Algebraic number fields

by

Benjamín Macías Quezada

2025
Santiago, Chile

Acknowledgments

Índice

1. Algebraic number fields

Part of this section's exposition is adapted from the author's undergrduate dissertation.

By the 1840s, Fermat's Last Theorem had already become embedded within the folklore of Number Theory, and although many top mathematicians had attempted to solve this problem, some with success in particular cases, a complete proof had yet to be found. A particularly eventful period surrounding the problem was March of 1847, as recalled by Edwards in [10, §4.1]. On March 1st, Gabriel Lamé announced a proof (in [21]) that turned out to be wrong. While we do not go into details of the article, we do cover the main idea and error of his proof. For a modern summary, see Runyeon in [24, p. 1].

Lamé tried to generalize some algebraic factorization tricks used for small n in correct proofs. For example, for $n = 3$ the identity used was $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$. For general n, this can be done by introducing an n-th root of unity, that is, an $r \in \mathbb{C}$ such that $r^n = 1$, which allows for the identity

$$x^n + y^n = (x + y)(x + ry)(x + r^2y) \ldots (x + r^{n-1}y) = z^n \tag{1.1}$$

when n is odd (it is enough to consider n prime, so this does not post an issue). He then claims that the factors of Equation 1.1 are coprime, which allows for a series of contradictions, concluding the proof.

Joseph Liouville commented on the argument's reliance on a questionable unique factorization assumption in a note at the end of Lamé's proof. The recollection of Edwards in [10, p. 77] of Liouville's critique of Lamé's attempt is quite harsh, so we offer a raw translation of the original passage instead:

> In the communication he has just made to the Academy, Mr. Lamé kindly declared that he followed an idea I had previously shared with him: that of introducing complex numbers derived from the binomial equation $r^n - 1 = 0$ into the theory of the equation $x^n - y^n = z^n$, to try to conclude the impossibility of this latter equation, either in ordinary integers or even in complex numbers of the indicated form. Such an idea is not new in itself and must have naturally presented itself to geometers from the form of the binomial $x^n - y^n$. Moreover, I have not deduced any satisfactory demonstration from it, and, to tell the truth, I have never even seriously occupied myself with the equation $x^n - y^n = z^n$. However, some attempts led me to believe that one should first seek to establish, for the new complex numbers, a theorem analogous to the elementary proposition for ordinary integers, that a product can only be decomposed into prime factors in one way. Mr. Lamé's analysis confirms this feeling in me; it seems to need the theorem I mentioned: and yet I do not see that our colleague has gone into the details that the subject seems to require. Is there not a gap to be filled here? I submit this observation to our colleague, while expressing the firm hope that he will overcome all

> the difficulties, and that he will achieve a new and more brilliant triumph in this thorny question in which he has already so distinguished himself. I will recall, in conclusion, that since Mr. Gauß, and even since Euler and Lagrange, geometers have often dealt with complex numbers. Volume XVII of our Memoirs contains a great work by Mr. Cauchy, where those of these numbers related to the equation $r^n - 1 = 0$ play an important role. But for the specific point I mentioned earlier, it is especially in an article by Mr. Jacobi (*Journal de Mathématiques*, volume VIII, page 268) that one can find useful information (Liouville on Lamé, in [21, p. 315–6], translated by the author).

The issue Liouville picked up on was that in Equation 1.1, it is not obvious that the factors are coprime, or what would even mean for said factors to be so. After Liouville, it was Augustin-Louis Cauchy who took the floor to declare his interest on the problem, which was also recorded, so we may offer a translation:

> Following the lecture given by Mr. Lamé, Mr. Cauchy also spoke and recalled a Memoir he presented to the Academy in a previous session (October 19, 1846), which was initialed at that time by one of the permanent secretaries. In this Memoir, Mr. Cauchy presented a method and formulas that were, in part, related to the theory of numbers and which seemed to him to potentially lead to the demonstration of Fermat's Last Theorem. Distracted by other work, Mr. Cauchy did not have the time to ascertain if this conjecture was founded. Moreover, the method in question was very different from that which Mr. Lamé appears to have followed, and it may become the subject of a new article (Cauchy on Lamé, in [21, p. 316], translated by the author).

Note that the product Equation 1.1 is, at the end of the day, of the form

$$a_0 + a_1 r + \cdots + a_{n-1} r^{n-1} \text{ with } a_j \in \mathbb{Z},$$

and we recognize these numbers as the ring $\mathbb{Z}[r]$ of cyclotomic integers of order n, for r is an n-th root of unity. Thus, the focus was shifted to investigating unique factorization in these cyclotomic rings. Moreover, as Edwards tells in [10, p. 78], the meeting was followed by a sort of race between Lamé and Cauchy to obtain an actual proof that lasted for several weeks, in which they deposited "secret packages" at the Academy (as proof of ownership of ideas), and published a series of "annoyingly vague, incomplete, and inconclusive" notices regarding the problem of unique factorization. We will not examine these papers, for they were not fruitful.

This exhibition was put to rest on May 24, when Ernst Kummer sent a letter to Liouville pointing out that he had already published the paper [19] in 1847 (originally from 1844, albeit in an obscure journal) which contained an example of a cyclotomic ring in which unique factorization failed. In the same letter, he also claimed that unique factorization “could be saved” through the theory of *ideal complex numbers* he had been developing in the recent time.

A common misconception—that I admit I’ve held myself—is that Kummer’s interest on unique factorization was motivated by Fermat’s Last Theorem, but Edwards argues in [10, pp. 79–80] with strong evidence that in fact his main concern was with higher reciprocity laws, inspired directly by the work of Carl Jacobi. We will not try to summarize this work of Kummer, but the curious reader may check upon the perhaps most systematic exposition available, that of Edwards in [10, §4]. Also there is memoir, published by Kummer in 1851 in French, that goes over a rather polished version of his theory (cf. [20]) which we may ocasionally refer to.

John Stilwell regards the *Vorlesungen über Zahlentheorie* by Lejeune Dirichlet and Richard Dedekind as one of the most influential mathematics books of the 19th century ([8, p. xi]), for it works as a transition from the “classic” number theory of Gauß to a more “modern” one (the likes of David Hilbert, for instance). Its merit lies primarily in that it extensively reflects the state of the art of Number Theory up to the 1840s, successfully covering the bulk of the famous *Disquisitiones Arithmeticae* ([12]) making it “understandable to ordinary mortals” ([8, p. xi]), and that ater that it threads on the frontiers of the knowledge of the time.

The original *Vorlesungen* ([7]) consisted of the 1856–7 Göttingen lectures by Dirichlet, and nine appendices containing posthumous results by Dirichlet, all compiled, written, and published by Dedekind in the year 1863. Later on, inspired by the previously discussed work of Kummer, Dedekind developed his own theory of ideals with the goal of reformulating and expanding its scope. He decided to divulgate his work as appendices to new editions of the *Vorlesungen* that he published from 1871 onward, because he had thought that “that was the surest means of gaining a larger circle of mathematicians for the cultivation of [the] field” ([9, pp. 349–50] on Dedekind), but correspondence from Dedekind indicates that the reception was nothing but dissapointing, at least from his point of view (again, see [9, p. 349]). Edwards argues that this is not particularly surpising:

> “The location of this sophisticate, demanding, and highly original material as the very last item in a book which is for the most part an expository and rather elementary account of classical number theory might be expected to have a discouraging effect. Inexpert readers would probably not get to the end of the book, and experts would probably not expect to find important new material in such a place and therefore would not look” (Edwards in [9, p. 349]).

For Dedekind, the reason for the lackluster reception was due to “the exaggerated brevity and conciseness” (Edwards’ translation of Dedekind, in [9, p. 349]) of his exposition, which led him to develop an even more extensive approach in following editions.

There are four total iterations of Dedekind’s theory of ideals, three of which appeared on the 1871, 1879, 1894 editions of the *Vorlesungen*, and one in the

Bulletin des Sciences Mathématiques et Astronomiques in [2]. We will now do a swift review of the theory of Dedekind, based on the 1876–7 version, which is in French, but has an English translation by John Stilwell available in [5]. We've taken this decision because while the results and concepts introduced are virtually the same in all versions, the exposition of the later is more akin to a contemporary one in language. Ocasionally, we may touch upon the 1871 version, for which there is a transition into English by Jeremy Avigad in [1].

The original concepts introduced by Dedekind are that of *abelian groups*, *number fields*, *algebraic integer rings*, and their *ideals*, while the most relevant theorems are the ones that settle unique factorization into prime ideals, and the finitude of the ideal class numbers. The terminology he employs is quite dated, but we will write everything in modern language. It is not our intention to re-do every proof of every result available from Dedekind, for this has been done several times in the almost 150 years that have passed since—in fact, we will assume the reader is already familiar with most concepts from Abstract Algebra that appeared for the first time in the *Vorlesungen*. We will offer modern references for most results, and we will opt to include proofs only if we are unable to provide such reference, or if there is value in actually re-writting it.

1.1. Algebraic numbers

In [2, §13–17], Dedekind establishes the foundations for the study of what we now call *algebraic extensions of* $\mathbb{Q}$, which later developed into modern *field theory*. While at that time these ideas were certainly a novelty, nowadays they are covered in any standard undegradute Algebra course, so we will just mention them rather unceremoniously, but always keeping in mind that he was the first to coin them. He defines several concepts, such as *algebraic numbers* (over $\mathbb{Q}$), the *minimal polynomial* of an algebraic number, the field[1] generated[2] by an algebraic number, and the *degree* of a field extension. Given an algebraic number θ over $\mathbb{Q}$ with minimal polynomial of degree n, one may consider the field $\mathbb{Q}[\theta]$, which will also have degree n, for the set $1, \theta, \theta^2, \ldots, \theta^{n-1}$ forms a $\mathbb{Q}$-basis of $\mathbb{Q}[\theta]$.

Dedekind also introduced the notion of *field isomorphisms* and of *conjugate elements*, and proved that when considering an element $\omega \in K/\mathbb{Q}$, all of the roots of the minimal polynomial of ω are conjugates of ω (hence of eachother). He writes $N(\omega)$ for the product[3] of all said conjugates, and calls it—somewhat arbitrarially—the *norm* of ω. To our impression, this norm is just a way to bundle up all these conjugates in a way that is invariant under conjugation.

[1] He actually introduced the notion of fields, but uses the word *Körper*, which should be translated as *body*. This nomenclature is not used in English.

[2] Recall that given field extension $E/\mathbb{Q}$ and $\theta \in E$ we may consider two algebraic objects: the $\mathbb{Q}$-algebra $\mathbb{Q}[\theta]$ of polynomial expressions in θ with coefficients in $\mathbb{Q}$, and $\mathbb{Q}(\theta)$, the *field over* $\mathbb{Q}$ *generated* by θ, which allows for division by θ. The algebra $\mathbb{Q}[\theta]$ is a field (equal to $\mathbb{Q}(\theta)$ actually) if and only if θ is algebraic (over $\mathbb{Q}$).

[3] This is ill-defined: this product only makes sense when all the conjugate fields involved are all embedded within one bigger field (possible an algebraic clousure of $\mathbb{Q}$).

Bear in mind that Dedekind considers only the case of extensions of $\mathbb{Q}$ of finite degree, generated by a single algebraic element, case in which the degree of the extension coincides with the degree of the minimal polynomial (over $\mathbb{Q}$) of said generator (i.e., the extension is separable). The study object of this first chapter are these finite extensions of $\mathbb{Q}$, which are now called generically *number fields*.

One of Dedekind's earliest concepts that did not become a standard in Abstract Algebra is the notion of the *discriminant* of a set of algebraic numbers in a number field K of degree n. For this reason, we shall elaborate further on this topic. To approach this systematically, we first introduce the discriminant of a polynomial, which necessitates a discussion of resultants.

Given two polynomials over the rationals,

$$f(x) := a_0 \prod_{i=1}^{m} (x - \alpha_i) \quad \text{and} \quad g(x) := b_0 \prod_{j=1}^{n} (x - \beta_j) \in \mathbb{Q}[x],$$

a natural question arises: under what conditions do they share a common factor? This occurs precisely when they possess a common root, meaning $\alpha_i = \beta_j$ for some i, j. Consequently, f and g have a common factor if and only if the expression

$$P := \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (\alpha_i - \beta_j),$$

vanishes. This product appears, for instance, when evaluating g in the roots of f: for each $i = 1, \ldots, m$, note that

$$g(\alpha_i) = b_0 \prod_{j=1}^{n} (\alpha_i - \beta_j),$$

so that

$$\begin{aligned} \prod_{i=1}^{m} g(\alpha_i) &= \prod_{i=1}^{m} \left(b_0 \prod_{j=1}^{n} (\alpha_i - \beta_j) \right) \\ &= b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = b_0^m P. \end{aligned} \tag{1.2}$$

Analogously, we may evaluate f in the roots of g, obtaining

$$\begin{aligned} \prod_{j=1}^{n} f(\beta_j) &= \prod_{j=1}^{n} \left(a_0 \prod_{i=1}^{m} (\beta_j - \alpha_i) \right) \\ &= \prod_{j=1}^{n} \left(a_0 \prod_{i=1}^{m} -(\alpha_i - \beta_j) \right) \\ &= a_0^n (-1)^{mn} \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = a_0^n (-1)^{mn} P. \end{aligned} \tag{1.3}$$

By Equations 1.2 and 1.3, we obtain two expressions for P, namely

$$\frac{1}{b_0^m}\prod_{i=1}^{m} g(\alpha_i) = \frac{1}{a_0^n(-1)^{mn}}\prod_{j=1}^{n} f(\beta_j),$$

or, in a more standard way,

$$a_0^n(-1)^{mn}\prod_{i=1}^{m} g(\alpha_i) = b_0^m\prod_{j=1}^{n} f(\beta_j). \tag{1.4}$$

Any of these two expressions is called the *resultant of f and g*, and we shall write it as $\mathrm{Res}(f,g)$. With this, we may state:

Proposition 1.1. *Two polynomials $f, g \in \mathbb{Q}[x]$ have a common factor if and only if* $\mathrm{Res}(f,g) = 0$.

The discriminant of a polynomial appears when using the resultant to determine wether a polynomial has a multiple root. Recall that a polynomial has a multiple root if and only if it shares a root with its (formal) derivative f'. This fact, along with Proposition 1.1, shows that:

Proposition 1.2. *A polynomial $f \in \mathbb{Q}[x]$ has a multiple root if and only if* $\mathrm{Res}(f, f') = 0$.

In this particular case, one may extract a more precise numerical invariant by explicit manipulation. Consider $f(x) = \sum_{i=0}^{m} a_i x^{m-i}$, so that

$$\begin{aligned}
\mathrm{Res}(f,f') &= a_0^{m-1}(-1)^{m(m-1)}\prod_{i=1}^{m} f'(\alpha_i) \\
&= a_0^{m-1}\prod_{i=1}^{m}\left(a_0 \sum_{k=1}^{m} \prod_{\substack{j=1 \\ j\neq k}}^{m} (\alpha_i - \alpha_j) \right) \\
&= a_0^{m-1}a_0^{m}\prod_{i=1}^{m}\prod_{\substack{j=1 \\ j\neq i}}^{m}(\alpha_i - \alpha_j) \\
&= a_0^{2m-1}(-1)^{\frac{m(m-1)}{2}} \prod_{\substack{1\leq i\leq m-1 \\ 2\leq j\leq m \\ i<j}} (\alpha_i - \alpha_j)^2.
\end{aligned}$$

The last product is the only part of the resultant that may vanish. Note that this product depends on the values of the α_k, and not on them actually being the roots of f. It is called the *discriminant of* $\alpha_1, \dots, \alpha_m$, and it is written as $\Delta(\alpha_1, \dots, \alpha_m)$. With this we obtain:

Proposition 1.3. *Given a polynomial $f \in \mathbb{Q}[x]$ with roots $\alpha_1, \dots, \alpha_m$, it has a multiple root if and only if* $\Delta(\alpha_1, \dots, \alpha_n) = 0$.

We have given, so far, a rather manual formulation, but the key to arrive at the concept of discriminant of a set of algebraic numbers one must first consider a matricial formulation. In Dedekind's time, the product

$$\prod_{1\leq i<j\leq m}(\alpha_i-\alpha_j)$$

had a well known formula as the determinant of the matrix

$$V(\alpha_1,\ldots,\alpha_m):=\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{m-1} & \alpha_2^{m-1} & \cdots & \alpha_m^{m-1} \end{pmatrix}.$$

Nowadays, matrices in which each column forms a geometric progression are generically called *Vandermonde matrices.* With this in mind:

Proposition 1.4. *Given $\alpha_1,\ldots,\alpha_m\in\mathbb{Q}$, one has*

$$[\det V(\alpha_1,\ldots,\alpha_m)]^2=\Delta(\alpha_1,\ldots,\alpha_m).$$

Building on this concept, Dedekind examined analogous matrices where the superscript notation indicates *conjugation* rather than exponentiation. This leads naturally to consideration of the matrix

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^{(1)} & \alpha_2^{(1)} & \cdots & \alpha_m^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{(m)} & \alpha_2^{(m)} & \cdots & \alpha_m^{(m)} \end{pmatrix},$$

where $\alpha_k^{(j)}$ denotes the j-th conjugate of α_k. In direct analogy with Proposition 1.4, Dedekind defines the *discriminant of* $\alpha_1,\ldots,\alpha_m$ as the square of the determinant of the conjugate-based matrix. To emphasize its dependence on the number field K over $\mathbb{Q}$, we denote this invariant by $\Delta_{K/\mathbb{Q}}$ and refer to it as the *number field discriminant of the α_k.*

To handle indices more clearly, it is convenient to introduce framework of *number field morphisms.* These are ring momorphisms that fix the base field $\mathbb{Q}$, that it, $\mathbb{Q}$-algebra morphisms. For a number field $K/\mathbb{Q}$, a number field morphism $K\to\mathbb{C}$ is also called a *complex embedding*, and we write the set of all these embeddings as $\mathrm{Emb}_{\mathbb{Q}}(K,\mathbb{C})$. If $[K:\mathbb{Q}]=m$, one may prove that there are m total $\mathbb{Q}$-embeddings $K\to\mathbb{C}$. Writting $\sigma_1,\ldots,\sigma_m$ for said embeddings (where σ_1 is the identity map), one has that

$$\Delta_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_m):=\det\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_m) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(\alpha_1) & \sigma_m(\alpha_2) & \cdots & \sigma_m(\alpha_m) \end{pmatrix}^2$$

Recall that the determinant of a matrix is zero if and only if its columns are linearly dependent. The discriminant is defined in terms of a determinant, so one may ask if there is a way check whether a set of m-many elements of K form a $\mathbb{Q}$-basis of K through the discriminant. This poses the following question: how does conjugation affect linear dependency?

For the number field $K := \mathbb{Q}(\theta)$ of degree m, let us compute the discriminant of the $\mathbb{Q}$-basis $1, \theta, \theta^2, \ldots, \theta^{m-1}$. Directly,

$$\begin{aligned}\Delta_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{m-1}) &= \det \begin{pmatrix} \sigma_1(1) & \sigma_1(\theta) & \cdots & \sigma_1(\theta^{m-1}) \\ \sigma_2(1) & \sigma_2(\theta) & \cdots & \sigma_2(\theta^{m-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(1) & \sigma_m(\theta) & \cdots & \sigma_m(\theta^{m-1}) \end{pmatrix}^2 \\ &= \det \begin{pmatrix} \sigma_1(1) & \sigma_1(\theta) & \cdots & \sigma_1(\theta)^{m-1} \\ \sigma_2(1) & \sigma_2(\theta) & \cdots & \sigma_2(\theta)^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(1) & \sigma_m(\theta) & \cdots & \sigma_m(\theta)^{m-1} \end{pmatrix}^2 \\ &= \prod_{0 \leq i < j \leq m} (\sigma_j(\theta) - \sigma_i(\theta))^2. \end{aligned}$$

Note that in this product, the differences are of the conjugates of θ, or equivalentrly, the roots of the minimal polynomial f_θ. Said roots are all distinct from eachother because f_θ is irreducible, thus:

Proposition 1.5. *For a number field $K = \mathbb{Q}(\theta)/\mathbb{Q}$ of degree m, one has that $\Delta_{K/\mathbb{Q}}(1, \ldots, \theta^{m-1}) \neq 0$.*

that (1) the discriminant of a $\mathbb{Q}$-basis of a number field of degree n is nonzero, and moreover, the discriminant of a set of any n algebraic numbers in a number field is zero if and only they are $\mathbb{Q}$-linearly dependent ([2, pp. 110–11]), and that (2) the norm of any algebraic number, and the discriminant of any collection of algebraic numbers, are rational numbers ([2, p. 112–13]).

1.2. Algebraic integers

Dedekind was certainly the first to introduce explicitly the notion of algebraic integer as we know it, although Stilwell in [25] argues that it was a fairly natural step in the study of algebraic equations and their arithmetic, specially given the problems and methods that Dedekind had at hand. For instance, Euler had proven the cubic case of Fermat's Last Theorem using thrid roots of unity in the 1600s (see Edwards' extended discussion in [10, Ch. 2]); he also proved a conjecture of Fermat that 27 is the only cube that may be written as a perfect square plus two using numbers of the form $a+b\sqrt{-2}$ in his *Vollständige Anleitung zur Algebra* (see [11]); and Gauß had studied the arithmetics of the numbers of the form $a + bi$, for $a, b \in \mathbb{Z}$, in [13], the now called *Gaussian integers*. From this, Stillwell concludes that

> "[...] by 1800 it was clear that irrational objects were good for number theory. What was not clear was the nature of these objects and the reasons they behaved like integers, if indeed they did. A lot more work had to be done before the right concept of "algebraic integer" was isolated" (Stillwell in [25, p. 267]).

In [2, §13], Dedekind calls an algebraic number an *algebraic integer* (over $\mathbb{Q}$) when the polynomial of which it is a root of is monic and has integer coefficients. Immediately, he proves a couple of basic properties. The one we have interest in is:

Proposition 1.6. (cf. [2, §13.1]) *The set of all algebraic integers (over $\mathbb{Q}$) is a (commutative) ring (with unity) with the sum and multiplication of the complex numbers.*

The idea behind Dedekind's proof is the simple observation that α is an algebraic integer, i.e. α satisfies an equation of some degree n, say $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some integers a_i, if and only if one may write α^n as a $\mathbb{Z}$-linear combination of the $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. With this in mind, given two arbitrary algebraic integers α, β, one could try to write $(\alpha+\beta)^n$, as a $\mathbb{Z}$-linear combination of lower powers of $(\alpha+\beta)$. For full details, we refer to [23, Proposition 2.4].

He writes $\mathfrak{o}$ for the ring of all algebraic integers, but we shall use the modern notation $\mathcal{O}_K$. He notes that given a number field $K/\mathbb{Q}$, the closure properties of algebraic integers and of K translate to the algebraic integers of K being a subring of K, which we shall write $\mathcal{O}_K$ conforming to modern notation. He immediately proceeds to prove that:

Proposition 1.7. (cf. [2, pp. 114–16]) *Given a number field $K/\mathbb{Q}$ of degree n, its ring of integers $\mathcal{O}_K$ is a finitely generated abelian group.*

His proof consists of finding what we would now call a $\mathbb{Z}$-basis for $\mathcal{O}_K$ (as a $\mathbb{Z}$-module, of course). He first notes that given any $\mathbb{Q}$-basis of K, one may appropriately scale the elements of said basis so they become (algebraic) integers, call this new basis $\alpha_1, \ldots, \alpha_n$. Thanks to the closure of algebraic integers, the $\mathbb{Z}$-linear combinations of this now integral $\mathbb{Q}$-basis for K will yield algebraic integers, that is $\mathbb{Z}[\alpha_1, \ldots, \omega_n] \subseteq \mathcal{O}_K$. Dedekind notes that is not obvious that every number in $\mathcal{O}_K$ can be written in said fashion, and in fact states that in general that is not the case. Thus it is necessary to construct a different $\mathbb{Z}$-basis. The actual idea of Dedekind is quite cumbersome, so we offer a slightly different, clearer statement instead:

Proposition 1.8. ([22, Theorem 9]) *Given a $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ of the degree n number field $K/\mathbb{Q}$, formed by algebraic integers of K, any element of $\mathcal{O}_K$ can be written as*

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{\Delta(\alpha_1, \ldots, \alpha_n)},$$

for some $m_i \in \mathbb{Z}$.

Thus, if we write $d := \Delta(\alpha_1, \ldots, \alpha_n)$, we obtain that $\mathcal{O}_K \subseteq \mathbb{Z}[\frac{\alpha_1}{d}, \ldots, \frac{\alpha_n}{d}]$. This shows that $\mathcal{O}_K$ contains, and is contained, in a free abelian group of rank n, and hence is one. These type of bases are nowadays named *integral bases* for $\mathcal{O}_K$.

There may be multiple possible integral bases for the integers of a number field, but the value of the discriminant of these bases will be same for all of them (see [22, Theorem 11] for a proof). In consequence, one may speak of the *fundamental discriminant* of a number field $K/\mathbb{Q}$ as the discriminant of any integral basis of its ring of integers, and we write it as $\Delta(K)$, just like Dedekind.

1.3. Ideal arithmetics

In [2, §19], Dedekind introduces the modern notion of an *ideal* in the integer ring $\mathcal{O}_K$ of a number field $K/\mathbb{Q}$, including *principal ideals.* He extends divisibility concepts from $\mathbb{Z}$ to ideals by defining that an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ *divides* another ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ (or $\mathfrak{b}$ is a *multiple* of $\mathfrak{a}$) if $\mathfrak{a} \supseteq \mathfrak{b}$, denoted $\mathfrak{a} \mid \mathfrak{b}$. For example, since all ideals of $\mathcal{O}_K$ are subsets of $\mathcal{O}_K$, they are all divisible by $\mathcal{O}_K$ itself.

In [2, §20], Dedekind defines congruence modulo an ideal: two elements $\omega, \omega' \in \mathcal{O}_K$ are *congruent modulo* $\mathfrak{a}$ (written $\omega \equiv \omega' \pmod{\mathfrak{a}}$) if $\omega - \omega' \in \mathfrak{a}$. He denotes the number of congruence classes modulo $\mathfrak{a}$ by $(\mathcal{O}_K, \mathfrak{a})$, though we will use the modern notation $[\mathcal{O}_K : \mathfrak{a}]$ for the index of $\mathfrak{a}$ in $\mathcal{O}_K$. He calls this the *norm of* $\mathfrak{a}$, and writes is as $N(\mathfrak{a})$.

Dedekind quietly uses a neat relationship between ideal inclusions and their norms, though he never spells it out explicitly. The key idea is simple: the bigger an ideal, the smaller its norm. The complete proof is a slick application of the Third Isomorphism Theorem, though we'll skip the details here:

Lemma 1.9. *Let $\mathcal{O}_K$ be the ring of integers of a number field K, and $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ two ideals. If $\mathfrak{b} \supseteq \mathfrak{a}$, then $N(\mathfrak{b}) \leq N(\mathfrak{a})$.*

Next, in [2, §21], Dedekind deals with *prime ideals*, which he defines, in clear analogy with the integers, as ideals of $\mathcal{O}_K$ with no proper divisors, that is, divisible only by $\mathcal{O}_K$ and by itself. He proves a few basic results regarding prime ideals, that come from trying to mimic fundamental properties of usual integer arithmetic, namely:

1. Every integer > 1 has some prime number factor.

2. If two integers $a, b \in \mathbb{Z}$ are coprime, their least common multiple is their product ab.

3. (Euclid's lemma) If a prime number p divides a product of numbers ab then $p \mid a$ or $p \mid b$.

4. If a prime number p divides $a \in \mathbb{Z}$, then there is $b \in \mathbb{Z}$ such that $\operatorname{lcm}(a, b)$ is a multiple of p.

The content of the following four propositions is the ideal analogues of the listed properties, along with their proofs in the style of Dedekind.

Proposition 1.10. (cf. [2, §21.1]) *Let K be a number field. Every proper ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ is divisible by some prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. That is, $\mathfrak{a}$ is contained in some prime ideal $\mathfrak{p}$.*

Demostración. If $\mathfrak{a}$ is itself prime, taking $\mathfrak{p} := \mathfrak{a}$ suffices. If not, $\mathfrak{a}$ is divisible by some ideal $\mathfrak{a}_1$, that is, $\mathfrak{a}_1 \supsetneq \mathfrak{a}$. Again, if $\mathfrak{a}_1$ is prime, we are done; if not, it is divisible by some ideal $\mathfrak{a}_2$, that is, $\mathfrak{a}_2 \supsetneq \mathfrak{a}_1$. Continuing in this fashion, we obtain an ascending chain of ideals $\mathfrak{a} \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$, which in turn, thanks to Lemma 1.9, gives a chain of norms, $N(\mathfrak{a}) \geq N(\mathfrak{a}_1) \geq N(\mathfrak{a}_2) \geq \dots$, and since the norm of an ideal is a positive integer, any descending chain of norms must terminate after finitely many steps. This forces the corresponding chain of ideals to stabilize as well. Consequently, there exists a maximal ideal $\mathfrak{a}_*$ in the chain (with minimal norm) that isn't properly contained in any other ideal—meaning $\mathfrak{a}_*$ admits no proper divisors and is therefore prime. □

Rings in which ascending chains of ideals terminate are called nowadays *Noetherian*, in honor of German mathematician Emmy Noether. Hence, the previous proof shows that:

Corollary 1.11. *The ring of integers $\mathcal{O}_K$ of a number field K is Noetherian.*

We continue with the analogue of (2), for which we need the notion of *least common multiple* of ideals. Given two ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$, the ideals that are divisible by both $\mathfrak{a}$ and $\mathfrak{b}$ are precisely the ideals contained by both $\mathfrak{a}$ and $\mathfrak{b}$. The smallest of them (with respect to the order $\supseteq$) is therefore the biggest ideal contained in both $\mathfrak{a}$ and $\mathfrak{b}$, that is, their intersection. Thus one may define

$$\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) := \mathfrak{a} \cap \mathfrak{b}.$$

This least common multiple, by definition, contains all other common multiples of $\mathfrak{a}$ and $\mathfrak{b}$. With this:

Proposition 1.12. (cf. [2, §21.2]) *Let K be a number field, $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal and $\alpha \in \mathcal{O}_K$. If $\mathfrak{p}$ does not divide α, then $\operatorname{lcm}(\mathfrak{p}, (\alpha)) = \alpha\mathfrak{p}$.*

Demostración. We must verify that $\mathfrak{p} \cap (\alpha) = \alpha\mathfrak{p}$. The inclusion $\supseteq$ is clear by absorption. Thus take an arbitrary $y \in \mathfrak{p} \cap (\alpha)$. In particular $y = \alpha x$ for some $x \in \mathcal{O}_K$. As $\mathfrak{p}$ is an ideal, it must be that $\alpha x \in \mathfrak{p}$. As $\mathfrak{p}$ does not contain α, it must be that $x \in \mathfrak{p}$. Hence, we conclude that $y \in \alpha\mathfrak{p}$. □

For (3), Dedekind actually first proves a slightly weaker version of the Lemma, and only after defining the product of ideals can state and prove a fuller version:

Proposition 1.13. (Weak Euclid's lemma for ideals, cf. [2, §21.3]) *Let K be a number field, $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal, and $\alpha, \beta \in \mathcal{O}_K$. If $\mathfrak{p} \mid \alpha\beta$, then $\mathfrak{p} \mid \alpha$ or $\mathfrak{p} \mid \beta$.*

Demostración. Reciprocally, assume $\alpha, \beta \notin \mathfrak{p}$. If $\alpha\beta \in \mathfrak{p}$, then $\alpha(\beta)$ would be contained in both $\mathfrak{p}$ and in (α)—that is, it would be a common multiple of $\mathfrak{p}$ and (α). But by the previous Proposition, $\alpha\mathfrak{p}$ is the least common multiple of (α) and $\mathfrak{p}$, thus $\alpha(\beta) \subseteq \alpha\mathfrak{p}$ (for $\mathfrak{p}$ does not contain α), and hence $(\beta) \subseteq \mathfrak{p}$. In particular $\beta \in \mathfrak{p}$, which is contradictory with our first assumption. □

There is a slick little application of this theorem, which will be actually very useful to the study of ramification:

Proposition 1.14. (cf. [2, p. 124]) *Let K be a number field. The rational numbers divisible by a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ form a cyclic group, generated by a single rational prime.*

Demostración. The integers divisible by $\mathfrak{p}$, that is, the n such that $\mathfrak{p} \ni n$ are precisely $\mathfrak{p} \cap \mathbb{Z}$, which is easly seen to be an ideal of $\mathbb{Z}$, hence cyclic, generated by the smallest number that divides $\mathfrak{p}$, call it p (this is because of the well-ordering principle). This p is prime: if it were composite, say $p = ab$ (with both $a, b < p$), then $\mathfrak{p} \mid ab$, hence by Theorem 1.13, $\mathfrak{p} \mid a$ or $\mathfrak{p} \mid b$; but then p would not be the smallest integer divisible by $\mathfrak{p}$, a contradiction. □

In such case, $\mathfrak{p}$ is said to *be over p*. One may compute $N(p\mathcal{O}_K)$:

Proposition 1.15. *Let $K/\mathbb{Q}$ be a number field of degree $[K : \mathbb{Q}] = n$, and $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal. For the prime p below $\mathfrak{p}$, one has that $N(p\mathcal{O}_K) = p^n$.*

Demostración. We wish to compute $\#(\mathcal{O}_K/p\mathcal{O}_K)$. Let $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. For two numbers in $\mathcal{O}_K$, being congruent modulo $p\mathcal{O}_K$ is equivalent to the respective coefficients being congruent modulo p. This way, each residue class of $\mathcal{O}_K/p\mathcal{O}_K$ is represented by a linear combination with coefficients in $\mathbb{Z}/p\mathbb{Z}$, so each of the n coordinates have p possible values (from 0 to $p-1$), which ammounts to p^n-many classes modulo $p\mathcal{O}_K$. □

Note that as $\mathfrak{p} \ni p$, we have that $\mathfrak{p} \supseteq p\mathcal{O}_K$. Taking norms, one sees that $N(\mathfrak{p}) \mid N(p\mathcal{O}_K) = p^n$, so $N(\mathfrak{p})$ is some power of p, say p^f, for some $1 \leq f \leq n$. Said f is called the *degree* of $\mathfrak{p}$. A way to state this result in modern terms is:

Proposition 1.16. *Let $K/\mathbb{Q}$ be a number field. Any prime number $p \in \mathbb{Z}$, and prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ over p, define a finite residue field extension $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$.*

In [2, §22], we are introduced the notion of the *product* of two ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ as the ideal

$$\mathfrak{a}\mathfrak{b} := (\{\alpha\beta \colon \alpha \in \mathfrak{a},\, \beta \in \mathfrak{b}\}) \subseteq \mathcal{O}_K.$$

Note that if we were to consider only the products $\alpha\beta$ we would not obtain an ideal, for the difference $\alpha\beta - \alpha'\beta'$ is not of that form. From the definition it is clear that ideal multiplication is commutative, that $\mathcal{O}_K$ is an identity element for it, and (with a little more work) that it is associative. If we put $\mathcal{I}(K)$ for the set of all ideals of $\mathcal{O}_K$, we can write:

Lemma 1.17. *For a number field K, the set $\mathcal{I}(K)$ is a commutative monoid with ideal multiplication.*

Inmediately, he proceeds to exhibit that this notion of multiplication satisfies reasonable properties with respect to divisibility. Namely, that the product $\mathfrak{a}\mathfrak{b}$ is divisible by $\mathfrak{a}$ and $\mathfrak{b}$ (this is direct by absorption, see [2, §22.1]), and:

Proposition 1.18. (Euclid's lemma for ideals, cf. [2, §22.3]) *Let $\mathcal{O}_K$ be the integer ring of a number field K, and $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ ideals. If a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ divides the product $\mathfrak{a}\mathfrak{b}$, then it divides $\mathfrak{a}$ or $\mathfrak{b}$.*

Demostración. In terms of inclusions, the statement to prove is that if $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, then $\mathfrak{a} \subseteq \mathfrak{p}$ or $b \subseteq \mathfrak{p}$. If the conclusion were false, then there would be $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ such that $\alpha, \beta \notin \mathfrak{p}$. Clearly, $\alpha\beta \in \mathfrak{a}\mathfrak{b}$, but it is not divisible by $\mathfrak{p}$ because of Proposition 1.13. In particular, $\mathfrak{p}$ does not divide $\mathfrak{a}\mathfrak{b}$. □

Dedekind in [2, §23] identifies a fundamental "difficulty in the theory": his use of Kummer's notion of divisibility (via set inclusion) conflicts with the conventional arithmetic definition where $a \mid b$ means $b = ac$ for some c. This tension becomes problematic when attempting to recover unique factorization through ideal theory. As he acknowledges:

> "This difficulty, which is the greatest and really the only one presented by the theory, cannot be surmounted by the methods we have employed thus far, and it is necessary to examine more closely the reason for this phenomenon, because it is connected with a very important generalisation of the theory" (Stillwell's translation of Dedekind in [2, p. 126]).

To resolve this, Dedekind develops the following strategy:

$$\begin{aligned} \text{Technical lemmas} &\implies \text{Prime ideals have principal multiples} \\ &\implies \text{All ideals have principal multiples} \\ &\implies \text{Ideal divisibility notions coincide} \\ &\implies \text{Unique factorization of ideals} \end{aligned}$$

However, we will follow Dedekind's alternative approach—one he later developed but personally disfavored, though we find it cleaner. This method employs his generalization of Gauß's Lemma on polynomials from [4], which he named his "Prague Theorem" (the name by which it's still known today). The proof path becomes:

$$\begin{aligned} \text{Prague Theorem} &\implies \text{Ideals have principal multiples} \\ &\implies \text{Divisiblity notions coincide} \\ &\implies \text{Unique factorization of ideals} \end{aligned}$$

This appreach appears in his lastest version of his ideal theory, which, as far as I am concerned, never has been translated into English. In spite of this, there is a close retelling of this method in Harris Hancock's *Foundations of the*

Theory of Algebraic Numbers from 1932 (cf. [15, pp. 24–29]), which we indeed follow.

Gauß's lemma appears originally in his *Disquisiciones* (cf. [12, Art. 42]), and states that if the product of two (monic) polynomials with rational coefficients has integer coefficients, then *a posteriori* the original polynomials have integer coefficients. Dedekind's version is more general for it involves the products of the coefficients and algebaric integers:

Theorem 1.19. (Dedekind's 1892 Prague Theorem, cf. [4]) *Let K be a number field, and $f, g \in K[x]$. If $fg \in \mathcal{O}_K[x]$, then* a posteriori *every product of any coefficient of f with any of g is an algebraic integer.*

Proof of this result may be found in [15, Art. 15, pp. 27–28]. With this, we can show:

Proposition 1.20. *Let K be a number field of degree n. Every ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ has a multiple (by some ideal $\mathfrak{b} \subseteq \mathcal{O}_K$) which is a principal ideal.*

Demostración. Consider an ideal $\mathfrak{a} := (\alpha_1, \ldots, \alpha_n) \subseteq \mathcal{O}_K$. We wish to find an ideal $\mathfrak{b} := (\beta_1, \ldots, \beta_r) \subseteq \mathcal{O}_K$ such that $\mathfrak{ab} = (g)$, for some $g \in \mathcal{O}_K$. That is, we wish to write each finite sum of the form $\sum_{i,j=1}^{k} \alpha_i \beta_j$ as a multiple of some fixed g, and viceversa.

Given any $\mathfrak{b}$, one may try consider the greatest common divisor of all such finite sums, for that gives $(g) \supseteq \mathfrak{ab}$ immediately. A major issue is that, as we have seen, the notion of greatest common divisor is not defined for algebraic integers. Thus, if we want to use gcd's to our advantage, we must find a way to obtain rational integers from the algebraic integers.

One way to achieve this is to note that we can regard the rational integers as the algebraic integers of $\mathbb{Q}$, that is, algebraic integers left invariant under all conjugations. And we know a way to obtain numbers invariant under conjugation starting from a single algebaric number: taking its norm—that is, the product of all its conjugates.

Let $\sigma_1, \ldots, \sigma_n$ be the $\mathbb{Q}$-embeddings $K \to \mathbb{C}$ (indexed so that σ_0 is the identity), and consider the product

$$P := \prod_{k=0}^{n-1} \sigma_k(\alpha_1 + \cdots + \alpha_n) = \prod_{k=0}^{n-1} (\sigma_k(\alpha_1) + \cdots + \sigma_k(\alpha_n)). \tag{1.5}$$

This P is indeed invariant under conjugation, thus $P \in \mathbb{Q}$. At this point one might be tempted to take the greatest common divisor of all summands that apear when expanding P, but this is also wrong: that $P \in \mathbb{Q}$ does not tell us that the summands are also in $\mathbb{Q}$, less that they are in $\mathbb{Z}$.

Do not be misguided: they are in $\mathbb{Z}$, but this is not a fruitful path to prove so. Dedekind's clever trick is to formulate the problem in terms of polynomials, making sure that the summands appear as coefficients, making possible to use his Prague Theorem to reach the desired conclusion.

Firstly, consider the polynomials whose coefficients are the α's and their conjugates: for each $k = 0, \dots, n-1$, let

$$A_k(x) := \sum_{i=1}^{n} \sigma_k(\alpha_i) x^{n-i}.$$

Each A_k is the polynomial analogue of each factor from Equation 1.5. In the same vein, we may consider $P(x) := \prod_{k=0}^{n-1} A_k(x)$, which is the analogue for the whole product from Equation 1.5. That $P(x)$ is invariant under conjugation means that is coefficients are symmetric polynomials in the $\sigma_k(\alpha_i)$, and thus the Fundamental Theorem of Symmetric Polynomials states that they must lie in the fixed field, which in this case is $\mathbb{Q}$.

To verify that they are rational integers, note that the coefficients of each $A_k(x)$ are algebraic integers, and thus the coefficients of $P(x)$ are products of algebraic integers, hence algebaric integers themselves. Therefore, the coefficients of $P(x)$ are rational numbers and algebraic integers, that is, they are rational integers.

We are now in our right to let g be greatest common divisor of all the coefficients of $P(x)$. We are yet to find a candidate for $\mathfrak{b}$, but that is natural looking at the polynomial world: note that to obtain $P(x)$ (i.e., the polynomial with the "right" numbers as coefficients), we had to multiply A_0 (the polynomial whose coefficients are the unconjugated α's) by each polynomial with conjugated coefficients, that is, by the factor

$$B(x) := \prod_{k=1}^{n-1} A_k(x);$$

do note that the index starts at $k = 1$ instead of $k = 0$. Thus we may consider $\mathfrak{b}$ to be the ideal generated by all the coefficients of B, call them $\beta_1, \dots, \beta_r$, so that when computing $\mathfrak{ab}$ we obtain, again, the "right" numbers.

This raises one red flag: why are the coefficients of B, namely, the $\beta_1, \dots, \beta_r$ algebraic integers? This is non-trivial, and answer lies in the Prague Theorem: note that $P(x) = A_0(x)B(x)$ and as this product has algebaric integer coefficients, Dedekind's Prague Theorem (cf. 1.19) states the the coefficients of both A_0 and B are themselves algebraic integers.

Let us verify that, indeed, $\mathfrak{ab} = (g)$. It is clear that $\mathfrak{ab} \subseteq (g)$. For the other inclusion, writting the coefficients of $P(x)$ as $g_1, \dots, g_s$, we may use Bézout's Identity to write g as a $\mathbb{Z}$-linear combination,

$$g = k_1 g_1 + \cdots + k_s g_s.$$

Each g_t is a finite sum of terms of the form $\alpha_i \beta_j$, thus the previous expression writes g a a $\mathbb{Z}$-linear combination of things of the form $\alpha_i \beta_j$, which is precisely that $(g) \subseteq \mathfrak{ab}$. □

With this:

Proposition 1.21. *Let K be a number field, and $\mathfrak{a}, \mathfrak{c} \subseteq \mathcal{O}_K$ ideals. If $\mathfrak{a} \mid \mathfrak{c}$, then there is an ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ such that $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.*

Demostración. By the previous Proposition, there is an ideal $\mathfrak{i} \subseteq \mathcal{O}_K$ such that $\mathfrak{a}\mathfrak{i} = (\alpha)$, for some $\alpha \in \mathcal{O}_K$. As $\mathfrak{c} \subseteq \mathfrak{a}$, it follows that $\mathfrak{c}\mathfrak{i} \subseteq \mathfrak{a}\mathfrak{i} = (\alpha)$. That is, every number of $\mathfrak{c}\mathfrak{i}$ is of the form $\omega\alpha$ for some $\omega \in \mathcal{O}_K$. Let $\mathfrak{b} := \mathfrak{c}\mathfrak{i}$. This $\mathfrak{b}$ is an ideal, for given any $\gamma \in \mathcal{O}_K$ one has that $\gamma(\omega\alpha) = (\gamma\omega)\alpha \in \mathfrak{b}$. Finally,

$$\begin{aligned} \mathfrak{c}\mathfrak{i} = \mathfrak{b}(\alpha) &\implies \mathfrak{a}\mathfrak{c}\mathfrak{i} = \mathfrak{a}\mathfrak{b}(\alpha) \\ &\implies \mathfrak{c}(\alpha) = \mathfrak{a}\mathfrak{b}(\alpha) \\ &\implies \mathfrak{c} = \mathfrak{a}\mathfrak{b}. \end{aligned}$$ □

Theorem 1.22. (Unique factorization for ideals, cf. [2, §25.4]) *Let K be a number field. Every proper ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ is uniquely descomposable as a product of prime ideals of $\mathcal{O}_K$.*

Demostración. By Proposition 1.10, there is some prime ideal $\mathfrak{p}_1 \subseteq \mathcal{O}_K$ dividing $\mathfrak{a}$, and thus Proposition 1.21 indicates there is some ideal $\mathfrak{a}_1 \subseteq \mathcal{O}_K$ such that $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$. Applying the same treatment to $\mathfrak{a}_1$ we obtain the respective $\mathfrak{p}_2$ and $\mathfrak{a}_2$ so that $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{a}_2$. Continuing in this fashion we obtain a finite list of primes, for the $\mathfrak{a}_i$ form an ascending chain of ideals, which all terminate (cf. 1.11). Moreover, it terminates in $\mathcal{O}_K$ because, by the construction, that the chain stabilizes means that there is an ideal without prime ideal divisors, which is precisely $\mathcal{O}_K$. Consequently, we have a decomposition in prime ideals,

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r,$$

for some $r > 0$.

To conclude that said factorization is unique, consider another such product of primes, say $\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s$. Consider the case of $\mathfrak{q}_1$: as it divides $\mathfrak{a}$, it must divide the product $\mathfrak{p}_1 \dots \mathfrak{p}_r$; by Euclid's Lemma (cf. 1.18), it must divide of the factor, say, up to a change of indices $\mathfrak{p}_1$. But this is a prime ideal, and therefore $\mathfrak{q}_1 = \mathcal{O}_K$ or $\mathfrak{q}_1 = \mathfrak{p}_1$. But $\mathfrak{q}_1$ is also prime, thus $\mathfrak{q}_1 \neq \mathcal{O}_K$, from which $\mathfrak{q}_1 = \mathfrak{p}_1$. This shows that

$$\mathfrak{p}_1(\mathfrak{p}_2 \dots \mathfrak{p}_r) = \mathfrak{p}_1(\mathfrak{q}_2 \dots \mathfrak{q}_s),$$

and therefore

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s.$$

Arguing in the same way for $\mathfrak{q}_2$ and the rest of the $\mathfrak{q}_i$'s, we arrive at the desired conclusion. □

1.4. Ideal classes

Dedekind closely follows Kummer's work on his "ideal complex numbers," which he credits as the direct inspiration for his own ideal theory. A central goal of Dedekind's approach was to put Kummer's results on firm theoretical ground using his new language of ideals. Such is the case of ideal classes.

We provide below our translation of Kummer's complete passage introducing ideal classes, which in the author's opinion sheds light upon such a central object:

> Thus, the ideal multipliers, which, when composed with all ideal complex numbers, yield existing complex numbers, can always be chosen such that their norms are smaller than $\lambda^{\frac{\lambda-1}{2}}$; and since the number of ideal factors whose norms do not exceed this fixed limit is finite, we have the following theorem:
>
> *There is always a finite number of ideal multipliers that, when composed with the infinitely many ideal numbers, render them all existing complex numbers.*
>
> The multipliers that make the ideal complex numbers existing, when composed with them, give rise to the classification of ideal complex numbers, which we establish by this definition:
>
> *All ideal complex numbers that yield existing products when multiplied by the same ideal number will be called* Equivalent Ideal Numbers, *and they will be assigned to the same* Class of ideal complex numbers (Author's translation of Kummer in [20, p. 443]).

Let us contextualize this discussion. When considering the product (what Kummer terms *composition*) of ideal complex numbers, he investigates whether such products can "actually represent" genuine (non-ideal) algebraic numbers. Remarkably, the answer is affirmative: there exist finitely many "special" ideal numbers that, when multiplied by any other ideal number, yield an actual algebraic number. Kummer uses these special ideals to classify all ideal numbers, grouping them into "special classes" where two ideals belong to the same class if their product with a fixed special ideal S results in an algebraic number. Formally, the class associated to S is

$$\{A \in \{\text{ideal complex numbers}\} : AS \text{ is an algebraic number}\}.$$

Dedekind, in [2, §28], seeks to adapt Kummer's concept to his ideal theory, but requires two crucial modifications. First, since ideal products yield other ideals (not algebraic numbers), the framework must accommodate entire families of numbers; and second, as these ideals reside in $\mathcal{O}_K$, their products contain only algebraic integers (not arbitrary algebraic numbers) Thus, Kummer's original question transforms into:

When does the product of two ideals result in an ideal that "represents" an algebraic integer?

This, in turn, raises the question of what it means for an ideal to "represent" an algebraic integer. The key insight lies in principal ideals which provide an embedded "copy" of the integer ring within $\mathcal{I}(K)$. Thus to "represent" an algebraic integer in this context means to be equal to the principal ideal generated by said integer. Proposition 1.20 offers a lead: every ideal has some multiplier $\mathfrak{m}$ rendering it principal, hence, following Kummer's approach, we now ask: are there finitely many such multipliers $\mathfrak{m}$? An affirmative answer would naturally lead to a robust notion of ideal classes.

Following Kummer, we then wish to prove that multiplier norms are uniformly bounded, and then be able to conclude that there are only finitely many ideals with norm bounded by a given number. This second part is actually direct:

Proposition 1.23. *Let K be a number field. For any integer $s > 0$, there exist only finitely many ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ with $N(\mathfrak{a}) \leq s$.*

Demostración. Let $\mathfrak{m}$ be an ideal with norm $m := N(\mathfrak{m})$. Since any ideal is divisible by only finitely many ideals, the principal ideal (m) must be contained in finitely many ideals of $\mathcal{O}_K$, and as that every ideal contains its norm as an element, this means than only finitely many ideals of $\mathcal{O}_K$ may have m as norm. Moreover, as for any fixed bound $s > 0$, there are only finitely many positive integers not exceding s, we conclude the desired result. □

Proposition 1.24. *Let K be a number field of degree n. Any ideal $\mathfrak{m} \subseteq \mathcal{O}_K$ that, when multiplied with another ideal $\mathfrak{a}$, yields a principal ideal, has norm bounded depending only on K (and not on $\mathfrak{a}$).*

Demostración. Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be an arbitrary ideal, and fix an integral $\mathbb{Q}$-basis $\omega_1, \ldots, \omega_n$ for K. For any integer $k > 0$, consider the $(k+1)^n$ algebraic integers of the form

$$h_1\omega_1 + \cdots + h_n\omega_n \quad \text{with} \quad 0 \leq h_i \leq k.$$

Since $N(\mathfrak{a})$ is the maximum number of incongruent integers modulo $\mathfrak{a}$, choosing k such that

$$k^n \leq N(\mathfrak{a}) < (k+1)^n$$

ensures (by the pigeonhole principle) that at least two such numbers, say

$$\beta = b_1\omega_1 + \cdots + b_n\omega_n \quad \text{and} \quad \gamma = c_1\omega_1 + \cdots + c_n\omega_n,$$

are congruent mod $\mathfrak{a}$, that is $\alpha := \beta - \gamma \in \mathfrak{a}$.

Let $E := \mathrm{Emb}_{\mathbb{Q}}(K, \mathbb{C})$. A straightforward computation using the $\mathbb{Q}$-linearity of embeddings and the triangle inequality yields

$$|N_{K/\mathbb{Q}}(\alpha)| \leq k^n \prod_{\sigma \in E} \left(\sum_{i=1}^{n} |\sigma(\omega_i)| \right).$$

Writting s for the product on the right side, this shows that $|N_{K/\mathbb{Q}}(\alpha)| \leq k^n s$. Note that s depends only on the chosen basis.

Since $\mathfrak{a} \mid \alpha$, Proposition 1.21 shows there exists an ideal $\mathfrak{m} \subseteq \mathcal{O}_K$ such that $(\alpha) = \mathfrak{a}\mathfrak{m}$. Taking norms gives,

$$N((\alpha)) = N(\mathfrak{a})N(\mathfrak{m}) = |N_{K/\mathbb{Q}}(\alpha)| \leq sk^n.$$

As $N(\mathfrak{a}) \geq k^n$, we conclude that $N(\mathfrak{m}) \leq s$. □

This shows that the multiplier ideals that yield principal ideals when multiplied with another ideal, can always be chosen with norms smaller than some uniform bound s. As there is finitely many ideals with norm less than s (see Proposition 1.23) we conclude:

Theorem 1.25. *There is a finite number of ideal multipliers that, when multiplied with ideals, result in principal ideals.*

With this, following Dedekind ([2, §28]) and Kummer ([20, p. 443], cf. the translated passage above), declare equivalent all ideals that yield principal ideals when multiplied by same ideal $\mathfrak{m}$; that is, for $\mathfrak{a}, \mathfrak{a}' \subseteq \mathcal{O}_K$,

$$\mathfrak{a} \sim \mathfrak{a}' \iff \text{there's an ideal } \mathfrak{m} \subseteq \mathcal{O}_K \text{ such that } \mathfrak{a}\mathfrak{m} \text{ and } \mathfrak{a}'\mathfrak{m} \text{ are principal.} \tag{1.6}$$

This is an equivalence relation in $\mathcal{I}(K)$:

Proposition 1.26. *Let K be a number field. The relation $\sim$ defined in 1.6 is an equivalence relation in the set $\mathcal{I}(K)$ of all ideals of $\mathcal{O}_K$.*

Demostración. That $\mathfrak{a} \sim \mathfrak{a}$ is the content of Proposition 1.20. That, if $\mathfrak{a} \sim \mathfrak{a}'$, then $\mathfrak{a}' \sim \mathfrak{a}$, is obvious. Let us verify transitivity. Suppose that $\mathfrak{a} \sim \mathfrak{b}$ and $\mathfrak{b} \sim \mathfrak{c}$, that is, there are ideals $\mathfrak{m}, \mathfrak{n} \subseteq \mathcal{O}_K$ such that $\mathfrak{a}\mathfrak{m}, \mathfrak{b}\mathfrak{m}, \mathfrak{b}\mathfrak{n}, \mathfrak{c}\mathfrak{n}$ are all principal. Note that, in this case, $\mathfrak{m} \sim \mathfrak{n}$, that is all ideals that make $\mathfrak{m}$ and $\mathfrak{n}$ principal are equivalent. Such is the case of $\mathfrak{a}$ and $\mathfrak{c}$, thus $\mathfrak{a} \sim \mathfrak{c}$. □

So we may consider $\mathrm{Cl}(K) := \mathcal{I}(K)/\sim$, the set of all ideal classes of $\mathcal{O}_K$. By means of ideal product, we may define an operation in the classes, as

$$[\mathfrak{a}][\mathfrak{b}] := [\mathfrak{a}\mathfrak{b}].$$

That this is well-defined, that the operation is associative, commutative, and that the class $[\mathcal{O}_K] = [(1)]$ (the *principal class*) is the identity, is shown by Dedekind in [2, p. 146–7] or Hancock in [15, p. 98]. We will ommit it here. Proposition 1.20 show that any class is invertible with respect to this product: the relation $\mathfrak{a}\mathfrak{b} = (\alpha)$, viewed in $\mathrm{Cl}(K)$, is simply $[\mathfrak{a}][\mathfrak{b}] = [(1)]$. This shows, together with Theorem 1.25, that:

Theorem 1.27. *For any number field K, the set $\mathrm{Cl}(K)$ of ideal clases of $\mathcal{O}_K$ modulo principality is a finite abelian group with the operation of ideal (class) multiplication.*

Thus, from now on, when we refer to $\mathrm{Cl}(K)$ we will always do so with its group structure, and to emphasize this, we will refer to it as the *ideal class group of K*[4]. The cardinal of $\mathrm{Cl}(K)$ is called the *class number*, and, following trandition[5], we will write it as h_K.

From basic algebra, we know that in a finite group, any element to the power of the order of the group is the identity. This, applied to the class group of a number field, yields:

[4] It should be of $\mathcal{O}_K$, but this is a recurring abuse of language; in any case, the integer ring is uniquely determined by the number field, so there is not ambiguity.

[5] Apparently, the use of h for class numbers goes back to Dirichlet in 1838. See `https://mathoverflow.net/questions/17062/why-is-h-the-notation-for-class-numbers` for a discussion.

Theorem 1.28. *Let K be a number field. For any $[\mathfrak{a}] \in \mathrm{Cl}(K)$,*

$$[\mathfrak{a}]^{h_K} = [(1)].$$

That is, any ideal of $\mathcal{O}_K$ has a power which is principal.

1.5. Divisors of the discriminant

1.6. Units of an integer ring

1.7. Ramification in Galois number fields

Ramification in number theory may be traced[6] to the influential *Theorie der algebraischen Functionen einer Veränderlichen* by Dedekind and Weber ([26], see Stillwell's translation into English in [6]), in which they applied methods of algebraic number theory to the geometric setting of Riemman surfaces, which allowed them to formulate said theory in purely algebraic terms. That includes the phenomenom of ramification points, which they codified in a *ramification ideal*, which, according to Emmylou Haffner ([14, fn. 80]) was later translated into number theory by Dedekind in his *Über die Diskriminanten endlicher Körper* ([3]).

The first complete treatise on the topic is David Hilbert's foundational paper on the ideal theory of Galois number fields, [17]. The contents of this work is mirrored in his *Zahlbericht* ([16, §§39–43], see Stillwell's translation into English in [18]), which we shall reference. One difference between both is an initial commentary, that sheds light on his motivations:

> The systematic development of the general theory of ideals of a Galois field proves to be necessary if we wish to successfully follow the suggestions contained in Kummer's treatises on the higher laws of reciprocity and to gain full mastery over the results obtained therein (Author's translation of Hilbert in [17, p. 13]).

Hilbert begins with the usual setting: let $K(\theta)/\mathbb{Q}$ be a *Galois* number field of degree n. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal of degree f, and let $p \in \mathbb{Z}$ the rationa2l prime below $\mathfrak{p}$. By modding out $\mathfrak{p}$ we obtain a finite (cf. Proposition 1.15) extension $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$. He wishes to study the Galois action in this extension. In the case of $K/\mathbb{Q}$ this is done by studying the different roots of the minimal polynomial of θ, thus it makes sense to study the minimal polynomial Φ of a generator $[P]$ of the extension $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$.

By definition, $\Phi(P) \equiv 0 \pmod{\mathfrak{p}}$, and to obtain all roots of Φ, Hilbert makes the observation that the p-th powers of $[P]$,

$$[P], [P]^p, [P]^{p^2}, \ldots, [P]^{p^{f-1}} \tag{1.7}$$

are f elements, the degree of Φ. They are all the diffrenents roots of Φ, becuase

$$\Phi(P^p) \equiv \Phi(P)^p \equiv 0 \pmod{\mathfrak{p}}.$$

Let us try to describe this in terms of the action of $\mathrm{Gal}(K/\mathbb{Q})$. For $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, the only condition for $\sigma(P)$ being another root of Φ modulo $\mathfrak{p}$ is that σ stabilizes $\mathfrak{p}$. Hilbert recognizes that the automorphisms that fix $\mathfrak{p}$ form a group, which he calls the *decomposition group of* $\mathfrak{p}$ (*Zerlegungsgruppe*) and writes it as g_z. We will use the modern notation $D_\mathfrak{p}$, which emphazises the importante of the ideal considered. So for $\sigma \in D_\mathfrak{p}$, one has that $\sigma(P) \equiv P^{p^i}$ with $0 \leq i < f$.

[6] The author is indebted to professor Keith Conrad for pointing the information of this parragraph out.

By looking at 1.7, it is apparent that all roots of Φ are obtained by taking successive p-th powers. If the map $[x] \mapsto [x]^p$ came from an element of $\mathrm{Gal}(K/\mathbb{Q})$ that fixes $\mathfrak{p}$, we would have succeded in describing the roots of Φ in terms of the Galois action.

Let $P \in \mathcal{O}_K$ be a representative of $[P]$, and consider its minimal polynomial

$$f_P(x) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} x - \sigma(P) \in \mathcal{O}_K[x].$$

With this, one has that

$$\begin{aligned} f_P(P)^p \pmod{\mathfrak{p}} &\equiv f_P(P^p) \pmod{\mathfrak{p}} \\ &\equiv \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} P^p - \sigma(P) \pmod{\mathfrak{p}} \\ &\equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

As $[P]$ is a generator of $\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p$:

Proposition 1.29. *There is some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(x) \equiv x^p \pmod{\mathfrak{p}}$ for all $x \in \mathcal{O}_K$. In particular, $\sigma(P) \equiv P^p \not\equiv 0 \pmod{\mathfrak{p}}$.*

Now, we prove that $\sigma \in D_{\mathfrak{p}}$, that is $\sigma(\mathfrak{p}) = \mathfrak{p}$, or equivalently, that $\sigma^{-1}(\mathfrak{p}) = \mathfrak{p}$. If not, $\mathfrak{p}$ and $\sigma^{-1}(\mathfrak{p})$ are coprime ideals, so the Chinese Remainder Theorem shows there is a solution to the system

$$\begin{aligned} x &\equiv 0 \pmod{\sigma^{-1}(\mathfrak{p})} \\ x &\equiv P \pmod{\mathfrak{p}}. \end{aligned}$$

Applying σ to the first congruence one obtains that

$$\sigma(x) \equiv \sigma(0) \pmod{\sigma\sigma^{-1}(\mathfrak{p})} \implies \sigma(P) \equiv 0 \pmod{\mathfrak{p}},$$

which is contradictory with the Proposition above. Thus:

Proposition 1.30. *All the roots of Φ are obtained by successive applications of an automorhpism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, which modulo $\mathfrak{p}$ acts as $x \mapsto x^p$.*

By Fermat's Theorem,

$$\sigma^{\circ f}(x) \equiv x^{p^f} \equiv x \pmod{\mathfrak{p}},$$

and Hilbert recognizes that the automorphisms that fix $\mathcal{O}_K/\mathfrak{p}$ pointwise are a group, which he calls the *inertia group* (*Trägheüsgruppe*) of $\mathfrak{p}$, and writes as g_t. We shall use the modern notation,

$$I_{\mathfrak{p}} := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q})\colon \sigma(x) \equiv x \pmod{\mathfrak{p}}, \text{ for all } x \in \mathcal{O}_K\}.$$

We shall prove:

Proposition 1.31. *$I_{\mathfrak{p}}$ is a subgroup of $D_{\mathfrak{p}}$.*

Demostración. Firstly, note that $I_{\mathfrak{p}}$ is not empty, as it contains $\mathrm{id}_{\mathrm{Gal}(K/\mathbb{Q})}$. Now, given $\sigma \in I_{\mathfrak{p}}$, then for all $x \in \mathfrak{p}$ one has that

$$x \equiv 0 \pmod{\mathfrak{p}} \implies \sigma(x) \equiv 0 \pmod{\mathfrak{p}},$$

that is, $\sigma(x) \in \mathfrak{p}$, so $\sigma(\mathfrak{p}) \subseteq \mathfrak{p}$. But ring morphisms map prime ideals to prime ideals, and these, by definition don't have any proper ideals, so it must be that $\sigma(\mathfrak{p}) = \mathfrak{p}$.

To finish, we must prove that for any $\sigma, \tau \in I_{\mathfrak{p}}$, it holds that $\sigma\tau^{-1} \in I_{\mathfrak{p}}$. Let $\alpha \in \mathcal{O}_K$, and note

$$\begin{aligned} \sigma\tau^{-1}(\alpha) - \alpha &\equiv \sigma\tau^{-1}(\alpha) - \tau\tau^{-1}(\alpha) \pmod{\mathfrak{p}} \\ &\equiv \tau^{-1}(a) - \tau^{-1}(a) \pmod{\mathfrak{p}} \\ &\equiv 0 \pmod{\mathfrak{p}}, \end{aligned}$$

so $\sigma\tau^{-1}(\alpha) \equiv \alpha \pmod{\mathfrak{p}}$, which proves that indeed $\sigma\tau^{-1}$ fixes $\mathcal{O}_K/\mathfrak{p}$ pointwise. □

1.8. Modern approach to ramification

Let $K/\mathbb{Q}$ be a number field. Any prime number $p \in \mathbb{Z}$ defines a prime ideal $\mathfrak{p} := p\mathcal{O}_K$ of $\mathcal{O}_K$. In particular, we may write the unique factorization

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \quad \mathfrak{p}_i \ni p \text{ prime ideal of } \mathcal{O}_K. \tag{1.8}$$

Any of the $\mathfrak{p}_i$ is said to *be over p*. Depending on this factorization, the following terminology is adopted:

1. If $p\mathcal{O}_K$ remains prime (as an ideal of $\mathcal{O}_K$), then we say it is *inert* in k. In this case, in its factorization will appear only one prime (that is, $g = 1$), and with exponent 1.

2. If not, $p\mathcal{O}_K$ will factor. If said factorization is not square-free (some e_i is greater that 1), we say that *p ramifies*. Particularly, if there is only one prime with exponent $e = [K : \mathbb{Q}]$, we say that *p ramifies completely* in K.

3. If the factorization is square-free (all the e_i are 1), we say that *p unramified* in K.

Each exponent e_i is called the *ramification index of p in $\mathfrak{p}_i$*. In case we need to emphasize that this index depends on both p and $\mathfrak{p}_i$ we shall write it as $e_{\mathfrak{p}_i|p}$. In the context of ramification, the ideal norm of $\mathfrak{p}_i$ is called the *inertia degree of p in $\mathfrak{p}_i$*, and written as f_i—and $f_{\mathfrak{p}_i|p}$ if needed.

Thus, to determine whether primes split, and how they do so, one may study the numbers e_i, f_i, and g, which can be done via standard counting arguments.

For instance, using the multiplicativity of the ideal norm, and that $\mathrm{N}(p\mathcal{O}_K) = \mathrm{N}(p\mathbb{Z})^{[K:\mathbb{Q}]}$, we may deduce that

$$\begin{aligned} \mathrm{N}(p\mathcal{O}_K) &= \mathrm{N}\left(\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}\right) \\ &= \prod_{i=1}^{g} \mathrm{N}(\mathfrak{p}_i)^{e_i} \\ &= \prod_{i=1}^{g} \mathrm{N}(p\mathbb{Z})^{f_i e_i} \\ &= \mathrm{N}(p\mathbb{Z})^{\sum_{i=1}^{g} e_i f_i}. \end{aligned}$$

Comparing exponents yields:

Proposition 1.32. *Let $K/\mathbb{Q}$ be a number field. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_g \subseteq \mathcal{O}_K$ are the prime ideals over a prime number $p \in \mathbb{Z}$, then*

$$[K : \mathbb{Q}] = \sum_{i=1}^{g} e_i f_i.$$

Further counting arguments may be done in prescence of a group acting in $\mathcal{O}_K$. By excelence, the groups of choice that act naturally in this context are Galois groups. Thus, from now on, we will assume $K/\mathbb{Q}$ is Galois, case in which:

Proposition 1.33. *Given a Galois number field $K/\mathbb{Q}$, the group* $\mathrm{Gal}(K/\mathbb{Q})$ *acts upon $\mathcal{O}_K$.*

Demostración. For given $\alpha \in \mathcal{O}_K$ with minimal polynomial f_α, and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, one has that $\sigma(\alpha)$ is a root of the polynomial $\sigma(f_\alpha)$ (defined coefficient-wise by $\mathbb{Q}$-linearity), which has rational integer coefficients, as σ fixes $\mathbb{Q} \supseteq \mathbb{Z}$. □

Just as in rational number theory we study the quotients $\mathbb{Z}/p\mathbb{Z}$, a fairly natural pathway is to study the quotients $\mathcal{O}_K/\mathfrak{p}$. The action of $\mathrm{Gal}(K/\mathbb{Q})$ does not descend into said quotient, as for that it must fix $\mathfrak{p}$ beforehand. Hence, we may consider the action of the stabilizer of $\mathfrak{p}$, which will be well-defind. The set $D_\mathfrak{p}$ of automorphisms that fix a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ is called the *decomposition group* of $\mathfrak{p}$ in K. It is an actual group, for it is a stabilizer:

$$D_\mathfrak{p} := \mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \colon \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

This way, $D_\mathfrak{p}$ clearly acts in $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$.

Recall that any prime $p \in \mathbb{Z}$ and prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ over p define a finite field extension $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$. And as $D_\mathfrak{p}$ fixes p (as it lies inside $\mathfrak{p}$), and fixes $\mathbb{Z}$ (lies inside $\mathbb{Q}$), it also fixes $\mathbb{F}_p$. So $D_\mathfrak{p}$ acts by shuffling $\mathbb{F}_\mathfrak{p}$ while fixing $\mathbb{F}_p$. As any finite extension of a finite field is Galois, the action of $D_\mathfrak{p}$ upon $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$ induces a group morphism

$$\begin{aligned} \Phi \colon D_\mathfrak{p} &\longrightarrow \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p) \\ \sigma &\longmapsto ([\alpha] \mapsto [\sigma(\alpha)]). \end{aligned}$$

The kernel of this action is

$$\begin{aligned}\ker\Phi &= \{\sigma \in D_{\mathfrak{p}} \colon [\sigma(\alpha)] = \alpha \text{ for all } [\alpha] \in \mathbb{F}_{\mathfrak{p}}\}\\ &= \{\sigma \in D_{\mathfrak{p}} \colon \sigma(\alpha) \equiv \alpha \quad \text{mód } \mathfrak{p} \text{ for all } \alpha \in \mathcal{O}_K\}.\end{aligned}$$

In this context, it is called the *inertia group of* $\mathfrak{p}$ *in* K, and it is written as $I_{\mathfrak{p}}$. By the First Isomorphism Theorem, we obtain an injective morphism

$$\tilde{\Phi}\colon D_{\mathfrak{p}}/I_{\mathfrak{p}} \longrightarrow \operatorname{im}\Phi,$$

but it turns out Φ is surjective:

Proposition 1.34. *Let $K/\mathbb{Q}$ be a number field, $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal over a rational prime $p \in \mathbb{Z}$. The action map $\Phi\colon D_{\mathfrak{p}} \to \operatorname{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is surjective.*

Demostración. We shall use the Primitive Element Theorem, to establish some $[\theta] \in \mathbb{F}_{\mathfrak{p}}$ such that $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_p([\theta])$. Let $\gamma \in \operatorname{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$. Firstly, we show there is some $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ that coincides with γ modulo $\mathfrak{p}$. Consider $\theta \in K$ any representative of $[\theta]$, and let $f_\theta \in \mathbb{Q}[x]$ be the minimal polynomial of θ in $K/\mathbb{Q}$, so its roots are the different $\sigma(\theta)$ for $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$. Modulo $\mathfrak{p}$, the polynomial $[f_\theta] \in \mathbb{F}_p[t]$ has as roots the $[\sigma(\theta)]$, and, while it is not the minimal polynomial of $[\theta]$—which has $\gamma([\theta])$ as a root—surely it is divisible by it. So, in particular, $\gamma([\theta])$ is a root of $[f_\theta]$, hence it must coincide with one of the $[\sigma(\theta)]$, as claimed. Call this $[\sigma_0]$

Now, we prove that $\sigma_0 \in D_{\mathfrak{p}}$, that is, $\sigma_0(\mathfrak{p}) = \mathfrak{p}$, or equivalently, that $\mathfrak{p} = \sigma_0^{-1}(\mathfrak{p})$. If not, then $\mathfrak{p}$ is coprime to $\sigma_0^{-1}(\mathfrak{p})$, so the Chinese Remainder Theorem shows there is a solution $\theta_0 \in \mathcal{O}_K$ to the system

$$\begin{aligned} x &\equiv 0 \quad (\text{mód } \sigma_0^{-1}(\mathfrak{p}))\\ x &\equiv \theta \quad (\text{mód } \mathfrak{p})\end{aligned}$$

Applying σ_0 to the first congruence, and then using thea second one, we obtain that

$$\sigma_0(\theta_0) \equiv 0 \equiv \theta \quad (\text{mód } \mathfrak{p}),$$

which cannot be as θ is a primitive root modulo $\mathfrak{p}$, hence non-zero modulo $\mathfrak{p}$.

So, we have found an automorphism $\sigma_0 \in D_{\mathfrak{p}}$ that, modulo $\mathfrak{p}$, acts as the given γ at $[\theta]$. But $[\theta]$ is a primitive root, so by $\mathbb{F}_p$-linearity said action extends to all of $\mathbb{F}_{\mathfrak{p}}$. Hence, Φ not only maps $\sigma_0(\alpha) \mapsto [\gamma(\alpha)]$, but $\sigma_0 \mapsto \gamma$, as needed. □

So Φ in fact defines an isomorphism $D_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \operatorname{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$, which proves that the quotient is also cyclic. As we have the group group inclusions

$$\{1\} \longrightarrow I_{\mathfrak{P}} \longrightarrow D_{\mathfrak{p}} \longrightarrow \operatorname{Gal}(K/\mathbb{Q}),$$

the Galois correspondence gives a tower of fields

$$\mathbb{Q} \subseteq K^{D_{\mathfrak{p}}} \subseteq K^{I_{\mathfrak{p}}} \subseteq K.$$

The intermediate fields are called the *decomposition field* and the *inertia field* of $\mathfrak{p}$, respectively.

1.9. Higher ramification

The construction of the inertia group was generalized by Hilbert by considering the automorphisms that fix elements modulo powers of $\mathfrak{p}$, namely, he defined

$$V_j := \left\{\sigma \in \mathrm{Gal}(K/\mathbb{Q})\colon \sigma\alpha \equiv \alpha \quad \text{mód } (\mathfrak{p}^{j+1}) \text{ for all } \alpha \in \mathcal{O}_K\right\}$$

for all $j \geq 0$, and calling them the *j-th ramification groups.*

Proposition 1.35. *Let $K/\mathbb{Q}$ be a of number field. For any prime $\mathfrak{p} \subseteq \mathcal{O}_K$, the quotient $I_\mathfrak{p}/V_1$ is (isomorphic to) a subgroup of $(\mathbb{F}_\mathfrak{p})^\times$, hence it is cyclic of order dividing $|\mathbb{F}_\mathfrak{p}|-1$. For $j \geq 1$, each quotient V_j/V_{j+1} is (isomorphic to) a subgroup of $\mathbb{F}_p$ (as an additive group). In particular, if $\operatorname{char} \mathbb{F}_\mathfrak{p} = p$, said quotients are products of cyclic groups of order p (or trivial).*

Referencias

[1] Jeremy Avigad. Dedekind's 1871 version of the theory of ideals, 2004. `https://www.andrew.cmu.edu/user/avigad/Papers/ideals71.pdf`.

[2] R. Dedekind. Sur la théorie des nombres entiers algébriques. *Bulletin des Sciences Mathématiques et Astronomiques*, 11:278–288, 1876.

[3] Richard Dedekind. *Über die discriminanten endlicher Körper*, volume 29. Dieterich, 1882.

[4] Richard Dedekind. Über einen arithmetischen satz von Gauss. *Mitteilungen der Deutschen Mathematischen Gesellschaft in Prag*, pages 1–11, 1892. Also published in *Werke*, Vol. 2, pp. 28–38.

[5] Richard Dedekind. *Theory of algebraic integers.* Cambridge mathematical library. Cambridge University Press, 1996.

[6] Richard Dedekind and Heinrich Weber. *Theory of algebraic functions of one variable.* History of Mathematics. London Mathematical Society, Providence, Rhode Island, 2012.

[7] Peter Gustav Dirichlet and Richard Dedekind. *Vorlesungen über Zahlentheorie.* Vieweg, Braunschweig, 1863.

[8] Peter Gustav Dirichlet and Richard Dedekind. *Lectures on number theory.* History of mathematics. American Mathematical Society; London Mathematical Society, Providence, RI: [London], 1999.

[9] Harold M. Edwards. The genesis of ideal theory. *Archive for History of Exact Sciences*, 23(4):321–378, 1980.

[10] Harold M. Edwards. *Fermat's last theorem: a genetic introduction to algebraic number theory.* Graduate texts in mathematics. Springer, New York, corr. 5th print edition, 1996.

[11] Leonhard Euler, Joseph-Louis Lagrange, and Johann Bernoulli. *Vollständige Anleitung zur Algebra.* Kayserliche Academie der Wissenschaften, 1771. First part: VII pages, 256 pages; second part: I page, 384 pages, 8 pages appendix.

[12] Carl Friedrich Gauss. *Disquisitiones Arithmeticae.* In commissis libraria Schäferi, Gottingae, 1801.

[13] Carl Friedrich Gauss. *Theoria Residuorum Biquadraticorum Commentatio Secunda*, pages 93–148. Cambridge Library Collection - Mathematics. Cambridge University Press, 1832.

[14] Emmylou Haffner. Strategical use(s) of arithmetic in richard dedekind and heinrich weber's theorie der algebraischen funktionen einer veränderlichen. *Historia Mathematica*, 44(1):31–69, 2017.

[15] Harris Hancock. *Foundations of the Theory of Algebraic Numbers*, volume II. Dover Publications, New York, 2. ed edition, 1964.

[16] David Hilbert. Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 4:175–546, 1897.

[17] David Hilbert. *Grundzüge einer Theorie des Galoisschen Zahlkörpers*, pages 13–23. Springer Berlin Heidelberg, Berlin, Heidelberg, 1932.

[18] David Hilbert. *The Theory of Algebraic Number Fields.* Springer-Verlag, Berlin, New York, 1998.

[19] E. E. Kummer. De numeris complexis, qui radicibus unitatis et numeris integris realibus constant. *Gratulationschrift der Univ. Breslau zur Jubelfeier der Univ. Königsberg; reprint, Journal de Mathématiques Pures et Appliquées*, 12:185–212, 1847. Also reprinted in [K4], 165–192.

[20] Ernst Eduard Kummer. Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers. *Journal de Mathématiques Pures et Appliquées*, 16:377–498, 1851.

[21] Gabriel Lamé. Démonstration générale de théorème de fermat, sur l'impossibilité. en nombres entiers, de l'équation $x^n + y^n = z^n$. *Comptes rendus des séances de l'Académie des sciences*, pages 310–316, 1847.

[22] Daniel A. Marcus. *Number Fields.* Universitext. Springer International Publishing: Imprint: Springer, Cham, 2nd ed. 2018 edition, 2018.

[23] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[24] Samuel Runyeon. Cyclotomic fields and Fermat's Last Theorem, 2021.

[25] John Stillwell. What are algebraic integers and what are they for? *The American Mathematical Monthly*, 101(3):266–270, 1994.

[26] H. Weber and R. Dedekind. Theorie der algebraischen functionen einer veränderlichen. *Journal für die reine und angewandte Mathematik*, 92:181–290, 1882.