Contents

1 Introduction to the problem **1**

2 Dual basis **1**

3 Formal power series **2**

4 Forms and Modules **4**

5 Coefficient rings and orders **8**

6 Solutions to $N(\mu) = a$, where μ is in a full module **9**

7 Only finite many solutions up to associates **9**

8 Fields with an absolute value **13**

9 Completions of fields **19**

10 Local manifold **30**

11 Local fields **32**

12 Logarithms and Exponentials **35**

13 Skolem's Method **37**
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 $\square$

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 forms in 2 variables are actually always decomposable. We shall use this fact once we start looking at

Thues theorem. (NOT SURE IF WE NEED A PROOF FOR THIS) Furthermore, 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 $\mathbb{Q}$. 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. Let F be the Galois closure of K and let $G = \text{Gal}(F/K)$ and let H be the subgroup of G corresponding to L. Set now $n = [G : H] = [K : \mathbb{Q}]$ and find $\sigma_1, ..., \sigma_n$ so that $G = \cup_{i=1}^{n} \sigma_i H$ is a disjoint union. We have that

$$\alpha = x_1\mu_1 + ...x_k\mu_k$$

with all the x_i in $\mathbb{Z}$. For ease of notation, let us denote by N the field norm $N_{K/\mathbb{Q}}$. We then see that

$$\begin{aligned} N(\alpha) &= N(x_1\mu_1 + ... + x_k\mu_k) \\ &= \prod_{i=1}^{n} \sigma_i(x_1\mu_1 + ... + x_k\mu_k) \\ &= \prod_{i=1}^{n} (x_1\sigma_i(\mu_1) + ... + x_k\sigma_i(\mu_k)) \end{aligned}$$

This can clearly be regarded as a homomgenous polynomial of degree n in the variables $x_1, ..., x_k$ and the coefficients are sums of products of the form $\prod_{i=1}^{n} \sigma_i(\mu_{\pi(i)})$ with π being a map from $\{1, ..., n\}$ into $\{1, ..., k\}$. Let now $\sigma \in G$. Now of course $\sigma\sigma_i \in G$ so there is some $j \in 1, ..., n$ so that $\sigma\sigma_i \in \sigma_j H$. If both $\sigma\sigma_i$ and $\sigma\sigma_{i'}$ were in $\sigma_j H$ then we would have $i = i'$ and therefore there is a permutation $\tau : \{1, ..., n\} \to \{1, ..., n\}$, depending on σ so that $\sigma\sigma_i \in \sigma_{\tau(i)} H$. In

other words, we can write $\sigma\sigma_i = \sigma_{\tau(i)}h_i$ for a suitable $h_i \in H$. But then

$$\begin{aligned}\sigma\prod_{i=1}^{n}\sigma_i(\mu_{\pi(i)}) &= \prod_{i=1}^{n}\sigma\sigma_i(\mu_{\pi(i)}) \\ &= \prod_{i=1}^{n}\sigma_{\tau(i)}h_i(\mu_{\pi(i)}) \\ &= \prod_{i=1}^{n}\sigma_{\tau(i)}(\mu_{\pi(i)}) \\ &= \prod_{i=1}^{n}\sigma_i(\mu_{\pi(i)})\end{aligned}$$

Thus, the element $\prod_{i=1}^{n}\sigma_i(\mu_{\pi(i)})$ is fixed by every single $\sigma \in G$ hence it must belong to $\mathbb{Q}$ so the coefficients of $N(\alpha)$ must belong to $\mathbb{Q}$ and hence it is a form. A form created in this way is called

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**.

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 the finitely generated free abelian groups, which means that concepts such as rank and basis now make sense for modules. In general, if we have a basis for N, say $\mu_1, ..., \mu_m$ and we choose to consider $\mathbb{Q}$-linear combinations of these, say

$$a_1\mu_1 + ... + a_m\mu_m = 0 \tag{1}$$

Then we can always find an integer $c \neq 0$ so that ca_i is an integer for all i. For example we can choose c to be th product of all denominators of the a_i, all of which are non-zero. So if $m > n$ then we would be able to choose at least one of the a_i to be non-zero. But that would mean that multiplying (1) by a suitable c would yield a non-trivial $\mathbb{Z}$-linear combination, which is a contradiction. Hence the rank of a module has to be smaller than or equal to n. If we have $m = n$, then N is a full module, because multiplication by $c \neq 0$ in (1) will give a $\mathbb{Z}$-linear combination of the μ_i's which is zero, which implies that the ca_i's are all zero, which forces the a_i to be zero. On the other hand, if N is a full module, then it has rank n since a basis for K over $\mathbb{Q}$ is in particular also linearly independent over $\mathbb{Z}$. But then the μ_i must be a basis for N, so it has rank n. Thus the full modules are exactly the modules of rank n, and the nonfull modules are those of rank less than n.

Once we have a module, we can of course consider the norm of the elements in it. Let $\sigma_1, ..., \sigma_n$ be the n embeddings of K into $\mathbb{C}$. We then have

$$N(x_1\mu_1 + ... + x_k\mu_k) = \prod_{i=1}^{n} \sigma_i(x_1\mu_1 + ... + x_k\mu_k) = \prod_{i=1}^{n} x_1\sigma_i(\mu_1) + ... + x_k\sigma_i(\mu_k)$$

Any term in this product occurs from choosing one of the k terms in each of the n factors, so multiplying this expression out, we get a homogenous polynomial in the variables $x_1, ..., x_n$. Let us think about what the coefficients of this polynomial are. Any term will have the form

$$x_{i_1}\sigma_1(\mu_{i_1}) \dots x_{i_n}\sigma_n(\mu_{i_n}) = x_{i_1}...x_{i_n}\sigma_1(\mu_{i_1})...\sigma_n(\mu_{i_n})$$

where the i_j signify which of the k terms in the n factors we chose. There could be many choices that lead to the same monomial, $x_{i_1}...x_{i_n}$. As such, the coefficient of this monomial will be

$$\sum_i \sigma_1(\mu_{i_1})...\sigma_n(\mu_{i_n})$$

where each i in the sum corresponds to a unique way of choosing the k terms in the n factors. Acting with an embedding on the set of all embeddings will simply permute them. Thus, acting with an embedding on the above sum will just permute the order in which the terms are added. Thus, the sum is fixed by all embeddings. But this means that all coefficients are fixed by every single embedding, which means that the coefficients are in $\mathbb{Q}$. Hence,

$$F(x_1, ..., x_k) = N(x_1\mu_1 + ... + x_k\mu_k)$$

is a form, and we call it the form associated to the generators $\mu_1, ..., \mu_k$, of the module. Since there may be many generators that lead to the same module, the forms achieved in this way may not be equal. However, it turns out that they are equivalent. If $\nu_1, ..., \nu_s$ is another set of generators for the same module, then we can write each ν_i as a $\mathbb{Z}$-linear combination of the μ_i's, i.e. for $j = 1, ..., s$, we have $\nu_j = \sum_{i=1}^{k} a_{ij}\mu_i$. Set for each $j = 1, ..., k$

$$x_j = \sum_{i=1}^{s} a_{ji}y_i$$

We see that

$$\sum_{i=1}^{s} y_i\nu_i = \sum_{i=1}^{s} y_i \sum_{j=1}^{k} a_{ji}\mu_j = \sum_{j=1}^{k}(\sum_{i=1}^{s} a_{ji}y_i)\mu_j = \sum_{j=1}^{k} x_j\mu_j$$

Which means that the forms associated to the generators $\mu_1, ..., \mu_k$ and $\nu_1, ..., \nu_s$ are equivalent.

We have seen that it is possible to construct forms from modules. The other direction is also possible. We have the theorem

Theorem 4.1.

Because of this correspondence between forms and norms of elements, we will now spend some more time investigating norms.

5 Coefficient rings and orders

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 $\mathfrak{D}_M$, or simply $\mathfrak{D}$, 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. We check that $\mathfrak{D}$ is a subring of K. First 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

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

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. 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 module since subgroups of modules are modules. But then also $\mathfrak{D} = \gamma^{-1}\gamma\mathfrak{D}$ is a module. Before we show that $\mathfrak{D}$ is full, we need the following small intermediate result.

Lemma 5.1. *Let M be a full module with basis $\mu_1, ..., \mu_n$. Then $\alpha\mu_i$ is in M for all 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. □

This allows us to prove the following lemma

Lemma 5.2. *Suppose M is a full module of K and suppose $\alpha \in K$. Then there exists an integer $c \neq 0$ so that $c\alpha$ is in the coefficient ring of M.*

Proof. Since M is full we can assume that $\mu_1, ..., \mu_n$ is not only a basis for M but also a basis for K over $\mathbb{Q}$. Then for each μ_i we can find a $\mathbb{Q}$ linear combination

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

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 i. By (5.1), we now have $c\alpha$ is in $\mathfrak{D}$. □

Lemma 5.3. *If M is a full module then there exists a non-zero integer b so that $bM \subseteq \mathfrak{D}$.*

Proof. By (5.2) we can find a non-zero integer c_i for every μ_i so that $c_i\mu_i$ is in $\mathfrak{D}$. We can then take b to be the product of all the c_i's. This will be a non-zero integer, satisfying that $b\mu_i$ is in $\mathfrak{D}$ for all i. It now follows from (5.1) that bx is in $\mathfrak{D}$ for all $x \in M$, meaning that that $bM \subseteq \mathfrak{D}$. □

This means that we can find non-zero integer b, so that $b\mu_1, ..., b\mu_n$ are all in $\mathfrak{D}$. This is clearly still a basis for K over $\mathbb{Q}$, which means that $\mathfrak{D}$ is full, and so $\mathfrak{D}$ is an order in K.

6 Solutions to $N(\mu) = a$, where μ is in a full module

Let $\mathfrak{D}$ be the coefficient ring of a full module M and assume that

$$N(\mu) = a,$$

for some μ in M. We have that $\epsilon\mu$ is in M if and only if ϵ is in $\mathfrak{D}$. So take now $\epsilon\mu \in M$ with $\epsilon \in \mathfrak{D}$. We get

$$N(\epsilon\mu) = N(\epsilon)N(\mu) = aN(\epsilon)$$

This means that a single solution to So if ϵ has norm 1, also $\epsilon\mu$ will be a solution. The units of $\mathfrak{D}$ are the elements with norm ± 1.

Maybe all we really need to show is what all of these solutions are like. Maybe we do not need all the other parts.

7 Only finite many solutions up to associates

Suppose we have a finite extension of fields, K/k. Multiplication by an element, α, in K can be regarded as a k-linear map, $\phi_\alpha(x) = \alpha x$, from K to itself, and we have that $\phi_\alpha^k(x) = \alpha^k x$, for $k \in \mathbb{N}$. Hence, $\phi_\alpha^k(1) = \alpha^k$. The characteristic polynomial, χ_{ϕ_α}, of ϕ_α is then a monic polynomial with coefficients in k and we have $\chi_{\phi_\alpha}(\phi_\alpha) = 0$. In words, this means that $\chi_{\phi_\alpha}(\phi_\alpha)$ is the zero map. Hence evaluating it in 1 gives a polynomial expression in α with coefficients in k which equals 0. This means that α is a root of χ_{ϕ_α}. We will therefore call the polynomial χ_{ϕ_α} the characteristic polynomial of α relative to the extension K/k.

If now K is instead a number field with degree n over $\mathbb{Q}$. If α now is an element in an order $\mathfrak{D} \subseteq K$, and $\mu_1, ..., \mu_n$ is a basis for $\mathfrak{D}$ then we can write each $\alpha\mu_i \in \mathfrak{D}$ as a linear combination with coefficients in $\mathbb{Z}$, which means that the matrix representation of $x \mapsto \alpha x$ has integer entries, so the characteristic polynomial of α has integer coefficients. But as we saw above, α is a root of this polynomial, which is monic. Hence α is an algebraic integer and therefore $\mathfrak{D}$ is a subring of the ring of algebraic integers, $\mathcal{O}$. We therefore already know some things about $\mathfrak{D}$. All its units are characterized by having norm ± 1, the norm

and trace of an element in $\mathfrak{D}$ are integers, and if $\alpha \in \mathfrak{D}$ then α divides $N(\alpha)$ in $\mathfrak{D}$. But perhaps more interestingly, Dirichlet's unit theorem generalizes to orders, such as $\mathfrak{D}$. We have the following result.

Theorem 7.1 (Dirichlet's unit theorem)**.** *Let $\mathfrak{D}$ 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*

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

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

Proof. THIS ARGUMENT IS PROBABLY TOO LONG. IT COULD BE REDUCED. Let $\mathcal{O}$ be the ring of algebraic integers in K. For the order $\mathcal{O}$ we know that the above theorem holds, so we get

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

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

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

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 $\mathfrak{D}$ and that $t' = t$. For the first claim, if we have any root of unity $\xi \in \mathfrak{D}$, 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 $\mathcal{O}/\mathfrak{D}$. Both of these have rank n, so this quotient is finite, and so we know that $f = [\mathcal{O} : \mathfrak{D}]$ is a natural number. Thus, if $x \in \mathcal{O}$ then $\overline{fx} = 0$ in $\mathcal{O}/\mathfrak{D}$ so $fx \in \mathfrak{D}$, so $f\mathcal{O} \subseteq \mathfrak{D}$. Of course $f\mathcal{O}$ is also a free abelian group of rank n, so again $R = \mathcal{O}/f\mathcal{O}$ is finite. But $f\mathcal{O}$ is also an ideal of the ring $\mathcal{O}$, so in fact R is a finite ring. Consider now any unit $\epsilon \in V$. Then ϵ is in $\mathcal{O}^*$, 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 $\alpha, \beta \in \mathcal{O}$. But as we argued above, $f\alpha$ and $f\beta$ both belong to $\mathfrak{D}$ and so $\epsilon^k \in \mathfrak{D}^*$. Thus, ϵ^k is either in W' or V' and the first option is impossible as that would imply that ϵ^k would also be in W. Therefore, ϵ^k is in V' so V/V' is finite meaning that $t' = t$. □

We say that two elements, α, β in a module M are **associated** if there is a unit $\epsilon \in \mathfrak{D}$ 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 7.2. *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 $M = \mathfrak{D}$. The ring $\mathfrak{D}$ is a full module so it is a free abelian group of rank n, hence isomorphic to $\mathbb{Z}^n$. Considering $\mathfrak{D}$ as an abelian group with respect to addition, the subgroup $c\mathfrak{D}$, is normal in $\mathfrak{D}$. We can therefore quotient out this subgroup to get the isomorphism

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

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

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

Denote by $\bar{\alpha}$ as the image of the canonical projection of α in $\mathfrak{D}/c\mathfrak{D}$ 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

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

given by $\phi(\bar{\alpha}) = [\alpha]$. Suppose $\bar{\alpha}, \bar{\beta}$ are in $\overline{M}_c/c\mathfrak{D}$ so that $\bar{\alpha} = \bar{\beta}$. Thus, α, β are in $\overline{M}_c$, so $|N(\alpha)| = |N(\beta)| = c$. We show that $[\alpha] = [\beta]$ - In other words, we show that α and β are associates. We have

$$\alpha = \beta + c\gamma = \beta + |N(\beta)|\gamma,$$

for some γ in $\mathfrak{D}$. But β divides $N(\beta)$ in $\mathfrak{D}$ so it also divides $|N(\beta)|$ in $\mathfrak{D}$. Hence, β divides α in $\mathfrak{D}$ and similarly α divides β in $\mathfrak{D}$. 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 $\#(\overline{M}_c/\sim) \leq \#\overline{M}_c/c\mathfrak{D}$, since each element in $\overline{M}_c/\sim$ has at least one preimage. Now the inclusion $\overline{M}_c/c\mathfrak{D} \subseteq \mathfrak{D}/c\mathfrak{D}$ implies that $\#(\overline{M}_c/\sim) \leq \#\overline{M}_c/c\mathfrak{D} \leq \#\mathfrak{D}/c\mathfrak{D} = c^n$. We will now prove the general statement. Suppose that M is a full module and that $\mathfrak{D}$ is the coefficient ring of M. Then $\overline{\mathfrak{D}}_c/\sim$ has finitely many elements. By use of (5.3), take now a non-zero integer b so that we obtain the inclusions

$$M \hookrightarrow bM \hookrightarrow \mathfrak{D}$$

It is clear that if α and β are associated then also $b\alpha$ and $b\beta$ are associated. Hence we get the inclusions

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

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 $\mathfrak{D}$.

Theorem 7.3. *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 $N(\epsilon) = 1$. □

We are therefore interested in finding the units in the ring of algebraic integers that have norm 1. We will first look at the roots of unity.

Theorem 7.4. *Let K be a number field of degree n over $\mathbb{Q}$. Suppose n is odd. Then the only roots of unity in $\mathcal{O}_K$ 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 $\mathcal{O}_K$ have norm 1.*

Proof. Suppose first that n is odd and let ζ be a primitive kth root of unity in $\mathcal{O}_K$. Then

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathcal{O}_K$$

As $\phi(k) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$, we have $\phi(k) \mid n$. Thus, $\phi(k)$ has to be odd. But this happens only when k is 1 or 2. Hence $\zeta = \pm 1$. We see that $N(-1) = (-1)^n = -1$. Next, assume that n is even. We then clearly have $1 = N(1) = N(-1)$. Take again $\zeta \in O_K$ to be a primitive kth root of unity. Then any embedding $\sigma : K \hookrightarrow \mathbb{C}$ must send ζ to a primitive kth root of unity $\mathbb{C}$. So if $k \geq 3$ then $\sigma(\zeta)$ is an imaginary number. This implies that there are no real embeddings, so $n = 2s$. All the embeddings come in complex conjugate pairs and so we can list them as: $\sigma_1, \overline{\sigma_1}, ..., \sigma_s, \overline{\sigma_s}$. We then have

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

□

Theorem 7.5. *Let K be a number field of degree $n = r + 2s$ over the rationals and let $c \in \mathbb{Z}$. Assume further that M is a full module with ring of coefficients $\mathfrak{D}$. Then there exists a system of fundamental units, $\epsilon_1, ..., \epsilon_r$ in $\mathfrak{D}$ and a finite*

set of elements $\gamma_1, ..., \gamma_k$ in M such that every element $\alpha \in M_c$ can be written as

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

for $i \in \{1, ..., k\}$ and $u_1, ..., u_t \in \mathbb{Z}$.

Proof. Using Dirichlet's unit theorem, we take a fundamental system of units of $\mathfrak{D}$, say $\epsilon_1, ..., \epsilon_t$ where $t = r + s - 1$ and by use of (???), let $\gamma_1, ..., \gamma_k$ be a system of representatives of the quotient set $M_c/\sim$. We split the proof into two cases. Suppose first that n is even. By the above (???) we know that the only primitive roots of unity are ± 1. So if any ϵ_i has norm -1, we can just swap it out with $-\epsilon_i$ to obtain a unit with norm 1. Modifying all such ϵ_i we obtain a new system of fundamental units, where each ϵ_i has norm 1, and so we can write every unit in $\mathfrak{D}$ with norm 1 as a product $\epsilon_1^{u_1} ... \epsilon_t^{u_t}$. Thus by (???) we can now write every $\alpha \in M_c$ as $\alpha = \gamma_i \epsilon_1^{u_1} ... \epsilon_r^{u_t}$. Suppose now n is odd. Then by (???) all the roots of unity have norm 1, so if it happens that all the ϵ_i also have norm 1, then all units have this property as well. Suppose now that $1 = N(\epsilon_1) = ... = N(\epsilon_q)$ and $-1 = N(\epsilon_{q+1}) = ... = N(\epsilon_t)$. Define then $\mu_i = \epsilon_i$ 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. Thus, 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 $\mathfrak{D}$. By the unit theorem, there are only finitely such ζ. Hence there are only finitely many, let's say h, numbers $\zeta \gamma_i$, where ζ is a root of unity. We can therefore list all of these, $\gamma_1', ..., \gamma_h'$ and by (???) write any element $\alpha \in M_c$ as

$$\alpha = \gamma_i' \mu_1^{u_1} ... \mu_r^{u_r}$$

□

8 Fields with an absolute value

Definition 8.1 (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

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

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

field. A field with a non-archimedian absolute value is called a non-archimedian valued field and similarly a field with an archimedian absolute value is called an archimedian 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 archimedian 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.

Proposition 8.1. *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 8.1. *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 8.2. *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 8.2. *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 8.3 (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-archimedian 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-archimedian 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-archimedian absolute values and valuations. As such, fields with non-archimedian 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-archimedian 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 8.4. *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 8.5 (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 8.3. *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* $n \geq 0$

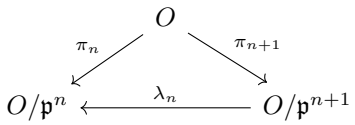
Proof. Suppose that v is discrete and normalized. Let now $x \in K^*$. Then $v(x) = m \in \mathbb{Z}$, since $v(K^*) = \mathbb{Z}$ by assumption, and so $v(x\pi^{-m}) = v(x) - mv(\pi) = 0$ meaning that $x\pi^{-1} \in O^*$. Thus $x\pi^{-1} = u$ for some $u \in O^*$ which means that $K^* = (\pi) \times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

□

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



Thus, we get a sequence of maps

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

This leads us the following definition.

Definition 8.6. *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 8.1. *The map* $O \to \lim_{\leftarrow} O/\mathfrak{p}^n$ *is an isomorphism of rings and a homeomorphism.*

9 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 9.1. *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 $d(x, y) = |x - y|$.*

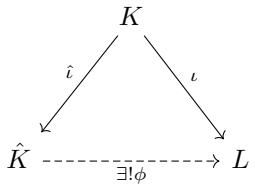
(Maybe we should say here that $\mathbb{Q}$ is dense in $\mathbb{R}$).

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 9.1. *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 $a \in A$. □

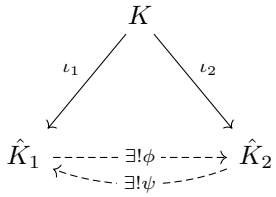
Definition 9.2 (Completion)**.** *Suppose $(K, |\cdot|)$ is a valued field. A completion of K is a complete valued field $\hat{K}$ together with a homomorphism $\hat{\iota} : K \to \hat{K}$ preserving the absolute value, satisfying the following universal property; If L is any other complete valued field 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*



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 9.2. *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



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 9.1. *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

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

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 9.3. *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 9.2 (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 $\hat{\iota}$ preserves the absolute value.*

- *K is dense in $\hat{K}$*
- *$\hat{K}$ is complete with respect to $|\cdot|'$*

Furthermore, the pair $(\hat{K}, \hat{\iota})$ 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 (9.3). 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 9.1. *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 (9.4) 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 9.4. *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 (8.1). □

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 9.3 (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 9.1 (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 □

Theorem 9.4. *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

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

Denote by $\alpha_1, ..., \alpha_d$ the d conjugates of α. Then we can write

$$f(x) = (x - \alpha_1)...(x - \alpha_d).$$

Setting $F = K(\alpha)$ we see that $a_0 = \pm\alpha_1...\alpha_d = N_{F/K}(\alpha)$. As such

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

where $m = [L : F]$. 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 9.5. *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 9.2. *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 $\alpha, \beta \in \mathcal{O}$, where $\beta \neq 0$.*

Proof. Let F be the field of fractions of $\mathcal{O}_K$. Then $F \subseteq K$ as F is the smallest field containing $\mathcal{O}_K$. 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 $d\alpha \in \mathcal{O}_K$, 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 9.3. $\mathrm{Frac}(R/\mathfrak{p})$ *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 9.6. *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*

$$\forall x \in O \setminus \{0\} : v_\mathfrak{p}(x) = m \iff (x) = \mathfrak{p}^m A,\ A \text{ an ideal of } O \text{ and } \mathfrak{p} \nmid A. \quad (2)$$

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 (9.3) it follows that $O/\mathfrak{p} \cong O_{(\mathfrak{p})}/\mathfrak{P}_{v_\mathfrak{p}}$. The other isomorphism is just (9.5).

(((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 9.2. *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 9.1. *Let K be a number field and pick a prime $\mathfrak{p}$ of O_K. From (9.2) 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 valuation on the completion, $K_\mathfrak{p}$. We know that $O_K/\mathfrak{p}$ is finite and that $\mathfrak{p}$ lies above a unique prime number $p \in \mathbb{Z}$ and we have $\mathfrak{p} = (p)O_K$. Hence $v_\mathfrak{p}(p) = 1$ so $v_\mathfrak{p}$ is discrete and normalized. Hence the valuation on $K_\mathfrak{p}$ is discrete and so it is a local field. In the special case where $K = \mathbb{Q}$ 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. Notice that we now have a field extension $K_\mathfrak{p}/\mathbb{Q}_p$ for every number field K and prime $\mathfrak{p}$ of K. It can be shown that this extension is finite.*

Lemma 9.4. *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 9.2. *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.*

10 Local manifold

Definition 10.1 (Analytic function)**.** *Suppose K is a complete field. A function, f, defined on a domain contained $C \subseteq K$, is called analytic if it can be represented as a power series which is convergent on C.*

Definition 10.2 (Local manifold)**.** *Suppose K is complete with respect to a valuation v, and let $|\cdot|$ be a corresponding absolute value. 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 $i = 1, ..., n$, we call an ϵ-neighborhood of the origin. Let $R = \overline{K}[[x_1, ..., x_n]]$ (WHAT IS THE RING OF COEFFICIENTS HERE?) denote the set of all format power series, $f(x_1, ..., x_n)$ with coefficients in $\overline{K}$ and let F be the set of all $f \in R$ so that f converges in some ϵ-neighborhood of the origin.*

Assume $f_1, ..., f_m \in F$ all of which have zero constant term. The set V of points $X \in \overline{K}^n$ such that

$$f_1(X) = ... = f_m(X) = 0$$

where X belongs to some ϵ-neighborhood of the origin is called a local manifold. We say that two local manifolds are equal if there is an ϵ-neighborhood in which they are the same.

Definition 10.3 (Curve)**.** *A curve in $\overline{K}^n$ is a collection of n power series, $\omega_1(t), ..., \omega_n(t) \in \overline{K}[[t]]$, not all identically zero, but with constant term zero. We say the curve lies on a manifold V, if for every $f \in I_V$ we have*

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

Proposition 10.1. *The set F in the definition above is actually a ring. Suppose V is a local manifold. The subset, $I_V \subseteq F$, given by*

$$I_V = \{f \in F \mid f(X) = 0 \text{ for all } X \in V\}$$

is an ideal of F.

Remark 10.1. *Recall that all the units in the ring of formal power series over a field are those that have constant term different from 0. So if we were to allow such formal power series in (10.2), then the ideal I_V would be the entire ring F, and so the quotient ring F/I_V would be the zero ring. This explains why we require the constant term of the power series to be zero.*

Theorem 10.1. *A local manifold is either equal to the set containing just the origin, or it contains a curve.*

Theorem 10.2. *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 10.2. *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 $V \subseteq V'$.*

EXPLAIN WHY: Elements in the quotient ring $\mathfrak{D}_\epsilon/I_V$ can be thought of as functions on the local manifold V.

11 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 11.1. *A field K is called a **local field** if it is complete with regards to a discrete valuation and has finite residue field.*

Proposition 11.1. *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 (9.4) 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 11.1. *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 $|H| \mid n$ meaning that $n = |H|k$ for some $k \in \mathbb{Z}$. As H is cyclic we have $x^{|H|} = 1$ and so $x^n = 1^k = 1$. □

Proposition 11.2. *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 (8.3) 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 (11.1) 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 11.2. *Let K be a local field with residue field $\kappa = \mathcal{O}/\mathfrak{p}$, and let $q = \#\kappa$. For any $n \in \mathbb{N}$ we have $\#(\mathcal{O}/\mathfrak{p}^n) = q^n$.*

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 $\#(\mathcal{O}/\mathfrak{p}^n) = q^n$. We have the isomorphism

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

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

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

□

Proposition 11.3. *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

$$|y_n - y_m| = |x_n - y_n + x_m - y_m + x_n - x_m| \tag{3}$$

A three fold application of the triangle inequality on the right hand side basically gives the result immediately. 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 11.1. *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 $\varprojlim \mathcal{O}/\mathfrak{p}^n$ which is then of course also closed. This inverse limit is contained in $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$, which is compact by Tychonoff's theorem since all the $\mathcal{O}/\mathfrak{p}^n$ are finite by (11.2), and hence they are compact. It follows that $\mathcal{O}$ is compact. □

Remark 11.1. *Since the absolute value K induces a metric on K, it means that compactness is equivalent to sequential compactness. Thus every sequence in $\mathcal{O}$ 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 11.4. *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 $u, \alpha \in \mathcal{O}$. Then the exponential function $\alpha^u = \exp(u \log \alpha)$ is well-defined whenever $u \in \mathcal{O}$ and $\alpha \in U^{(n)}$.*

Proof. Suppose that $u \in \mathcal{O}$ 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 11.3. *Suppose $\mathfrak{p}$ is a prime of a local field K and set $q = \#(\mathcal{O}/\mathfrak{p}^n)^*$. If $\alpha \in \mathcal{O}_K$ and $\mathfrak{p} \nmid \alpha$ then $\alpha^q \in U^{(n)}$. In particular, if ϵ is any unit of $\mathcal{O}_K$ then $\epsilon^q \in U^{(n)}$.*

Proof. First of all, the number q is a natural number by (11.2). Take α in $\mathcal{O}_K$ 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 $\alpha\mathcal{O}_K$, which means that $\gcd(\alpha\mathcal{O}_K, \mathfrak{p}) = \mathcal{O}_K$, hence also $\gcd(\alpha\mathcal{O}_K, \mathfrak{p}^n) = \mathcal{O}_K$. But that means that $\alpha\beta + l = 1$ for some $l \in \mathfrak{p}^n$ and $\beta \in \mathcal{O}_K$, and so α is a unit in $\mathcal{O}_K/\mathfrak{p}^n$. But then $\overline{\alpha^q} = \overline{1}$ in $\mathcal{O}_K/\mathfrak{p}^n$. Hence, $\alpha^q \in U^{(n)}$. Suppose now that ϵ is a unit in $\mathcal{O}_K$. Then $\epsilon\mathcal{O}_K = \mathcal{O}_K$, meaning that $\mathfrak{p} \nmid \epsilon$. By what we just proved, it now follows that $\epsilon^q \in U^{(n)}$. □

12 Logarithms and Exponentials

In this section, we describe how to define logarithmic and exponential functions on a p-adic field.

Lemma 12.1. *(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 12.2. *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 $\left\lfloor \frac{k}{p^i} \right\rfloor = 0$.

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

□

Proposition 12.1. *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 $(1 + x) \in U^{(1)}$ we have

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - ...$$

Proof. We first show that log actually converges on principal units. So suppose $(1+x) \in U^(1)$. Then $x \in \mathfrak{p}$ and so $v_p(x) > 0$, which means that $c = p^{v_p(x)} > 0$. Thus we can apply the usual logarithm and get $v_p(x) = \frac{\ln c}{\ln p}$. 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 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

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

Clearly, $\ln c^k/k \to \infty$ as $k \to \infty$. Hence, $v_p(\frac{x^k}{k}) \to \infty$ as $k \to \infty$. By (8.1), this means that the sum $x - \frac{x^2}{2} + \frac{x^3}{3} - ...$ converges. UNIQUENESS MISSING $\square$

13 Skolem's Method

In particular,

Since all the ideals of $\mathcal{O}$ are powers of the maximal ideal, and the maximal ideal is generated by a single element, so every ideal is finitely generated. As $\mathcal{O}$ is an integral domain, this means that it is in fact a Dedekind domain.

Lemma 13.1. *Suppose that K is a number field and that v is a discrete valuation on K. Denote by $\mathcal{O}_v$ the valuation ring of v. Then $\mathcal{O}_K \subset \mathcal{O}_v$. In particular, the valuation ring of the completion of K with respect to v contains $\mathcal{O}$.*

Proof. Let $\overline{R}^S$ denote the integral closure of R in S. We know that $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ inside of K and also that the ring of fractions of O_K is K. Furthermore, $\mathbb{Z} \subseteq \mathcal{O}_v$ and $\mathcal{O}_v$ is integrally closed in its field of fractions, F, since it is a Dedekin domain. We have something like

$$O_K = \overline{\mathbb{Z}}^K \subseteq \overline{\mathcal{O}_v}^K \subseteq \overline{\mathcal{O}_v}^F = \mathcal{O}_v$$

$\square$

We know from ? that there is an n so that $\exp : \mathfrak{p}^n \to U^{(n)}$ and $\log : U^{(n)} \to \mathfrak{p}^n$ are inverses of each other. By the above lemma, we know that the ring $\kappa_n = \mathcal{O}/\mathfrak{p}^n$ is finite, so also κ_n^* is finite. So if $\alpha \in \mathcal{O}$ is a unit then, since ring maps preserve units, $\bar{\alpha} \in \kappa_n$ is certainly also a unit. But then $\bar{\alpha}$ has finite order, since κ_n^* is finite. In other words, we can find $k \in \mathbb{N}$ so that $\bar{\alpha}^k = \bar{1}$. But this is really just another way of saying that α^k is in $U^{(n)}$.

Theorem 13.1. *Let K be a number field over $\mathbb{Q}$ of degree n and fix some $c \in \mathbb{Q}$. Suppose F is an irreducible, decomposable and nonfull form of degree $m < n$. If the equation*

$$F(x_1, ..., x_m) = c$$

has infinitely many solutions (OVER WHAT SET?) then there exists a local manifold in which there is an analytic curve that parametrizes an infinite set of solutions over the $\mathfrak{p}$-adic numbers.

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

$$F(x_1, ..., x_m) = c$$

Let k be a number field and let M be a non-full module generated by $\mu_1, ..., \mu_m \in k$. We can assume that these are linearly independent over $\mathbb{Q}$ since they could otherwise be replaced by a linearly independent set of generators.

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, K, which has finite degree, n, over $\mathbb{Q}$ and which is splitting field for the irreducible polynomial f. Hence K is a number field and is Galois over $\mathbb{Q}$. Let $\sigma_1, ..., \sigma_n$ be the elements of $\mathrm{Gal}(K/\mathbb{Q})$.

be a set of $\mathbb{Q}$-linearly independent elements of k. These generate a nonfull module, M. Starting from these generators we can build a basis for k over $\mathbb{Q}$. We will call this basis $\mu_1, ..., \mu_m, \mu_{m+1}, ..., \mu_n$. Considering the module, call it $\bar{M}$, generated by these will give us a full module and $M \subset \bar{M}$. We wish to find solutions to the equation $N(\alpha) = a$, where α is in M. This is really the same as allowing α to be in $\bar{M}$, so finding solutions of the form

$$\alpha = \sum_{i=1}^{n} x_i \mu_i$$

where the x_i are in $\mathbb{Z}$, with the added restriction that

$$x_{m+1} = ... = x_n = 0$$

Let now $\mu_1^*, ..., \mu_m^*$ be the dual basis of $\mu_1, ..., \mu_m$. The computation

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

shows that we can recover the x_i variables in α by taking the trace of $\mu_i^*\alpha$. We can use this to reformulate the above restriction to

$$\mathrm{Tr}(\mu_m^*\alpha) = ... = \mathrm{Tr}(\mu_n^*\alpha) = 0$$

Since α has norm a, we can write

$$\alpha = \gamma_k \epsilon_1^{u_1} ... \epsilon_r^{u_r} \tag{4}$$

Where $u_i \in \mathbb{Z}$, and γ is taken from a finite set of elements with norm a, and the ϵ_i is a system of independent units of K. Let $\sigma_1, ..., \sigma_n$ be the embeddings of K into $\mathbb{C}$. The restriction on the last $n-m$ variables can be written as

$$\mathrm{Tr}(\mu_i^*\alpha) = \sum_{j=1}^{n} \sigma_j(\gamma \mu_i^* \epsilon_1^{u_1} ... \epsilon_n^{u_r}) = \sum_{i=1}^{n} \sigma_j(\gamma_k \mu_i^*) \sigma_j(\epsilon_1)^{u_1} ... \sigma_j(\epsilon_n)^{u_r} = 0$$

for $i = m+1, ..., n$. If we can show that, no matter what γ we choose among the k possibilities, there are only finitely many possibilities for the u_i, the we would have established that there are only finitely many $\alpha \in M$ such that $N(\alpha) = a$. Right now, the u_i live in $\mathbb{Z}$. Take $\mathfrak{p}$ a prime divisor of the field K and let us see how we can extend the values of the u_i to the valuation ring $\mathcal{O} \subseteq K_{\mathfrak{p}}$.

The ϵ_i are all units of the coefficient ring $\mathfrak{D}$ of M. Hence, these are in fact units of O_K. By (???) there is natural number q so that ϵ_i^q is in $U^{(n)}$ for all i.

Each of the u_i in (4) can be written on the form $u_i = \rho_i + qv_i$, with $0 \leq \rho_i < q$ and $v_i \in \mathbb{Z}$. This allows us to write

$$\prod_{i=1}^{r} \epsilon_i^{u_i} = \prod_{i=1}^{r} \epsilon_i^{\rho_i + qv_i} = \prod_{i=1}^{r} \epsilon_i^{\rho_i} \prod_{i=1}^{r} \epsilon_i^{qv_i}$$

Setting $\delta = \prod_{i=1}^{r} \epsilon_i^{\rho_i}$, $\gamma' = \delta\gamma_k$ we can write $\alpha = \gamma_k' \epsilon_1^{qv_1} ... \epsilon_r^{qv_r}$. Let now Γ' be the set of all possible γ'. The number of possible δ is q^r so $\#\Gamma' = (\#\Gamma)q^r$. Of course, all elements in Γ' still have norm a. Hence taking $\phi_i = \epsilon_i^q$ we can write any element of norm a as

$$\alpha = \gamma \phi_1^{v_1} ... \phi_r^{v_r}$$

where $\gamma \in \Gamma'$ with the added benefit that we can now allow the v_i to take on any value in $\mathcal{O}$. This gives us the following lemma

Lemma 13.2. *There exists a finite set $\Gamma' \subseteq M_a$ and a system of independent units $\phi_1, ..., \phi_r \in U^{(n)}$, so that for any $\alpha \in M_a$ we can write*

$$\alpha = \gamma \phi_1^{v_1} ... \phi_r^{v_r},$$

where $\gamma \in \Gamma'$.

and so we can replace Γ with Γ'.
Now the set of all possible γ' is equa
Now we can allow the v_i to take on any value in $\mathcal{O}$.

However we can fix this using (??), and we will from now on just assume that it is. Define now

$$L_j(u_1, ..., u_r) = \sum_{k=1}^{r} u_k \log \sigma_j(\epsilon_k)$$
$$A_{ij} = \sigma_j(\gamma \mu_i^*)$$

We then have

$$\exp L_j(u_1, ..., u_r) = \prod_{k=1}^{r} \sigma_j(\epsilon_k)^{u_k}$$

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

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

And so we can rewrite our original equations as (AVOID TALKING ABOUT MANIFOLDS HERE BECAUSE WE DONT KNOW IF THE CONSTANT TERMS OF THE F_i ARE ZERO).

$$F_i(u_1, ..., u_r) = 0$$

for $i = m+1, ..., n$. These power series, F_i, converge in any ϵ-neighborhood around the origin as long as $\epsilon \leq 1$ since in that case the u_i belong to the valuation ring $\mathcal{O} \subseteq K_{\mathfrak{p}}$. Hence the set of all solutions to this system is a local manifold and all the u_i are in $\mathcal{O}$. Assume that we have infinitely many solutions to this system. Then we can construct an infinite sequence of distinct elements, $U_s = (u_{1s}, ..., u_{rs})$, for $s \in \mathbb{N}$. As $\mathcal{O}$ is compact, so is the product $\mathcal{O}^r$, equipped with the product topology. But $\mathcal{O}$ is a metric space so $\mathcal{O}^r$ is metrizable, and therefore sequentially compact. This means that the sequence U_s has a convergent subsequence, U_s^*, converging to a point, say $u^* = (u_1^*, ..., u_r^*) \in \mathcal{O}^r$. As the F_i are continuous, we know that $F_i(U_s^*)$ converges to $F_i(u^*)$. But the F_i also converge to 0 since $F_i(U_s^*) = 0$ for all $s \in \mathbb{N}$. By uniqueness of limits in metric spaces we therefore have $F_i(u^*) = 0$. Hence, u^* belongs to the manifold defined by the F_i. Lastly, any neighborhood of u^* contains infinitely many points of the manifold; Take any open ϵ-ball, B around u^*. Because U_s^* converges to u^*, we know that there is an N so that $U_s^* \in B$ for all $s > N$, all of which are distinct and belong to the manifold. Let us now write $u_i = u_i^* + v_i$, where $v_i \in \mathcal{O}$. Plugging this into the F_i we get

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

Setting $A^*_{ij} = A_{ij} \exp L_j(u^*_1, ..., u^*_r)$ and $G_i(v_1, ..., v_r) = \sum_{j=1}^n A^*_{ij} L_j(v_1, ..., v_r)$, we therefore get

$$F_i(u_1, ..., u_r) = G_i(v_1, ..., v_r)$$

Viewing the G_i as formal power series in the variables $u_1, ..., u_r$, we see that they all have constant term 0, since all the $L_j(v_1, ..., v_r)$ have constant term 0. Let V be the local manifold defined by the G_i. Clearly, the point at the origin is a solution, and there are infinitely many solutions in any neighborhood of the origin. Therefore V contains an analytic curve, by (??)

By the contrapositive of this, we now have a way to show that a norm equation has only finitely many solutions.

(THIS SHOULD NOT BE HERE)

We have the equations

We have $n - r = 2s$

There is an $n-r \times n$ matrix B with coefficients in K with linearly independent rows, so that

$$\sum_{j=1} A^*_{ij} \exp P_j(t) = 0 \text{ (for } i = m+1, ..., n)$$

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

The rows of A^*_{ij} are also linearly independent. Let us explain why, one system at a time. For the first one, we know that the $\gamma\mu^*_i$ constitute a basis for K over $\mathbb{Q}$. Hence the discriminant of this basis is non-zero. In fact the discriminant of this basis equals $|\sigma_j(\gamma\mu^*_i)|^2$ (p. 18 in Numberfields). Therefore, the matrix A_{ij} has full rank, $n-m$ and so also A^*_{ij}. Let us move on to the next system. Define $U = \text{span}\{\omega_1, ..., \omega_r\}$. As each P_i is in U, we can now define the linear map

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

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

The dimension of U is at most r. Hence the rank of T is also at most r. By rank nullity, the nullity of T is therefore larger than or equal to $n - r$. In other words, there are at least $n - r$ linearly independent elements in the kernel of T.

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

Theorem 13.2. *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 $c \in \mathbb{Z}$.*

One might think this should not take too much effort to prove. After all, the theorem is relatively simple to parse.

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 $a_n x \mapsto t$. Hence we can, and will, without loss of generality, assume that h is monic, i.e that $a_n = 1$. Furthermore, h is irreducible over $\mathbb{Q}$ since $f(x,y)$ is irreducible. Let now K be the splitting field of h. Then K is a Galois extension of $\mathbb{Q}$, and it has finite degree, n, over the rational. Let now $\sigma_1, ..., \sigma_n$ be the n embeddings of K into $\mathbb{C}$ and take a root, $\theta \in K$, of h. Such an element gives rise to a subfield, $F = \mathbb{Q}(\theta) \subseteq K$.

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

So in this case we are working with the module M generated by 1 and θ.

For any curve on $\omega_1(t), ..., \omega_r(t)$ on V we know from lemma (13.4) 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.

□

Lemma 13.3. *Suppose K is a field and $f \in K[[t]]$, f a unit. Then f is transcendental over K.*

Proof. MISSING □

Lemma 13.4. *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*

$$\sum_{j=1}^{n} a_{ij} \exp P_j = 0, \quad i = 1, ..., n_1$$

$$\sum_{j=1}^{n} b_{ij} P_j = 0, \quad i = 1, ..., n_2,$$

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

Proof. (FIX THIS PROOF)

Let $V = \text{span}_K\{\exp P_1, ..., \exp P_n\}$ 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 $\text{rank}(T) = \dim V \leq 2$. 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 $U = \text{span}\{P_1, ..., P_n\}$ 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).

□

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.