Contents

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 fraction field, 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 of $\mathbb{Q}$, then it is called decomposable. The forms in 2 variables are actually always decomposable.

Theorem 4.1. *Let $F(x, y)$ be a form of degree k in two variables and let α be any root of $F(x, 1)$. Then*

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

In particular, F is decomposable.

Proof. We can assume without loss of generality that $F(x, 1)$ is monic. Start by writing

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

where the a_i are in $\mathbb{Q}$. Since $F(x, 1)$ is monic we have $a_k = 1$. Now

$$F(x, 1) = \sum_{i=0}^{k} a_i x^{k-i}$$

Which can be written as

$$\prod_{i=1}^{k} (x - \alpha_i)$$

in the splitting field for $F(x, 1)$. The coefficients are symmetric functions of the roots, which we denote by $s_1(\alpha_1, ..., \alpha_k), ..., s_k(\alpha_1, ..., \alpha_k)$. Notice that $s_i(\alpha_1, ..., \alpha_k)$ is a monomial of degree i in the variables α_i. Hence $s_i(\alpha_1 y, ..., \alpha_k y) = y^i s_i(\alpha_1, ..., \alpha_k)$ become the coefficients of

$$\prod_{i=1}^{k} (x - \alpha_i y)$$

But these are exactly the coefficients of $F(x, y)$, when regarded as a polynomial in x with coefficients in $\mathbb{Q}[y]$. Thus, the above expression is in fact equal to $F(x, y)$ and is a factorization of it in terms of linear factors and hence it 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

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

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 4.2.

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 $x = 0$. (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

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

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. For convenience we will typically just say that $(K, |\cdot|)$ is a valued field.*

Sometimes we will be working with two valued fields, K and F. To distinguish the absolute values on these fields we will write $|\cdot|_K$ and $|\cdot|_F$. The usual absolute value on $\mathbb{R}$ is an example of a non-archimedian absolute value, so $\mathbb{R}$ is an example of a valued field. We will denote this absolute value by $|\cdot|_\infty$. If it happens to be the case that K is a field extension of F, we will say that the absolute value on K extends (or preserves) the absolute value on F if $|\cdot|_K$ restricted to F is the same function as $|\cdot|_F$. In this case we will typically not be explicit about which absolute value we are using - instead we will just write $|\cdot|$.

Proposition 8.1. *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 $|\phi(x)|_L = |x|_K$.*

Proposition 8.2. *Let K, L be valued fields and suppose $\phi : K \to L$ is a homomorphism, preserving absolute values. Then ϕ is uniformly continuous.*

Proof. This follows from the fact that $|\cdot|_K$ is uniformly continuous and that

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

□

Once we have an absolute value on field K, we can of course 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 on K induce 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.

Note that it is always possible to define at least one absolute value on any given field. namely the function sending everything in a field to 1 except for 0 which is sent to 0. This satisfies all the above criteria but does not lead to anything interesting. For example, it induces the discrete topology on K. For this reason we will not consider it.

We now turn to a notion that is closely related to 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*

- *$v(x) = \infty$ 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 $x, y \in K$.*

(NOT SURE ABOUT EVERYTHING WRITTEN HERE) 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 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. 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 non-archimedian places and the equivalence classes of valuations on K.

Definition 8.4. *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 8.3. *(MENTION HERE THAT WE CAN TAKE ANY EQUIVALENT VALUATION OR ABSOLUTE VALUE ON K) 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 PID. 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 $n \geq 0$. In particular, $\mathcal{O}$ is a local Dedekin domain. Furthermore, the residue field is isomorphic to subsequent quotients of powers of $\mathfrak{p}$, i.e,

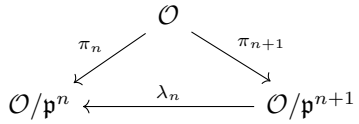
$$\mathcal{O}/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}$$

Proof. □

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

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

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

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

We are now ready to define the projective limit, which will turn out to be the same thing as $\mathcal{O}$.

Definition 8.5. *The set*

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

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

Because of the commutative diagram above we obtain a ring map

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

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

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

9 Completions of fields

As soon as we have a metric on a field K we can start to talk about convergence of sequences in this field. It is possible that every imaginable Cauchy sequence converges to some element in K. Such a field is called a complete field and not all fields are complete. For fields which are not complete there are points where there exist no sequences converging to them. These points can in a sense be thought of as holes of K, with respect to the metric. The completion of a field is essentially the process of patching up all these holes without adding anything unnecessary. Let's try to be a little more precise about these concepts.

Definition 9.1 (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* $|\cdot|$*.*

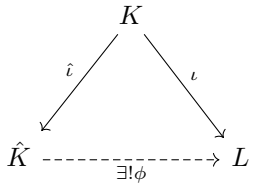
$\mathbb{R}$ equipped with the standard absolute value is an example of a complete valued field. In fact, $\mathbb{R}$ is the completion of $\mathbb{Q}$. We will get to this later when we have properly defined the completion of a field.

Definition 9.2 (Closed set in a metric space)**.** *Let* X *be a metric space and* $A \subseteq X$*. The set* A *is closed if it contains all of its limit points. That is, whenever there is a sequence in* A *converging to some point* $a \in X$ *then* $a \in A$*.*

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 9.3 (Completion)**.** *Suppose K is a field with absolute value, $|\cdot|$. The* ***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*



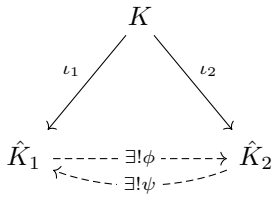
The map ϕ in the diagram above is actually uniformly continuous since it preserves absolute values and is ring map. Note also that we speak about *the* completion, as if there is only one possible extensions of K making the diagram commute. This is not entirely accurate, but still accurate enough to justify the use of the word. It turns out that fields satisfying the condition in the definition above are unique up to unique isomorphism. This is a quite strong statement - much stronger than just being unique up to isomorphism. But proving it turns out to be quite simple and in fact it can be done in category-theoretic language; $\hat{K}$ is an initial object in the coslice category with respect to K and initial objects are always unique up to unique isomorphism. However, we will do this using a more hands on approach.

(FIND A REFERENCE FOR THIS)

Proposition 9.2. *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 $\tilde{f} : X \to Y$.*

Proposition 9.3. *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 $\iota_2 = \phi \circ \iota_1$. □

There is another, perhaps more down-to-earth way of characterizing the completion of a field.

Proposition 9.4. *Let K be a valued field, $\hat{K}$ a complete valued field and $\hat{\iota} : K \to \hat{K}$ a homomorphism preserving the absolute value. Then $\hat{K}, \hat{\iota}$ is the completion of K if and only if K is dense in $\hat{K}$.*

Proof. Assume first that the pair $(\hat{K}, \hat{\iota})$ is in fact the completion of K and let us show that K is dense in $\hat{K}$, by which we of course mean that the image $\hat{\iota}(K)$ is dense in $\hat{K}$. In the same vein, when we write $\overline{K}$ we really mean $\overline{\hat{\iota}(K)}$. Now, as $\hat{K}$ is complete also $\overline{K}$ is complete, since it is closed. Also, $\overline{K}$ is a subfield of $\hat{K}$ (SHOW THIS). In other words we have the inclusion map $\psi : \overline{K} \to \hat{K}$ which is of course a homomorphism, satisfies $\psi \circ \hat{\iota} = \hat{\iota}$ and preserves the absolute value. Hence ψ is in particular continuous and it is clear that $\hat{\iota}(K)$ is dense in $\overline{K}$. Hence ψ is uniquely determined by the condition $\psi \circ \hat{\iota} = \hat{\iota}$. This shows that $(\overline{K}, \hat{\iota})$ satisfies the same universal property as $(\hat{K}, \hat{\iota})$ and hence $(\overline{K}, \hat{\iota})$ is the completion of K.

Let us now prove the converse. So suppose that $\hat{\iota}(K)$ is dense in $\hat{K}$ and that (L, ι) is a pair as in (**??**). Let us try to 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 $(\hat{\iota}(x_n)) = (y_n)$. As ι preserves the absolute value the sequence (x_n) is also Cauchy. As ι preserves the absolute value on K, 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, λ'. By uniqueness of limits we therefore obtain a well defined map $\phi : \hat{K} \to L$ and by construction we have $\phi \circ \hat{\iota} = \iota$. It preserves absolute values since

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

Therefore ϕ is continuous and the condition $\phi \circ \hat{\iota} = \iota$ makes ϕ uniquely determined. The map ϕ is also a ring map because the limit of the sum of two Cauchy sequences is the sum of the limits of the sequences and similarly for the product of two Cauchy sequences. Thus the pair $(\hat{K}, \hat{\iota})$ is the completion of K. □

As we can see, the completion has some rather nice properties - if it exists, that is. This we haven't demonstrated yet. All we have done so far is to suppose that it exists and derived some consequences of that. So our next goal will be to construct a field that actually satisfies the property of being the completion of a field. The process of constructing such an object is very similar to the idea of the concrete construction of 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 operations on R are defined element wise and it is therefore follows from analysis that R is a ring. The set I is non-empty, as it most certainly contains the constant sequence $\tilde{0}$. 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. Let us now show that I is a maximal ideal. Take an element in $x_n \in R$ which is not also in I. We wish to show that the ideal $J = (x_n) + I$ contains $\tilde{1}$, 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

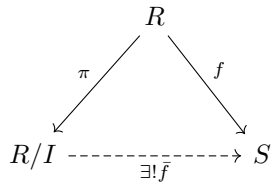
$$\tilde{x} = (x, x, x, ...) + \mathfrak{m} \in \hat{K}$$

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 $\hat{K}$. The field $\hat{K}$ is exactly the object we have been looking for - it is actually the completion of K. To do this we will need a little help from the following proposition.

Proposition 9.5. *(Universal property for quotients) Let R, S be a rings and $I \subseteq R$ an ideal. Suppose we have a function $f : R \to S$, which vanishes on I and is an additive group homomorphism when restricted to I. Then there exists a uniquely determined function*

$$\bar{f} : R/I \to S$$

such that the following diagram commutes



In this case we say that f descends to the quotient, R/I. If f is a ring map then so is $\bar{f}$.

Proof. If there is a map $\bar{f}$ so that the diagram commutes then what that means is that we have, for all $r \in R$

$$\bar{f}(\pi(r)) = f(r)$$

But π is surjective so this condition forces how $\bar{f}$ is defined, and hence $\bar{f}$ is unique if it exists. Suppose now that $x, y \in R$ so that $\bar{x} = \bar{y}$. Then $x - y \in I$ and so $f(x - y) = 0$, so $f(x) = f(y)$ as f is an additive homomorphism when restricted to I. Hence $\bar{f}$ is well defined. If f is a ring map, then $\bar{f}$ also be a ring map because the diagram commutes. □

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 $\phi : R \to \mathbb{R}$, given by*

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

descends to a unique function, $|\cdot|'$, on the quotient $\hat{K} = R/\mathfrak{m}$. We have the following properties

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

Proof. Let us first show that ϕ descends to a unique 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. Hence the map ϕ is well defined. Suppose that $(x_n) \in \mathfrak{m}$. Then x_n converges to 0 so $|x_n|$ converges to $0 \in \mathbb{R}$ as $|\cdot|$ is continuous. In other words, the map ϕ vanishes on $\mathfrak{m}$. If $(x_n), (y_n) \in \mathfrak{m}$ then by the triangle inequality we get

$$|x_n + y_n| \leq |x_n| + |y_n|$$

But the right hand side converges to 0, and $0 \leq |x_n + y_n|$ so ϕ is an additive group homomorphism when restricted to $\mathfrak{m}$. So by the universal property for quotients, ϕ descends to a unique function, $|\cdot|'$ on the quotient $\hat{K}$. Let us now prove that $|\cdot|'$ is actually an absolute value on K. Let us first show that it possesses the zero-detection property. Suppose $x = \overline{(x_n)} \in \hat{K}$ so that $|x|' = 0$. As $|\cdot|$ is continuous we have

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

But $|\cdot|$ is an absolute value on K so we must have $\lim_{n\to\infty} x_n = 0$ and therefore $(x_n) \in m$ meaning that $x = 0$. For the converse, ϕ vanishes on $\mathfrak{m}$. Thus if $x \in \hat{K}$ we have $|x|' = 0$ if and only if $x = 0$. The remaining properties for $|\cdot|'$ to be an absolute value are simply inherited from the absolute value $|\cdot|$ on K. It is also easily seen that $|\cdot|'$ extends $|\cdot|$. For if $x \in K$ then

$$|x| = \lim_{n\to\infty} x = \phi(\tilde{x}) = |\overline{\tilde{x}}|'$$

(IS IT OKAY TO JUST CONSIDER THE POINT 0) Let us now show that K is dense in $\hat{K}$. What we mean by this is that the image of K under the map $x \mapsto \tilde{x}$ 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. As (x_n) is Cauchy we can find $N \in \mathbb{N}$ so that $|x_n - x_m| < \epsilon/2$ for all $m, n \geq N$. Define now the constant sequence $y = (x_N)$. Now, 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 $lambda_i$, we can find an element $y_i \in K$ so that $|\lambda_i - \tilde{y}_i|' < \frac{1}{i}$. This way we get a sequence $(\tilde{y}_n)$ in $\hat{K}$ and we observe that

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

Hence, by MISSING $(\tilde{y}_n)$ 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

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

and we are therefore done. □

Remark 9.1. *Because $|\cdot|'$ is an extension of $|\cdot|$, we will, for ease of notation, simply denote $|\cdot|'$ by $|\cdot|$.*

Let us now look at some examples. We have already mentioned that $\mathbb{R}$ is the completion of $\mathbb{Q}$. We have the inclusion $\mathbb{Q} \to \mathbb{R}$ which preserves absolute values, so this statement follows if we are willing to accept that $\mathbb{R}$ is complete and that $\mathbb{Q}$ is dense in $\mathbb{R}$. Here is another example. Suppose that K is a field and consider the formal power series $K[[x]]$. As we have mentioned already this is a local ring with maximal ideal $\mathfrak{p} = (x)$. Consider the valuation $v_m frakp$ on $K[[x]]$ defined by

Theorem 9.3 (Ostrowski)**.** *Suppose that K is field which is complete with respect to an archimedian valuation. Then there is an isomorphism σ from K into $\mathbb{R}$ or $\mathbb{C}$ and a constant $s \in (0, 1]$ so that*

$$|x| = |\sigma(x)|^s$$

for all $x \in K$.

Lemma 9.1. *Let K be a field with a valuation v and let $\hat{K}$ be the completion of K. We have*

$$v(K) = \hat{v}(\hat{K})$$

Thus, $\hat{v}$ is discrete and normalized if v is.

Lemma 9.2. *Let K be a number field. The fraction field of $\mathcal{O}$ 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 fraction field of $\mathcal{O}$. Then $F \subseteq K$ as F is the smallest field containing $\mathcal{O}$. 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 $F = K$. □

Proposition 9.6. *Let R be a Dedekind domain and K its field of fractions. For any prime $\mathfrak{p}$ of R there exists a valuation $v_\mathfrak{p}$ on R that extends to a valuation on K. This valuation is called the $\mathfrak{p}$-adic valuation.*

Valuation on Dedekind domains. For any $\alpha \in R$ different from 0, we can consider the factorization

$$\alpha R = \mathfrak{p}^k A$$

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 Dedekind domains. This means that we can define $v_\mathfrak{p}(\alpha) = k$ and so we get a valuation on R,

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

once we formally define $v_\mathfrak{p}(0) = \infty$. We can even extend this function to the fraction field, K, of R; For any $\frac{\alpha}{\beta} \in K$ $\alpha, \beta \in R$ where $\beta \neq 0$ we can now define

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

This is a well defined function for if $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}$ then $\alpha\beta' = \alpha'\beta \in R$ and applying $v_\mathfrak{p}$ on both sides and using that it takes multiplication to addition we obtain

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

The function $v'_\mathfrak{p}$ is an extension of $v_\mathfrak{p}$ since $v'_\mathfrak{p}(\frac{\alpha}{1}) = v_\mathfrak{p}(\alpha) - v_\mathfrak{p}(1) = v_\mathfrak{p}(\alpha)$. For ease of notation we will refer to this extension simply as $v_\mathfrak{p}$. We can now talk about the completion, $K_\mathfrak{p}$ of K with respect to $v_\mathfrak{p}$. Denote by $\hat{v}_\mathfrak{p}$ the valuation on $K_\mathfrak{p}$.

Let now $\mathfrak{P}$ be the unique maximal ideal of the valuation ring $\mathcal{O}_{K_\mathfrak{p}}$. Then $\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$ is an ideal of $\mathcal{O}_{K_\mathfrak{p}}$ so

$$\mathfrak{P}^e = \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$$

Suppose $v_\mathfrak{p}$ is discrete and normalized. Then we can find an element $\pi \in K$ so that $\mathfrak{p} = (\pi)\mathcal{O}_K$ so that $v_\mathfrak{p}(\pi) = 1$. Also $\hat{v}_\mathfrak{p}$ is discrete and normalized, so we can similarly find an element $\hat{\pi} \in K_\mathfrak{p}$ so that $\hat{v}_\mathfrak{p}(\hat{\pi}) = 1$.

But $(\pi)\mathcal{O}_K = \mathfrak{p}$

As the valuation ring $\mathcal{O}_K$

□

Remark 9.2. *Because $v'_\mathfrak{p}$ in the proof above is an extension of $v_\mathfrak{p}$ we will typically just write $v_\mathfrak{p}(x)$ instead of $v'_\mathfrak{p}(x)$.*

This construction actually gives rise to some important examples.

Lemma 9.3. *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 9.1. *Let K be a field. Then $K[x]$ 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 $K[x]$ that extends to a valuation on $K(x)$. The field $K(x)$ is dense in $K((x))$*

The valuation ring of $K((x))$ is $K[[x]]$ and it has unique maximal ideal (x). Thus, the residue field is $K[[x]]/(x) \cong K$, so if K is finite then $K((x))$ is a local field.

Example 9.2. *Let K be a number field and pick prime a $\mathfrak{p}$ in $\mathcal{O}_K$. As $\mathcal{O}_K$ is a Dedekind domain and because of (9.2) we obtain from the above construction above the $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}} : K \to \mathbb{Z} \cup \{\infty\}$. The prime $\mathfrak{p}$ lies above a unique prime p in $\mathbb{Z}$. In other words, $pO_K = \mathfrak{p}$, and so $v_{\mathfrak{p}}(p) = 1$. This valuation is therefore also discrete and normalized. The completion of K with respect to this valuation is denoted by $K_{\mathfrak{p}}$ and is called the $\mathfrak{p}$-adic numbers. We know that the extended valuation the completion is discrete and normalized because of (9.1). Thus there is an element $\pi \in K_{\mathfrak{p}}$ so that $v_{\mathfrak{p}}(\pi) = 1$. Also we know that $\mathfrak{P}^e = \mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}} = p\mathcal{O}_{K_{\mathfrak{p}}}$ for some $e \in \mathbb{N}$. Therefore, $\hat{v}(p) = e$ and so $\hat{v}(\pi^e p) = 0$ meaning that $\pi^e p$ is a unit in $\mathcal{O}_{K_{\mathfrak{p}}}$.*

If $\mathcal{O}$ is the valuation ring of K, we then see that we have the inclusions (WE NEED TO SHOW THAT VALUATION RING CONTAINS ALL ALGEBRAIC INTEGERS)

$$\mathcal{O}_K \subseteq \mathcal{O} \subseteq \mathcal{O}_{K_{\mathfrak{p}}},$$

meaning that we have a map

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

Now, $\mathfrak{p} \subseteq \mathfrak{P}$ and so the kernel of this map is $\mathfrak{p}$.

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

It is also surjective (SHOW THIS) and therefore we have an isomorphism

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

But $\mathcal{O}_K/\mathfrak{p}$ is finite so also $\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{P}$ is finite.

We now present an important special case of the above example.

Definition 9.4 (p-adic numbers)**.** *Set $K = \mathbb{Q}$ and $\mathfrak{p} = (p)$ for a prime number p in $\mathbb{Z}$. In this situation we denote $K_{\mathfrak{p}}$ by $\mathbb{Q}_p$ and call it the field of p-adic numbers. The valuation ring of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$ and is called the ring of p-adic integers.*

Lemma 9.4. *Let $|\cdot|$ 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.

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 very frequently 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 of characteristic 0 is the same thing as a finite extension of $\mathbb{Q}_p$.*

Lemma 11.1. *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 11.2. *Let K be a valued field and (x_n) and (y_n) sequences of K. If (x_n) is Cauchy and $\lim_{n\to\infty} |x_n - y_n| = 0$ then (y_n) is also Cauchy. If it is also known that $\lim_{n\to\infty} x_n = a$ then $\lim_{n\to\infty} y_n = a$.*

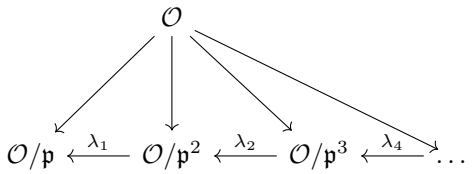
Proof. Observe that

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

A three fold application of the triangle inequality on the right hand side basically 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 (11.1), 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 11.3. *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 11.2. *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 (11.1). 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 (9.4), this means that the sum $x - \frac{x^2}{2} + \frac{x^3}{3} - ...$ converges. UNIQUENESS MISSING $\square$

13 Formal power series

We will briefly take a look at formal power series, as we will use them in the following section. Let K be a field. A power series is an infinite sum of

$$\sum_{n=0}^{\infty} a_n x^n$$

where $a_n \in K$ and x should be thought of as simply a formal symbol. The set of all of these is a ring, called the ring of formal power series over K, and we denote it by $K[[x]]$. This ring contains no zero divisors, so we can consider its field of fractions, which we denote by $K((x))$. This field is called the field of formal Laurent series over K.

This is a local ring with maximal ideal (x). Hence all units in $K[[x]]$ are those with constant term different from 0.

(TODO CONSTRUCT THIS RING USING COMPLETION)

This ring can actually be constructed used the tools we have already developed. The ring $K[x]$ is a PID, since K is a field. Hence the ideals factors uniquely into prime ideals. Now,

$$K[x]/(x) \cong K$$

and so (x) is in particular a prime.

14 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 14.1. *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

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

□

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 14.1. *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.

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

$$\alpha = \gamma_k \epsilon_1^{u_1} ... \epsilon_r^{u_r} \tag{3}$$

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

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

Setting $\delta = \prod_{i=1}^{r} \epsilon_i^{\rho_i}$, $\gamma' = \delta \gamma_k$ we can write $\alpha = \gamma_k' \epsilon_1^{q v_1} ... \epsilon_r^{q v_r}$. 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 14.2. *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 14.2. *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 (14.4) 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 14.3. *Suppose K is a field and $f \in K[[t]]$, f a unit. Then f is transcendental over K.*

Proof. MISSING □

Lemma 14.4. *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

$$\exp P_i = a_i \exp P_{n-1} + b_i \exp P_n \tag{4}$$

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 $i = 1, ...n-1$,

$$Q_i = P_i - P_n, \tag{5}$$

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 (4) and (5) 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'

$$\begin{aligned}Q_i' &= \frac{(a_i Q_{n-1}' \exp Q_{n-1})}{\exp Q_i} \\ &= \frac{a_i Q_{n-1}' \exp Q_{n-1}}{a_i \exp Q_{n-1} + b_i} \\ &= \frac{Q_{n-1}' \exp Q_{n-1}}{\exp Q_{n-1} + c_i}\end{aligned} \tag{6}$$

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 (6) 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

$$\sum_{i=1}^{n-1} \frac{d_i}{\exp Q_{n-1} + c_i} = 0 \tag{7}$$

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 (7) 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 (4) 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.