CYCLOTOMIC EXTENSIONS AND QUADRATIC RECIPROCITY

ALEXANDER BERTOLONI MELI

Abstract. We develop some of the basic theory of algebraic number fields and cyclotomic extensions and use this to give a proof of quadratic reciprocity. We construct the discrete valuation rings corresponding to the completion of the ring of integers at each prime and then piece together this information to find the ring of integers of the cyclotomic extensions. We prove quadratic reciprocity by considering the action of the Frobenius automorphism on the unique quadratic sub-extension of the splitting field of pth roots of unity for prime p.

Contents

I seek to develop some of the basic theory of algebraic number fields and then use this to give a proof of quadratic reciprocity. In order to prevent the preliminary sections from becoming too lengthy, I expect the reader to be familiar with undergraduate ring and Galois theory. Moreover, the reader is referenced to another text for certain select proofs.

1. Discrete Valuation Rings

Definition 1.1. Let K be a field. A function $v : K \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation if it satisfies the following properties.

1)$v(a) = \infty$ if and only if $a = 0$
2)$v(ab) = v(a) + v(b)$
3)$v(a + b) \geq \min(v(a), v(b))$

Definition 1.2. Corresponding to a discrete valuation $v : K \to \mathbb{Z} \cup \{\infty\}$ is the discrete valuation ring: $D_K = \{x \in K : v(x) \geq 0\} \cup \{0\}$.

Date: August 19, 2013.

It is an exercise to check that the set D_K as defined above is a ring.

One of the most familiar examples of a discrete valuation is the p-adic valuation on $\mathbb{Q}$ for each prime p of $\mathbb{Z}$, which is given by $v(\frac{a}{b}) = n$ if $\frac{a}{b} = \frac{a'}{b'}p^n$ and $(p, a') = (p, b') = 1$. In this case, the valuation ring is $\mathbb{Z}_{(p)}$-the localization of $\mathbb{Z}$ at p. We will discuss this example in detail later, but this is a good ring to keep in mind for the following propositions.

Alternatively, one can consider $F(x)$ for F a field and a valuation defined by $v(\frac{g}{h}) = n$ where $\frac{a}{b} = f^n\frac{a'}{b'}$ where f does not divide a' or b' and is an irreducible polynomial in $F(x)$.

Proposition 1.3. *$a \in D_K$ is a unit in D_K precisely when $v(a) = 0$.*

Proof. Observe that $v(1) = v(1 \cdot 1) = v(1) + v(1)$ so that $v(1) = 0$ If $a \in D_K$ is a unit, then $0 = v(1) = v(a \cdot a^{-1}) = v(a) + v(a^{-1})$. Both $a, a^{-1} \in D_K$ so in order for the preceding equation to hold, $v(a) = v(a^{-1}) = 0$. Conversely, if $v(a) = 0$, then the preceding equation gives that $v(a^{-1})$ is also 0. □

Proposition 1.4. *If $v(\pi) = 1$, then π generates the unique maximal ideal of D_K.*

Proof. First we observe that such a π does indeed exist since $v|_{K^*}$ is by definition a surjection onto $\mathbb{Z}$. If $a \in D_K$ is not a unit then $v(a) = n$ for some $n \geq 1$ and so $v(\frac{a}{\pi^n}) = v(a) - nv(\pi) = 0$. Thus, $\frac{a}{\pi^n} = u$ for some unit in D_K and so $a = u\pi^n \in (\pi)$. Thus, (π) contains all non-units and so is a maximal ideal (no proper ideal contains a unit). Any other proper ideal is therefore also a subset of (π). □

Proposition 1.5. *Any nonzero proper ideal of D_K is of the form $(\pi)^n$ for some $n \in \mathbb{N}$. In particular, this means (π) is the unique nonzero prime ideal of D_K.*

Proof. If I is a proper ideal of D_K then pick some $a \in I$ with minimal valuation. Then if $v(a) = n$, we have shown that $a = u\pi^n$ for some $u \in D_K$ and so $(\pi)^n \subset I$. Conversely, if $b \in I$, then $v(b) = m \geq n$ and $b = v\pi^m$ for some unit $v \in D_K$. Thus, $b \in (\pi)^n$. □

We have seen that D_K is a principal ideal domain with some rather striking properties. In fact, D_K is also a Euclidean domain. Indeed we see that v gives a Euclidean norm since if $a, b \in D_K$, then $a = u\pi^n, b = v\pi^m$ and if we assume $m \geq n$, then $b = a \cdot (\frac{v}{u}\pi^{m-n}) + 0$. Finally, we observe that a discrete valuation on K gives a notion of absolute value on K

Proposition 1.6. *Corresponding to a discrete valuation v is an absolute value $|\cdot|_v : K \to \mathbb{R}$ satisfying the following properties:*

1) $|x|_v \geq 0$ with equality if and only if $x = 0$
2) $|xy|_v = |x|_v \cdot |y|_v$
3) $|x + y|_v \leq \max(|x|_v, |y|_v)$

Proof. We define $|\cdot|_v$ by picking some positive $r \in \mathbb{R}$ and defining $|x|_v = r^{-v(x)}$ for all $x \in K^*$ and $|0|_v = 0$. Then property 1) is trivially satisfied and for 2) we see that

$$|xy|_v = r^{-v(xy)} = r^{-v(x)-v(y)} = r^{-v(x)}r^{-v(y)} = |x|_v \cdot |y|_v$$

For 3), we observe that

$$|x + y|_v = r^{-v(x+y)} \leq r^{-\min(v(x),v(y))} = r^{\max(-v(x),-v(y))} = \max(|x|_v, |y|_v)$$

□

2. Completions and the p-adics

Definition 2.1. Given a rational number $\frac{a}{b} \in \mathbb{Q}$ and a prime p, we can write $\frac{a}{b} = p^n \frac{a'}{b'}$ where $(a'b', p) = 1$. Then the p-adic valuation on $\mathbb{Q}$ is given by $v(\frac{a}{b}) = n$.

Proposition 2.2. *The p-adic valuation gives a discrete valuation on $\mathbb{Q}$.*

Proof. The proof follows the definitions and is a good exercise for the reader. □

As we noted above, any discrete valuation gives rise to an absolute value. In fact, such an absolute value also defines a metric and topology on $\mathbb{Q}$ via $d(x, y) = |x-y|_v$.

Definition 2.3. Given any field K with a metric $d(x, y)$, we say a sequence (a_n) in K is Cauchy if for any $\epsilon > 0$, there is an $N \in \mathbb{N}$ so that if $m, n \geq N$, then $d(a_n, a_m) < \epsilon$.

Proposition 2.4. *Every convergent sequence in K is Cauchy.*

Proof. If (a_n) converges to $x \in K$ then for each ϵ, there is an N so that $d(a_n, x) < \frac{\epsilon}{2}$. Then if $n, m \geq N$, $d(a_n, a_m) < d(a_n, x) + d(a_m, x) < \epsilon$. □

Notice that this proof uses the triangle inequality which holds for all metrics. For a discrete valuation, we have the stronger ultrametric inequality $d(x, z) \leq \max(d(x, y), d(y, z))$ for all $x, y, z \in K$ which follows from property 3) of $|\cdot|_v$.

Definition 2.5. A metric space is complete if every Cauchy sequence converges. L is a completion of K if there is a dense embedding of K into L and L is complete. If the completion of K is with respect to the discrete valuation v, I will refer to the completion as K_v.

The space L of all Cauchy sequences of K modulo the equivalence $(a_n) \sim (b_n)$ if $\lim_{n\to\infty}(a_n - b_n) = 0$ is a completion of K. The completion is unique since if L, L' are completions of K, then the map $T : K \subset L \to K \subset L'$ extends to an isomorphism.

We can define a metric on L by $d((a_n), (b_n)) = \lim_{n\to\infty} d(a_n, b_n)$. K embeds into L as the constant sequences and in the case where v is a discrete valuation on K, we define $v((a_n)) = \lim_{n\to\infty} v(a_n)$. If (a_n) is Cauchy, we see that this is well defined, and we observe that $v((a_n)) = \infty$ precisely when $(a_n) \sim (0)$. Thus, the completion is also a discrete valuation ring. We denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ with the p-adic valuation.

Proposition 2.6 (Milne, 7.25)**.** *If a field K has a discrete valuation v, then $D_K/(\pi) \cong D_{K_v}/\pi D_{K_v}$.*

Proof. K embeds as a subfield into K_v and clearly this embedding respects the valuation v. Thus, D_K embeds into D_{K_v} and $D_{K_v} \cap K = D_K$. Thus, $\pi D_K = \pi D_{K_v} \cap K$ (if $x \in \pi D_{K_v} \cap K$ then x is of the form $a\pi$ for $a \in D_{K_v}$. $a\pi \in K$ and $\pi \in K$ so $a \in K$. Then $a \in D_K$ and so $a\pi \in \pi D_K$ and the converse is clear) and so we have a natural injection $i : D_K/(\pi) \to D_{K_v}/\pi D_{K_v}$.

Now, $a+\pi D_{K_v} = \{x \in D_{K_v} : |x-a|_v < 1\}$ which is open. Thus, if $x \in a+\pi D_{K_v}$, we can find some open ball about x contained within $a + \pi D_{K_v}$. K is dense in K_v and so there is some $x' \in i(D_K)$ contained within this ball. Thus, we have found a representative in D_K for the equivalence class $a+\pi D_{K_v}$ and so i is a surjection. □

The following proposition will prove useful later.

Proposition 2.7 (Neukirch 2.4.9)**.** *If K is complete with respect to a discrete valuation v and V is an n-dimensional normed vector space over K, then all norms are equivalent (in the sense that they generate the same topology) on V. In particular, we show that each norm is equivalent to the maximum norm on a fixed basis $(v_1, ..., v_n)$ given by $||x_1v_1 + ... + x_nv_n|| = \max(|x_i|_v)$.*

Before proving the proposition, we observe that in the maximum norm, a sequence (y_m) in V is Cauchy precisely when the sequences of coefficients $(x_i)_m$ of (y_m) are all Cauchy. Thus, since K is complete, each of these sequences is convergent and this allows us to construct a limit for (y_m) in V. So V is complete. Thus, a proof of the proposition implies that V is complete under any norm.

Proof. If $||\cdot||'$ is the given norm, it suffices to find positive constants p, q so that for all $x \in V$, $p||x|| \leq ||x||' \leq q||x||$. For q, we notice that

$$||x||' = ||x_1v_1+...+x_nv_n||' \leq |x_1|_v \cdot ||v_1||'+...+|x_n|_v \cdot ||v_n||' \leq \max(|x_i|_v) \cdot n \max(||v_j||')$$

Thus we let $q = n\max(||v_j||')$.

We construct p by induction. In the base case when $n = 1$ we pick some nonzero vector v_1 and then, $||x|| = ||x_1v_1|| = |x_1|_v$ and so we can let $p = ||v_1||$. Suppose that we have shown the $n-1$ case. Then suppose V is n-dimensional and pick any basis $v_1, ..., v_n$. Choose some v_i and let V_i be the span of the other $n-1$ vectors. Now, the norms $||\cdot||, ||\cdot||'$ restrict to the $n-1$-dimensional subspace V_i and so by the induction hypothesis and our remark above, V_i is complete with respect to $||\cdot||'$ and therefore closed in V. Thus, the translation $V_i + v_i$ is also closed. But then $\bigcup_{i=1}^n V_i + v_i$ is a closed set, and we observe that $0 \notin V_i + v_i$ since $v_1, ..., v_n$ is a basis. Thus, $0 \notin \bigcup_{i=1}^n V_i + v_i$ and since the complement is open, there is some ball about 0 of some radius p so that for each $w_i \in V_i$, $||w_i + v_i||' > p$. Then for any $x = x_1v_1 + ... + x_nv_n$, we have for each i, $||\frac{x}{x_i}||' = ||\frac{x_1}{x_i}v_1 + ... + v_i + ... + \frac{x_n}{x_i}v_n||' > p$ so that $||x||' > p|x_i|_v$ for each i and therefore $||x||' \geq p||x||$. □

Alternatively, one can define completions algebraically

Definition 2.8. If R is a ring and I is an ideal, then the completion of R at I which we denote $\varprojlim R/I^n$ is $\{(a_n) : \pi_n(a_{n+1}) = a_n\} \subset \prod_{n=1}^{\infty} R/I^n$ (where $\pi_n : R/I^{n+1} \to R/I^n$ are the canonical projections).

Let (b_k) be a Cauchy sequence of integers according to the p-adic valuation. Then for each n, there is some M_n so that if $k, k' > M_n$, then $v(b_k - b_{k'}) > n$ in other words, k, k' are all in the same coset of the ideal $\mathbb{Z}/p^n\mathbb{Z}$. If we label this coset a_n, then we get a sequence (a_n) that clearly satisfies the projection condition we wanted above. Conversely, given (a_n) we can construct a Cauchy sequence (a'_n) by letting a'_n be some random element in the coset a_n. Then we observe that for any n, if $k > \max(M_n, n)$, then $v(a'_k - b_k) > n$ so that these Cauchy sequence are equivalent. Thus, we have given a correspondence between our two notions of completion for the p-adic integers. One can check that this correspondence is well-behaved under the ring operations. For a module M over a ring R, we can define a similar notion of completion by picking some ideal I of R and then letting $M_n = I^nM$ and then $\varprojlim M/M_n = \{(m) : \pi_n(m_{n+1}) = m_n)\} \subset \prod_{n=1}^{\infty} M/M_n$. Recall that an R sub-module of a ring R is just an ideal and observe that in this case, the definitions match.

Proposition 2.9 (Atiyah, McDonald 10.12)**.** *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of finitely generated modules over a Noetherian ring R. Then if I is an ideal of R and we take completions with respect to I, then $0 \to \varprojlim M'/M'_n \to \varprojlim M/M_n \to \varprojlim M''/M''_n \to 0$ is exact.*

Proposition 2.10 (Atiyah, McDonald 10.15)**.** *If R is Noetherian and $\varprojlim R/I^n$ its completion with respect to I, then $\varprojlim I/I^n = I \cdot \varprojlim R/I^n$ and $\varprojlim I^k/I^n = (\varprojlim I/I^n)^k$*

If we take the natural map $M \to \varprojlim M/M_n$ where $x \mapsto (x)$ (the constant sequence of x), then the kernel of this map is clearly $\bigcap_n M_n$. Krull's Thereom gives another characterization of this kernel.

Proposition 2.11 (Atiyah, McDonald 10.17)**.** *[Krull's Theorem] If M is an R module and we take the completion with respect to the ideal I, then the kernel of the natural map $M \to \varprojlim M/M_n$ is precisely the set of $x \in M$ that are annihilated by some element of $1 + I$.*

Proposition 2.12. *If M is an R-module, then $M = \{0\}$ if and only if $M_{(\mathfrak{m})} = \{0\}$ (localization at $\mathfrak{m}$) for every maximal ideal $\mathfrak{m}$ of R.*

Proof. If $M = \{0\}$, then clearly the localizations at every maximal ideal will be $\{0\}$. Conversely we see that $M_{(\mathfrak{m})} = 0$ means that every $x \in M$ is annihilated by some $s \in R - \mathfrak{m}$. But now, let $x \in M$ be some nonzero element. Then the annihilator of x is some proper ideal and so must be contained within some maximal ideal $\mathfrak{m}$. Then $M_{(\mathfrak{m})} \neq \{0\}$ since no element of the annihilator of x is in $R - \mathfrak{m}$. □

Proposition 2.13 (Atiyah, McDonald chapter 10 exercise 3)**.** *Let R be Noetherian, I an ideal, and M a finitely generated R-module. Then $\bigcap_{n=1}^{\infty} I^n M = \bigcap_{\mathfrak{m} \supset I} \ker(f_{\mathfrak{m}} : M \to M_{(\mathfrak{m})})$ for $\mathfrak{m}$ a maximal ideal.*

Proof. By Krull's theorem proposition 2.11, $\bigcap_{n=1}^{\infty} I^n M$ are the elements of M annihilated by some element of $1+I$. Now consider the set $M' = \bigcap_{\mathfrak{m} \supset I} \ker(f_{\mathfrak{m}} : M \to M_{(\mathfrak{m})})$. Then this is an R sub-module of the finitely generated module M. Since R is Noetherian, M is Noetherian and so M' is a finitely generated R module as well. Consider M'/IM' as a finitely generated R/I-module and observe that by construction (and since localization preserves exact sequences) that for each maximal ideal $\mathfrak{m}$ of R/I, $(M'/IM')_{(\mathfrak{m})} = M'_{(\mathfrak{m})}/IM'_{(\mathfrak{m})} = \{0\}$. Thus, by the proposition above, $M'/IM' = \{0\}$ and so $M' = IM'$. Thus, by Nakayama's lemma, there is some $x \in 1 + I$ that annihilates M' and so $M' \subset \bigcap_{n=1}^{\infty} I^n M$.

Conversely, if a is annihilated by $x \in 1 + I$, then $x = 1 + i$ for some $i \in I$ and so if $x \in \mathfrak{m}$ for any maximal ideal containing I, then $1 \in \mathfrak{m}$, which is impossible. Thus, $x \in R - \mathfrak{m}$ for each $\mathfrak{m}$, and so $\frac{a}{1} \sim 0 \in M_{(\mathfrak{m})}$ so that $a \in \bigcap_{\mathfrak{m} \supset I} \ker(f_{\mathfrak{m}} : M \to M_{(\mathfrak{m})})$. □

Proposition 2.14. *If M is a finitely generated R-module over a Noetherian ring R, then $M = \{0\}$ if and only if $\varprojlim M/M_n = \{0\}$, completing at each maximal ideal $\mathfrak{m}$ of R.*

Proof. If $M = \{0\}$, then the completions at any maximal ideal must be $\{0\}$.

Conversely, if $\mathfrak{m}$ is a maximal ideal and we take the completion $\varprojlim M/M_n$ at $\mathfrak{m}$, then we proved in the above proposition that the kernel of the natural map

$M \to \varprojlim M/M_n$ is $\bigcap_{n=1}^{\infty} \mathfrak{m}^n M = \ker(f_{\mathfrak{m}} : M \to M_{(\mathfrak{m})})$. Then if $\varprojlim M/M_n = \{0\}$, then the kernel of this map is M and so $\ker(f_{\mathfrak{m}} : M \to M_{(\mathfrak{m})}) = M$. Thus, $M_{(\mathfrak{m})} = \{0\}$. If this holds for all maximal ideals $\mathfrak{m}$ of R, then by proposition 2.12, $M = \{0\}$. □

3. Number Fields and Rings of Integers

Definition 3.1. We call K a number field if it is a finite algebraic extension of $\mathbb{Q}$.

Definition 3.2. If A, B are rings and $A \subset B$, then an element $b \in B$ is integral over A if b is the root of a monic polynomial with coefficients in A. The integral closure of A in B is the set of all integral elements of A in B

We state some of the basic results of integral extensions without proof. The proofs are standard and can be found in any commutative algebra text, such as [1], pg59

Proposition 3.3. *b is integral over A if and only if $A[b]$ is a finite A-module.*

Proposition 3.4. *Integrality is transitive in the sense that if B is integral over A (i.e. all elements of B are integral over A) and C is integral over B then C is integral over A.*

Proposition 3.5. *The integral closure of A in B is a ring and is integrally closed.*

Proposition 3.6. *Let K be the field of fractions of a ring A and let L be an extension of K. Then if α is algebraic over A, there exists a $d \in A$ so that $d\alpha$ is integral over A.*

Proposition 3.7. *If A is a UFD, then A is integrally closed in its field of fractions K.*

Definition 3.8. If K is a number field, then we define the ring of integers of K, O_K, to be the integral closure of $\mathbb{Z}$ in K.

Definition 3.9. A ring R is a Dedekind Domain if it is Noetherian, integrally closed, and has Krull dimension 1.

It is a theorem that R is Dedekind if and only if ideals in R admit a unique factorization into prime ideals. This is an important result but the proof uses a significant amount of commutative algebra and so instead of reproducing it here, we reference the reader to three proofs in increasing order of succinctness. [4] pg 765; [1] pg 95 ; [5] pg 10

Theorem 3.10 (Milne 3.29)**.** *If A is a Dedekind Domain with field of fractions K and L is a finite separable extension of K, then B, the integral closure of A in L is a Dedekind Domain. In particular, since $\mathbb{Z}$ clearly has the Dedekind Domain property, the ring of integers of a number field is a Dedekind Domain.*

We remind the reader that an element of L is separable if its minimal polynomial over K has distinct roots and that L is a separable extension of K if every element in L is so. Any finite field or field of characteristic zero can only have separable extensions, so this is not a serious restriction in our present situation.

Given $A \subset B$ rings such that B is a free A-module of rank n, we define three very important functions from B to A.

Definition 3.11. Given $b \in B$ and a basis $e_1, ..., e_n$ of A, there exists a matrix M_b which, when applied to $x \in B$ gives bx. We define the trace of b, $Tr(b)$, to be the trace of this matrix and the norm $N(b)$ to be the determinant. We define the discriminant of an n-element subset $\{b_1, ..., b_n\} \subset B$ to be $\det(Tr(b_i b_j))$.

The following propositions are very useful for analyzing algebraic extensions of fields but they are also useful in other situations (for instance, rings of integers as $\mathbb{Z}$-modules). Thus, care has been taken to present results in terms of free modules in general rather than just vector spaces.

Proposition 3.12. *The Norm and Trace of an element are independent of the choice of basis of B. Norm and Trace satisfy for all $\alpha, \beta \in B$ and $a \in A$:*

1) $N(\alpha\beta) = N(\alpha)N(\beta)$, $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$
2) $Tr(a\beta) = aTr(\beta)$
3) $N(a) = a^n$, $Tr(a) = na$

Proof. Suppose $f_1, ..., f_n$ is a new basis and U is the corresponding change of basis matrix. Then $\det(UM_bU^{-1}) = \det(U)\det(M_b)\det(U^{-1}) = \det(UU^{-1})\det(M_b) = \det(M_b)$. For Trace, we observe that $Tr(CD) = \sum_{ij} C_{ij}D_{ji} = Tr(DC)$. Thus, $Tr(U(M_bU^{-1})) = Tr(M_bU^{-1}U) = Tr(M_b)$.

Property 1) follows immediately from the behavior of the determinant and trace operations on matrices. If $\beta \in B$, and $\beta e_i = \sum_{j=1}^{n} a_{ij}e_j$, then we see that $a\beta e_i = \sum_{j=1}^{n} aa_{ij}e_j$. Thus, taking traces of the corresponding matrices, $Tr(a\beta) = aTr(\beta)$. Since $a \in A$, M_a is a scalar matrix with a on the diagonal, and so property 3) follows. □

Proposition 3.13. *If $e_1, ..., e_n$ is a basis of B, and $f_1, ..., f_n$ are elements in B and U is the matrix of coefficients for the f_i as a linear combination of e_j, then $disc(f_1, ..., f_n) = \det(U^2)disc(e_1, ..., e_n)$.*

Proof. Take the matrix

$$[Tr(f_k f_l)] = [Tr((\sum_{i=1}^{n} u_{ik}e_i)(\sum_{j=1}^{n} u_{jl}e_j))] = [\sum_{i,j} u_{ik}u_{jl}Tr(e_ie_j)] = U[Tr(e_i, e_j)]U^T$$

So taking determinants of both sides gives the desired result. □

Proposition 3.14. *If L/K is a finite separable extension of fields then if $Hom(L/K)$ denotes the different embeddings of L/K into its Galois closure,*
$N_{L/K}(\alpha) = \prod_{\sigma \in Hom(L/K)} \sigma(\alpha)$ *and* $Tr(\alpha) = \sum_{\sigma \in Hom(L/K)} \sigma(\alpha)$.

Proof. For each $\sigma \in \mathrm{Hom}(L/K)$, we see that $\sigma(\alpha)$ is some other root of the minimal polynomial of α. Thus, we see that $\prod_{\sigma \in \mathrm{Hom}(L/K)} \sigma(\alpha)$ is simply the product of all the roots of the minimal polynomial of α, raised to the exponent $[L : K[\alpha]]$ and similarly, that $\sum_{\sigma \in \mathrm{Hom}(L/K)} \sigma(\alpha)$ is the sum of all the roots multiplied by $[L : K[\alpha]]$. If a_0, a_{n-1} are the last and second coefficients of the minimal polynomial of α, then we see that these products and sums are just $(-1)^{[L:K]}a_0^{[L:K[\alpha]]}$ and $-[L : K[\alpha]]a_{n-1}$ respectively.

We must show that the definition of norm and trace we have given also yields these numbers. First, we consider the case where $L = K[\alpha]$ and take the basis $1, \alpha, ..., \alpha^{n-1}$. Then α satisfies the characteristic polynomial of the matrix M_α. But the characteristic polynomial is monic, and of the same degree as the minimal polynomial of α (since the size of M_α corresponds to $[L : K]$) and so must be the minimal polynomial. Then the determinant and trace of M_α are precisely $(-1)^{[L:K]}a_0$ and $-a_{n-1}$ where a_0, a_{n-1} are the last and second coefficients of this minimal polynomial.

In the general case, let $\beta_1, ..., \beta_k$ be a basis of $L/K[\alpha]$ and $1, \alpha, ..., \alpha^{l-1}$ be a basis of $K[\alpha]$. Then the products $\beta_i\alpha^j$ form a basis of L/K. Then if (a_{ij}) are the elements of M_α, we see that $\alpha \cdot \alpha^i\beta_j = \sum_{r=0}^{l-1} a_{ri}\alpha^r\beta_j$ and so the matrix is simply blocks of M_α down the diagonal and zeroes elsewhere. Thus, the determinant and trace of this matrix are what we want. □

Proposition 3.15. *If $L \supset K \supset F$ are finite separable extensions of fields, then $Tr_{L/F} = Tr_{K/F} \circ Tr_{L/K}, N_{L/F} = N_{K/F} \circ N_{L/K}$.*

Proof. If we take the Galois closure $\overline{L}$ of L over F, then there is a natural action of $\mathrm{Gal}(\overline{L}/F)$ on $\mathrm{Hom}(L/F)$ given by $g \cdot \sigma = g \circ \sigma$ as well as an action on $\mathrm{Hom}(K/F)$ of the same form. Then since every element of $\mathrm{Hom}(L/F)$ lifts to an element of this Galois group and groups act transitively on themselves, this action must be transitive.

Moreover, there is a natural surjection $R : \mathrm{Hom}(L/F) \to \mathrm{Hom}(K/F)$ given by $\sigma \mapsto \sigma|_K$ and this map is $\mathrm{Gal}(\overline{L}/F)$-equivariant. Note that $\mathrm{Hom}(L/F), \mathrm{Hom}(K/F)$ are not necessarily groups and so we cannot call R a homomorphism. However, we can work out the size of the pre-image of each point by noticing that the action of $\mathrm{Gal}(\overline{L}/F)$ is transitive on both sets and so the stabilizers are all the same cardinality. Thus, if x, y are the sizes of stabilizers in the $\mathrm{Hom}(L/F), \mathrm{Hom}(K/F)$-actions then the pre-image of a point has y/x elements and this is the same for each point. But the pre-image of the identity homomorphism is just $\mathrm{Hom}(L/K)$. The upshot of this is that the different pre-images partition $\mathrm{Hom}(L/F)$ into sets of the same cardinality.

We would like to show the set of pairs $\{\sigma, \gamma\}$ for $\sigma \in \mathrm{Hom}(K/F), \gamma \in \mathrm{Hom}(L/K)$ is in bijection with $\mathrm{Hom}(L/F)$ and moreover, that if for each $\sigma \in \mathrm{Hom}(K/F)$ we choose some lift $\overline{\sigma} \in \mathrm{Gal}(\overline{L}/K)$, then the set $\{(\overline{\sigma} \circ \gamma)_L\}$ is precisely $\mathrm{Hom}(L/F)$. To show this, we need to show that if $\overline{\sigma'}, \overline{\sigma}$ are lifts of σ', σ respectively, $\gamma, \gamma' \in \mathrm{Hom}(L/K)$, and we have $(\overline{\sigma'} \circ \gamma')_L = (\overline{\sigma} \circ \gamma)_L$, then $\sigma = \sigma'$ and $\gamma = \gamma'$. First we observe that γ, γ' fix K and so $(\overline{\sigma'})_L, (\overline{\sigma})_L$ must be pre-images of the same point under R and so $\sigma = \sigma'$. Applying $\overline{\sigma}^{-1}$ to both sides gives $\gamma = \gamma'$.

It follows that if $\overline{\sigma}$ is some arbitrary element in $R^{-1}(\sigma)$,

$$N_{K/F}(N_{L/K}(\alpha)) = \prod_{\sigma \in \mathrm{Hom}(K/F)} \sigma\Big(\prod_{\gamma \in \mathrm{Hom}(L/K)} \gamma(\alpha)\Big) = \prod_{\sigma \in \mathrm{Hom}(K/F)} \overline{\sigma}\Big(\prod_{\gamma \in \mathrm{Hom}(L/K)} \gamma(\alpha)\Big)$$

$$= \prod_{\sigma \in \mathrm{Hom}(K/F), \gamma \in \mathrm{Hom}(L/K)} \overline{\sigma}(\gamma(\alpha)) = \prod_{\eta \in \mathrm{Hom}(L/F)} \eta(\alpha) = N_{L/F}(\alpha)$$

The same is true for Trace. □

Proposition 3.16. *If $e_1, ..., e_n$ is a basis of B, then $f_1, ..., f_n$ is also a basis of B if and only if $disc(e_1, ..., e_n)$, $disc(f_1, ..., f_n)$ differ by the square of a unit of A.*

Proposition 3.17. *$f_1, ..., f_n$ is a basis if and only if the transformation matrix U is invertible if and only if the determinant is a unit. The discriminants differ by the square of this determinant.*

Proof. These propositions follow directly from 3.13. The key fact is that U takes bases to bases if and only if it is invertible, if and only if $\det(U)$ is a unit. □

For B a free A-module, we can define $\text{disc}(B/A)$ to be the set of discriminants of bases of B as an A-module. In general, this is an element in the collection of cosets $A/(A^*)^2$. However, for the case that $A = \mathbb{Z}$, we observe that 1 is the only square of a unit, so that $\text{disc}(B/A)$ is a well-defined integer.

Proposition 3.18 (Milne 2.24)**.** *Let $A \subset B$ and assume B is a free A-module of rank m and $disc(B/A) \neq 0$. $\gamma_1, ..., \gamma_m$ form a basis for B as an A-module if and only if $(disc(\gamma_1, ..., \gamma_m)) = (disc(B/A))$ as ideals.*

Proof. By the previous propositions, $\gamma_1, ..., \gamma_m$ form a basis for B precisely when the discriminant differs from any element of $\text{disc}(B/A)$ by the square of a unit. But then any element of the set of $\text{disc}(B/A)$ is in $(\text{disc}(\gamma_1, ..., \gamma_m))$ and so $(\text{disc}(\gamma_1, ..., \gamma_m)) = (\text{disc}(B/A))$. Conversely, if the discriminant ideals are the same, there is some unit u so that $\text{disc}(\gamma_1, ..., \gamma_m)u = k$ for some $k \in \text{disc}(B/A)$. Thus, $\gamma_1, ..., \gamma_m$ gives a basis. □

Proposition 3.19. *If $K[\alpha]$ is a finite separable extension of a field K and f is the minimal polynomial of α over K, then $disc(1, \alpha, ..., \alpha^n) = \prod_{i<j} (\alpha_i - \alpha_j)^2$ where $\alpha_1, ..., \alpha_n$ are the different roots of f.*

Proof. We have $\text{disc}(1, \alpha, ..., \alpha^n) = \det(Tr(\alpha^i \alpha^j)) = \det(\sum_{k=1}^{n} \sigma_k(\alpha^i \alpha^j))$

$= \det(\sum_{k=1}^{n} \sigma_k(\alpha^i)\sigma_k(\alpha^j)) = \det(\sigma_k(\alpha^i)) \det(\sigma_k(\alpha^j)) = \det(\sigma_k(\alpha^i))^2 = \det({\alpha_k}^i)^2$

(where σ_k are the homomorphisms of $K[\alpha]$ into its Galois closure). Now, by manipulating the matrix of this determinant we can show that the determinant is equal to $\prod_{k<i} (\alpha^k - \alpha^i)^2$ which is what we wanted. □

We observe that the discriminant is symmetric in the roots of f and therefore is fixed by every homomorphism of $K[\alpha]$ into its Galois closure. Thus, the discriminant lies in K.

The following proposition gives a fairly general situation in which we can use the above theory. In particular, this will show that the ring of integers of a number field is a free $\mathbb{Z}$-module.

Proposition 3.20 (Milne, 2.29)**.** *Let A be an integrally closed domain with field of fractions K and let B be the integral closure of A in a separable extension L of K of degree m. Then there exist free (and finitely-generated) A-sub-modules M, M' of L such that $M \subset B \subset M'$. In particular, if A is a PID, then we recall that a sub-module of a free module over a PID is itself free and so B is free. B is finitely generated as long as A is Noetherian.*

We first prove the following lemma.

Lemma 3.21. *If $e_1, ..., e_m$ is a basis for L over K, then there exists a basis $e'_1, ..., e'_m$ so that $Tr(e_i e'_j) = \delta_{ij}$. This is the dual basis of $e_1, ..., e_m$.*

Proof. Pick some i. We write $e_i' = a_{1i}e_1 + ... + a_{mi}e_m$. Then each condition $Tr(e_k e_i') = 0$ gives us an equation $0 = a_{1i}Tr(e_k e_1) + ... + a_{mi}Tr(e_k e_m)$ and $Tr(e_i e_i') = 1$ gives us $1 = a_{1i}Tr(e_i e_1) + ... + a_{mi}Tr(e_k i e_m)$. Then if we consider what these equations are telling us in matrix form, they say that if $a = (a_{1i}, ..., a_{mi})$, then $Ma = (0, 0, ..., 1, 0, ..., 0)$ with 1 in the ith position. Thus, if we apply M^{-1} to both sides, we see that the coefficients in the e_i basis of e_i' are just the result of applying M^{-1} to the coefficient vector for e_i. Since M^{-1} is a linear transformation, it takes bases to bases and so the e_i' form a basis. □

We observe that by construction, if each e_i is integral, then each e_i' is integral. Now we prove the proposition.

Proof. Let $e_1, ..., e_m$ be a basis of L. By proposition 3.6 we have that there is some d so that de_i is integral for each i. $de_1, ..., de_m$ is still a basis for L so we can assume that $e_1, ..., e_m$ were all elements of B from the start. Now by the previous lemma, we have a basis $e_1', ..., e_m'$ so that $Tr(e_i e_j') = \delta_{ij}$. To conclude the proof, we need to show that $Ae_1 + ... + Ae_m \subset B \subset Ae_1' + ... + Ae_m'$.

The first inclusion is clear since the e_i are elements of B. Pick some $\beta \in B$ and write $\beta = b_1 e_1' + ... + b_m e_m'$. It suffices to show each $b_i \in A$. For each i, we have $\beta, e_i \in B$ so $Tr(\beta e_i) \in A$. But $Tr(\beta e_i) = \sum_{j=1}^{m} b_j Tr(e_j' e_i) = b_i$. □

4. Extending Valuations

Suppose L/K is a finite separable extension. If $P \subset O_L$ is a prime ideal, then we define a valuation on L as follows. $v(\alpha)$ for αO_L is the exponent of the maximal power of P that divides the ideal (α). Then we extend v to L by defining $v(\frac{\alpha}{\beta}) = v(\alpha) - v(\beta)$.

Proposition 4.1. *The above construction is indeed a valuation. Moreover, we observe that the valuation is clearly discrete.*

Proof. Clearly, $v(\alpha) = 0$ if and only if $(\alpha) = 0$ if and only if $\alpha = 0$. We also see that $v(\alpha\beta) = v(\alpha) + v(\beta)$. Consider $v(\alpha + \beta)$ for $\alpha, \beta \in O_L$. P^n is in the factorization of α precisely when $(\alpha) \subset P^n$. Then if $\min(v(\alpha), v(\beta)) = n$, then $(\alpha) \subset P^n, (\beta) \subset P^n$ and so $(\alpha, \beta) \subset P^n$. Thus, $v(\alpha + \beta) \geq \min(v(\alpha), v(\beta))$. These statements hold for L in general if we consider fractional ideals. □

Theorem 4.2 (Milne 7.38)**.** *Let K be complete with respect to the discrete valuation v and let L be a finite separable extension of degree n. Then v extends uniquely to a complete absolute value w on L. For all $\beta \in L$, $w(\beta) = \frac{1}{n} v(N_{L/K}(\beta))$.*

By proposition 2.7, L is complete with respect to w.

Definition 4.3. Let K be a field that is complete with respect to the discrete valuation v and maximal ideal (π). Then $f \in D_K[X]$ is primitive if $\min(v(a_i)) = 0$ for a_i the coefficients of f.

Theorem 4.4 (Neukirch 4.6, Milne 7.33)**.** *(Hensel's Lemma)*

Take conditions as in the previous definition and $f \in D_K[x]$ primitive. Then if $f \equiv \overline{g}\overline{h} \mod (\pi)$ and $\overline{g}, \overline{h}$ are relatively prime in $(D_K/(\pi))[x]$, there exist $g(x), h(x) \in D_K[x]$ so that $f(x) = g(x)h(x)$, $\overline{g(x)} \equiv g(x), \overline{h(x)} \equiv h(x) \mod (\pi)$, $\deg(g) = \deg(\overline{g}), \deg(h) = \deg(\overline{h})$, and $(g(x), h(x)) = D_K[x]$.

Proof. The proof proceeds by recursively constructing g, h in $D_K/(\pi)^k$ for successively higher values of k. The details can be found in the cited references. □

Proposition 4.5. *Let K be complete with respect to the discrete valuation D_K. Then if $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$ is irreducible and $a_0a_n \neq 0$, then $\min(v(a_i)) = \min(v(a_0), v(a_n))$.*

Proof. Each $a_i \in K$ and so we can multiply through by some power of a generator π of D_K so that we get some $f'(x)$ whose coefficients are all in D_K and $\min(v(a_i)) = 0$. Then let a_r be the first coefficient satisfying $v(a_r) = 0$. Then $f'(x) \equiv x^r(a_r + a_{r+1}x + ... + a_nx^{n-r}) \mod (\pi)$. Now, if both $v(a_0), v(a_n)$ are greater than 1, then $0 < r < n$, in which case $f'(x)$ has coprime factors modulo (π) but not in D_K (since $f(x)$ is irreducible) which contradicts Hensel's Lemma. □

Proposition 4.6. *Suppose that L is a separable extension of K of degree n with K complete with respect to a discrete valuation v. Then if w is the extension of v to L, we have that D_L is the integral closure of D_K in L.*

Proof. $D_L \supset D_K$ and D_L is integrally closed in L (D_L is a PID and so UFD and so by proposition 3.7 is integrally closed). Thus, D_L contains the integral closure of D_K in L.

Since $w(\alpha) = \frac{1}{n}v(N_{L/K}(\alpha))$ for each $\alpha \in L$, we have that D_L is precisely the set of elements of L whose norm is in D_K. Pick such an α and let $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_0$ be the minimal polynomial of α in L. Then $f(x)$ is irreducible and so the minimal valuation of the coefficients is $\min(v(a_0), v(1))$. But $v(1) = 0$ and $v(a_0) \geq 0$ since $N_{L/K}(\alpha) \in D_K$ by assumption and up to a sign, this norm is just a power of a_0. Thus, all the coefficients of f are in D_K and so α is integral over D_K. This proves the opposite inclusion. □

To finish this section, we briefly discuss the relation between the ideal structure in the number fields O_L, O_K where L is a finite separable extension of K.

Proposition 4.7. *If B is a finitely generated A-module and is also a ring, and I is a proper ideal of A, then IB is a proper ideal.*

Proof. If IB is not a proper ideal, then $IB = B$ and so by the Nakayama Lemma, there is some $i \in I$ so that $(1+i)B = 0$. But then $(1+i)1 = 0$ and so $i = -1$ which contradicts $i \in I$ (since I is proper). Thus, IB is a proper ideal. □

Suppose P is a non-zero prime ideal of O_K. Then PO_L is a proper ideal and so factors into a product of prime ideals. Thus, $PO_L = \prod_{i=1}^{m} Q_i^{e_i}$ for Q_i prime. Observe that if P, P' are primes in O_L, then if Q is a prime in O_L it can only contain one of P, P' (since otherwise since non-zero primes are maximal in a Dedekind domain, it would contain all of O_K and so all of O_L). Thus, Q is in the factorization of precisely one prime in O_K and so we can unambiguously call e_i the ramification

index of Q_i over O_K. Now, $Q_i \cap O_K$ is a prime ideal in O_K and so must be P. So $O_L/Q_i \supset O_K/P$. Both of these are fields and so we call the degree of the extension $[O_L/Q_i : O_K/P] = f$ the inertia degree of Q_i over O_K.

Proposition 4.8 (Neukirch 8.2)**.** *If $[L : K] = n$ is an extension of number fields and $P \subset O_K$ a prime that factors in O_L as $PO_L = \prod_{i=1}^{m} {Q_i}^{e_i}$ and inertia degrees f_i, then $\sum_{i=1}^{m} e_i f_i = n$*

Proof. First we consider the case where $K = \mathbb{Q}$. We take the completion of O_L as a $\mathbb{Z}$-module at the prime p. On the one hand, O_L is a free $\mathbb{Z}$-module (proposition 3.20) and so is isomorphic as a $\mathbb{Z}$-module to $\mathbb{Z}^d$ for some d so that the completion is $\varprojlim \mathbb{Z}^d/p^n\mathbb{Z}^d = {\mathbb{Z}_p}^d$ (the inverse limit commutes with the direct product since completions preserve exact sequences). On the other hand, $\varprojlim O_L/p^n O_L \equiv \varprojlim O_L/(\prod_{i=1}^{m} {Q_i}^{e_i})^n O_L \equiv \bigoplus_{i=1}^{m} \varprojlim O_L/({Q_i}^{e_i})^n O_L$. The completion at an ideal I is the same as the completion at I^k (having the value at $O_L/I^k O_L$ of some coherent sequence automatically determines the value at $O_L/I^j O_L$ for $j \leq k$. Thus, $\bigoplus_{i=1}^{m} \varprojlim O_L/({Q_i}^{e_i})^n O_L \equiv \bigoplus_{i=1}^{m} \varprojlim O_L/{Q_i}^n O_L$.

Now, if we pick some element $O_{L_i} = \varprojlim O_L/{Q_i}^n O_L$ of this product, then we can determine the dimension of this completion as a $\mathbb{Z}_p$-module. Completing O_L with respect to the prime Q_i gives D_{L_i}, the discrete valuation ring of L_i where L_i denotes the completion of L at Q_i. If we take a maximal collection $a_1, ..., a_m$ of $\mathbb{Z}_p$-linearly independent units of O_{L_i}, then we see that this has dimension $[O_{L_i}/Q_i : \mathbb{Z}_p/p\mathbb{Z}_p] = f_i$. The $\mathbb{Z}_p$ span of such a set only includes elements with valuation some multiple of $v(p)$. Now, if π is a uniformizer, consider the set of elements $a_i\pi^j$ for $0 \leq j \leq e_i - 1$. Then if we have a dependence relation over $\mathbb{Z}_p$ of the form $\sum_{i,j} c_{ij} a_i \pi^j = 0$. Now, the π^j are all independent and we must have $\sum_i c_{ij} a_i = 0$ and so all of the c_{ij} must be 0. Thus, these elements form an independent (and spanning) set for O_{L_i} of dimension $e_i f_i$ and so we have $d = \sum_i e_i f_i$. We conclude by noting that since the field of fractions of O_L is L, the dimension of O_L over $\mathbb{Z}$ is the same as L over $\mathbb{Q}$. Thus, $n = d = \sum_i e_i f_i$.

For the case when $K \neq \mathbb{Q}$, we use the fact that degrees are multiplicative and that we know the situation for $K/\mathbb{Q}$ and $L/\mathbb{Q}$. □

Proposition 4.9 (Milne 3.35)**.** *Let L/K be a finite separable extension of number fields. Then if O_L is a free O_K module and P is a prime of O_K, P ramifies in O_L if and only if $P | disc(O_L/O_K)$.*

5. Computing Rings of Integers Locally

We eventually aim to show that if ζ_N is a primitive Nth root of unity over $\mathbb{Q}$, then the ring of integers of $\mathbb{Q}(\zeta_N)$ is $\mathbb{Z}[\zeta_N]$. We attack the problem locally by working at the completion of each prime and then use this to piece together the structure of the ring of integers in the global case.

Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial satisfying Eisenstein's criterion and let π be some root of f. Consider the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ at the prime ideal (p).

Then since $\mathbb{Q}[\pi]$ is a finite algebraic extension of $\mathbb{Q}$, we must certainly have that $K = \mathbb{Q}_p[\pi]$ is finite and of some degree e.

We observe that the standard valuation v on $\mathbb{Q}_p$ extends to a discrete valuation w on all of K given by $w(\alpha) = \frac{1}{e}v(N_{K/\mathbb{Q}_p}(\alpha))$. Also, $w(\pi) = v(N_{K/\mathbb{Q}_p}(\pi)) = v(a \cdot p)$ where $a \in \mathbb{Q}$ and $w(a) = 0$ (by the Eisenstein property). Thus, $w(\pi) = v(a \cdot p) = v(a) + v(p) = 0 + 1 = 1$. So π generates the unique maximal ideal of the valuation ring D_K corresponding to w.

Proposition 5.1. *pD_K factors as $(\pi)^e$ in K.*

Proof. pD_K is some ideal in D_K and so must be of the form $(\pi)^n$ for some n. But $(\pi)^n$ is generated by p and $w(p) = 1 = w(\pi^e)$. Thus, $n = e$. □

Proposition 5.2. *$D_K/(\pi) \cong D_{\mathbb{Q}_p}/(p)$ under the natural embedding.*

Proof. Note that $D_{\mathbb{Q}_p/(p)}$ is a subfield of D_K and that $(\pi) \cap \mathbb{Q}_p = (p)$ so that $D_{\mathbb{Q}_p}/(p) \subset D_K/(\pi)$. Then if $f = [D_K/(\pi) : D_{\mathbb{Q}_p}/(p)]$ is the inertia degree of (π), then we recall prop 4.8 which shows $ef = [K : \mathbb{Q}_p] = e$. Thus, $f = 1$ and so we have the desired result. □

Lemma 5.3. *If $x \in D_K$, there exists some $a_0 \in \mathbb{Z}$ so that $w(x - a_0) \geq 1$.*

Proof. From the previous proposition, we know that $D_K/(\pi) = \mathbb{Z}_p/(p)$. From proposition 2.8, we know that since $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ at p, that $\mathbb{Z}_p/(p) \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$ under the natural embedding. Now, $0, 1, ..., p-1$ is a collection of representatives of each equivalence class of this last quotient. Thus, we consider x modulo π and get that $x \equiv a_0 \mod (\pi)$ for $a_0 \in \mathbb{Z}$. Then $x = a_0 + x_1\pi$ for $x_1 \in D_K$ and $w(x - a_0) \geq 1$. □

Proposition 5.4. *$D_K = \mathbb{Z}_p[\pi]$*

Proof. Pick $x \in D_K \subset K[\pi]$. By the lemma, we can take some $a_0 \in \mathbb{Z}$ so that $x = a_0 + x_1\pi$ for some $x_1 \in D_K$. We can then apply the lemma to x_1 to get a_1 so that $x_1 = a_1 + x_2\pi$ and, therefore $x = a_0 + a_1\pi + x_2\pi^2$. It is clear that we can continue this process to any finite number of stages. Let s_n be the expansion after finitely many stages. Now we note that if we have a term of the form $a_i\pi^i$ for $i \geq e$ then we can use the minimal polynomial of π to rewrite this as an expansion in $1, \pi, ..., \pi^{e-1}$ with coefficients in $\mathbb{Z}$. Thus, we see that each s_n can be written as a sum of terms of the form $a_i\pi^i$ with $0 \leq i < e$. Now, $|x - s_n|_w \leq \frac{1}{p^n}$ and so (s_n) converges in K to x. In particular, this means (s_n) is Cauchy. Now by proposition 2.7 we see that the given absolute value $|\cdot|_w$ is topologically equivalent to the max norm given by $||a_0 + a_1\pi + ... + a_{e-1}\pi^{e-1}|| = \max(|a_i|_v)$. Thus, we observe that for each i, if we write $s_n = a_{0,n} + a_{1,n}\pi + ... + a_{e-1,n}\pi^{e-1}$, then the sequence $(a_{i,n})$ must also be Cauchy. This is a sequence of integers and so converges to some $a_i \in \mathbb{Z}_p$. Then clearly s_n converges to $a_0 + ... + a_{e-1}\pi^{e-1} \in \mathbb{Z}_p[\pi]$. Since a sequence can only converge to one point in a Hausdorff space such as $\mathbb{Q}_p[\pi]$ (our absolute value gives a metric and all metrizable spaces are Hausdorff), this must be x and so $x \in \mathbb{Z}_p[\pi]$. □

Proposition 5.5. *Let p be a prime number in $\mathbb{Z}$ and let K be a finite extension of $\mathbb{Q}_p$. Let $L = K[\alpha]$ be a degree n extension such that the minimal polynomial of α has coefficients in $\mathbb{Z}_p$ and let $\Delta = disc(1, \alpha, ..., \alpha^{n-1})$. Then $\Delta \in \mathbb{Z}_p$ and if Δ is a unit in $\mathbb{Z}_p$, then $D_L = D_K[\alpha]$.*

Proof. To show that $\Delta \in \mathbb{Z}_p$, it suffices to show that $Tr(\alpha^i \alpha^j) \in \mathbb{Z}_p$ for each i, j. But this follows from the fact that the matrix given by the operation of α on D_L contains only elements of $\mathbb{Z}_p$ since the minimal polynomial of α has coefficients in $\mathbb{Z}_p$.

For the other part of the result, we aim to apply proposition 3.18 to $1, \alpha, ..., \alpha^{n-1}$ since it would tell us that $1, \alpha, ..., \alpha^{n-1}$ is a basis for D_L if and only if $(\Delta) = (\text{disc}(D_L/D_K))$. Since $D_k[\alpha] \subset D_L$, we have $(\Delta) \subset (\text{disc}(D_L/D_K))$. Now, Δ is a unit and so both ideals are just (1).

To apply prop 3.18, we need to show that D_L is a free D_K-module. To do this, we aim to apply prop 3.20 for which we need to show that D_K is integrally closed, and that D_L is the integral closure of D_K in D_L and D_K is a PID. To prove the first two, it suffices to show that if we have an extension L over K, then the integral closure of D_K is D_L (but this is just proposition 4.5). The third requirement is satisfied in virtue of the fact that D_K is a discrete valuation ring. □

6. Cyclotomic Extensions

Definition 6.1. An Nth root of unity is a root of the polynomial in $x^N - 1$. An Nth root of unity ζ is primitive if there is no $0 < M < N$ such that $\zeta^M = 1$.

Proposition 6.2. *The polynomial* $\frac{x^{p^\alpha}-1}{x^{p^{\alpha-1}}-1} = \sum_{i=0}^{p-1} x^{p^{\alpha-1}i}$ *is the minimal polynomial of the primitive* p^α *roots of unity where* p *is prime.*

Proof. Clearly, any primitive p^α root of unity satisfies this equation and all its roots are primitive p^α roots of unity. To show this cyclotomic polynomial is irreducible, it suffices to show that $\frac{(x+1)^{p^\alpha}-1}{(x+1)^{p^{\alpha-1}}-1}$ is Eisenstein. But modulo p, $\frac{(x+1)^{p^\alpha}-1}{(x+1)^{p^{\alpha-1}}-1} = \sum_{i=0}^{p-1}(x+1)^{p^{\alpha-1}i} \equiv \sum_{i=0}^{p-1}(x^{p^{\alpha-1}}+1)^i = \frac{(x^{p^{\alpha-1}}+1)^p-1}{x^{p^{\alpha-1}}}$, which by the binomial theorem has all but the first coefficient congruent to 0 mod p. Finally, the constant term in this expansion is given by $\sum_{i=0}^{p-1}(0+1)^{p^{\alpha-1}i} = p$. Thus, the polynomial is indeed Eisenstein. □

Proposition 6.3. *There are* $\varphi(N)$ *primitive* N*th roots of unity where* $\varphi(N)$ *is Euler's* φ*-function and they satisfy a polynomial of degree* $\varphi(N)$ *that divides* $X^N - 1$.

Lemma 6.4. $\sum_{d|N} \varphi(d) = N$.

Proof. The group $\mathbb{Z}/N\mathbb{Z}$ is cyclic and so there is precisely one subgroup of order d for each d dividing N. Then each such subgroup has $\varphi(d)$ generators and these are of order d. Thus, $\mathbb{Z}/N\mathbb{Z}$ has $\varphi(d)$ elements of order d. But any element has order d for some d dividing N and so $\sum_{d|N} \varphi(d) = N$. □

Proof. We prove the proposition by induction on N. Observe this is trivial for $N = 1$.

Suppose we have shown this for every natural less than N. Then if we consider $x^N - 1$, we can divide out all the polynomials for the primitive dth roots of unity for each d dividing N. By the induction hypothesis, these all have degree $\varphi(d)$ and so by the lemma, we are left with a polynomial of degree $\varphi(N)$ whose roots are precisely the primitive Nth roots of unity. □

We call the polynomial we found in the above proposition Φ_N.

Proposition 6.5. *Φ_N is irreducible.*

Proof. Take some p not dividing N. Then the derivative of $X^N - 1$ is NX^{N-1}. The function and its derivative don't share any roots modulo p and so $X^N - 1$ has all distinct roots modulo p. $\Phi_N | X^N - 1$ and therefore this has distinct roots as well. Now, working over $\mathbb{Z}/p\mathbb{Z}$, we see that for any polynomial f, if ζ is a root of f and K is the splitting field of f over $\mathbb{Z}/p\mathbb{Z}$, then in K, $f(\zeta^p) = f(\zeta)^p = 0$. In other words, since the Frobenius map is indeed a field automorphism, it permutes the roots of f. What this means is that if ζ is a primitive Nth root of unity with minimal polynomial f over $\mathbb{Q}$, then ζ^p is a root of f modulo p. But ζ^p can only be a root of one factor of $x^N - 1$ modulo p (since its roots are distinct) and so ζ^p is a root of f over $\mathbb{Q}$. This works for each prime not dividing N and so we see that since any integer coprime to N is a product of such primes, all primitive Nth roots of unity have the same minimal polynomial over $\mathbb{Q}$, which must therefore be Φ_N. □

Proposition 6.6. *The splitting field of Φ_N has Galois group $(\mathbb{Z}/N\mathbb{Z})^*$.*

Proof. If $\zeta = e^{\frac{2\pi i}{N}}$, the roots of Φ_N are given by ζ^a for $(a, N) = 1$. Notice that adjoining a single root gives all the others and so the splitting field K is degree $\varphi(N)$. Observe that $\zeta^a\zeta^b = \zeta^{a+b}$. Thus, there is a group isomorphism $T : \{\zeta^a : 0 \leq a \leq n\} \to \mathbb{Z}/N\mathbb{Z}$ given by $T(\zeta^a) = a$. Then for any automorphism σ, we have $\sigma(\zeta^a) = \sigma(\zeta)^a$ so that the action of σ on the Nth roots of unity is determined by $\sigma(\zeta)$. If $\sigma(\zeta) = \zeta^b$, then σ corresponds to the automorphism defined by multiplication by b in $\mathbb{Z}/N\mathbb{Z}$. In other words, $\mathrm{Gal}(K/\mathbb{Q}) \subset (\mathbb{Z}/N\mathbb{Z})^*$. By degree considerations, this inclusion is an equality. □

Proposition 6.7. *If ζ_m, ζ_n are primitive mth, nth roots of unity respectively and $(m, n) = 1$, then Φ_n is the minimal polynomial of ζ_n over $\mathbb{Q}(\zeta_m)$.*

Proof. Since $(m, n) = 1$, the φ-function is multiplicative and so $\varphi(mn) = \varphi(m)\varphi(n)$. Also, we can pick integers x, y so that $xm + yn = 1$. Then ${\zeta_m}^y + {\zeta_n}^x$ is a primitive mnth root of unity, and so $\mathbb{Q}(\zeta_m, \zeta_n)$ contains all primitive mnth roots of unity. Since this splitting field is degree $\varphi(mn)$, adjoining ζ_n to $\mathbb{Q}(\zeta_m)$ must be a degree $\varphi(n)$ extension and so Φ_n is the minimal polynomial. □

Proposition 6.8. *The discriminant of Φ_{p^α} over $\mathbb{Q}$ is*

$$disc(1, \zeta, ..., \zeta^{p^\alpha - 1}) = (-1)^{\varphi(p^\alpha)(\varphi(p^\alpha)-1)/2} p^{(\alpha p - \alpha - 1)p^{\alpha-1}}$$

Proof. Let K be the splitting field of Φ_{p^α} over $\mathbb{Q}$. The discriminant is given by $\prod_{i<j} (\zeta^i - \zeta^j)^2$ where ζ^i, ζ^j are the roots of Φ_{p^α}. We observe that this is simply

$$(-1)^{\varphi(p^\alpha)(\varphi(p^\alpha)-1)/2} \prod_i \Phi'_{p^\alpha}(\zeta^i) = (-1)^{\varphi(p^\alpha)(\varphi(p^\alpha)-1)/2} N_{K/\mathbb{Q}}(\Phi'_{p^\alpha}(\zeta))$$

where ζ is some primitive p^αth root of unity. We have $(x^{p^{\alpha-1}} - 1)\Phi_{p^\alpha}(x) = x^{p^\alpha} - 1$. Differentiating both sides, we get

$$p^{\alpha-1}x^{p^{\alpha-1}-1}\Phi_{p^\alpha}(x) + (x^{p^{\alpha-1}} - 1)\Phi'_{p^\alpha}(x) = p^\alpha x^{p^\alpha - 1}$$

If $\zeta = e^{\frac{2\pi i}{p^\alpha}}$ is a root of Φ_{p^α}, then plugging in, we get

$$(\zeta^{p^{\alpha-1}} - 1)\Phi'_{p^\alpha}(\zeta) = p^\alpha \zeta^{p^\alpha - 1}$$

Taking norms, we get

$$N_{K/\mathbb{Q}}(\zeta^{p^{\alpha-1}}-1)N_{K/\mathbb{Q}}(\Phi'_{p^\alpha}(\zeta)) = N_{K/\mathbb{Q}}(p^\alpha \zeta^{p^\alpha-1})$$

The norm on the right hand side is of a constant times a root of Φ_{p^α} which has norm $(-1)^{\varphi(p^\alpha)}$. So the right-hand side is $p^{\alpha\varphi(p^\alpha)}(-1)^{\varphi(p^\alpha)}$. On the left-hand side, we have the norm we want and then the norm of $\zeta^{p^{\alpha-1}}-1$. This is just one less than a primitive pth root of unity. The minimal polynomial is simply $\frac{(x+1)^p-1}{x}$ which has p as its constant term and so has norm $[(-1)^{p-1}p]^{\frac{\varphi(p^\alpha)}{p-1}}$. Thus, the norm that we want is

$$(-1)^{2\varphi(p^\alpha)}p^{(\alpha p-\alpha-1)p^{\alpha-1}} = p^{(\alpha p-\alpha-1)p^{\alpha-1}}$$

and the discriminant we end up with is

$$(-1)^{\varphi(p^\alpha)(\varphi(p^\alpha)-1)/2}p^{(\alpha p-\alpha-1)p^{\alpha-1}}$$

□

Proposition 6.9. *If ζ is a primitive p^αth root of unity (for some prime $p \in \mathbb{Z}$) and q is any prime of $\mathbb{Z}$, then if we denote the splitting field of ζ over $\mathbb{Q}_q$ as K, then $D_K = \mathbb{Z}_q[\zeta]$.*

Proof. If $q = p$, then the minimal polynomial of $\zeta - 1$ over $\mathbb{Q}$ is Eisenstein in $\mathbb{Z}_p$ and irreducible over $\mathbb{Z}_p$. Thus, we can apply proposition 5.4 to show that $D_K = \mathbb{Z}_p[\zeta - 1] = \mathbb{Z}_p[\zeta]$ in this case.

If $q \neq p$, then we have shown that all the roots of Φ_{p^α} are distinct in $\mathbb{Q}$. By proposition 3.19, we see that if n is the degree of the minimal polynomial M of ζ over $\mathbb{Z}_q$, then $\text{disc}(1, \zeta, ..., \zeta^{n-1}) = \prod_{i<j}(\zeta_i - \zeta_j)^2$ where ζ_i are the roots of the minimal polynomial of ζ. Notice, that this must divide $\prod_{i<j}(\zeta_i - \zeta_j)^2 = \text{disc}(1, \zeta, ..., \zeta^{\varphi(p^\alpha)-1})$ in K (where this time the product ranges over all primitive p^αth roots of unity). But we have just computed this discriminant and it is a unit in $\mathbb{Z}_q$ and also K. Thus, the discriminant corresponding to M must also be a unit in $\mathbb{Z}_q$.

If we can show that the minimal polynomial M of ζ over $\mathbb{Q}_q$ has coefficients in $\mathbb{Z}_q$ then by proposition 5.5, we will have $D_K = \mathbb{Z}_q[\zeta]$. But Φ_{p^α} has integer coefficients and $\mathbb{Z} \subset \mathbb{Z}_q$. Thus, by Gauss's Lemma, Φ_{p^α} factors in $\mathbb{Z}_q$ if and only if it factors in $\mathbb{Q}_q$. Thus, $M \in \mathbb{Z}_q[x]$. □

Suppose $K/\mathbb{Q}$ is a finite separable extension. Now pick a primitive element α of K and let $f \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Let $(p) \subset \mathbb{Z}$ be a prime and let $P \subset O_K$ sit over (p). Then we can complete K with respect to the p-adic valuation extended to P and this gives some completion K_P. We have a natural map $T : K \to K_P$ which embeds a canonical copy of $\mathbb{Q}_p$ into K_P. Then if we take the minimal polynomial of $T(\alpha)$ over this copy of $\mathbb{Q}_p$, we see that it is equal to some f_i where f_i is an irreducible factor of f over $\mathbb{Q}_p$. Now, by proposition 2.7, $\mathbb{Q}_p[T(\alpha)]$ is complete and since it contains $T(K)$, we must have $\mathbb{Q}_p[T(\alpha)] = K_P$.

Alternatively, we can consider the polynomial f over $\mathbb{Q}_p$. f factors into irreducible polynomials $f_1, ..., f_r$ over $\mathbb{Q}_p$ and we can pick any factor f_i and adjoin some root α_i to $\mathbb{Q}_p$. Then $\mathbb{Q}_p[\alpha_i]$ is complete and the valuation on $\mathbb{Q}_p$ extends uniquely (proposition 4.2). α_i is some root of f, and so $\mathbb{Q}_p[\alpha_i]$ must contain a copy of K and therefore is a completion of K. Then the intersection of the maximal ideal of the valuation ring with K is some prime P_i of K sitting over p. Thus, we have

shown there is a correspondence between primes sitting over (p) and the extensions of the p-adic valuation to K and the irreducible factors of f over $\mathbb{Q}_p$.

Now, we prove a result that allows one to use the structure of the discrete valuation rings over each $\mathbb{Q}_p$ corresponding to a given extension to compute the ring of integers over $\mathbb{Q}$ of that extension. Specifically, we prove the following proposition.

Proposition 6.10. *Suppose $K/\mathbb{Q}$ is some finite separable extension. Let α be some primitive element of K with minimal polynomial $f \in \mathbb{Z}[x]$. If at each prime ideal P of O_K, we have $D_{K_P} \cong \mathbb{Z}_p[\alpha_i]$ (where p is the prime in $\mathbb{Z}$ that P sits over) for α_i some root of f, then $O_K \cong \mathbb{Z}[\alpha]$ if and only if no prime of $\mathbb{Z}[\alpha]$ splits into distinct primes in O_K.*

One direction of the biconditional is trivial. Before diving into the proof of the second direction, we discuss the proof strategy. We use the algebraic description of completion. Now, O_K is a finite $\mathbb{Z}$-module and so definitely a finite $\mathbb{Z}[\alpha]$-module. Moreover, since α is an algebraic integer by assumption, $\mathbb{Z}[\alpha] \subset O_K$. Moreover, O_K is integral over $\mathbb{Z}[\alpha]$ and so every prime in $\mathbb{Z}[\alpha]$ is the restriction of some prime of O_K to $\mathbb{Z}[\alpha]$. Observe that we have the exact sequence $0 \to \mathbb{Z}[\alpha] \to O_K \to O_K/\mathbb{Z}[\alpha] \to 0$. By Hilbert's basis theorem, $\mathbb{Z}[\alpha]$ is Noetherian and O_K is a finite $\mathbb{Z}[\alpha]$-module and so by the exactness property of completions (proposition 2.9) if we complete at some ideal I, then we have the exact sequence $0 \to \varprojlim \mathbb{Z}[\alpha]/I^n\mathbb{Z}[\alpha] \to \varprojlim O_K/I^nO_K \to \varprojlim (O_K/\mathbb{Z}[\alpha])/I^n(O_K/\mathbb{Z}[\alpha])$. If we can show that the inclusion $\varprojlim \mathbb{Z}[\alpha]/I^n\mathbb{Z}[\alpha] \to \varprojlim O_K/IO_K$ is in fact an isomorphism, then by exactness, this will show that the completion of $O_K/\mathbb{Z}[\alpha]$ at I is $\{0\}$. If P is a prime ideal of $\mathbb{Z}[\alpha]$ containing I, then since for each n, $(O_K/\mathbb{Z}[\alpha])/P^n(O_K/\mathbb{Z}[\alpha])$ is a quotient of $(O_K/\mathbb{Z}[\alpha])/I^n(O_K/\mathbb{Z}[\alpha])$, it will follow that the completion of $O_K/\mathbb{Z}[\alpha]$ at P will be 0 also. If we can show that the completion of $O_K/\mathbb{Z}[\alpha]$ at P for each nonzero prime P is $\{0\}$, then by proposition (2.14) this will mean that $O_K/\mathbb{Z}[\alpha] = \{0\}$ which is the same as $O_K = \mathbb{Z}[\alpha]$ as desired.

If we pick a prime p of $\mathbb{Z}$, then f factors as $\prod_{i=1}^{n} {f_i}^{e_i}$ over $\mathbb{Z}/p\mathbb{Z}$ where each f_i is irreducible and the ${f_i}^{e_i}$ are all pairwise coprime. By Hensel's lemma, each power ${f_i}^{e_i}$ lifts to some factor F_i of f over $\mathbb{Q}_p$ so that we can write $f = \prod_{i=1}^{n} F_i$ where if $i \neq j$, then $(F_i, F_j) = \mathbb{Z}_p[X]$.

Proposition 6.11. *Let I_i be the ideal $(p, f_i(\alpha)^n)$ of $\mathbb{Z}[\alpha] \subset O_K$ where ${f_i}^n$ is the maximal power dividing f of some irreducible factor f_i of f modulo p. Suppose that no prime in $\mathbb{Z}[\alpha]$ splits over O_K. Then every prime P sitting over $p \in \mathbb{Z}$ contains $f_i(\alpha)^n$ for some i and no prime can contain more than one such term. Moreover, $(p, f_i(\alpha)^n)O_K = P^k$ where P^k is some prime sitting over p and containing $f_i(\alpha)^n$.*

Proof. $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(f(x))$ and the prime ideals of this ring are of the form $(p, f_i(\alpha))$ for $p \in \mathbb{Z}$ prime and f_i is an irreducible factor of f modulo p. Since each prime in O_K sits over some prime of $\mathbb{Z}[\alpha]$, each prime contains some $f_i(\alpha)$ and therefore some $f_i(\alpha)^n$. Now, if $i \neq j$, then ${f_i}^n, {f_j}^{n'}$ are coprime modulo p and so in particular, there exist polynomials $r, s, t \in \mathbb{Z}[x]$ so that $r{f_i}^n + s{f_j}^{n'} + pt = 1$. Plugging in α everywhere, we observe that any ideal of O_K containing $f_i(\alpha)^n, f_j(\alpha)^{n'}, p$ must contain 1 and so is all of O_K. Thus, no prime in O_K contains more than one $f_i(\alpha)^n$. Finally, $(p, f_i(\alpha)^n)O_K$ is some ideal of O_K. Any prime containing it

contains $p, f_i(\alpha)^n$ and so also $f_i(\alpha)$ (by primality). By assumption, $(p, f_i(\alpha))O_K$ does not split into distinct primes and so only one prime can be in the factorization of $(p, f_i(\alpha)^n)$. Thus, $(p, f_i(\alpha)^n)O_K$ must factor as ${P_i}^k$ for some $k \in \mathbb{N}$ and prime $P_i \subset O_K$. □

Lemma 6.12. *If I_i is the ideal $(p, f_i(x)^n) \subset \mathbb{Z}[x]/(f(x))$ as defined above, then for each k, $(({p, {f_i}^n})^k, f) = (p^k, F_{ik})$ where F_{ik} is some element with integer coefficients of the equivalence class containing $F_i \mod p$ (where F_i is the lift of ${f_i}^n$ in $\mathbb{Q}_p$).*

Proof. We proceed by successively reducing the left ideal until it is the one on the right. Fix some k. We have $F_{ik} \equiv f_i \mod p$ and so ${f_i}^n = F_{ik} + pr$ for $r \in \mathbb{Z}[x]$. Thus, expanding out $(p, {f_i}^n)^k$, we get the ideal $(p^k, {f_i}^n p^{k-1}, ..., {f_i}^{nk})$. Substituting, ${f_i}^n p^{k-1}$ becomes $F_{ik}p^{k-1} + p^k r$. Since p^k is already in the ideal, this term reduces to $F_{ik}p^{k-1}$. Continuing, ${f_i}^{2n}p^{k-2}$ becomes $({F_{ik}}^2 + 2F_{ik}pr + p^2r^2)p^{k-2}$. Since $p^k, F_{ik}p^{k-1}$ are in the ideal, this reduces to ${F_{ik}}^2 p^{k-2}$. Continuing to reduce in this way, we show that the original ideal is equivalent to $(f, p^k, F_{ik}p^{k-1}, ..., {F_{ik}}^k)$. Now, $f \equiv F_{ik}G_k \mod p^k$ where G_k is some element in with integer coefficients in the equivalence class of $f/F_i \mod p^k$ and since p^k is in the ideal, we can replace f by $F_{ik}G_k$. By Hensel's Lemma, $(F_i, G) = \mathbb{Z}_p[x]$ and so we can find polynomials A, B so that $AF_i + BG = 1$. Then modulo p^k, this becomes $A_kF_{ik} + B_kG_k \equiv 1 \mod p^k$. Then $A_k{F_{ik}}^k + (B_k{F_{ik}}^{k-2})F_{ik}G_k = {F_{ik}}^{k-1}$ and the elements on the left are in our ideal, so the right is too. Continuing, we conclude that F_{ik} is in our ideal. Since any element of the ideal is a combination of F_{ik}, p^k and these elements generate the ideal, we are done. □

Now, we are ready to prove the key proposition. We take $\mathbb{Z}[\alpha]$ and complete it at some I_i. By the lemma, $\mathbb{Z}[\alpha]/{I_i}^k \equiv \mathbb{Z}[x]/(p^k, F_{ik})$. If we can show that $\varprojlim \mathbb{Z}[x]/(p^k, F_{ik}) = \mathbb{Z}_p[x]/(F_i)$, then we can find $\varprojlim O_K/{I_i}^k O_K$. By the above proposition, $I_iO_K = {P_i}^m$ for some prime P_i of O_K and so this is just $\varprojlim O_K/{P_i}^{mk}O_K$ which is $\mathbb{Z}_p[x]/(F_i)$ by assumption. Thus, the completions are the same and so by the exact sequences property, we conclude that $O_K = \mathbb{Z}[\alpha]$ as desired.

We need to show that $\varprojlim \mathbb{Z}[x]/(p^k, F_{ik}) = \mathbb{Z}_p[x]/(F_i)$. Suppose $g + (F_i) \in \mathbb{Z}_p[x]/(F_i)$. Then we have a map $T : \mathbb{Z}_p[x]/(F_i) \to \varprojlim \mathbb{Z}[x]/(p^k, F_{ik})$ that takes $g + (F_i)$ to the sequence $[g_k + (p^k, F_{ik})]_k$. i.e, it reduces the coefficients of g modulo p^k to some polynomial g_k with integer coefficients. If g, g' differ by some element of (F_i), then modulo p, then their projections into $(\mathbb{Z}/p^k\mathbb{Z})[x]$ differ by some element of (F_{ik}) and so T is well-defined. If $T(g) = 0$, then $g_k + (F_{ik}, p^k) = (F_{ik}, p^k)$ for each k. Thus, we can write $g_k - h_k \equiv 0 \mod p^k$ for some $h_k \in (F_{ik})$. Observe that $g_k \equiv g_{k+1} \mod p^k$. Thus, $h_k \equiv h_{k+1} \mod p^k$ as well. Thus, (h_k) is a coherent sequence in $\varprojlim \mathbb{Z}[x]/(p^k)$ and so we can think of it as some element $h \in \mathbb{Z}_p[x]$. $h_k \in (F_{ik})$ for each k and the elements for which this is the case are those that are actually multiples of F. Thus, $h \in (F)$ and so $h + (F) = (F)$. But also $g \sim h$ and so $g + (F) = (F)$. This proves injectivity. For surjectivity of T, we take some coherent sequence $[g_k + (p^k, F_{ik})]_k$. Then we have $g_1 \equiv g_2 \mod p^1, F_{i1}$ and so there is some c_1 so that $g_2 + c_1F_{i1} \equiv g_1 \mod p^1$. Let $g_1' = g_1, g_2' = g_2 + c_1F_i$. In this way, we can build a sequence (g_k') so that $g_{k+1}' \equiv g_k' \mod p^k$. Thus, $(g_k') \in \mathbb{Z}_p[x]$ and we see that $T(g_k') = (g_k)$. This completes our proof of the result.

Before proving a useful corollary, we give a word of warning to the reader. One may be tempted to think that the requirement that primes in $\mathbb{Z}[\alpha]$ do not split in O_K can be removed somehow. In general, this is not the case. For instance, the ring of integers of the splitting field of x^2+7 over $\mathbb{Q}$ is $\mathbb{Z}[\frac{-7+\sqrt{-7}}{2}]$ which is strictly bigger than $\mathbb{Z}[\sqrt{-7}]$. However, for any odd prime $p \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Z}_p$ so that $\mathbb{Z}_p[\sqrt{-7}] = \mathbb{Z}_p[\frac{-7+\sqrt{-7}}{2}]$. If $p=2$, then $\mathbb{Z}_2$ actually contains $\sqrt{-7}$. Thus, $\frac{-7+\sqrt{-7}}{2} \in \mathbb{Q}_2$ and since $\mathbb{Z}_2$ is integrally closed (among other reasons, it is a UFD), it must contain $\frac{-7+\sqrt{-7}}{2}$. Thus, in all cases, $\zeta_p[\sqrt{-7}] = \zeta_p[\frac{-7+\sqrt{-7}}{2}]$ and so the above theorem would force us to conclude that the ring of integers for this extension is $\mathbb{Z}[\sqrt{-7}]$ which it is not. However, the reader can check that the prime $(2, 1+\sqrt{-7}) \subset \mathbb{Z}[\sqrt{-7}]$ splits in $\mathbb{Z}[\frac{-7+\sqrt{-7}}{2}]$.

Corollary 6.13. *For ζ a primitive p^αth root of unity, $K = \mathbb{Q}[\zeta]$, $O_K = \mathbb{Z}[\zeta]$.*

Proof. By 6.8, we need only conclude that no prime in $\mathbb{Z}[\zeta]$ splits over O_K. Pick some prime $q \in \mathbb{Z}$, let $(q, f_i(\zeta))$ be a prime sitting over q in $\mathbb{Z}[\zeta]$ (so f_i is an irreducible factor of Φ_{p^α} modulo q. Crucially, we recall that the primes of O_K sitting over q correspond to factors of Φ_{p^α} over $\mathbb{Q}_p$. If $q=p$, then Φ_{p^α} is actually Eisenstein and so irreducible over $\mathbb{Q}_p$. Also, $\Phi_{p^\alpha} \equiv x^{\varphi(p^\alpha)} \mod p$. Thus, there is only a single prime over q in both O_K and $\mathbb{Z}[\zeta]$ and so there can be no splitting. If $q \neq p$, then all the roots of Φ_{p^α} are distinct modulo q. In other words, there are no repeated irreducible factors of $\Phi_{p^\alpha} \mod q$. Thus, each irreducible factor is coprime to the others and so lifts to a factorization in $\mathbb{Q}_q$ via Hensel's Lemma. Thus, the factorization of Φ_{p^α} is the same over $\mathbb{Q}_q$ as over $\mathbb{Z}/q\mathbb{Z}$. and so the number of primes sitting over q is the same in $\mathbb{Z}[\zeta]$. Since we have argued that no prime in O_K can sit over two different primes in $\mathbb{Z}[\zeta]$ and that each prime in O_K sits over some prime, it follows that each prime of O_K sits over exactly one prime of $\mathbb{Z}[\zeta]$. Thus, there is no splitting. □

Incidentally, this sort of argument will work for any polynomial that at each prime q is either Eisenstein or has all its factors distinct modulo q.

We now show how to combine our knowledge of the ring of integers and discriminants of primitive p^αth roots of unity, to find the ring of integers at any N.

Proposition 6.14. *If L, K are finite separable extensions of a field F so that LK/F is in extension of degree $[L:F][K:F]$, then if $e_1, ..., e_m$ is a basis for L and $f_1, ..., f_n$ a basis for K, we have that $e_i f_j$ form a basis for LK/F and $disc(e_i f_j) = disc(e_i)^n\, disc(f_j)^m$.*

Proof. A typical element of the matrix whose determinant gives $\text{disc}(e_i f_j)$ is of the form $Tr_{LK/F}(e_i f_j e_k f_l)$. Now, we observe that since $e_1, ..., e_m$ are all elements of L, $Tr_{L/F}(e_i e_k) = Tr_{LK/K}(e_i e_k)$ (we can construct the matrix $M_{e_i e_k}$ in L and then the same matrix works in LK). In particular, this means $Tr_{LK/K}(e_i e_k) \in F$. Then by proposition 3.15,

$$Tr_{LK/F}(e_i f_j e_k f_l) = Tr_{K/F}(Tr_{LK/K}(e_i f_j e_k f_l)) = Tr_{K/F}(f_j f_l \cdot Tr_{LK/K}(e_i e_k))$$
$$= Tr_{K/F}(f_j f_l \cdot Tr_{L/F}(e_i e_k)) = Tr_{L/F}(e_i e_k) \cdot Tr_{K/F}(f_j f_l)$$

Thus, if we consider the matrix A for the discriminant of $(e_i f_j)$, the matrix B for $\text{disc}(e_i)$, and C for $\text{disc}(f_j)$, then we simply have $A = B \otimes C$. It is a well known fact that $\det(B \otimes C) = \det(B)^n \det(C)^m$. □

Notice that if we can show that $O_K \cdot O_L = O_{KL}$ then this gives an expression of $\text{disc}(O_{LK}/\mathbb{Z})$ in terms of $\text{disc}(O_K/\mathbb{Z}), \text{disc}(O_L/\mathbb{Z})$.

Proposition 6.15 (Milne 6.5)**.** *Suppose that L, K are finite separable extensions of $\mathbb{Q}$ so that $[LK : \mathbb{Q}] = [L : \mathbb{Q}][K : \mathbb{Q}]$. Then $O_{K\cdot L} \subset \frac{1}{d} O_K \cdot O_L$ where d is the GCD of $disc(O_K/\mathbb{Z})$, $disc(O_L/\mathbb{Z})$.*

Proof. Let $(\alpha_1, ..., \alpha_m), (\beta_1, ..., \beta_n)$ be integral bases of K and L respectively. Then $\alpha_i\beta_j$ is a basis for $K \cdot L$ and so any element of $\gamma \in O_{KL}$ can be written in the form $\gamma = \sum_{ij} \frac{a_{ij}}{r} \alpha_i\beta_j$ for $a_{ij}, r \in \mathbb{Z}$. After cancelling out common divisors between the a_{ij} and r, it suffices to show that $r|d$.

We consider the set of field homomorphisms from $LK/L \to \mathbb{C}$ and notice that these are in bijection under the restriction map with the homomorphisms $K/\mathbb{Q} \to \mathbb{C}$. If we let $x_i = \sum_j \frac{a_{ij}}{r} \beta_j$ and consider the homomorphisms $\sigma_1, ..., \sigma_m$ from $LK/L \to \mathbb{C}$, then applying each one gives an equation $\sum_i \sigma_k(\alpha_i)x_i = \sigma_k(\gamma)$.

If we let $D = \det(\sigma_j(\alpha_i))$, then Cramer's rule gives $Dx_i = D_i$ (D_i is the matrix where we replace the ith column of D with x_i). $D^2 = \text{disc}(O_K/\mathbb{Z}) = \delta$ and so $\delta x_i = DD_i$. By construction, both D, D_i are algebraic integers and so therefore so is δx_i. But then $\delta x_i = \sum_j \frac{\delta a_{ij}}{r} \beta_j$ and since δx_i is algebraic and the β_j form an integral basis, $\frac{\delta a_{ij}}{r} \in \mathbb{Z}$ so that $r|\delta$. Similarly, we can get this result for $\text{disc}(O_L/\mathbb{Z})$. □

In particular, if the discriminants $\text{disc}(O_K/\mathbb{Z}), \text{disc}(O_L/\mathbb{Z})$ are relatively prime, then we see that $O_{KL} = O_K \cdot O_L$.

By proposition 6.14, we can combine the discriminant values for each prime power dividing N to get that $\text{disc}(\Phi_N) = (-1)^{\frac{\varphi(N)}{2}} \frac{n^{\varphi(n)}}{\prod_{p|N} p^{\frac{\varphi(N)}{p-1}}}$. Moreover, we can multiply the rings of integers to show that the ring of integers of a primitive Nth root of unity is $\mathbb{Z}[\zeta]$.

7. Galois Extensions

Suppose L, K are fields and L is a finite extension of K. Suppose we consider a prime ideal P of O_K. Then since O_L is a Dedekind domain, PO_L has a unique factorization into prime ideals of O_L. PO_L contains P which is a maximal ideal of O_K, and $PO_L \cap O_K$ is prime. Thus, $PO_L \cap O_K = P$ so that PO_L sits over P. Conversely, if Q sits over P, then $P \subset Q$ and so Q is in the factorization of P.

Proposition 7.1. *If $Aut(L/K)$ is the group of automorphisms of L fixing K, and P is a prime ideal of O_K then $Aut(L/K)$ acts on the set of prime ideals lying over P.*

Proof. Suppose $a \in O_L$. Then a is the root of some of some polynomial $f \in O_K[X]$. Then $\sigma(a)$ must also be a root of f and so is in O_L. Thus, each $\sigma \in \text{Aut}(L/K)$ restricts to an automorphism of O_L. Now, the image of a prime ideal is prime under an automorphism. Moreover, if Q sits over P then $\sigma(Q) \cap P = \sigma(Q \cap P) = \sigma(P) = P$ and so $\sigma(Q)$ sits over P. □

Proposition 7.2. *If L is Galois over K, then $Gal(L/K)$ acts transitively on the prime ideals sitting over P.*

Proof. Suppose that $\mathrm{Gal}(L/K)$ does not act transitively on the primes over P. Then if Q lies over P, there is some Q' not in the $\mathrm{Gal}(L/K)$-orbit of Q. Now all the primes ideals of O_L are maximal and so pairwise coprime. Thus, by the Chinese Remainder Theorem, we can pick some $x \in O_L$ so that $x \equiv 1 \mod \sigma(Q)$ for all $\sigma \in \mathrm{Gal}(L/K)$ and $x \equiv 0 \mod Q'$. Then $N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in K$. Since x is one of the terms of this product, the product is in Q' and so in P. However, since $x \notin \sigma(Q)$ for each σ, $\sigma^{-1}(x) \notin Q$ for each σ. This is true for each σ and since Q is prime, this implies $N_{L/K}(x) \notin Q$ and so cannot be in P. This is a contradiction and so proves transitivity as desired. □

If Q, Q' are primes in O_L sitting over P, then there is some $\sigma \in \mathrm{Gal}(L/K)$ so that $\sigma(Q) = Q'$. Thus, $\sigma(Q^e) = Q'^e$ and so if one of the prime powers contains P, so does the other. Such a σ also gives an isomorphism between O_L/Q and O_L/Q'. Thus, if L/K is a Galois extension, then any prime P of O_K factors as $\prod_{i=1}^{n} {Q_i}^e$ where the ramification index e and the inertia degree f is fixed for all Q_i.

Proposition 7.3. *Suppose $L = K[\alpha]$ is a finite separable extension of fields. Suppose that $O_L = O_K[\alpha]$. If $f(x)$ is the minimal polynomial of α and P is a prime ideal of O_K, then the factorization of $f(x)$ modulo P determines the factorization of the ideal PO_L. In particular, if $f(x) \equiv g_1(x) \cdot \ldots \cdot g_n(x) \mod P$, then $PO_L = \prod_{i=1}^{n} P_i$ where $P_i = (P, g_i(\alpha))$ and is prime.*

Proof. $O_L \cong O_K[x]/(f(x))$. The prime ideals of O_L sitting over P are precisely the prime ideals of $O_K[X]$ that contain $(f(x), P)$ or in other words, prime ideals of $O_K[x]/(f(x), P)$ which is the same as prime ideals of $(O_K/P)[x]/(f(x))$. But O_K is a Dedekind domain and so prime ideals are maximal. Thus, O_K/P is a field and so $(O_K/P)[x]$ is a PID. If $(g(x))$ is a prime ideal of $(O_K/P)[x]$ containing $(f(x))$, then $g(x)|f(x) \in (O_K/P)[x]$ and $g(x)$ is irreducible. In other words, the prime ideals sitting over P in O_L correspond precisely to the irreducible factors of $f \mod P$ and are given by $(P, g_i(\alpha))$.

□

Observe that the situation described in the previous proposition is precisely the situation we have for the primitive cyclotomic extensions. Thus, to determine how the prime ideals $(p) \subset \mathbb{Z}$ decompose in $\mathbb{Q}(\zeta_N)$, we need only investigate how $\Phi_N(x)$ factors modulo (p). Moreover, the extension $\mathbb{Q}(\zeta)$ is Galois and so by the remark after proposition 7.2, the irreducible factors of $\varphi_N(x)$ modulo (p) all have the same degree and divide $\Phi_N(x)$ the same number of times. To figure out the factorization of $\Phi_N(x)$ modulo (p) we consider its splitting field over $\mathbb{Z}/p\mathbb{Z}$.

Proposition 7.4. *There is precisely one finite field of characteristic p of cardinality p^n for each $n \in \mathbb{N}$.*

Proof. We recall that splitting fields are isomorphic. Thus, we need only show that if K has cardinality p^n, then it is the splitting field of a particular polynomial.

If $\alpha \in K^*$, then $\alpha^{|K^*|} = 1$ and so α is a zero of $x^{p^n-1} - 1$. Thus, any element of K is a zero of $x^{p^n} - x$. But the derivative of this polynomial is $p^n x^{p^n-1} - 1 = -1$ in any field of characteristic p, so that this polynomial has no multiple roots. Since it is degree p^n, it has exactly p^n roots and so these must be all the elements of K. Thus, K is precisely the splitting field of $x^{p^n} - x$. □

Proposition 7.5. *A splitting field K of cardinality p^N has Galois group $\mathbb{Z}/N\mathbb{Z}$ over $\mathbb{Z}/p\mathbb{Z}$ and the Frobenius automorphism $\sigma_p : \alpha \mapsto \alpha^p$ generates the Galois group.*

Proof. Just by consideration of elements, K is an N-dimensional vector-space over $\mathbb{Z}/p\mathbb{Z}$ and so must be a degree N extension. Thus, the Galois group has N elements. We recall that the multiplicative group of a finite field is cyclic and so is isomorphic to $\mathbb{Z}/(p^N - 1)\mathbb{Z}$. Thus, we can pick some generator $g \in K$ and we observe that $g^{p^N} = g$ but this is true for no smaller power. Thus, σ_p has order N and so generates the entire Galois group. □

Proposition 7.6. *If K is the finite field of cardinality p^N, then it is the splitting field of every irreducible polynomial f of degree N over $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Let L be the splitting field of some irreducible polynomial f of degree N. By the previous arguments $\mathrm{Gal}(L/(\mathbb{Z}/p\mathbb{Z}))$ must be cyclic and generated by the Frobenius automorphism σ_p. Now, since f is irreducible, $\mathrm{Gal}(L/(\mathbb{Z}/p\mathbb{Z}))$ acts transitively on the roots of f and so for any roots α, β, there is some power a of σ_p so that ${\sigma_p}^a(\alpha) = \beta$. Thus, the orbit of any root of f given by the action of σ_p contains all roots. In particular, this means that the order of σ_p is just N (since f has N distinct roots) and so the Galois group is $\mathbb{Z}/N\mathbb{Z}$. Thus, the extension is degree N and so $L = K$. □

Proposition 7.7. *Let K be the splitting field of Φ_N over $\mathbb{Z}/p\mathbb{Z}$. Then if p^α is the maximal power of p that divides N, we have that e, the ramification index of primes dividing pO_K, is $\varphi(p^\alpha)$ where φ is Euler's φ-function.*

Proof. The Nth roots of unity are given by ζ^a where $\zeta = e^{\frac{2\pi i}{N}}$. All of these are contained in K and since $K = [\mathbb{Z}/p\mathbb{Z}](\zeta)$, the action of any automorphism is totally determined by its action on ζ. Now, if σ_p is the Frobenius map, then we observe that this must be an automorphism of K (in fact it generates the Galois group). If p^α is the largest power of p dividing N, then consider the action of ${\sigma_p}^\alpha$. This takes any Nth root of unity to an N/p^αth root of unity. Moreover, if ζ^a is primitive, then it has order N, and so ${\sigma_p}^\alpha$ has order N/p^α and so is a primitive N/p^αth root of unity. If we consider the action of ${\sigma_p}^\alpha$ on the exponents of the ζ^a, then we see that it gives a homomorphism from $\mathbb{Z}/N\mathbb{Z}$ to $p^\alpha\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/(N/p^\alpha)\mathbb{Z}$. Since we know ${\sigma_p}^\alpha$ is an automorphism, it follows that all the roots in the kernel of this map must be the same element in K. However, since $(N/p^\alpha, p) = 1$ all the roots in the image of the homomorphism are distinct (proof of proposition 6.5) and so this is precisely the number of roots that are the same. σ is surjective, since for any $cp^\alpha \in p^\alpha\mathbb{Z}/N\mathbb{Z}$, ${\sigma_p}^\alpha(c) = cp^\alpha$. Thus, the kernel has p^α elements. Now, since the irreducible factors of Φ_N don't share roots, we see that the number of primitive Nth roots of unity that are actually the same element gives the exponent of each factor in the factorization of Φ_N modulo p and this corresponds to the ramification index. Now, primitive Nth roots map to primitive N/p^αth roots. There are $\varphi(N)/\varphi(p^\alpha)$ of the latter roots and $\varphi(N)$ of the former. Thus, each primitive Nth root is identified with $\varphi(p^\alpha)$ others. □

We recall that the inertia degree of p with respect to the splitting field L of Φ_N over $\mathbb{Q}$ is precisely the degree of the field extension $(O_L/PO_L)/(\mathbb{Z}/p\mathbb{Z})$ which is just $K/(\mathbb{Z}/p\mathbb{Z})$ whose degree is the order of σ_p. σ_p acts as multiplication by p on the exponents of the primitive N/p^αth roots of unity and so f is precisely the order of

p in the multiplicative group $\mathbb{Z}/(N/p^\alpha\mathbb{Z})$. Since we have determined e, f, it follows from proposition 4.7 that the number of different primes that (p) splits into is given by $\varphi(N)/ef$.

Proposition 7.8. *If $\mathbb{Q}(\sqrt{n})$ is a quadratic extension (so n is squarefree), then the rings of integers are $\mathbb{Z}[n+\sqrt{n}]$ if $n \equiv 2, 3 \mod 4$ and $\mathbb{Z}[\frac{n+\sqrt{n}}{2}]$ otherwise.*

Proof. By propositions (5.4, 5.5, 6.10) it suffices to show the ring of integers in $\mathbb{Q}_p$ are $\mathbb{Z}[n+\sqrt{n}], \mathbb{Z}[\frac{n+\sqrt{n}}{2}]$ respectively and that at any prime p, these polynomials are either Eisenstein or have distinct roots modulo p. If $n \equiv 2, 3 \mod 4$, then consider $n+\sqrt{n}$. Its minimal polynomial is $x^2 - 2nx + n^2 - n$ which has discriminant $4n^2 - 4(n^2 - n) = 4n$. This polynomial is Eisenstein for any prime dividing n and is also Eisenstein for 2. So for each prime dividing the discriminant, $D_{\mathbb{Q}_p} = \mathbb{Z}_p[n+\sqrt{n}]$. If p does not divide the discriminant over $\mathbb{Q}$, it certainly does not divide the discriminant over $\mathbb{Q}_p$ and so then $D_{\mathbb{Q}_p} = \mathbb{Z}_p[n+\sqrt{n}]$ also. The derivative of $x^2 - 2nx + n^2 - n$ is $2x - 2n$ which modulo p for any odd p not dividing n (i.e. when we are not in the Eisenstein case) has the root n. But $n^2 - 2n^2 + n^2 - n \equiv -n \not\equiv 0 \mod p$ and so n is not a root of the polynomial. Thus, its roots are distinct modulo p.

If $n \equiv 1 \mod 4$, then we consider $\frac{n+\sqrt{n}}{2}$ which has minimal polynomial $x^2 - nx + (\frac{n^2-n}{4})$. This has discriminant $n^2 - n^2 + n = n$. Modulo each prime dividing n, this polynomial is Eisenstein, and any other prime does not divide the discriminant. So at each p, the ring of integers is $\mathbb{Z}_p[\frac{n+\sqrt{n}}{2}]$. The derivative is $2x - n$ and so when we are not in the Eisenstein case and are at some odd prime, the root is $\frac{n}{2}$. But $\frac{n}{2}^2 - \frac{n^2}{2} + \frac{n^2-n}{4} = \frac{-n}{4}$. $n \not\equiv 0 \mod p$ and so this is not a root. If $p = 2$, then there is no root of the derivative. So in all cases, the roots are all distinct and so $\mathbb{Z}[\frac{n+\sqrt{n}}{2}]$ is the ring of integers. □

Consider $\mathbb{Q}(\zeta_p)$. Then the Galois group is cyclic and so there is exactly one subgroup of order $\frac{p-1}{2}$, and this corresponds to a unique quadratic extension within $\mathbb{Q}(\zeta_p)$. Now the discriminant of a quadratic extension is $4n$ or n, and by proposition 4.9 the primes that ramify are those that divide the discriminant. But if a prime ramifies in a quadratic subextension of $\mathbb{Q}(\zeta_p)$, then it must ramify in $\mathbb{Z}[\zeta_p]$ as well. This means one of $4n, n$ divides $\text{disc}(\mathbb{Q}(\zeta_p)) = \pm p^{p-2}$. Thus, the only possibility is if $n = \pm p$ and $n \equiv 1 \mod 4$.

8. Frobenius Elements and Quadratic Reciprocity

Let $K/\mathbb{Q}$ be a finite Galois extension. If we pick some prime $(p) \subset \mathbb{Z}$, then we can choose a prime $P \subset O_K$ that sits over (p) and consider the stabilizer G_P of P with respect to the action of the Galois group on the primes sitting over p. This is a subgroup of the Galois group called the decomposition group of P. Since G_P maps P to itself and O_K to O_K, each element of G_P restricts to an automorphism of $(O_K/P)/(\mathbb{Z}/p\mathbb{Z})$.

Proposition 8.1. *If K' is the fixed field of G_P and P_1 is some lift of (p) in $O_{K'}$ so that P sits over P_1, then the inertia degree f and ramification index e for P_1 over K are both 1.*

Proof. Observe that by the identity of proposition 4.8 we have for $P \subset O_K$ that for P over $\mathbb{Q}$, $efr = [K : \mathbb{Q}]$ where r is the number of primes P splits into. Similarly,

we can consider the same identity for P over K' (K is a Galois extension of K'). We get that $e'f'r' = [K : K']$. But since every element of the Galois group G_P fixes P and recalling that the Galois group acts transitively on primes sitting over P_1, we see that P_1 cannot split over K. Thus, $r' = 1$. Also, the number of cosets of $\text{Gal}(K/\mathbb{Q})/G_P$ (this need not be a group but we can still look at cosets) correspond to the number of primes that (p) splits into. Thus, $[K' : \mathbb{Q}] = r$ and so $e'f'r' = e'f' = [K : K'] = ef$. We can also consider the inertia and ramification behavior of P_1 and observe that since we have the identity $\sum_{i=1}^{r} e_i f_i = r$, we must have each $e_i = f_i = 1$ and so in particular, $e_1 = f_1 = 1$. Now, $e = e'e_1, f = f'f_1$ and so $e = e', f = f'$. □

Proposition 8.2. *The restriction map $R : G_P \to Gal((O_K/P)/(\mathbb{Z}/p\mathbb{Z}))$ defined in the above discussion gives a surjective homomorphism of groups. If the extension is unramified at P, it is an isomorphism.*

Proof. Observe that if K' is the fixed field of G_P, then since the inertia degree of any prime P' sitting under P in $O_{K'}$ is 1 over $\mathbb{Q}$, we have $\mathbb{Z}/p\mathbb{Z} \cong O_{K'}/P'$ and so clearly any element of $\text{Gal}((O_K/P)/(\mathbb{Z}/p\mathbb{Z}))$ is also an element of $\text{Gal}((O_K/P)/(O_{K'}/P')$ (since we also have the inclusions $\mathbb{Z} \subset O_{K'}, (p) \subset P'$).

Pick some primitive element $\overline{\alpha} \in O_K/P$ so that $\mathbb{Z}/p\mathbb{Z}[\overline{\alpha}] = O_K/P$ and so $O_{K'}/P'[\overline{\alpha}] = O_K/P$ as well. Then we can choose some $\alpha \in O_K$ as a representative of the $\overline{\alpha}$ equivalence class. If f is the minimal polynomial of α over $O_{K'}$ and g the minimal polynomial of $\overline{\alpha}$ over $O_{K'}/P'$, we see that g divides $f \mod P'$. Since K contains a root of f and is Galois, it splits f and so gives a transitive action on the roots. Now take some $\overline{\sigma} \in G_P$. Then the action of $\overline{\sigma}$ is determined by where it maps $\overline{\alpha}$ and so to find a $\sigma \in G_P$ satisfying $R(\sigma) = \overline{\sigma}$, we need only find some σ that maps α to some α' that restricts to $\overline{\sigma\alpha}$. But $\overline{\sigma\alpha}$ is a root of g and so is the restriction of some root α' of f. Since $\text{Gal}(K/K') = G_P$ acts transitively on the roots of f (since f is minimal and so irreducible) we can pick some $\sigma \in \text{Gal}(K/\mathbb{Q})$ that maps α to α'. This shows surjectivity.

If K is unramified at P, then $|G_P| = f$ and since $|\text{Gal}((O_K/P)/(\mathbb{Z}/p\mathbb{Z}))| = f$ we must have an isomorphism. □

Suppose we are in the situation where $K/\mathbb{Q}$ is a Galois extension and is unramified at the the prime $(q) \subset \mathbb{Z}$. Then if Q is some prime sitting over (q) in O_K, $\text{Gal}((O_K/Q)/(\mathbb{Z}/q\mathbb{Z}))$ is generated by the Frobenius automorphism $\overline{\sigma_q}$ and this has a unique lift to an automorphism $\sigma_q \in \text{Gal}(K/\mathbb{Q})$ that restricts modulo Q to $\overline{\sigma_q}$. Let $K = \mathbb{Q}(\zeta_p)$ for some prime p and let q be an odd prime of $\mathbb{Z}$ with $p \neq q$. Now, pick some prime $Q \subset O_K$ sitting over (q) and consider σ_Q. Suppose Q' is some other prime sitting over Q. Then $\text{Gal}(K/\mathbb{Q})$ acts transitively on $\mathbb{Q}$ and so there is some $\tau \in \text{Gal}(K/\mathbb{Q})$ so that $\tau(Q) = Q'$. Then by definition, for any $\alpha \in \text{Gal}(K/\mathbb{Q})$, $\sigma_Q(\alpha) = \alpha^q + a$ for some $a \in Q$. Then $(\tau \circ \sigma_p \circ \tau^{-1})(\alpha) = \tau(\tau^{-1}(\alpha)^q + a) = \alpha^q + \tau(a)$ where we see that $\tau(a) \in Q'$. Thus, $\sigma_{Q'} = \tau\sigma_Q\tau^{-1}$. Since the Galois group of $K/\mathbb{Q}$ is Abelian (in fact it is isomorphic to $\mathbb{Z}/p-1\mathbb{Z}$) we see that $\sigma_Q = \sigma_{Q'}$ for any Q, Q' sitting over (q) and so we can unambiguously call such an element σ_q. Now, the primitive pth roots of unity are all distinct $\mod q$ and so σ_q must map $\zeta_p \mapsto \zeta_p{}^q$. There is only one automorphism that does this and so this is σ_q.

Proposition 8.3. *q is a square in $\mathbb{Z}/p\mathbb{Z}$ if and only if $q^{\frac{p-1}{2}} \equiv 1 \mod p$.*

Proof. If q is a square in $\mathbb{Z}/p\mathbb{Z}$, then there is some a so that $a^2 \equiv q \mod p$. Then $1 \equiv a^{p-1} \equiv q^{\frac{p-1}{2}} \mod p$. Conversely, if $q^{\frac{p-1}{2}} \equiv 1 \mod p$, then pick some g that generates the multiplicative group (since it is cyclic). We have $g^x = q$ for some x and $g^{\frac{p-1}{2}x} \equiv q^{\frac{p-1}{2}} \equiv 1 \mod p$. Since g is a generator of the multiplicative group, this means that $p-1|\frac{p-1}{2}x$, and so in particular, x is even. Then $(g^{\frac{x}{2}})^2 \equiv q \mod p$ and so q is a square. □

In particular, we have proven that q is a square $\mod p$ if and only if it lies in the maximal subgroup of the multiplicative group that is of order $\frac{p-1}{2}$. But this is precisely the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ that fixes the unique quadratic sub-extension $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$. In other words, σ_q acts as the identity map on K' and so for any prime lying above Q, $\mathrm{Gal}((O_{K'}/Q)/\mathbb{Z}/q\mathbb{Z})$ is trivial. Thus, $x^2 - (-1)^{\frac{p-1}{2}}p$ must factor modulo q and so $(-1)^{\frac{p-1}{2}}p$ is a square modulo q precisely when q is a square modulo p. In Legendre Symbols, this is $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}(\frac{p}{q}) = (\frac{(-1)^{\frac{p-1}{2}}p}{q}) = (\frac{q}{p})$ which is quadratic reciprocity.

Acknowledgements. I would like to thank Professor Matthew Emerton for suggesting this project and advising me throughout the summer. I would also like to thank my mentor Daniel Johnstone who read, discussed, and suggested improvements on virtually every part of this paper and was always willing to meet up and talk about my proofs. Finally, I want to thank Professor Peter May for organizing the REU and for reading and correcting this paper.

References

[1] Atiyah, M. F., and I. G. Macdonald. Introduction to Commutative Algebra. Boulder, CO: Westview, 1969. Print.

[2] J.S. Milne's online Algebraic Number Theory course notes. http://www.jmilne.org/math/CourseNotes/ant.html

[3] Neukirch, Jürgen. Algebraic Number Theory. Berlin: Springer, 1999. Print.

[4] Dummit, David Steven., and Richard M. Foote. Abstract Algebra. Hoboken, NJ: Wiley, 2004. Print.

[5] Serre, Jean-Pierre. Local Fields. New York: Springer-Verlag, 1979. Print.