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

Theorem 0.1. *Suppose $f(x, y)$ is an irreducible form of degree $n \geq 3$. 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.

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.

Definition 0.1. *A field K equipped with a valuation, v, is said to be complete with respect to v, if every Cauchy sequence in K converges to an element in K.*

Theorem 0.2. *The valuation ring of 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, hence compact. It follows that $\mathcal{O}$ is compact. □

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. We will use this fact in section (?????)

1 Local manifold

Definition 1.1 (Local manifold). *Suppose K is complete with respect to a valuation v, and let $|\cdot|$ be a corresponding multiplicative valuation. 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 1.2 (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 1.1. *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.

Theorem 1.1. *A local manifold is either equal to the set containing just the origin, or it contains a curve.*

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

2 Forms and Modules

A form $F(x_1, ..., x_m)$ of degree k is a homogenous polynomial in the variables $x_1, ..., x_m$, of degree k with coefficients in $\mathbb{Q}$. If it splits into linear factors in some extension of $\mathbb{Q}$, then it is called decomposable. It is called reducible if it can be written as the product of two forms of lower degree. 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 $\mathbb{Q}$. This defines an equivalence relation on the set of forms. Consider the equation

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

where a is in $\mathbb{Q}$.

Once we know the solutions to one form, we can transform them into solutions of an equivalent form. Thus, we

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 the μ_i's are called the generators of the module. 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 inside K - This 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

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

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 2.1.

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

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 2.1. *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 2.2. *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 (2.1), we now have $c\alpha$ is in $\mathfrak{D}$. □

Lemma 2.3. *If M is a full module then there exists a non-zero integer b so that $bM \subseteq \mathfrak{D}$.*

Proof. By (2.2) 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 (2.1) that bx is in $\mathfrak{D}$ for all $x \in M$, meaning that that $bM \subseteq \mathfrak{D}$. $\square$

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.

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.

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 2.2 (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 $t' = t$. $\square$

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 2.3. *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 (2.3), 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 $M_c \subseteq \overline{M}_c$.

$\square$

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 2.4. *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 $N(\epsilon) = 1$. $\square$

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 2.5. *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

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

$\square$

Theorem 2.6. *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 $\mathfrak{O}$, 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 $\mathfrak{O}$ 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 $\mathfrak{O}$ can now be written as $\zeta \mu_1^{u_1}...\mu_t^{u_t}$, where ζ is a root of unity in $\mathfrak{O}$. 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

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

□

Completions of fields

Definition 2.1 (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* $x = 0$*. (Zero detection)*
- $|xy| = |x||y|$ *for every* $x, y \in K$*. (Multiplicativity)*
- $|x + y| \leq |x| + |y|$ *for every* $x, y \in K$*. (Triangle inequality)*

When the triangle inequality can be upgraded to the stronger condition

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

the absolute value is said to be ***non-archimedian****. Otherwise it is called* ***archimedian****.*

It is always possible define the trivial absolute value on a field, that is, the function that sends everything in K to 1 except for 0 which is sent to 0. This satisfies all the above criteria but does not lead to anything interesting, so we will not consider it.

Once we have an absolute value on field K, we can think about the topology it generates. It might very well happen that two absolute values generate the same topology and whenever this happens 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. We now turn to a notion that is closely related to absolute values - namely valuations.

Definition 2.2 (Valuation)**.** *A valuation on a field K is a function $v : K \to \mathbb{R} \cup \{\infty\}$ with the following properties*

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

We stipulated that these concepts 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 $q > 0$ we get a corresponding non-archimedian absolute value on K by setting $|x| = q^{-v(x)}$. No matter the choice of $q > 0$, all of these absolute values will be equivalent. In other words, they are all representatives of the same place. Thus, we will say that two valuations are equivalent if they correspond to the same place, giving us now an equivalence relation on the set of valuations on K. We can also go the other way around, so in fact there is a bijective correspondence between places and the equivalence classes of valuations on K.

Definition 2.3. *A valuation on a field K is called discrete if there is an element $\pi \in K$ so that $0 < v(\pi) \leq v(x)$ for every $x \in K$. Such an element π is called a prime element of the valuation, and if $v(\pi) = 1$ we say that v is normalized.*

Proposition 2.1. *The object*

$$\mathcal{O} = \{x \in K | v(x) \geq 0\} = \{x \in K | |x| \leq 1\}$$

is a ring with unity, called the valuation ring of K. It is in fact a local ring, with maximal ideal

$$\mathfrak{p} = \{x \in K | v(x) > 0\} = \{x \in K | |x| < 1\}$$

Hence the quotient ring $\mathcal{O}/\mathfrak{p}$ is a field and is called the residue field of K, and we typically denote it by κ. It follows that the units are

$$O^* = \mathcal{O} \setminus \mathfrak{p} = \{x \in K | v(x) = 0\} = \{x \in K | |x| = 1\}$$

If the valuation is discrete, then the valuation ring is a local Dedekin domain. If v is normalized and $\pi \in \mathcal{O}$ is a prime element then $(\pi) = \mathfrak{p}$ and all non-zero ideals are given by

$$\mathfrak{p}^n = \{x \in K | v(x) \geq n\}$$

for $n \geq 0$. Furthermore, the residue field is isomorphism to subsequent quotients of powers of $\mathfrak{p}$, i.e,

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

Proof. $\square$

Definition 2.4 (Complete valued field)**.** *We say that a valued field, K, with absolute value, $|\cdot|$, is complete if every Cauchy sequence in K converges to some element in K with respect to $|\cdot|$.*

Not all fields are complete valued fields. For example, $\mathbb{Q}$ is not complete with respect to the usual absolute value; For instance, one can find a Cauchy sequence converging to $\sqrt{2}$ which of course does not belong to $\mathbb{Q}$. There are many other such numbers, and adjoining all of them to $\mathbb{Q}$ gives us $\mathbb{R}$. This process can be thought of as filling out all the holes of $\mathbb{Q}$.

Intuitively, the completion of a field, K, is the smallest extension of K which is complete.

Theorem 2.7. *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 operations on R are defined element wise and it is therefore rather clear that R is a ring. The set I is non-empty, as it most certainly contains the constant sequence $0, 0, 0, \ldots$. 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, I is an ideal. NEED THE MAXIMAL IDEAL PART $\square$

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

$$\tilde{x} = (x, x, x, \ldots) + \mathfrak{m} \in \hat{R}$$

for any $x \in K$. This map is a homomorphism of fields and is thus injective. We can therefore think of K as a subfield of $\hat{R}$.

Definition 2.5 (Completion)**.** *Let K, R and $\mathfrak{m}$ be as above and define $\hat{R} = R/\mathfrak{m}$. There is a well defined function $|\cdot| : \hat{R} \to \mathbb{R}$, given by*

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

where x_n is a representative of $x \in \hat{R}$. We have the following properties

- *$|\cdot|$ is an absolute value on $\hat{R}$.*
- *$\hat{R}$ is complete with respect to $|\cdot|$.*
- *$|\cdot|$ is an extension of the absolute value on K.*

We say that the field $R/\mathfrak{m}$ is the completion of K with respect to the absolute value $|\cdot|$.

Proof. Suppose first that $x_n \in \mathfrak{m}$. We then know that x_n converges to 0 with respect to $|\cdot|$.

Suppose that $\bar{x}, \bar{y} \in \hat{R}$. Then $x - y \in \mathfrak{m}$ so $|x - y| = 0$, meaning that $|x| = |y|$. $\square$

Right now, we don't have an absolute value on $R/\mathfrak{m}$, so saying that this field is complete would not make much sense. But it turns out that the absolute value on K can be extended to $R/\mathfrak{m}$ and with respect to this absolute value, $R/\mathfrak{m}$ is indeed complete.

Example 2.1. *Consider an algebraic number field K and fix a prime $\mathfrak{p}$ of this field. For any $\alpha \in \mathcal{O}_K$ different from 0, we can consider the factorization*

$$\alpha\mathcal{O}_K = \mathfrak{p}^k A$$

where A is an ideal so that $\mathfrak{p} \nmid A$ and $k \in \mathbb{N}_0$. From this requirement, it follows that k is uniquely determined because we have unique prime factorization of ideals in Dedekin domains. This means that we now have a function,

$$v_{\mathfrak{p}} : \mathcal{O}_K \to \mathbb{Z},$$

once we formally define $v_{\mathfrak{p}}(0) = \infty$. This function can even be extended to all of K; For any $\frac{\alpha}{\beta} \in K$ we have $\alpha, \beta \in \mathcal{O}_K$ (DEMONSTRATE THIS) so we can define

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

This function is called the $\mathfrak{p}$-adic valuation of K and is non-archimedean. It is also discrete and normalized, since $v_{\mathfrak{p}}(\mathfrak{p}) = 1$ and this is the smallest possible value that is strictly positive. The completion of K with respect to this valuation is denoted by $K_{\mathfrak{p}}$. Let $\mathfrak{P}$ be the unique maximal ideal of $\mathcal{O}_{K_{\mathfrak{p}}}$. Consider the map

$$\mathcal{O}_K \to \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{P}$$

We show that the residue field $\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{P}$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}$. We have the surjective ring homomorphism given by the natural projection,

To verify this, we only need to show that the residue field $\mathcal{O}_{\mathfrak{p}}/\mathfrak{P}$, where

We can then define the function

Lemma 2.4. *Let $||$ be a non-achimedian absolute value on a field K and let v be an additive valuation corresponding to $||$. 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. *$|y_n| \to 0$ as $n \to \infty$.*
3. *$v(y_n) \to \infty$ as $n \to \infty$.*

Proof. A sequence being Cauchy clearly implies that y_n converges to 0. For the next implication, consider that $v(x) = -\log|x|$ by definition (IS THIS REALLY THE CASE). For the last implication, (FIX THIS PROOF)

Let $N \in \mathbb{N}$ be so large that makes $|y_n| \leq \epsilon$. Suppose now $n > m > N$. We obtain

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

□

In particular, we can use this lemma to show that a sum $\sum_{n=1}^{\infty} x_n$ converges by showing that the individual terms x_n converge to 0. This is certainly not something we can do in the archimedian setting - consider for example the harmonic series.

To show that a sequence converges, one can use both the exponential and the multiplicative valuation.

3 Logarithms and Exponentials

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

Lemma 3.1. *(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 3.2. *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 3.1. *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

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

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

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

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 (2.4), this means that the sum $x - \frac{x^2}{2} + \frac{x^3}{3} - ...$ converges. UNIQUENESS MISSING □

Skolem's Method

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 3.2. *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 3.3. *Suppose $\mathfrak{p}$ is a prime of 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. 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 $\alpha\beta + q = 1$ for some $q \in \mathfrak{p}^n$ and $\beta \in \mathcal{O}_K$, and so α is a unit in $\mathcal{O}_K/\mathfrak{p}^n$. But

$\mathcal{O}_K/\mathfrak{p}^n$ is finite, which means that $\overline{\alpha^q} = \overline{1}$ in $\mathcal{O}_K/\mathfrak{p}^n$ where $q = \#(\mathcal{O}_K/\mathfrak{p}^n)^*$. 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 $\mathfrak{p} \nmid \epsilon$. □

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 3.4. *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

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

□

Definition 3.1. *A field K is called a **local field** if it is complete with regards to a discrete valuation and has finite residue field.*

Proposition 3.3. *A local field of characteristic 0 is the same thing as a finite extension of $\mathbb{Q}_p$.*

Lemma 3.5. *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

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

□

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 $U^{(n)}$.

Let K be a number field of degree n and let $\mu_1, ..., \mu_m$ 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

$$\alpha = \gamma_k \epsilon_1^{u_1} ... \epsilon_r^{u_r} \tag{2}$$

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.

Consider the set

$$\{\epsilon_1^{u_1} \dots \epsilon_r^{u_r} \mid 0 \leq u_i < q\}$$

$$G = \{\gamma \mid \gamma_1, ..., \gamma_k\}$$
$$B = \{\epsilon_i^{qu_1} \dots \epsilon_r^{qu_r} \mid u_i \in \mathbb{Z}\}$$
$$C = \{\epsilon_1^{u_1} \dots \epsilon_r^{u_r} \mid u_i \in \mathbb{Z}\}$$
$$A \times B \to C$$

Each of the u_i in (2) can be written on the form $u_i = \rho_i + qv_i$, with $0 \le \rho_i < q$ 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 $\delta = \prod_{i=1}^{r} \epsilon_i^{\rho_i}$, $\gamma_k' = \delta\gamma_k$ and $\phi_i = u_i$ we can write $\alpha = \gamma_k \delta \phi_1^{v_1} ... \phi_r^{v_r}$.
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

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

And so we can rewrite our original equations as for $i = m+1, ..., n$

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

These are power series in the variables $u_1, ..., u_r$, and they all converge as long as the u_i belong to $\mathcal{O}$. Hence the set of all solutions to this system is a local manifold.