NOTES ON ALGEBRAIC NUMBER THEORY: MILNE

ALAN ZHAO

Change all cross citations to Schoof citations. The following notes seek to consolidate my memory of the material within [Mil08] that does not intersect with [Sch03]. To that end I will be summarizing chapters 6-8 of Milne's notes. My goal is to write about the most critical techniques in the construction of key results in algebraic number theory. Proofs will be presented with principal focus on main ideas and motivic ideas behind constructed objects. This will be more helpful for a review of the material, as the details of the proof are already written in [Mil08], so reproducing them would not do much good.

1. Cyclotomic Extensions and Fermat's Last Theorem

Cyclotomic extensions are those of the form $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta)$, where $\zeta^n = 1$ for some positive integer n. Assume that ζ is a primitive nth root of unity. Then $\mathbb{Q}(\zeta)$ is the splitting field for the polynomial $X^n - 1$, and so is Galois. Its minimal polynomial is the ***n*th cyclotomic polynomial**, defined by

$$\Phi_n(T) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^*} (T - \zeta^a). \tag{1.1}$$

Clearly, $\Phi_n(\zeta) = 0$. Since $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ permutes the roots of $X^n - 1$, it is evident that $\Phi_n(T)$ is invariant under action by $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and so is a rational polynomial. It was shown in my summary of Schoof's notes on algebraic number theory (Proposition **??**) that $\Phi_n(T)$ is actually irreducible, and so is the minimal polynomial for ζ.

The arithmetic of cyclotomic fields is heavily interwined with the arithmetic in $\mathbb{Z}$. Indeed, many fundamental theorems on cyclotomic polynomials make use of the Euler φ-function and divisors of integers, for example. Hence, we first consider $\mathbb{Q}(\zeta)$ in the case where $n = p^r$, with p a prime and $r \in \mathbb{Z}^{\geq 1}$.

Proposition 1.1. *Let ζ be described as above. Then,*

i. The field $\mathbb{Q}(\zeta)$ is of degree $\varphi(p^r)$ over $\mathbb{Q}$.
ii. $O_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$.
iii. The element $1 - \zeta$ is a prime element of O_K, with $(p) = (1 - \zeta)^{\varphi(p^r)}$.
iv. The discriminant of $O_{\mathbb{Q}(\zeta)}$ is $\pm p^c$, where $c = p^{r-1}(pr - r - 1)$. In particular, only p ramifies in $\mathbb{Q}(\zeta)$.

Proof. (iii): We have to show that $p = u \cdot (1 - \zeta)^{\varphi(p^r)}$ for some unit $u \in O_{\mathbb{Q}(\zeta)}$. It is natural to ask for the form of $\Phi_{p^r}(T)$. By combining Equation 1.1 with the observation that $\sum_{d|n} \varphi(d) = n$, we see that

$$\Phi_{p^r}(T) = 1 + T^{p^{r-1}} + \cdots + T^{(p-1)p^{r-1}}. \tag{1.2}$$

In particular, $\Phi_{p^r}(1) = p$, and so

$$p = \prod_{a \in (\mathbb{Z}/p^r\mathbb{Z})^*} (1 - \zeta^a). \tag{1.3}$$

Date: August 2020.

By consideration of a geometric series, it is easy to see that $(1-\zeta^a)/(1-\zeta^b)$ is a unit for any $a, b \in (\mathbb{Z}/p^r\mathbb{Z})^*$. From here it is easy to rewrite the above equation into the desired form. With this, we can combine Galois theory with the classic efg-formula (Proposition **??**(ii)) to obtain (i). With this observation, we see that π must generate a prime ideal, so (iii) is proved.
(iv): We recall from my summary of Schoof's notes (Proposition **??**) the following relation:

$$\operatorname{disc}(\mathbb{Z}[\zeta]/\mathbb{Z}) = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) \cdot [\mathcal{O}_{\mathbb{Q}(\zeta)} : \mathbb{Z}[\zeta]]^2. \tag{1.4}$$

Because the formula for $\Phi_{p^r}(T)$ is particularly simple, it is fruitful to consider the following identity from Schoof's summary (Proposition **??**):

$$\operatorname{disc}(\mathbb{Z}[\zeta]/\mathbb{Z}) = \pm N(\Phi'_{p^r}(\zeta)). \tag{1.5}$$

Remark. *This aligns with Schoof's formula as there is a more generic notion of discriminant. Let A be a commutative ring with unit, and let B be an A-module with basis $\beta_1, \ldots \beta_m$. Then,*

$$disc(B/A) = ((Tr_{B/A}(\beta_i\beta_j))_{1\le i,j\le m}), \tag{1.6}$$

where the trace can still be defined with respect to a a matrix with A-entries.

A little algebra reduces the proof of (iv) to (ii). We mark the proof of (iv) as done, and prove (ii).
(ii): We know from (i) and the efg-formula that $[\mathcal{O}_{\mathbb{Q}(\zeta)}/(\pi) : \mathbb{Z}/p\mathbb{Z}] = 1$. What this means is that

$$\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]] + (1-\zeta)\mathcal{O}_{\mathbb{Q}(\zeta)}. \tag{1.7}$$

We continuously multiply the above by π on both sides, and we will find that

$$\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta] + \pi^m\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta] + p^m\mathcal{O}_{\mathbb{Q}(\zeta)}, \tag{1.8}$$

which is sufficient for large enough m. □

Remark. *In the proof of* [Sch03, Theorem 2.6]*, there is a matrix whose determinant is $(2i)^{-r_2} \cdot \det(\varphi_k(\omega_j))_{k,j}$, where the matrix runs over all embeddings and the basis elements of a number field K. This quantity must be real. So, the sign of r_2 determines if $\det(\varphi_k(\omega_j))_{k,j}$ is real or pure imaginary. Then,* [Sch03, Proposition 3.4]*(i) would gives us if the discriminant of K is negative or positive! In the case of cyclotomic fields K in the above proposition, we already know that they are already pure imaginary unless $\zeta = \pm 1$. So the sign of r_2 is very easy to find since we have an expression for $[K : \mathbb{Q}]$ in terms of p and r.*

We now move to the general case n. Note that the case of $n = p^r$ serves as a base case. This sets the grounds for an induction-based proof of the following theorem.

Theorem 1.2. *Let ζ be a primitive nth root of 1.*

i. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.
ii. $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$.
iii. If $p \mid n$, then p ramifies in $\mathbb{Q}(\zeta)$. If we write $n = p^r \cdot m$ with $(m, p) = 1$, then

$$(p) = \prod \beta_i^{\varphi(p^r)}. \tag{1.9}$$

Proof. We induct on the number of prime divisors of n, and so we write $n = p^r \cdot m$. Considering the two fields $\mathbb{Q}(\zeta_{p^r})$ and $\mathbb{Q}(\zeta_m)$ separately and using the efg-formula, we deduce all of (iii). The induction easily strikes down (i). The proof of (ii) falls to the following lemma, whose proof largely follows the linear algebra of number fields (e.g., embeddings and the trace and determinant).

Lemma 1.3. *Let K and L be finite extensions of $\mathbb{Q}$ such that*

$$[KL : \mathbb{Q}] - [K : \mathbb{Q}][L : \mathbb{Q}] \tag{1.10}$$

and let d be the GCD of $disc(\mathcal{O}_K/\mathbb{Z})$ and $disc(\mathcal{O}_L/\mathbb{Z})$. Then, $\mathcal{O}_{KL} \subset d^{-1}\mathcal{O}_K\mathcal{O}_L$.

□

We end this section with an elegant proof of special cases of Fermat's Last Theorem, due to Kummer. We begin with a definition.

Definition 1.4. *Call a rational prime p **regular** if p does not divide the class number of $\mathbb{Q}(\zeta_p)$.*

We now introduce the result by Kummer.

Theorem 1.5. *Fermat's Last Theorem is true for odd regular primes.*

Proof. Assume we have $x^p + y^p = z^p$ violating the conclusion of Fermat's Last Theorem. The cases of $p = 3, 5$ are easy. For $p \geq 7$, we assume $p \nmid x - y$ after observing that one of the congruences $x \cong y \cong -z \pmod{p}$ cannot hold and rewriting $x^p + y^p = z^p$ as $x^p + (-z)^p = (-y)^p$ if necessary. Now notice that we can write

$$\prod_{i=0}^{p-1}((x + \zeta^i y)) = (z)^p. \tag{1.11}$$

This means each ideal $(x + \zeta^i y)$ is actually the power of a principal ideal since p doesn't divide the order of the class group of $\mathbb{Q}(\zeta)$ and since the ideals in the product are pairwise coprime. Take $i = 1$ and write $x + \zeta y = u\alpha^p$. The result [Mil08, Proposition 6.7] tells us we can write $u = \zeta^r \cdot v$ where ζ and v are both units and $\overline{v} = v$. An easy argument shows that we can find $a \in \mathbb{Z}$ such that $\alpha^p \cong a \pmod{p\mathbb{Z}[\zeta]}$. So, we end up combining two relations to get

$$x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y \cong 0 \pmod{p}. \tag{1.12}$$

If $1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ are distinct, then since $p \geq 7$, a consideration of the size of the basis of $\mathbb{Z}[\zeta]/\mathbb{Z}$ shows that $p \mid x, y$, a contradiction. Possible equalities between these 4 elements are resolved by the same consideration. □

2. Local Fields and Absolute Values

An **absolute value** on a field K is a a function $|\cdot| : K \to \mathbb{R}$ such that

i. $|x| > 0$ when $x \neq 0$, and $|0| = 0$.
ii. The restriction $|\cdot| : K^* \to \mathbb{R}$ is a homomorphism.
iii. The triangle inequality holds.

If it is true that $|x + y| \leq \max\{|x|, |y|\}$, we call $|\cdot|$ a **nonarchimedean absolute value**. Note that $|\cdot| : K^* \to \mathbb{R}_{>0}$ being a homomorphism implies that $|\mu_K| = \{1\}$ since $\mathbb{R}_{>0}$ is torsion-free. A very important absolute value is the **normalized $\mathfrak{p}$-adic absolute value**, with $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal:

$$|a|_\mathfrak{p} = (1/N(\mathfrak{p})^{\mathrm{ord}_\mathfrak{p}(a)}. \tag{2.1}$$

One will notice that taking logarithms of this absolute value can give us an additive valuation. We address this in the following proposition.

Proposition 2.1. *Let $|\cdot|$ be a nontrivial nonarchimedean absolute value and set $v(x) = -\log|x|$ for $x \neq 0$. Then, $v : K^* \to \mathbb{R}$ is a valuation on K^*, and if $v(K^*)$ is discrete, then it is a multiple of a discrete valuation $ord : K^* \twoheadrightarrow \mathbb{Z}$.*

Proof. Only the last assertion isn't obvious, which follows from the statement that a subgroup of $\mathbb{R}$ is discrete if and only if it is a $\mathbb{Z}$-lattice. This can be proved using induction. □

To test if an absolute value is nonarchmiedian, we may employ a consideration of the binomial theorem which yields an easy test.

Proposition 2.2. *An absolute value $|\cdot|$ is nonarchimedean if and only if takes bounded values on $\mathbb{Z}$.*

Remark. *It is then clear that fields of positive characteristic can only have non-archimedean absolute values.*

We can continue this thread of classification up to complete classification of absolute values over $\mathbb{Q}$ by Ostrowski. For this we need a notion of equivalent absolute values.

Definition 2.3. *We say that two absolute values $|\cdot|_1$ and $|\cdot|_2$ are **equivalent** if they define the same topology on K.*

We now introduce some tests for this equivalence. The proof is left to algebra using logarithms and exponentials, and so will be omitted.

Proposition 2.4. *Let $|\cdot|_1$ and $|\cdot|_2$ be two absoltue values on K, with $|\cdot|_1$ non-trivial. TFAE:*

i. $|\cdot|_i$ *are equivalent.*
ii. $|\alpha|_1 < 1 \implies |\alpha|_2 < 1$
iii. $|\cdot|_2 = |\cdot|_1^a$ *for some* $a > 0$.

With this we can now present the aforementioned theorem by Ostrowski.

Theorem 2.5 (Ostrowski)**.** *Let $|\cdot|$ be a nontrivial absolute value on $\mathbb{Q}$.*

i. If $|\cdot|$ is archimedean, then it is equivalent to the usual absolute value.
ii. If $|\cdot|$ is nonarchimedean, it is equivalent to $|\cdot|_p$ for exactly one prime p.

Proof. We recall Corollary 2.2, which leads to trying to establish an inequality for $|m|$ for $m \in \mathbb{Z}$. We are interested in exponentials and logarithms, so we try to express m in such terms. So, let $m, n, t \in \mathbb{Z}_{>1}$ and $m^t = a_0 + a_1 n + \cdots + a_r n^r$, where $r \leq \log(m)/\log(n)$ and $0 \leq a_i < n$. Then, the triangle inequality tells us

$$|m^t| \leq \sum |a_i| N^r \tag{2.2}$$

where $N = \max\{1, |n|\}$. Since $|a_i| \leq n$, we have that

$$|m^t| \leq \left(1 + \frac{\log(m)}{\log(n)}\right) n N^{\frac{\log(m)}{\log(n)}}. \tag{2.3}$$

Taking tth roots and taking $t \to \infty$ yields the cleaner relation

$$|m| \leq N^{\log(m)/\log(n)}. \tag{2.4}$$

Now, the case where $|n| > 1$ for all $n > 1$ takes us to the proof of (i). Assuming $|n| \leq 1$ for some $n > 1$ tells us $|m| \leq 1$, and so $|\cdot|$ is nonarchimedean. The proof of this second part relies on Proposition 2.7 presented below. □

Before presenting this Proposition, we pause to mention a very important result that will ultimately generalize to number fields in §3.

Theorem 2.6 (Product Formula for $\mathbb{Q}$)**.** *Over $\mathbb{Q}$:*

$$\prod_p |a|_p = 1 \tag{2.5}$$

for all places p and any non-zero $a \in \mathbb{Q}$.

Now, nonarchimedean absolute values have a habit of becoming associated with local rings. In fact, although these absolute values are the "strange" ones, one of the most important applications of valuation theory — that is, the Mordell-Weil theorem for elliptic curves — usually excludes "normal" or archimedean absolute values entirely (see [Sil09, Chapter 8] for example). This aforementioned habit is displayed below.

Proposition 2.7. *Let $|\cdot|$ be a nonarchimedean absolute value. Then,*

i. $A := \{a \in K : |a| \leq 1\}$ *is a subring of K.*
ii. $U := \{a \in K : |a| = 1\}$ *is equal to A^*.*
iii. $\mathfrak{m} := \{a \in K : |a| < 1\}$ *is the unique maximal ideal of A.*

Also, $|\cdot|$ is discrete if and only if $\mathfrak{m}$ is principal, in which case A is a discrete valuation ring (integral domain, Noetherian, integrally closed, exactly one non-zero prime ideal).

With Ostrowski's Theorem and the Product Formula for $\mathbb{Q}$ in mind, we now move to discuss the primes of a number field and their respective absolute values. We call an equivalence class of absolute values on K a **place** of K. It will be shown in §3 that there is exactly one place for each prime ideal of K, real embedding of K, and each pair of conjugate complex embeddings of K. We choose the following normalized absolute values for each:

i. For a prime ideal $\mathfrak{p}$, set $|a|_\mathfrak{p} = (1/N(\mathfrak{p}))^{\mathrm{ord}_\mathfrak{p}(a)}$.
ii. For a real embedding σ, set $|a|_\sigma = |\sigma(a)|$.
iii. For a complex embedding σ, set $|a|_\sigma = |\sigma(a)|^2$.

We leave further discussion of this topic to §3. We instead move to discuss the Weak Approximation Theorem, in some sense motivated by the lattice structure of the ring of integers in a sufficiently good embedding. Indeed, it is shown in [Con] that by stripping away just one copy of $\mathbb{R}$ or $\mathbb{C}$ from the codomain of this embedding, the resulting image is dense. By considering a diagonal embedding of K using its absolute values, we can partially characterize the resulting image.

The results leading up to the Weak Approximation Theorem can be proven just by considering numbers that are sufficiently good, and so we just state the theorem directly.

Theorem 2.8 (Weak Approximation Theorem)**.** *Let $|\cdot|_1, \ldots |\cdot|_n$ be nontrivial inequivalent absolute values of a field K. Let $a_1, \ldots a_n$ be elements of K. For every $\epsilon > 0$ there exists an element $a \in K$ such that $|a - a_i|_i < \epsilon$ for all i.*

Proof. We are able to choose b_i such that $|b_i - 1|_i$ is small and $|b_i|_j$ is small for $j \neq i$. Then $\sum a_i b_i$ works. □

An easy consequence of this theorem is that there can be no finite product formula.

It is worth noting that a slightly stronger statement can be achieved with the Chinese Remainder Theorem, but only in the case of places over prime ideals, which might be preferred in some cases.

Theorem 2.9. *The above theorem holds for the $|\cdot|_i$ being places over prime ideals and with the further constraint that $|a| \leq 1/|d|$ for all absolute values corresponding to prime ideals other than the $|\cdot|_i$ and where d is a common denominator for the a_i.*

Proof. Readily follows from the Chinese Remainder Theorem for the da_i. □

Another thing we can do with absolute values of a field K is consider its completion $\hat{K}$ with respect to an absolute value $|\cdot|$, which is "unique" in the sense of a universal mapping property. This is summarized in the following theorem.

Theorem 2.10. *Let K be a field with an absolute value $|\cdot|$. Then there exists a complete valued field $(\hat{K}, |\cdot|)$ and a homomorphism $K \to \hat{K}$ that is universal in the sense that every homomorphism $K \to L$ where L is complete with respect to $|\cdot|$ (preserving the absolute value) extends uniquely to a homomorphism $\hat{K} \to L$.*

As usual, things in the nonarchimedean case are often a bit nicer. We now consider completions in this case, with the added assumption of a discrete nonarchimedean absolute value $|\cdot|$. Using the notation in Proposition 2.7, we let π generate $\mathfrak{m}$. The fact that $|K^*|$ is discrete means that $|K| = |\hat{K}|$. It will now be useful to define

$$\hat{A} := \{a \in \hat{K} : |a| \leq 1\}. \tag{2.6}$$

Similarly, the corresponding maximal ideal is

$$\hat{\mathfrak{m}} := \{a \in \hat{K} : |a| < 1\}. \tag{2.7}$$

This makes sense as all Cauchy sequences must stabilize at a subsequence that is a multiple of a power of π due to discreteness. With that, we have the following isomorphism.

Lemma 2.11. *For every $n \in \mathbb{Z}_{\geq 1}$, the natural map $A/\mathfrak{m}^n \to \hat{A}/\hat{\mathfrak{m}}^n$ is an isomorphism.*

Proof. It is clear it is a homomorphism, so it remains to show it is bijective. If $a - b \notin \mathfrak{m}^n$ but $(a, a, ...)$ and $(b, b, ...)$ are equal in the codomain, then $(b-a, b-a, ...) \in \hat{\mathfrak{m}}^n$. But since $\mathfrak{m}^n$ is closed, $b - a$ cannot be a limit point of $\mathfrak{m}^n$, a contradiction.

We now seek to prove surjectivity. Since the right-hand side is open, the fact that $A \hookrightarrow \hat{A}$ has dense image means that each equivalence class in the codomain has a sequence of the form $(a, a, ...)$ for $a \in A$. Thus, we're done. □

The next proposition shows that we can actually express Cauchy sequences uniquely as an infinite sum. It is this power series representation that will be incredibly powerful in $\mathbb{Q}_p$-arithmetic later in this section.

Proposition 2.12. *Choose a set S of representatives for $A/\mathfrak{m}$, and let π generate $\mathfrak{m}$. The series*

$$a_{-n}\pi^{-n} + \cdots + a_0 + a_1\pi + \ldots \tag{2.8}$$

is a Cauchy series, and every Cauchy series is equvialent to exactly one of this form.

Proof. It is easy to see this is Cauchy by the strong triangle inequality. To show it is unique, we use the fact that $|\hat{K}| = |K|$ to write an $\alpha \in \hat{K}$ as $\alpha = \pi^n \alpha_0$, with α_0 a unit in $\hat{A}$. A little algebra finishes off the proof. □

A simple question dating back to the earliest studies of number theory is: in a given system of numbers, which ones are a square power of another? This is a very important question in $\mathbb{Z}/p\mathbb{Z}$ whose answers ultimately yield to deep theorems utilizing class field theory. See, for instance, the text by David A. Cox titled "Primes of the Form $x^2 + ny^2$". With this, we continue to ask this question in $\mathbb{Q}_p$. To do this, we have to somehow construct a power series whose square is a desired element of $\mathbb{Q}_p$. For this, we naturally turn to induction, which in this context translates to a root

lifting theorem. This is the substance of the next three results, where the machinery of Taylor series also comes to mind. We begin with a simple application of Taylor series.

Proposition 2.13. *Let A be a complete DVR with maximal ideal generated by π. Let a_0 be a simple root of $f(T)$ modulo π. Then, there is a unique root a of $f(T)$ such that $a - a_0 \in (\pi)$.*

Proof. We construct a Cauchy sequence $a_n \to a$, proceeding by induction. We suppose that we have an $a_n \in A$ such that $f(a_n) \cong 0 \pmod{\pi^{n+1}}$. We want to construct an a_{n+1} such that $f(a_{n+1}) \cong 0 \pmod{\pi^{n+2}}$. A consideration of the Taylor series expansion of $f(a_n + h\pi^{n-1})$ does the job. □

We now seek to consider more approximation tools. Newton's Lemma is one such tool, and so we see what we can do with it in the theorem below. Recall that Newton's Lemma over $\mathbb{R}$ starts with a function f and an $a_0 \in \mathbb{R}$ such that $f(a_0)$ has small magnitude. Then we get better approximations via the recursion

$$a_{n+1} = a_n - f(a_n)/f'(a_n). \tag{2.9}$$

Lemma 2.14 (Newton's Lemma over DVR)**.** *Let $f(T) \in A[T]$. Let $a_0 \in A$ satisfy $|f(a_0)| < |f'(a_0)|^2$. Then there is a root a of $f(X)$ in A such that*

$$|a - a_0| \leq \left| \frac{f(a_0)}{f'(a_0)^2} \right|. \tag{2.10}$$

Proof. Define a sequence a_n as in the discussion before the Lemma statement. See [Lan13, §II.2, Proposition 2]. □

We now present a generalization of Proposition 2.13 to roots of arbitrary multiplicity.

Theorem 2.15 (Hensel's Lemma)**.** *Let k be the residue field for A and let $f(T_\in A[T]$ be monic, and write $\tilde{f}$ for the image of f in k. If $\tilde{f} = g_0 h_0$ in $k[T]$, where g_0 and h_0 are monic and relatively prime, then $f = gh$ where $g, h \in A[T]$ and $\tilde{g} = g$ and $\tilde{h} = h$. Moreover, g and h are unique and they generate $A[T]$.*

Proof. An application of Nakayama's Lemma will prove the following:

Lemma 2.16. *Let A be a local ring with residue field k. IF $f, g \in A[T]$ such that $\tilde{f}$ and $\tilde{g}$ are relatively prime and f is monic, then $(f, g) = A[T]$.*

The uniqueness of g and h is easy to show just by considering combinations of the form $uf + vg$. Finally, constructing the g and h follows something akin to the proof of Proposition 2.13, but instead with an application of the Lemma. □

With the presentation of these three results now complete, we now leave these approximation theorems and return once more to absolute values. This time, we discuss how absolute values on a field adapt in a field extension. This is the content of the theorem below. It turns out that it is true without the discrete or nonarchimedean assumption, but for illustrative purposes we assume these two.

Theorem 2.17. *Let K be complete with respect to a discrete absolute value $|\cdot|_K$, and let L be a finite separable extension of K of degree n. Then $|\cdot|_K$ extends uniquely to an absolute value $|\cdot|_L$, on which L is complete. For all $\beta \in L$:*

$$|\beta|_L = |N_{L/K}(\beta)|_K^{1/n} \tag{2.11}$$

where of course we take the positive real root.

Proof. If we let A be the DVR in K, $\mathfrak{p}$ its maximal ideal, and B its integral closure in L, it is a fact that B is also Dedekind ([Mil08, Theorem 3.29]). Also, any absolute value of L extending $|\cdot|_{\mathfrak{p}}$ corresponds to the ideals of B lying over $\mathfrak{p}$.

With the identification of $A[\beta] \simeq A[T]/(f(T))$ where f is the minimal polynomial of β over K, we see that

$$A[\beta]/\mathfrak{p}A[\beta] \simeq k[T]/(\tilde{f}(T)) \tag{2.12}$$

which is a local ring. If we had unique prime ideals β_1 and β_2 over $\mathfrak{p}$, then this would lead to a contradiction. The formula is easily verified by a consideration of the unique extension of $|\cdot|_L$ to a Galois closure of L, which is finite. Lastly, it is easy to show that L is complete. □

Corollary 2.17.1. *The above theorem is true with L being a possibly infinite separable algebraic extension of K.*

Corollary 2.17.2. *With K and L as in the theorem, $n = ef$, where $n = [L : K]$, e is the ramification index, and f is the degree of the residue field extension.*

Proof. The proof of the Theorem shows that a prime ideal of K extends to a prime ideal of L uniquely. □

If $e = n$, we say L is **totally ramified** over K. When $f = n$, we say that L is **unramified** over K. With this terminology we seek to understand these types of extensions further. We start with the latter.

Let K be a field complete with respect to a discrete absolute value $|\cdot|$. Assume that K and the residue field k be perfect. Let A be the DVR of K corresponding to $|\cdot|$. If L is an algebraic (possibly infinite) extension of K, we define B to be its associated DVR and $\mathfrak{p}$ to be its maximal ideal. The following proposition is very important in the theory of unramified extensions of local fields.

Proposition 2.18. *Let L be an algebraic extension of K, and let ℓ be the residue field of K. There is a one-to-one correspondence:*

$$\{K' \subset L, \textit{finite and unramified over } K\} \Longleftrightarrow \{k' \subset \ell, \textit{finite over } k\}. \tag{2.13}$$

Furthermore

i. The correspondence preserves inclusion.
ii. K' is Galois over K if and only if k' is Galois over k. If so, there is a canonical isomorphism between the two Galois groups.

Proof. Proof is standard local field theory. □

Corollary 2.18.1. *There is a maximal unramified extension of K which is a subset of $\overline{K}$ and contained in $\overline{K}$.*

Proof. Falls to basic considerations of the properties of algebraic closure. □

We now move to discuss totally ramified extensions of local fields. This turns out to be quite simple, as Eisenstein polynomials provide us with an explicit description of all totally ramified extensions of K. Recall that $f(T) \in K[T]$ is said to be Eisenstein if (1) the leading coefficient is unit in A, the constant coefficient is in $(\pi) \setminus (\pi)^2$, and all other coefficients are non-unit in A.

Proposition 2.19. *Let L be a finite extension of K. Then L is totally ramified if and only if $L = K[\alpha]$ with α a root of an Eisenstein polynomial.*

Proof. The proof from right to left is just consideration of the extended normalized discrete valuation. The proof from left to right uses the fact that if $\sum_{i=1}^{n} a_i = 0$, the maximal value of the summands must be attained for at least two subscripts. Here we consider $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. □

We now begin to wonder what happens if L is Galois over K. Let $G = \mathrm{Gal}(L/K)$. By Theorem 2.17, G preserves the absolute value on L, and in particular fixes B and $\mathfrak{p}$. Let Π generate $\mathfrak{p}$, and define subgroups that split the elements of G with respect to the discrete valuation as follows: for $i \in \mathbb{Z}_{\geq 0}$, define $G_i \subset G$ as the elements $\sigma \in G$ such that $|\sigma(\alpha) - \alpha| < |\Pi|^i$. The proof of the following is intuitive.

Proof. Eventually, the G_i become trivial. □

The reason we introduce these groups is to go into further detail about unramified extensions.

Theorem 2.20. *Let L/K Galois, and assume that ℓ/k is separable. Then, the fixed field of G_0 is the largest unramified extension K_0 of K in L.*

One will note from Proposition 2.18 that the roots of distinct polynomials will often give the same extension of a local field K. We explore this in the final few results of this section. We begin with a result of Krasner.

Lemma 2.21 (Krasner)**.** *Let $\alpha, \beta \in \overline{K}$ and assume that α is separable over $K[\beta]$. If α is closer to β than to any conjugate of α over K, then $K[\alpha] \subset K[\beta]$. The proof is quite easy, using basic Galois theory, so we omit it.*

In the remainder of this section, the distance between two polynomials f and g will be the supremum of the absolute values of coefficients of $f - g$. This allows us to use "close enough" in the following results. By a simple bounding argument, it is easy to see that, given a fixed $f(T) \in K[T]$ (with roots $\alpha_1, \ldots, \alpha_n$), we can choose a close enough polynomial $g(T) \in K[T]$ with root β such that $|\beta - \alpha_i| < |\alpha_i - \alpha_j|$ for $i \neq j$. Here, we say that β **belongs to** α_i. By a brief consideration of the degrees of $K[\alpha_i]$ and $K[\beta]$, we obtain the following Proposition.

Proposition 2.22. *Let $f(T) \in K[T]$ be monic and irreducible. Then, every monic polynomial $g(T) \in K[T]$ sufficiently close to f is also irreducible, and each root β of g belongs to some root α of f. For such a root, $K[\alpha] = K[\beta]$.*

As a corollary we have a relation between extensions of $\mathbb{Q}$ and extensions of its p-adic completions.

Corollary 2.22.1. *Let $K/\mathbb{Q}_p$ finite. Then there is a finite extension $L/\mathbb{Q}$ with $L \subset K$ such that $[L : \mathbb{Q}] = [K : \mathbb{Q}_p]$ and $L \cdot \mathbb{Q}_p = K$.*

Proof. Use the identification of $\mathbb{Q} \subset \mathbb{Q}_p$. □

Next, consider a sequence of polynomials $g_i \to f$, where f has roots $\alpha_1, \ldots \alpha_n$. Let the roots of g_i be $\beta_{i1}, \ldots \beta_{in}$. Each root β_{ij} approaches some $\alpha_{k(i)}$, and $k(i)$ becomes fixed for i large enough. Let f_s be the polynomial with roots $\alpha_{k(i)}$ (*possibly with repetitions*. Since g is close to f_s when it is close to f, then it is clear that g cannot be closer to f than f can be to any possible f_s. This shows the following:

Proposition 2.23. *We have*

$$\{K[\alpha] : f(\alpha) = 0\} = \{K[\beta] : g(\beta) = 0\}. \tag{2.14}$$

This result can be applied to yield the following proposition.

Proposition 2.24. *Assume K is a local field. Then there are only finitely many totally ramified extensions of K of a given degree.*

Proof. The main ingredient is Proposition 2.19 and the observation that $\mathfrak{m}^{n-1} \times A^*\pi$ is compact combined with the above proposition. □

3. Global Fields

We know from Proposition 2.17 that the absolute value of a complete field extends uniquely in a given field extension. For global fields (number fields, finite extension of $\mathbb{F}_q(T)$), this isn't necessarily the case. Fix a global field K and let L/K be a finite separable extension. Then, we have two ways of characterizing the extension of an absolute value $|\cdot|$ of K to L. The first is standard, and the second is just a consideration of tensor products combined with the first.

Proposition 3.1. *Let $L = K[\alpha]$ be a finite separable extension of K, and let f be the minimum polynomial of α over K. Then, there is a natural one-to-one correspondence between the extensions of $|\cdot|$ to L and the irreducible factors of f in $\hat{K}[X]$.*

Proposition 3.2. *With notation as in the previous proposition, $|\cdot|$ has finitely many extensions $|\cdot|_1, \ldots |\cdot|_g$ to L. If L_i denotes the completion of L with respect to $|\cdot|_i$. Then,*

$$L \otimes_K \hat{K} \simeq \prod_{i=1}^{g} L_i. \tag{3.1}$$

Since the norm and trace of a linear map are invariant under tensoring, we have that $N_{L/K}(\alpha) = \prod N_{L_i/K}(\alpha)$ and $Tr_{L/K}(\alpha) = \sum Tr_{L_i/K}(\alpha)$. We now step back for a moment to an extension of local fields L/K. Let $\|\cdot\|$ be the normalized absolute value on L correpsonding to the absolute value $|\cdot|$ on K. Then, $\|a\| = |a|^{[L:K]}$. Combining everything in this paragraph, we obtain the following Proposition.

Proposition 3.3. *Let L/K be a finite extension of number fields. For any prime v of K and $\alpha \in L$,*

$$\prod_{w|v} \|\alpha\|_w = \|N_{L/K}(\alpha)\|_v. \tag{3.2}$$

An easy corollary is the product formula for a number field K.

Corollary 3.3.1 (Product Formula for Number Fields)**.** *Let K be an algebraic number field. For all non-zero $\alpha \in K$,*

$$\prod_{w} \|\alpha\|_w = 1. \tag{3.3}$$

We now turn to generalizing the groups G_i introduced in the discussion preceding Theorem 2.20. Let L/K be a finite Galois extension of a number field K, and let $G = \mathrm{Gal}(L/K)$. Let w be an absolute value of L, and write σw for the absolute value such that $|\sigma\alpha|_{\sigma w} = |\alpha|_w$. Defin the **decomposition group** of w to be

$$G_w := \{\sigma \in G : \sigma w = w\}. \tag{3.4}$$

A consideration of the degree of local field extensions yields the following proposition.

Proposition 3.4. *The homomorphism $G_w \to Gal(L_w/K_v)$ — given by the natural extension of $\sigma \in G_w$ to an automorphism of L_w — is an isomorphism.*

We now let $D(\beta)$ be the decomposition group of β and we let $I(\beta)$ be the inertia group. Denote by $L^{I(\beta)}$ the fixed field of $I(\beta)$ and similarly for $D(\beta)$. The following proposition lists key properties of these groups, the proofs of which are relatively straightforward.

Proposition 3.5. *We have the following:*

i. The only prime ideal of L lying over $\beta \cap L^{D(\beta)}$ is β.
ii. The prime ideal $\beta \cap L^{D(\beta)}$ is unramified in $L^{I(\beta)}$.
iii. The prime ideal $\beta \cap L^{I(\beta)}$ is totally ramified in L.
iv. If $D(\beta)$ is normal in G, then

$$\mathfrak{p}\mathcal{O}_{L^{D(\beta)}} = \prod_{\sigma \in G/D(\beta)} \sigma(L^{D(\beta)}). \tag{3.5}$$

References

[Con] Brian Conrad, *Math 154. density for the ring of integers*, http://virtualmath1.stanford.edu/~conrad/154Page/handouts/intdensity.pdf, Online; accessed August 11, 2020.

[Lan13] Serge Lang, *Algebraic number theory*, vol. 110, Springer Science & Business Media, 2013.

[Mil08] James S Milne, *Algebraic number theory*, JS Milne, 2008.

[Sch03] René Schoof, *Algebraic number theory*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.168.6261&rep=rep1&type=pdf, 2003, Online; accessed August 11, 2020.

[Sil09] Joseph H Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer Science & Business Media, 2009.

Email address: asz2115@columbia.edu