Fermat's Last Theorem

Víctor Blasco Jiménez

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Director del trabajo: Alberto C. Elduque Palomo
23 de junio de 2020

Abstract

Fermat's last theorem states that the equation $x^n + y^n = z^n$ does not have any non-trivial integral solution. In this work we will show the general setting of this theorem and discuss the principal ideas of Kummer's approach and the most natural relations between the mathematical objects that are behind it, which will allow us to understand the proof of the cases $n = p$, with p regular prime. Finally, we will give a short comment about the relations between elliptic curves and modular forms that allowed Andrew Wiles to achieve a general and definitive proof for Fermat's conjecture.

Acknowledgements

First of all, I would sincerely like to thank my advisor Alberto Elduque for choosing this nice topic for me and for being very helpful with any problem or question I had. Also, I would like to thank Müge Kanuni from Düzce University for being a second mother for me during this year and for valuing me as a student. Thanks to all the people who always enjoy having a conversation about maths, specially to my friends Miguel, Javi and Abel. Thank you Sergio for every moment we have spent together and for showing me the way to get better. Thanks to my parents and my sister for believing in me.

Resumen

El objetivo de este trabajo es introducir los conceptos necesarios para entender la demostración del Último Teorema de Fermat para el caso de primos regulares. La mayor parte de las nociones nuevas que explicaremos aparecen de forma natural a la hora de tratar con problemas algebraicos relacionados con la teoría de anillos conmutativos y las extensiones finitas de cuerpos, las cuales han sido objeto de estudio en las asignaturas de Estructuras algebraicas, Grupos y Teoría de Galois impartidas en el grado de matemáticas de la Universidad de Zaragoza. Por ello, se ha intentado que todo lo ilustrado aquí sea accesible a cualquier estudiante de matemáticas con un conocimiento básico sobre estos temas. Debido a eso mismo, este trabajo está más focalizado en discutir las ideas fundamentales que rodean al Último Teorema de Fermat, y establecer las relaciones más generales entre ellas, que en comprender de manera exhaustiva cada una de las mismas.

En la introducción se hará un breve comentario sobre los orígenes del Último Teorema de Fermat y los intentos y métodos empleados para resolver ciertos casos particulares, como el caso $n = 3$ o $n = 4$. Se mencionará además, de manera esquemática, las ideas que permitieron a Ernst Kummer demostrar el Último Teorema de Fermat para el caso de primos regulares.

El capítulo primero lo empezaremos con un breve repaso de los conceptos básicos de la teoría algebraica de números, como lo son los números algebraicos y los polinomios mínimos asociados a ellos, así como las relaciones entre estos y las extensiones finitas de cuerpos. Después introduciremos los enteros algebraicos, más concretamente, el anillo de enteros de un cuerpo de números, y describiremos la norma de un número algebraico y el discriminante de un cuerpo de números como objetos que permiten "trasladar" información de una estructura matemática más o menos compleja a otra más simple.

En el capítulo segundo tomaremos un nivel mayor de abstracción. Repasaremos nociones básicas de la teoría de anillos, tales como dominio de integridad o ideal, y generalizaremos estos últimos definiendo lo que se viene a llamar un ideal fraccionario. Esto nos permitirá hablar de dominios de Dedekind, definidos como dominios de integridad en los cuales cualquier ideal fraccionario no nulo es invertible, y estudiar propiedades de ellos relacionadas con la factorización de sus ideales y elementos. En concreto, probaremos que cualquier ideal no nulo de un dominio de Dedekind factoriza de manera única como producto de ideales primos. Veremos que cada anillo de enteros es un dominio de Dedekind, y acabaremos definiendo el grupo de clase H_K de un cuerpo de números K como cierto cociente de su grupo de ideales fraccionarios, probando su finitud.

En el capítulo tercero introduciremos la noción de primo regular. Concretamente, se dice que un número primo p impar es regular si no divide el orden del grupo de clase del cuerpo $\mathbb{Q}(\zeta_p)$, donde ζ_p es una raíz distinta de 1 del polinomio $x^p - 1$. Veremos que el anillo de enteros de $\mathbb{Q}(\zeta_p)$ es precisamente $\mathbb{Z}[\zeta_p]$. Después de estudiar las características generales de este anillo a partir de los resultados de los capítulos anteriores, mencionaremos los enunciados técnicos necesarios para poder demostrar el primer caso del Último Teorema de Fermat para primos regulares, y expondremos una demostración del mismo.

En el capítulo cuarto haremos un breve repaso de las ideas que fundamentan la llamada teoría de cuerpos de clases, tales como la ramificación de un ideal primo de un anillo de enteros en otras ex-

tensiones y la existencia del cuerpo de clases de Hilbert. Definiremos el discriminante relativo de una extensión finita de cuerpos de números, como generalización del discriminante anteriormente introducido, y veremos su relación con las ramificaciones de ideales primos de $\mathbb{Z}$ en $\mathbb{Z}[\zeta_p]$ y de $\mathbb{Z}[\zeta_p]$ en cualquier extensión finita que lo contenga. Esto nos permitirá demostrar una versión débil del Lemma de Kummer sobre las unidades de $\mathbb{Z}[\zeta_p]$ y, con ello, mostrar una demostración del segundo caso del Último Teorema de Fermat para primos regulares.

Finalmente, en el último capítulo esbozaremos de manera esquemática los objetos matemáticos e ideas que permitieron obtener una demostración general del Último Teorema de Fermat.

Contents

Chapter 0

Introduction

Fermat's Last Theorem is probably the most famous theorem of all time. Since its origins in the early 17^{th} century until mathematicians found a definitive proof for it, more than 350 years passed and many mathematical objects which we are nowadays used to work with were introduced or developed in order to find a solution to that problem.

Fermat's Last Theorem was firstly stated as a conjecture in 1637 by Pierre de Fermat, a jurist and an amateur mathematician, while he was reading the classic text of mathematics *Arithmetica* from Diophantus of Alexandria. In that book he found a page were Pythagoras's Theorem was explained and Fermat asked himself if that theorem could be extended somehow. Euclides's Theorem tells us that any solution to the equation $x^2+y^2=z^2$ with pairwise coprime natural numbers x,y,z is, after a possible permutation of x and y, of the form $x=2rs,\ y=r^2-s^2,\ z=r^2+s^2$, where r,s are coprime, $r>s$ and exactly one of them is odd. Therefore, there are infinitely many non-trivial solutions to the equation $x^2+y^2=z^2$, where $x,y,z\in\mathbb{Z}$. So Fermat wondered about what may happen if we change the exponent 2 by another different natural number. After playing a bit with the equation he claimed that in fact there are no non-trivial solutions in $\mathbb{Z}$ for any natural number greater or equal than 3. More formally: If $0\neq x,y,z\in\mathbb{Z}$ then the equation

$$x^n+y^n=z^n$$

does not have a solution for any natural number $n\geq 3$. He realised that if his conjecture was true for some natural number n then it should be true for any multiple m of it. For that let $m=nr$ and assume the conjecture is false for m, that is the equation $x^m+y^m=z^m$ has a non-trivial solution. If that happens, then $(x^r)^n+(y^r)^n=(z^r)^n$ is a solution for n, which contradicts the conjecture being true for n. From this argument he deduced that in order to prove his conjecture he should only focus on the cases $n=4$ and $n=p$ odd prime number. In fact, he claimed to have found a method for proving all the cases, but no one has ever found any evidence of this fact. Anyway, by using an infinite descent argument he proved correctly the case $n=4$. We show the proof here.

Theorem 0.1. *If $0\neq x,y,z\in\mathbb{Z}$ then the equation $x^4+y^4=z^4$ does not have a solution.*

Proof. It is enough to prove that there are no solutions to the equation $x^4+y^4=z^2$ because if there is a solution to $x^4+y^4=z^4$ then x,y,z^2 is a solution for the first equation. As every exponent is even we may assume x,y,z positive integers. We can also assume x,y,z pairwise relatively prime because if there is a prime number dividing two of them then it must divide the other one, so we can take that factor out.

Let's take a solution (x,y,z) of mimimal z. By Euclides's Theorem we have

$$x^2=r^2-s^2,\ y^2=2rs,\ z=r^2+s^2$$

where x,z are odd, y is even and r,s are coprime. We have $x^2=r^2+s^2$ with x,s coprime because otherwise r,s would have a common factor. Thus, by Euclides's Theorem again we get, since x is odd,

$$x^2=a^2-b^2,\ s=2ab,\ r=a^2+b^2$$

with a, b coprime positive integers. If we substitute it in $y^2 = 2rs$ we get $y^2 = 4ab(a^2+b^2)$, so y must be even. Let's write $y = 2k$, then we have $k^2 = ab(a^2+b^2)$. But, since a, b, a^2+b^2 are pairwise relatively prime and $ab(a^2+b^2)$ is a square we must have $a = c^2,\ b = d^2,\ a^2+b^2 = e^2$ for some c, d, e pairwise relatively prime. Therefore, substituting we get

$$e^2 = a^2 + b^2 = c^4 + d^4$$

which is a solution to $x^4 + y^4 = z^2$. But $e = a^2 + b^2 = r < z$, as $z = r^2 + s^2$, which contradicts the mimimality of z. □

More than one century after Fermat's discovery, Leonhard Euler gave several proofs for the case $p = 3$. In one of those proofs, while studying the possible factorization of the equation $x^3 + y^3 = z^3$, Euler used complex numbers of the form $x + 3iy$, where $x, y \in \mathbb{Z}$, which helped him to solve the problem. However, the proof contained some gaps because he was assuming properties of these numbers as if they were ordinary integers. More concretely, by the Fundamental Theorem of Arithmetic, we know that every element $0 \neq z \in \mathbb{Z}$ can be factored uniquely, up to the order of the factors, as $z = up_1^{r_1}...p_s^{r_s}$, where each p_i is a different prime number and u is an invertible element in $\mathbb{Z}$. Recall that the only invertible elements in $\mathbb{Z}$ are ± 1. Euler did not realise that but in his proof he was using the same property of the factorization in $\mathbb{Z}$ but in the ring $\mathbb{Z}[i] := \{a + bi :\ a, b \in \mathbb{Z}\}$. In fact this property holds in $\mathbb{Z}[i]$ but Euler did not realise he needed to prove it in order to prove his theorem.

In the more general case, given a ring R, any invertible element is called a unit. Also, we say that an element $0 \neq p \in R$ is prime if p is not a unit and whenever p divides ab for some $a, b \in R$, then either p divides a or p divides b. The property of factorization that holds in particular in $\mathbb{Z}$ and in $\mathbb{Z}[i]$ can be stated as follows:

Definition. *Let R be a ring which is commutative, unital $(1 \in R)$ and with the property that whenever $ab = 0$, then either $a = 0$ or $b = 0$. Then we say that R is a unique factorization domain (UFD) if every $0 \neq a$ factors uniquely as $a = up_1^{r_1}...p_s^{r_s}$, where u is a unit of R and each p_i is a distinct prime element of R.*

Anyway, Euler gave another proof just using elementary notions and an infinite descent argument, so from that moment on mathematicians could focus only on the case $n = p$, with p prime grater or equal than 5. However, the problem is still complicated because there are infinitely many primes, so it would be nice to find more general methods to solve it. It was the mathematician Sophie Germain the first one to do it. She found it convenient to divide the problem into two cases:

$$1.\ p \nmid x, y, z$$

$$2.\ p | x \text{ and } p \nmid y, z$$

As Fermat realised, if $p|x, y$ then p must divide z and we can take the factor p out. Also, as p is odd, if (a, b, c) is a solution for $x^p + y^p = z^p$, then $(a, b, -c)$ is a solution for $x^p + y^p + z^p = 0$ and viceversa, so the equation is symmetric and we can assume $p|x$. Therefore, if mathematicians were able to prove both cases, Fermat's Last Theorem would be finally solved. She proved the first case for all prime numbers $p \leq 97$. Legendre proved the second case for $p = 5$ using ideas on Dirichlet, and Gabriel Lamé proved the case $p = 7$.

On 1 March 1847, Lamé adressed the Paris Academy and announced a complete proof of Fermat's Last Theorem and explained it to his colleagues. He had factorized the equation $x^p + y^p = z^p$ as

$$(x + y)(x + \zeta_p y)...(x + \zeta_p^{p-1}) = z^p$$

where $1 \neq \zeta_p$ is root of the polynomial $x^p - 1$ and claimed that any of those linear factors was prime to the others. From that fact he derived a contradiction. While checking the proof, Liouville pointed out that in his argument he was assuming that $\mathbb{Z}[\zeta_p]$ was UFD for any odd prime, and that may not be true.

In fact, three years before the german mathematician Ernst Kummer showed that for $p = 23$ the ring $\mathbb{Z}[\zeta_p]$ is not UFD so Lamé argument failed.

In 1850 Kummer produced a very nice proof for what he called "regular primes". It was the most important step taken in 200 years since Fermat stated his conjecture. In order to prove that, Kummer wondered if some good properties of factorization in $\mathbb{Z}$ could be extended to some $\mathbb{Z}[\zeta_p]$. He defined the concept of "ideal number", what was further developed by Dedekind as the notion of ideal of a ring we are used to, and proved that even if we cannot talk about the unique factorization of elements in $\mathbb{Z}[\zeta_p]$ we can say somehow that its ideals factor uniquely. Recall that any ζ_p is a root of the monic polynomial $x^p - 1 \in \mathbb{Q}[x]$ and the polynomial ring is an Euclidean domain, meaning that we have division algorithm for its elements in a similar way we do in $\mathbb{Z}$, so it is a nice polynomial ring to work with. In fact, given any root α of a monic polynomial $p(x) \in \mathbb{Q}[x]$ we can define the field $\mathbb{Q}(\alpha)$. This field contains $\mathbb{Q}$ so it is a field extension of it. Kummer worked in field extensions of $\mathbb{Q}$ of the form $\mathbb{Q}(\zeta_p)$ because $\mathbb{Z}[\zeta_p] \subset \mathbb{Q}(\zeta_p)$, and revealed valuable information of those domains. This led him to introduce the notion of the class group of a field of the form $\mathbb{Q}(\zeta_p)$ and define what is called a regular prime.

We will introduce all the necessary concepts to understand Kummer's approach and study them in a more general way. After that, we will be able to prove Fermat's Last Theorem for regular primes.

Chapter 1

The ring of integers of a number field

We start by doing a review of some basic concepts of algebraic number theory. Then we will introduce the ring of integers of a number field and see some properties of it.

Definition. *Given a subfield K of $\mathbb{C}$, an element $\alpha \in \mathbb{C}$ is said to be algebraic over K if $\exists p(x) \in K[x]$ monic such that $p(\alpha) = 0$. If $K = \mathbb{Q}$ we say that α is an algebraic number.*

Example 1. *$\sqrt{2}$ is an algebraic number, as $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbb{Q}[x]$, but for example π is not, as it is not a root of any polynomial in $\mathbb{Q}$.*

For any algebraic number α we denote by $\mathbb{Q}(\alpha)$ the smallest field that contains $\mathbb{Q}$ and α. It can be checked that $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(p(x))$ as fields, where $(p(x))$ is the maximal ideal generated by $p(x)$ and $p(x)$ is the unique monic irreducible polynomial over $\mathbb{Q}$ of minimal degree satisfying $p(\alpha) = 0$. In that case, $p(x)$ is called the minimum polynomial of α over $\mathbb{Q}$.

Having now that $\mathbb{Q}(\alpha)$ is a field , which contains $\mathbb{Q}$ by definition, we can see $\mathbb{Q}(\alpha)$ as a field extension of $\mathbb{Q}$ and also as a vector space over $\mathbb{Q}$. We denote $[\mathbb{Q}(\alpha) : \mathbb{Q}] = dim_{\mathbb{Q}}\mathbb{Q}(\alpha)$.

Lemma 1.1. *([2, 1.4]) For any algebraic number α, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n = deg(p(x))$ where $p(x)$ is its minimum polynomial over $\mathbb{Q}$.*

In Example 1 we can see that $p(x) = x^2 - 2$ is the minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ because otherwise $p(x)$ should have degree 1, which is impossible since $\sqrt{2} \notin \mathbb{Q}$. At the same time, as $(\sqrt{2})^2 = 2 \in \mathbb{Q}$, we have $\mathbb{Q}(\alpha) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, so $dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}) = 2 = deg(x^2 - 2)$.

On the other hand, we have said that π is not an algebraic number, which actually depends on the fact that $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. This led us to characterize algebraic numbers in terms of finite field extensions of $\mathbb{Q}$.

Proposition 1.2. *([3, Thm 1.11]) An element $\alpha \in \mathbb{C}$ is an algebraic number if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$.*

We call $\overline{\mathbb{Q}}$ the set of algebraic numbers. For any $\alpha, \beta \in \overline{\mathbb{Q}}$, we have $\alpha + \beta, \alpha\beta, \alpha^{-1}, \beta^{-1} \in \mathbb{Q}(\alpha, \beta)$, which is a finite field extension of $\mathbb{Q}$, so we get:

Theorem 1.3. *([3, Thm 2.1]) $\overline{\mathbb{Q}}$ is a field.*

Definition. *A subfield K of $\mathbb{C}$ is called a number field if $[K : \mathbb{Q}] < \infty$.*

By Proposition 1.2 this implies $K \subset \overline{\mathbb{Q}}$, in other words, $K = \mathbb{Q}(\alpha_1, ..., \alpha_m)$ for some $m \in \mathbb{N}$, where $\alpha_i \in \overline{\mathbb{Q}}$ $\forall i = 1, ..., m$. Using induction on m we can prove the following:

Theorem 1.4. *([3, Thm 2.2]) If K is a number field then $K = \mathbb{Q}(\theta)$ for some $\theta \in \overline{\mathbb{Q}}$.*

Remark. *As a finite dimensional vector space over $\mathbb{Q}$, a $\mathbb{Q}$-basis of a number field $K = \mathbb{Q}(\theta)$ exists in the natural sense. If $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, $\{1, \theta, ..., \theta^{n-1}\}$ is a common basis to work with.*

As we have said, any number field $K = \mathbb{Q}(\theta)$ is isomorphic to $\mathbb{Q}[x]/(p(x))$, where $p(x)$ is the minimum polynomial of θ over $\mathbb{Q}$. The study of these number fields in terms of groups of permutations acting on the roots of their respective associated irreducible polynomials is a part of an abstract algebraic theory known as Galois Theory, in honor to the mathematician Évariste Galois, who was the first one to take this approach. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ of a number field K is exactly
$\mathrm{Aut}K := \{\sigma : K \to K : \sigma \text{ isomorphism}\}$. The next theorem relates the number of elements in $\mathrm{Gal}(K/\mathbb{Q})$ with $[K : Q]$.

Theorem 1.5. *Let $K = \mathbb{Q}(\theta)$ be a number field with $[K : Q] = n$. Then there are exactly n different monomorphisms $\sigma_i : K \to \mathbb{C}$. The elements $\sigma_i(\theta) = \theta_i$ are the distinct zeros of $p(x)$, where $p(x)$ is the minimum polynomial of θ over $\mathbb{Q}$.*

Proof. First recall that as $p(x)$ is monic of minimal degree then it is irreducible, that is it cannot be factored into two non-constant polynomials of degree less than n. As the characteristic of $\mathbb{Q}$ is 0, we know that every irreducible polynomial over $\mathbb{Q}$ is separable, that is, all its roots are distinct. So call $\theta_1, ..., \theta_n$ the different roots of $p(x)$. Given any θ_i with $p_i(x)$ its minimum polynomial, then
$0 = p_i(\theta_i) = p(\theta_i)$. Recall that $\mathbb{Q}[x]$ is an Euclidean Domain, so we can apply division algorithm. Using the fact that $p_i(x)$ is monic of minimal degree we get $p_i(x)|p(x)$ and $p(x)$ monic and irreducible implies $p_i(x) = p(x), \forall i = 1, ..., n$. So we have $\mathbb{Q}(\theta_i) \cong \mathbb{Q}[x]/(p_i(x)) = \mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}(\theta)$, hence they are isomorphic. So given any field isomorphism $\sigma : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ as $\sigma(1) = 1$ and $\sigma(a+b) = \sigma(a) + \sigma(b)$ we have $\sigma(n) = n \ \forall n \in \mathbb{N}$, and as $\sigma(\frac{1}{n}) = (\sigma(n))^{-1}$ we deduce $\sigma(q) = q \quad \forall q \in \mathbb{Q}$. Therefore, as $\mathbb{Q}(\theta), \mathbb{Q}(\theta_i)$ can be seen as $\mathbb{Q}$-vector spaces with basis $\{1, \theta, ..., \theta^{n-1}\}$,$\{1, \theta_i, ..., \theta_i^{n-1}\}$ respectively, σ is determined by the value of $\sigma(\theta)$. From here it is easy to see that, for $i = 1, ..., n$, each $\sigma(\theta) = \theta_i$ induces a different field isomorphism and therefore a different monomorphism from K into $\mathbb{C}$.

On the other hand, if $\sigma : K \to \mathbb{C}$ is a monomorphism then by the same reason $\sigma(q) = q \ \forall q \in \mathbb{Q}$. Hence, $0 = \sigma(p(\theta)) = p(\sigma(\theta))$, so $\sigma(\theta) = \theta_i$ for some i. □

Corollary 1.6. *If $[K : \mathbb{Q}] = n$ then $|Gal(K/\mathbb{Q})| \leq n$*

Proof. Any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ induces a unique monomorphism $\sigma' : K \to K \subseteq \mathbb{C}$ so by the previous theorem it has to be one of the n possible ones. □

Remark. *There are some examples, as $K = \mathbb{Q}(\sqrt[3]{2})$, where $Gal(K/\mathbb{Q}) < [K : \mathbb{Q}]$. In case $Gal(K/\mathbb{Q}) = [K : \mathbb{Q}]$, we say that $K/\mathbb{Q}$ is a Galois extension. This is equivalent to say that every root of $p(x)$ is in K. In the more general case, given any two fields K, F and a finite field extension K/F we can also define its Galois group as $Gal(K/F) := \{\sigma \in AutK : \ \sigma(\alpha) = \alpha \ \forall \alpha \in F\}$ but in that case it is a subgroup of $AutK$, not necessarily equal to it. In case $F = \mathbb{Q}$ the equality holds because any automorphism of K fixes $\mathbb{Q}$. We say that K/F is a Galois extension if $|Gal(K/F)| = [K : F] = dim_F K$ as a vector space.*

For any $\alpha \in K$ the elements $\sigma_i(\alpha)$ $i = 1, ..., n$ are called the K-conjugates of α. Recall that they do not need to be different i.e. $\sigma_i(q) = q \ \forall q \in \mathbb{Q} \ \forall i$. The product of these K-conjugates of α is called the norm of α in K and is denoted by $N(\alpha)$. As all the $\sigma_i's$ are homomorphisms, this norm is multiplicative. Also, it can be checked (see [3, Thm 2.6]) that the K-conjugates of α are the roots of some polynomial $q(x) = p(x)^s \in \mathbb{Q}[x]$, where $s \in \mathbb{N}$ and $p(x)$ is the minimum polynomial of α, so by Cardano-Vieta relations we know that the product of the K-conjugates of α, that is $N(\alpha)$, is up to sign, the term of degree 0 of $q(x)$. Hence, $N(\alpha) \in \mathbb{Q} \ \forall \alpha \in K$.

Using the K-conjugates, the next definition, as the norm does, gives a nice tool to study number fields.

Definition. *Let $K = \mathbb{Q}(\theta)$ be a number field and $\{\alpha_1, ..., \alpha_n\}$ a $\mathbb{Q}$-basis for it. Then the discriminant of the basis is defined as $\Delta[\alpha_1, ..., \alpha_n] = (det[\sigma_i(\alpha_j)])^2$*

Taking the basis $\{1,\theta,...,\theta^{n-1}\}$ one can check that

$$0 \neq \Delta[1,\theta,...,\theta^{n-1}] = \Pi_{i\neq j}(\theta^i-\theta^j)^2 \in \mathbb{Q}$$

Then, as $K=\mathbb{Q}(\theta)$ is a $\mathbb{Q}$-vector space and the discriminant is multiplicative, if $\{\alpha_1,...,\alpha_n\}$ is another basis then there exists and invertible matrix C with coeffiecients in $\mathbb{Q}$ such that
$\Delta[\alpha_1,...,\alpha_n] = (detC)^2\Delta[1,\theta,...,\theta^{n-1}] \in \mathbb{Q}$. So we have:

Proposition 1.7. *Given $K=\mathbb{Q}(\theta)$ a number field and $\alpha_1,...,\alpha_n$ a $\mathbb{Q}$-basis for it. Then*
$0 \neq \Delta := \Delta[\alpha_1,...,\alpha_n] \in \mathbb{Q}$

In the introduction we have mentioned in some rings the unique factorization of elements does not always hold, so it would be nice to find domains that help us to study the structure behind those factorizations. The best choice for that is the ring of integers of a given number field.

Definition. *An algebraic number α is called an algebraic integer if its minimum polynomial belongs to $\mathbb{Z}[x]$. We denote the set of algebraic integers by $\mathfrak{D}$.*

Example 2. *$\sqrt{2} \in \mathfrak{D}$ as $x^2-2 \in \mathbb{Z}[x]$, but $\frac{1}{2} \notin \mathfrak{D}$ since $x-\frac{1}{2} \notin \mathbb{Z}[x]$. In fact, $\forall q \in \mathbb{Q}\setminus\mathbb{Z}$ we have $q \notin \mathfrak{D}$.*

Remark. *In some mathematical articles algebraic integers are defined in a different way. They say that α an algebraic integer if $\exists p(x) \in \mathbb{Z}[x]$ monic such that $p(\alpha)=0$. In fact these two definitions are equivalent (see [3, Lemma 2.13])*

In the same way that we characterize algebraic numbers in terms of finite field extensions of $\mathbb{Q}$ we can characterize algebraic integers in terms of finitely generated additive groups.

Proposition 1.8. *([3, Lemma 2.8]) $\theta \in \mathfrak{D}$ if and only if the additive group generated by $\{1,\theta,\theta^2,...\}$ is finitely generated.*

The proof depends mostly of the fact that if the minimum polynomial of θ has degree n then $\theta^n = \sum_{i=0}^{n} a_i\theta^i$ and hence all $\theta^m, m \geqslant n$, can be written as a linear combination of $\{1,\theta,...,\theta^{n-1}\}$.

Corollary 1.9. *$\mathfrak{D}$ is a ring.*

Proof. Let α,$\beta \in \mathfrak{D}$ and G_α,G_β their respective finitely generated additive groups. Then $G_\alpha G_\beta$ is also a finitely generated additive group and it contains all the powers of α+β and $\alpha\beta$.
Hence, α+β, $\alpha\beta$ $\in \mathfrak{D}$. □

We can see any field as a ring itself and as the intersection of two rings is a ring we have:

Definition. *Given $K=\mathbb{Q}(\theta)$ number field then $\mathfrak{D}_K = \mathfrak{D} \cap K$ is called the ring of integers of K.*

Lemma 1.10. *Let K be a number field. If $\alpha \in K$ then $\exists c \in \mathbb{Z}$ such that $c\alpha \in \mathfrak{D}_K$.*

Proof. Let $p(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Then $0=p(\alpha)=\alpha^n+\frac{a_{n-1}}{b_{n-1}}+..+\frac{a_0}{b_0}$ $a_i, bi \in \mathbb{Z}\ \forall i$.
Take $c=\Pi b_i$. Then $0=c^n p(\alpha)=...=(c\alpha)^n+c\frac{a_{n-1}}{b_{n-1}}(c\alpha)^{n-1}+...+c^n\frac{a_0}{b_0}=q(c\alpha)\in\mathbb{Z}[c\alpha]$
and $c\alpha \in \mathfrak{D}_K$. □

Corollary 1.11. *If K is a number field then $K=\mathbb{Q}(\theta)$ for some $\theta \in \mathfrak{D}_K$*

Proof. By Theorem 1.4 and Lemma 1.10 $\exists \phi \in \overline{\mathbb{Q}}$, $c \in \mathbb{Z}$ such that $K=\mathbb{Q}(\phi)$ and $c\phi \in \mathfrak{D}_K$. Clearly $\mathbb{Q}(c\phi) \subset \mathbb{Q}(\phi)$. Also, as $c \in \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{Q}(c\phi)$, c is invertible in $\mathbb{Q}(c\phi)$ and $\phi = c^{-1}c\phi$.
Hence, $K=\mathbb{Q}(\phi)=\mathbb{Q}(c\phi)$. □

From Example 2 we deduce $\mathfrak{D}_\mathbb{Q}=\mathbb{Z}$. For any number field $K=\mathbb{Q}(\theta)$ it is clear that $\mathbb{Z}(\theta) \subseteq \mathfrak{D}_K$, where $\mathbb{Z}(\theta)$ denotes the smallest subring of $\mathbb{C}$ that contains $\mathbb{Z}$ and θ, but the equality is not always true.

Example 3. *Let* $K = \mathbb{Q}(\sqrt{5})$. *Then* $\alpha = \frac{1+\sqrt{5}}{2} \in K$ *and* $\alpha^2 - \alpha - 1 = 0$ *so* $\alpha \in \mathfrak{D}_K$, *but* $\alpha \notin \mathbb{Z}[\sqrt{5}]$.

The ring of integers $\mathfrak{D}_K$ is an abelian group under addition, so it has a natural structure of $\mathbb{Z}$-module. Recall that a module over a ring is a generalization of a vector space over a field, as any field is a ring.

Definition. *A* $\mathbb{Z}$*-basis for* $(\mathfrak{D}_K, +)$ *is called an integral basis for* K.

Let K be a number field with $[K : \mathbb{Q}] = n$. From Lemma 1.10 we can deduce that any $\mathbb{Z}$-basis for $\mathfrak{D}_K$ is a $\mathbb{Q}$-basis for K, so $n = dim_{\mathbb{Q}} K = dim_{\mathbb{Z}} \mathfrak{D}_K$. But, even if every finite dimensional vector space over a field has a basis, it is not always the case with finite dimensional modules over a ring. We may think that a basis of K consisting of integer numbers will be an integral basis for K but in Example 3 $\{1, \sqrt{5}\}$ is a $\mathbb{Q}$-basis but $\alpha \notin \mathbb{Z}(\sqrt{5})$, so it is not an integral basis. In order to prove that an integral basis for K always exists, we need to use properties of the discriminant of a basis.

Lemma 1.12. *If* $\{\alpha_1, ..., \alpha_n\}$ *is a basis of* K *consisting of algebraic integers then* $0 \neq \Delta = \Delta[\alpha_1, ..., \alpha_n] \in \mathbb{Z}$.

Proof. By Proposition 1.7 and Corollary 1.9, $0 \neq \Delta \in \mathbb{Q} \cap \mathfrak{D}_K$ so, by Example 2, $0 \neq \Delta \in \mathbb{Z}$. □

Now, as given any basis of K consisting of integers we have $|\Delta| \in \mathbb{N}$ we can apply an infinite descent argument to show that the integral basis must exist.

Theorem 1.13. *([3, Thm 2.16]) Every number field* K *posseses an integral basis and* $\mathfrak{D}_K$ *is a finitely generated* $\mathbb{Z}$*-module with* $n = dim_{\mathbb{Z}} \mathfrak{D}_K$.

Let $\{\alpha_1, ..., \alpha_n\}$,$\{\beta_1, ..., \beta_n\}$ be two integral basis for K and C the matrix of the change of basis. C is an invertible matrix with coefficients in $\mathbb{Z}$ so $detC = \pm 1$. Hence,

$$0 \neq \Delta[\beta_1, ..., \beta_n] = (detC)^2 \Delta[\alpha_1, ..., \alpha_n] = \Delta[\alpha_1, ..., \alpha_n]$$

so the discriminant of an integral basis of a number field K is independent of the integral basis we choose. In fact, it is an invariant of the number field known as the discrimant of K.

Chapter 2

Dedekind domains and the Class Group

The ring of integers of a number field appears as a particular case of a more general abstract object, a Dedekind domain. We will see some properties of these domains and relate them with our rings of integers. After that, we will define the class group of a given number field and prove its finiteness.
We start with a review of some basic terminology of ring theory.

Definition. *Given a commutative ring D and a subset $I \subset D$ we say that I is an ideal of D if I is closed under the sum and $\forall x \in I \ \ \forall r \in D$ we have $xr \in I$. This property is usually written as $ID \subset I$.*

Remark. *Recall that if $1 \in D$ then $I = I \cdot 1 \subset ID$, hence we have $ID = I$ for any ideal I. Clearly 0 and D are ideals of D. We say that an ideal I of D is proper if $I \neq 0, D$. Also, we can give a multiplicative structure to the set of ideals of D. That is, for any ideals I, J of D we define $IJ := \{\sum b_i b_j : b_i \in I, b_j \in J\}$ where all the sums are finite sums. It is easy to check that IJ is also an ideal of D.*

Definition. *A ring D is called an integral domain if it is unital, commutative and if $ab = 0$ for some $a, b \in D$ then either $a = 0$ or $b = 0$.*

Example 4. *For any number field K, $\mathfrak{D}_K$ is commutative and unital as $1 \in \mathbb{Z} \subset \mathfrak{D}_K \subset K$ and K is commutative by definition. Also, for any $0 \neq a \in \mathfrak{D}_K$ such that $ab = 0$ for some $b \in \mathfrak{D}_K$ then, in particular, $ab, a^{-1} \in K$ so $0 = a^{-1}ab = b$. Hence, it is an integral domain. In particular $\mathbb{Z}$ is. On the other hand, for example Z_6 is not an integral domain as $2 \cdot 3 = 0$.*

Lemma 2.1. *Any finite integral domain D is a field.*

Proof. Let $0 \neq x \in D$, we just need to check that x is invertible. Take the map $\Phi_x : D \to D$ given by $\Phi_x(y) = xy \ \forall y \in D$. Given $y, y' \in D$, $y \neq y'$ then $xy = xy' \Leftrightarrow x(y - y') = 0 \Leftrightarrow y = y'$ since D is an integral domain. Therefore, Φ_x is inyective and as D is finite it is surjective, so in particular $\exists z \in D$ such that $1 = \Phi_x(z) = xz = zx$, so x is invertible. As this happens $\forall x \in D$ we conclude that D is a field. □

Definition. *We say that an ideal I of D is principal if there is an element $b \in D$ such that $I = \{br : r \in D\}$. That is, I is generated by b. We write $I = \langle b \rangle$ or $I = bD$.*

Principal ideals are related to factorization of elements in the sense that an integral domain with most part of its ideals being principal will have in general lot of elements with unique factorization. The following two lemmas ilustrate some nice properties of these ideals.

Lemma 2.2. *Let D be an integral domain and $I = \langle \alpha \rangle$, $J = \langle \beta \rangle$ two proper principal ideals of D. Then $I = J \Leftrightarrow \beta = u\alpha$, where u is a unit of D.*

Proof. Assume $\langle \alpha \rangle = \langle \beta \rangle$, in particular $\alpha \in J$, $\beta \in I$. So $\exists u, v \in D$ such that $\alpha = v\beta$ and $\beta = u\alpha$. Thus, $\alpha = v\beta = vu\alpha \Leftrightarrow \alpha(1 - vu) = 0$. As I is proper then $0 \neq \alpha$, so D integral domain implies $1 - vu = 0$ and hence $1 = vu = uv$ as D is commutative, so u is invertible. Conversely, if we assume $\beta = u\alpha$ then $b \in I$. Also, $\alpha = u^{-1}\beta \in \langle \beta \rangle = J$. Hence, $I = J$. □

Lemma 2.3. *Let D be an integral domain and $I = \langle\alpha\rangle$, $J = \langle\beta\rangle$. Then $\langle\alpha\rangle\langle\beta\rangle = \langle\alpha\beta\rangle$.*

Proof. We have $1 \in D$, so $\alpha\beta = \alpha \cdot 1\ \beta \cdot 1 \in \langle\alpha\rangle\langle\beta\rangle$. Hence, $\langle\alpha\beta\rangle \subset \langle\alpha\rangle\langle\beta\rangle$. On the other hand, $\langle\alpha\rangle\langle\beta\rangle = \{\sum(a_i\alpha)(b_i\beta) : a_i, b_i \in D\} = \{\sum a_i b_i \alpha\beta : a_i, b_i \in D\} = \{\sum d_i \alpha\beta : d_i \in D\} \subset \langle\alpha\beta\rangle$, so we have the equality. □

From now on , D will denote an integral domain and $F = Q(D) = \{\frac{a}{b} : a, b \in D, b \neq 0\}$ its field of fractions.

Recall that any non-zero ideal I of D can be seen as a D-module. Also, by definition, F is a D-module. Hence, I has a natural structure of D-submodule of F, as $I \subset D \subset F$. Furthermore, for any $0 \neq b \in F$, bI is a D-submodule of F. This motivates the following:

Definition. *A fractional ideal I of D is a nonzero D-submodule of F such that $aI = J$ for some $0 \neq a \in D$ and some non-zero ideal J of D.*

Any non-zero ideal I of D is also a fractional ideal, just taking $a = 1$; and if I is a fractional ideal then for some $a \in D$ aI is a non-zero ideal of D. Calling $\mathfrak{F}_D$ the set of fractional ideals of D the definition tells us that $\mathfrak{F}_D = \{\frac{1}{a}J : 0 \neq a \in D,\ J \text{ non-zero ideal of D}\}$. In order to avoid confusion we will write $I \leq D$ when I is an ideal of D. Otherwise we will say that I is a fractional ideal of D.

Example 5. *Let $D = \mathbb{Z}$, $F = \mathbb{Q}$. Every fractional ideal of $\mathbb{Z}$ is of the form $r\mathbb{Z}$, for some $0 \neq r \in \mathbb{Q}$.*

Let $I_1, I_2 \in \mathfrak{F}_D$ then $\exists a, b \in D$ such that aI_1, bI_2 are non-zero ideals of D. The product $I_1 I_2$ is defined in the same way than before and we can check that $I_1 I_2$ is a D-submodule of F with $abI_1 I_2$ non-zero ideal of D, so $I_1 I_2 \in \mathfrak{F}_D$. Also, as $1 \in D$ then $DI = I\ \ \forall I \in \mathfrak{F}_D$. Hence, $(\mathfrak{F}, *)$ is a commutative monoid with identity D.

There is an analogue to the concept of a principal ideal in the fractional case. That is, we say that I is a principal fractional ideal of D if $I = bD$, $0 \neq b \in F$. We denote the set of principal fractional ideals of D by $\mathfrak{P}_D$.

Lemma 2.4. *$(\mathfrak{P}_D, *)$ is a submonoid of $(\mathfrak{F}_D, *)$*

Proof. Let $I_1, I_2 \in \mathfrak{P}_D$, then $I_1 = b_1 D$, $I_2 = b_2 D$ for some $0 \neq b_1, b_2 \in F$. Hence, $0 \neq I_1 I_2 = (b_1 D)(b_2 D) = b_1 b_2 D \in \mathfrak{P}_D$ just taking $b = b_1 b_2$. □

Recall that a monoid is a generalization of a group in the sense that we allow some elements not to have an inverse, but groups contain much more information, so it would be nice to have a group structure in these monoids. For that, we need to talk about the inverse of a fractional ideal.

Let I be a fractional ideal of D. We define $I^{-1} := \{c \in F : cI \subset D\}$. As I is fractional, $\exists 0 \neq a \in D$ such that $aI \subset D$, so $0 \neq I^{-1}$. It is clear that I^{-1} is a D-submodule of F. Also, taking $0 \neq b \in I \cap D$ then bI^{-1} is a non-zero ideal of D. Hence, by definition, I^{-1} is a fractional ideal of D.

Definition. *Let I be a fractional ideal of D. We say that I is invertible if $II^{-1} = D$.*

From the definition of I^{-1} we can deduce $II^{-1} = I^{-1}I \subset D$, but the other containment does not always hold. Anyway, in some cases we know it is true.

Lemma 2.5. *Every principal fractional ideal is invertible.*

Proof. I principal fractional $\Rightarrow I = bD$ for some $0 \neq b \in F$. So it is clear that $I^{-1} = b^{-1}D$. Then, $I^{-1}I = (b^{-1}D)(bD) = b^{-1}bD = D$. □

Now we are ready to characterize the domains that concern us in this chapter.

Definition. *An integral domain D is called a Dedekind domain if every D-fractional ideal of $F = Q(D)$ is invertible.*

Example 6. *Let $D = \mathbb{Z}$. Every $\mathbb{Z}$-fractional ideal of $\mathbb{Q}$ is of the form $r\mathbb{Z}$ with $0 \neq r \in \mathbb{Q}$. Hence, every fractional ideal is principal fractional so by Lemma 2.5 every fractional ideal is invertible and hence $\mathbb{Z}$ is a Dedekind domain. On the other hand, not every integral Domain is Dedekind, as for example $D = \mathbb{Z}(\sqrt{5})$.*

We know that $\mathbb{Z}$ is a principal ideal domain, that is, every ideal of $\mathbb{Z}$ is principal. If we take any other principal ideal domain, we can also characterize its fractional ideals very easily and a similar argument as the one in Example 6 tells us that any Principal ideal domain is a Dedekind domain.

In Dedekind Domains we find out the following nice result about what is concerning us all the time, that is, to find domains with good properties regarding the factorizations of its elements.

Theorem 2.6. *([4, Prop 4.42]) A Dedekind domain D is a unique factorization domain if and only if it is a Principal ideal domain.*

In the same way that given $a, b \in D$ we say that a divides b if $\exists u \in D$ such that $au = b$, we can talk in general about an ideal I "dividing" an ideal J , and in Dedekind domains we can characterize these divisions very nicely.

Definition. *Let D be an integral domain and let $I, J \in \mathfrak{F}_D$. We say that I divides J, written $I|J$, if $\exists K \leq D$ such that $J = IK$.*

Proposition 2.7. *Let D be a Dedekind domain and let $I, J \in \mathfrak{F}_D$. Then $I|J \Leftrightarrow J \subset I$.*

Proof. $J = IK$ and $K \subset D$ implies $J \subset ID = I$. Conversely, if $J \subset I$ then $I^{-1}J \subset I^{-1}I = D$, so $K = I^{-1}J \leq D$ and $IK = I(I^{-1}J) = J$ □

In $\mathbb{Z}$ a prime number p is characterized by the property that whenever $p|ab$, $0 \neq a, b \in \mathbb{Z}$ then $p|a$ or $p|b$. The characterization of prime ideals in a Dedekind domain D is analogous to that one. For that, recall that an ideal P in a ring R is prime if and only if R/P is an integral domain and $P \neq R$. So take $R = D$ and let $0 \neq I, J \leq D$ such that $IJ \subset P$. Hence, $IJ = 0$ in D/P which is an integral domain so either $J \subset P$ or $I \subset P$. By the last proposition this is the same that saying $P|IJ$ implies $P|I$ or $P|J$. In particular, if P is prime and $P = IJ$, then $I = P$ and $J = D$ or $I = D$ and $J = P$.

Definition. *An ideal M in a ring is maximal if for any ideal I of D such that $M \subsetneq I$ we have $I = D$.*

Theorem 2.8. *Any non-zero prime ideal in a Dedekind domain D is maximal.*

Proof. Let $0 \neq I$ a prime ideal of D which is not maximal. Then $\exists J \leq D$ such that $I \subsetneq J \subsetneq D$. So by Proposition 2.7 $\exists K \leq D$ such that $I = JK$ and as I is prime then either $J \subset I$ or $K \subset I$. Since $J \neq I$ we have $J \nsubseteq I$, so we must have $K \subset I$. But $I = JK \subset DK = K$, so $I \subset K$ and we get $I = K$. But then $K = I = JK \Rightarrow D = KK^{-1} = JKK^{-1} = J$, which is a contradiction since $J \neq D$. Hence, I is maximal. □

Dedekind domains are named after the mathematician Richard Dedekind who was one of the first mathematicians that studied Ideal theory and related it with number theoretical problems. He did the amazing discovery that, even if we cannot factor an element uniquely in a Dedekind domain, we can always factor any ideal as a unique product of prime ideals. We are going to prove it here but before that we need to introduce the concept of a ring being Noetherian, named also after the mathematician Emmy Noether.

Definition. *A ring R is called Noetherian if every ideal I of R is a finitely generated R-module, that is for some $n \in \mathbb{N}$ $\exists\{b_1, ..., b_n\} \subset I$ such that $\forall m \in I$ $m = r_1 b_1 + ... + r_n b_n$ for some $r_i \in R$. This is equivalent to say that every non-empty set of ideals of R has a maximal element.*

Proposition 2.9. *Every Dedekind domain D is Noetherian.*

Proof. Let $0 \neq I \leq D$. We will see that I is finitely generated. We have $1 \in D = I^{-1}I$ so , for some $n \in \mathbb{N}$, $\exists b_1, ..., b_n \in I$, $c_1, ..., c_n \in I^{-1}$ such that $1 = \sum_{i=1}^{n} c_i b_i$. Now let $b \in I$, then $b = b \cdot 1 = \sum_{i=1}^{n} (bc_i) b_i$ with $bc_i \in D$. Thus, $I = \sum_{i=1}^{n} D b_i$ and hence $I = \langle b_1, ..., b_n \rangle$, which is finitely generated. □

Now that we have seen that every Dedekind domain is Noetherian we are ready to prove the result:

Theorem 2.10. *Every proper ideal of a Dedekind domain D can be written uniquely as a non-zero finite product of prime ideals.*

Proof. Let $0 \neq J \leq D$. We will show first that J is a non-zero finite product of prime ideals. Assume it is not true, so $\emptyset \neq S = \{0 \neq J \lneq D : J \text{ has no prime factorization}\}$. As D is Noetherian, S contains a maximal element $I \lneq D$ in S. Recall that I is maximal in D if and only if D/I is a field. So, as every field is an integral domain and D/I is an integral domain if and only if I is prime we deduce that I is not maximal in D. So $\exists I_1 \in D$ such that $I \subsetneq I_1 \lneq D$ and $I = I_1 I_2$ for some $I_2 \lneq D$. We have $I \subset I_2$ and $I_2 = I \Rightarrow D = II^{-1} = I_1 I_2 I_2^{-1} = I_1$ which is impossible, so $I \subsetneq I_i \lneq D$ for $i = 1, 2$. But I maximal in S implies that $I_1, I_2 \notin S$ so they are non-zero finite products of prime ideals. As $I = I_1 I_2$ we get $I \notin S$, which is a contradiction.
So $J = P_1 ... P_n$ for some non-zero prime ideals P_i. We need to check now that this is the only possible factorization. Assume $P_1 ... P_n = J = Q_1 ... Q_m$, Q_j prime $\forall j$. We have $P_1 | Q_1 ... Q_m$ and P_1 is prime so we can assume $P_1 | Q_1$. By Theorem 2.8, $P_1 = Q_1$. Multiplying by $P_1^{-1} = Q_1^{-1}$ we get $D = Q_2 ... Q_m$ if $n = 1$ and $P_2 ... P_n = Q_2 ... Q_m$ if $n > 1$. The first expression is impossible since $Q_j | D \Rightarrow D = Q_j$, and every Q_j is prime. In the second case, we repeat the argument with P_2, Q_2 instead of P_1, Q_1, and we continue like that, so after a finite number of steps we will get $n = m$ and $P_i = Q_1$ $\forall i = 1, ..., n$. □

Recall that our interest is to study the rings of integers of some specific number fields. We will show that these rings, in particular any ring of integers, is a Dedekind domain so we will be able to study properties of those rings in the context of Dedekind domains and reveal valuable information. Before that we are going to see one more property of Dedekind domains that will help us to characterize them in a less abstract way.

Definition. *An integral domain D is called integrally closed if for any $\alpha \in F = Q(D)$ which is a root of a monic polynomial $p(x) \in D[x]$ we have $\alpha \in D$.*

Example 7. *For any number field K, $\mathfrak{D}_K$ is integrally closed. For that, let $\theta \in K$ and $p(x) \in \mathfrak{D}_K[x]$ such that $0 = p(\theta) = \theta^n + a_{n-1}\theta^{n-1} + ... + a_0$, with $a_i \in \mathfrak{D}_K$ $\forall i$. Then the set $\{\theta^i\}$ of all the powers of θ lies in a $\mathfrak{D}_K$-module M generated by $\{1, \theta, ..., \theta^{n-1}\}$. By Theorem 1.13, $\mathfrak{D}_K$ is a finitely generated additive group with basis $\{\alpha_1, ..., \alpha_n\}$, where $n = [K : \mathbb{Q}]$. Therefore, M lies in the additive group generated by $\{\alpha_1, ..., \alpha_n\} \times \{1, \theta, ..., \theta^{n-1}\}$, which is finitely generated. Hence, by Proposition 1.8, $\theta \in \mathfrak{D} \cap K = \mathfrak{D}_K$.*

We are going to prove that, in fact, any Dedekind domain is integrally closed. For that we need this useful lemma:

Lemma 2.11. *Let I be a fractional ideal of a Dedekind domain D such that $I^2 = I$. Then $I = D$.*

Proof. $D = II^{-1} \Leftrightarrow D = I^2 I^{-1} \Leftrightarrow D = I(II^{-1}) \Leftrightarrow D = ID \subset I$. Also, as $1 \in D$ we get $I = I \cdot 1 \subset ID$. Hence, $D = ID = I$. □

Theorem 2.12. *Any Dedekind domain D is integrally closed.*

Proof. Let $0 \neq \alpha \in F = Q(D)$ D- integral, that is, $\exists p(x) = x^n + a_1 x^{n-1} + ... + a_n \in D[x]$ such that $p(\alpha) = 0$. We need to check that $\alpha \in D$. Write $M = D1 + ... + D\alpha^{n-1}$. M is clearly a finitely generated D-module and $\alpha \in M$. Also, writing $\alpha = \frac{b}{c}$ with $0 \neq b, c \in D$, then $c^{n-1}M$ is an ideal of D, so M is a fractional ideal of D. The construction of M, and the fact that $p(\alpha) = 0$, imply that $M^2 = M$. So, by the last lemma, $\alpha \in M = D$ and we are done. □

Summarizing, what we have seen until now is that any Dedekind domain is integrally closed, Noetherian and every non-zero prime ideal is maximal. In fact, these three properties characterize Dedekind domains.

Theorem 2.13. *([1, Thm 10.3]) An integral domain D is Dedekind if and only if D is integrally closed, Noetherian and every non-zero prime ideal is maximal.*

Now that we know this characterization we are in good conditions to prove that every ring of integers is a Dedekind domain.

Theorem 2.14. *For any number field K, $\mathfrak{D}_K$ is a Dedekind domain.*

Proof. Let K be a number field. We just need to check that $\mathfrak{D}_K$ is integrally closed, Noetherian and every non-zero prime ideal is maximal. By Example 7 we know that $\mathfrak{D}_K$ is integrally closed.

Let $0 \neq I \leq \mathfrak{D}_K$. By Theorem 1.13 we know that $\mathfrak{D}_K$ is a finitely generated $\mathbb{Z}$-module with $dim_{\mathbb{Z}}\mathfrak{D}_K = n = [K:\mathbb{Q}]$, and then I is also finitely generated as a $\mathbb{Z}$-module, and hence as an ideal too. We conclude that $\mathfrak{D}_K$ is Noetherian.

So we are left to prove that every non-zero prime ideal of $\mathfrak{D}_K$ is maximal. For that, let $0 \neq P \leq \mathfrak{D}_K$ a prime ideal and let $0 \neq \alpha \in P$. Let $N(\alpha)$ be the norm of α in K. We have $N(\alpha) = \alpha_1 ... \alpha_n$ where $\{\alpha_i\}$ are the K-conjugates of α. By Theorem 1.5 we know that $\sigma_i(\alpha) = \alpha_i$, where $\{\sigma_i\}$ are the n distinct monomorphisms of K in $\mathbb{C}$. As the identity on K is one of these monomorphisms, we get $\alpha = \alpha_i$ for some i. Assume $\alpha = \alpha_1$. Hence, as P is an ideal, $N = N(\alpha) = \alpha ... \alpha_n \in P$, so $\langle N \rangle \subset P$, where $\langle N \rangle$ is the ideal of $\mathfrak{D}_K$ generated by N. Also, by Example 2, $N \in \mathbb{Z}$. Recall that P is prime if and only if $\mathfrak{D}_K/P$ is an integral domain and P is maximal if and only if $\mathfrak{D}_K/P$ is a field. By Lemma 2.1 we know that any finite integral domain is a field, so we just need to check that $\mathfrak{D}_K/P$ is finite. Let $0 \neq x \in \mathfrak{D}_K$. By what we have said we know $Nx \in \langle N \rangle \subset P$ so $Nx = 0$ in $\mathfrak{D}_K/P$, $\forall x \in \mathfrak{D}_K$. Now, looking at $(\mathfrak{D}_K, +)$ as a finitely generated abelian group, P can be seeing as a finitely generated abelian subgroup of $\mathfrak{D}_K$. $(\mathfrak{D}_K/P, +)$ is also a finitely generated abelian group as the quotient of two abelian groups is a group. Then, as $N \in \mathbb{Z}$, every $x \in \mathfrak{D}_K/P$ has finite order. Thus, $(\mathfrak{D}_K/P, +)$ is finitely generated with every element of finite order, so $\mathfrak{D}_K/P$ is finite. Hence, P is maximal and we conclude that $\mathfrak{D}_K$ is a Dedekind Domain. □

Remark. *During the proof we have seen that $\mathfrak{D}_K/P$ is finite for any $0 \neq P \leq \mathfrak{D}_K$. In fact, by the same argument, we can show that $\mathfrak{D}_K/I$ is finite for any $0 \neq I \leq \mathfrak{D}_K$. We define the norm of I in K as $N_K(I) := |\mathfrak{D}_K/I| \in \mathbb{N}$. Clearly $N_K(\mathfrak{D}_K) = 1$. It can be checked (see [5, Thm 2.2]) that this norm is multiplicative, that is, for any $0 \neq I, J \leq \mathfrak{D}_K$ we have $N_K(IJ) = N_K(I)N_K(J)$. Also, for any principal ideal $0 \neq \langle \alpha \rangle \leq \mathfrak{D}_K$ we have $N_K(\langle \alpha \rangle) = N(\alpha)$.*

Lemma 2.15. *Let K be a number field and $0 \neq P \leq \mathfrak{D}_K$. If $N_K(P)$ is prime then P is a prime ideal.*

Proof. Assume $P = IJ$ then by the multiplicative property of $N_K(\cdot)$ we have $p = N_K(P) = N_K(I)N_K(J)$ for some prime number p. Hence, either $N_K(I) = p$ or $N_K(J) = p$. By commutativity of the ideals, we can assume $N_K(I) = p$. But then $N_K(J) = 1 = |\mathfrak{D}_K/J|$, so $J = D$. Hence, $P = IJ = ID = I$ and P is a prime ideal. □

Lemma 2.16. *Let K be a number field, then $N_K(I) \in I$ for any $0 \neq I \leq \mathfrak{D}_K$.*

Proof. $N_K(I) = |\mathfrak{D}_K/I| \Rightarrow N_K(I)x \in I \ \ \forall x \in \mathfrak{D}_K$. In particular it is true for $x = 1$. □

Lemma 2.17. *Only finitely many ideals of $\mathfrak{D}_K$ have a given norm.*

Proof. By last Lemma, for any $0 \neq I \leq \mathfrak{D}_K$ we have $N_K(I) \in I$, so $\langle N_K(I) \rangle \subset I$ and by Proposition 2.7 $\exists 0 \neq J \leq \mathfrak{D}_K$ such that $IJ = \langle N_K(I) \rangle$. At the same time, as $\mathfrak{D}_K$ is a Dedekind Domain, $\langle N_K(I) \rangle$ factors as a product of prime ideals $IJ = \langle N_K(I) \rangle = P_1^{r_1} ... P_n^{r_n}$ and this factorizacion is unique, so I must be a product of some $P_i^{s_i}$'s, $1 \leq i \leq n$, $1 \leq s_i \leq r_i$. Hence, there are only finitely many possibilities for this I and so only finitely many ideals I_i can have $N_K(I) = N_K(I_i)$. □

Previously, we have said that given any integral domain D, in particular any Dedekind domain, then $(\mathfrak{F}_D, *)$ is a commutative monoid. The only required condition for being in fact a group is that every element must be invertible, that is, every fractional ideal must be invertible. But, if we remember the definition of a Dedekind domain we see that this condition is satisfied so, for any Dedekind domain D, $(\mathfrak{F}_D, *)$ is an abelian group. In the same way we see that $(\mathfrak{P}_D, *)$ is an abelian subgroup of $(\mathfrak{F}_D, *)$. Hence, as the quotient of two abelian groups is an abelian group we get that $(\mathfrak{F}_D/\mathfrak{P}_D, *)$ is an abelian group, with $1 = D\mathfrak{P}_D$, whose elements are equivalence classes of fractional ideals of $\mathfrak{F}_D$ due to the relation: $I \sim J \Leftrightarrow IJ^{-1} \in \mathfrak{P}_D$, and the product is defined as $[I]\cdot[J] = [IJ]$ for any $I, J \in \mathfrak{F}_D$, where $[I]$ denotes the equivalence class of I. This group contains plenty of information about the fractional ideals of the domain. If $D = \mathfrak{D}_K$ for some number field K we call this group the class group of K and we denote it by H_K. One of the main properties of this group is that it is a finite group for any number field K. We will show it, but first of all let us see how this group encapsulates information about the ideals and the factorization of the elements in $\mathfrak{D}_K$.

Lemma 2.18. *For any Dedekind domain D and any $I \in \mathfrak{F}_D$, $[I]$ contains an ideal $0 \neq J \leq D$.*

Proof. $I \in \mathfrak{F}_D \Rightarrow I = \frac{1}{c}J$, where $c \in F = Q(D)$ and $0 \neq J \leq D$. So $J = cI$ and hence $JI^{-1} = cD \in \mathfrak{P}_D$ and $J \sim I$, in other words $J \in [I]$. □

Lemma 2.19. *For any number field K, factorization of elements in $\mathfrak{D}_K$ is unique $\Leftrightarrow |H_K| = 1$.*

Proof. We know by Theorem 2.6 that factorization in $D = \mathfrak{D}_K$ is unique if and only if every ideal of D is principal. If we remember the construction of $\mathfrak{F}_D$ and $\mathfrak{P}_D$ we see that this is equivalent to say that every fractional ideal is principal fractional, which means $\mathfrak{F}_D = \mathfrak{P}_D$, and hence it is the same that saying $|H_K| = |\mathfrak{F}_D/\mathfrak{P}_D| = |\mathfrak{P}_D/\mathfrak{P}_D| = 1$. □

Thus, $h_K := |H_K|$ measures somehow how far $\mathfrak{D}_K$ is from being a unique factorization domain. We call h_K the class number of K.

Theorem 2.20. *([5, Thm 35]) For any number field K, $h_K \in \mathbb{N}$.*

Proof. Let's prove first that $\exists \lambda \in \mathbb{R}^+$ such that for every $0 \neq I \leq \mathfrak{D}_K$ $\exists \alpha \in I$ such that $|N(\alpha)| \leq \lambda \cdot N_K(I)$. By Theorem 1.13 we know that an integral basis $\{\alpha_1, ..., \alpha_n\}$ of $\mathfrak{D}_K$ exists. Let $\sigma_1, ..., \sigma_n$ denote the distinct monomorphisms of K in Theorem 1.5. Take $\lambda = \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(\alpha_j)|$ and $0 \neq I \leq \mathfrak{D}_K$.
As $N_K(I) \in \mathbb{N}$ $\exists m \in \mathbb{N}$ such that $m^n \leq N_K(I) < (m+1)^n$, where $n = [K : \mathbb{Q}]$. Consider the family

$$S = \{\sum_{i=1}^n m_j \alpha_j : m_j \in \mathbb{Z},\ 0 \neq m_j \leq m\}$$

Clearly $|S| = (m+1)^n$ and $S \subset \mathfrak{D}_K$, so as $N_K(I) = |\mathfrak{D}_K/I| < (m+1)^n$ there must be $\beta_1, \beta_2 \in S$ such that $\beta_1 + I = \beta_2 + I$, by the Pidgeon's hole principle. So, $\alpha = \beta_1 - \beta_2 = \sum_{i=1}^n r_j \alpha_j \ \in I, r_j \in \mathbb{Z}, |r_j| \leq m$. Hence,

$$N(\alpha) = \prod_{i=1}^n |\sigma_i(\alpha)| \leq \prod_{i=1}^n \sum_{j=1}^n |r_j||\sigma_i(\alpha_j)| \leq m^n \lambda \leq N_K(I) \cdot \lambda$$

Let's prove now that, calling $D = \mathfrak{D}_K$, every class of fractional ideals of $\mathfrak{F}_D/\mathfrak{P}_D$ contains $0 \neq I \leq D$ such that $N_K(I) \leq \lambda$. Take $C \in \mathfrak{F}_D/\mathfrak{P}_D$. By Lemma 2.18 $\exists 0 \neq J \leq D$ such that $J \in C^{-1}$. Recall that $C^{-1}C = \mathfrak{P}_D$. By what we have said before $\exists \alpha \in J$ such that $N(\alpha) \leq \lambda \cdot N_K(J)$. We have $\langle \alpha \rangle \subset J$ and $\langle \alpha \rangle \in \mathfrak{P}_D$. So, $\exists 0 \neq I \leq D$,
$I \in (C^{-1})^{-1} = C$ such that $\langle \alpha \rangle = IJ$. Hence, as this $N_K(\cdot)$ is multiplicative we have

$$\lambda \cdot N_K(J) \geq N_K(\alpha) = N_K(I)N_K(J)$$

so $N_K(I) \leq \lambda$, and we can do this for every $C \in \mathfrak{F}_D/\mathfrak{P}_D$.

Finally, calling s the integral part of λ, we know by Lemma 2.17 that for any $i = 1, ..., s$ there are only finitely many ideals $0 \neq I \leq D$ such that $N_K(I) = i$, so there are only finitely many ideals such that $N_K(I) \leq \lambda$. Hence, as every $C \in \mathfrak{F}_D/\mathfrak{P}_D$ contains an ideal I such that $N_K(I) \leq \lambda$ we conclude that $\mathfrak{F}_D/\mathfrak{P}_D$ contains only a finite number of elements, that is, $h_K \in \mathbb{N}$. □

Chapter 3

Regular primes: First case

We proceed now to prove the first case of Fermat's Last Theorem using the notions we have introduced in the last two chapters. In the introduction we have mentioned that, for any odd prime p the equation $x^p + y^p + z^p = 0$ can be factored as $(x+y)(x+\zeta_p y)...(x+\zeta_p^{p-1}y) = -z^p$, where $1 \neq \zeta_p$ is a root of $x^p - 1$. So, the best number field to work with is $K = \mathbb{Q}(\zeta_p)$ and as we are studying the possible integer solutions of $x^p + y^p = z^p$ it will be helpful for us to work in $\mathfrak{D}_K$, which is a Dedekind domain with the property that h_K is finite, as we saw in the last chapter.

Definition. *We say that an odd prime number p is regular if $p \nmid h_K$ where $K = \mathbb{Q}(\zeta_p)$.*

We know that if we work with principal ideals is easier to study properties of factorization of elements. The main advantage of regular primes can be understood in the following lemma.

Lemma 3.1. *Let p be a regular prime and let $K = \mathbb{Q}(\zeta_p)$. Assume $\exists I \leq \mathfrak{D}_K$ such that I^p is a principal ideal. Then I must be principal.*

Proof. Write $\mathfrak{F} = \mathfrak{F}_{\mathfrak{D}_K}$ and $\mathfrak{P} = \mathfrak{P}_{\mathfrak{D}_K}$. In $H_K = \mathfrak{F}/\mathfrak{P}$, $1 = \mathfrak{D}_K\mathfrak{P} = \mathfrak{P}$, so I^p principal implies that $I^p \in \mathfrak{P}$ and $[I]^P = 1$ in H_K. So the order of $[I]$ is either 1 or p. If the order is 1 then I is clearly principal. Otherwise, the order is p and we know that the order of every element in a finite group divides the order of the group, so $p|h_K$, which is a contradiction. □

The lemma above will help us to prove that , for a regular prime p, and for every $i = 0, ..., p-1$ we have $x + \zeta_p^i y = u_i \alpha_i^p$, where $\alpha_i, u_i \in \mathfrak{D}_K$ and u_i is a unit. Before that we are going to see some useful properties of $\mathbb{Q}(\zeta_p)$.

Proposition 3.2. *For every odd prime p the minimum polynomial of $\zeta_p \in K = \mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is $\Phi_p(x) = x^{p-1} + ... + x + 1$.*

Proof. ζ_p is a root of $x^p - 1 = (x-1)(x^{p-1} + ... + x + 1)$, so as $1 \neq \zeta_p$, the mimimum polynomial of ζ_p must divide $\Phi_p(x)$, so we just need to see that $\Phi_p(x)$ is irreducible in $\mathbb{Q}$. For that we are going to use the well-known Eisenstein's criterion: If for $p(x) = x^n + a_{n-1} + ... + a_0 \in \mathbb{Q}[x]$ $\exists p$ prime number such that $p|a_i \ \forall i = 0, ..., n-1$ but $p^2 \nmid a_0$, then $p(x)$ is irreducible in $\mathbb{Q}[x]$.

Doing the change of variable $y = x + 1$ then clearly $\Phi_p(y)$ irreducible implies $\Phi_p(x)$ irreducible. So, as $\Phi_p(y) = \sum_{r=1}^{p} \binom{p}{r}(y-1)^{r-1} = \sum_{r=1}^{p} \binom{p}{r} x^{r-1}$, and $p|\binom{p}{r}$ $\forall 1 \leq r \leq p-1$, but $p^2 \nmid \binom{p}{1} = p$, we conclude that $\Phi_p(y)$ is irreducible. Hence, $\Phi_p(x)$ is irreducible.

□

Corollary 3.3. *For any odd prime p, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ and $\{1, \zeta_p, ..., \zeta_p^{p-2}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta_p)$.*

Corollary 3.4. *$\mathbb{Q}(\zeta_p)$ contains all the roots of $\Phi_p(x)$. Thus, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a Galois extension and $|Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = p - 1$.*

Remark. *$\Phi_p(x)$ can be generalized to every $n \in \mathbb{Z}$ greater than 1. For that we take ζ_n as a primitive n-th root of unity, that is $\zeta_n^m = 1 \Rightarrow n|m$, and we define*

$$\Phi_n(x) = \prod_k (x - \zeta_n^k)$$

where k runs over all natural numbers coprime to and lower than n. In particular, for $n = 2$, $\zeta_2 = -1$ and $\Phi_2(x) = x+1$. These irreducible polynomials are called cyclotomic polynomials, and an important property of them is that if m and n are coprime then $\Phi_{mn}(x) = \Phi_m(x)\Phi_n(x)$.

Any field extension $K/\mathbb{Q}$ induces a natural ring extension $\mathfrak{D}_K/\mathbb{Z}$. Therefore, any ideal $n\mathbb{Z}$ "extends" to $n\mathfrak{D}_K$. Also, in the same way that an irreducible polynomial over $\mathbb{Q}$ may not be irreducible over K, a prime ideal of $\mathbb{Z}$ may not be prime in $\mathfrak{D}_K$. The study of the "extensions" of prime ideals, called ramifications, will be very important to prove the second case of Fermat's Last Theorem. The following theorem illustrates an important example of the ramification of a prime ideal.

Theorem 3.5. *For any odd prime p set $\lambda_p := \zeta_p - 1 \in \mathbb{Z}[\zeta_p]$. Then $\langle \lambda_p \rangle$ is a ideal in $\mathfrak{D}_K$, where $K = \mathbb{Q}(\zeta_p)$, and $\langle \lambda_p \rangle^{p-1} = p\mathfrak{D}_K =: \langle p \rangle$.*

Proof. Clearly $\lambda_p \in \mathfrak{D}_K$. We claim that for any $1 \leq i \leq p-1$ the element $u_i = \frac{1-\zeta_p^i}{1-\zeta_p}$ is a unit in $\mathfrak{D}_K$. As p is prime, $\mathbb{Z}_p$ is a field, so given any $0 \neq i \in \mathbb{Z}_p$, $\exists 0 \neq j \in \mathbb{Z}$ such that $ij \equiv 1 (mod\ p)$. Then, as ζ_p is a p-th root of unity, we have $u_i^{-1} = \frac{1-\zeta_p}{1-\zeta_p^i} = \frac{1-\zeta_p^{ij}}{1-\zeta_p^i} = 1 + \zeta_p^i + ... + (\zeta_p^i)^{j-1} \in \mathfrak{D}_K$.

Thus, for any $i = 1, ..., p-1$ we have $(1 - \zeta_p^i) = (1 - \zeta_p)u_i$, where u_i is a unit, and

$$p = \Phi_p(1) = \prod_{i=1}^{p-1} (1 - \zeta_p^i) = (1 - \zeta_p)^{p-1} U$$

where $U = \prod_{i=1}^{p-1} u_i$ is a unit. Hence, by Theorem 3.5 $\langle p \rangle = \langle (1 - \zeta_p) \rangle^{p-1} = \langle \lambda_p \rangle^{p-1}$. Let's see now that $\langle \lambda_p \rangle$ is prime. Recall that $\langle p \rangle = \langle \lambda_p \rangle^{p-1} = \langle \lambda_p^{p-1} \rangle$, so $\langle p \rangle$ is a principal ideal in $\mathfrak{D}_K$. Hence, as $p \in \mathbb{Q}$, $\sigma(p) = p \ \ \forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have $p^{p-1} = N(p) = N_K(\langle p \rangle) = N_K(\langle \lambda^{p-1} \rangle) = (N_K(\langle \lambda_p \rangle))^{p-1}$ and p prime implies $N_K(\langle \lambda_p \rangle) = p$. Hence, by Lemma 2.15, $\langle \lambda_p \rangle$ is a prime ideal. □

Corollary 3.6. *$1 + \zeta_p$ is a unit in $\mathfrak{D}_K$.*

Corollary 3.7. *For any $i \neq j$ $\langle \lambda_p \rangle = \langle \zeta_p^i - \zeta_p^j \rangle$.*

In Chapter 1 we saw that given any number field K, then K can be written as $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer. We also showed that $\mathbb{Z}[\theta] \subset \mathfrak{D}_K$ but the equality is not always true, as in Example 3. Anyway, for $K = \mathbb{Q}(\zeta_p)$, it behaves nicely.

Theorem 3.8. *([6, Prop 3.3]) For any odd prime p and $K = \mathbb{Q}(\zeta_p)$ we have $\mathbb{Z}[\zeta_p] = \mathfrak{D}_K$.*

Corollary 3.9. *An integral basis for $K = \mathbb{Q}(\zeta_p)$ is $\{1, \zeta_p, ..., \zeta_p^{p-2}\}$.*

Proof. For any $i = 0, ..., p-2$, ζ_p^i is an algebraic integer as it is a root of $\Phi_p(x) \in \mathbb{Z}[x]$. By Corollary 3.3 $\{1, \zeta_p, ..., \zeta_p^{p-2}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta_p)$. Also, it spans $\mathbb{Z}[\zeta_p]$. Hence, by the last theorem, it is an integral basis. □

Remark. *In chapter 1 we saw that given any integral basis $\{\alpha_1, ..., \alpha_n\}$ of a number field K, then $\Delta[\alpha_1, ..., \alpha_n]$ is an invariant of K known as the discriminant of K. In our case, for any odd prime p, $\Delta[1, \zeta_p, ..., \zeta_p^{p-2}] = (-1)^{\frac{p-1}{2}} p^{p-2}$ ([3, Thm 3.6]). The discriminant of K will be related with the ramification of prime ideals in K in the proof of the second case of Fermat's Last Theorem.*

The study of the units of $\mathbb{Z}[\zeta_p]$ plays a fundamental role in the proof of Fermat's Last Theorem for regular primes. We proceed now to characterize the roots of unity in $\mathfrak{D}_K$, a special type of units, where $K = \mathbb{Q}(\zeta_p)$.

Proposition 3.10. *The only roots of unity in $\mathbb{Q}(\zeta_p)$ are $\pm\zeta_p^s$, $s \in \mathbb{Z}$.*

Proof. Every element in $\{\pm\zeta_p^s\}$ is a root of the polynomial $x^{2p}-1$ and these are its only roots. Recall that in $\mathbb{C}$ the only roots of unity are by definition of the form $\zeta_n = \exp\frac{2\pi ri}{n}$ $r,n \in \mathbb{Z}$. We only have to show that there is no primitive k-root in $\mathbb{Q}(\zeta_p)$ if $k \nmid 2p$, as any root of unity is a power of some primitive root. Let's prove first that if k, p are relatively prime, $k \neq 1$, then there is no primitive k-root of unity ζ_k in $\mathbb{Q}(\zeta_p)$. For that, we will show $\mathbb{Q}(\zeta_p,\zeta_k) = \mathbb{Q}(\zeta_{kp})$, where ζ_{kp} is any primitive kp-root of unity. It is clear that $\zeta_p\zeta_k$ is a primitive kp-root of unity as p,k are relatively prime, so $\mathbb{Q}(\zeta_{kp}) \subset \mathbb{Q}(\zeta_p,\zeta_k)$ as any primitive kp-root of unity generates the same number field. On the other hand, $\zeta_{pk}^p, \zeta_{kp}^k \in \mathbb{Q}(\zeta_{kp})$ are primitive k, p-roots of unity respectively, so we have the other containment. Now, from the remark after Corollary 3.4 we know that for any $n \in \mathbb{N}$, $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \deg(\Phi_n(x))$ and $\Phi_{kp}(x) = \Phi_k(x)\Phi_p(x)$, so we have

$$\deg(\Phi_{kp}(x)) = [\mathbb{Q}(\zeta_{kp}):\mathbb{Q}] = [\mathbb{Q}(\zeta_p,\zeta_k):\mathbb{Q}] = [\mathbb{Q}(\zeta_p,\zeta_k):\mathbb{Q}(\zeta_p)][\mathbb{Q}(\zeta_p):\mathbb{Q}]$$

and we deduce $[\mathbb{Q}(\zeta_p,\zeta_k):\mathbb{Q}(\zeta_p)] = \deg(\Phi_k(x)) \neq 1$, as $\zeta_k \neq 1$, which implies $\zeta_k \notin \mathbb{Q}(\zeta_p)$.

It only remains to show that same happens just with the condition $k \nmid 2p$. For that, as p is an odd prime, we can write $k = ap^n$, where a, p are relatively prime. If $a = 1$ $\deg(\Phi_{p^n}(x)) > p-1$. If $a > 1$, $ap^n \neq 2p$. Assume that, for some primitive k-root of unity, $\zeta_k \in \mathbb{Q}(\zeta_p)$. Then $\zeta_k^{p^n} \in \mathbb{Q}(\zeta_p)$ is a primitive a- root of unity, which is a contradiction to what we have said above, since a, p are relatively prime. □

The following standard result is a nice tool to know if an element is a root of unity.

Theorem 3.11. *([7, Prop 2.5]) Let $\alpha \in \mathfrak{D}_K$, K number field, all of whose K-conjugates have complex absolute value bounded by* 1. *Then α is a root of unity.*

Using these two propositions and Corollary 3.4 we find out a nice result that will be much helpful in the proof of the First case of Fermat's Last Theorem.

Lemma 3.12. *Let $u \in \mathbb{Z}[\zeta_p]$ be a unit. Then $u/\bar{u} \in \{1, \zeta_p, ..., \zeta_p^{p-1}\}$.*

We have now almost all the ingredients to start the proof of the First case of Fermat's Last Theorem. The following technical lemma is the last result we need.

Lemma 3.13. *For any odd prime p, take $\alpha \in \mathfrak{D}_K$, where $K = \mathbb{Q}(\zeta_p)$, and let $\bar{\alpha}$ denote the complex conjugate of α. Then $\alpha^p \equiv \bar{\alpha}^p (mod\ \langle p\rangle)$.*

Proof. Using the integral basis $\{1, \zeta_p, ..., \zeta_p^{p-2}\}$, we write $\alpha = \sum_{i=0}^{p-2} a_i\zeta_p^i$, $a_i \in \mathbb{Z}$ $\forall i$. Then $\alpha^p = (\sum_{i=0}^{p-2} a_i\zeta_p^i)^p \equiv \sum_{i=0}^{p-2} a_i^p(\zeta_p^i)^p = \sum_{i=0}^{p-2} a_i^p$ $(mod\ \langle p\rangle)$, as $pa_i\zeta_p^i \equiv 0$ $(mod\ \langle p\rangle)$ and $(\zeta_p^i)^p = 1$, $\forall i$. On the other hand, $\bar{\alpha}^p = (\sum_{i=0}^{p-2} \bar{a}_i\overline{\zeta_p^i})^p \equiv \sum_{i=0}^{p-2} \bar{a}_i{}^p\overline{(\zeta_p^i)^p} = \sum_{i=0}^{p-2} a_i^p (mod\ \langle p\rangle)$, as $\overline{c}^p = \overline{c^p}$ for any $c \in \mathbb{C}$ and $\bar{z} = z$ $\forall z \in \mathbb{Z}$. □

We are going to start firstly with the case $p = 3$, which is a regular prime and then we will prove it for the rest of regular primes.

Theorem 3.14. *Let $0 \neq x, y, z \in \mathbb{Z}$ pairwise relatively prime. Then, if $3 \nmid x, y, z$, the equation $x^3 + y^3 + z^3 = 0$ does not have a solution.*

Proof. Assume there is solution x, y, z, so if we look at the equation *mod* 9 we have $\bar{x}^3 + \bar{y}^3 + \bar{z}^3 \equiv 0$ $(mod\ 9)$. Now, as $3 \nmid x, y, z$, x, y, z are of the form $9k + r$, $r \neq 0, 3, 6$. So looking at the congruences we have $x^3, y^3, z^3 \equiv \pm 1$ $(mod\ 9)$. But then

$$\bar{x}^3 + \bar{y}^3 + \bar{z}^3 \equiv 0\ (mod\ 9) \Leftrightarrow \pm 1 \pm 1 \pm 1 \equiv 0\ (mod\ 9)$$

which is impossible. □

Theorem 3.15. *(Fermat's Last Theorem-First case) Let $p \geq 5$ be a regular prime and let $0 \neq x,y,z \in \mathbb{Z}$ pairwise relatively prime. Then , if $p \nmid x,y,z$, the equation $x^p + y^p + z^p = 0$ does not have a solution.*

Proof. Assume there is a solution x,y,z. So $x^p + y^p + z^p = 0 \Leftrightarrow (x+y)(x+\zeta_p y)...(x+\zeta_p^{p-1}y) = -z^p$ factorizes in $\mathbb{Z}[\zeta_p]$. Lemma 2.3 implies that $\langle x+y\rangle\langle x+\zeta_p y\rangle...\langle x+\zeta_p^{p-1}y\rangle = \langle z\rangle^p$.

Claim 1. *$\langle x+\zeta_p^i y\rangle, \langle x+\zeta_p^j y\rangle$ are coprime $\forall i \neq j$*

Assume there is a prime ideal P such that, for some $i \neq j$ $P|\langle x+\zeta_p^i y\rangle$ and $P|\langle x+\zeta_p^j y\rangle$. Then, P divides the difference , that is, $P|\langle(\zeta_p^i - \zeta_p^j)y\rangle$. Also, by the above factorization of ideals, $P|\langle z\rangle^p$ and, as P is prime, $P|\langle z\rangle$. By Lemma 2.3 and Corollary 3.7 $P|\langle\lambda_p\rangle\langle y\rangle$, so either $P|\langle\lambda_p\rangle$ or $P|\langle y\rangle$. In the first case , P and $\langle\lambda_p\rangle$ are prime ideals, so they are maximal, and hence $P = \langle\lambda_p\rangle$. But in that case $\langle\lambda_p\rangle|\langle z\rangle$, and taking norms we have $p = N_K(\langle\lambda_p\rangle)|N_K(\langle z\rangle) = z^p$, so $p|z$, which is a contradiction as p and z are coprime. In the second case we have $P|\langle y\rangle$ and $P|\langle z\rangle$, so $y,z \in P$, but y,z coprime implies, by Bezout's theorem, that $\exists r,s \in \mathbb{Z}$ such that $ry+sz = 1 \in P$. Hence, $P = \mathbb{Z}[\zeta_p]$, which is a contradiction as P is prime.

So they are pairwise relatively prime and, as given P_i prime ideal such that $P_i|\langle x+\zeta_p^i y\rangle$, we have $P_i|\langle z\rangle$ and so $P_i^p|\langle z\rangle^p$, the unique factorization of ideals in terms of prime ideals implies that , for any $i = 0,...,p-1$, $\langle x+\zeta_p^i y\rangle = M_i^p$, for some ideal M_i. Hence, M_i^p is a principal ideal so, by Lemma 3.1, M_i is principal and $x+\zeta_p^i = u_i\alpha_i^p$, where u_i is a unit and $M_i = \langle\alpha_i\rangle$. Since $x+\zeta_p^{p-i}y = x+\overline{\zeta_p^i}y \ \ \forall i$, we can choose α_i, u_i such that $\alpha_{p-i} = \bar{\alpha}_i$, $u_{p-i} = \bar{u}_i \ \ \forall i = 0,...,p-1$.

By Lemma 3.12 $\exists k \in \mathbb{N}$ such that $u_1/\bar{u_1} = \zeta_p^k$ and by Lemma 3.13

$$x+\zeta_p y = u_1\alpha_1^p \equiv u_1\bar{\alpha}^p \equiv \zeta_p^k\bar{u_1}\bar{\alpha_1}^p = \zeta_p^k(x+y\zeta_p^{-1}) \ (mod\ \langle p\rangle)$$

Claim 2. *$x+\zeta_p y-\zeta_p^k x-\zeta_p^{k-1}y \equiv 0\ (mod\ \langle p\rangle)$ only if $k = 1$:*

Suppose $k = 0$, then $\langle p\rangle$ divides the ideal $\langle y(\zeta_p - \zeta_p^{-1})\rangle = \langle y\rangle\langle\lambda_p\rangle$ by Corollary 3.7, so as $\langle\lambda_p\rangle^{p-1} = \langle p\rangle$, $\langle\lambda_p\rangle^{p-2}|\langle y\rangle$. In particular $\langle\lambda_p\rangle|\langle y\rangle$, and taking norms we get $p|y$, which is a contradiction. In the same way, if $k = 2$ then we get $\langle p\rangle|\langle x\rangle\langle(1-\zeta_p^2)\rangle = \langle x\rangle\langle\lambda_p\rangle$ and by the same argument $p|x$, which is again a contradiction. Assume now $2 < k < p-1$, and suppose $x+\zeta_p y-\zeta_p^k x-\zeta_p^{k-1}y = p\alpha$, $\alpha \in \mathbb{Z}[\zeta_p]$. Take the integral basis $\{1,\zeta_p,...,\zeta_p^{p-2}\}$ of $\mathbb{Z}[\zeta_p]$. Then, $\alpha = \sum_{i=0}^{p-2} a_i\zeta_p^i$, $a_i \in \mathbb{Z}$ and $x+\zeta_p y-\zeta_p^k x-\zeta_p^{k-1}y = \sum_{i=0}^{p-2} pa_i\zeta_p^i$. Thus, as $\{1,\zeta_p,...,\zeta_p^{p-2}\}$ is a basis, the coefficients in both sides must be identical. From here we deduce $p|x$ which is a contradiction. The case $k = p-1$ is different as the element ζ_p^{p-1} is not an element on the basis, so we cannot apply the same argument. But, multiplying both sides by ζ_p^2, we get $\zeta_p^2 x+\zeta_p^3 y-\zeta_p x-y = \sum_{i=0}^{p-2} pa_i\zeta_p^{i+2}$ and we can apply it now. We get $p|y$, which is again a contradiction.

Hence, the only option is $k = 1$. But then we can write $x+\zeta_p y-\zeta_p x-y = (x-y)+\zeta_p(y-x)$ and applying the basis coefficient argument again we get $p|(x-y)$ or $x \equiv y\ (mod\ \langle p\rangle)$. Finally, as the equation $x^p + y^p + z^p = 0$ is symmetric in x,y,z we can apply the whole argument to

$$\langle x+z\rangle\langle x+\zeta_p z\rangle...\langle x+\zeta_p^{p-1}z\rangle = \langle y\rangle^p$$

and get $x \equiv z\ (mod\ \langle p\rangle)$ So, we get $x^p + y^p + z^p \equiv 3x^p \equiv 0\ (mod\ \langle p\rangle)$. Hence, $p|3x^p$, but $p \geq 5$, so $p|x$, which is a contradiction. □

Chapter 4

Regular primes: Second case

Most part of the proof we have just seen depends on the fact that $p \nmid x,y,z$, so in order to prove the Second case we need to go further. In his original paper, Kummer proved this second case thanks to a deeper understanding of the units in $\mathbb{Z}[\zeta_p]$. This study led him to find the last important piece he needed to prove the theorem, which is his well-known Lemma: Any unit in $\mathbb{Z}[\zeta_p]$ which is congruent to an integer modulo $\langle p \rangle$ is a p^{th} power of some unit in $\mathbb{Z}[\zeta_p]$. His original proof just uses elementary notions as the ones we introduced in chapter 1 but it is a bit tedious. We will take a different approach to prove a weaker version of this lemma, which will be enough to give a complete proof of this second case. In order to do that, we will do a small trip to class field theory, one of the nicest topics in modern number theory.

Let L/K be a finite extension of number fields. We have seen that this extension leads to an extension of rings of integers $\mathfrak{D}_L/\mathfrak{D}_K$. Let P be a prime ideal in $\mathfrak{D}_K$, then P extends to the ideal $P\mathfrak{D}_L$ in $\mathfrak{D}_L$. The unique factorization of ideals into prime ideals implies that $P\mathfrak{D}_L = Q_1^{r_1}...Q_s^{r_s}$ for some unique distinct prime ideals $Q_j \leq \mathfrak{D}_L$. We say that P ramifies in $\mathfrak{D}_L$ if $r_i > 1$ for some i, otherwise we say that P is unramified.

Recall that $\mathfrak{D}_K/P$, $\mathfrak{D}_L/Q_j$ are fields for any j, as every nonzero prime ideal in a ring of integers is maximal. Furthermore, any of these fields is finite. Calling $F = \mathfrak{D}_K/P$, $F_q^j = \mathfrak{D}_L/Q_j$, then F_q^j/F is a finite field extension as $\mathfrak{D}_K \subset \mathfrak{D}_L$ and $P \subset Q_j$, as $Q_j|P$. Under these conditions, calling $f_j = [F_q^j : F]$ it can be checked that $[L:K] = n = \sum_{i=1}^{s} r_j f_j$.

Assume now that L/K is a Galois extension. In that case the situation is better because $\mathrm{Gal}(L/K)$ fixes $\mathfrak{D}_K$ and acts transitively on the set of primes $\{Q_j\}$ lying over P. That is, given any Q_i, Q_j then $\sigma(Q_i) = Q_j$ for some $\sigma \in \mathrm{Gal}(L/K)$. From this fact and the unique factorization into prime ideals it follows that $r \equiv r_i = r_j$, $f \equiv f_i = f_j$ $\forall i,j = 1,...s$. So, $P\mathfrak{D}_L = (Q_1...Q_s)^r$ and $n = rsf$. Choose now any of these Q_j and define $D_{Q_j} := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(Q_j) = Q_j\}$, which is a subgroup of $\mathrm{Gal}(L/K)$ of order rf. For any $\sigma \in D_{Q_j}$, in particular $\sigma \in \mathrm{Gal}(L/K)$ so $\sigma(k) = k \ \ \forall k \in K$ and $\sigma(P) = P$. Therefore, for any $a+P \in F$, $\sigma(a+P) = \sigma(a) + \sigma(P) = a+P$. Thus, D_{Q_j} leaves F fixed. Also, any $\sigma \in D_{Q_j}$ is an automorphism of L that leaves Q_j fixed, so σ induces an automorphism of F_q^j. Hence, there is a reduction map $\Gamma_j : D_{Q_j} \to \mathrm{Gal}(F_q^j/F)$, which can be checked to be surjective.

Any finite extension of finite fields is a Galois extension, so $|\mathrm{Gal}(F_q^j/F)| = [F_q^j : F] = f$ for any $j = 1,...,s$. Therefore, if P is unramified in $\mathfrak{D}_L$, then $r = 1$, so the order of D_{Q_j} is equal to f and as Γ_j is a surjective map we have $D_{Q_j} \cong \mathrm{Gal}(F_q^j/F)$, and this happens for every such Q_j.

Recall that F is a finite field, so $|F| = p^m$ for some $m \in \mathbb{N}$, where p is the characteristic of F. The theory of finite field extensions tells us that F_q^j is a finite field of the same characteristic than F and $|F_q^j| = p^{m+f_j}$ as $[F_q^j : F] = f_j$. Every element of F has order $p^m - 1$, so $a^{p^m} = a \ \ \forall a \in F$, and as F_q^j has characteristic p, the map $\varphi_q^j : F_q^j \to F_q^j$ given by $\varphi_q^j(a) = a^{p^m}$ $\forall a \in F_q^j$ is an automorphism of F_q^j that fixes F, that is $\varphi_q^j \in \mathrm{Gal}(F_q^j/F)$. Furthermore, the order of φ_q^j is precisely f, so it is a generator of the cyclic group $\mathrm{Gal}(F_q^j/F)$. This φ_q^j is known as the Frobenius element of F_q^j.

We have said that if P is unramified in $\mathfrak{D}_L$ then $D_{Q_j} \cong \text{Gal}(F_q^j/F)$ for every Q_j lying over P. Hence, D_{Q_j} is a cyclic group with generator $\Gamma_j^{-1}(\varphi_q^j)$. Recall that D_{Q_j} is a subgroup of $\text{Gal}(L/K)$ so we can say that every Q_j induces an element $\Gamma_j^{-1}(\varphi_q^j) \in \text{Gal}(L/K)$. Furthermore, it can be checked that for any Q_i, Q_j lying over P, $\exists \tau \in \text{Gal}(L/K)$ such that $\Gamma_i^{-1}(\varphi_q^i) = \tau^{-1}\,\Gamma_j^{-1}(\varphi_q^j)\,\tau$.

Assume now that L/K is an abelian extension, that is it is a Galois extension and $\text{Gal}(L/K)$ is an abelian group. Then we deduce $\Gamma^{-1}(\varphi_q) := \Gamma_j^{-1}(\varphi_q^j) = \Gamma_i^{-1}(\varphi_q^i)\ \forall i, j = 1, ..., s$, so every Q_j lying over P induces the same element of $\text{Gal}(L/K)$. Therefore, if L/K is an unramified extension, meaning that every prime ideal of $\mathfrak{D}_K$ is unramified in $\mathfrak{D}_L$, we can say that every prime ideal P induces an element $(\frac{L\,K}{P}) := \Gamma^{-1}(\varphi_q) \in \text{Gal}(L/K)$. The map that sends any prime ideal P to $(\frac{L\,K}{P})$ is called the Artin map, and it can be extended in a multiplicative way to every fractional ideal of K as follows. By Theorem 2.10 we deduce that any fractional ideal I of K can be written as $I = P_1^{r_1}...P_s^{r_s}$, for some $r_i \in \mathbb{Z}$ and some different prime ideals P_i. Then, as every $(\frac{L\,K}{P_i})$ is invertible, we can define $(\frac{L\,K}{I}) = \prod_{i=1}^{s} (\frac{L\,K}{P_i})^{r_i}$.

I think we are in good conditions now to appreciate the beauty of the following astonishing theorem:

Theorem 4.1. *([10, Ch.8 Thm 7]) Given a number field K, let L be the unique unramified abelian extension of K which contains all other unramified abelian extensions of K. Then the Artin map of K induces an isomorphism $H_K \cong Gal(L/K)$.*

This L is normally called the Hilbert class field of K because its existence was conjetured by Hilbert. Philipp Furtwngler proved the conjecture and the result was extended by Emil Artin as the Artin's Reciprocity Law, which is one of the cornerstones of Class field theory.

Going back to the number fields we are interested in , which are of the form $K = \mathbb{Q}(\zeta_p)$, when p is a regular prime, this theorem is telling us that if we find an unramified abelian extension K' of K then this extension K' is contained in the Hilbert class field L of K. Also, as K'/K is a Galois extension, then $|\text{Gal}(K'/K)| = [K' : K]$ and $|H_K| = |\text{Gal}(L/K)| = [L : K] = [L : K'][K' : K]$, so as p is regular, p cannot divide $[K' : K]$; and this happens for any unramified abelian extension of K. Therefore, if we find some field extension K'/K such that $p|[K' : K]$, then some prime ideal of K must ramify at K'. So, we wonder if there is a good criteria to know exactly under which conditions a prime ideal ramifies in a further extension. In fact it exists in the case that $K = \mathbb{Q}$, and it is related to the discriminant of a number field.

Theorem 4.2. *([8, Thm 5.5]) Let K be a number field and Δ_K its discriminant. Then a prime ideal $\langle p \rangle \leq \mathbb{Z}$ ramifies in $K \Leftrightarrow p|\Delta_K$.*

Corollary 4.3. *Only a finite number of prime ideals of $\mathbb{Z}$ ramifies in K.*

Example 8. *Consider the case $K = \mathbb{Q}(\zeta_p)$ for some prime number p. Then $\{1, \zeta_p, ..., \zeta_p^{p-2}\}$ is an integral basis of K, so $\Delta_K = \Delta[1, ..., \zeta_p^{p-2}] = (-1)^{\frac{p-1}{2}} p^{p-2}$ and the only prime ideal that ramifies in K is $\langle p \rangle = \langle \lambda_p \rangle^{p-1}$.*

Notice that for this theorem we are only considering finite field extensions of the form $K/\mathbb{Q}$. If we want to study ramifications in arbitrary number field extensions L/K we need to refine a bit the definition of the discriminant.

Definition. *Let L/K be a number field extension and let $\{\sigma_1, ..., \sigma_n\}$ the different monomorphisms $\sigma_i : L \to \mathbb{C}$ that are the identity on K. For any K-basis of L of the form $\{\alpha_1, ..., \alpha_n\}$, where $\alpha_i \in \mathfrak{D}_L\ \forall i$, we call $\Delta[\alpha_1, ..., \alpha_n] = (det[\sigma_i(\alpha_j)])^2$. Then the ideal of $\mathfrak{D}_L$ generated by the set $\{\Delta[\alpha_1^j, ..., \alpha_n^j]\}$, where $\{\alpha_i^j\}$ runs over all K-basis of L with $\alpha_i^j \in \mathfrak{D}_L\ \forall i$, is called the relative discriminant of L/K.*

We can always find a K-basis of L consisting of algebraic integers. Appart from that, in chapter 1 we saw that, given a number field K such that $[K : \mathbb{Q}] = n$ then there are exactly n different monomorphisms

from K into $\mathbb{C}$ that fix $\mathbb{Q}$. In the more general case with $[L:K]=n$ this result is also true, so the definition makes sense. Also, it is clear that the relative discriminant L/K is an ideal of $\mathfrak{D}_L$ as it is generated by elements of $\mathfrak{D}_L$ because $\mathfrak{D}_L$ is a ring. Recall that if we take $K=\mathbb{Q}$ in the definition, then the relative discriminant of $K/\mathbb{Q}$ is precisely the principal ideal generated by the discrminant of K. We may think that for any two basis $\{\alpha_1,...,\alpha_n\}$, $\{\beta_1,...,\beta_n\}$ in the definition then $\Delta[\alpha_1,...,\alpha_n]=det(C)^2\Delta[\beta_1,...,\beta_n]$, for some matrix C with coefficients in $\mathfrak{D}_K$ as happens when we consider $K=\mathbb{Q}$ and the integral basis of K, but for that we need that some of these basis to be a $\mathfrak{D}_K$-basis for $\mathfrak{D}_L$, and that basis may not exist. That is why we cannot define the relative discriminant as an element rather than as an ideal, because is not a principal ideal in general.

Anyway, we still have a nice criteria to determine if a prime ideal of K ramifies in L.

Theorem 4.4. *([9, Corollary 4.8]) Let L/K be an extension of number fields. Then a prime ideal $P\leq\mathfrak{D}_K$ ramifies in $\mathfrak{D}_L$ if and only if $P|\Delta_K^L$, where Δ_K^L denotes the relative discriminant of L/K.*

Corollary 4.5. *Let $\alpha_1,...,\alpha_n$ be a K-basis for L where $\alpha_i\in\mathfrak{D}_L\ \forall i$. If a prime ideal $P\leq\mathfrak{D}_K$ ramifies in $\mathfrak{D}_L$, then $N_L(P)|\Delta[\alpha_1,...,\alpha_n]$.*

Proof. We can see P as an ideal of $\mathfrak{D}_L$. Also, $\Delta[\alpha_1,...,\alpha_n]$ is one of the generators of Δ_K^L, so $\langle\Delta[\alpha_1,...,\alpha_n]\rangle\subset\Delta_K^L$ and then $\Delta_K^L|\langle\Delta[\alpha_1,...,\alpha_n]\rangle$ as they are both ideals of the same number field. If P is ramified in $\mathfrak{D}_L$, then $P|\Delta_K^L|\langle\Delta[\alpha_1,...,\alpha_n]\rangle$ and taking norms we have in particular $N_L(P)|N_L(\langle\Delta[\alpha_1,...,\alpha_n]\rangle)=\Delta[\alpha_1,...,\alpha_n]$. □

We are ready now to prove our weaker version of Kummer's Lemma.

Theorem 4.6. *Let $p\geq 3$ be a regular prime and let e be a unit in $\mathbb{Z}[\zeta_p]$ which is congruent to a p^{th} power modulo $\langle\lambda_p\rangle^p$. Then e is the p^{th} power of some unit in $\mathbb{Z}[\zeta_p]$.*

Proof. Recall that $e^{1/p}$ is a root of the monic polynomial $f(x)=x^p-e\in\mathbb{Z}[\zeta_p]$, so as $\mathbb{Z}[\zeta_p]$ is integrally closed, if $e^{1/p}\in\mathbb{Q}(\zeta_p)$, then $e^{1/p}$ must belong to $\mathbb{Z}[\zeta_p]$. Therefore, it suffices to show $e^{1/p}\in\mathbb{Q}(\zeta_p)$.

Assume $e^{1/p}\notin\mathbb{Q}(\zeta_p)$ and consider the extension $K:=\mathbb{Q}(\zeta_p,e^{1/p})$. So, $[K:\mathbb{Q}(\zeta_p)]>1$. The roots of $f(x)$ are of the form $\zeta_p^k e^{1/p}$, $k=0,1...,p-1$ and clearly every root is in K so every root $\zeta_p^k e^{1/p}$ induces an element $\sigma_k\in\mathrm{Gal}(L/K)$ by $\sigma_k(e^{1/p})=\zeta_p^k e^{1/p}$. As $\deg(f(x))=p$ this implies that L/K is a Galois extension and $[L:K]=|\mathrm{Gal}(L/K)|=p$.

Also, $\{e^{1/p},...,\zeta_p^{p-1}e^{1/p}\}$ is a $\mathbb{Q}(\zeta_p)$-basis for K. Furthermore, by Example 7 we know that if an element is a root of a polynomial whose coefficients are algebraic integers then the element is also an algebraic integer so, as $f(x)\in\mathbb{Z}[\zeta_p][x]$, every element of the basis is an algebraic integer that belongs to K. Therefore, $\zeta_p^k e^{1/p}\in\mathfrak{D}_K\ \ \forall k=0,...,p-1$. Computing the discriminant of this basis, we get

$$\Delta[e^{1/p},...,\zeta_p^{p-1}e^{1/p}]=\pm p^p e^{p-1}$$

As e is a unit and $\langle p\rangle=\langle\lambda_p\rangle^{p-1}$, the unique factorization into prime ideals and Corollary 4.5 tell us that the only prime ideal of $\mathbb{Z}[\zeta_p]$ that may ramify in $\mathfrak{D}_K$ is $\langle\lambda_p\rangle$.

We are going to show that in fact $\langle\lambda_p\rangle$ does not ramify. By assumption $\exists\alpha\in\mathbb{Z}[\zeta_p]$ such that $\alpha^p\equiv e\ (mod\ \langle\lambda_p\rangle^p)$. Take the polynomial $g(x):=\frac{(\lambda_p x+\alpha)^p-e}{\lambda_p^p}$. It can be checked that $g(x)\in\mathbb{Z}[\zeta_p][x]$. The roots of $g(x)$ are $\tau_i:=\frac{\zeta_p^i e^{1/p}-\alpha}{\lambda_p}$, $i=0,...,p-1$.

Calling $K'=\mathbb{Q}(\zeta_p,\tau_0)$, as $\deg(f(x))=\deg(g(x))=p$ and $\tau_i\in K\cap K'\ \ \forall i$, we have $K=K'$. Now, by the same reason above, $\tau_0,...,\tau_{p-1}$ are algebraic integers, and also they form a $\mathbb{Q}(\zeta_p)$-basis for K. So, computing $\Delta[\tau_0,...,\tau_{p-1}]$ we must have $\lambda_p=N_K(\langle\lambda_p\rangle)|\Delta[\tau_0,...,\tau_{p-1}]$. But,

$$\Delta_0:=\Delta[\tau_0,...,\tau_{p-1}]=\pm\, e\cdot\prod_{0\leq i<j\leq p-1}\frac{\zeta_p^i-\zeta_p^j}{\lambda_p}$$

and $\frac{\zeta_p^i-\zeta_p^j}{\lambda_p} = \zeta_p^j \frac{1-\zeta_p^i}{1-\zeta_p}$ is a unit as ζ_p^j is a unit and $\frac{1-\zeta_p^i}{1-\zeta_p}$ is a unit by Theorem 3.5, $\forall 0 \leq i < j \leq p-1$. Hence, as e is a unit by assumption, we conclude that Δ_0 is a unit. But then the ideal generated by Δ_0 is the whole ring $\mathbb{Z}[\zeta_p]$, so if $\langle \lambda_p \rangle$ ramifies then by Corollary 4.5 $p = N_K(\langle \lambda_p \rangle)|N_K(\langle \Delta_0 \rangle) = 1$, which is impossible.

Thus, $K/\mathbb{Q}(\zeta_p)$ is an unramified Galois extension of degree p, so $|\text{Gal}(K/\mathbb{Q}(\zeta_p))| = p$ and $\text{Gal}(K/\mathbb{Q}(\zeta_p))$ is an abelian group because it is cyclic (p prime). Therefore, K is contained in the Hilbert Class field L of $\mathbb{Q}(\zeta_p)$, and by Theorem 4.1, $h_{\mathbb{Q}(\zeta_p)} = |\text{Gal}(L/\mathbb{Q}(\zeta_p))| = [L:\mathbb{Q}(\zeta_p)] = [L:K][K:\mathbb{Q}(\zeta_p)]$, so $p|h_{\mathbb{Q}(\zeta_p)}$, which is a contradiction since p is regular. Hence, $e^{1/p} \in \mathbb{Z}[\zeta_p]$, and as e is a unit, $ee' = 1$ for some $e' \in \mathbb{Z}[\zeta_p]$ so $e^{1/p}((e^{1/p})^{p-1}e') = 1$ and we conclude that $e^{1/p}$ is a unit in $\mathbb{Z}[\zeta_p]$. □

We need a technical lemma before going through the proof of the Second case.

Lemma 4.7. *Let $v \in \mathbb{Z}[\zeta_p]$ such that $\langle v \rangle, \langle \lambda_p \rangle$ are relatively prime. Then $\exists k \in \mathbb{Z}$ such that $\zeta_p^k v \equiv m \ (mod\ \lambda_p^2)$, with $m \in \mathbb{Z}$.*

Proof. Recall that $\{1, \lambda_p, ..., \lambda_p^{p-2}\}$ is also a basis for $\mathbb{Z}[\zeta_p]$ and $\langle p \rangle = \langle \lambda_p \rangle^{p-1}$, so we can write $v \equiv m + n\lambda_p \ (mod\ \lambda_p^2)$, where $m, n \in \mathbb{Z}$ and m and p are relatively prime. By the binomial theorem we have $\zeta_p^k = (1+\lambda_p)^k \equiv 1 + k\lambda_p \ (mod\ \lambda_p^2)$. As m and p are coprime we can choose $k \in \mathbb{Z}$ such that $n + mk \equiv 0 \ (mod\ p)$. We know that $\langle p \rangle \subset \langle \lambda_p^2 \rangle$. Therefore,

$$\zeta_p^k v \equiv (1+k\lambda_p)(m+n\lambda_p) \equiv m + (n+km)\lambda_p \equiv m \ (mod\ \lambda_p^2)$$

□

Theorem 4.8. *(Fermat's Last Theorem-Second Case). Let $p \geq 3$ be a regular prime. Then the equation $x^p + y^p + z^p = 0$ does not have any non-trivial solution in $\mathbb{Z}$ if $p|xyz$.*

Proof. Assume there is a solution. As $\langle \lambda_p \rangle^{p-1} = \langle p \rangle$ we may, without loss of generality, assume that x, y, z are pairwise relatively prime with $\langle \lambda_p \rangle | \langle z \rangle$. It follows that $0 \neq -z = \lambda_p^m z_0$ with $\langle \lambda_p \rangle$,$\langle z_0 \rangle$ relatively prime and $\lambda_p \nmid x, y$, because otherwise it would divide all three coefficients. Therefore, to prove the theorem it is enough to show that there are no non-trivial solutions $x, y, z \in \mathbb{Z}[\zeta_p]$ to the equation $x^p + y^p = u\lambda_p^{pm} z^p$ with $\langle x \rangle, \langle y \rangle, \langle z \rangle, \langle \lambda_p \rangle$ pairwise relatively prime, $m \geq 1$ and u a unit in $\mathbb{Z}[\zeta_p]$; which is in fact a stronger result.

We are going to show first that $m > 1$. Assume there is a solution of this form. Recall that ζ_p^i is a unit $\forall i$, so by Lemma 4.7 $\exists k, r \in \mathbb{Z}$ such that $x \equiv a\zeta_p^k \ (mod\ \lambda_p^2)$, $y \equiv b\zeta_p^r \ (mod\ \lambda_p^2)$, for some $a, b \in \mathbb{Z}$. Also, $\exists s \in \{0, 1, ..., p-1\}$ such that $\zeta_p^r \zeta_p^s = \zeta_p^k$, and then we have $x \equiv a\zeta_p^k \ (mod\ \lambda_p^2)$ and $y\zeta_p^s \equiv b\zeta_p^k \ (mod\ \lambda_p^2)$.

Passing to ideals we have $\langle x+y \rangle ... \langle x+\zeta_p^{p-1} \rangle = \langle \lambda_p \rangle^{pm} \langle z \rangle$. By the unique factorization into prime ideals, $\langle \lambda_p \rangle$ must divide some ideal on the left hand side of the above equation. Also, in the proof of the first case we showed that $\langle \lambda_p \rangle$ divides the difference $\langle (x+\zeta_p^i y) - (x+\zeta_p^j y) \rangle$ for any $i \neq j$, so $\langle \lambda_p \rangle$ must divide any ideal $\langle x+\zeta_p^i y \rangle$. In particular, $\langle \lambda_p \rangle | \langle x+\zeta_p^s y \rangle$. Then as $x+\zeta_p^s y \equiv \zeta_p^k(a+b) \ (mod\ \lambda_p^2)$ we have $\langle \lambda_p \rangle | \langle \zeta_p^k(a+b) \rangle = \langle a+b \rangle$ and taking norms we get $p|a+b$. Recall that $\langle \lambda_p \rangle^{p-1} = \langle p \rangle$, so $p, a+b \in \langle \lambda_p^2 \rangle$ and $x+\zeta_p^s y \equiv \zeta_p^k(a+b) \equiv 0 \ (mod\ \lambda_p^2)$. Hence,$\langle \lambda_p^2 \rangle | \langle x+\zeta_p^s y \rangle$ and therefore $\langle \lambda_p^{p+1} \rangle$ divides the left hand side, so $m > 1$.

Notice that, writing $x_1 = \zeta_p^{-k} x$, $y_1 = \zeta_p^{-r} y$, then $x_1^p + y_1^p = x^p + y^p$, so if x, y, z is a solution, then x_1, y_1, z is another solution. Therefore, we may assume $k = r = 0$ and $x + y \equiv a + b \ (mod\ \lambda_p^2)$.

Let x, y, z be a solution to the equation $x^p + y^p = u\lambda_p^m z^p$ with minimal m. We have $x + \zeta_p^i y = (x+y) + (\zeta_p^i - 1)y$, so for $i > 1$, as $\langle \lambda_p^2 \rangle | \langle x+y \rangle$ and $\langle \zeta_p^i - 1 \rangle = \langle \lambda_p \rangle$ by Corollary 3.7, then $\langle \lambda_p^2 \rangle \nmid \langle x+\zeta_p^i y \rangle$ because otherwise $\langle \lambda_p \rangle | \langle y \rangle$ which is a contradiction as both ideals are relatively prime. Hence, we find out that

$$\langle x+y \rangle = \langle \lambda_p \rangle^{p(m-1)+1} C_0$$

$$\langle x+\zeta_p^i y \rangle = \langle \lambda_p \rangle C_i \ \forall i = 1, ..., p-1$$

where the ideals C_i are principal and prime to $\langle \lambda_p \rangle$.

Claim 3. *The ideals C_i are pairwise relatively prime*

If there exists a prime ideal P dividing $\langle x+\zeta_p^i y\rangle, \langle x+\zeta_p^j y\rangle$ for some $i \neq j$, then in the proof of the first case we showed that either $P = \langle \lambda_p \rangle$ or $P|\langle y \rangle$. The first case is impossible since any C_i is coprime to $\langle \lambda_p \rangle$. For the second case, by the same reason, and the unique factorization into prime ideals, it follows that $P|\langle z \rangle$, which is a contradiction with $\langle y \rangle$, $\langle z \rangle$ being coprime.

From here we deduce $C_0 C_1 ... C_{p-1} = \langle z \rangle^p$ and therefore each C_i equals D_i^p for some ideal D_i. Since p is a regular prime and C_i is principal, D_i must be principal too and we can write $D_i = \langle \alpha_i \rangle$ for some $\alpha_i \in \mathbb{Z}[\zeta_p]$. By lemma 2.2 we have

$$x + y = u_0 \lambda_p^{p(m-1)+1} \alpha_0^p \tag{4.1}$$

$$x + \zeta_p y = u_1 \lambda_p \alpha_1^p \tag{4.2}$$

$$x + \zeta_p^2 y = u_2 \lambda_p \alpha_2^p \tag{4.3}$$

for some units $u_0, u_1, u_2 \in \mathbb{Z}[\zeta_p]$. Solving the system of equations (4.2) and (4.3) we get

$$x = u_2 \alpha_2^p - \zeta_p u_1 \alpha_1^p$$

$$y = \zeta_p^{-1}(u_1 \alpha_1^p - u_2 \alpha_2^p)$$

and substituting into (4.1) we have

$$-\lambda_p \zeta_p^{-1}((1+\zeta_p)u_1 \alpha_1^p - u_2 \alpha_2^p) = u_0 \lambda_p^{p(m-1)+1} \alpha_0^p$$

By corollary 3.6, $1+\zeta_p$ is a unit so $-\zeta_p^{-1}(1+\zeta_p)u_1$ is also unit. Therefore we can cancel λ_p from both sides and multiply by $(-\zeta_p^{-1}(1+\zeta_p)u_1)^{-1}$. Thus, $e := u_0(-\zeta_p^{-1}(1+\zeta_p)u_1)^{-1}$ and $e_2 := u_2((1+\zeta_p)u_1)^{-1}$ are units in $\mathbb{Z}[\zeta_p]$ and we have

$$\alpha_1^p + e_2 \alpha_2^p = e \lambda_p^{p(m-1)} \alpha_0^p \tag{4.4}$$

Notice that as C_2 and $\langle \lambda_p \rangle$ are coprime then so D_2 and $\langle \lambda_p \rangle^p$ are. Therefore, $\mathbb{Z}[\zeta_p] = D_2 + \langle \lambda_p \rangle^p$, so in particular $1 = r\alpha_2 + h\lambda_p^p$ for some $r, h \in \mathbb{Z}[\zeta_p]$, and taking congruences modulo $\langle \lambda_p \rangle^p$ we get $r\alpha_2 \equiv 1 \ (mod\ \langle \lambda_p \rangle^p)$, which implies $(r\alpha_2)^p \equiv 1 \ (mod\ \langle \lambda_p \rangle^p)$. So, taking congruences modulo $\langle \lambda_p \rangle^p$ in (4.4) we have, as $m > 1$ and p is odd, $\alpha_1^p \equiv -e_2 \alpha_2^p \ (mod\ \langle \lambda_p \rangle^p)$ which implies $e_2 \equiv (-\alpha_1 r)^p \ (mod\ \langle \lambda_p \rangle^p)$. In other words, e_2 is congruent to a p^{th} power modulo $\langle \lambda_p \rangle^p$, so applying Theorem 4.6 we have $e_2 = f^p$ for some unit f in $\mathbb{Z}[\zeta_p]$. Finally, setting $x' = \alpha_1,\ y' = f\alpha_2,\ z' = \alpha_0$, we see that x', y', z' is a solution of the equation $x^p + y^p = e\lambda_p^{pm'} z^p$, with $\langle x' \rangle, \langle y' \rangle, \langle z' \rangle, \langle \lambda_p \rangle$ pairwise relatively prime, $m' = m-1$ and e unit in $\mathbb{Z}[\zeta_p]$. This is a contradiction with m being minimal. Thus, the second case of Fermat's Last Theorem is proved. □

Chapter 5

Final breaktrough

In retrospective, the introduction of the notion of regular primes has allowed us to prove Fermat's Last Theorem for a quantitative amount of prime numbers just carrying information from the unique factorization into prime ideals of some number rings into the factorization of its elements, but what happens with the primes that are not regular? In fact, there are infinitely many irregular primes and the methods we have introduced are not enough to prove those cases in a general way, so we need to take a different approach. It was not until the second half of last century when some mathematicians started to think that a deeper connection between two apparently distinct branches of mathematics could help to give a general proof of Fermat's Last Theorem. These two topics are respectively elliptic curves and modular forms.

Definition. *An elliptic curve E over $\mathbb{Q}$, denoted by $E/\mathbb{Q}$, is an algebraic curve defined by an equation of the form $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}$, which is non-singular, meaning that $P(x) = x^3 + ax + b$ does not have a multiple root.*

An elliptic curve can be defined in an arbitrary field L but we are just interested in what happens when $L = \mathbb{Q}$. Any solution (x, y) of $y^2 = P(x)$ lies on $\mathbb{C} \times \mathbb{C}$. Let K be any field extension of $\mathbb{Q}$. We say that any of these solutions (x, y) is a K-rational point of E if $x, y \in K$ or $(x, y) = O$, where O denotes the point at infinity we add to the curve. We denote the set of K-rational points of E as $E(K)$. By symmetry of $y^2 = P(x)$ to the x-axis, if $P \in E(K)$, then $-P \in E(K)$ too. Also, given any $O \neq P, Q \in E(K)$, with $Q \neq -P$, we can associate $P + Q$ to an unique $R \in E(K)$. Furthermore, defining $P + O = P = O + P$ and $P + (-P) = O$ for any $P \in E(K)$ we get that $(E(K), +)$ is an abelian group with identity O. In particular, this happens when we consider $K = \overline{\mathbb{Q}}$. A point $P \in E(\overline{\mathbb{Q}})$ is called an n-torsion point if its order divides n. We denote by $E[n]$ the set of all n-torsion points in $E(\overline{\mathbb{Q}})$, which can be checked to be a finite subgroup of $(E(\overline{\mathbb{Q}})+)$.

Let p be a prime number, we have $\mathbb{Z}_{(p)} := \{\frac{m}{n} \in \mathbb{Q} : m, n \in \mathbb{Z} \ \ m, n \text{ prime to } p\}$. For any $a = \frac{m}{n} \in \mathbb{Z}_{(p)}$ we define the reduction of $a \ mod \ p$ as $(a \ mod \ p) = (m \ mod \ p)(n^{-1} \ mod \ p)$, which is an element of the finite field $\mathbb{Z}_p$. It is well-defined since n is prime to p. If we take an elliptic curve $E/\mathbb{Q}$ we can always find a change of coordinates such that each coefficient of $P(x)$ belongs to $\mathbb{Z}_{(p)}$. Therefore, its reduction $mod \ p$ will be an equation with coefficients in $F_p := \mathbb{Z}_p$. This motivates the following definitions:

Definition. *Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime number. We say that $E/\mathbb{Q}$ has good reduction mod p if we can choose a change of coordinates such that the reduced equation in F_p does not have a multiple root. We say that $E/\mathbb{Q}$ has a multiplicative reduction if the reduced equation contains a double root but not a triple root. Otherwise we say that $E/\mathbb{Q}$ has an additive reduction.*

Remark. *These definitions may make sense also when $p = 2$ but the characterizations is quite different (see [11, Def 1.5]).*

If an elliptic curve $E/\mathbb{Q}$ has either good or multiplicative reduction at all primes we say that E is semistable. It can be seen that any elliptic curve has good reduction at almost all primes. For a

semistable elliptic curve $E/\mathbb{Q}$ we define the conductor of E, written N_E, as the product of all primes at which E has not a good reduction.

Let p an odd prime at which $E/\mathbb{Q}$ has a good reduction and consider the reduced elliptic curve *mod* p defined by $y^2 = \overline{P}(x) \in F_p[x]$, and let $E_p(F_p) := \{(x,y) \in F_p \times F_p : y^2 = \overline{P}(x)\} \cup O$. We define $a_p(E) := p+1-|E_p(F_p)|$. We can also define $a_2(E)$ and $a_p(E)$ and for odd primes with multiplicative reduction, but the construction is a bit different (see [11, Def 1.13]). One nice property of these coefficients $a_p(E)$ is that they do not depend neither on the defining equation for $E/\mathbb{Q}$ nor on the reduced equation in F_p. Thus, these coefficients contain plenty of information about the elliptic curve.

We introduce now the concept of a modular form. Let's denote $\mathscr{H} := \{z \in \mathbb{C} : Imz > 0\}$. The special linear group $SL(2,\mathbb{Z})$ acts on $\mathscr{H}$ by fractional linear transformations with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$ acting as $z \to \frac{az+b}{cz+d}$. For any $N \in \mathbb{N}$, we define $\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2,\mathbb{Z}) : c \equiv 0 \pmod{N}\}$, which is a subgroup of $SL(2,\mathbb{Z})$. Modular forms arise as holomorphic functions on $\mathscr{H}$ that behave nicely under the action induced by certain of these subgroups of $SL(2,\mathbb{Z})$. More concretely:

Definition. *For $k \in \mathbb{Z}$, a weight-k modular form of level N is a holomorphic function $f : \mathscr{H} \to \mathbb{C}$, which is also holomorphic at $i\infty$, and satisfies*

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad \forall \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$$

From this definition we deduce $f(z+1) = f(z)\ \forall z \in \mathscr{H}$, so f is 1-periodic. As f is holomorphic, it can be deduced from these two facts that f has a power series expansion $f(z) = \sum_{i=1}^{\infty} a_n(f) q^n$ for any $z \in \mathscr{H}$, where $q = e^{2\pi i z}$ and $a_n(f) \in \mathbb{C}\ \ \forall n \in \mathbb{N}$. We call such series the q-expansion of f.

We will only consider weight-2 modular forms from now on. Let's denote by $S(N)$ the set of all weight-2 modular forms of level N, which is a finite dimensionl vector space over $\mathbb{C}$. For each integer $n \geq 1$, we have the so-called n^{th} Hecke operator T_n , which is an endomorphism of $S(N)$. The elements of $S(N)$ having special arithmetic interest are the normalized eigenforms of $S(N)$. These are non-zero $f = \sum_{i=1}^{\infty} a_n(f) q^n$ which are eigenvectors for all the T_n and which satisfy the normalizing condition $a_1 = 1$. Furthermore, for such eigenforms, $T_n(f) = a_n(f) f\ \ \forall n \geq 1$, and any $a_n = a_n(f)$ is an algebraic integer. In fact, the subfield $K \subset \mathbb{C}$ generated by all the coefficients a_n is a number field. We say that any $f = \sum_{i=1}^{\infty} a_n(f) q^n \in S(N)$ is a new form if it is a normalized eigenform of $S(N)$ for which the space $\{g \in S(N) : T_p(g) = a_p(g) g$ for all p prime to $N\}$ contains only f and its multiples.

The main point that led to prove Fermat's Last Theorem was the hidden relation between elliptic curves and modular forms. We say that an elliptic curve $E/\mathbb{Q}$ is modular if there exists a new form $f \in S(N_E)$ that satisfies $a_p(E) = a_p(f)$ for all primes p such that $p \nmid N_E$. In the 1950s and 1960s Goro Shimura, drawing on ideas posed by Yutaka Taniyama, conjectured that every elliptic curve $E/\mathbb{Q}$ was modular. This conjecture was known as the Taniyama-Shimura conjecture. André Weil made some advances on the conjecture giving conceptual evidence for that, but its possible proof looked inacessible for the techniques of those years. In 1985 Gerhard Frey made a crucial connection between Taniyama-Shimura conjecture and Fermat's Last Theorem. He assumed that for some prime $p \geq 5$ there is a non-trivial integral solution $a^p + b^p = c^p$. After manipulating the coefficients he could assume b even and $c \equiv 1\ (mod\ 4)$. Then he defined the elliptic curve $y^2 = x(x-a^p)(x+b^p)$, which is known as a Frey curve. This elliptic curve is therefore defined over $\mathbb{Z} \subset \mathbb{Q}$ and satisfies some interesting properties. For example, it is semistable and all its 2-torsion points are $\mathbb{Q}$-rational. In 1986 Ken Ribet proved that any Frey curve is not modular. Therefore, if Taniyama-Shimura conjecture was true this curve could not exist, which would imply that there cannot be a counterexample for Fermat's Last Theorem. Hence, as any Frey curve is semistable, the only step needed for achieving a general proof of Fermat's Last Theorem was to prove Taniyama-Shimura conjecture for the semistable case.

For any $n \in \mathbb{Z}$, $E[n]$ is a free module of rank 2 over $\mathbb{Z}/n\mathbb{Z}$. Also, it is clear that for any $P \in E[n]$, the coordinates of P are algebraic numbers, so $E[n]$ is stable under the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E(\overline{\mathbb{Q}})$. Therefore, any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ induces an automorphism of $E[n]$. The main disadvantage of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is that it is an infinite group, so we may not be able to apply all Galois Theory we know. But it has also a structure of topological group, meaning a group with an atttached topology, which let us find analogous theorems to the ones in finite Galois groups. Finite groups can also be attached with a topology. In fact, chosen a $\mathbb{Z}/n\mathbb{Z}$- basis for $E[n]$ and the accurate topologies, we have a (continuous) homomorphism, called a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(2, \mathbb{Z}/n\mathbb{Z})$$

as $Aut(E[n]) \cong GL(2, \mathbb{Z}/n\mathbb{Z})$. Looking at $H = \mathrm{Ker}\rho_{E,n}$ we see that it is a normal subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ so, thanks to the topological structure of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, it can be related to a finite Galois extension $K_n/\mathbb{Q}$ in a unique way. More concretly, K_n is the number field generated by the coordinates of every element in $E[n]$ and $H = \mathrm{Gal}(\overline{\mathbb{Q}}/K_n)$. Even if some of these extensions are infinite we can apply first isomorphism theorem and say

$$\mathrm{Im}\rho_{E,n} \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{\mathbb{Q}}/K_n) \cong \mathrm{Gal}(K_n/\mathbb{Q})$$

Thus, we can identify $\mathrm{Gal}(K_n/\mathbb{Q})$ with the image of $\rho_{E,n}$, which is a subgroup of $GL(2, \mathbb{Z}/n\mathbb{Z})$. A very nice property of this extension $K_n/\mathbb{Q}$ is that if there is a prime $p \nmid n$ such that $E/\mathbb{Q}$ has good reduction at p then p is unramified in K_n. So, regarding what we did in the last chapter, for any prime ideal Q_i lying over $\langle p \rangle$ in $\mathfrak{O}_{K_n}$ we can find an unique element $\sigma_{p_i} \in \mathrm{Gal}(K_n/\mathbb{Q})$ related to the Frobenius element φ_p of the residue field $\mathfrak{O}_{K_n}/Q_i$. This σ_{p_i} is also known as the Frobenius element for Q_j. We said also that any of this σ_{p_i} is conjugate to all the others, where Q_i runs over all prime ideals lying over $\langle p \rangle$, so writing σ_p for one of them, it is well-defined up to conjugation. By linear algebra we know that the trace of a matrix is independent of the basis we choose and also it is invariant under conjugation of matrices. Therefore, for any prime number $p \nmid n$ with good reduction, $tr(\sigma_p)$ is well-defined. Furthermore, we have the nice relation $tr(\sigma_p) \equiv a_p \ (mod\ n)$. Thus, these representations $\rho_{E,n}$ encapsulates lot of information about $E/\mathbb{Q}$.

On the other hand, we know that the coefficients $a_n(f)$ of any normalized eigenform $f \in S(N)$ are algebraic integers and that $K = \mathbb{Q}(a_1(f), a_2(f), ...)$ is a number field. Let p a prime number and let λ a prime ideal $\mathfrak{O}_K$ lying over $\langle p \rangle$. Therefore, $F_\lambda = \mathfrak{O}_K/\lambda$ is a finite field of characteristic $0 \neq l$. We can also define, for any p prime, a conjugacy class $Frob_p$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in a slightly different way from what we have done for K_n. Similarly as above, we can find a (continuous) representation

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(2, F_\lambda)$$

which is characterized by the property that for any prime number $p \nmid Nl$ then
$tr(\rho_{f,\lambda}(\mathrm{Frob}_p)) \equiv a_p(f) \ (mod\ \lambda)$.

We see that these representations, known as Galois representations, could let us find deeper relations between elliptic curves and modular forms. In fact, it was through the study of Galois representations attached to elliptic curves and modular forms how Andrew Wiles after several years of effort, with the final help of Richard Taylor, proved Taniyama-Shimura conjecture for semistable elliptic curves over $\mathbb{Q}$ and, finally, Fermat's Last Theorem.

Bibliography

[1] N. JACOBSON, *Basic Algebra II* (Second Edition), Dover Publications Inc., 2012.

[2] A. ELDUQUE, *Groups and Galois Theory*, http://personal.unizar.es/elduque/files/GroupsGalois2019.pdf.

[3] I. STEWART AND D. TALL, *Algebraic Number Theory and Fermat's Last Theorem* (Third edition), A K Peters/CRC Press, Natick, Massachusetts, 2001.

[4] ROBERT G. UNDERWOOD, *Fundamentals Of Modern Algebra: A Global Perspective*, World Scientific Publishing Company, 2015 .

[5] DANIEL A. MARCUS, *Number Fields* (Second Edition), Springer-Verlag, New York, 1977.

[6] EMILY RIEHL, *Kummers Special Case of Fermats Last Theorem*, https://wstein.org/129-05/final_papers/Emily_Riehl.pdf.

[7] DAVID JAO, *FERMATS LAST THEOREM FOR REGULAR PRIMES*, https://epdf.pub/fermats-last-theorem-for-regular-primes.html.

[8] ANTHONY W. KNAPP, *Advanced Algebra*, Birkhuser 1st ed. 2008, Corr. 2nd printing 2015.

[9] KENZ KALLAL, *RAMIFICATION IN ALGEBRAIC NUMBER THEORY AND DYNAMICS*, http://math.uchicago.edu/~may/REU2018/REUPapers/Kallal.pdf.

[10] E. ARTIN AND J. TATE, *CLASS FIELD THEORY*, W.A.BENJAMIN, INC. ADVANCED BOOK PROGRAM, Reading, Massachusetts, 1967.

[11] TAKESHI SAITO, *Fermat's Last Theorem: Basic Tools*, Translations of Mathematical Monographs,Iwanami Series in Modern Mathematics, 2013.

[12] KENNETH A. RIBET, *Galois representations and modular forms*, Bull. Amer. Math. Soc.(N.S.) **32** (1995), 375-402.