A PROOF OF THE KRONECKER-WEBER THEOREM

JINFEI HUANG

Abstract. The present exposition presents an approximately self-contained proof of the global Kronecker-Weber theorem, making extensive use of higher ramification groups in the spirit of Hilbert. Along the way, we examine the rudiments of algebraic number theory, cyclotomic fields, and the basic theory of valuations.

1. Introduction

The celebrated Kronecker-Weber theorem asserts that every finite abelian extension of the rational numbers is contained within a cyclomotic field. First announced in 1853, the result is one of the earliest in what is now known as class field theory, or the study of abelian extensions of local and global fields. Proclaiming his discovery, Kronecker writes,

> "...We obtain the remarkable result that the root of every abelian equation with integer coefficients can be represented as a rational function of roots of unity..."

Kronecker's attempted approach, featuring Lagrange resolvents, succeeded in only giving a partial proof, by his own admission; alas, Kronecker-Weber did not succumb[1] for the case of cyclic extensions with degree 2^n, $n \geq 3$, and therefore retained its status as a conjecture.

In 1886, Weber supplied a proof using much of the similar ideas as his predecessor. Accordingly, he was credited for being the first to provide a complete and valid justification. Over ninety years elapsed before Olaf Neumann finally noticed a flaw in Weber's argument, which overturned a widely-held belief within the mathematical community and somewhat undermined the historical accuracy of the main result's naming convention.

By contemporary accounts, Hilbert became the first to prove the Kronecker-Weber theorem in full generality, as originally conjectured, in his 1896 paper (in which he too accredited Weber, with no small amount of irony). Hilbert attacked the problem from a different angle, and found a way to leverage his then recently-developed theory of higher ramification groups. It is worth mentioning the strategy he employed has connections to later ideas in class field theory.

Concerning the layout of this paper, Section 2 is divided into four subsections, each intended to rapidly treat a topic of necessary background information. Integrality (2.1) is split from the rest of the commutative algebra preliminaries (2.2), as the latter contains more specialized lemmas to be used in the sequel. In subsection 2.3, we state the fundamentals of field and classical Galois theory, followed by a discussion on cyclotomic fields. Subsection 2.4 focuses on bilinear forms, dual bases, and nondegeneracy.

Section 3 marks the end of review material and makes the transition to algebraic number theory by defining the trace, norm, and discriminant. Section 4 introduces fractional ideals and proves a central property about unique factorization of ideals in Dedekind domains. In the subsequent Section 5, we devoted our attention a special class of Dedekind domains called discrete valuation rings and the closely associated notion of a discrete valuation. The aim of Section 6 is to synthesize some of these concepts while laying the groundwork for a particular setup we are interested in. Sections 7 and 8 investigate the situation when additional assumptions are imposed; importantly,

Date: July 17, 2023.

[1]Based space and OMORI-pilled.

here we begin the study of ramification theory. We note that Section 7 includes a proof of the fundamental identity; then, Section 8 will sharpen the result in the Galois case by considering an action of the Galois group. Higher ramification groups are detailed in Section 9, and a number significant properties are given. Section 10 on algebraic number fields and in their rings of integers brings us back to a concrete framework; we determine the prime numbers which ramify in an algebraic number field in terms of its discriminant. In Section 11, we perform some calculations with cyclotomic fields in order to understand them on a deeper level. This puts us in a position to finally tackle the Kronecker-Weber theorem.
In Section 12, a series of lemmas builds up to the main result, which, by an application of ramification theory, reduces to a special case in the penultimate Section 13. The conclusion is that one only has to consider cyclic extensions of prime power degree p^m where p is the only prime that ramifies. At this point, we examine two separate cases depending on the parity of p; both are covered in Section 14, but the harder case, when $p = 2$, relies on a technical induction argument and is accordingly reserved for last.

2. Preliminaries and conventions

All rings are tacitly assumed to be commutative and unital, because noncommutative rings are a hoax. Accordingly, we use the terms "domain" and "integral domain" interchangeablely. Every ring homomorphism φ respects the identity; that is, φ carries 1 to 1. Definitions, commonly embedded into the text, shall be indicated in bold.

2.1. **Integrality.** Recall there is a ring theoretic generalization for the notion of algebraic elements in a field extension. Given an extension B/A of rings, we say an element $x \in B$ is ***integral*** over A if x is a root of some monic polynomial with coefficients in A. If every element of B is integral over A, we shall say that B is ***integral*** over A, and, in the case when A is a domain and B its field of fraction $\mathbb{K}$, that A is ***integrally closed***.
As in the theory of fields, the notation $A[x]$ denotes the smallest subring of B containing A and x. It is easily checked that $A[x]$ is the set of polynomials in x with coefficients in A. Let now us state a technical-sounding proposition that will play a crucial role in the proof of Theorem 4.4 later on.

Proposition 2.1. Let B/A be a ring extension. Then an element $x \in B$ is integral over A if and only if there exists a faithful $A[x]$-module M that is finitely generated as an A-module [AM69, Proposition 5.1].

The set of elements of a ring B that are integral over a subring A is called the ***integral closure*** of A in B. The basic fact to keep in mind about integrality is this:

Proposition 2.2. If B/A is a ring extension, the integral closure of A in B is a subring of B containing A [AM69, Corollary 5.3].

Morevover, integral dependence is transitive. The proof thereof is not unlike that of its field theory counterpart (transitivity of algebraic extensions).

Proposition 2.3. Let $A \subseteq B \subseteq C$ be rings. If C is integral over B and if B is integral over A, then C is integral over A [AM69, Corollary 5.4].

Corollary 2.4. If B/A is a ring extension and $\overline{A}$ is the integral closure of A in B, then B is integral over $\overline{A}$.

Proof. By the above, the integral closure of $\overline{A}$ in B is integral over A, and thus contained in $\overline{A}$. ∎

2.2. **Review of commutative algebra.** This subsection records some algebraic results for the reader's convenience, starting off with a well-known fact concerning modules over PIDs. Adopt the convention where the zero module is free with an empty basis.

Theorem 2.5. Every submodule N of a free module M over a principal ideal A is free with $\operatorname{rank} N \leq \operatorname{rank} M$.

Remark 2.6. Theorem 2.5 is true whether $\operatorname{rank} M$ is finite or infinite. The latter case can be shown per an application of Zorn's lemon.

Proof. We want to show every submodule N of A^n is free of $\operatorname{rank} N \leq n$. Proceed by induction. The case $n = 0$ is trivial. If $n = 1$, then N is just an ideal of A. By assumption, $N = (a)$ has a single generator. If a is nonzero, one has $A \cong (a)$ $(x \mapsto ax)$, since A is an integral domain.
Suppose the theorem has been proved for some $n \geq 1$. Let N be a submodule of $A^{n+1} = A^n \oplus A$. If $\pi : A^n \oplus A \to A^n$ denotes projection to the first component, then $\pi(N)$ is a submodule of A^n. By the induction hypothesis, $\pi(N)$ is free of rank $d \leq n$. Take a basis $\pi(e_1), \ldots, \pi(e_d)$, $e_i \in N$, of $\pi(N)$. The elements $e_1, \ldots, e_d$ are linearly independent in N, so $Ae_1 \cdots + Ae_d \cong A^d$. It is easy to check that N is the sum of A-submodules $Ae_1 + \cdots + Ae_d$ and $\ker(\pi|_N)$. But $\ker(\pi|_N) \subseteq \ker \pi = 0 \oplus A$ is a submodule of A. As we know from the $n = 1$ case, $\ker(\pi|_N)$ is free of rank 0 or 1. This says either $\ker(\pi|_N) = 0$, in which case $N \cong A^d$ is free of rank $d \leq n + 1$, or that $\ker(\pi|_N) = Ae$ for some nonzero e, so that $e_1, \ldots, e_d, e$ is a basis for N, a free module of rank $d + 1 \leq n + 1$. ∎

Lemma 2.7. If A is a Noetherian ring, every A-submodule of A^n is finitely generated, for all n.

Proof. Induct on n, as above. The Noetherian condition takes care of the base case $n = 1$, where submodules of A are ideals by a different name. Now suppose $n \geq 1$, and that every submodule of A^n is finitely generated. Let N be a submodule of $A^{n+1} = A^n \oplus A$, and let $\pi : A^n \oplus A \to A^n$ be the natural projection. By the induction hypothesis, $\pi(N)$ has a finite set of generators, say $\pi(e_1), \ldots, \pi(e_d)$, $e_i \in N$. Then N is the sum of submodules $Ae_1 + \cdots + Ae_d$ and $\ker(\pi|_N)$. But $\ker(\pi|_N) \subseteq \ker \pi = 0 \oplus A$ is finitely generated, and (hence) so is N. ∎

Corollary 2.8. Every finitely generated module M over a Noetherian ring A is Noetherian.

Proof. If $e_1, \ldots, e_n \in M$ is a set of generators, then $((a_1, \ldots, a_n) \mapsto a_1e_1 + \cdots + a_ne_n) : A^n \to M$ exhibits M as a quotient of A^n. This implies every submodule of M is finitely generated, in light of Lemma 2.7 and the correspondence theorem. ∎

Lemma 2.9. If A is a ring and $\mathfrak{m}$ is a maximal ideal, then $A/\mathfrak{m} \cong A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$.

Proof. Let us consider the natural composition $A \to A_\mathfrak{m} \to A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$, the kernel of which contains $\mathfrak{m}$. The induced homomorphism $A/\mathfrak{m} \to A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$ is injective as the domain is a field. For any $s \in A - \mathfrak{m}$, this map sends the inverse of $s \pmod{\mathfrak{m}}$ to the element $1/s \pmod{\mathfrak{m}A_\mathfrak{m}}$, by uniqueness of inverses for $s/1 \pmod{\mathfrak{m}A_\mathfrak{m}}$. This proves surjectivity. ∎

Lemma 2.10. Let A be an integral domain with field of fractions $\mathbb{K}$. The conditions below are equivalent:

(i) A is integrally closed;
(ii) $A_\mathfrak{p}$ is integrally closed for all prime ideals $\mathfrak{p}$;
(iii) $A_\mathfrak{m}$ is integrally closed for all maximal ideals $\mathfrak{m}$.

Proof. Assume A is integrally closed, and let $\mathfrak{p}$ be a prime ideal. Suppose $x \in \mathbb{K} = \operatorname{Frac} A_\mathfrak{p}$ satisfies a monic polynomial equation $x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0$ for $a_i \in A_\mathfrak{p}$. Multiplying by a common denominator $s \in A - \mathfrak{p}$ of the coefficients a_i, and then by s^{m-1}, one obtains an equation of integral dependence for sx over A, which means $sx \in A$ and $x \in A_\mathfrak{p}$. Therefore $A_\mathfrak{p}$ is integrally closed.
Now suppose $A_\mathfrak{m}$ is integrally closed for all maximal ideals $\mathfrak{m}$. If $x \in \mathbb{K}$ is integral over A, it is *a fortiori* integral over the localization $A_\mathfrak{m} \supseteq A$ at every maximal ideal $\mathfrak{m}$, and $x \in A_\mathfrak{m}$. But the ideal $\{a \in A \mid ax \in A\}$ of denominators of x cannot be proper: otherwise, it would be contained in a maximal ideal $\mathfrak{m}$, while $x \in A_\mathfrak{m}$ can be written as a fraction with denominator in $A - \mathfrak{m}$. Therefore $1 \in \{a \in A \mid ax \in A\}$. ∎

Lemma 2.11. Let A be a Noetherian local integral domain. If the unique maximal ideal $\mathfrak{m}$ of A is principal, then A is a PID.

Proof. Let $\pi \in A$ generate $\mathfrak{m}$. Every nonzero nonunit element in a Noetherian domain admits a (possibly nonunique) factorization into irreducibles. But each irreducible element of the local ring A is contained in $\mathfrak{m}$, and hence is an associate of π. In other words, every nonzero element $a \in A$ can be written as $a = \pi^{v(a)}u$ for some $v(a) \geq 0$ and $u \in A^\times$. Now for an arbitrary ideal $\mathfrak{a}$ with a finite system of generators $a_1, \ldots, a_k$, the element π^v with $v = \min v(a_i)$ generates $\mathfrak{a} = (\pi^v)$. ∎

Theorem 2.12 (Hilbert basis theorem)**.** If A is a Noetherian ring, the polynomial ring $A[X]$ is Noetherian.

Remark 2.13. By iteration, the polynomial ring $A[X_1, \ldots, X_n]$ in n variables is also Noetherian, provided A is Noetherian (for example, when A is a field).

2.3. **Miscellaneous field theory.** Fix an arbitrary field $\mathbb{K}$. Given two field extensions $\mathbb{L}_1, \mathbb{L}_2$ of $\mathbb{K}$, define $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}_1, \mathbb{L}_2)$ to be the set of ring homomorphisms $\mathbb{L}_1 \to \mathbb{L}_2$ that restrict to the identity on $\mathbb{K}$.
An irreducible polynomial f in $\mathbb{K}[X]$ is inseparable if f has double roots in some extension field of $\mathbb{K}$, and ***separable*** otherwise. We say an algebraic extension $\mathbb{L}/\mathbb{K}$ is ***separable*** if every element $x \in \mathbb{L}$ is separable, i.e. the minimial polynomial of x over $\mathbb{K}$ is separable. Every algebraic extension in characteristic zero is separable; see [Kna16, Proposition 9.27]. It can also be shown that every algebraic extension of a finite field is separable [Kna16, p. 477]. To check that a finite extension is separable, it suffices to find a set of separable generators [Kna16, Corollary 9.30].
Just like algebraic extensions, separability behaves nicely in towers.

Proposition 2.14. Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ be a tower of algebraic field extensions. If $\mathbb{M}/\mathbb{K}$ is separable, then $\mathbb{M}/\mathbb{L}$ and $\mathbb{L}/\mathbb{K}$ are separable.[2]

Proof. Let $x \in \mathbb{M}$ be an arbitrary element with minimal polynomial $p(X)$ over $\mathbb{L}$. Note that $p(X)$ divides the minimal polynomial $p_0(X)$ of x over $\mathbb{K}$. Since the latter does not have double roots in any extension field of $\mathbb{K}$, the former cannot have double roots in any extension field of $\mathbb{L}$. ∎

Let $\mathbb{L}/\mathbb{K}$ be an extension, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$. The cardinality of $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$, denoted $[\mathbb{L} : \mathbb{K}]_{\mathrm{sep}}$, is independent of the choice of $\overline{\mathbb{K}}$ since all algebraic closures of a field are isomorphic. This sets up the following characterization of separability in the case when $\mathbb{L}$ is a finite extension.

Proposition 2.15. For any finite $\mathbb{L}/\mathbb{K}$, the value $[\mathbb{L} : \mathbb{K}]_{\mathrm{sep}}$ is finite. In fact, one has

$$[\mathbb{L} : \mathbb{K}]_{\mathrm{sep}} \leq [\mathbb{L} : \mathbb{K}],$$

with equality if and only if $\mathbb{L}$ is a separable extension of $\mathbb{K}$.

Proof. Combine [Kna16, Corollary 9.29] and [Kna16, Corollary 9.30]. ∎

Theorem 2.16 (Primitive element theorem)**.** Every finite separable extension $\mathbb{L}/\mathbb{K}$ is simple, i.e. there exists some $\gamma \in \mathbb{L}$ such that $\mathbb{L} = \mathbb{K}(\gamma)$ [Kna16, Theorem 9.34].

Corollary 2.17. If $\mathbb{L}/\mathbb{K}$ and $\mathbb{L}'/\mathbb{K}$ are finite separable, then so is the compositum $\mathbb{L}\mathbb{L}'/\mathbb{K}$.

Proof. Write $\mathbb{L} = \mathbb{K}(\alpha)$ and $\mathbb{L}' = \mathbb{K}(\alpha')$ by the primitive element theorem. Then $\mathbb{L}\mathbb{L}' = \mathbb{K}(\alpha, \alpha')$, which is a separable extension of $\mathbb{K}$, since α, α' are separable. ∎

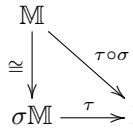
Lemma 2.18. Let $\mathbb{L}/\mathbb{K}$ be an algebraic extension. Any embedding of $\mathbb{K}$ into an algebraically closed field $\mathbb{K}'$ extends to one of $\mathbb{L}$ into $\mathbb{K}'$.

Proof. See [Kna16, Theorem 9.23] for a proof with a set-theoretic flavor. ∎

[2]The converse is equally true, albeit less relevant in the present paper.

Lemma 2.19. Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ be a tower of field extensions, and fix an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. Define an equivalence relation on $\mathrm{Hom}_{\mathbb{K}}(\mathbb{M}, \overline{\mathbb{K}})$ by declaring $\sigma_1 \sim \sigma_2$ if and only if $\sigma_1|_{\mathbb{L}} = \sigma_2|_{\mathbb{L}}$. Suppose $\mathbb{M}/\mathbb{L}$ is separable and finite. Then each equivalence class contains exactly $[\mathbb{M} : \mathbb{L}]$ elements.

Proof. For each $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{M}, \overline{\mathbb{K}})$, the isomorphism $\sigma : \mathbb{M} \to \sigma\mathbb{M}$ induces a one-to-one correspondence $\tau \mapsto \tau \circ \sigma$ from $\mathrm{Hom}_{\sigma\mathbb{L}}(\sigma M, \overline{\mathbb{K}})$ onto the equivalence class $[\sigma]_\sim$, as in



Now since $\mathbb{M}$ is a separable finite extension of $\mathbb{L}$, by Proposition 2.15,

$$|[\sigma]_\sim| = |\,\mathrm{Hom}_{\sigma\mathbb{L}}(\sigma M, \overline{\mathbb{K}})| = [\sigma\mathbb{M} : \sigma\mathbb{L}]_{\mathrm{sep}} = [\mathbb{M} : \mathbb{L}]_{\mathrm{sep}} = [\mathbb{M} : \mathbb{L}].$$

The second equality is obtained by considering $\overline{\mathbb{K}}$ as an algebraic closure of $\sigma\mathbb{L}$, which makes sense because, via Lemma 2.18, the inclusion $\mathbb{K} \hookrightarrow \overline{\mathbb{K}}$ extends to an embedding of $\sigma\mathbb{L}$ into $\overline{\mathbb{K}}$. ■

An algebraic field extension $\mathbb{L}/\mathbb{K}$ is ***normal*** if every irreducible polynomial in $\mathbb{K}[X]$ with a root in $\mathbb{L}$ splits completely in $\mathbb{L}[X]$. For an arbitrary extension $\mathbb{L}/\mathbb{K}$, its ***Galois group*** $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is the group of $\mathbb{K}$-automorphisms of $\mathbb{L}$. A Galois extension whose Galois group is abelian (resp. cyclic) is aptly called an ***abelian extension*** (resp. ***cyclic extension***). There are a number of useful characterizations for normality.

Proposition 2.20. Suppose $\mathbb{L}/\mathbb{K}$ is finite. Then the following are equivalent:

(i) $\mathbb{L}$ is normal over $\mathbb{K}$,
(ii) $\mathbb{L}$ is the splitting field of some nonconstant $f(X) \in \mathbb{K}[X]$,
(iii) every $\mathbb{K}$-homomorphism of $\mathbb{L}$ into an algebraic closure $\overline{\mathbb{L}}$ carries $\mathbb{L}$ into itself.

Proof. This is essentially a restatement of [Kna16, Proposition 9.34A]. ■

In a finite normal field extension $\mathbb{L}/\mathbb{K}$, by the above, corestriction onto $\mathbb{L}$ defines a bijection from $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})$ onto $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{L})$. Now assuming $\mathbb{L}/\mathbb{K}$ is furthermore ***Galois*** (separable and normal), the size of the Galois group $|\,\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$ is equal to the degree [Kna16, Proposition 9.35], which, in turn, is equal to the separable degree $[\mathbb{L} : \mathbb{K}]_{\mathrm{sep}} = |\,\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})|$ (choosing $\overline{\mathbb{L}}$ as an algebraic closure of $\mathbb{K}$). In short, we have a one-to-one correspondence $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{L}) \longleftrightarrow \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})$ by corestriction.
Given a field extension $\mathbb{L}/\mathbb{K}$, there is an inclusion-reversing correspondence between intermediary fields $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}$ and subgroups H of the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$. Explicitly, each intermediary field $\mathbb{F}$ maps to $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, and, conversely, every subgroup H corresponds to its fixed field $\mathbb{L}^H = \{x \in \mathbb{L} \mid \sigma x = \sigma \text{ for all } \sigma \in H\}$. When is this correspondence one-to-one?

Theorem 2.21 (Fundamental theorem of Galois theory)**.** If $\mathbb{L}/\mathbb{K}$ is a finite Galois extension, the inclusion-reversing maps $\mathbb{F} \mapsto \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ and $H \mapsto \mathbb{L}^H$ between intermediary fields of $\mathbb{L}/\mathbb{K}$ and subgroups of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ are inverses [Kna16, Theorem 9.38].

Lemma 2.22. If $\mathbb{L}/\mathbb{K}$ and $\mathbb{L}'/\mathbb{K}$ are normal extensions, then $\mathbb{L}\mathbb{L}'$ and $\mathbb{L} \cap \mathbb{L}'$ are normal over $\mathbb{K}$.

Proof. We first leverage Proposition 2.20. Let $\mathbb{L}, \mathbb{L}'$ be the splitting fields of $f(X), f'(X) \in \mathbb{K}[X]$, respectively. Then $\mathbb{L}\mathbb{L}'$ is the splitting field of the product of f and f'. Now suppose $g(X)$ is an irreducible polynomial in $\mathbb{K}[X]$ with a root in $\mathbb{L} \cap \mathbb{L}'$. The same root lies in $\mathbb{L}$ and $\mathbb{L}'$, so $g(X)$ splits in both fields. By unique factorization, these two decompositions coincide, and the roots belong to $\mathbb{L} \cap \mathbb{L}'$. Thus, $g(X)$ splits completely in $(\mathbb{L} \cap \mathbb{L}')[X]$. ■

Proposition 2.23. Let $\mathbb{L}, \mathbb{L}'$ be finite Galois extensions of a given field $\mathbb{K}$. The compositum $\mathbb{L}\mathbb{L}'$ is a finite Galois extension of $\mathbb{K}$, and its Galois group $\mathrm{Gal}(\mathbb{L}\mathbb{L}'/\mathbb{K})$ is isomorphic to a subgroup of the product $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \times \mathrm{Gal}(\mathbb{L}'/\mathbb{K})$:

$$\mathrm{Gal}(\mathbb{L}\mathbb{L}'/\mathbb{K}) \cong \{(\sigma, \sigma') \mid \sigma\big|_{\mathbb{L}\cap\mathbb{L}'} = \sigma'\big|_{\mathbb{L}\cap\mathbb{L}'}\} \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \times \mathrm{Gal}(\mathbb{L}'/\mathbb{K})$$

In particular, if $\mathbb{L}/\mathbb{K}$ and $\mathbb{L}'/\mathbb{K}$ are abelian, then so is $\mathbb{L}\mathbb{L}'/\mathbb{K}$ [DF04, Ch. 14, Proposition 21].

We shall borrow a result from Galois theory over finite fields.

Theorem 2.24. Any finite extension $\mathbb{L}$ of $\mathbb{F}_p$ is Galois. The Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{F}_p)$ is cyclic of order $n = [\mathbb{L} : \mathbb{F}_p]$, a generator of which is given by the Frobenius automorphism $x \mapsto x^p$.

Proof. A special case of [Kna16, Proposition 9.40]. ■

Of special interest to algebraic number theory are extensions obtained by adjoining a complex root of unity $\zeta_n = \exp(2\pi i/n)$ to the field of rational numbers $\mathbb{Q}$. These are the ***cyclotomic fields***. In fact, our main result is a partial converse of the fact that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a finite abelian extension; we prove a stronger statement.[3]

Proposition 2.25. The cyclotomic field $\mathbb{Q}(\zeta_n)$ is a finite Galois extension of $\mathbb{Q}$ of degree $\phi(n)$, whose Galois group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. First, $\mathbb{Q}(\zeta_n)$ is the splitting field of the n-cyclotomic polynomial

$$\Phi_n(X) \equiv \prod_{\gcd(k,n)=1} (X - \zeta_n^k) \in \mathbb{Q}[X]$$

over $\mathbb{Q}$. In other words, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is normal. Separability is immediate in characteristic 0. Recall that $\Phi_n(X)$ is irreducible in $\mathbb{Q}[x]$; as such it is the minimal polynomial of ζ_n, and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n(X) = \phi(n)$.
Every $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_n)$ is determined by its action on ζ_n. The image of ζ_n under such an automorphism σ must be another root of $\Phi_n(X)$, which is to say that $\sigma\zeta_n$ can only take on the values ζ_n^a for $0 \leq a < n$, $\gcd(a, n) = 1$. Since there are $\phi(n) = |\mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q})|$ such integers, we know that each value is achieved as σ varies over all the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q})$. We thus have a bijection $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, where each residue $a \bmod n$ gets mapped to the automorphism defined by $\zeta_n \mapsto \zeta_n^a$. ■

There is an elementary fact about cyclotomic polynomials that plays a useful role in calculations:

Lemma 2.26. Let $q = p^r$ be a prime power ($r > 0$). Then $\Phi_q(1) = \prod_{\gcd(k,q)=1}(1 - \zeta_q^k) = p$.

Proof. If $r = 1$, the claim is immediate from $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$. Moreover, the identity $X^n - 1 = \prod_{d|n} \Phi_d(X)$ applied to $n = q = p^r$ shows that

$$1 + X + \cdots + X^{q-1} = \Phi_p(X)\Phi_{p^2}(X) \cdots \Phi_{p^r}(X).$$

Now set $X = 1$ and proceed by strong induction. ■

2.4. **Bilinear forms.** As a brief multilinear algebra review, let us restrict to the finite dimensional case, where V is a $\mathbb{K}$-vector space of dimension n. A ***bilinear form*** over V is another word for a bilinear map from $V \times V$ to its base field $\mathbb{K}$.

[3]The reader at this point may want to familiarize themselves with the basic properties of cyclotomic polynomials if needed.

3. Trace and norm

Definition 3.1. Let B/A be a ring extension such that B is a free A-module of rank n. For each x in B, multiplication by x defines an A-linear endomorphism $T_x : B \to B$, the trace and determinant of which we call the ***trace*** $\mathrm{Tr}_{B/A}(x)$ and ***norm*** $N_{B/A}(x)$ of x, respectively. In symbols,

$$\mathrm{Tr}_{B/A}(x) = \mathrm{Tr}(T_x), \qquad N_{B/A}(x) = \det(T_x).$$

Thus, $\mathrm{Tr}_{B/A}$ and $N_{B/A}$ specify maps from B to A. Using properties of trace and determinant, it is fairly easy to verify the following properties:

Proposition 3.2. If B/A is a ring extension such that B is a free A-module of rank n,

(i) $\mathrm{Tr}_{B/A} : B \to A$ is A-linear,
(ii) $N_{B/A} : B \to A$ is multiplicative and defines a group homomorphism from $B^\times$ to $A^\times$, and
(iii) $N_{B/A}(a) = a^n$ for all $a \in A$.

Lemma 3.3. Let $\mathbb{L}/\mathbb{K}$ be a finite separable extension. Let $f_x(X) = \det(X\,\mathrm{id}_n - T_x) \in \mathbb{K}[X]$ be the characteristic polynomial of T_x (in the notation of Definition 3.1). Then $f_x(X)$ is a power of the minimal polynomial $p(X)$ of x over $\mathbb{K}$:

$$f_x(X) = p(X)^d,$$

where $d = [\mathbb{L} : \mathbb{K}(x)]$.

Proof. Let $m = [\mathbb{K}(x) : \mathbb{K}]$. We know that $1, x, \ldots, x^{m-1}$ is a basis for $\mathbb{K}(x)$ over $\mathbb{K}$. Now choose a basis $a_1, \ldots, a_d$ for $\mathbb{L}$ over $\mathbb{K}(x)$. Then the pairwise products

$$a_1, a_1x, \ldots, a_1x^{m-1}; \ldots; a_d, a_dx, \ldots, a_dx^{m-1}$$

for $\mathbb{L}$ over $\mathbb{K}$. What happens if we express T_x with respect to this basis? By definition, a_jx^ℓ gets sent to $a_jx^{\ell+1}$ under T_x, which has the effect of "shifting" each of $a_j, a_jx, \ldots, a_jx^{m-2}$ forward to the next basis vector. Writing $p(X) = X^m + c_{m-1}X^{m-1} + \ldots + c_0$ for $c_i \in \mathbb{K}$, each a_jx^m can be rewritten as $-c_0a_j - c_1a_jx - \cdots - c_{m-1}a_jx^{m-1}$. Therefore, the matrix of T_x can be written as a block matrix

$$T_x = \begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M \end{pmatrix}, \qquad M = \begin{pmatrix} 0 & 0 & 0 & \cdots & -c_0 \\ 1 & 0 & 0 & \cdots & -c_1 \\ 0 & 1 & 0 & \cdots & -c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -c_{m-1} \end{pmatrix} \in M_m(\mathbb{K}),$$

with d copies of M along the main diagonal. The characteristic polynomial of M is then checked to be $X^m + c_{m-1}X^{m-1} + \cdots + c_0 = p(X)$ by inducting on m and performing cofactor expansion on the leftmost column. We conclude that $f_x(X) = \det(X\,\mathrm{id}_n - T_x) = \det(X\,\mathrm{id}_m - M)^d = p(X)^d$. ∎

Proposition 3.4. If $\mathbb{L}$ is a finite separable extension of $\mathbb{K}$, then for each $x \in \mathbb{L}$, one has

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = \sum_\sigma \sigma x, \qquad N_{\mathbb{L}/\mathbb{K}}(x) = \prod_\sigma \sigma x,$$

where $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$ ranges over all $\mathbb{K}$-embeddings of $\mathbb{L}$ into a fixed algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. For a finite Galois extension $\mathbb{L}/\mathbb{K}$, the sum and product above are indexed by the elements $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

Proof. Let $d = [\mathbb{L} : \mathbb{K}(x)]$ and $m = [\mathbb{K}(x) : \mathbb{K}]$. Define an equivalence relation on $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$ by declaring $\sigma_1 \sim \sigma_2$ if and only if $\sigma_1(x) = \sigma_2(x)$. According to Lemma 2.19, each equivalence class with respect to $\sim$ contains d elements, so the number of classes is $[\mathbb{L} : \mathbb{K}]_{\mathrm{sep}}/d = [\mathbb{L} : \mathbb{K}]/d = m$. Now let $\sigma_1, \ldots, \sigma_m$ be a system of representatives. The minimal polynomial $p(X)$ of x over $\mathbb{K}$ is

of degree m, and the elements $\sigma_1(x), \ldots, \sigma_m(x)$ of $\overline{\mathbb{K}}$ are distinct roots of $p(X)$. Hence, $p(X) = (X - \sigma_1(x)) \cdots (X - \sigma_m(x))$. Lemma 3.3 tells us that $f_x(X) = p(X)^d$. But now

$$f_x(X) = \prod_{i=1}^{m} (X - \sigma_i(x))^d = \prod_{\sigma} (X - \sigma(x)).$$

Vieta's formula yields the desired result. The second assertion evidently follows from our discussion of normal and Galois extensions back in subsection 2.3. ∎

Definition 3.5. Let B/A be a ring extension such that B is a free A-module of rank n, and let $\alpha_1, \ldots, \alpha_n$ be a basis for B over A. The ***discriminant*** $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ of the basis $\alpha_1, \ldots, \alpha_n$ is defined as the determinant of its trace pairing matrix:

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(\operatorname{Tr}_{B/A}(\alpha_i \alpha_j)) \in A.$$

In the notation above, let $\alpha'_1, \ldots, \alpha'_n$ be second basis for the free A-module B. Write $\alpha'_j = \sum a_{ji}\alpha_i$, and let $A = (a_{ij})$ be the change of basis matrix. Then

$$\operatorname{Tr}_{B|A}(\alpha'_k \alpha'_\ell) = \sum_{i,j} \operatorname{Tr}_{B|A}(a_{ki}\alpha_i a_{\ell j}\alpha_j) = \sum_{i,j} a_{ki} \operatorname{Tr}_{B|A}(\alpha_i \alpha_j) a_{ji},$$

so $(\operatorname{Tr}_{B|A}(\alpha'_k \alpha'_\ell)) = A \cdot (\operatorname{Tr}_{B|A}(\alpha_i \alpha_j)) \cdot A^T$ and $\operatorname{disc}(\alpha'_1, \ldots, \alpha'_n) = (\det A)^2 \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. Therefore, as the matrix A is invertible, the discriminant is well-defined up to multiplication by the square of a unit in A. Consequently, the condition $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$ is independent of the choice of basis $\alpha_1, \ldots, \alpha_n$. Another corollary is that discriminant is truly well-defined when $A = \mathbb{Z}$ (the only units in $\mathbb{Z}$ are -1 and 1). We now define the ***discriminant*** $\operatorname{disc}(B/A)$ of B over A as the discriminant $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ of an A-basis for B, regarding the latter as an equivalence class under

$$a_1 \sim a_2 \quad \Longleftrightarrow \quad a_1 = u^2 a_2 \text{ for some } u \in A^\times, \quad (a_1, a_2 \in A).$$

Lemma 3.6. Let $\mathbb{L}/\mathbb{K}$ be a separable field extension with $\mathbb{K}$-basis $\alpha_1, \ldots, \alpha_n$. Then one has

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i \alpha_j)^2,$$

where $\sigma_i \in \operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$ ranges over all $\mathbb{K}$-embeddings of $\mathbb{L}$ into a fixed algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. In particular, a $\mathbb{K}$-basis of the form $1, \gamma, \ldots, \gamma^{n-1}$ has discriminant $\prod_{i<j}(\sigma_i\gamma - \sigma_j\gamma)^2$, by the Vandermonde determinant from linear algebra.

Proof. Applying Proposition 3.4, we find that $\operatorname{Tr}_{B/A}(\alpha_i\alpha_j) = \sum(\sigma_k\alpha_i)(\sigma_k\alpha_j)$, so the trace pairing matrix is $(\sigma_i\alpha_j)^T(\sigma_i\alpha_j)$. ∎

Proposition 3.7. In a separable extension $\mathbb{L}/\mathbb{K}$, the discriminant $\operatorname{disc}(\mathbb{L}/\mathbb{K})$ is nonzero.

Proof. By the primitive element theorem (Theorem 2.16), we have $\mathbb{L} = \mathbb{K}(\gamma)$ for some $\gamma \in \mathbb{L}$. Let $\operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) = \{\sigma_1, \ldots, \sigma_n\}$. Since $1, \gamma, \ldots, \gamma^{n-1}$ is a basis for the $\mathbb{K}$-vector space $\mathbb{L}$ ($n = [\mathbb{L} : \mathbb{K}]$), we deduce that $\operatorname{disc}(1, \gamma, \ldots, \gamma^{n-1}) \neq 0$ from the previous lemma ($\sigma_i\gamma \neq \sigma_j\gamma$ whenever $i < j$, for a $\mathbb{K}$-embedding σ of $\mathbb{L}$ is completely determined by $\sigma\gamma$). ∎

4. Dedekind domains

Definition 4.1. Let A be an integral domain. One says that A is a ***Dedekind domain*** if A is Noetherian, integrally closed, and each nonzero prime ideal in A is maximal.

Remark 4.2. Equivalently, a Dedekind domain is a Noetherian, integrally closed domain A of Krull dimension $\dim A \leq 1$. Some authors prefer to modify the above definition by appending a condition that excludes fields; note the conventional differences.

Example. The ring $\mathbb{Z}$ is a Dedekind domain. In fact, every PID is Dedekind. This is because every UFD is integrally closed, which is essentially just a generalization of the rational root theorem. Indeed, let A be a unique factorization domain; let $\mathbb{K}$ be the quotient field of A. Suppose $x \in \mathbb{K}$ is integral over A. We have a polynomial equation of the form $x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0$ for $a_i \in A$. Writing $x = a/s$ for $a, s \in A$ gives $a^m + a_{m-1}a^{m-1}s + \cdots + a_0 s^m = 0$. If s_i is an irreducible factor of s, then s_i necessarily divides a^m and (hence) $s_i | a$. It follows that $x = a/s \in A$.

Example. Insert example from algebraic geometry (very cool)

Definition 4.3. Let A be an integral domain with field of fractions $\mathbb{K}$. A ***fractional ideal*** $\mathfrak{a}$ of A is an A-submodule of $\mathbb{K}$ such that there is some $a \in \mathfrak{a}$ with $a\mathfrak{a} \subseteq A$.

Ideals of the domain A is are fractional ideals. Conversely, any fractional ideal contained in A is necessarily an ideal. Every fractional ideal is of the form $(1/a)\mathfrak{a}'$ for some ideal $\mathfrak{a}'$ and $a \in A - \{0\}$. One can multiply two fractional ideals $\mathfrak{a}, \mathfrak{b}$. The elements of the ***product*** $\mathfrak{a}\mathfrak{b}$ are finite sums of elements of the form $a_i b_i$ ($a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$). A fractional ideal $\mathfrak{a}$ is said to be ***invertible*** if there is another fractional ideal $\mathfrak{a}^{-1}$ with $\mathfrak{a}\mathfrak{a}^{-1} = A$. The invertible fractional ideals form an abelian group with identity element A. If the inverse $\mathfrak{a}^{-1}$ of $\mathfrak{a}$ exists, it is necessarily given by the ***generalized ideal quotient*** $(A : \mathfrak{a}) = \{x \in \mathbb{K} \mid x\mathfrak{a} \subseteq A\}$. This implies inversion of fractional ideals is inclusion reversing.
More generally, the quotient $(\mathfrak{b} : \mathfrak{a}) = \{x \in \mathbb{K} \mid x\mathfrak{a} \subseteq \mathfrak{b}\}$ of fractional ideals $\mathfrak{a}, \mathfrak{b}$ with $\mathfrak{a} \neq 0$ is also fractional ideal: indeed, find $a, b \in A - \{0\}$ such that $a\mathfrak{a} \subseteq A$ and $b\mathfrak{b} \subseteq A$. For any nonzero element $a_0 \in ab\mathfrak{a} \subseteq A$, we have $a_0(\mathfrak{b} : \mathfrak{a}) = a_0(ab\mathfrak{b} : ab\mathfrak{a}) \subseteq ab\mathfrak{b} \subseteq A$; thus $a_0(\mathfrak{b} : \mathfrak{a}) \subseteq A$ for some $a_0 \in A - \{0\}$.
For any domain A with fractional field $\mathbb{K}$, a finitely-generated A-submodule of $\mathbb{K}$ is a fractional ideal by clearing denominators on a system of generators. In fact, the former can be taken as an equivalent definition if A is Noetherian (due to ideals being finitely generated). We now obtain the handy characterization of Dedekind domains below.

Theorem 4.4. Let A be an integral domain with field of fractions $\mathbb{K}$. Then A is Dedekind if and only if every nonzero fractional ideal is invertible.

First, a couple of lemmas are in order.

Lemma 4.5. If A is an integral domain with field of fractions $\mathbb{K}$, then every invertible fractional ideal $\mathfrak{a}$ of A is a finitely generated A-module.

Proof. Let $\mathfrak{a}^{-1}$ be the inverse of $\mathfrak{a}$, i.e. $\mathfrak{a}\mathfrak{a}^{-1} = A$. This yields an equation $a_1 a_1' + \cdots + a_n a_n' = 1$ for suitable $a_i \in \mathfrak{a}, a_j' \in \mathfrak{a}^{-1}$. Then for any $a \in \mathfrak{a}$, we find that $a_1(aa_1') + \cdots + a_n(aa_n') = a$, so $a \in Aa_1 + \cdots + Aa_n$. ∎

Lemma 4.6. Every ideal (resp. nonzero ideal) $\mathfrak{a}$ in a Noetherian ring A contains a finite product of prime ideals (resp. of nonzero prime ideals).

Proof. Suppose otherwise, i.e. the set Σ of ideals in A that do not contain any finite product of prime ideals is nonempty. Since A is Noetherian, Σ has a maximal element $\mathfrak{a}$. In particular, the ideal $\mathfrak{a}$ itself cannot be prime, so there exist $x, y \notin \mathfrak{a}$ with $xy \in \mathfrak{a}$. Then $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ both contain finite products of prime ideals by the maximality of $\mathfrak{a}$, and so does their product. But $(\mathfrak{a} + (x))(\mathfrak{a} + (y)) = \mathfrak{a}^2 + \mathfrak{a}(x) + \mathfrak{a}(y) + (xy) \subseteq \mathfrak{a}$, contradicting the fact that $\mathfrak{a} \in \Sigma$.
A very similar argument, replacing Σ with the collection of nonzero ideals not containing any finite product of nonzero primes, verifies the parallel claim of the lemma. ∎

Lemma 4.7. Let A be a Noetherian integral domain with field of fractions $\mathbb{K}$, such that every nonzero prime ideal in A is maximal. Then for every nonzero proper ideal $\mathfrak{a}$, there is an element $x \in \mathbb{K} - A$ with $x\mathfrak{a} \subseteq A$.

Proof. Let $a \neq 0$ be an arbitrary nonzero element of $\mathfrak{a}$. According to Lemma 4.6, the nonzero ideal (a) contains a product $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n$ of nonzero primes; let n be minimal with respect to this property. Now choose a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$. Then $\mathfrak{m} \supseteq \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n$, so $\mathfrak{m} \supseteq \mathfrak{p}_i$ for some i, which means $\mathfrak{m} = \mathfrak{p}_i$ because $\mathfrak{p}_i$ is maximal. By the minimality of n, there is an element $b \in \mathfrak{p}_1\cdots\mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\cdots\mathfrak{p}_n$ with $b \notin (a)$. In particular, the element $x = b/a \in \mathbb{K}$ is not contained in A. Since $\mathfrak{a} \subseteq \mathfrak{p}_i$ and $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n \subseteq (a)$, we conclude that $b\mathfrak{a} \subseteq (a)$ and $x\mathfrak{a} = (b/a)\mathfrak{a} \subseteq A$. ∎

Proof of Theorem 4.4. Suppose that A is a Dedekind domain. By the discussion following Definition 4.3, particularly the first paragraph, it suffices to check that every nonzero ideal $\mathfrak{a}$ of A is invertible. Recall the generalized ideal quotient $(A : \mathfrak{a}) = \{x \in \mathbb{K} \mid x\mathfrak{a} \subseteq A\}$ of A and $\mathfrak{a}$ is a fractional ideal. By definition, we have $\mathfrak{a}(A : \mathfrak{a}) \subseteq A$. The claim is that $\mathfrak{a}(A : \mathfrak{a}) = A$. Otherwise, Lemma 4.7 would gives us $x\mathfrak{a}(A : \mathfrak{a}) \subseteq A$ for some $x \in \mathbb{K} - A$ (since $\mathfrak{a}(A : \mathfrak{a}) \supseteq \mathfrak{a}A \supsetneq 0$). Hence $x(A : \mathfrak{a}) \subseteq (A : \mathfrak{a})$, so $M = (A : \mathfrak{a})$ is closed under multiplication by elements of $A[x]$. This allows us to view $M = (A : \mathfrak{a})$ as an $A[x]$-module. Because A is Noetherian, M is finitely generated as an ideal and an A-module, so x is integral over A in view of Proposition 2.1. Finally, the hypothesis that A is integrally closed tells us $x \in A$, clearly a contradition.
Conversely, suppose all nonzero fractional ideals of A are invertible. All invertible ideals are finitely generated by Lemma 4.5, implying that A is Noetherian. Now if $x \in \mathbb{K}$ is integral over A, in other words $x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0$ for some $a_i \in A$, then x^m is in the nonzero fractional ideal $\mathfrak{a} = (1, x, \ldots, x^{m-1})$. Observe that $\mathfrak{a}$ is closed under multiplication by x, or $\mathfrak{a}(x) \subseteq \mathfrak{a}$. Therefore, $x \in (x) = \mathfrak{a}^{-1}\mathfrak{a}(x) \subseteq \mathfrak{a}^{-1}\mathfrak{a} = A$, and A is integrally closed. It remains to prove that every nonzero prime ideal $\mathfrak{p}$ is maximal. Find a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$. Note that $\mathfrak{p} = (\mathfrak{p}\mathfrak{m}^{-1})\mathfrak{m}$, where $\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} = A$ is an ideal. *A fortiori,* either $\mathfrak{p} \supseteq \mathfrak{p}\mathfrak{m}^{-1}$ or $\mathfrak{p} \supseteq \mathfrak{m}$. The first case would yield $\mathfrak{m} = A$ after multiplying by $\mathfrak{p}^{-1}$. This is impossible, so $\mathfrak{p} = \mathfrak{m}$ is maximal. ∎

Remark 4.8. Theorem 4.4 can be taken as a consequence of the Lasker–Noether theorem on the existence of primary decompositions in Noetherian rings (see e.g. the proof of [AM69, Proposition 9.1]).

One can define division of ideals of a ring in the obvious manner: by $\mathfrak{b}|\mathfrak{a}$, we mean that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for an ideal $\mathfrak{c}$. Dedekind domains feature a nice equivalence concerning divisibility, summarized in words by the maxim "to contain is to divide."

Corollary 4.9. If $\mathfrak{a}, \mathfrak{b}$ are ideals in a Dedekind domain A, then $\mathfrak{b} \supseteq \mathfrak{a}$ if and only $\mathfrak{b}|\mathfrak{a}$.

Proof. Suppose that $\mathfrak{b}$ contains $\mathfrak{a}$. By Theorem 4.4, one can find a fractional ideal $\mathfrak{b}^{-1}$ such that $\mathfrak{b}\mathfrak{b}^{-1} = A$. Then $\mathfrak{c} = \mathfrak{b}^{-1}\mathfrak{a} \subseteq A$ is an ideal with $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. ∎

Our goal is to show that ideals in a Dedekind domains satisfy an analogue of the unique factorization of elements in a UFD.

Theorem 4.10. Every nonzero proper ideal $\mathfrak{a}$ in a Dedekind domain A can be factored into a finite product $\mathfrak{a} = \mathfrak{p}_1^{u_1}\mathfrak{p}_2^{u_2}\cdots\mathfrak{p}_n^{u_n}$ $(u_i > 0)$ of distinct prime ideals $\mathfrak{p}_i \neq \mathfrak{p}_j$. Further, this factorization is unique up to permutation.

Proof. To show existence, we argue by contradiction. Suppose the set Σ of nonzero proper ideals without such a prime factorization is nonempty. Since Dedekind domains are Noetherian by definition, we can take a maximal element $\mathfrak{a}$ of Σ. There is a nonzero maximal ideal $\mathfrak{p}$ containing $\mathfrak{a}$. Note that $A \subseteq \mathfrak{p}^{-1}$ because $\mathfrak{p} \subseteq A$, so

$$\mathfrak{a} = \mathfrak{a}A \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A.$$

Neither inclusions can be equalities: $\mathfrak{a}A = \mathfrak{a}\mathfrak{p}^{-1}$ would imply $\mathfrak{p}^{-1} = A = \mathfrak{p}$, and $\mathfrak{a}\mathfrak{p}^{-1} = A$ would yield $\mathfrak{a} = \mathfrak{p}$, contradicting $\mathfrak{a} \in \Sigma$. Thus, by the maximality of $\mathfrak{a}$, we see that $\mathfrak{a}\mathfrak{p}^{-1}$ admits a prime decomposition, and so does $\mathfrak{a}$.

Now suppose $\mathfrak{a} = \mathfrak{p}_1^{u_1} \cdots \mathfrak{p}_n^{u_n} = \mathfrak{q}_1^{v_1} \cdots \mathfrak{q}_r^{v_r}$ are two factorizations of $\mathfrak{a}$ in terms of prime ideals $\mathfrak{p}_i, \mathfrak{q}_j$, with $\mathfrak{p}_{i_1} \neq \mathfrak{p}_{i_2}$ whenever $i_1 \neq i_2$ and similarly for the $\mathfrak{q}_j$. Then $\mathfrak{p}_1$ contains $\mathfrak{q}_1^{v_1} \cdots \mathfrak{q}_m^{v_m}$, so $\mathfrak{p}_1 \supseteq \mathfrak{q}_j$. Assume $j = 1$ without loss of generality. It follows that $\mathfrak{p}_1 = \mathfrak{q}_1$ because $\mathfrak{q}_1$ is a maximal ideal. Cancelling $\mathfrak{p}_1$ from both sides, which is possible thanks to Theorem 4.4, the distinctness of $\mathfrak{p}_i$ and $\mathfrak{q}_j$ (in the suitable sense) forces $u_1 = v_1$. Repeating this process gives the desired conclusion. ■

5. Discrete valuation rings

Theorem 5.1. The local Dedekind domains that are not fields are precisely the local PIDs that are not fields.

A ring A satisfying one of these two equivalent conditions is called a ***discrete valuation ring*** (abbreviated DVR). They are the simplest rings except for fields.

Proof. We have seen that every PID is a Dedekind domain; it suffices prove every local Dedekind domain A is a PID. Let $\mathfrak{m}$ be the unique maximal ideal of A. We are done if A is a field[4]. Otherwise, $\mathfrak{m} \neq 0$. Since $\mathfrak{m}$ is a finitely generated A-module, we have $\mathfrak{m} \neq \mathfrak{m}^2$ by Nakayama's lemon. Pick an element $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$. Note that (0) and $\mathfrak{m}$ are the only primes of A. Since $\pi \neq 0$, the local quotient $A/(\pi)$ only has one prime ideal $\mathfrak{m}/(\pi)$. This means $A/(\pi)$ is Noetherian of dimension 0, and hence Artinian. By properties of local Artinian rings, the maximal ideal $\mathfrak{m}/(\pi)$ is nilpotent. Take $e \geq 1$ minimal such that $\mathfrak{m}^e \subseteq (\pi)$. Assume $e > 1$ toward contradiction. Since $\mathfrak{m}^{e-1} \not\subseteq (\pi)$, one can find $r \in \mathfrak{m}^{e-1}$ with $r \notin (\pi)$. These conditions imply $x = r/\pi \notin A$ and $x\mathfrak{m} \subseteq (1/\pi)\mathfrak{m}^e \subseteq A$; it follows that $x\mathfrak{m}$ is an ideal of A. Since $\pi \notin \mathfrak{m}^2$ and $r \in \mathfrak{m}$ (this step rests on the assumption that $e > 1$), we cannot have $x\pi = (1)$. Therefore $x\mathfrak{m} \subseteq \mathfrak{m}$. The multiplication-by-$x$ endomorphism $\phi : \mathfrak{m} \to \mathfrak{m}$ on the finitely generated A-module $\mathfrak{m}$ satisfies a monic polynomial relation with coefficients in A, from Proposition **??**. Now evaluate at a nonzero element of $\mathfrak{m}$ and cancel it from the equation. We obtain an equation of integral dependence for x over A, contradicting the fact that A is integrally closed. Hence, $e = 1$, and $\mathfrak{m} = (\pi)$ is principal. From Lemma 2.11, A is a PID. ■

In a principal ideal domain, the nonzero prime ideals are precisely the principal ideals (π) generated by an irreducible element π. Thus, given a discrete valuation ring A with unique maximal ideal $\mathfrak{m}$, there is exactly one irreducible element up to multiplication by a unit (any irreducible π would generated $\mathfrak{m}$). Such an element is called a ***uniformizer*** of A.

Proposition 5.2. If A is a Dedekind domain with field of fractions $\mathbb{K}$, then $A_\mathfrak{p}$ is a DVR for any nonzero prime ideal $\mathfrak{p}$ of A.

Proof. (Nontrivial) localizations of a Noetherian domains are Noetherian domains. By Lemma 2.10, $A_\mathfrak{p}$ is integrally closed. The fact that nonzero prime ideals of $A_\mathfrak{p}$ are maximal follows from the one-to-one correspondence between prime ideals of $A_\mathfrak{p}$ and those of A contained in $\mathfrak{p}$. Moreover, it is known that $A_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$. The point of stipulating $\mathfrak{p} \neq 0$ is to ensure that $A_\mathfrak{p}$ is not a field (the maximal ideal is nonzero). ■

Definition 5.3. Let K be a field. A ***discrete valuation*** v on K is a surjective group homomorphism $v : K^\times \to \mathbb{Z}$, extended to the whole of K by setting $v(0) = \infty$, such that $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in K$.

Let A be a DVR with field of fractions $\mathbb{K}$, and fix a uniformizer $\pi \in A$. By unique factorization of elements, any nonzero $x \in A$ can be expressed in the form $\pi^m u$ for unique $m \in \mathbb{Z}_{\geq 0}$ and $u \in A^\times$. The integer m does not depend on the choice of uniformizer; we call it the ***valuation*** $v(x)$ of x. Now every nonzero element $x \in \mathbb{K}$ admits a unique representation of the form $\pi^m u$, where $m \in \mathbb{Z}$ this time (and $u \in A^\times$). So v extends to a map from $\mathbb{K}^\times$ to $\mathbb{Z}$ by setting $v(x) = m$. One can easily verify that v is indeed a discrete valuation on $\mathbb{K}$, and that A is the set $\{x \in \mathbb{K} \mid v(x) \geq 0\}$, whose unique maximal ideal $\mathfrak{m} = (\pi) = \{x \in \mathbb{K} \mid v(x) > 0\}$ is the set of elements with positive valuation.

[4]Remember how, by our definition, fields are Dedekind domains (but not DVRs).

Conversely, we can start with a discrete valuation v on a field K. The ***valuation ring*** of K is $A = \{x \in K \mid v(x) \geq 0\}$. Since $v(xy) = v(x)v(y)$ for all $x, y \in K$, A is an integral domain; its fraction field is K. Moreover, every element of A not in the proper ideal $\mathfrak{m} = \{x \in \mathbb{K} \mid v(x) > 0\}$ is a unit (for if $v(x) = 0$, then $v(x^{-1}) = v(xx^{-1}) = v(1) = 0$, so $x^{-1} \in A$); this makes A into a local ring. Due to surjectivity, we can pick some $\pi \in \mathfrak{m}$ with $v(\pi) = 1$. For any $x \in K$ with $v(x) = n$, we have $x = \pi^n u$ for a unit $u \in A$ ($v(x/\pi^n) = 0$). Any ideal $\mathfrak{a}$ of A is generated by an element $x \in \mathfrak{a}$ with minimal $v(x)$. We conclude that A is a DVR with v as its associated discrete valuation.
In a Dedekind domain A with fraction field $\mathbb{K}$, the localization $A_\mathfrak{p}$ at nonzero prime ideal $\mathfrak{p}$ is a DVR (Proposition 5.2), which also has fraction field $\mathbb{K}$. Let $v_\mathfrak{p}$ denote the discrete valuation on $\mathbb{K}$ associated with $A_\mathfrak{p}$.

Example. For each prime p, the localization $\mathbb{Z}_{(p)}$ of the Dedekind domain $\mathbb{Z}$ at $(p) \neq 0$ gives rise to the ***p-adic valuation*** on $\mathbb{Q}$.

Definition 5.4. Let K be a field. By an ***absolute value*** on K, we mean a multiplicative function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying the triangle inequality (i.e. $|x + y| \leq |x| + |y|$ for all $x, y \in K$) such that $|x| = 0$ if and only if $x = 0$.

Choose a real number $b > 1$. Every discrete valuation v on a field K induces an absolute value $|\cdot|_v$ on K by $|x|_v = b^{-v(x)}$. If $\mathfrak{p}$ is a prime ideal of a Dedekind domain A with field of fractions $\mathbb{K}$, the absolute value arising from v_p will be denoted by $|\cdot|_\mathfrak{p}$.

6. The "AKLB setup"

This section, chiefly based on [Neu99], uses the following notation: let A be an integrally closed integral domain with field of fractions $\mathbb{K}$, let $\mathbb{L}$ be a finite separable extension of $\mathbb{K}$, and let B be the integral closure of A in $\mathbb{L}$. Also, let $n = [\mathbb{L} : \mathbb{K}]$ denote the degree of $\mathbb{L}$ over $\mathbb{K}$.

Proposition 6.1. Every element $x \in \mathbb{L}$ can be written in the form $x = \beta/\alpha$ for some $\beta \in B$ and nonzero $\alpha \in A$.

Proof. We really only need $\mathbb{L}/\mathbb{K}$ to be an algebraic extension and A an arbitrary integral domain: any $x \in \mathbb{L}$ satisfies a nontrivial polynomial equation of the form

$$a_r x^r + a_{r-1} x^{r-1} + \cdots + a_0 = 0$$

with coefficients $a_i \in \mathbb{K}$. Clearing denominators, we may take each a_i to be in A. Multiplying by a_r^{r-1} yields

$$(a_r x)^r + a'_{r-1}(a_r x)^{r-1} + \cdots + a'_0 = 0$$

for $a'_i \in A$. Thus $\beta = a_r x$ is integral over A, and the claim follows after solving for x. ∎

Corollary 6.2. The field of fractions $\operatorname{Frac} B$ of the integral domain B is $\mathbb{L}$.

Proof. The previous proposition gives $B \subseteq \mathbb{L} \subseteq \operatorname{Frac} B$. On the other hand, $\mathbb{L}$ is a field and thus contains every fraction of elements of B. ∎

Proposition 6.3. If $x \in B$, the minimal polynomial $p(X)$ of x over $\mathbb{K}$ takes coefficients in A.

Proof. Find a monic polynomial $f(X) \in A[x]$ of which x is a root. Then $p(X)$ divides $f(X)$ in $\mathbb{K}[x]$. Hence, working within a splitting field, all the zeros of $p(X)$ are integral over A, and so are the coefficients, by Vieta. But $\mathbb{K} \cap B = A$ (here we only use that A is integrally closed), and the proposition follows. ∎

Lemma 6.4. For any $x \in B$, the trace $\operatorname{Tr}_{\mathbb{L}/\mathbb{K}}(x)$ and norm $N_{\mathbb{L}/\mathbb{K}}(x)$ of x are contained in A.

Proof. Since x is integral over A, so are the elements σx for each $\sigma \in \operatorname{Hom}_\mathbb{K}(\mathbb{L}, \overline{\mathbb{K}})$. The claim now follows from Proposition 3.4 and the hypothesis that A is integrally closed. ∎

Lemma 6.5. Let $\alpha_1, \ldots, \alpha_n$ be a basis of $\mathbb{L}$ over $\mathbb{K}$ contained in B, and let $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. Then one has

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

Proof. Let $\alpha \in B$ be arbitrary. Then if $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ ($a_j \in \mathbb{K}$), observe that

$$\operatorname{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha) = \sum_j \operatorname{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha_j)a_j,$$

exhibiting the column vector $(\operatorname{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha))$ as the product of the trace pairing matrix $(\operatorname{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha_j))$ with the vector (a_j). In light of Lemma 6.4, every entry appearing with $\operatorname{Tr}_{\mathbb{L}/\mathbb{K}}$ in the above equation is an element of A. Multiplying both sides by the adjugate of the trace pairing matrix, we see that $da_j \in A$ for all j, and $d\alpha \in A\alpha_1 + \cdots + A\alpha_n$, as required. ∎

A basis for B as an A-module is known as an ***integral basis***. By Proposition 6.1, every integral basis $\alpha_1, \ldots, \alpha_m$ is automatically a basis for $\mathbb{L}$ over $\mathbb{K}$, hence $m = n$. The following result gives us a sufficient condition for existence of A-bases.

Proposition 6.6. There exist free A-submodules M, M' of $\mathbb{L}$ such that $M \subseteq B \subseteq M'$. Therefore, B is a finitely generated A-module if A is Noetherian, and free of rank n if A is a principal ideal domain.

Proof. Pick a basis $x_1, \ldots, x_n$ of $\mathbb{L}$ over $\mathbb{K}$. Using Proposition 6.1, write $x_i = \beta_i/\alpha_i$ for $\beta_i \in B$ and nonzero $\alpha_i \in A$. Clearly the set of $x_i' = (\alpha_1\alpha_2\cdots\alpha_n)x_i \in B$ forms a basis of $\mathbb{L}/\mathbb{K}$ contained in B. So by Lemma 6.5 and Corollary 3.7, one has $dB \subseteq Ax_1 + \cdots + Ax_n$ for $d = \operatorname{disc}(x_1, \ldots, x_n) \neq 0$. Note that $Ax_1 + \cdots + Ax_n$ is a rank-n free module. In view of Theorem 2.5, we know that $dB \cong B$ is a free A-module with $\operatorname{rank} B \leq n$. But every integral basis has size n, i.e. $\operatorname{rank} B = n$. ∎

Proposition 6.7. If A is a Dedekind domain, then B is a Dedekind domain.

Proof. We immediately see that B is integrally closed by Corollaries 6.2 and 2.4. Next, suppose $\mathfrak{P}$ is a nonzero prime ideal of B. Then $\mathfrak{P} \cap A$, being the contraction of $\mathfrak{P}$, is a prime ideal of A. Pick a nonzero element $y \in \mathfrak{P}$. We can find a monic polynomial equation $y^r + a_{r-1}y^{r-1} + \cdots + a_0 = 0$ with $a_i \in A$ and $a_0 \neq 0$. Clearly $a_0 \in \mathfrak{P} \cap A$, so $\mathfrak{P} \cap A$ is a maximal ideal of A. ∎

7. Factorization in extensions

Within the "AKLB" setup of the previous section, let us investigate the splitting behavior of prime ideals in extensions. Suppose throughout that A is a Dedekind domain, meaning nonzero ideals factor uniquely in B by Theorem 4.10 and Proposition 6.7.

Definition 7.1. Let A be a Dedekind domain with field of fractions $\mathbb{K}$, and let B be the integral closure of A in a finite separable extension $\mathbb{L}$ of $\mathbb{K}$. If $\mathfrak{p}$ is a nonzero prime ideal in A, the extension of which decomposes as a product

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \quad e_i > 0$$

of distinct prime ideals $\mathfrak{P}_i$ in B, the exponents $e_1, \ldots, e_g$ are called the ***ramification indices***. For each i, the canonical map $A/\mathfrak{p} \to B/\mathfrak{P}_i$ is an embedding of fields, and the integer $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$ is called the ***inertia degree*** of $\mathfrak{P}_i$ over $\mathfrak{p}$; they are always finite, as we shall see in Theorem 7.2. When $g = n = [\mathbb{L} : \mathbb{K}]$, the prime ideal $\mathfrak{p}$ is ***totally split*** in $\mathbb{L}$, whereas if $g = 1$, it is said that $\mathfrak{p}$ is ***nonsplit*** in $\mathbb{L}$.

The prime ideal $\mathfrak{P}_i$ is ***unramified*** if $e_i = 1$ and if the extension $B/\mathfrak{P}_i$ is separable over $A/\mathfrak{p}$. If not, it is ***ramified***, and ***totally ramified*** if furthermore we have $f_i = 1$. We say that $\mathfrak{p}$ ***ramifies*** in $\mathbb{L}$ if at least one of the $\mathfrak{P}_i$ are ramified. Similarly, the extension $\mathbb{L}/\mathbb{K}$ itself is ***ramified*** if A has at least one prime ideal $\mathfrak{p}$ which ramifies, and so on and so forth.

Example. When $A = \mathbb{Z}$ and $\mathfrak{p} = (p)$ for some prime number p, we shall simply say that p ramifies in $\mathbb{L}$. This amounts to asserting that one of the ramification indices is > 1, because any algebraic extension of the finite field $\mathbb{Z}/(p)$ is separable by default. For instance, the prime 2 ramifies in $\mathbb{L} = \mathbb{Q}(i)$ because $(2) = (1+i)(1-i) = (1+i)^2$ in $\mathbb{Z}[i]$, the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$.

Let B/A be ring extension. Let $\mathfrak{p}$ and $\mathfrak{P}$ be prime ideals of A and B, respectively. If $\mathfrak{P} \cap A = \mathfrak{p}$, we shall say that $\mathfrak{P}$ ***lies over*** $\mathfrak{p}$. In the above definition, the prime factors $\mathfrak{P}_i$ of $\mathfrak{p}$ are precisely the prime ideals of B that lie over $\mathfrak{p}$: indeed, if $\mathfrak{P} \cap A = \mathfrak{p}$, then $\mathfrak{P}$ divides $\mathfrak{p}$ by Corollary 4.9. Conversely, the prime $\mathfrak{P}_i \cap A \subseteq A$ contains the maximal ideal $\mathfrak{p}$, so $\mathfrak{P}_i \cap A = \mathfrak{p}$.

Theorem 7.2 (Fundamental identity)**.** Let A be a Dedekind domain with field of fractions $\mathbb{K}$, let B be the integral closure of A in a finite separable extension $\mathbb{L}$ of $\mathbb{K}$, and let $\mathfrak{p}$ be a nonzero prime ideal in A. Suppose $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ ($e_i > 0$) is the decomposition of $\mathfrak{p}B$ into distinct prime ideals $\mathfrak{P}_i$ in B. Then $\dim_{A/\mathfrak{p}}(B/\mathfrak{P}_i^{e_i}) = e_i f_i$ and

$$\sum_{i=1}^{g} e_i f_i = n,$$

where $n = [\mathbb{L} : \mathbb{K}]$ and $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$.

Proof. Since the $\mathfrak{p}_i$ are coprime, so are their powers $\mathfrak{p}_i^{e_i}$. The Chinese remainder theorem gives us $B/\mathfrak{p}B \cong \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$. Regarding $B/\mathfrak{p}B$ and $B/\mathfrak{P}_i^{e_i}$ as vector spaces over $\kappa = A/\mathfrak{p}$, this means

$$\dim_\kappa(B/\mathfrak{p}B) = \sum_{i=1}^{g} \dim_\kappa(B/\mathfrak{P}_i^{e_i}).$$

Note that $m = \dim_\kappa(B/\mathfrak{p}B) < \infty$ because B is finitely generated as an A-module (Proposition 6.6). Let $\bar{\omega}_1, \ldots, \bar{\omega}_m$ be a basis for $B/\mathfrak{p}B$ over κ. We claim that $\omega_1, \ldots, \omega_m$ form an integral basis of B over A, and (hence) basis for $\mathbb{L}/\mathbb{K}$, from which the desired $\dim_\kappa(B/\mathfrak{p}B) = n$ directly follows. If there exist $a_1, \ldots, a_m \in A$, not all zero, such that $a_1\omega_1 + \cdots + a_m\omega_m = 0$, then consider the nonzero ideal $\mathfrak{a} = (a_1, \ldots, a_m)$ of A. Pick an element $a \in \mathfrak{a}^{-1} \setminus \mathfrak{a}^{-1}\mathfrak{p}$. The elements $aa_1, \ldots, aa_m$ lie in A but do not all belong to $\mathfrak{p}$. We arrive at a nontrivial linear dependence relation $aa_1\omega_1 + \cdots + aa_m\omega_m \equiv 0 \bmod \mathfrak{p}$ among the $\bar{\omega}_1, \ldots, \bar{\omega}_m$, which gives a contradiction. Now define the A-submodule $N = A\omega_1 + \cdots + A\omega_m$ of B. Since $\bar{\omega}_1, \ldots, \bar{\omega}$ generate $B/\mathfrak{p}B$ over κ, B is the sum of submodules N and $\mathfrak{p}B$, which means $B/N = (N + \mathfrak{p}B)/N = \mathfrak{p}(B/N)$. Recall that B is a finitely generated A-module (Proposition 6.6), and so is B/N. By the determinant trick [AM69, Corollary 2.5], there exists some $x \equiv 1 \pmod{\mathfrak{p}}$ with $x(B/N) = 0$; in other words, $xB \subseteq N = A\omega_1 + \cdots + A\omega_m$. Clearly $x \neq 0$. Therefore, in light of Proposition 6.1, one has $\mathbb{L} = x\mathbb{L} = \mathbb{K}\omega_1 + \cdots + \mathbb{K}\omega_m$.
It remains to prove $\dim_\kappa(B/\mathfrak{P}_i^{e_i}) = e_i f_i$. For each r, we view the B-module $\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}$ as a vector space over $B/\mathfrak{P}_i$. Any proper subspace of $\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}$ would correspond to an ideal of B that is strictly contained between $\mathfrak{P}_i^r$ and $\mathfrak{P}_i^{r+1}$, of which there are none. Hence $\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}$ has dimension 1 over $B/\mathfrak{P}_i$ and dimension $f_i = [B/\mathfrak{P}_i : A/\kappa]$ over κ. Since $\mathfrak{P}^r/\mathfrak{P}^{e_i}$ is a κ-subspace of $B/\mathfrak{P}^{e_i}$ for each $r \leq e_i$, we have the following descending chain

$$B/\mathfrak{P}^{e_i} \supseteq \mathfrak{P}/\mathfrak{P}^{e_i} \supseteq \cdots \supseteq \mathfrak{P}^{e_i-1}/\mathfrak{P}^{e_i} \supseteq 0.$$

of κ-vector spaces. Finally, as the successive quotients are isomorphic to $\mathfrak{P}^r/\mathfrak{P}^{r+1}$, one has

$$\dim_\kappa(B/\mathfrak{P}^{e_i}) = \sum_{r=0}^{e_i-1} (\dim_\kappa(\mathfrak{P}^r/\mathfrak{P}^{e_i}) - \dim_\kappa(\mathfrak{P}^{r+1}/\mathfrak{P}^{e_i})) = \sum_{r=0}^{e_i-1} \dim_\kappa(\mathfrak{P}^r/\mathfrak{P}^{r+1}) = e_i f_i.$$

■

Proposition 7.3. Let $\mathfrak{p}$ be a prime ideal of A, and $\mathfrak{P}$ a prime ideal lying over $\mathfrak{p}$ with ramification index e. Then $v_{\mathfrak{P}}(x) = e v_{\mathfrak{p}}(x)$ for all $x \in \mathbb{K}$.

Proof. If π is a uniformizer of $A_{\mathfrak{p}}$, let us write $x = \pi^k u$ for some unit $u \in A_{\mathfrak{p}}$, so that $k = v_{\mathfrak{p}}(x)$ by definition. ∎

8. Hilbert's ramification theory

The notation of this section will be the same as that of the previous, with the additional assumption that $\mathbb{L}/\mathbb{K}$ is a Galois extension. Let $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ be the Galois group of $\mathbb{L}/\mathbb{K}$. In this case, we have $|G| = n = [\mathbb{L} : \mathbb{K}]$.
Observe that $\sigma B = B$ for any $\sigma \in G$, because the conjugate σx of an integral element $x \in B$ also satisfies the same equation of integrality; this shows $\sigma B \subseteq B$, and symmetrically $\sigma^{-1} B \subseteq B$. Let $\mathfrak{P}$ be a prime ideal of B over $\mathfrak{p}$, a nonzero prime of A. Then $\sigma\mathfrak{P} \cap A = \sigma(\mathfrak{P} \cap A) = \sigma(\mathfrak{p}) = \mathfrak{p}$ for every $\sigma \in G$, so the image $\sigma\mathfrak{P} \subseteq \sigma B = B$ is another prime ideal of B over p. That is to say, we have a group action of G on the set of prime ideals over $\mathfrak{p}$. The prime ideals $\sigma\mathfrak{P}$ in the orbit of $\mathfrak{P}$ are said to be the ***conjugates*** of $\mathfrak{P}$. So far, that $\mathbb{L}/\mathbb{K}$ is Galois has not been used, but the following relies on this hypothesis to prove the group action in question is transitive:

Proposition 8.1. The prime ideals of B over $\mathfrak{p}$ are conjugates of each other. Put another way, the orbit of each $\mathfrak{P}$ over $\mathfrak{p}$ is the entire set of prime ideals over $\mathfrak{p}$.

Proof. Let $\mathfrak{P}, \mathfrak{P}'$ be two such prime ideals. Assume, for sake of contradiction, that $\sigma\mathfrak{P} \neq \mathfrak{P}'$ for any $\sigma \in G$. The Chinese remainder theorem says there is an $x \in B$ with $x \equiv 0 \pmod{\mathfrak{P}'}$ and $x \equiv 1 \pmod{\sigma\mathfrak{P}}$ for every $\sigma \in G$. From Proposition 3.4, we know that $N_{\mathbb{L}/\mathbb{K}}(x) = \prod_{\sigma \in G} \sigma x$ is a multiple of x (each σx lies in B). This, combined with Lemma 6.4, tells us $N_{\mathbb{L}/\mathbb{K}}(x) \in \mathfrak{P}' \cap A = \mathfrak{p} \subseteq \mathfrak{P}$. However, $\sigma x \notin \mathfrak{P}$ for any $\sigma \in G$, so $N_{\mathbb{L}/\mathbb{K}}(x) \notin \mathfrak{P}$. ∎

In the Galois case, the fundamental identity becomes considerably simpler.

Theorem 8.2 (efg Theorem)**.** As in Theorem 7.2, let $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ be the prime factorization of a nonzero prime ideal $\mathfrak{p}$ of A. If the extension $\mathbb{L}/\mathbb{K}$ is Galois, the ramification indices $e_1 = \cdots = e_g = e$ are equal, and likewise for the inertia degrees $f_1 = \cdots = f_g = f$. In this case, the fundamental identity reads

$$n = efg.$$

Definition 8.3. Let $\mathfrak{P}$ be a prime ideal of B. The subgroup $D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ is called the ***decomposition group*** of $\mathfrak{P}$ over $\mathbb{K}$. The fixed field $Z_{\mathfrak{P}} = \mathbb{L}^{D_{\mathfrak{P}}} = \{x \in \mathbb{L} \mid \sigma x = x \text{ for all } \sigma \in D_{\mathfrak{p}}\}$ of $D_{\mathfrak{P}}$ is called the ***decomposition field*** of $\mathfrak{P}$ over $\mathbb{K}$.

Henceforth, we write $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ and $\kappa(\mathfrak{P}) = B/\mathfrak{P}$.

Proposition 8.4. The extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is normal.

Proof. Let $\bar{x} \in \kappa(\mathfrak{P})$, and let $g(X)$ be the minimal polynomial of $\bar{x}$ over $\kappa(\mathfrak{p})$. Denote by $f(X)$ the minimal polynomial of $x \in B$ over $\mathbb{K}$. Note that $f(X)$ takes coefficients in A, by Proposition 6.3. ∎

Proposition 8.5. If $\mathfrak{P}$ is a prime ideal of B, each $\sigma \in D_{\mathfrak{P}}$ induces an automorphism $\bar{\sigma}$ on $\kappa(\mathfrak{P})$ by $x \bmod \mathfrak{P} \mapsto \sigma x \bmod \mathfrak{P}$. This defines a surjective group homomorphism $D_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$.

Definition 8.6. Let $\mathfrak{P} \subseteq B$ be a prime ideal lying over $\mathfrak{p}$. The kernel $I_{\mathfrak{P}} \subseteq D_{\mathfrak{P}}$ of the homomorphism $D_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is called the ***inertia group*** of $\mathfrak{P}$ over K.

9. Higher ramification groups

Proposition 9.1. The group $I_{\mathfrak{P}}/V_1$ is isomorphic to a subgroup of $\kappa(\mathfrak{p})^{\times}$.

Lemma 9.2. The ramification groups V_i are normal subgroups of $D_{\mathfrak{P}}$, and form a descending chain: $V_0 \trianglerighteq V_1 \trianglerighteq V_2 \ldots$

10. Rings of integers

Definition 10.1. An algebraic number field K is a finite extension field of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in an algebraic number field K is called the ring of integers $\mathcal{O}_K$ of K.

The ring of integers $\mathcal{O}_K$ of an algebraic number field K is a Dedekind domain by Proposition 6.7.

Lemma 10.2. Let K be an algebraic number field, and let $\alpha_1, \ldots, \alpha_n$ be an integral basis for $\mathcal{O}_K$ over $\mathbb{Z}$. Then for any prime number p, the residues $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ are a basis for $\mathcal{O}_K/p\mathcal{O}_K$ over $\mathbb{Z}/(p)$ satisfying

$$\operatorname{disc}(\bar{\alpha}_1, \ldots, \bar{\alpha}_n) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) \pmod{p}.$$

Proof. If one has a linear dependence $\bar{a}_1\bar{\alpha}_1 + \cdots + \bar{a}_n\bar{\alpha}_n = 0$ ($a_i \in \mathbb{Z}$) among the $\bar{\alpha}_i$, then $a_1\alpha_1 + \cdots + a_n\alpha_n \in p\mathcal{O}_K$. This means $a_i \in p\mathbb{Z}$ and $\bar{a}_i = 0$ for each i. Now for any $x \in \mathcal{O}_K$, the matrix for multiplication by x (with respect to the basis $\alpha_1, \ldots, \alpha_n$) reduces modulo p to the multiplication matrix for $\bar{x}$ on $\mathcal{O}_K/p\mathcal{O}_K$ (with respect to $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$). It follows that $\operatorname{Tr}(\bar{x}) = \operatorname{Tr}(x) \pmod{p}$ for all $x \in \mathcal{O}_K$. Taking determinants of the trace pairing matrices gives the desired. ∎

Lemma 10.3. Let A be a ring. If B_1, B_2 are ring extensions of A that are finite free A-modules. Choosing bases $\{e_i\}$ and $\{f_j\}$ for B_1 and B_2, respectively, the basis $e_1, \ldots, e_n, f_1, \ldots, f_m$ of $B_1 \times B_2$ satisfies

$$\operatorname{disc}(e_1, \ldots, e_n, f_1, \ldots, f_m) = \operatorname{disc}(e_1, \ldots, e_n) \operatorname{disc}(f_1, \ldots, f_m).$$

A fortiori, the discriminant of $(B_1 \times B_2)/A$ vanishes if and only if one of $\operatorname{disc}(B_1/A)$, $\operatorname{disc}(B_2/A)$ equals zero (this condition is independent of which basis we choose).

Proof. For any $x \in B_1$, multiplication by x on $B_1 \times B_2$ kills the second component and acts on the first component the same way x multiplies on B_1. Writing out the multiplication matrix for x on $B_1 \times B_2$ in terms of $e_1, \ldots, e_n, f_1, \ldots, f_m$, one can see that $\operatorname{Tr}_{(B_1\times B_2)/A}(x) = \operatorname{Tr}_{B_1/A}(x)$ for all $x \in B_1$. Likewise, $\operatorname{Tr}_{(B_1\times B_2)/A}(x) = \operatorname{Tr}_{B_2/A}(x)$ for all $x \in B_2$. Since $e_i f_j = 0$ in $B_1 \times B_2$, we calculate the trace pairing matrix for $e_1, \ldots, e_n, f_1, \ldots, f_m$:

$$\begin{pmatrix} (\operatorname{Tr}_{B_1\times B_2}(e_i e_k)) & 0 \\ 0 & (\operatorname{Tr}_{B_1\times B_2}(f_j f_\ell)) \end{pmatrix} = \begin{pmatrix} (\operatorname{Tr}_{B_1/A}(e_i e_k)) & 0 \\ 0 & (\operatorname{Tr}_{B_2/A}(f_j f_\ell)) \end{pmatrix}$$

(writing $\operatorname{Tr}_{B_1\times B_2}$ instead of $\operatorname{Tr}_{(B_1\times B_2)/A}$ to simplify notation). Now take determinants. ∎

An elegant theorem of Dedekind classifies precisely which primes ramify in a number field.

Theorem 10.4 (Dedekind)**.** Let p be a prime number and K an algebraic number field. Then p ramifies in K if and only if p divides the integer $\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$.

Proof. Say $(p) = p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ in $\mathcal{O}_K$, so that, by the Chinese remainder theorem, $\mathcal{O}/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{P}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{P}_g^{e_g}$. Each factor $\mathcal{O}_K/\mathfrak{P}_i^{e_i}$ is a ring extension of $\mathbb{Z}/p\mathbb{Z}$, and a finite dimension $\mathbb{Z}/p\mathbb{Z}$-vector space (this is covered in Theorem 7.2). Combining the previous two lemmas, one sees that $p|\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$ if and only if $\operatorname{disc}((\mathcal{O}_K/p\mathcal{O}_K)/(\mathbb{Z}/p\mathbb{Z})) = 0$ in $\mathbb{Z}/p\mathbb{Z}$, which is equivalent to one of the $\operatorname{disc}((\mathcal{O}_K/\mathfrak{P}_i^{e_i})/(\mathbb{Z}/p\mathbb{Z}))$ vanishing. We finish off the proof with one additional lemma. ∎

Lemma 10.5. Let p be a prime number, K an algebraic number field, and $\mathfrak{P} \subseteq \mathcal{O}_K$ a prime which lies over p with ramification index e. Then $\operatorname{disc}((\mathcal{O}_K/\mathfrak{P}^e)/(\mathbb{Z}/p\mathbb{Z})) = 0$ if and only if $e > 1$.

Proof. If $e = 1$, then $\mathcal{O}_K/\mathfrak{P}^e = \mathcal{O}_K/\mathfrak{P}$ is a finite extension of the finite field $\mathbb{Z}/p\mathbb{Z}$, so its discriminant is nonzero by Corollary 3.7. Suppose $e > 1$, and take an element $x \in \mathfrak{P} - \mathfrak{P}^e$; this is possible because $\mathfrak{P}$ is invertible in the Dedekind domain $\mathcal{O}_K$. Note that $\bar{x}$ is nonzero nilpotent in $\mathcal{O}_K/\mathfrak{P}^e$. We can extend the linearly independent subset $\{\bar{x}\}$ to a $\mathbb{Z}/p\mathbb{Z}$-basis $\{\bar{x}_1, \ldots, \bar{x}_r\}$ of $\mathcal{O}_K/\mathfrak{P}^e$ with $x_1 = x$. The first column of the trace pairing matrix for this basis consists of the values $\operatorname{Tr}(x_i x)$. But since $x_i x$ is nilpotent, the corresponding multiplication map on $\mathcal{O}_K/\mathfrak{P}^e$ is nilpotent and all its eigenvalues are zero. The trace of $x_i x$ is just the sum of those eigenvalues. Therefore, the entire first column dies, and so $\operatorname{disc}(\bar{x}_1, \ldots, \bar{x}_r) = 0$ in $\mathbb{Z}/p\mathbb{Z}$. ∎

11. Ramification in $\mathbb{Q}(\zeta_p)$

Cyclotomic fields were defined in Section 2. We now investigate their properties more closely. The first objective of this section is to explicitly describe the ring of integers B of $\mathbb{Q}(\zeta_n)$, which proves to be rather nontrivial. Proofs in the literature examine the case when n is a prime power, before deducing the general theorem. Following [], we shall instead opt for a less standard approach.
Certainly $\zeta_n \in B$ itself is integral over $\mathbb{Z}$, so $\mathbb{Z}[\zeta_n]$ is contained in B. Our claim is that $\mathbb{Z}[\zeta_n] = B$. Observe that $\mathrm{Frac}(\mathbb{Z}[\zeta_n]) = \mathbb{Q}(\zeta_n)$: the inclusion $\mathbb{Z}[\zeta_n] \hookrightarrow \mathbb{Q}(\zeta_n)$ extends to an embedding of its field of fractions $\mathrm{Frac}(\mathbb{Z}[\zeta_n])$ into $\mathbb{Q}(\zeta_n)$, by the relevant universal property. Since $\mathrm{Frac}(\mathbb{Z}[\zeta_n]) \supseteq \mathbb{Z}$ is a field, it contains $\mathbb{Q}$; whence $\mathrm{Frac}(\mathbb{Z}[\zeta_n]) \supseteq \mathbb{Q}(\zeta_n)$. It therefore is enough to prove that $\mathbb{Z}[\zeta_n]$ is integrally closed.

Lemma 11.1. Let A be a local integral domain with field of fractions $\mathbb{K}$. Then a nonzero fractional ideal $\mathfrak{a}$ of A is invertible if and only if $\mathfrak{a}$ is principal.

Proof. Suppose $\mathfrak{a}$ is invertible; that is, there exists a fractional $\mathfrak{b}$ of A such that $\mathfrak{ab} = 1$, yielding an equation $a_1b_1 + \cdots + a_mb_m = 1$ for $a_i \in \mathfrak{a}, b_i \in \mathfrak{b}$. Each element a_ib_i lies in A, so one of these products (say, a_1b_1) does not belong to the maximal ideal $\mathfrak{m}$ of the local ring A. This means a_1b_1 is a unit. Every element $x \in \mathfrak{a}$ can be exhibited as an element $x = a_1(xb_1)(a_1b_1)^{-1}$ of Aa_1 (since $xb_1 \in A$). Hence the fractional ideal $\mathfrak{a}$ is generated by a_1. ∎

Notation. For a polynomial $f(X) \in \mathbb{Z}[X]$, the image of $f(X)$ under the homomorphism $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ which reduces coefficients modulo p will be written as $f(X) \bmod p$.

Lemma 11.2. Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Z}$ with minimal polynomial $f(X)$ over $\mathbb{Q}$. For every maximal ideal $\mathfrak{m}$ of $\mathbb{Z}[\alpha]$, there exists a prime number p and a polynomial $g(X)$ in $\mathbb{Z}[X]$ such that $g(X) \bmod p$ is an irreducible factor of $f(X) \bmod p$, and $\mathfrak{m} = (p, g(\alpha))$ divides the principal ideal $(p) = p\mathbb{Z}[\alpha]$.

Reducing the coefficients of $f(X) \in \mathbb{Z}[X]$ modulo p makes sense by Proposition 6.3.

Proof. Every nonzero ideal of $\mathbb{Z}[\alpha]$, including $\mathfrak{m}$, contains a nonzero rational integer: indeed, if we pick an element $x \neq 0$ of the ideal, the minimal polynomial of x over $\mathbb{Q}$ has a nonzero constant term. Multiply out by a common denominator of the coefficients to obtain a constant term in $\mathbb{Z}$ contained in the ideal. Hence $\mathfrak{m} \cap \mathbb{Z}$ is a nonzero prime ideal of $\mathbb{Z}$, necessarily of the form $p\mathbb{Z}$ for a certain prime p.
The evaluation map $\mathbb{Z}[X] \to \mathbb{Z}[\alpha]$ (which has kernel $f(X)$ by the division algorithm in $\mathbb{Z}[X]$) descends to an isomorphism $\mathbb{Z}[X]/(f(X)) \cong \mathbb{Z}[\alpha]$. Whence, we identify $\mathbb{Z}[\alpha]/(p)$ The key now is to $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$ with $\mathbb{F}_p[X]/(f(X) \bmod p)$. ∎

Lemma 11.3. For each maximal ideal $\mathfrak{m}$ of $\mathbb{Z}[\zeta_n]$, the unique maximal ideal of $(\mathbb{Z}[\zeta_n])_{\mathfrak{m}}$ is principal.

Theorem 11.4. The ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.

Proof. In view of Lemma ∎

Theorem 11.5. Let p be a prime. Then $(p) = \mathfrak{P}^{p-1}$ in $\mathbb{Z}[\zeta_p]$, where $\mathfrak{P} = (1 - \zeta_p)$ is a prime ideal. When p is odd, $\mathfrak{P}$ is totally ramified.

Proof. Assume p is an odd prime. One has $p = \prod_i (1-\zeta_p^i)$ as a special case of Lemma 2.26. Consider $u_i = (1 - \zeta_p^i)/(1 - \zeta_p) = 1 + \zeta_p + \cdots + \zeta_p^{i-1}$, which we claim is a unit in $\mathbb{Z}[\zeta_p]$. Indeed, pick j such that $ij \equiv 1 \pmod p$. Then $u_i^{-1} = (1-\zeta_p^{ij})/(1-\zeta_p^i) \in \mathbb{Z}[\zeta_p]$. Since $p = \prod(1-\zeta_p^i) = (1-\zeta_p)^{p-1} \prod u_i$, we conclude that $(p) = (1-\zeta_p)^{p-1}$. On the other hand, $efg = p-1$ from the fundamental identity in the Galois case. This means $\mathfrak{P} = (1-\zeta_p)$ cannot decompose further, and must be prime. Hence $e = p - 1 > 1$ and $f = 1$.
Now if $p = 2$, then $\mathbb{Q}(\zeta_2) = \mathbb{Q}(-1) = \mathbb{Q}$, so trivially $(p) = \mathfrak{P}$. ∎

Proposition 11.6. If p is an odd prime, the discriminant of $K = \mathbb{Q}(\zeta_p)$ is $\Delta_K = (-1)^{(p-1)/2}p^{p-2}$. In particular, p is the only prime which ramifies in $\mathbb{Q}(\zeta_p)$.

Proof. Via Theorem 10.4, the second claim is immediate from the first. The ring of integers $\mathbb{Z}[\zeta_p]$ of K admits a $\mathbb{Z}$-basis $1, \zeta_p, \ldots, \zeta_p^{p-2}$. If $\sigma_1, \ldots, \sigma_{p-1}$ are the $\mathbb{Q}$-embeddings of $\mathbb{Q}(\zeta_p)$ into a fixed algebraic closure $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, the conjugates $\{\sigma_i\zeta_p\}$ are precisely the powers $\zeta_p, \ldots, \zeta_p^{p-1}$ (the roots of the minimal polynomial $\Phi_p(X) \in \mathbb{Q}[x]$ of ζ_p). Proposition 3.6 says that

$$\Delta_K = \operatorname{disc}(1, \zeta_p, \ldots, \zeta_p^{p-1}) = \prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j).$$

Since $X^p - 1 = \prod_{j=0}^{p-1}(X - \zeta_p^j)$, substituting $X = 0$ gives the auxiliary identity

$$(-1)^{p-1} = \prod_{j=0}^{p-1} \zeta_p^j.$$

Differentiating both sides of $X^p - 1 = \prod_{j=0}^{p-1}(X - \zeta_p^j)$ and substituting $X = \zeta_p^i$, then multiplying over all such i gives

$$p^p(-1)^{(p-1)^2} = \prod_{i,j=0,\, i \ne j}^{p-1} (\zeta_p^i - \zeta_p^j).$$

After some algebra, we see that $\Delta_K = (-1)^{(p-1)/2}p^{p-2}$. ∎

12. A series of lemmast

Lemma 12.1. Let $K/\mathbb{Q}$ be a finite Galois extension. If a prime number p is the only prime that ramifies in K, then p is totally ramified.

Lemma 12.2. Let p be a prime and let $K/\mathbb{Q}$ be a finite p-power abelian extension such that no prime other than p ramifies in K. Then $K/\mathbb{Q}$ is cyclic.

Lemma 12.3. Let p be an odd prime, and let $K/\mathbb{Q}$ be an extension of degree p such that no prime other than p ramifies. Then the second ramification group V_2 is trivial.

13. A twofold reduction

Theorem 13.1 (Kronecker-Weber)**.** Every finite abelian extension of $\mathbb{Q}$ is contained within a cyclotomic field $\mathbb{Q}(\zeta_n)$.

Lemma 13.2. It suffices to show Theorem 13.1 for cyclic extensions $K/\mathbb{Q}$ of prime-power degree.

Proof. Suppose $K/\mathbb{Q}$ is finite abelian. Then $\operatorname{Gal}(K/\mathbb{Q})$ decomposes into a direct product of cyclic groups $G_1, \ldots, G_r$ of prime-power degree. If K_i is the fixed field of $\prod_{j \ne i} G_j$, then $K_i \subseteq \mathbb{Q}(\zeta_{n_i})$ for some n_i. Setting $n = n_1 \cdots n_r$ yields

$$K = K_1 \cdots K_r \subseteq \mathbb{Q}(\zeta_n),$$

∎

Lemma 13.3. It suffices to show Theorem 13.1 is true for cyclic extensions $K/\mathbb{Q}$ of prime-power degree p^m such that p is the only prime that ramifies in K.

14. The final ascent

Acknowledgments

I would like to thank Simon Rubinstein-Salzedo for directing the Euler Circle institute and suggesting the topic of this paper. I am also especially grateful to Ryan Catullo for insightful conversations and continuous mentorship. Much thanks goes out to Woong Choi, Owen Jiang, and Jihan Lee for their helpful feedback.

References

[AM69] Michael Francis Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley-Longman, 1969. URL: http://math.univ-lyon1.fr/~mathieu/CoursM2-2020/AMD-ComAlg.pdf, doi:10.2307/2316241.

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Chichester: Wiley, third edition, 2004.

[Kna16] Anthony W. Knapp. *Basic Algebra*. Second edition, 2016. URL: https://www.math.stonybrook.edu/~aknapp/download/b2-alg-inside.pdf.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer Berlin, Heidelberg, first edition, 1999. URL: https://web.math.ucsb.edu/~agboola/teaching/2021/fall/225A/neukirch.pdf, doi:10.1007/978-3-662-03983-0.