1. Definitions and basic principles.

Assume we have a finite algebraic extension $k \setminus K$. Let α be a number in K. It is known that α satisfies a monic minimal polynomial $f_\alpha \in k[X]$ such that $f_\alpha(\alpha) = 0$, and its degree is $m = [k(\alpha) : k]$. The characteristic polynomial of α with respect to the extension is the monic polynomial $ch_\alpha(x) = f(x)^{[K:k(\alpha)]}$. Define also T_α be the linear transformation of K (regarded as a vector space of dimension $n = [K : k]$ over k) given by multiplication by α. The following are well-known:

1.1. ch_α is the characteristic polynomial of T.

Proof: Assume $w_1, w_2, \ldots, w_r$ is a basis of K over $k(\alpha)$. Then $K = \oplus w_i k(\alpha)$. Each component $w_i k(\alpha)$ is stable under T_α and hence the characteristic polynomial of T_α is the product of the characteristic polynomials of its restrictions to each $w_i k(\alpha)$. However each such restriction has minimal polynomial f_α hence the characteristic polynomial of T_α is $f_\alpha^r = ch_\alpha$.

1.2. If G is the set of all injective morphisms of K that fix k ($|G| = n$) then $ch_\alpha(x) = \prod_{\sigma \in G}(x - \sigma(\alpha))$.

Now we are ready to define the norm, according to any of the following equivalent definitions:

Definition 1.3. For $\alpha \in K$, we define $N_{k\setminus K}(\alpha) \in k$ (or $N(\alpha)$ for simplicity) be any of the following (which are equal):

a) $det(T_\alpha)$

b) $(-1)^n ch_\alpha(0)$

c) $(-1)^n f_\alpha^{[K:k(\alpha)]}(0)$

d) $\prod_{\sigma \in G} \sigma(\alpha)$

It is obvious to check that all these expressions are indeed equal, once we use 1.1. and 1.2. a) and d) make it clear that the norm is multiplicative.

1.4. If $a \in k$ then $N(a) = a^n$. In general, $N_{k\setminus K}(\alpha) = (N_{k\setminus k(\alpha)}(\alpha))^{[K:k(\alpha)]}$.

The proof essentially follows the idea used in the proof of 1.1.

1.5. If $k \setminus K \setminus L$ is a tower of extensions and $\alpha \in L$, then

$$N_{k\setminus L}(\alpha) = N_{k\setminus K}(N_{K\setminus L}(\alpha))$$

Proof: Let $[L : K] = r, [K : k] = s, [L : k] = rs$. Let $\tau_1, \tau_2, \ldots, \tau_s$ be the morphisms of K preserving k and let $\tau_i(K) = K_i$. Each τ_i can be lifted in r ways to a morphism of L, and in this way we get all the rs morphisms of L preserving k. Consider π_i be any lift of τ_i, then all lifts of τ_i $\sigma_{i,j} \circ \pi_i$ where $\sigma_{i,j}$ are all morphisms of $L_i = \pi_i(L)$ that preserve K_i.We the conclude that $N_{k\setminus L}(\alpha) = \prod_{i=1}^s \prod_{j=1}^r \sigma_{i,j}(\pi_i(\alpha))$. Now $\prod_{j=1}^r \sigma_{i,j}(\pi_i(\alpha)) = N_{K_i\setminus L_i}(\alpha)(\pi_i(\alpha)) = N_{\pi_i(K)\setminus \pi_i(L)}(\alpha)$. Since this is the determinant a certain matrix, i.e. an algebraic expression, we are allowed to extract the π_i, yielding $\pi_i(N_{K\setminus L}(\alpha)) = \tau_i(N_{K\setminus L}(\alpha))$. Taking the product over all $i = 1, 2, \ldots, s$ gives exactly $N_{k\setminus K}(N_{K\setminus L}(\alpha))$, according to 1.3.c).

1.6. If $k \setminus K \setminus L$ is a tower of extensions and $\alpha \in K$, then

$$(N_{k\setminus L}(\alpha) = N_{k\setminus K}(\alpha))^{[L:K]}$$

Proof: Straightforward from 1.4. and 1.5.

2. Norms in complete DVR's and extensions of valuations.

For a brief moment, assume that k is a field whose ring of integers O_k is a DVR with maximal ideal P. We also assume that O_k is complete (and so is k) with respect to the valuation v_P. Now let K be a finite algebraic extension of k with ring of integers O_L. It turns out that O_L is also a complete DVR and the norm comes handy in determining the extension on the valuation. The following important theorem is well-known.

2.1. Let e be the ramification index of the extension $k \setminus K$, f the degree of the residue field extension. Then $ef = [K : k]$, and the principal ideal Q of B consists of all elements in B with norm in P. The valuation of the norm of the uniformizer of B is f, and therefore $v_Q(\alpha) = \frac{1}{f} v_P(N(\alpha))$.

The local case is important for extending valuations of number fields.

Assume that k is a number field with P a prime ideal of the ring of integers O_k, and valuation v_P corresponding to it. Consider K a finite algebraic extension of k with ring of integers O_K. It is known that the ideal $PO_K = \prod_{Q_i}^{e_i}$ for some prime ideals Q_i of O_K.

Denote by $\hat{k}$ the completion of k with respect to v_P. $\hat{k}$ is the field of fractions of the DVR $\hat{O_k}$, the completion of O_k, with maximal ideal $P\hat{O_k}$, which we will denote by $\hat{P}$. We may assume that $k \subset \hat{k}$ (and is dense in it). v_P matches $v_{\hat{P}}$ on k.

2.2 Let $\tau_1, \ldots, \tau_m$ be all isomorphisms of K into $\overline{\hat{k}}$, and set $tau_i(K) = K_i$. Then K_i is a finite algebraic extension of $\hat{k}$ with a valuation v_{Q_i} given by 2.1. The prime ideal of K_i is then $\hat{Q_i}$ the completion of Q_i with respect to v_{Q_i} and e_i is then the ramification index of $\hat{k} \setminus K_i$.

The following important theorem is also known.

2.3. $\oplus K_i \cong K \otimes \hat{k}$ as vector spaces over $\hat{k}$, and $\oplus O_{K_i} \cong O_K \otimes \hat{O_k}$ as $\hat{O_k}$-modules. The isomorphism is given by the natural projection $u \otimes \alpha \to (\tau_i(u)\alpha)_i$.

The projection of the ideal $P \times \hat{O_k}$ onto O_{K_i} is $\hat{Q_i}^{e_i}$, and hence as a corollary one gets

2.4. $\oplus O_{K_i} \setminus \hat{Q_i}^{e_i} \cong O_K \setminus P$ (as modules over $O_K \setminus P$).

As a corollary of 2.3, T_α acting on $K \otimes \hat{k}$ is the direct sum of the linear operators $T_{\tau_i(\alpha)}$ acting on K_i and from here one gets

2.5. $ch_\alpha = \prod_{i=1}^m ch_{\tau_i(\alpha)}$ (all polynomials are regarded with respect to their corresponding algebraic extensions)

Note that the last identity takes place in $\hat{k}$, it just happens that the product of all polynomials lies in the copy of k which is sitting inside $\hat{k}$. We now plug in 0 in the polynomial identity and take take the valuation $v_{\hat{P}}$ of both sides of the identity. As we know $v_{\hat{P}}$ matches v_P on k, we have

2.6. $v_P(N_{k\setminus K}(\alpha)) = \sum_{i=1}^{n} v_{\hat{P}}(N_{\hat{k}\setminus K_i}(\tau_i(\alpha)))$

3. Norms of ideals.

3.0. Let $k \setminus K$ be an extension of number fields. Then $\alpha \in O_K$ is a unit in O_K if and only if $N_{k\setminus K}(\alpha)$ is a unit in O_K.

Proof: Let $x^n + b_{n-1}x^{n-1} + \ldots + b_0 = ch_\alpha(x) \in O_k[x]$, $N_{k\setminus K}(\alpha) = \pm b_0$. If α is a unit then $\frac{1}{\alpha} \in O_K$ hence its norm is in O_k(being a coefficient of its characteristic polynomial) thus $\frac{1}{N(\alpha)}$ is in O_k hence $N(\alpha)$ is a unit. Conversely, if $N(\alpha)$ is a unit then $\frac{N(\alpha)}{\alpha} = \pm(\alpha^{n-1} + b_{n-1}\alpha^{n-2} + \ldots + b_1) \in O_K$ hence α is invertible in O_K so is a unit.

We now seek to define a norm for ideals. If an ideal if principal, we might try to set its norm equal the norm of its generator, since all generators must have morns equal according to a unit, from 3.0. Unfortunately, not every ideal is principal. However, in completions with respect to prime ideals every ideal is principal, and 2.6. provides a bridge between the local and global case. Note that the norm of an ideal is then defined only up to a unit. Even worse: in general, the norm of an ideal is an ideal.

First, we start with the local case.

Definition 3.1. Assume the conditions of 2.1. For Q a prime ideal of O_K dividing P a prime ideal of O_k, define $N_{k\setminus K}(Q)$ to be the ideal generated by the norm of the uniformizer of Q, that is, $N_{k\setminus K}(Q) = P^f$. It is the ideal generated by the norms of all elements of Q.

The proof of the last sentence follows from 2.6. and 2.1., since the ideal generated by the norms of all elements of Q is in fact generated by the norm of the uniformizer of Q.

Now we define norms of prime ideals in number fields.

Definition 3.1. If $k \setminus K$ is a finite extension of number fields, and Q is a prime ideal of O_K dividing P a prime ideal of O_L, we define $N_{k\setminus K}(Q)$ be P^f where f is the degree of the finite field extension $[O_K \setminus Q : O_k \setminus P]$. It can also be defined as the ideal generated by the norms of the elements of Q.

The proof of the last assertion of the statement follows from 3.1. and the Chinese Remainder Theorem applied to Q and any other ideal of K (not divisible by Q).

We now extend the definition of norm to have it multiplicative.

Definition 3.2. If $k \setminus K$ is a finite extension of number fields and I is an ideal of O_L, the norm of I is defined to be the product of the norms of all ideals dividing Q (counted with multiplicity). It is the ideal generated by the norms of all elements of the ideal.

By multiplicativity, the norm can be extended to fractional ideals too.

4. The norm as the cardinality of the residue class.

Note that, in general, the norm of an ideal I in O_K must be an ideal in O_k, which is not always principal. When $k = \mathbb{Q}$, or $k = \mathbb{Q}_p$, every ideal is principal and therefore we talk of the norm of I as a number in O_k, the number in O_k being uniquely determined up to a unit. In case I is principal, that number is in fact the old norm of the generator, up to a unit in O_k. In the case $k = \mathbb{Q}_p$, every ideal of O_k is generated by a power of f,

so we may assign the norm of I as that power of p. In both of these cases, the norm may be chosen to be a positive integer.

Definition 4.1. In the case $k = \mathbb{Q}$ or $k = \mathbb{Q}_p$, we may identify $N_{k\backslash K}(I)$ as a number in O_k, the generator of the ideal $N_{k\backslash K}(I)$. In both cases, this number can be uniquely be chosen to be a non-negative integer.

This definition is justified by the following theorem:

4.2. If K is a finite algebraic extension of either $\mathbb{Q}$ or $\mathbb{Q}_p$ and I is an ideal of O_K, then the number of residue classes in $O_K \setminus I$ is exactly $N_{k\backslash K}(I)$ as defined in 4.1., where k is either $\mathbb{Q}$ or $\mathbb{Q}_p$.

Proof: Assume first that $k = \mathbb{Q}_p$ and that $I = P$ is the maximal ideal of K. The norm of I is the p^f where f is the degree of the residue class field extension. As the residue class field of $\mathbb{Q}_p$ has p, elements, the residue class field of K must then be a finite field of p^f elements, as desired.

If $I = P^r$ is a power of the maximal ideal, then its norm is p^{rf}. If $0 = w_1, w_2, \ldots, w_{p^f-1}, w^{p^f}$ are a complete set of representatives of $\mathbb{O}_K \backslash P$ and l is a uniformizer of K, then $\sum_{j=0}^{r-1} w_{i_j} l^j$ are a complete set of representatives of $O_K \backslash I$ where i_j run independently over $1, 2, \ldots, p^f$. Hence there are $p^{rf} = N(I)$ representatives for $O_K \setminus I$, and this concludes the proof in the p-adic case.

Now assume $k = \mathbb{Q}$ and $P|p$ is a prime ideal of K, where p is an integer prime. The isomorphism of 2.3. sends P to the maximal ideal in one of the components O_{K_i} and to the entire O_{K_j} for all $j \neq i$. The conclusion now follows from the case proven above, along with the observation that the observation of 2.3. naturally induces an isomorphism between P and the direct sum of the residue classes of its images under the maps τ_i (this is only in the case $P|p$). The same argument can be used to show directly the conclusion in the case when P is a power of a prime ideal, or when it's norm is a power of an integer prime.

Finally we prove the theorem when P is any ideal in O_K. To do this, it is enough to show how the conclusion for two ideals I, J implies the conclusion for the ideal IJ. Indeed, if $w_1, w_2, \ldots, w_m$ is a complete set of representatives modulo I and $u_1, u_2, \ldots, u_s$ is a complete set of representatives modulo J, chosen in such a way that the greatest common divisor of $\frac{<u_j>}{gcd(<u_j, J>)}$ is coprime to I (this can be done according to the Chinese Remainder Theorem in the Dedekind Domain O_K), then $w_i u_j$ can be proven to be a complete set of ms representatives modulo IJ, so the conclusion of the theorem follows from the assumptions for I, J and the fact that $N(IJ) = N(I)N(J)$.

As a corollary of 4.2., we have the following:

4.3. If K is a finite algebraic extension of either $\mathbb{Q}$ or $\mathbb{Q}_p$ and I is an ideal of O_K, then the norm of I as defined in 4.1. equals the index of I in O_K.

5. Norm as the volume of the fundamental parallelepiped in a lattice. Minkowki's Theorem and the finiteness of the ideal class group

In this section we will assume $k = \mathbb{Q}$ and K is a number field. Let $[K : k] = n$. As-

sume that there are s embeddings $\sigma_1, \sigma_2, \ldots, \sigma_s$ of K into $\mathbb{R}$ that preserve k, and t pairs of conjugate embeddings $(\tau_1, \overline{\tau_1}), \ldots, (\tau_t, \overline{\tau_t})$ of K into $\mathbb{C}$ that preserve k. The $s+2t = n$. The linear injective map $\phi\colon K \to \mathbb{R}^s \times \mathbb{C}^t$ given by $\phi(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_s(\alpha), \tau_1(\alpha), \ldots, \tau_t(\alpha))$ maps the $\mathbb{Z}$-module O_K into a $\mathbb{Z}$-module lattice $L \in \mathbb{R}^s \times \mathbb{C}^t$. $\mathbb{R}^s \times \mathbb{C}^t$ is naturally isomorphic to $\mathbb{R}^{s+2t}$, and so we may assume that L is a lattice in $\mathbb{R}^n$ via this isomorphism. As O_K is finitely generated over $\mathbb{Z}$, it must be free so it is the direct sum $w_1 Z \oplus w_2\mathbb{Z} \oplus \ldots \oplus w_n\mathbb{Z}$. Then $L = \phi(w_1)\mathbb{Z} \oplus \phi(w_2)\mathbb{Z} \oplus \ldots \oplus \phi(w_n)\mathbb{Z}$ is a lattice isomorphic to $\mathbb{Z}^n$ in $\mathbb{R}^n$. The volume of the fundamental parallelepiped of this lattice (defined by the vectors $\phi(w_1), \phi(w_2), \ldots, \phi(w_n)$) can be computed to be $v_K = 2^{-t}\sqrt{|D|}$ where D is the discriminant of K.

Now, assume that I is an ideal of O_K. Because I has finite index in O_K according to 4.3., $phi(I)$ has finite index in L, and it equal $N(I)$. The following lemma allows us to connect the $N(I)$ to the volume of the volume V_I of the fundamental parallelepiped of $\phi(I)$.

5.1. Assume $L_1 \subset L_2$ are finitely-generated free $\mathbb{Z}$ modules of the same rank n, and the index of L_1 in L_2 is finite. If L_2 is generated by $w_1, w_2, \ldots, w_n$, then L_1 is generated by n numbers $w_1' = c_{1,1}w_1 + c_{1,2}w_2 + \ldots + c_{n,n}w_n, w_2' = c_{2,2}w_2 + c_{2,3}w_3 + \ldots + c_{2,n}w_n, \ldots, w_n' = c_{n,n}w_n$ where $c_{i,j}$ are integers with $c_{1,1}, c_{2,2}, \ldots, c_{n,n} > 0$, and the index of L_1 in L_2 is $c_{1,1}c_{2,2}\ldots c_{n,n}$.

Proof: Consider the projection π of L_2 onto $\mathbb{Z}w_1$. Then the set $\pi(L_1)$ is a non-zero ideal of $\mathbb{Z}$, so it's generated by some positive integer $c_{1,1}$. We can pick up w_1' be any number in $\pi^{-1}(c_{1,1})$. Then subtracting from each element of L_1 a suitable integer multiple of w_2', we end in $\mathbb{Z}w_2 \oplus \mathbb{Z}w_3 \oplus \ldots \oplus \mathbb{Z}w_n$, and we now continue our process with the newly obtained modules of rank $n-1$. This method yields a desired "upper-triangular" basis of L_1, and to check that its index in L_2 is $c_{1,1}c_{2,2}\ldots c_{n,n}$, we just observe that the numbers $\sum_{i=1}^{n} k_i w_i$ form a complete set of representatives for $L_2 : L_1$, where each of k_i spans independently the set $0, 1, \ldots, c_{i,i} - 1$.

5.2. For an ideal I of O_K, the volume v_I of the fundamental parallelepiped of the lattice $\phi(I)$ is $N(I)v_K$.

Proof: Let $w_1, w_2, \ldots, w_n$ be a set of generators of L. 5.1. ensures we can select $w_1', w_2', \ldots, w_n'$ generators for $\phi(I)$ such that the matrix of $w_1', w_2', \ldots, w_n'$ written in the base $w_1, w_2, \ldots, w_n$ is an upper-triangular integer matrix. Its determinant will then be d the product of all diagonal entries of the matrix, and so according to 5.1. and 5.3 we have $d = N(I)$. Since $w_1', w_2', \ldots, w_n'$ are obtained from $w_1, w_2, \ldots, w_n$ via a linear transformation of determinant d, the volume of the parallelepiped determined by $w_1', w_2', \ldots, w_n'$ is $|d| = N(I)$ times the volume of the parallelepiped determined by $w_1, w_2, \ldots, w_n$.

The following is Minkowski's Theorem:

5.3. Let L be a free lattice of rank n over $\mathbb{Z}$ in $\mathbb{R}^n$, and let V_L be the volume of the fundamental parallelepiped of L. Consider C a closed convex body in $\mathbb{R}^n$, symmetric

with respect to the origin and with volume V. If $V \leq 2^n V_L$, then C contains a point in L, different from the origin.

5.4. If I is an ideal of O_K, then I contains a non-zero number α whose norm is at most $cN(I)$ in absolute value where c is a positive constant independent on I

Proof: Consider the convex body C, in $\mathbb{R}^n \cong \mathbb{R}^s \times \mathbb{C}^t$, such that $(x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_t) \in C$ if and only if $|x_i| \leq c_i, |y_i|^2 \leq d_i$ for some appropriate $c_i, d_i > 0$ (we have x_i as reals and y_i as complex numbers). It's easy to see that the volume of C in $\mathbb{R}^n$ is $2^s \pi^t \prod c_i \prod d_i = 2^n \times (\frac{\pi}{4})^t \prod c_i \prod d_i$. Particularly choosing $\prod c_i \prod d_i = (\frac{4}{\pi})^t v_I = (\frac{2}{\pi})^t \sqrt{|D|} N(I)$ we can apply Minkowski's Theorem and conclude that $\phi(I)$ contains a non-zero element in $\phi(\alpha) = (x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_t) \in C$. Hence $\prod |x_i| \prod |y_i|^2 \leq (\frac{2}{\pi})^t \sqrt{|D|} N(I)$. However $\prod |x_i| \prod |y_i|^2 = |\prod \sigma_i(\alpha) \prod_i \tau_i(\alpha) \overline{\tau_i}(\alpha)|$ is in fact $|N(\alpha)|$, according to 1.3. d), and hence the conclusion holds for $c = (\frac{2}{\pi})^t \sqrt{|D|}$.

Note that theorem 5.4. holds for fractional ideals too, since every fractional ideal becomes principal when multiplied by a suitable positive integer. One calls two ideals I, J in O_K equivalent $I = \alpha J$ for some $\alpha \in K$, i.e. IJ^{-1} is a principal fractional ideal. This is clearly an equivalence relation, and can be extended to fractional ideals. The group of fractional ideals of K modulo this relation (i.e. fractional ideals modulo principal fractional ideals) is called the ideal class group of K.

5.5. The ideal class group of any number field K is finite.

Proof: Let I be any fractional ideal. According to 5.4., I^{-1} contains a number α with norm at most $cN(I)$. Therefore the ideal αI is an ideal of O_K and as norm at most c. Hence I is equivalent to an ideal of bounded norm. However, there are only finitely many ideals of bounded norm.