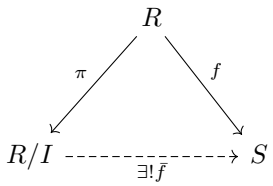
**Proposition 0.1.** *(Universal property for quotients) Let $R, S$ be a rings and $I \subseteq R$ an ideal. Suppose we have a function $f : R \to S$, which vanishes on $I$ and is an additive group homomorphism when restricted to $I$. Then there exists a uniquely determined function*

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

*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 $\pi$ 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. □

Suppose that $v$ is a valuation as above. Let us briefly go through some important properties. Note first that property 2. above makes $v$ into a homomorphism $v : K^* \to \mathbb{R}$. Thus, if $x \in K^*$ has finite order, then also $v(x)$ has finite order. But then $v(x) = 0$ as 0 is the only element in $\mathbb{R}$ that has finite order with respect to addition. In particular, $v(-1) = 0$ so $v(-x) = v(-1) + v(x) = v(x)$ for all $x \in K$. It follows that $v(x + y) = v(y)$ if $v(x) > v(y)$, since

$$v(y) = v(x + y - x) \geq \min\{v(x + y), v(x)\} \geq \min\{v(x), v(y)\} = v(y)$$

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

Now for the alternative characterization.

**Proposition 0.2.** *Let $K$ be a valued field, $\hat{K}$ a complete valued field and $\hat{\imath} : K \to \hat{K}$ a homomorphism preserving the absolute value. Then $(\hat{K}, \hat{\imath})$ is a completion of $K$ if and only if $K$ is dense in $\hat{K}$.*

*Proof.* Assume first that the pair $(\hat{K}, \hat{\imath})$ 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 $\hat{\imath}(K)$

is dense in $\hat{K}$. Now, as $\hat{K}$ is complete also $\overline{K}(=\overline{\hat{\iota}(K)})$ is complete since it is closed and contained in $\hat{K}$. Also, as $K$ is dense in $\overline{K}$ the inclusion is a subfield of $\hat{K}$ (SHOW THIS). Thus, we have the inclusion map $\psi : \overline{K} \to \hat{K}$. 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 $K$. (THIS PART IS UNFINISHED)

Let us now prove the converse. So suppose that $\hat{\iota}(K)$ is dense in $\hat{K}$ and that $(L, \iota)$ is a pair as in (**??**). □

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

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

*for all $x \in K$.*

A nonarchimedian absolute value $|\cdot|$ on a field $K$ extends to a nonarchimedian absolute value on $K(t)$ by setting $|f| = \max |a_0|, ..., |a_n|$ where $f \in K[x]$ and $f(x) = a_n x^n + ... + a_0$. For an arbitrary element $\frac{g}{h} \in K(x)$ where $h \neq 0$ we then define $|\frac{g}{h}| = |g| - |h|$.

**Theorem 0.2.** *Let $F(x, y)$ be a form of degree $k$ in two variables and let $\alpha$ be any root of $F(x, 1)$ and set $K = \mathbb{Q}(\alpha)$. Then*

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

*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 $\alpha_i$. 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. □

Let $F$ be the Galois closure of $K$ and let $G = (F/\mathbb{Q})$ and let $H = (F/K)$. Set now $n = [G:H] = [K:\mathbb{Q}]$ and find $\sigma_1,...,\sigma_n$ so that $G = \cup_{i=1}^{n}\sigma_i H$ is a disjoint union. For ease of notation, let us denote by $N$ the field norm $N_{K/\mathbb{Q}}$. For $x_1,...,x_k \in \mathbb{Z}$ we now define $F(x_1,...,x_k) := N(x_1\mu_1 + ... + x_k\mu_k)$.

Let now $\sigma \in G$. Of course $\sigma\sigma_i \in G$ so there is a unique $j \in \{1,...,n\}$ so that $\sigma\sigma_i \in \sigma_j H$. If both $\sigma\sigma_i$ and $\sigma\sigma_{i'}$ were in $\sigma_j H$ then we would have $i = i'$ and therefore there is a permutation $\tau : \{1,...,n\} \to \{1,...,n\}$, depending on $\sigma$ so that $\sigma\sigma_i \in \sigma_{\tau(i)}H$. In other words, we can write $\sigma\sigma_i = \sigma_{\tau(i)}h_i$ for a suitable $h_i \in H$. But then as $h_i$ fixes $K$ we have

$$\sigma\sigma_i(\mu_j) = \sigma_{\tau(i)}h_i(\mu_j) = \sigma_{\tau(i)}(\mu_j)$$

And therefore

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

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 $\nu_i$ as a $\mathbb{Z}$-linear combination of the $\mu_i$'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 0.3.**

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

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 (**??**) 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 (**??**) will give a $\mathbb{Z}$-linear combination of the $\mu_i$'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 $\mu_i$ 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 $n$.

**Lemma 0.1.** *If $M$ is a full module then there exists a non-zero integer $b$ so that $bM \subseteq \mathfrak{D}$.*

*Proof.* By (**??**) we can find a non-zero integer $c_i$ for every $\mu_i$ 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 (**??**) that $bx$ is in $\mathfrak{D}$ for all $x \in M$, meaning that that $bM \subseteq \mathfrak{D}$. □

As all the $\mu_i$ belong to $K$ we can by (**??**) find $b_i$ so that $b_i\mu_i \in \mathfrak{D}$. Taking

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

Suppose we have a finite extension of fields, $K/k$. Multiplication by an element, $\alpha$, 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, $\chi_{\phi_\alpha}$, of $\phi_\alpha$ 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 $\alpha$ with coefficients in $k$ which equals 0. This means that $\alpha$ is a root of $\chi_{\phi_\alpha}$. We will therefore call the polynomial $\chi_{\phi_\alpha}$ the characteristic polynomial of $\alpha$ relative to the extension $K/k$.

If now $K$ is instead a number field with degree $n$ over $\mathbb{Q}$. If $\alpha$ 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 $\alpha$ has integer coefficients. But as we saw above, $\alpha$ is a root of this polynomial, which is monic. Hence $\alpha$ 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 $\pm 1$, the norm and trace of an element in $\mathfrak{D}$ are integers, and if $\alpha \in \mathfrak{D}$ then $\alpha$ 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.

# 1 Solutions to $N(\mu) = a$, where $\mu$ 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 $\mu$ in $M$. We have that $\epsilon\mu$ is in $M$ if and only if $\epsilon$ 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 $\epsilon$ has norm 1, also $\epsilon\mu$ will be a solution. The units of $\mathfrak{D}$ are the elements with norm $\pm 1$.

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

We obtain the following corollary

**Corollary 1.1.** *Assume $x_1, ..., x_k \in K$ and that $|x_i| > |x_j|$ for all $i \neq j$. Then $|x_1 + ... + x_k| = |x_i|$.*

*Proof.* This follows by induction and the base case is clear. Suppose we have $x_1, ..., x_{k+1} \in K$ and assume without loss of generality that $x_1$ has absolute value strictly larger than all the other $k$ elements. Set now $A = x_2 + ... + x_{k+1}$. We have $|A| \leq \max\{|x_2|, ..., |x_{k+1}|\}$ so $|x_1| > |A|$. By the above proposition we now have $||$ □

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

**Lemma 1.1.** *Suppose that $K$ is a number field and that $v$ is a discrete valuation on $K$. Denote by $O_v$ the valuation ring of $v$. Then $O_K \subset O_v$. In particular, the valuation ring of the completion of $K$ with respect to $v$ contains $O$.*

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

$$O_K = \overline{\mathbb{Z}}^K \subseteq \overline{O_v}^K \subseteq \overline{O_v}^F = O_v$$

□

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 $\kappa_n^*$ is finite. So if $\alpha \in O$ 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 $\kappa_n^*$ 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 $\alpha^k$ is in $U^{(n)}$.