion $K(x) \hookrightarrow K((x))$ preserves absolute values, so $K((x)) \cong K_{\mathfrak{p}}$. It is clear that $v_{\mathfrak{p}}(x) = 1$ so the valuation on $K((x))$ is discrete. Also, $O_{\mathfrak{p}} = K[[x]]$ and $\hat{\mathfrak{p}} = (x)O_{\mathfrak{p}}$ so $K((x))$ has residue field $O_{\mathfrak{p}}/\hat{\mathfrak{p}} \cong K$. Hence $K((x))$ is a local field if and only K is a finite field.*

9 Local manifold

Suppose that K is a complete field with valuation v. Say that we have a power series $f \in K[[X]]$,

$$f(X) = \sum_{n=0} a_n X^n.$$

The set C containing all points $x \in K$ so that $f(x)$ converges is called the region of convergence for f. In fact $C = \{x \in K \mid v(x) \geq \mu\}$ where $\mu = \min_{x \in C} v(x)$. We get an induced function $f : C \to K$ given by $x \mapsto f(x)$ and this function is continuous. (PROVE THIS OR PROVIDE A REFERENCE)

Suppose U is an open neighborhood around a point $x_0 \in K^n$ and that we have a function $f : U \to K$ and a formal power series $g \in K[[X_1, ..., X_n]]$ that converges to $f(x)$ for all $x \in U$. Then the function f is called an analytic function and is said to be represented by the formal power series g. If $f' : U' \to K$ is another analytic function, with U' another open neighborhood around x_0, and also represented by g, we will consider f and f' to be equal if $U \subseteq U'$ or $U' \subseteq U$.

Next, let us define what is called a local manifold. These are closely related to varieties known from algebraic geometry. Let $|\cdot|$ be an absolute value corresponding to v and let $\overline{K}$ denote the algebraic closure of K. We will refer to the elements, $(\alpha_1, ..., \alpha_n)$ of the cartesian product, $\overline{K}^n$, as points. The set of points where $|\alpha_i| < \epsilon$ for all $i = 1, ..., n$, is called an ϵ-neighborhood of the origin. Let D be the set containing all $f \in \overline{K}[[x_1, ..., x_n]]$ that converge in some ϵ-neighborhood of the origin. This set is in fact a subring of $K[[x_1, ..., x_n]]$.

Definition 9.1 (Local manifold)**.** *Assume $f_1, ..., f_m \in D$ all of which have zero constant term. The set V of points $(\alpha_1, ..., \alpha_n) \in \overline{K}^n$ belonging to some ϵ-neighborhood of the origin so that*

$$f_1(\alpha_1, ...\alpha_n) = ... = f_m(\alpha_1, ..., \alpha_n) = 0$$

is called a local manifold.

We only really care about what a local manifold looks like near the origin. As such we will regard two local manifolds as equal if there is an ϵ-neighborhood in which they are the same. Let V be a local manifold and consider the set, I_V, of elements $f \in D$ so that f vanishes in some ϵ-neighborhood of the origin. This set is an ideal of D and therefore we can consider the quotient ring $\overline{D} = D/I_V$.

Definition 9.2 (Curve)**.** *A curve in $\overline{K}^n$ is a collection of n integral (WHAT IS MEANT BY THIS) power series, $\omega_1(t), ..., \omega_n(t) \in \overline{K}[[t]]$, not all identically zero, and with constant term zero. We say the curve lies on a manifold V, if for every power series $f \in I_V$ we have*

$$f(\omega_1(t), ..., \omega_n(t)) = 0$$

Not that a curve in the sense of this definition above is not a set of points. It is merely a collection of formal power series. We need the following theorems.

Theorem 9.1. *A local manifold is either equal to the set containing just the origin, or it contains a curve.*

Theorem 9.2. *Suppose V and V' are local manifolds in $\overline{K}^n$ such that $V \nsubseteq V'$. Then there is a curve on V that does not lie on V'.*

Remark 9.1. *Note that by contraposition, we have the following: If for all curves, C, we have that C is not on V or C is on V', then $V \subseteq V'$. This is the same as saying: If every curve on V is also on V' then $V \subseteq V'$.*

10 Local fields

In algebraic number theory we study finite extensions of $\mathbb{Q}$, known as number fields. Similarly, it turns out to be fruitful to consider the finite extensions of $\mathbb{Q}_p$, the field of p-adic numbers. These fields are called local fields and we will take a look at them now. We start out by giving another definition of these fields.

Definition 10.1. *A field K is called a **local field** if it is complete with regards to a discrete valuation and has finite residue field.*

Proposition 10.1. *A local field K of characteristic 0 is the same thing as a finite extension of $\mathbb{Q}_p$. Such a field is called a $\mathfrak{p}$-adic number field.*

Proof. Suppose first that $K/\mathbb{Q}_p$ is a finite extension of degree n. Then by (8.4) the absolute value on $\mathbb{Q}_p$ extends uniquely to the nonarchimedian absolute value $|\alpha| = \sqrt[n]{|N_{K/\mathbb{Q}_p}|}$ on K and K is complete with respect to it. The absolute value on $\mathbb{Q}_p$ is discrete, so this must also be the case for the absolute value on K. Let κ be the residue field of K and set $m = [\kappa : \mathbb{F}_p]$. To show that κ has finitely many elements it suffices to show that $m \leq n$ as that implies that $\#\kappa \leq p^n$. Suppose that $x_1, ..., x_n \in K$ are linearly dependent over $\mathbb{Q}_p$. Then we can find $\lambda_1, ..., \lambda_n \in \mathbb{Q}_p$ with at least one $\lambda_i \neq 0$ so that

$$\lambda_1 x_1 + ... + \lambda_n x_n = 0.$$

The coefficient, λ_i, having the largest absolute value has to have absolute value strictly larger than 0, as otherwise $\lambda_i = 0$ which would imply that all coefficients are 0. Hence we can divide the above linear combination by λ_i to achieve a linear combination where all coefficients have absolute value smaller than or equal to 1. In other words, a linear combination with coefficients in $\mathbb{Z}_p$, the valuation ring of $\mathbb{Q}_p$. But then the ith coefficient is 1, so this linear combination is still non-trivial when mapped to κ. (NOT COMPLETELY DONE WITH THIS ONE. ASK ABOUT IT)

(NOT VERY SURE ABOUT THIS PART EITHER)

On the other hand, suppose that K is a local field with characteristic 0 and discrete valuation v. Let O be the valuation ring of K and $\mathfrak{p}$ be its unique maximal ideal. The residue field of K is then $\kappa = O/\mathfrak{p}$ and as K is a local field, we know that κ is a finite field so its characteristic is a prime number, say p. But that means that p is zero in κ, which is to say that $p \in \mathfrak{p}$, meaning that $v(p) > 0$. This implies (TODO: SHOW WHY) that v and v_p are equivalent valuations when restricted to $\mathbb{Q}$. The closure of $\mathbb{Q}$ in K is the smallest closed containing $\mathbb{Q}$ and as K is complete, it is therefore the smallest complete set containing $\mathbb{Q}$

therefore $\mathbb{Q}_p$ and is contained in K. As K is a metric space it is Hausdorff and by **??** K is locally compact. It therefore follows by a theorem which can be found HERE that the $\mathbb{Q}$-vector space K has finite dimension. □

Lemma 10.1. *Let G be a group of order n. Then $x^n = 1$ for all $x \in G$.*

Proof. Let $x \in G$ and consider the cyclic subgroup H generated by x. As G is finite so is H so by Lagrange's theorem, $|H|$ divides n meaning that $n = |H|k$ for some $k \in \mathbb{Z}$. As H is cyclic we have $x^{|H|} = 1$ and so $x^n = x^{|H|k} = 1^k = 1$. □

Proposition 10.2. *Let K be a local field, O its valuation ring, $\mathfrak{p}$ the maximal ideal of O, κ its residue field and $q = \#\kappa$. Then K^* contains μ_{q-1}, the group of $(q-1)$st roots of unity and we have*

$$K^* = \{\pi^k \mid k \in \mathbb{Z}\} \times \mu_{q-1} \times U^{(1)}$$

Proof. Because of (7.3) we really only need to show that $O^* = \mu_{q-1} \times U^{(1)}$. From the natural projection $O \twoheadrightarrow \kappa$ we obtain a group homomorphism $\phi : O^* \to \kappa^*$. Let us first show that O^* contains μ_{q-1}. First, κ^* is a group of order $q-1$ so if z is any element in κ^* then by (10.1) we have $z^{q-1} = 1$ and so $f(x) = x^{q-1} - 1 \in O[x]$ splits into distinct linear factors over κ. Thus we have the factorization $f(x) \equiv (x-z)g(x) \pmod{\mathfrak{p}}$ with $x - z$ and g being coprime and both belonging to $\kappa[x]$. By Hensel's Lemma we get a factorization $f(x) = \alpha(x)\beta(x)$ where both α and β are in $O[x]$ and where $\deg \alpha = \deg(x - z) = 1$. Hence $\alpha(x) = x - \zeta$ for some $\zeta \in O$. Hensel's Lemma also tells us that $x - \zeta \equiv x - z \pmod{\mathfrak{p}}$, so $z \equiv \zeta \pmod{\mathfrak{p}}$. In other words, $\phi(\zeta) = z$. Now since $\alpha(\zeta) = 0$ we have $f(\zeta) = 0$, that is, ζ is a $q-1$st root of unity and therefore in particular we have $\zeta \in O^*$. As z was an arbitrary element of κ^*, we conclude that f has all of its $q-1$ roots in O^*, all of which are distinct so O^* contains μ_{q-1} and these are mapped bijectively onto κ^* since $q - 1 = \#\kappa = \#\mu_{q-1}$. To show that $O^* = U^{(1)} \times \mu_{q-1}$ it suffices to show that $U^{(1)} \cap \mu_{q-1} = \{1\}$ and $O^* = U^{(1)}\mu_{q-1}$. To do this, let us first show that $\ker \phi = U^{(1)}$. Saying that $\phi(x) = 1$ for some $x \in O^*$ is the same as saying that $1 \equiv x \pmod{\mathfrak{p}}$ which is equivalent to $x - 1 \in \mathfrak{p}$ which is also equivalent to $x \in 1 + \mathfrak{p} = U^{(1)}$, so $\ker \phi = U^{(1)}$. Now if $x \in U^{(1)} \cap \mu_{q-1}$ then $\phi(x) = 1$ as $x \in U^{(1)}$ and as $x \in \mu_{q-1}$ we must have $x = 1$ since ϕ maps μ_{q-1} bijectively onto κ^* and $\phi(1) = 1$ simply because ϕ is a homomorphism so $U(1) \cap \mu_{q-1} = \{1\}$. Suppose that $u \in O^*$. Then $\phi(u) \in \kappa^*$ and we can find $\zeta^{-1} \in \mu_{q-1}$ so that $1 = \phi(u)\phi(\zeta^1)$. But then $u\zeta^{-1} \in \ker \phi = U^{(1)}$, so we can write $u\zeta^{-1} = v$ for some $v \in U^{(1)}$. Hence $u = v\zeta$ showing that $O^* = U^{(1)}\mu_{q-1}$. We conclude that $O^* = U^{(1)} \times \mu_{q-1}$. □

Lemma 10.2. *Let K be a local field with residue field $\kappa = O/\mathfrak{p}$, and let $q = \#\kappa$. For any $n \in \mathbb{N}$ we have $\#(O/\mathfrak{p}^n) = q^n$.*

Proof. Since the valuation on K is discrete, we know that for any $k \in \mathbb{N}$ we have

$$\mathfrak{p}^k/\mathfrak{p}^{k+1} \cong \kappa,$$

as groups under addition. We prove the statement using induction on n. The base case $n = 1$ is clear. So suppose that $\#(O/\mathfrak{p}^n) = q^n$. We have the isomorphism

$$(O/\mathfrak{p}^{n+1})/(\mathfrak{p}^n/\mathfrak{p}^{n+1}) \cong O/\mathfrak{p}^n$$

But since $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ and $O/\mathfrak{p}^n$ have finite order, also $O/\mathfrak{p}^{n+1}$ must have finite order. By Lagrange's theorem, it now follows that

$$\#(O/\mathfrak{p}^{n+1}) = \#(O/\mathfrak{p}^n) \cdot \#(\mathfrak{p}^n/\mathfrak{p}^{n+1}) = q^{n+1}$$

□

Proposition 10.3. *Let K be a valued field and (x_n) and (y_n) sequences of K. If (x_n) is Cauchy and $\lim_{n\to\infty} |x_n - y_n| = 0$ then (y_n) is also Cauchy. If it is also known that $\lim_{n\to\infty} x_n = a$ then $\lim_{n\to\infty} y_n = a$.*

Proof. Observe that

$$|y_n - y_m| = |x_n - y_n + x_m - y_m + x_n - x_m| \tag{2}$$

A three fold application of the triangle inequality on the right hand side basically tells us that (y_n) is Cauchy. For the last part, use the triangle inequality on the right hand side of

$$|y_n - a| = |x_n - y_n + x_n - a|$$

and take the limit. □

Theorem 10.1. *The valuation ring of a local field K is compact.*

Proof. The valuation ring can be thought of as the closed unit ball around 0 with respect to the absolute value on K. Hence it is closed and is homeomorphic to $\varprojlim O/\mathfrak{p}^n$ which is then of course also closed. This inverse limit is contained in $\prod_{n=1}^{\infty} O/\mathfrak{p}^n$, which is compact by Tychonoff's theorem since all the $O/\mathfrak{p}^n$ are finite by (10.2), and hence they are compact. It follows that O is compact. □

Remark 10.1. *Since the absolute value K induces a metric on K, it means that compactness is equivalent to sequential compactness. Thus every sequence in O has a convergent subsequence.*

In the real numbers we are used to that the function $u \mapsto \alpha^u$ is well-defined regardless of what u and α is. For some fields this is not the case, and we will now see an example of this.

Proposition 10.4. *Let K be a local $\mathfrak{p}$-adic number field and let n be the smallest natural number so that we obtain an isomorphism $\mathfrak{p}^n \cong U^{(n)}$ as in (???). Suppose $u, \alpha \in O$. Then the exponential function $\alpha^u = \exp(u \log \alpha)$ is well-defined whenever $u \in O$ and $\alpha \in U^{(n)}$.*

Proof. Suppose that $u \in O$ and $\alpha \in U^{(n)}$. This means that $\log \alpha \in \mathfrak{p}^n$ and so $u \log \alpha \in \mathfrak{p}^n$ because $\mathfrak{p}^n$ is an ideal. Thus, it makes sense to apply exp on $u \log \alpha$. □

Lemma 10.3. *Suppose $\mathfrak{p}$ is a prime of a local field K and set $q = \#(O/\mathfrak{p}^n)^*$. If $\alpha \in O_K$ and $\mathfrak{p} \nmid \alpha$ then $\alpha^q \in U^{(n)}$. In particular, if ϵ is any unit of O_K then $\epsilon^q \in U^{(n)}$.*

Proof. First of all, the number q is a natural number by (10.2). Take α in O_K and suppose $\mathfrak{p} \nmid \alpha$ for some prime $\mathfrak{p}$ of K. This means that $\mathfrak{p}$ does not occur in the prime factorization of αO_K, which means that $\gcd(\alpha O_K, \mathfrak{p}) = O_K$, hence also $\gcd(\alpha O_K, \mathfrak{p}^n) = O_K$. But that means that $\alpha\beta + l = 1$ for some $l \in \mathfrak{p}^n$ and $\beta \in O_K$, and so α is a unit in $O_K/\mathfrak{p}^n$. But then $\overline{\alpha^q} = \overline{1}$ in $O_K/\mathfrak{p}^n$. Hence, $\alpha^q \in U^{(n)}$. Suppose now that ϵ is a unit in O_K. Then $\epsilon O_K = O_K$, meaning that $\mathfrak{p} \nmid \epsilon$. By what we just proved, it now follows that $\epsilon^q \in U^{(n)}$. □

11 Logarithms and Exponentials

In this section, K is a $\mathfrak{p}$-adic field. As such it is by (10.1) a finite extension of $\mathbb{Q}_p$ and by (8.4) the valuation v_p on $\mathbb{Q}_p$ therefore extends uniquely to K. This valuation is discrete so there is $\pi \in K$ so that $v_p(\pi) = \frac{1}{e} > 0$ is the smallest attainable strictly positive value for this function. Hence defining $v_\mathfrak{p} = ev_p$ we get a normalized valuation on K. In this section we will see how one can define logarithm- and exponential functions on K. We start by looking at the formal power series

$$\log(1+X) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{X^k}{k}$$

$$\exp(X) = \sum_{k=1}^{\infty} \frac{X^k}{k!}$$

To emphasize that these are really just formal power series, we have written the variable in uppercase. As the coefficients of both belong to $\mathbb{Q}$ these are certainly elements of $K[[X]]$.

(ADD BETTER ARGUMENT FOR LOG AND EXP ACTUALLY BEING HOMOMORPHISMS)

Lemma 11.1. *(Legendre's formula) Suppose we have $k \in \mathbb{N}$. Then*

$$v_p(k!) = \sum_{i=1}^{\infty} \left\lfloor \frac{k}{p^i} \right\rfloor$$

Proof. First of all, there are only finitely many terms in the sum since $\left\lfloor \frac{k}{p^i} \right\rfloor$ is eventually zero when i is large enough so it converges. For natural numbers q and n we define the function

$$f_q(n) = \begin{cases} 1 & \text{if } q \mid n \\ 0 & \text{otherwise} \end{cases}$$

We then have for any $m \in \mathbb{N}$ that

$$v_p(m) = \sum_{i=1}^{\infty} f_{p^i}(m)$$

Thus,

$$\begin{aligned} v_p(k!) &= \sum_{j=1}^{k} v_p(j) \\ &= \sum_{j=1}^{k}\sum_{i=1}^{\infty} f_{p^i}(j) \\ &= \sum_{i=1}^{\infty}\sum_{j=1}^{k} f_{p^i}(j) \end{aligned}$$

But clearly, $\sum_{j=1}^{k} f_{p^i}(j) = \left\lfloor \frac{k}{p^i} \right\rfloor$, so we get the result. □

Using this result we can prove the following

Lemma 11.2. *Assume that $k \in \mathbb{Z}$ and suppose that $k = \sum_{i=0}^{r} a_i p^i$ is the p-adic expansion of k. Then we have that*

$$v_p(k!) = \frac{k - s_k}{p - 1}$$

where $s_k = \sum_{i=0}^{r} a_i$.

Proof. Suppose $i \in \mathbb{N}$. We then get $\sum_{j=0}^{i-1} a_j p^{j-i} < 1$, so

$$\begin{aligned} \left\lfloor \frac{k}{p^i} \right\rfloor &= \left\lfloor \sum_{j=0}^{r} a_j p^{j-i} \right\rfloor \\ &= \left\lfloor \sum_{j=0}^{i-1} a_j p^{j-i} + \sum_{j=i}^{r} a_j p^{j-i} \right\rfloor \\ &= \left\lfloor \sum_{j=i}^{r} a_j p^{j-i} \right\rfloor \\ &= \sum_{j=i}^{r} a_j p^{j-i} \end{aligned}$$

So when $i > r$, we have $\left\lfloor \frac{k}{p^i} \right\rfloor = 0$.

$$\begin{aligned} v_p(k!) &= \sum_{i=1}^{r} \left\lfloor \frac{k}{p^i} \right\rfloor \\ &= \sum_{i=1}^{r} \sum_{j=i}^{r} a_j p^{j-i} \\ &= \sum_{j=1}^{r} \sum_{i=j}^{r} a_j p^{j-i} \\ &= \sum_{j=1}^{r} a_j \sum_{i=1}^{j} p^{j-i} \end{aligned}$$

□

We define $U^{(k)} := 1 + \mathfrak{p}^k$ for $k \in \mathbb{N}_0$. Each of these are multiplicative groups and we have $U^{(0)} = O^*$. The group $U^{(1)}$ is called the principal units.

Proposition 11.1. *Let K be a $\mathfrak{p}$-adic number field. There is a uniquely determined group homomorphism taking multiplication to addition,*

$$\log : K^* \to K$$

so that $\log p = 0$ and for $(1+z) \in U^{(1)}$ this function is given by

$$\log(1+z) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{z^k}{k}$$

Proof. We first show that log actually converges on principal units. So suppose $(1+z) \in U^{(1)}$. Then $z \in \mathfrak{p}$ and so $v_p(z) > 0$, which means that $c = p^{v_p(z)} > 0$. (WE THINK OF v_p as extended to K.) Thus we can apply the usual logarithm and get $v_p(z) = \frac{\ln c}{\ln p}$. If k is any natural number, then we always have

$$p^{v_p(k)} \leq k,$$

since $p^{v_p(k)}$ divides k. Applying ln to both sides of this inequality is valid, as both sides are strictly positive and from doing so we get

$$v_p(k) \ln p \leq \ln k$$

and so,

$$v_p(k) \leq \frac{\ln k}{\ln p}$$

Now for any $k \in \mathbb{N}$ we get

$$\begin{aligned} v_p(\frac{z^k}{k}) &= v_p(z^k) - v_p(k) \\ &= k v_p(z) - v_p(k) \\ &\geq k\frac{\ln c}{\ln p} - \frac{\ln k}{\ln p} \\ &= \frac{\ln c^k/k}{\ln p} \end{aligned}$$

Clearly, $\ln c^k/k \to \infty$ as $k \to \infty$. Hence, $v_p(\frac{z^k}{k}) \to \infty$ as $k \to \infty$. By (7.1), this means that the sum $z - \frac{z^2}{2} + \frac{z^3}{3} - ...$ converges. We have the following equality of formal power series

$$\log((1+z)(1+y)) = \log(1+z) + \log(1+y)$$

So if $1+z, 1+y \in U^{(1)}$ then also $(1+z)(1+y) \in U^{(1)}$ meaning that all the series occurring in the above equation converge. Thus $\log : U^{(1)} \to K$ is a homomorphism. Suppose that $\alpha \in K^*$ and that $\pi \in K$ is an element so that $v_{\mathfrak{p}}(\pi) = 1$. By (10.2) there exists a unique elements $k_\alpha \in \mathbb{Z}$, $\zeta_\alpha \in \mu_{q-1}$ and $u_\alpha \in U^{(1)}$ (WHAT IS q??) so that $\alpha = \pi^{k_\alpha}\zeta_\alpha u_\alpha$, and we have $v_{\mathfrak{p}}(\alpha) = k_\alpha$. $v_{\mathfrak{p}} = e v_p$. Note that $v_{\mathfrak{p}}(p) = e$. So as $p \in K^*$ we can write $p = \pi^e \zeta_p u_p$. Let us now define $\log \pi = -\frac{1}{e}\log u_p$. Since log is 0 on all of $U^{(1)}$ we now get an extension of log to all of K^* by setting

$$\log \alpha = v_{\mathfrak{p}}(\alpha)\log(\pi) + \log(u_\alpha)$$

This function is continuous because addition of continuous functions are continuous and it is also a homomorphism by inheritance. Furthermore we have that

$$\log p = e\log(\pi) + \log(u_p) = \frac{-e\log u_p}{e} + \log(u_p) = 0$$

Suppose that we have another extension, $\lambda : K^* \to K$, of log so that $\lambda(p) = 0$ and which is also a homomorphism. Note first that for any $\alpha \in K^*$ we have

$$\lambda(\alpha) = \lambda(\pi^{v_{\mathfrak{p}}(\alpha)}\zeta_\alpha u_\alpha) = v_{\mathfrak{p}}(\alpha)\lambda(\pi) + \lambda(\zeta_\alpha) + \lambda(u_\alpha)$$

By assumption we know that $\log(u_\alpha) = \lambda(u_\alpha)$ since $u_\alpha \in U^{(1)}$. Hence

$$\lambda(\alpha) - \log(\alpha) = v_{\mathfrak{p}}(\alpha)(\lambda(\pi) - \log(\pi)) + \lambda(\zeta_\alpha)$$

So to show that $\lambda = \log$ it suffices to show that λ vanishes on μ_{q-1} and that $\lambda(\pi) = \log(\pi)$. Take any $\zeta \in \mu_{q-1}$. Since $\zeta^{q-1} = 1$ and $\lambda(1) = 0$ we see that

$$\lambda(\zeta) = \frac{1}{q-1}\lambda(\zeta^{q-1}) = 0$$

By assumption $0 = \lambda(p) - \log(p)$. Since $\lambda(\zeta_p) = 0$ and $v_{\mathfrak{p}}(p) = e \neq 0$ we must have $\lambda(\pi) - \log(\pi) = 0$. □

Proposition 11.2. *The formal power series*

$$\log(1+z) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{x^k}{k}$$

$$\exp(z) = \sum_{k=1}^{\infty} \frac{z^k}{k!}$$

induce, for $m > \frac{e}{p-1}$, isomorphisms

$$\log : U^{(m)} \to \mathfrak{p}^m$$

$$\exp : \mathfrak{p}^m \to U^{(m)}$$

and these are inverses of one another.

Proof. We have already established that the power series for the logarithm converges on $U^{(1)}$, hence it also converges on $U^{(m)}$ for all $m \in \mathbb{N}$. Our first goal is to show that log maps $U^{(m)}$ into $\mathfrak{p}^m$ for all $m > \frac{e}{p-1}$. To do this we need a little help from the following inequality. We have for $k \in \mathbb{N}$ that

$$\frac{v_p(k)}{k-1} \leq \frac{1}{p-1},$$

Let us show that this actually holds. Write $k = p^a k_0$, where $p \nmid k_0$. Then $v_p(k) = a$ and so the inequality is satisfied when $a = 0$. So suppose $a > 0$. Then we can write

$$p^a - 1 = (p-1)(p^{a-1} + ... + p + 1).$$

We have $a \leq p^{a-1} + ... + p + 1$, since the right side of the inequality consists of a total of a terms all of which are larger than 1. Now

$$\frac{v_p(k)}{k-1} = \frac{a}{p^a k_0} \leq \frac{a}{p^a - 1} = \frac{1}{p-1} \cdot \frac{a}{p^{a-1} + ... + p + 1} \leq \frac{1}{p-1}$$

Suppose now that $1 + z \in U^{(m)}$ with $m > \frac{1}{p-1}$. Then $z \in \mathfrak{p}^m$ which is the same as saying that $v_\mathfrak{p}(z) \geq m$, since $v_\mathfrak{p}$ is normalized and so $v_\mathfrak{p}(z) > \frac{e}{p-1}$, which means that $v_p(z) > \frac{1}{p}$. Let us show that $\log(1+z) \in \mathfrak{p}^m$ by showing that $v_\mathfrak{p}(z) = v_\mathfrak{p}(\log(1+z))$. By what we showed above we have

$$v_p(\frac{z^k}{k}) - v_p(z) = (k-1)v_p(z) - v_p(k) > (k-1)(\frac{1}{p-1} - \frac{v_p(k)}{k-1}) \geq 0$$

Hence $v_\mathfrak{p}(\frac{z^k}{k}) > v_\mathfrak{p}(z)$ for all $k \in \mathbb{N}$. Thus, for all $s \in \mathbb{N}$ we have

$$v_\mathfrak{p}(A_s) \geq \min\{v_\mathfrak{p}(\frac{z^2}{2}), ..., v_\mathfrak{p}(\frac{z^s}{s})\}$$

with $A_s = \sum_{i=2}^{s} \frac{z^i}{i}(-1)^{(i-1)}$ meaning that $v_\mathfrak{p}(A_s) > v_\mathfrak{p}(z)$. It now follows from (7.1) that

$$v_\mathfrak{p}(z + A_s) = \min\{v_\mathfrak{p}(z), v_\mathfrak{p}(A_s)\} = v_\mathfrak{p}(z)$$

From this it follows that $v_{\mathfrak{p}}(z + A_s) \to v_{\mathfrak{p}}(z)$. We also know that $z + A_s \to \log(1+z)$ as $s \to \infty$ and $v_{\mathfrak{p}}$ is continuous so $v_{\mathfrak{p}}(z + A_s) \to v_{\mathfrak{p}}(\log(1+z))$. By uniqueness of limits we now have $v_{\mathfrak{p}}(z) = v_{\mathfrak{p}}(\log(1+z))$.

Let us now show that the power series for the exponential function converges on $\mathfrak{p}^m$ for $m > \frac{e}{p-1}$. Using Legendre's formula we get the following inequality

$$v_{\mathfrak{p}}(k!) = e(\lfloor \frac{k}{p} \rfloor + \lfloor \frac{k}{p^2} \rfloor + ...) < ek \sum_{i=1}^{\infty} \frac{1}{p^i} = \frac{ek}{p-1}$$

Let us again assume that $z \in \mathfrak{p}^m$. Then

$$v_{\mathfrak{p}}(\frac{z^k}{k!}) = kv_{\mathfrak{p}}(z) - v_{\mathfrak{p}}(k!) > k(v_{\mathfrak{p}}(z) - \frac{e}{p-1})$$

But $v_{\mathfrak{p}}(z) - \frac{e}{p-1} \geq 0$, so $v_{\mathfrak{p}}(\frac{z^k}{k!}) \to \infty$ for $k \to \infty$. Let us now move on to showing that exp maps $\mathfrak{p}^m$ to $U^{(m)}$. Maintaining the assumption that $z \in \mathfrak{p}^m$ we will do this by showing that $v_{\mathfrak{p}}(\exp(z) - 1) = v_{\mathfrak{p}}(z)$ since this implies that $\exp(z) - 1 \geq m$ meaning that $\exp(z) - 1 \in \mathfrak{p}^m$. Let us show that $v_{\mathfrak{p}}(\frac{z^k}{k!}) > v_{\mathfrak{p}}(z)$ for all $k > 1$. We have

$$v_{\mathfrak{p}}(\frac{z^k}{k!}) - v_{\mathfrak{p}}(z) = (k-1)v_{\mathfrak{p}}(z) - v_{\mathfrak{p}}(k!) > (k-1)v_{\mathfrak{p}}(z) - \frac{ek}{p-1} \geq 0$$

Hence $v_{\mathfrak{p}}(\frac{z^k}{k!}) > v_{\mathfrak{p}}(z)$ for all $k > 1$ and it now follows by an argument similar to one we gave a moment ago that $v_{\mathfrak{p}}(\exp(z) - 1) = v_{\mathfrak{p}}(z)$. We have the following equalities of formal power series

$$\exp\log(1+z) = 1 + z, \ \log\exp z = z$$

and when $z \in \mathfrak{p}^m$ these series converge so these are also equalities in K. (NEED TO SHOW THAT THIS IS ACTUALLY TRUE) □

12 Skolem's Method

Suppose that F is an irreducible, decomposable, nonfull form of degree m and consider the equation

$$F(x_1, ..., x_m) = c \qquad (\dagger)$$

where $c \in \mathbb{Q}$. Let us study the solutions to this equation. Because of our assumptions on F there exists a module M of rank m living inside some number field, K, of degree n, with $n > m$, so that $F(x_1, ..., x_m) = N_{K/\mathbb{Q}}(x_1\mu_1 + ... + x_m\mu_m)$, where the μ_i are in K and are generators for M. We are therefore interested in the elements $\alpha \in M$ so that

$$N_{K/\mathbb{Q}}(\alpha) = c$$

That is, we want a better understanding of the set M_c. We can safely assume that the generators for M are linearly independent over $\mathbb{Q}$. For if they were not we could just take a generating set for M which *are* linearly independent over $\mathbb{Q}$ and the form connected to this set would be equivalent to F. Extend now the μ_i's to a basis, $\mu_1, ..., \mu_m, \mu_{m+1}, ..., \mu_n$ for K over $\mathbb{Q}$. These elements generate a full module, M', and $M \subset M'$. Let now $\alpha \in M'$. We can then find a unique $\mathbb{Z}$-linear combination so that

$$\alpha = x_1\mu_1 + ... + x_n\mu_n$$

Thus, $\alpha \in M_c$ if and only if $\alpha \in M'_c$ and $x_{m+1} = ... = x_n = 0$. This restriction can be reformulated a bit. Let $\mu_1^*, ..., \mu_n^*$ be the dual basis of $\mu_1, ..., \mu_n$. The following computation shows that we can recover the value of x_i. For ease of notation we will write Tr instead of $\mathrm{Tr}_{K/\mathbb{Q}}$

$$\mathrm{Tr}(\mu_i^*\alpha) = \mathrm{Tr}(\sum_{j=1}^{n} \mu_i^* x_j \mu_j) = \sum_{j=1}^{n} x_j \mathrm{Tr}(\mu_i^*\mu_j) = x_i$$

Therefore the above restriction is the same as the requirement that

$$\mathrm{Tr}(\mu_{m+1}^*\alpha) = ... = \mathrm{Tr}(\mu_n^*\alpha) = 0$$

To be able to work more effectively with the trace, let $\sigma_1, ..., \sigma_n$ be the n embeddings of K into $\mathbb{C}$. By the primitive element theorem we know that $K = \mathbb{Q}(\beta)$ for some $\beta \in K$. Letting $N = \mathbb{Q}(\sigma_1(\beta), ..., \sigma_n(\beta))$ we get a subfield of $\mathbb{C}$ which is splitting field for the minimal polynomial for β over $\mathbb{Q}$ meaning that N is Galois over $\mathbb{Q}$, and it also has finite degree over $\mathbb{Q}$, which is another way saying that N is a number field. As M' is full we already have a description of M'_c. Let $\mathfrak{D}$ be the coefficient ring of M'. By (6.3) there exists a fundamental system of units $\epsilon_1, ..., \epsilon_t$ for $\mathfrak{D}$ and a finite set of elements $\Gamma := \{\gamma_1, ..., \gamma_k\} \subseteq M'_c$ so that

$$M'_c = \{\gamma\epsilon_1^{u_1}...\epsilon_t^{u_t} \mid \gamma \in \Gamma, (u_1, ..., u_t) \in \mathbb{Z}^t\} \qquad (\star)$$

Suppose that $\alpha \in M_c \subset M'_c$. Then we can write $\alpha = \gamma\epsilon_1^{u_1}...\epsilon_t^{u_t}$, where $\gamma \in \Gamma$ and we now have for all $i \in \{m+1, ..., n\}$ that

$$0 = \mathrm{Tr}(\mu_i^*\alpha) = \sum_{j=1}^{n} \sigma_j(\gamma\mu_i^*\epsilon_1^{u_1}...\epsilon_t^{u_t}) = \sum_{i=1}^{n} \sigma_j(\gamma\mu_i^*)\sigma_j(\epsilon_1)^{u_1}...\sigma_j(\epsilon_t)^{u_t} \qquad (\dagger\dagger)$$

From this we see that if $\#M_c = \infty$ then there has to exists some γ so that there are infinitely many possibilities for the $u_i \in \mathbb{Z}$. To make things easier for us we will allow u_i to take on values from a certain set containing the integers. More concretely, take a prime ideal, $\mathfrak{p}$, from the ring of integers of N. By 8.1 (ALSO MENTION THESE OBJECTS IN THE EXAMPLE WE ARE REFERENCING) we get the local field $N_\mathfrak{p}$ and its corresponding valuation ring and maximal ideal $O_\mathfrak{p}$ and $\hat{\mathfrak{p}}$ respectively. We want the u_i to take on values from $O_\mathfrak{p}$ but this does lead us to a problem, which is, fortunately for us, amendable.

The u_i occur as exponents of the $\sigma_j(\epsilon_i)$ in (††) and the only sensible way to define exponentiation of an element α is by defining

$$\alpha^u := \exp(u \log \alpha) \tag{$\star\star$}$$

But since we are working with the local field $N_\mathfrak{p}$, this is ill defined if we are not careful. Let κ be a natural number as in (**??**) so that the pair of functions $\log : U^{(\kappa)} \to \hat{\mathfrak{p}}^\kappa$ and $\exp : \hat{\mathfrak{p}}^\kappa :\to U^{(\kappa)}$, where $U^{(\kappa)} = 1 + \hat{\mathfrak{p}}^\kappa$ are mutual inverses. We now see that we can make the above definition, $\star\star$ make sense if we insist that $\alpha \in U^{(\kappa)}$ and that $u \in O_\mathfrak{p}$ since that way $u \log \alpha \in \hat{\mathfrak{p}}^\kappa$ as $\hat{\mathfrak{p}}^\kappa$ is an ideal. Suppose that we only know that $\alpha \in O_K$ and that $\mathfrak{p} \nmid \alpha$. We claim that $\alpha^q \in U^{(\kappa)}$ where $q = \#(O_\mathfrak{p}/\hat{\mathfrak{p}}^\kappa)$. The condition $\mathfrak{p} \nmid \alpha$ means that $\mathfrak{p}$ does not occur in the prime factorization of αO_K in O_K and that means that $\gcd(\alpha O_K, \mathfrak{p}) = O_K$ so also $\gcd(\alpha O_K, \mathfrak{p}^\kappa) = O_K$. But that means that $\alpha\beta + l = 1$ for some $l \in \mathfrak{p}^\kappa$ with $\beta \in O_K$, and so α is a unit in $O_K/\mathfrak{p}^\kappa$ so it is also a unit in $O_\mathfrak{p}/\hat{\mathfrak{p}}^\kappa$, (REFERENCE, maybe prop 8.6, the where we extend valuation on dedekind domain) meaning that $\alpha^q \equiv 1 \pmod{\hat{\mathfrak{p}}^\kappa}$ and so $\alpha^q \in U^{(\kappa)}$. In particular, if α is any unit in O_K then $\mathfrak{p} \nmid \alpha$ since $\alpha O_K = O_K$ and so $\alpha^q \in U^{(\kappa)}$. Thus, $\epsilon_i^q \in U^{(\kappa)}$ so $\sigma_j(\epsilon_i^q) \in U^{(\kappa)}$ (EXPLAIN THIS). Let $\Delta = \{\prod_{i=1}^t \epsilon_i^{\rho_i} \mid \rho_i \in \{0, ..., q-1\}\}$ and define $\Gamma' = \{\delta\gamma \mid (\delta, \gamma) \in \Delta \times \Gamma\}$. By letting $\phi_i = \epsilon_i^q$ we see that

$$M_c' = \{\gamma \phi_1^{v_1} ... \phi_t^{v_t} \mid \gamma \in \Gamma', (v_1, ..., v_t) \in \mathbb{Z}^t\}$$

Note that we have written M_c' on the same form as in ($\star$) - the only difference is that the ϵ_i have been swapped out with ϕ_i and that Γ has been swapped out with Γ'. Importantly, Γ' is, like Γ, also a finite subset of M_c' and all the ϕ_i are also independent units - although they do not necessarily constitute a fundamental system of units anymore, but we don't actually care about that in what follows. The upshot is that all the $\sigma_j(\phi_i)$ now belong to $U^{(\kappa)}$ which means that $\sigma_j(\phi_i)^u$ is now well defined for any $u \in O_\mathfrak{p}$. We can, and will, therefore without loss of generality, assume that the ϵ_i and the set Γ have been chosen in a way that allows us to make sense of (††) when the u_i take on values inside $O_\mathfrak{p}$. Having resolved this issue we can now define

$$L_j(u_1, ..., u_t) = \sum_{i=1}^{t} u_i \log \sigma_j(\epsilon_i)$$
$$A_{ij} = \sigma_j(\gamma \mu_i^*)$$

For $i = m+1, ..., n$ we now define

$$G_i(u_1, ..., u_t) = \sum_{j=1}^{n} A_{ij} \exp L_j(u_1, ..., u_t)$$

Note that the L_j can be thought of as power series in $P := N_\mathfrak{p}[u_1, ..., u_t]$. These have 0 constant term so it makes sense to consider the formal power series $\exp L_j(u_1, ..., u_t) \in P$. All of these have constant term 0 and therefore the

$G_i \in P$ also have constant term 0. The G_i also converge for all $(u_1, ..., u_t) \in O_\mathfrak{p}^t$, so the G_i are analytic functions. Observe that we can now rewrite (††) to

$$G_i(u_1, ..., u_t) = 0, \text{ for all } i \in \{m+1, ..., n\} \tag{†††}$$

Assume that there are infinitely many solutions in integers to (†). It follows there has to exists some $\gamma \in \Gamma$ so that there are infinitely many solutions $(u_1, ..., u_t) \in \mathbb{Z}^k$ to (†††) and these can be regarded as elements of $O_\mathfrak{p}^k$. Construct now a sequence of distinct solutions, $U_s = (u_{1s}, ..., u_{ts}) \in O_\mathfrak{p}^t$. As $O_\mathfrak{p}$ is compact, it follows from Tychonoff's theorem that O^t, equipped with the product topology, is also compact. But $O_\mathfrak{p}$ is a metric space so O^r is metrizable, (STATE THIS IN A THEOREM SOMEWHERE), and therefore it is sequentially compact. This means that the sequence U_s has a convergent subsequence, U_s^*, converging to a point, say $u^* = (u_1^*, ..., u_t^*) \in O_\mathfrak{p}^t$. As the G_i are analytic they are continuous (NEED A PROOF FOR THIS), we know that $G_i(U_s^*)$ converges to $G_i(u^*)$ for $s \to \infty$. But also $G_i(U_s^*)$ converges to 0 since $G_i(U_s^*) = 0$ for all $s \in \mathbb{N}$. By uniqueness of limits in metric spaces we therefore have $G_i(u^*) = 0$. Lastly, any neighborhood of u^* contains infinitely many solutions to (†††); Take any open ϵ-ball, B, with center u^*. Because U_s^* converges to u^*, we know that there is an $N \in \mathbb{N}$ so that $U_s^* \in B$ for all $s \geq N$, all of which are distinct and are solutions to (†††). Let us now write $u_i = u_i^* + v_i$, where $v_i \in O_\mathfrak{p}$. We get

$$\begin{aligned} G_i(u_1, ..., u_r) &= \sum_{j=1}^{n} A_{ij} \exp L_j(u_1^* + v_1, ..., u_r^* + v_r) \\ &= \sum_{j=1}^{n} A_{ij} \exp L_j(u_1^*, ..., u_r^*) \exp L_j(v_1, ..., v_r) \end{aligned}$$

Setting $A_{ij}^* = A_{ij} \exp L_j(u_1^*, ..., u_r^*)$ and $H_i(v_1, ..., v_r) = \sum_{j=1}^{n} A_{ij}^* L_j(v_1, ..., v_r)$, we get $G_i(u_1, ..., u_r) = H_i(v_1, ..., v_r)$. Consider

$$H_i(v_1, ..., v_t) = 0 \text{ for all } i \in \{m+1, ..., n\} \tag{††††}$$

Clearly, the point at the origin, $(0, .., 0)$, is a solution, so we can consider the local manifold V determined by this system and from what we showed above there are infinitely many solutions in any neighborhood of the origin. Therefore, by (??), V contains an analytic curve, meaning that there are formal power series $\omega_1(X), ..., \omega_t(X)$, which are non-zero, have constant term 0 and have coefficients in a finite extension of $N_\mathfrak{p}$ so that

$$H_i(\omega_1(X), ..., \omega_t(X)) = 0 \text{ for all } i \in \{m+1, ..., n\} \tag{$\triangle$}$$

We summarize what we have found in the following theorem.

Theorem 12.1. *If (†) has infinitely many solutions in integers, then there is some $\gamma \in \Gamma$ which gives rise to a local manifold defined by (††††) and this local manifold necessarily contains an analytic curve.*

(HERE WE SHOULD SAY WHAT THIS CAN BE USED FOR)
(THIS SHOULD NOT BE HERE)

Let us explore some consequences of this theorem. First of all, the matrix (A_{ij}^*) has full rank. This is because of the following. We know that the $\gamma\mu_i^*$ constitute a basis for K over $\mathbb{Q}$ and so the discriminant of this basis is non-zero. In fact the discriminant of this basis equals $|\sigma_j(\gamma\mu_i^*)|^2$. Since $A_{ij} = \sigma_j(\gamma\mu_i^*)$ all the rows of this matrix must be linearly independent over $\mathbb{Q}$, meaning that it has full rank, $n - m$.Since $A_{ij}^* = A_{ij}\exp L_j(u_1^*, ..., u_t^*)$, the matrix A_{ij}^* also has full rank. (WHY DO WE KNOW THIS).

For $j \in \{1, ..., n\}$ we define the formal power series $P_j(X) = L_j(\omega_1(X), ..., \omega_t(X)) \in N_\mathfrak{p}[X]$ and consider $N_\mathfrak{p}[X]$ as vector space over $N_\mathfrak{p}$. We claim that there is an $n - t \times n$ matrix, B, with linearly independent rows so that

$$\sum_{j=1}^{n} B_{ij}P_j(t) = 0, \text{ for all } i \in \{1, ..., n-t\},$$

Let $U = \text{span}\{\omega_1(X), ..., \omega_t(X)\}$ and notice that each L_j is in U. This means we can define the following linear map

$$T : N_\mathfrak{p}^n \to U$$

$$T(a_1, ..., a_n) = \sum_{i=1}^{n} a_i P_i$$

The dimension of U is at most t, so the rank of T is also at most t. By rank nullity, the nullity of T is therefore larger than or equal to $n-t$. In other words, there are at least $n - t$ linearly independent elements in the kernel of T and we can therefore construct an $n - t \times n$ matrix, B as desired.

Unpacking what $(\triangle)$ says we now have the two systems of equations

$$\sum_{j=1}^{n} A_{ij}^* \exp P_j(t) = 0, \text{ for all } i \in \{m+1, ..., n\} \tag{3}$$

$$\sum_{j=1}^{n} B_{ij}P_j(t) = 0, \text{ for all } i \in \{1, ..., n-t\}, \tag{4}$$

Consider the special case where $m = 2$ and $n \geq 3$ where at least one of the σ_i is a complex embedding. The existence of such an embedding is the same as saying that $2s \geq 1$ which is the same as saying that $n - t \geq 2$. Setting $n_1 = n - m$ and $n_2 = n - t$ the following lemma tells us that there are indices $k \neq l$ so that $P_k(t) = P_l(t)$. We shall use this when we start proving (12.2). Here's the lemma.

Lemma 12.1. *Let K be a field of characteristic 0 and let $n, n_1, n_2 \in \mathbb{N}$ so that $n_1 = n-2$ and $n_2 \geq 2$ and suppose we have formal power series, $P_1(t), ..., P_n(t)$,* *with coefficients in K, and with zero constant term so that*

$$\sum_{j=1}^{n} a_{ij} \exp P_j(t) = 0, \text{ for all } i \in \{1, ..., n_1\}$$

$$\sum_{j=1}^{n} b_{ij} P_j(t) = 0, \text{ for all } i \in \{1, ..., n_2\},$$

with the a_{ij} and b_{ij} in K and where both matrices (a_{ij}) and (b_{ij}) have K-linearly independent rows. Then there are two indices $k \neq l$ so that $P_k(t) = P_l(t)$.

Proof. (FIX THIS PROOF)

Let $V = \operatorname{span}_K\{\exp P_1, ..., \exp P_n\}$ and consider the linear map

$$T : K^n \to V$$

given by

$$T(a_1, ..., a_n) = \sum_{i=1}^{n} a_i \exp P_i$$

By assumption we have $n_1 = n - 2$ linearly independent elements $v \in K^n$ so that $v \in \ker T$. Hence nullity$(T) \geq n - 2$. The map T is clearly surjective. Combining this with rank-nullity we get rank$(T) = \dim V \leq 2$. Thus, it has to be the case that two elements among $\{\exp P_1, ..., \exp P_n\}$ span all of V. After potentially renumbering these elements we can safely say that these elements are $\exp P_{n-1}$ and $\exp P_n$. Thus, we can, in particular, for any $i = 1, ..., n-1$ find elements $a_i, b_i \in K$ so that

$$\exp P_i = a_i \exp P_{n-1} + b_i \exp P_n \tag{5}$$

where we trivially have that $a_{n-1} = 1$ and $b_{n-1} = 0$. Suppose now that $a_i = 0$. Then $\exp P_i = b_i \exp P_n$. But both P_i and P_n have no constant term and that means that $\exp P_i$ and $\exp P_n$ have constant term 1. Therefore, $b_i = 1$ and so $P_i = P_n$, in which case we are done. We can therefore from now on assume that $a_i \neq 0$ for all $i = 1, ..., n_1$, and we are therefore allowed to divide by this element. Let us now define, for $i = 1, ...n - 1$,

$$Q_i = P_i - P_n, \tag{6}$$

If we had $Q_i = 0$ we would again be done, so let us assume this never happens. As the power series $\exp P_i$ have non-zero constant term, they are units in $K[[t]]$. Of course, also the Q_i have constant term 0, so also $\exp Q_i$ are units in $K[[t]]$. Thus, we can divide by these elements. Combining (5) and (6) we have for $i = 1, ..., n-1$ that

$$\begin{aligned}
\exp Q_i &= \exp P_i \exp(-P_n) \\
&= (a_i \exp P_{n-1} + b_i \exp P_n) \exp(-P_n) \\
&= a_i \exp(P_{n-1} - P_n) + b_i \\
&= a_i \exp Q_{n-1} + b_i
\end{aligned}$$

Differentiating both sides of this equation gives us

$$Q_i' \exp Q_i = a_i Q_{n-1}' \exp Q_{n-1}$$

Solving for Q_i'

$$\begin{aligned} Q_i' &= \frac{(a_i Q_{n-1}' \exp Q_{n-1})}{\exp Q_i} \\ &= \frac{a_i Q_{n-1}' \exp Q_{n-1}}{a_i \exp Q_{n-1} + b_i} \\ &= \frac{Q_{n-1}' \exp Q_{n-1}}{\exp Q_{n-1} + c_i} \end{aligned} \tag{7}$$

where $c_i = a_i^{-1} b_i$. Let us now deal with the next group of equations. Let $U = \operatorname{span}\{P_1, ..., P_n\}$ and define the linear map $F : K^n \to U$ as $F(a_1, ..., a_n) = \sum_{i=1}^n a_i P_i$. By assumption, the nullity of this map is at least 2. Hence we can find two linearly independent elements $\alpha, \beta \in \ker F$. We can therefore find (EXPLAIN WHY) a non-trivial linear combination,

$$\sum_{i=1}^{n-1} d_i Q_i = 0$$

where the d_i are in K. Differentiating this sum and using (7) we obtain

$$\sum_{i=1}^{n-1} d_i Q_i' = Q_{n-1}' \exp Q_{n-1} \sum_{i=1}^{n-1} \frac{d_i}{\exp Q_{n-1} + c_i} = 0$$

It must be the case that $Q_{n-1}' \neq 0$. Otherwise, we would have $Q_{n-1} \in K$, and since the P_i have zero constant term, we would then have $Q_{n-1} = 0$, which is a contradiction. Also, $\exp Q_{n-1} \neq 0$ so we must have

$$\sum_{i=1}^{n-1} \frac{d_i}{\exp Q_{n-1} + c_i} = 0 \tag{8}$$

Next let us show that this implies that the rational function

$$f(z) = \sum_{i=1}^{n-1} \frac{d_i}{c_i + z}$$

is the zero function on K. As this is a rational function we can find polynomials $\phi, \psi \in K[z]$ so that $f(z) = \frac{\phi(z)}{\psi(z)}$. Let us for contradiction suppose that f is not identically zero. Then ϕ cannot be identically 0. But then because of (8) we now have (HOW ARE WE SURE THAT DENOMINATOR NOT ZERO)

$$0 = f(\exp Q_{n-1}) = \frac{\phi(\exp Q_{n-1})}{\psi(\exp Q_{n-1})},$$

meaning that $\phi(\exp Q_{n-1}) = 0$. But then ϕ cannot be a constant, since if it where it would have to be equal to 0. Thus, ϕ must have degree strictly larger than 0. But $\exp Q_{n-1} \in K((t)) \setminus K$, so $\exp Q_{n-1}$ is apparently algebraic over over K. But this is not possible (SHOW WHY). Hence f is identically 0. We then have $c_k = c_j$, where $k \neq j$ (WHY). Now from (5) we get

$$a_k^{-1} \exp P_k = \exp P_{n-1} + c_k \exp P_n$$
$$a_j^{-1} \exp P_j = \exp P_{n-1} + c_j \exp P_n$$

But since $c_k = c_j$ we conclude that

$$\exp P_k = a_k a_j^{-1} \exp P_j$$

But as we previously mentioned, both $\exp P_k$ and $\exp P_j$ have constant term 1 because P_k and P_j have zero constant term. Thus $a_k a_j^{-1} = 1$ and so $P_k = P_j$ as exp is injective (IS THIS REALLY TRUE). □

In total there are $N = (n-m) + (n-t)$ equations. So if $n - m \geq t$, then $N = (n-m) + (n-t) \geq t + (n-t) = n$.

Lemma 12.2. *Suppose K is a field and $f \in K((t))$. If $f \notin K$ then f is transcendental over K. That is, there exists no polynomial with coefficients in K having f as a root.*

Proof. Let $\omega : K((t)) \to \mathbb{Z}$ be defined by $\omega(\sum_{n=m}^{\infty} a_n x^n) = m$. Suppose that $f \in K((t)) \setminus K$. First, let us assume that $\omega(f) > 0$. Then the numbers $\omega(f^0), \omega(f^1), \omega(f^2)$... constitute a strictly increasing sequence in $\mathbb{Z}$. In particular, these are all different numbers. So if we have a K-linear combination

$$a_0 + a_1 f_1 + ... + a_n f^n = 0,$$

then we must have $0 = a_0 = ... = a_n$. A similar argument can be made when $\omega(f) < 0$ and thus f cannot be algebraic when $\omega(f) \neq 0$. Lastly, suppose that $\omega(f) = 0$. This means that f has a non-zero constant term, say $a_0 \in K$. For contradiction, assume that f is algebraic over K. Then also $f - a_0$ would be algebraic. But that cannot be the case since $\omega(f - a_0) > 0$ and so f is not algebraic. □

Theorem 12.2 (Thue)**.** *Suppose $f(x, y)$ is an irreducible form with integer coefficients, of degree $n \geq 3$ and with at least one complex root. Then there are only finitely many integer solutions to the equation $f(x, y) = c$, for some fixed $c \in \mathbb{Z}$.*

Proof. By assumption we can write

$$f(x, y) = \sum_{i=0}^{n} a_i x^i y^{n-i}$$

where the a_i are in $\mathbb{Z}$ and not all zero. We must have that $a_n \neq 0$. Otherwise y would divide $f(x, y)$ which is impossible since f is irreducible by assumption. Let $h(x) = f(x, 1)$. We have that h is a polynomial of degree n with leading coefficient a_n. The leading term of $a_n^{n-1}h(x)$ is $a_n^n x^n = (a_n x)^n$, so h can be regarded as a monic polynomial in the variable t using the substitution $a_n x \mapsto t$. So assume without loss of generality that h is monic, i.e. that $a_n = 1$. Let $K = \mathbb{Q}(\beta)$, where β is a root of h. This extension has degree n over $\mathbb{Q}$ since h is irreducible. Let now $\sigma_1, ..., \sigma_n$ be the n embeddings from K into $\mathbb{C}$ and set $N = \mathbb{Q}(\sigma_1(\beta), ..., \sigma_n(\beta))$. Since f is a form in two variables we know from (4.1) that f is decomposable. In fact we see from the proof of this proposition that

$$f(x, y) = N_{K/\mathbb{Q}}(x + \theta y)$$

We can now consider the module M of rank $m = 2$ generated by $\mu_1 = 1$ and $\mu_2 = \beta$. Since $n \geq 3$ we have $m < n$. This shows that f is a nonfull form. Assume now that f has infinitely many solutions in integers. We have just verified that f is an irreducible, decomposable and nonfull form so by (12.1) there is a local manifold given by (††††) which contains an analytic curve and this curve implies the existence of a solution in power series to a system of the type (3)

These are linearly independent over $\mathbb{Q}$ and we can extend them to a basis $\mu_1, ..., \mu_n$ for K over $\mathbb{Q}$. The modules M and M'

For any curve on $\omega_1(t), ..., \omega_r(t)$ on V we know from lemma (12.1) that $P_k(t) = P_j(t)$ for two different indices k and j. Consider then the local manifold, W, given by the equation

$$\prod_{i \leq k < j \leq n}^{r} (P_k(t) - P_j(t)) = 0$$

Hence, whenever we have a curve on V, that curve is also on W. By (???) this implies that $V \subseteq W$. We will now show that any neighborhood of the origin contains a point of V which is not in W. This is of course a contradiction to $V \subseteq W$, so there must be only finitely many solutions.

□

First show that all of these conditions are indeed satisfied.

It is clear that forms of degree 1 have infinitely many solutions. What about the forms of degree 2?

Consider the form $F(x, y) = x^2 - 2y^2$ and the equation

$$F(x, y) = 7$$

Suppose we already have a solution, (x, y). Then also $(3x + 4y, 2x + 3y)$ is a solution. Thus a single solution can inductively produce infinitely many distinct. But $(3, 1)$ is indeed a solution, and therefore $F(x, y) = 7$ has infinitely many solutions. This highlights the importance of the assumption that the degree of F must be greater than or equal to 3.

One might ask if the assumption that F has a complex root is really necessary and perhaps more interestingly, if all the solutions can be found. A big limiting factor about the statement we have proved is that we never know when we have found all solutions. This is of course expected, since this is just the nature of contradiction proofs - there are not constructive. But both of these questions can actually be answered if we look to [Baker(1975)], **Theorem 4.1** on page 38. Here we see that we can simply drop the assumption that there has to be a complex root and it is even possible to find all solutions.

References

[Baker(1975)] Alan Baker. *Transcendental Number Theory*. Cambride University Press, 1975. ISBN 978-1-009-22994-4.