SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

From the Riemann Zeta L-function to the Artin L-function

av

Sejad Ali Kais

2026 - No K19

From the Riemann Zeta L-function to the Artin L-function

Sejad Ali Kais

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Jonas Bergström

2026

1 Abstract

The thesis starts by talking about the Riemann Zeta function and then goes to develop the necessary algebraic number theory and representation tools to define and motivate the Artin L-function.

The Artin L-function generalizes the Riemann Zeta function and the Dirichlet, Dedekind, and Hecke L-functions.

We further prove that the Artin L-function admits a meromorphic continuation.

The thesis focuses more on building the foundation to motivate the necessary machinery to define the Artin L-function and prove its meromorphic continuation, starting from the integers, expanding proofs and giving examples.

Uppsatsen inleds med en diskussion om Riemanns Zeta-funktion och utvecklar därefter nödvändig algebraisk talteori och representationsverktyg för att definiera och motivera Artins L-funktion.

Artins L-funktion generaliserar Riemanns Zeta-funktion, och Dirichlet Dedekind och Hecke L-funktioner.

Vi visar vidare att Artins L-funktion medger en meromorf fortsättning.

Uppsatsen fokuserar främst på att bygga fundamentet för att motivera det maskineri som krävs för att definiera Artins L-funktion och bevisa dess meromorfa fortsättning, med utgångspunkt i heltalen, genom att expandera bevis och ge exempel.

2 Introduction

We will start with considering a specific sum, $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Mathematicians knew that this sum converged for $s > 1$, but they did not know any values, that is until Euler in the year 1734 proved that for $s = 2$ we have that $\zeta(2) = \frac{\pi^2}{6}$, this is called the Basel Problem, after his hometown, Basel at the time.

What he also showed is that this function encodes information about primes, we will sketch his idea below:

Sketch 1. $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ *, if we factor out* $\frac{1}{2^s}$ *we get that* $\zeta(s) - \frac{1}{2^s}\sum_{n=1}^{\infty} \frac{1}{n^s} = (\sum_{n=1,2\nmid n}^{\infty} \frac{1}{n^s})$*. So we have* $\zeta(s)(1 - \frac{1}{2^s}) = (\sum_{n=1,2\nmid n}^{\infty} \frac{1}{n^s})$*, now if we do this for all primes we eventually get* $\zeta(s)\Pi(1 - \frac{1}{p^s}) = 1$*, and solving for* $\zeta(s)$ *we have that* $\prod_p \frac{1}{1-p^{-s}}$*. We call* $\prod_p \frac{1}{1-p^{-s}}$ *the Euler product.*

This is a sketch of Euler's idea.

Here are some properties of this function.

Theorem 1 ([1, prop. 419-420])**.** *Let* $E = \{s \in \mathbb{C} | \Re(s) > 1\}$*, then* $\zeta(s)$ *converges* $\forall s \in E$*.*

Theorem 2 ([1, theorem 425-426]). *Denote* $\mathfrak{Z}(s) := \pi^{-s\frac{1}{2}}\Gamma(\frac{1}{2}s)\zeta(s)$. *The function* $\mathfrak{Z}(s)$ *is analytic for all* $s \in \mathbb{C}/\{0,1\}$ *and satisfies the following functional equation.*

$$\mathfrak{Z}(s) = \mathfrak{Z}(1-s).$$

Theorem 3 ([1, cor 425-426]). *The Riemann Zeta Function* $\zeta(s)$ *admits an analytic continuation to* $\mathbb{C}/\{1\}$ *with a simple pole at* $s = 1$*, reside of 1, and satisfies the functional equation*

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

The function $\zeta(s)$ was first proven to analytically extend to $\mathbb{C}/\{1\}$ in Bernhard Riemann's famous paper called, "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse"in the German language, published in 1859 and translates to "On the Number of Primes Less Than a Given Magnitude" in English.

This functional equation played a key role in study the distribution of primes over $\mathbb{Z}$ using analytical methods. It played a key role in the proof of the prime number theorem, which was proven in 1896 by Jaques Hadamard, and De La Vallée Poussin, independently.

Riemann went beyond the analytic continuation in this paper, he made a striking conjecture , called the Riemann Hypothesis, connecting the (non-trivial) zeros of the function $\zeta(s)$ to the distribution of primes. If the hypothesis is true, the hypothesis implies a stronger result than that of the prime number theorem.

In this thesis we will build enough theory to define an L function defined by Emil Artin. We will need quite a bit of algebra, in chapter 3, named *Algebra* we will first how we will generalize the integers $\mathbb{Z}$ and the rationals $\mathbb{Q}$, what problems we stumble upon and how it was resolved. e will also define what a module is, since our extension of $\mathbb{Z}$ will be modules, which simplifies their study and which we cover in chapter 4, called "Our ring of integers are $\mathbb{Z}$-modules".

We will then introduce the necessary Galois Theory in chapter 5 and see how it acts on extensions of $\mathbb{Z}$, and the corresponding primes in chapter 6.

In Chapter 7, named Frobenius element, we will have a "new version of a prime" in the Euler product from sketch 1. In chapter 8 we will give a brief introduction to representation theory, including examples but also the theory necessary to define our Artin L-functions.

In chapter 9 we finally have built enough machinery to define the Artin L-function and we prove its well defined-ness and other important properties. We show that it is a generalization of some L-functions, including the Riemann zeta function $\zeta(s)$. But unlike $\zeta(s)$ it turns out that, there is no prove that the Artin L-functions admit an analytic continuation to $\mathbb{C}/\{1\}$, but there is a conjecture made by Emil Artin himself, conjecturing that it admits a analytic continuation to $\mathbb{C}$ except a potential pole at $s = 1$. Richard Brauer did however prove it

admits a meromorphic continuation, our main goal for the thesis is to build the machinery from scratch and in the end being able to state Artin's Conjecture and proving that they admit an meromorphic continuation in chapter 10.

3 Algebra

3.1 Field extensions and Ring extensions

Let $\mathbb{Q}$ be the rational numbers. Then we can ask, if there is a finite field extension K of $\mathbb{Q}$ so that the polynomial $x^2 - 1 = 0$ has all solutions in K and that $K \neq \mathbb{C}$. It turns out to be (infinitely) many such field extensions, and we thus ask , what is the smallest such field K.

For our specific case it turns out that it is the field:

$$\mathbb{Q}(i) := \{a + bi | a, b \in \mathbb{Q}\}$$

which is a $\mathbb{Q}$-Vector space of dimension two.

Another way to view $\mathbb{Q}(i)$ is by looking at the quotient $\mathbb{Q}[x]/(x^2 + 1)$ which is isomorphic to $\mathbb{Q}(i)$ via the fact that $x^2 - 1$ is the "minimal polynomial" for i over $\mathbb{Q}$.

This pattern holds more generally, and we will introduce the relevant definitions and propositions below. We will denote a field extension L over K as L/K. When our L is a finite extension of $\mathbb{Q}$ we will denote it as a number field.

Definition 1. *An element α i L is called algebraic if it satisfies a non-zero, polynomial in $K[x]$.*

Definition 2 ([2, prop p.520])**.** *The minimal polynomial for an algebraic element α over a field K, is the polynomial, denoted $m_\alpha(x)$ such that:*

1. $m_\alpha(\alpha) = 0$
2. $m_\alpha(x)$*is irreducible over* K
3. $m_\alpha(x)$ *is monic.*

Proposition 1 ([2, Ch 13])**.** *Let α is algebraic over a field L. Then $m_\alpha(x) \in L[x]$ exists and is unique.*

Proposition 2 ([2, prop 521])**.** *Let α be algebraic over the field K, and let $K(\alpha)$ be the field generated by α over K, then: $K(\alpha) \cong K[X]/m_\alpha(x)$ and in particular , the degree of $F(\alpha)$ over F, denoted as $|K(\alpha) : K| = deg(m_\alpha)$.*

Note that by a finite field extension we mean $|F(\alpha) : F| < \infty$. We will from now on say field extensions, instead of "finite field extensions" because we will not work over infinite field extensions.

Definition 3. *The splitting field of an irreducible polynomial $p(x)$ in a field K is the smallest field L such that $p(x)$ splits completely.*

Definition 4. *We will define $z \in \mathbb{C}$ as a nth root of unity if $z^n = 1$.*

We will denote a root of unity as a primitive nth root of unity as $\zeta_n := e^{\frac{2\pi ik}{n}}$ for $k < n$ and $gcd(n, k) = 1$.

Example 1. *For $\alpha = i$ over the field $K = \mathbb{Q}$, the minimal polynomial is $m_i(x) = x^2 + 1$.*

We have $m_i(i) = 0$. The polynomial $m_i(x)$ is also monic. If it were reducible, $i \in \mathbb{Q}$ would need to hold since $deg(m_i(x)) = 2$. And we know that is not true. And this has splitting field $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}(i)$.

Example 2. *An example is the minimal polynomial $m_{\sqrt{2}}(x) = x^2 - 2$, which gives rise to $\mathbb{Q}(\sqrt{2})$ via proposition 2 above.*

Example 3. *Let ζ_3 be a primitive third root of unity, we have the minimal polynomial $m_{\zeta_3}(x) = x^2 + x + 1$ as the minimal polynomial which gives rise to $\mathbb{Q}(\zeta_3)$.*

Definition 5. *We will define the cyclotomic polynomial $\Phi_n(x) := \prod_{i=1}^{n}(x - \zeta_i)$ where ζ_n are primitive nth roots of unity.*

Example 4.

We one might want to generalize the notion of integers and define a new extension to $\mathbb{Z}$ corresponding to our new field extension $\mathbb{Q}[i]$ which we discussed at the beginning of the chapter. It turns out that $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ would have the properties we desire.

But counter-intuitively, for the field extension $\mathbb{Q}(\sqrt{5})$ with minimal polynomial $x^2 - 5$, the ring $\mathbb{Z}[\sqrt{5}]$ turns out to not be enough. The issue is that $\mathbb{Z}[\sqrt{5}]$ is missing a crucial property over $\mathbb{Q}(\sqrt{5})$ that the integers $\mathbb{Z}$ posses over $\mathbb{Q}$.

Namely consider, $\alpha := \frac{1+\sqrt{5}}{2}$ which satisfies the polynomial $x^2 - x - 1 = 0$, which is a monic polynomial in $\mathbb{Z}[x]$. And one sees that $\alpha \notin \mathbb{Z}[\sqrt{5}]$.

We would want every element in $\mathbb{Q}(\sqrt{5})$ which satisfies a monic non-zero polynomial over $\mathbb{Z}[x]$ to be in our extension over $\mathbb{Z}$ which we are trying to define.

Remark 1. *The elements $q \in \mathbb{Q}$ which satisfy an irreducible monic, non-zero equation over $\mathbb{Z}$ turn out to be the elements $q \in \mathbb{Q} \cap \mathbb{Z} = \mathbb{Z}$.*

We will define the property we want down below.

Definition 6. *For commutative rings A, B and $A \subseteq B$, we say that $b \in B$ is called integral over a sub-ring A if b satisfies a non-zero monic polynomial in $A[x]$. If every element in B satisfies this property we call B an integral extension of A.*

We will from now we assume that our rings are commutative with a 1, unless we say otherwise.

Definition 7. *For rings $A \subseteq B$ we define:*

$$\overline{A} := \{b \in B |\ b \text{ integral over } A\}.$$

We call $\overline{A}$ the integral closure of A over B.

If $A = \overline{A}$ we say that A is integrally closed.

Proposition 3 ([1, Prop. on p. 7])**.** *For a tower of ring extensions $A \subseteq B \subseteq C$ we have transitivity, i.e. if B is integral over A and C integral over B , then C is integral over A.*

More specifically from now on we consider integral domains A , which is integrally closed, with field of fraction K where $K/\mathbb{Q}$, and B being its integral closure in L/K.

Definition 8. *Let K be a field and $K \subset L$ be a field extension. Then we denote the ring of integers as $\mathcal{O}_L$ is defined as:*

$$\mathcal{O}_L = \{\alpha \in L | \alpha \text{ integral over } \mathbb{Z}\}.$$

Definition 9. *An element u in a ring R is called a unit, if there exists an element v such that:*

$$uv = vu = 1.$$

Definition 10. *Two elements x, y in a ring R are called associates if they can be written as $ux = y$ where u is a unit in R.*

For example in $\mathbb{Z}$ our units are $-1, 1$ while in any field, every element except 0 is a unit.

Remember that over $\mathbb{Z}$ we have unique factorization of the integers into irreducible elements factors, up to units.

We would want this to hold for our ring of integers. But sadly this does not hold, consider the example below.

Example 5. *We will consider $\mathbb{Q}(i\sqrt{5})$. It turns out that its ring of integers is $\mathbb{Z}(\sqrt{-5})$ by proposition 13.*

Consider $6 \in \mathbb{Z}(i\sqrt{5})$. We then get:

$$6 = 3 \cdot 2 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

We will show that our elements are irreducible in $\mathbb{Z}(\sqrt{-5})$.

Let $\alpha, \beta \in \mathbb{Z}(\sqrt{-5})$. We define:

$$N_{\mathbb{Q}(\sqrt{-5})}(\alpha) := (a + b\sqrt{5})(a - b\sqrt{5}) = (a^2 + 5b^2).$$

and it is easy to see that it is multiplicative, i.e.:

$$N_{\mathbb{Q}(\sqrt{-5})}(\alpha\beta) = N_{\mathbb{Q}(\sqrt{-5})}(\alpha) N_{\mathbb{Q}(\sqrt{-5})}(\beta)$$

. *We justify this generally later, via proposition 4 and theorem 14.*

If 2 *were reducible, then there would exist two elements* $\alpha, \beta \in \mathbb{Z}(\sqrt{-5})$ *such that:*

$$\begin{aligned} 2 = \alpha\beta \implies \\ N_{\mathbb{Q}(\sqrt{-5})}(2) = \\ 4 = \\ N_{\mathbb{Q}(\sqrt{-5})}(\alpha\beta) = \\ N_{\mathbb{Q}(\sqrt{-5})}(\alpha)N_{\mathbb{Q}(\sqrt{-5})}(\beta). \end{aligned}$$

Now one can conclude that $(N_{\mathbb{Q}(\sqrt{-5})}(\alpha), N_{\mathbb{Q}(\sqrt{-5})}(\beta))$ *must take on the values* $(1,4),(2,2)$ *or* $(4,1)$*. But the values containing* 1 *would just give us associates of* 2 *in* $\mathbb{Z}$ *by propositions 16, 17.*

WLOG if $N_{\mathbb{Q}(\sqrt{-5})}(\alpha) = 2$ *then:*

$$2 = a^2 + 5b^2$$

which has no integer solutions, and if $N_{\mathbb{Q}(\sqrt{-5})}(\alpha) = 4$ *then:*

$$4 = a^2 + 5b^2$$

only has solutions $a = \pm 2$*, so they are associates to* 2*.*

For the same pattern follows. We do the same for 3 *and we get:*

$$9 = N_{\mathbb{Q}(\sqrt{-5})}(\alpha), N_{\mathbb{Q}(\sqrt{-5})}(\beta)).$$

It directly follows that $N_{\mathbb{Q}(\sqrt{-5})}(\alpha) = 3$ *has no solutions and the case* $(1,9)$ *has only trivial solutions as noted for the earlier example.*

For $1 \pm \sqrt{-5}$ *we do the same argument:*

$$N_{\mathbb{Q}(\sqrt{-5})}(1 \pm \sqrt{-5}) = 6 = N_{\mathbb{Q}(\sqrt{-5})}(\alpha)N_{\mathbb{Q}(\sqrt{-5})}(\beta)$$

, we already know that any tuple containing 3 *or* 2 *cannot happen, and our only option is thus* $(1,6)$ *or* $(6,1)$ *which will imply that either* $\alpha = \pm 1$ *or* $\beta = \pm 1$ *and this is a unit and so the elements they will be associates once again.*

And $3, 2, 1 \pm \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ *are not units because their multiplicative inverses are not in the ring.*

This illustrates that we might lose the ability to factorize elements too unique irreducible factors up to units and that even though 2 *and* 3 *divide the product* $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$ *they don't divide either of the elements* $(1+\sqrt{-5})(1-\sqrt{-5})$ *separately.*

And the same holds for the other direction, by definition $(1 \pm \sqrt{-5})|2 \cdot 3 = 6$*, but it does not divide* 2 *or* 3*.*

But there is some hope to save the example above. Kummer thought we could save this by introducing something he called "ideal numbers" and "ideal prime numbers" which would return unique factorization of "ideal numbers" into these "ideal prime numbers".

Dedekind, inspired by Kummer's ideas introduced these "ideal numbers" as ideals to the ring of integers. We will define notion of ideal division for ideals of a Ring of integers.

Definition 11. *For two ideals* $\mathfrak{a}, \mathfrak{b} \in \mathcal{O}_k$ *we define:*

$$\mathfrak{a}|\mathfrak{b}$$

as

$$\mathfrak{b} \subseteq \mathfrak{a}$$

.

Example 6. *Now here is Kummer's/Dedekind's attempt to save unique factorization. We have* $(6) = (2)(3)$ *as ideals. It turns out that* $(3) = \mathfrak{p}_1\mathfrak{p}_2$ *for two ideals of* $\mathbb{Z}[\sqrt{-5}]$*. We will work out the case of* (3) *and the rest follow similarly. We want* $\mathfrak{p}_1|(3)$*, so by definition we need* $\mathfrak{p}_1$ *to include* (3) *and we need* $\mathfrak{p}_2$ *to include* (3) *for the same reason.*

We also need $\mathfrak{p}_1\mathfrak{p}_2 = (3)$ *in the end. So, we would want the products of all generators to lie in* (3) *when multiplied together. One can see that* $\mathfrak{p}_1 = (3, 1 + \sqrt{-5})$ *and* $\mathfrak{p}_2 = (3, 1 - \sqrt{-5})$ *work. The fact :*

$$(3) \subset \mathfrak{p}_1, \quad (3) \subset \mathfrak{p}_2$$

is evident.

Now we want to show the equality, notice that:

$$\mathfrak{p}_1\mathfrak{p}_2 = (9, 3(1 + \sqrt{-5}), 3(1 - \sqrt{5}), 6).$$

Then $3 \in \mathfrak{p}_1\mathfrak{p}_2$ *because* $9 - 6 = 3$ *and so:*

$$(3) \subset \mathfrak{p}_1\mathfrak{p}_2.$$

The other inclusion follows directly because generators of $\mathfrak{p}_1\mathfrak{p}_2$ *are all products of* 3*.*

Following similar reasoning one can find that for:

$$\mathfrak{p}_3 = (2, 1 + \sqrt{-5}), \mathfrak{p}_4 = (2, 1 - \sqrt{-5})$$

we get,

$$(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = \mathfrak{p}_3\mathfrak{p}_4$$
$$(3, 1 - \sqrt{-5}) = \mathfrak{p}_4\mathfrak{p}_2.$$

So as ideals we have

$$(6) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_3\mathfrak{p}_1)(\mathfrak{p}_4\mathfrak{p}_2)$$

We can consider the ring homomorphism

$$\varphi : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_2, \quad (a + b\sqrt{-5}) \mapsto a - b \mod 2.$$

The surjection is clear, and $\ker(\varphi) = (2, 1 - \sqrt{5}) = \mathfrak{p}_4$. *Then the first isomorphism theorem gives us*

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}_4 \cong \mathbb{Z}_2$$

which prove that $\mathfrak{p}_4$ *is prime, since* $\mathbb{Z}_2$ *is a field. A similar proof works for the other prime ideals, so our elements o factor uniquely as prime ideals , and this is actually true for ring of Integers.*

Now the reader might remember that at the beginning of the chapter we defined the notion of integral elements and required this for ring of integers, and we said that this will be motivated later. Definition 13 and the theorem under it are the main motivation behind introducing Integrality.

Definition 12. *A ring is Noetherian if every ideal is finitely generated.*

Definition 13. *A Noetherian, integrally closed domain in which every non-zero prime ideal is maximal is called a Dedekind Domain.*

Theorem 4 ([1, Thm. p. 17])**.** *The Ring* $\mathcal{O}$ *is a Dedekind domain.*

Remark 2. *A proof will be shown in later at 4 , we need to introduce the necessary theory if finite fields and module theory for the proof. While modules and finite field theory is used to prove this, we think that our approach is more pedagogical.*

And now to theorem we have built up for.

Theorem 5 ([1, Thm. p. 18])**.** *In a Dedekind domain every prime ideal* $\mathfrak{a}$ *factorizes uniquely up to order as:*

$$\mathfrak{a} = \mathfrak{p}_1 ... \mathfrak{p}_r.$$

So as noted in example 6 we saw that we could save it introducing ideals. And the theorem above shows that, this is always doable.

3.2 Finite field discussion

We will also need to know about finite fields to understand our Ring of integers better. We will also later define Galois extensions and the finite fields will play a significant role in defining the Artin L-function.

Definition 14. *Let $\mathbb{F}$ be a finite field with q elements, we will define the character, $char(\mathbb{F}) = p$ as the lowest number p such that:*

$$1_{\mathbb{F}} + ... + 1_{\mathbb{F}} = p \cdot 1_{\mathbb{F}} = 0$$

.

Proposition 4 ([2, Ch 13])**.** *The characteristic of a field is either a prime number p or 0.*

As a immediate consequence of the proposition above we can conclude that a finite field has characteristic p for a prime number p, otherwise we would have infinitely many distinct elements in a finite field. For this reason we will denote finite fields with $\mathbb{F}_p$.

We can in the same way as we considered a finite field extensions K over $\mathbb{Q}$ a $\mathbb{Q}$-vector space, look at finite field extensions of $\mathbb{F}_p$ as finite $\mathbb{F}_p$-vector spaces.

Combining the characteristic argument and basic counting gives us that a finite extension over $\mathbb{F}_p$ of dimension n has p^n elements.

Proposition 5 ([4, Ch 7])**.** *Let $\mathbb{F}_{p^n}$ be a nth dimensional field extension over $\mathbb{F}_p$. The subfield of $\mathbb{F}_{p^n}$ are in one-to-one correspondents with divisors of n.*

This essentially says that:

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m|n$$

.

We will define an endomorphism for a finite field $\mathbb{F}$. This is the definition that will "replace" the primes in the Euler product for the Artin L-function.

Definition 15. *For $a, b \in \mathbb{F}_{p^n}$ we have the following fact. We define the Frobenius Endomorphism as:*

$$\varphi(a) = a^p$$

Proposition 6 ([2, Ch 13])**.** *The Frobenius Endomorphism defined on finite fields is injective and surjective, i.e. an automorphism.*

[2] ch 13.5, prop 35 and cor 36.

And we also have an existence result.

Theorem 6 ([4, Ch 7])**.** *Let $n \geq 1$ and p a prime number, then there exists a field $\mathbb{F}_{p^n}$.*

Theorem 7 ([2, Ch 13])**.** *A finite field of order p with p^n elements is unique up to isomorphism.*

Example 7. *The first example is $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. We give the explicit map:*

$$\psi(1_{\mathbb{F}}) = 1_{\mathbb{Z}/p\mathbb{Z}}, \quad \psi(n_{\mathbb{F},}) = n_{\mathbb{Z}/p\mathbb{Z}}.$$

Field homomorphisms are injective, both sides have the same characteristic, and so we also get that its surjective.

We will give an example of a more non-trivial finite field:

Example 8. *Consider $p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. To check that $p(x)$ is irreducible in $\mathbb{F}_2[x]$ it is sufficient to check that it admits no linear terms because it is of degree two. We check $f(1) = 1 \neq 0$ and $f(0) = 1 \neq 0$. So it is monic and irreducible. By theorem 6 there exists a field extension K and an $\alpha \in K$ such that $f(\alpha) = 0$. So $f(x)$ is a minimal polynomial of α over $\mathbb{F}_2[x]$.*

Then proposition 2 gives,

$$\mathbb{F}_2[x]/(x^2 + x + 1) \cong \mathbb{F}_2(\alpha), \quad [\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2.$$

By the uniqueness from proposition 7 we have:

$$\mathbb{F}(\alpha) \cong \mathbb{F}_4$$

3.3 Modules

We will define the notion of an $R - module$ since the ring of integers, as we will see will turn out to be $R - modules$. This turns out to be an important point of view in their study. We will also use module language in proving the meromorphic extension of our Artin L-functions which we are working towards.

Definition 16. *Let R be a ring. A left $R - module$ is a set M that has two binary operations. An internal law of addition:*

$$M \times M \to M, \quad (m, n) = m + b.$$

and scalar multiplication:

$$R \times M \to M, \quad (r, m) = rm$$

with the following axioms:

1. *i) $(M, +)$ is an abelian group.*
2. *For $1_r \in R$ and any $m \in M$ we have $1_r m = m$.*
3. *For any $r, r' \in R$ and any $m \in M$ we have $r(r'm) = (rr')m$*
4. *For any $r, r' \in R$ and any $m \in M$ we have $(r + r')m = rm + r'm$.*
5. *For any $r \in R$ and any $m, n \in M$ we have $r(m + n) = rm + rn$.*

A right $R - module$ is defined similarly but with the scalar action on the right. If R is commutative we do not have to worry about M being a left or right $R - module$.

Example 9. *An $R-$module is an abelian group from by the definition.*

More specifically if $R=\mathbb{Z}$ we get an equivalence. I.e every abelian group A is also a $\mathbb{Z}-$module defined via the map:

$$\mathbb{Z}\times A\to A,\quad n\in\mathbb{Z}, g\in A,\quad ng=\underbrace{g+g+g+...+g}_{n\ times}$$

It is straightforward to check that is a $\mathbb{Z}-$module from the axioms.

Example 10. *If R is field, then the $R-$module is just a vector space.*

Example 11. *Let R be a ring, then:*

$$R\times R\to R$$

is an $R-$module where the scalar is defined as just the internal ring multiplication.

If I is a left R ideal, then

$$R\times I\to I$$

is a left $R-$module with the multiplication from R on the left ideal I.

Definition 17. *Let R e a ring and M,N be two left $R-$modules, a homomorphism of $R-$modules is defined as a map:*

$$f:M\to N,\quad f(rm+r'n)=rf(m)+r'f(n)$$

for all $r,r'\in R$ and all $m\in M, n\in N$.

Definition 18. *If M is a left $R-$module , we say that N is a left $R-$submodule of M if:*

$(N,+)$ is an abelian subgroup of $(M,+)$.

for all $r\in R$ and all $n\in N$ we have $an\in N$.

Definition 19. *We say that M is a finitely generated, free R-module if we have a finite set $B=\{m_1,...,m_n\}$ which generates every element $m\in M$ as a finite sum $\sum r_im_i$ for $r_i\in R, m_i\in M$ and if $\sum r_im_i=0$ we must have all $r_i=0$.*

The module theory folloes the treatment from [[3, Ch 3]].

4 Our ring of integers are $\mathbb{Z}$-modules

Definition 20. *A polynomial $p(x)\in K[x]$ is called separable if it has no multiple factors in its splitting field. I.e. if $p(x)$ splits as*

$$p(x)=a(x-\alpha)^{m_1}...(x-\alpha_n)^{m_n}$$

in its splitting field, all m_i are equal to one.

Proposition 7 ([2, Ch 13]). *If a field F is finite , or its characteristic is equal to zero, a polynomial is irreducible if and only if it is separable*

All our fields we will work with will be separable unless we say otherwise.

Proposition 8 ([1, prop. pp. 12–13]). *If L/K is separable and $A = frac(K)$ is a principal domain, and B its integral closure then every finitely generated B-submodule $M \neq 0$ of L is a free A-module of rank $[L : K]$, in particular B admits an integral basis over A.*

In particular an if $K = \mathbb{Q}$ then $A = \mathbb{Z}$ we get that every ring of integer $\mathcal{O}_L$ is a free $\mathbb{Z}$-module.

Proposition 9 ([1, prop. p. 15]). *If $\alpha \subseteq \alpha'$ are two non-zero finitely generated $\mathcal{O}_k$-modules of K , then we have:*

$$d(\alpha) = (\alpha' : \alpha)^2 d(\alpha')$$

and The index above $(\alpha' : \alpha)^2$ is finite and denotes the index $|\alpha'/\alpha|$ of the additive subgroups form the underlying module structure.

Definition 21. *If $\mathfrak{p}$ is any non-zero ideal of $\mathcal{O}_k$, then $N(\mathfrak{p}) = |\mathcal{O}_k/\mathfrak{p}|$ is called the **Ideal Norm**.*

Finiteness comes from the fact that $\mathcal{O}_k$ is a module over itself and that the ideal $\mathfrak{p}$ is a $\mathcal{O}_k - module$ and prop 9. $\mathcal{O}_k$ is also multiplicative.

Proposition 10 ([1, prop. p. 35]). *If $\mathfrak{a} = \mathfrak{p_1}^{f_1}\mathfrak{p_2}^{f_2}...\mathfrak{p_n}^{f_n}$ is the prime factorization of a non-zero prime ideal $\mathfrak{a} \neq 0$ we have:*

$$N(\mathfrak{a}) = N(\mathfrak{p_1})^{f_1} N(\mathfrak{p_2})^{f_2} ... N(\mathfrak{p_n})^{f_n}.$$

As a direct consequence of proposition 10 and unique prime factorization at the ideal level we have the following result.

Corollary 1. *For $\mathfrak{a}, \mathfrak{b} \in \mathcal{O}$ we have:*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Proof. Since we are in a Dedekind domain we can factor our ideals, into prime ideals as:

$$\mathfrak{a} = \mathfrak{p}_1^{f_1}\mathfrak{p}_2^{f_2}...\mathfrak{p}_a^{f_a} \text{ and } \mathfrak{b} = \mathfrak{P}_1^{k_1}\mathfrak{P}_2^{k_2}...\mathfrak{P}_b^{k_b}.$$

We then further have:

$$\begin{aligned} N(\mathfrak{ab}) = \\ N(\prod_{i=1}^{a} \mathfrak{p}_i^{f_i} \prod_{i=1}^{b} \mathfrak{P}_i^{k_i}) = \\ \prod_{i=1}^{a} N(\mathfrak{p}_i)^{f_i} \prod_{i=1}^{b} N(\mathfrak{P}_i)^{k_i} = \\ N(\mathfrak{a})N(\mathfrak{b}), \end{aligned}$$

where the second equality follows by proposition 4. □

Definition 22. *If the prime ideal $p \in \mathbb{Z}$ splits as:*

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2{}^{e_2}...\mathfrak{p}_n{}^{e_n}$$

in $\mathcal{O}_K$ and we say that the prime ideals

$$\mathfrak{p}_1, ..., \mathfrak{p}_n$$

lie over (p). We denote this as:

$$(p)\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2{}^{e_2}...\mathfrak{p}_n{}^{e_n}.$$

Proposition 11. *The definition above of primes $\mathfrak{p}_i$ lying over (p) is equivalent to:*

$$\mathbb{Z} \cap \mathfrak{p}_i = (p) \quad \forall i \in \{1, 2, ..., n\}.$$

Proof. Assume that $p \in \mathbb{Z}$ splits as:

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2{}^{e_2}...\mathfrak{p}_n{}^{e_n}.$$

By definition we have :

$$p \subseteq \mathfrak{p}_i \quad \forall i \in \{1, 2, ..., n\}.$$

Now intersect both sides by $\mathbb{Z}$ and we get:

$$\mathbb{Z} \cap p = p \subseteq \mathbb{Z} \cap \mathfrak{p}_i \quad \forall i \in \{1, 2, ..., n\}.$$

For the other direction, take arbitrary $a, b \in \mathbb{Z}$, we then have that if:

$$ab \in \mathbb{Z} \cap \mathfrak{p}_i,$$

then

$$a \in \mathfrak{p}_i, \text{ or } b \in \mathfrak{p}_i$$

since $\mathfrak{p}_i$ is a prime ideal.

So if $ab \in \mathbb{Z} \cap \mathfrak{p}_i$, then:

$$a \in \mathbb{Z} \cap \mathfrak{p}_i, \text{ or } b \in \mathbb{Z} \cap \mathfrak{p}_i$$

and so $\mathbb{Z} \cap \mathfrak{p}_i$ is a prime ideal over $\mathbb{Z}$. It contains (p) so it is non-empty and so $\mathbb{Z} \cap \mathfrak{p}_i = (p)$.

The other direction follows directly because if:

$$\mathbb{Z} \cap \mathfrak{p}_i = p \quad \forall i \in \{1, 2, ..., n\}$$

then $p \subseteq \mathfrak{p}_i$ which by definition means $\mathfrak{p}_i | p$ and so $\mathfrak{p}_i \in (p)\mathcal{O}_K \ \forall i \in \{1, 2, ..., n\}$. □

Remark 3 ([1, . p. 45])**.** *These both definitions are equal in a more general setting. If $\mathfrak{P} \in \mathcal{O}_L$ and $\mathfrak{p} \in O_K$ and $\mathfrak{P}$ lies over $\mathfrak{p}$ then:*

$$\mathcal{O}_k \cap \mathfrak{P} = \mathfrak{p}.$$

Remember that in Dedekind domains, non zero prime ideals are maximal. As a consequence: $\mathcal{O}_k/\mathfrak{p}$ is a field. We will call this a residue field and show it below.

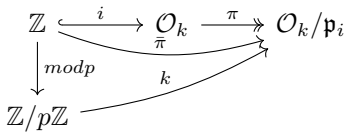
We also know that it has finite size from the discussion above and so it is actually a finite field. Its character is the prime p which $\mathfrak{p}$ lies over, no other character works since $p \subset \mathfrak{p}$. Then combining the discussion below proposition 4 which says that all finite fields with character p have p^n elements we get the following definition.

Proposition 12 ([5, p. 31])**.** *If $p \in \mathbb{Z}$ splits into prime ideals as:*

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2{}^{e_2}...\mathfrak{p}_n{}^{e_n}$$

in $\mathcal{O}_k$ we have that: $\mathcal{O}_k/\mathfrak{p}_i$ is a field extension of $\mathbb{Z}/p\mathbb{Z}$.

Proof. We get the following diagram.



Notice that $\ker(\overline{\pi}) = (p)$ because all $z \in \mathbb{Z}$ such that $z \in (\mathfrak{p}_i)$ is precisly $z \in (p)$ by proposition 11 which gives us that:

$$\mathbb{Z} \cap \mathfrak{p}_i = (p).$$

And so by the first isomorphism theorem theres an isomorphism:

$$\mathbb{Z}/\ker(\overline{\pi}) = \mathbb{Z}/p\mathbb{Z} \cong im(\overline{\pi}) \subseteq \mathcal{O}_k/\mathfrak{p}_i$$

and thus specifically an injection:

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}_i.$$

Since $\mathfrak{p}_i$ is a prime ideal, $\mathcal{O}_K/\mathfrak{p}_i$ is an integral domain and thus has no zero divisors. By proposition 9, to keep the notation consistent, $\alpha' = \mathcal{O}_k$ and $\alpha = \mathfrak{p}_i$ in our case. Since the determinant is non-zero and finite we get that $\mathcal{O}_K/\mathfrak{p}_i$ is finite. Assuming that $\exists x \in \mathcal{O}_K/\mathfrak{p}_i$ with no inverse, we would have an element with infinite order, contradicting finiteness, thus our integral domain is a field. □

Remark 4. *The same proof works for the general setting in remark 3 which also gives us that $\mathcal{O}_L/\mathfrak{P}$ is a finite field extension of $\mathcal{O}_K/\mathfrak{p}$.*

Definition 23. *If $p \in \mathbb{Z}$ splits as:*

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2{}^{e_2}...\mathfrak{p}_n{}^{e_n}$$

in $\mathcal{O}_k$ we have:

$$N(\mathfrak{p}) = p^f \quad p, f \in \mathbb{Z}$$

for some $f \geq 1$ by the discussion above and we call this f as the residue degree.

We have built enough material to actually give a proof of theorem 4.

Proof. Consider the tower of extensions, $\mathbb{Z} \subseteq \mathcal{O}_K \subseteq \overline{\mathcal{O}}_K$ and $\mathbb{Q} \subseteq K$, where :

$$\overline{\mathcal{O}}_K = \{\alpha \in K | \alpha \text{ integral over } \mathcal{O}_K\}.$$

1) We will first prove that $\mathcal{O}_K$ is integrally closed. I.e. if an element in $\alpha \in K$ is integral over $\mathbb{Z}$ it lies in $\mathcal{O}_K$. We will do this by proving:

$$\mathcal{O}_K = \overline{\mathcal{O}}_K.$$

The following inclusion is straightforward:

$$\mathcal{O}_K \subset \overline{\mathcal{O}}_K.$$

And what remains to show is that $\overline{\mathcal{O}}_K \subseteq \mathcal{O}_K$.

By definition $\mathcal{O}_K$ is integral over $\mathbb{Z}$ and $\overline{\mathcal{O}}_K$ integral over $\mathcal{O}_K$. Applying proposition 3 we get that $\overline{\mathcal{O}}_K$ is integral over $\mathbb{Z}$, hence by definition of $\mathcal{O}_K$ we get $\overline{\mathcal{O}}_K \subseteq \mathcal{O}_K$ which gives us the equality:

$$\overline{\mathcal{O}}_K = \mathcal{O}_K.$$

2) To prove that $\mathcal{O}_K$ is Noetherian we use 8 to conclude that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module, specificly finitely generated. From example 11 we get that any ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. So

$$\mathfrak{a} = \{\sum_{i=1}^{j} n_i x_i | n_i \in \mathbb{Z}, x_i \in \mathcal{O}_K\} = (x_1, ..., x_j)$$

which is an ideal in $\mathcal{O}_K$ since $\mathbb{Z} \subseteq \mathcal{O}_K$ and finitely generated by $\{x_1, ...x_j\}$ and thus $\mathcal{O}_K$ is Noetherian.

3) By proposition 12 know that quoiting $\mathcal{O}_K$ by a prime ideal yields us a field.

This proves that prime ideals are maximal.

Combining these three we get that $\mathcal{O}_K$ is a Dedekind domain. □

The proof of 1) above, proves that the property we were missing for $\mathbb{Z}[\sqrt{5}]$ is included in definition of ring of integers, namely the integral closure property.

Proposition 13 ([1, Ex. p. 15]). *For a quadratic extension $\mathbb{Q}(\sqrt{D})$, the corresponding ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, where D is square free takes the form below.*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \begin{cases} \mathbb{Z}[\sqrt{D}] \ \textbf{\textit{if}}\ D \equiv 2,3 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] \ \textbf{\textit{if}}\ D \equiv 1 \mod 4. \end{cases}$$

Proof. By proposition 8 we know that

$$Rank(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}) = [\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 2.$$

, where rank is how many bases our module has as a finitely generated free $\mathbb{Z}$-module. So all possible nontrivial integral elements in $\mathbb{Q}(i)$ come from a monic two degree polynomial in $\mathbb{Z}[x]$.

Consider $p(x) = x^2 + bx + c = 0 \in \mathbb{Z}[x]$ and $\gamma = \alpha + \beta\sqrt{D} \in \mathbb{Q}(\sqrt{D})$.

Considering:

$$\begin{aligned} p(\gamma) = \\ \gamma^2 + b\gamma + c = \\ (\alpha + \beta\sqrt{D})^2 + b(\alpha + \beta\sqrt{D}) + c = \\ \alpha^2 + \beta^2 D + b\alpha + c + \sqrt{D}(b + 2\alpha) = 0. \end{aligned}$$

The fact that $\{1, \sqrt{D}\}$ is a basis in $\mathbb{Q}(\sqrt{D})$ gives us the following equation system:

$$\begin{cases} \alpha^2 + \beta^2 D + b\alpha + c = 0 \\ (b + 2\alpha) = 0. \end{cases}$$

Solving the second equation we get the relation $b = -2\alpha$ and since $b \in \mathbb{Z}$ it follows that $2\alpha \in \mathbb{Z}$.

We will do two different cases, either $\alpha \in \mathbb{Z}$ or $\alpha = \frac{\alpha'}{2}$ for $\alpha' \in Z$ and $gcd(\alpha', 2) = 1$. *Case 1* In the first case we assume $\alpha \in \mathbb{Z}$ and then the first equation becomes:

$$\begin{aligned} \alpha^2 + \beta^2 D + -2\alpha^2 + c = \\ -\alpha^2 + D\beta^2 + c = 0 \iff \\ c = \alpha^2 - D\beta^2 \end{aligned}$$

Since $-c \in \mathbb{Z}$ it follows that $-\alpha^2 + D\beta^2 \in \mathbb{Z}$. So for all $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ independent of D, elements of the form $\alpha + \beta\sqrt{D}$ are integral.

Case 2 We assume that $\alpha = \frac{\alpha'}{2}$ and $gcd(\alpha', 2) = 1$. Now we look at equation one again and we get:

$$\begin{aligned} \alpha^2 + \beta^2 D + -2\alpha^2 + c = \\ -\alpha^2 + \beta^2 D + c = \\ -\frac{\alpha^2}{4} + D\beta^2 + c = 0. \end{aligned}$$

Multiplying both sides by 4 we get:

$$\begin{aligned} &(-\alpha')^2 + D(4\beta')^2 = -4c \qquad \iff \\ &(-\alpha')^2 + 4D(\beta')^2 \equiv 0 \mod 4. \end{aligned}$$

Also, $-(\alpha')^2, 4c \in \mathbb{Z}$ are integers which forces $4D(\beta')^2$ to be an integer.

If $\beta' \in \mathbb{Z}$ we get:

$$-(\alpha')^2 + 4D(\beta)^2 \equiv -(\alpha')^2 \equiv 0 \mod 4$$

which contradicts $gcd(\alpha', 2) = 1$. So since D is square free the only way for us to have a solution is if $\beta = \frac{\beta'}{2}$, with $gcd(\beta', 2) = 1$ and $\beta' \in \mathbb{Z}$.

This gives us the equation:

$$-(\alpha')^2 + 4D(\frac{(\beta')^2}{4}) \equiv -(\alpha')^2 + D(\beta')^2 \equiv 0 \mod 4$$

. The image of the map $a \mapsto a^2 \mod 4$ takes on the only values $\{0, 1\}$, so for $D = 2, 3$ our equation admits no solution.

For $D = 1$ it does take solutions, for $gcd(\beta', 2) = 1$ and $gcd(\alpha', 2) = 1$ the image of the map is always equal to one. So $\gamma = \frac{\alpha + \beta\sqrt{D}}{2}$ is an integral element when $D \equiv 1 \mod 4$ for all odd $\alpha, \beta \in \mathbb{Z}$.

This shows that for $D \equiv 2, 3$ the basis $\{1, \sqrt{D}\}$ but for $D \equiv 1 \mod 4$ we also need the basis to "span" elements of the form $\frac{a+b\sqrt{D}}{2}$. One can rewrite the integral elements as:

$$\gamma = \frac{a + b\sqrt{D}}{2} = \frac{a - b}{2} + b\left(\frac{1 + 1\sqrt{D}}{2}\right)$$

which works since $\frac{a-b}{2} \in \mathbb{Z}$ because a, b are assumed odd. □

Definition 24. *For an extension L/K, a prime ideal $\mathfrak{p} \in \mathcal{O}_K$, and the following factorization*

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} ... \mathfrak{P}_n^{e_n}$$

in $\mathcal{O}_L$ we denote the e_i as the ramification degree of $\mathfrak{P}_i \in \mathcal{O}_K$ over the prime $\mathfrak{p} \in \mathcal{O}_k$..

Theorem 8 ([1, prop. p. 46])**.** *Let $\mathfrak{p}$ be a prime over $\mathcal{O}_k$ and write $\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ the factorization of $\mathfrak{p}$ in $\mathcal{O}_k$. Let f_i be the inertia degree over $\mathfrak{P}_i$ over $\mathfrak{p}$, we have:*

$$\sum_{i=1}^{r} e_i f_i = [L : K].$$

We will show an example of this, and one can notice how the primes split tell us something about the field extension and vice versa.

By the fact that $-1 \equiv 3 \mod 4$, proposition 13 shows that $\mathbb{Z}[i]$ is the ring of integers for $\mathbb{Q}(i)$ as we claimed earlier.

Example 12. *We know from our earlier that* $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ *with ring of integers* $\mathbb{Z}[i]$. *We will look at how the prime ideal* (2) *splits over* $\mathcal{O}_{\mathbb{Q}(i)}$.

$$(1+i)^2 = ((1+i)^2) = (2i) = (-i)(2i) = (2).$$

The second last equality follows since $-i$ *is a unit in* $\mathbb{Z}[i]$. *Also* $(1+i)$ *is irreducible.*

So the prime ideal $(2) = (1+i)^2$ *ramifies with ramification degree* $e_1 = 2$.

Then the theorem above gives us:

$$2 \cdot [\mathbb{Z}[i]/(i+1) : \mathbb{F}_2] = 2 \implies [\mathbb{Z}[i]/(i+1) : \mathbb{F}_2] = 1.$$

and so Inertia degree $[\mathbb{Z}[i]/(i+1) : \mathbb{F}_2] = 1$.

One can also concretely see the isomorphism $\mathbb{Z}[i]/(i+1) \cong \mathbb{F}_2$ *via the mapping below.*

$$\varphi : \mathbb{Z}[i] \to F_2, \quad a + bi \mapsto a + b \mod 2.$$

Now an element $a + bi \in \ker(\varphi) \iff a \equiv b \mod 2$. *We have the prime ideal* $(1+i) \subset \ker(\varphi)$ *because:*

$$(1+i)(a+bi) = (a-b) + (a+b)i \equiv 2a \equiv 0 \mod 2.$$

Also $\ker(\varphi) \subset (i+1)$ *which we will prove below. We have two cases.* ***Case 1*** *If* $a = b$ *then if* $a + bi \in \ker(\varphi)$ *then this comes from* $a(1+i) \in (1+i)$.

Case 2 *WLOG assume that* $a > b$ *and assume that* $a + bi \in \ker(\varphi)$ *and so* $a+b \equiv 0 \mod 2$. *In other words the parity of* a, b *is the same. Then we consider the explicit construction:*

$$\left(\frac{a+b}{2}\right)\left(\frac{(b-a)i}{2}\right)(1+i) = a + bi.$$

Note that since a, b *share parity by assumption,* $\left(\frac{a+b}{2}\right)$ *is an integer. This shows* $\ker(\varphi) \subset (1+i)$ *and so we have proven* $\ker(\varphi) = (1+i)$ *and using the first isomorphism theorem we get:*

$$\mathbb{F}_2 \cong \mathbb{Z}[i]/(1+i).$$

So using our formula above, we see that having done this direction first, we would have gotten:

$$\sum_{i=1}^{r} e_i f_i =$$
$$e_1 \cdot [\mathbb{Z}[i]/(i+1) : \mathbb{F}_2] =$$
$$e_1 \cdot 1 = 2 \implies$$
$$e_1 = 2$$

which tells us that the prime ideal (2) *over* $\mathbb{Z}$ *ramifies in the form* $\mathfrak{p}^2$ *for some prime ideal in* $\mathbb{Z}[i]$.

5 A bit of background for Galois Theory and Examples

We will focus on field extensions that are called Galois extensions, but first we will define normal extensions and and relate them to splitting fields.

Definition 25. *Splitting field A splitting field* K' *is a field extension of* K *for a irreducible polynomial* $f \in K[x]$ *such that* $f(x)$ *splits into a linear product of roots, i.e.* $f(x) = a(x-\alpha_1)...(x-\alpha_n)$ *where* $\alpha_i \in K'$ *are roots of* f*, and* a *is the leading coefficient of* f *in* K *and there is no strict subfield* L *of* K' *where* f *splits completely.*

Definition 26 (Normal extension)**.** *A algebraic field extension* L/K *is called a normal extension if* L *is the splitting field for some irreducible polynomials in* $K[x]$.

This definition does not give us a great calculation tool, but over separable extensions we can get a good criterion for checking normality.

We will introduce a theorem that's needed first, namely,

Theorem 9 ([2, Ch 13])**.** *If* L/K *is finite and separable, then* $L = K(\alpha)$ *for some* $\alpha \in L$.

Theorem 10 ([2, prop 650-651])**.** *Let* L/K *be a finite and separable extension of fields. Let* α *be the element with the property:*

$$L \cong K(\alpha)$$

which we know exists via theorem 9 , let $m_\alpha(x)$ *be its minimal polynomial in* $K[x]$*. Then:*

$$\begin{aligned} &L \text{ is a normal extension} \iff \\ &\text{whenever } m_\alpha(x) \text{ is irreducible in } K[x], \text{ and has a root in } L, \\ &\text{it splits completly roots in } L. \end{aligned}$$

By the above proposition, we get a useful criterion for us.

Corollary 2. *If L/K is an algebraic field extension (finite, sep) we get:*

$$L = K(\alpha) \text{ is a normal } \iff m_\alpha(x) \text{ splits completely in } L.$$

Proof. We start with $L = K(\alpha)$, by theorem 9. Now if $m_\alpha(x)$ splits in L then by definition, L is the splitting field for some polynomial which is irreducible over K, thus by definition a normal extension.

The other direction follows because we know that m_α by definition has α as solution and is irreducible over K.

Then using that its normal, the corollary 2 above gives us that m_α splits in L. □

For Separable and finite extensions , which as we said earlier is what we will work with, unless stated otherwise we have a rather nice criterion.

To check if an extension L/K is normal, we have to check whether the minimal polynomial $m_\alpha(x)$ of the primitive element α splits or not.

We will do a few examples below.

Example 13. *An example of a normal extension is $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. The minimal polynomial for $\sqrt{(2)}$ over $\mathbb{Q}$ is $m_{\sqrt{2}}(x) = x^2 - 2$. This splits completely in $\mathbb{Q}(\sqrt{2})$ as:*

$$m_{\sqrt{2}}(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

So we had a irreducible polynomial in $\mathbb{Q}$ which split in $\mathbb{Q}(\sqrt{2})$ which shows its a splitting field, by the definition of normal extension.

One sees here that checking for the minimal polynomial is enough, since its the unique polynomial that is irreducible over the base field, monic and has the element α as a solution.

Example 14. *If we instead consider $x^3 - 2$, and consider the extension*

$$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$$

we will get that:

$$m_{\sqrt[3]{2}}(x) = (x - \sqrt[3]{2})(x^2 + x + 1).$$

So this is not the splitting field of the minimal polynomial and thus or a normal extension by corollary 2.

Looking at the polynomial part that did not split, $p(x) = (x^2 + x + 1)$ we know that this has the primitive 3rd roots of unity as solutions, and so we adjoin ζ_3 to $\mathbb{Q}(\sqrt[3]{2})$ and we get:

$$m_{\sqrt[3]{2}}(x) = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta_3)(x - \sqrt[3]{2}\zeta_3^2)$$

in the extension $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Since it is the splitting field to an minimal polynomial the extension is normal.

This shows that one cannot heedlessly add the "natural" algebraic element to get a normal extension.

Definition 27 ([3, p. 277])**.** *For a field extension L/K, we define $Aut(L/K)$ as the set of field automorphisms $\sigma : L \to L$ which are K-linear.*

Remark 5. $\sigma \in Aut(L/K) \iff \sigma_{|K}(k) = k \quad \forall k \in K.$

Definition 28. *A extension L/K is called a **Galois Extension** if L/K is a normal extension and a separable extension.*

Theorem 11 ([2, p. 574])**.** *The definition 28 is equivalent to $[AUT(L/K)] = [L : K]$*

Theorem 12 ([2, Thm. p. 574])**.** *Let L/K be a Galois extension and let $G = Gal(L/K)$. Then there is a bijection:*

$$\left\{ \begin{array}{c} L \\ | \\ \textit{subfields } E \\ \textit{of } L \\ | \\ \textit{containing } K \\ | \\ K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array} \quad \begin{array}{c} \\ \\ \textit{subgroups } H \\ \textit{of } G \\ \\ \\ \\ \end{array} \right\}$$

Where we have:

$$E \to Gal(L/E)$$

and

$$H \to L^H$$

where they are inverses, so $H \to L^H \to Gal(L/L^H) = H$.

We will introduce a theorem that connects a certain type of Galois Extensions and the discussion about finite fields we had earlier.

Theorem 13 ([2, Thm. p. 596])**.** *The Galois group of the cyclotomic field $\mathbf{Q}(\zeta_\mathbf{n})$ of the nth root of unity is isomorphic to $(\mathbf{Z}/\mathbf{nZ})^*$. The isomorphism is explicitly given by:*

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^* &\to Gal(\mathbb{Q}(\zeta_\mathbf{n})/\mathbb{Q}) \\ a \mod n &\to \sigma_a \end{aligned}$$

Where $\sigma_a(\zeta_n) = \zeta_n^a$

Definition 29. *For Galois Extensions L/K we define our norm on elements as:*

$$N_{\mathbf{L/K}}(x) = \prod_{\sigma \in Aut(L/K)} \sigma(x).$$

Proposition 14 ([1, prop. p. 9])**.** *Let a separable extension L/K, and let the field L' be the splitting field for the minimal polynomial $m_\alpha(x)$ over K. Then minimal polynomial $m_\alpha(x)$ can be written using $Aut(L'/K)$ as:*

$$m_\alpha(x) = \prod_{\sigma \in Aut(L'/K)} (x - \sigma(x))$$

We will now justify a few properties about this norm, where we used it for example but did not define it properly or prove its properties.

Proposition 15. *For any extension L/K , and for any $\sigma \in Aut(L/K)$ we have:*

$$\sigma(\mathcal{O}_L) = \mathcal{O}_L.$$

Proof. To see this we will start by an element $l \in \mathcal{O}_L$, so by definition we have that $p(l) = l^n + k_{n-1}l^{n-1} + ... + k_1 l + a_0 = 0$ for some $k_i \in K$.

Then considering $\sigma(p(l))$ we have:

$$\sigma(l) = \sigma(l^n + k_{n-1}l^{n-1} + ... + k_1 l + k_0) =$$
$$\sigma(l^n) + \sigma(k_{n-1})\sigma(l^{n-1}) + ... + \sigma(k_1)\sigma(l) + \sigma(k_0).$$

Then σ fixes our base field so $\sigma(k_i) = k_i$, and so we have:

$$\sigma(l^n) + k_{n-1}\sigma(l^{n-1}) + ... + k_1\sigma(l) + (k_0).$$

Then we can write $\sigma(l^n) = \sigma(l \cdot l \cdot ... \cdot l) = \sigma(l)^n$, so we finally get:

$$\sigma(l)^n + k_{n-1}\sigma(l)^{n+1} + ... + k_1\sigma(l) + k_0 = p(\sigma(l)).$$

So we have $p(\sigma(l)) = \sigma(p(l)) = \sigma(0) = 0$ which shows that $\sigma(l) \in \mathcal{O}_L$ and so $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. □

Proposition 16 ([1, . p. 12])**.** *For a field extension L/K ,and $\forall \alpha \in \mathcal{O}_L$ we get $N(\alpha) \in \mathcal{O}_K$.*

Proof. By proposition 15 $\sigma(\alpha) \in \mathcal{O}_L$, $\forall \alpha \in \mathcal{O}_L$ and $\forall \sigma \in Aut(L/K)$. thus:

$$N_{\mathbf{L/K}}(x) = \left(\prod_{\sigma \in Aut(L/K)} \sigma(x) \right) \in \mathcal{O}_L.$$

Every finite group acting on itself via $h : g \mapsto gh$ maps has trivial kernel and is thus a bijection. Thus

$$\sigma_j(N_{\mathbf{L/K}}(\alpha)) = \prod_{\sigma \in Aut(L/K)} \sigma_j\sigma(\alpha) = \prod_{\sigma \in Aut(L/K)} \sigma(\alpha), \forall \sigma_j \in Aut(L/K).$$

But this proves that $N_{L/K} \in K$ by definition of $Aut(L/K)$. Thus, $N_{L/K}(\alpha) \in (K \cap \mathcal{O}_L = \mathcal{O}_K)$.. □

We also have the criterion ,

Proposition 17 ([1, . p. 12])**.** *For $L/\mathbb{Q}$, α is a unit in $\mathcal{O}_L \iff N(\alpha) = \pm 1$.*

Proof. First we prove that if α is a unit in $\mathcal{O}_L$, then $N(\alpha) = \pm 1$. Under our assumption $\exists u \in \mathcal{O}_L$ s.t that:

$$\alpha u = 1 \iff N(\alpha)N(u) = N(1) = 1.$$

and multiplicity follows by proposition 4. Then by proposition 16, $N(\alpha) \in \{1, -1\}$.

For the other direction, assume that $N(\alpha) = 1$ and so:

$$N(\alpha) = \sigma_{id}(\alpha) \prod_{\substack{\sigma \in Aut(L/K) \\ \sigma \neq \sigma_{id}}} \sigma(\alpha) = 1.$$

Define $\alpha^{-1} := \prod_{\substack{\sigma \in Aut(L/K) \\ \sigma \neq \sigma_{id}}} \sigma(\alpha)$, and by proposition 15 and the fact that $\mathcal{O}_L$ is a ring, our element α^{-1} is in $\mathcal{O}_L$. and then $\alpha\alpha^{-1} = 1$ which proves that α is a unit in $\mathcal{O}_L$. □

Theorem 14 ([1, p. 35])**.** *For principal ideals $\mathfrak{a} = (\alpha) \in \mathcal{O}_K$ we have*

$$|N_{K/\mathbb{Q}}(\alpha)| = N(\mathfrak{a}) = |\mathcal{O}_k/\mathfrak{a}|.$$

When we have a cyclic extension and n is prime we just get that the norm is $\prod_{k=1}^{p-1}(a + b\sigma^k)$.

We will do an example for a Galois Extension that is cyclotomic.

We will introduce the ring of integers for our cyclotomic extensions $\mathbb{Q}(\zeta_n)$.

Theorem 15 ([1, prop. p. 60])**.** *For a cyclotomic field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, for some primitive nth root of unity ζ_n, we have the following basis for $\mathcal{O}_{Q(\zeta_n)}$:*

$$\{1, \zeta_n^1, \zeta_n^2, ..., \zeta_n^{d-1}\}$$

where $d = \varphi(n)$ and φ is the Euler tuition function.

And so in particular $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

Example 15. *Consider the field extension $\mathbb{Q}(\zeta_3)/\mathbb{Q}$. This is cyclic of order 2 according to our discussion and its generated by $\sigma : \zeta_3 \to \zeta_3^2$. Taking the norm according to an arbitrary element $a + b\zeta_3 \in \mathbb{Z}(\zeta_3)$ we get:*

$$\begin{aligned} N_{\mathbb{Z}(\zeta_3)}(a + b\zeta_3) = \\ \sigma(a + b\zeta_3)\sigma^2(a + b\zeta_3) = \\ (a + b\zeta_3^2)(a + b\zeta_3^4) = \\ a^2 + b^2 + ab(\zeta_3 + \zeta_n^2) = \\ a^2 + b^2 - ab. \end{aligned}$$

The last equality follows from the fact that $\zeta_3 + \zeta_3^2 = -1$ $(a + b\zeta_n^2) = a^2 + b^2 + ab(\zeta_3 + \zeta_n^2)$.

Notice that for $a = 2, b = 3$ *we have*

$$a^2 + b^2 - ab = 7.$$

This means that 7 *splits as* $(2 + 3\zeta_3)(2 + 3\zeta_3^2)$ *and so it is not prime.*

To show that $(7) = (2 + 3\zeta_3)(2 + 3\zeta_3^2)$ *as prime ideals we need to show that the ideals on the right are prime.*

$$N_{\mathbb{Q}(\zeta_3)}(2 + 3\zeta_3) = 2^2 + 3^3 - 3 \cdot 2 = 7$$

,

$$\begin{aligned} N_{\mathbb{Q}(\zeta_3)}(2 + 3\zeta_3^2) = N_{\mathbb{Q}(\zeta_3)}(2 + 3(-1 - \zeta_3)) = \\ N_{\mathbb{Q}(\zeta_3)}(-1 - 3\zeta_3) = \\ (-1)^2 + (-3)^2 - (-1) \cdot (-3) = \\ 7. \end{aligned}$$

So since they have norm 7, if the ideals are prime, the quotient must be isomorphic to F_7.

Consider the following maps:

$$\varphi : \mathbb{Z}[\zeta_3] \to F_7, \quad \zeta_3 \mapsto 4.$$

and

$$\psi : \mathbb{Z}[\zeta_3] \to F_7, \quad \zeta_3 \mapsto 2.$$

To be a well-defined field homomorphism, 1 *must be mapped to* 1 *and* ζ_3 *has order 3 and must thus be mapped to an element in* F_7 *of order* 3.

One sees that $\ker \varphi = (2 + 3\zeta_3)$ *and* $\ker \psi = (2 + 3\zeta_3^2)$.

By the first isomorphism theorem we have the following isomorphisms:

$$\mathbb{Z}[\zeta_3]/(2 + \zeta_3) \cong F_7, \quad \mathbb{Z}[\zeta_3]/(2 + 3\zeta_3).$$

These ideals are not equal either, for example :

$$\psi_1((2 + 3\zeta_3)) = 8 \not\equiv 0 \mod 7.$$

Also notice how

$$\sigma(a + b\zeta_3) = a + b\zeta_3^2, \quad \sigma(a + b\zeta_3^2) = a + b\zeta_3$$

,so $\sigma^2 = \sigma_{id}$ *and so its cyclic as we proposed. Notice that* σ *acts transitivity on each prime ideal* $(2 + 3\zeta_3)$ *and* $(2 + 3\zeta_3^2)$.

6 Galois on primes

We will start by proving and discussing properties which our prime ideals and ring of integers posses under the symmetries of elements from the Galois group.

In the example we saw how $\sigma \in Gal(\mathbb{Q}[\zeta_3]/\mathbb{Q})$ acted transitively on the prime ideals $(2+3\zeta_3), (2+3\zeta_3^2) \in \mathbb{Z}[\zeta_3]$. One might ask how a general element $\sigma \in G(L/K)$ acts on the ring of integers $\mathcal{O}_L$ for a Galois extension.

Proposition 18 ([1, Prop. p.54])**.** *For any Galois extension L/K , and for any $\sigma \in G(L/K)$ we have:*

$$\sigma(\mathcal{O}_L) = \mathcal{O}_L.$$

Proof. See proposition 15 and theorem 11. □

Proposition 19 ([1, . p. 45])**.** *For $\sigma \in G(L/K)$and $\mathfrak{P} \in \mathcal{O}_L$ over $\mathfrak{p} \in \mathcal{O}_K$ we have that $\sigma\mathfrak{P} \in \mathcal{O}_L$ is also a prime ideal over $\mathfrak{p}$.*

Proof. By definition $\sigma(\mathcal{O}_K) = \mathcal{O}_K$. The second equality comes from the fact that σ is a automorphism of L and thus injective.

$$\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \sigma(\mathfrak{P}) \cap \sigma(\mathcal{O}_K) = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma(\mathfrak{p}) = \mathfrak{p}.$$

By definition this means that the rime ideal $\sigma(\mathfrak{P})$ lies over $\mathfrak{p}$. □

Definition 30. *We call $\sigma\mathfrak{P}$ elements prime ideal conjugates to $\mathfrak{P}$.*

Lemma 1. *If $\mathfrak{P}$ and $\mathfrak{P}'$ are two different prime ideals then $\mathfrak{P} + \mathfrak{P}' = \mathcal{O}_L$.*

Proof. Assume for the sake of contradiction that $\mathfrak{P} + \mathfrak{P}' \subset O_L$ is a strict inclusion. We have the following:

$$\mathfrak{P} \subseteq \mathfrak{P} + \mathfrak{P}', \quad \mathfrak{P}' \subseteq \mathfrak{P} + \mathfrak{P}'.$$

Our prime ideals $\mathfrak{P}, \mathfrak{P}'$ are maximal ideals. Thus the following inclusion:

$$\mathfrak{P} \subseteq \mathfrak{P} + \mathfrak{P}'$$

forces $\mathfrak{P} + \mathfrak{P}' = \mathfrak{P}$ since we assumed a strict inclusion $\mathfrak{P} + \mathfrak{P}' \subset \mathcal{O}_L$. And by the inclusion:

$$\mathfrak{P} \subseteq \mathfrak{P} + \mathfrak{P}'$$

we get that $\mathfrak{P}' = \mathfrak{P} + \mathfrak{P}'$.

So combining these two equalities we have that:

$$\mathfrak{P} = \mathfrak{P} + \mathfrak{P}' = \mathfrak{P}'$$

which contradicted our assumption of them not being equal. □

Theorem 16 ([1, Thm. p. 21]). *Let $\mathfrak{a}_1, ..., \mathfrak{a}_n$ be ideals in a Dedekind domain $\mathcal{O}$ such that $\mathfrak{a}_i + \mathfrak{a}_j = \mathcal{O}$ for all $i \neq j$. Then if $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i$ one has*

$$\mathcal{O}/\mathfrak{a} = \bigoplus_{i=1}^{n} \mathcal{O}/\mathfrak{a}_i$$

Theorem 17 ([1, prop. p. 54]). *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_k$ and denote by $X = \{\mathfrak{P}_1, ..., \mathfrak{P}_k\}$ the set of primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Then $G = Gal(L/K)$ acts transitively on the set X. I.e they are all prime ideal conjugates to each other.*

Proof. For the sake of contradiction, let us assume that $\mathfrak{P}, \mathfrak{P}'$ are two different prime ideals and assume that they are not in the same orbit, i.e $\sigma(\mathfrak{P}) \neq \mathfrak{P}' \quad \forall \sigma \in G$. Because of lemma 1 $\mathfrak{P} + \mathfrak{P}' = \mathcal{O}_L$ we can use the Chinese Remainder Theorem 16 then $\exists x \in \mathcal{O}_L$ such that:

$$\begin{cases} x \equiv 0 \mod \mathfrak{P}' \\ x \equiv 1 \mod \sigma_1(\mathfrak{P}) \\ ... \\ ... \\ x \equiv 1 \mod \sigma_i(\mathfrak{P}) \end{cases} \tag{1}$$

In words then we have $x \in \mathfrak{P}'$ and $x \notin \sigma_i(\mathfrak{P}), \forall \sigma_i \in G$.

We will now look at the norm $N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x)$. By proposition 16 $N_{L/K}(x) \in \mathcal{O}_K$. Now one of the elements in the product is $\sigma_{id}(x) = x$, and $x \in \mathfrak{P}'$. The rest of the elements are in $\mathcal{O}_L$ by proposition 19, and so:

$$N_{L/K}(x) = x \prod_{\substack{\sigma \in G \\ \sigma \neq \sigma_{id}}} \sigma(x) \in \mathfrak{P}'$$

since ideals are closed under multiplication by element of the ring.

So

$$N_{L/K}(x) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}.$$

But $x \notin \sigma_i(\mathfrak{P})$ for all $\sigma \in G$ means that $\sigma(x) \notin \mathfrak{P}$ for all σ. This implies that:

$$N_{L/K}(x) \notin \sigma\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}, \forall \sigma \in G$$

which is a contradiction because we got that $N_{L/K}(x) \in \mathfrak{p}$ and $N_{L/K}(x) \notin \mathfrak{p}$ cannot both be true. Thus, we have proved the proposition. □

Definition 31. *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_k$ and denote by $X = \{\mathfrak{P}_1, ..., \mathfrak{P}_k\}$ the set of primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$ and $G = Gal(L/K)$.*

$$G_{\mathfrak{P}_i} = \{\sigma \in G | \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}$$

*is called the **Decomposition Group** of $\mathfrak{P}_i$ over $\mathcal{P}$.*

Remark 6. *The group $G_{\mathfrak{P}_i}$ is actually a subgroup of G because it is a subset of G, the composition of two elements $\sigma, \sigma' \in G_{\mathfrak{P}_i}$ is in $G_{\mathfrak{P}_i}$ because both fix $\mathfrak{P}_i$. Associativity is inherited, the identity $\sigma_{id} \in G$ is the identity on $G_{\mathfrak{P}_i}$, and assuming some element $\sigma \in G_{\mathfrak{P}_i}$ doesn't have an inverse would give us an element with infinite order contradicting the finiteness of $G_{\mathfrak{P}_i}$.*

We have the definition of **Decomposition Field** as:

$$Z_{\mathfrak{P}_i} = \{x \in L | \forall \sigma \in G_{\mathfrak{P}_i}, \sigma(x) = x\}.$$

Definition 32. *Let $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$ be a prime ideal of $Z_{\mathfrak{P}}$ below $\mathfrak{P}$.*

Proposition 20 ([1, prop. p. 55])**.** *For $\mathfrak{P}_Z$, which we defined in definition 32,*

(i) $\mathfrak{P}_Z$ is non split in L, i.e., $\mathfrak{P}$ is the only prime ideal of L above $\mathfrak{P}_Z$.

(ii) $\mathfrak{P}$ over $Z_{\mathfrak{P}}$ has ramification index e and inertia degree f.

(iii) The ramification index and the inertia degree of $\mathfrak{P}_Z$ over K both equal 1.

We will denote $\mathcal{O}_L/\mathfrak{P}$ as $\kappa(\mathfrak{P})$ and $\mathcal{O}_L/P$ as $\kappa(P)$.

Lemma 2. *If we have a field extension L/K, and $m_\theta(x)$ is an minimal polynomial over K for an element in $\theta \in \mathcal{O}_L$, then its coefficients lie in $\mathcal{O}_K$.*

Proof. Assume that $\theta \in \mathcal{O}_L$, then by definition we have $m_\theta(x) \in K[x]$. Let L' be the splitting field for $m_\theta(x)$ ove K. Then by proposition 14 we have

$$m_\theta(x) = \prod_{\sigma \in Aut(L'/K)}^{n} (x - \sigma(\theta)) \in \mathcal{O}'_L[x].$$

By proposition 15 we get that all coefficients are sums and products of elements in $\mathcal{O}'_L$ which is a ring, and so the coefficients are in $K \cap \mathcal{O}'_L = \mathcal{O}_K$. □

Theorem 18 ([5, Rm. p. 32])**.** *Let L/K be a Galois extension and $\mathfrak{p}$ be a prime over $\mathcal{O}_k$ and write $\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ the factorization of $\mathfrak{p}$ in $\mathcal{O}_k$. Let f_i be the inertia degree over $\mathfrak{P}_i$ over $\mathfrak{p}$.*

1. *we get that $f_i = fj$ and $e_i = e_j$ for all i, j*
2. $$\sum_{i=1}^{g} e_i f_i = efr = [L : K]$$

where r is the amount of of primes our prime $\mathfrak{p}$ splits into in $\mathcal{O}_L$.

Theorem 19 ([1, Th. p. 56])**.** *L/K is a Galois extension, we also have a surjective mapping:*

$$\begin{aligned}\varphi : G_{\mathfrak{P}} &\to G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \\ \sigma &\mapsto \bar{\sigma}.\end{aligned}$$

where $\bar{x} := x \mod \mathfrak{P}$ and $\bar{\sigma}(\bar{x}) := \sigma(x) \mod \mathfrak{P}, \forall x \in \mathcal{O}_L$.

Proof. Via theorem 12 , we have that for any subgroup H of $Gal(L/K)$, t:

$$Gal(L/L^H) = H.$$

In our case, we get:

$$Gal(L/L^{G_{\mathfrak{P}}}) = Gal(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}.$$

Since $\kappa(\mathfrak{p}) \cong \kappa(\mathfrak{P}_Z)$ via proposition 20 we can instead look at the map:

$$\begin{aligned}\varphi : G(L/Z_{\mathfrak{P}}) &\to G(\kappa(\mathfrak{P}))/\kappa(\mathfrak{P}_Z)) \\ \sigma &\mapsto \bar{\sigma}.\end{aligned}$$

To show well defined-ness of $\bar{\sigma}$ on the residue field $\kappa(\mathfrak{P})$, take two elements $x, y \in \mathcal{O}_L$ such that $x \equiv y \mod \mathfrak{P}$. i.e $x - y \in \mathfrak{P}$. Then applying σ we get:

$$\sigma(x - y) = \sigma(x) - \sigma(y) \in \mathfrak{P}$$

Since $\sigma(\mathfrak{P}) = \mathfrak{P}$. So we proved that our function is well-defined, i.e. $\bar{x} = \bar{y} \implies \bar{\sigma}(x) = \bar{\sigma}(y)$.

We will start by showing that the extension $\kappa(\mathfrak{P}))/\kappa(\mathfrak{P}_Z)$ is Galois.

All our extensions we work with are separable and so it remains to prove that $\kappa(\mathfrak{P}))/\kappa(\mathfrak{P}_Z)$ is normal and that our map is surjective.

Let $\theta \in \mathcal{O}_L$ be a representative of an element $\bar{\theta} \in \kappa(\mathfrak{P})$, we denote the $m_{\theta(x)}$ as the minimal polynomials of θ over $\mathcal{O}_{Z_{\mathfrak{P}}}$, justified by lemma 2 and $m_{\bar{\theta}}(x)$ for $\bar{\theta}$ over $\kappa(\mathfrak{P}_Z)$.

Denote $\bar{m_\theta}(\bar{x}) := m_\theta(x) \mod \mathfrak{P}_Z$ which has coefficients in $\kappa(\mathfrak{P}_Z)$, and by definition $m_\theta(\theta) = 0$ which gives us

$$\bar{m_\theta}(\bar{\theta}) = \bar{0}.$$

By (DF) we have that $m_{\bar{\theta}}(\bar{x}) | \bar{m_\theta}(\bar{x})$.

Since our field extension L/K is normal, $m_\theta(x)$ splits completely over L as:

$$m_\theta(x) = \prod (x - \theta_i),$$

so we have

$$\bar{m_\theta}(\bar{x}) = \prod (\bar{x} - \bar{\theta_i})$$

with $\theta_i \in \mathcal{O}_L$.

Since $m_{\bar{\theta}}(\bar{x})|\bar{m}_\theta(\bar{x})$ this means that $m_{\bar{\theta}}(x)$ also splits over $\kappa(\mathfrak{P})$, so our extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_Z)$ is normal and thus also a Galois extension.

Now considering $\bar{\theta}$ as the primitive element, which we know we can pick by theorem 9 for the extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_Z)$,and pick an arbitrary

$$\bar{\sigma} \in Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_Z)).$$

By proposition 15, $\bar{\sigma}\bar{\theta}$ is a root to $m_{\bar{\theta}(x)}$.

From earlier we had that $m_{\bar{\theta}}(\bar{x})|\bar{m}_\theta(\bar{x})$ and so this means that $\bar{\sigma}(\bar{\theta}) = \bar{\theta}'$ for some root θ' of $m_\theta(x)$, where By definition $\bar{\theta}' = \theta' \mod \mathfrak{P}$, and by proposition 15 we know $\exists\sigma \in G(L/Z_{\mathfrak{P}})$ such that $\sigma\theta = \theta'$, which gives us:

$$\sigma(\theta) \equiv \bar{\sigma}(\bar{\theta}) \mod \mathfrak{P}$$

which shows that $\forall\bar{\sigma} \in G(\kappa(\mathfrak{P}))/\kappa(\mathfrak{P}_Z))$, $\exists\sigma \in G(L/Z_{\mathfrak{P}})$, proving surjectivity. □

Corollary 3. *The above mapping φ admits the following kernel:*

$$I_{\mathfrak{P}} = \{\sigma \in Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))|\sigma(x) \equiv x \mod \mathfrak{P}, \forall x \in \mathcal{O}_L\}.$$

and we have the following isomorphism:

$$G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong Gal(\kappa(\mathfrak{P})/\kappa(p)).$$

Proof. We will show that it is the kernel. Take an arbitrary element $\sigma \in \ker(\varphi)$. We have that $\sigma_{id} = \sigma(x) \equiv x \mod \mathfrak{P}, \forall x \in \mathcal{O}_L$ and so:

$$\ker(\varphi) \subseteq I_{\mathfrak{P}}.$$

Now take an element $\sigma \in I_{\mathfrak{P}}$. So $\sigma(x) \equiv x \mod \mathfrak{P}, \forall x \in \mathcal{O}_L$ and so $I_{\mathfrak{P}} \subseteq \ker(\varphi)$ which gives:

$$I_{\mathfrak{P}} = \ker(\varphi).$$

The kernel is a normal subgroup and so by the first isomorphism theorem we get our desired isomorphism:

$$G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong Gal(\kappa(\mathfrak{P})/\kappa(p))).$$

□

Definition 33. *The group $I_{\mathfrak{P}} = \{\sigma \in Gal(\kappa(\mathfrak{P})/\kappa(p))|\sigma(x) \equiv x \mod \mathfrak{P}, \forall x \in \mathcal{O}_L\}$ is called the inertia group.*

Proposition 21 ([5, thm. p. 32])**.** *The group $I_{\mathfrak{P}}$ is trivial $\iff$ $\mathfrak{P}$ is unramified over $\mathfrak{p}$.*

Proof. We will first prove that if $\mathfrak{P}$ unramified, $I_{\mathfrak{P}}$ is trivial. By proposition 20 i) we have that our prime $\mathfrak{P}$ is non-split over $\mathfrak{P}_Z$ which means that all splitting that occurs happens in the extension $Z_{\mathfrak{P}}/K$, and by ii), the inertia and ramification degree over L/K is the same as the one from $L/Z_{\mathfrak{P}}$. By theorem 18 and theorem 12 we have the following:

$$|Gal(L/Z_{\mathfrak{P}})| = |G_{\mathfrak{P}}| = ef.$$

since we have assumed that $\mathfrak{P}$ is unramified we get $e = 1$.

And so $f = |G_{\mathfrak{P}}|$. By corollary 3 we have

$$f = \frac{|G_{\mathfrak{P}}|}{|I_{\mathfrak{P}}|},$$

putting these together we have $f = \frac{f}{|I_{\mathfrak{P}}|} \iff |I_{\mathfrak{P}}| = 1$. We have proved that $I_{\mathfrak{P}}$ is trivial when $\mathfrak{P}$ is unramified.

For the other direction, assume that $I_{\mathfrak{P}}$ is trivial, we have

$$|G_{\mathfrak{P}}| = fe$$

, and

$$f = \frac{|G_{\mathfrak{P}}|}{|I_{\mathfrak{P}}|}.$$

Since we assumed $|I_{\mathfrak{P}}|$ being trivial , we get: $f = |G_{\mathfrak{P}}| = fe$, thus $fe = f \implies e = 1$. Thus, whenever $I_{\mathfrak{P}}$ is trivial, $\mathfrak{P}$ is unramified. □

7 Frobenius Element

We will keep looking at Galois Extensions L/K with Galois group G. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ that is unramified in $\mathcal{O}_L$ and let $\mathfrak{P}$ be a prime of L lying over it. Let f be the inertia degree of $\mathfrak{P}$. The group $G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is cyclic of order f and generated by the Frobenius automorphism we discussed earlier, but now to the prime norm, instead to a prime to the ideal norm, so $x \to x^{N(p)}$.

Definition 34. *In our setup above, if $\mathfrak{P}$ us unramified over $\mathfrak{p}$, the Frobenius Element, is the unique element $Frob_{\mathfrak{P}_i} \in G_{\mathfrak{P}_i}$ which maps to $Frob \in G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ by our map in φ from theorem 19. Explicitly:*

$$Frob_{\mathfrak{P}_i}(a) \equiv a^{|N(\mathfrak{p})|} \mod \mathfrak{P}_i, \quad \forall a \in \mathcal{O}_L.$$

Remark 7. *Proof of uniqueness down below.*

Proof. Such an element $Frob$ exists in $G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ by [[2, Ch 14.3]] discussion. And by proposition 21 we get:

$$G_{\mathfrak{P}} \cong G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$$

and since this is an isomorphism the map $\varphi_{\mathfrak{P}}$ corresponds to a unique element $Frob_{\mathfrak{P}}$ in $G_{\mathfrak{P}}$. □

This is a way to lift the Frobenius Automorphism globally , it is apriori defined only locally on the residue fields.

Definition 35. *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$, and let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ lying over it. Suppose that $\mathfrak{P}$ is unramified over $\mathfrak{p}$. Then we call :*

$$\left(\frac{L/K}{\mathfrak{P}}\right)$$

*the **Frobenius Symbol** which denotes the element $Frob_{\mathfrak{P}} \in G_{\mathfrak{P}}/I_{\mathfrak{P}}$..*

Remark 8. *When $\mathfrak{P}$ is ramified over $\mathfrak{p}$ we have several choices for the Frobenius element, $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ now has cosets. Now the Frobenius element $Frob_{\mathfrak{P}}$ is a unique coset which has a unique image,instead of one unique element in $G_{\mathfrak{P}}$.*

Because choosing a Frobenius element $Frob_{\mathfrak{P}}$ from a coset, and $\sigma \in I_{\mathfrak{P}}, \sigma \neq \sigma_{id}$. Then $\sigma(Frob_{\mathfrak{P}}) = Frob_{\mathfrak{P}}$ but the equality does not hold in $G_{\mathfrak{P}}$, and thus we don't have a pullback to $G_{\mathfrak{P}} \subseteq Gal(L/K)$.

Proposition 22 ([5, Rm. p. 34])**.** *Assume that $\mathfrak{P}'$ is another prime of $\mathcal{O}_L$ lying over $\mathfrak{p}$, then:*

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$$

.

Proof. Choose a σ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$ which we know exists by theorem 17, and take $a \in \mathcal{O}_L$. We have $Frob_{\mathfrak{P}}\sigma^{-1}(a) - \sigma^{-1}(a)^{|N(\mathfrak{p})|} \in \mathfrak{P}$. Now apply σ on both sides and we get:

$$\sigma Frob_{\mathfrak{P}}\sigma^{-1}(a) - \sigma\sigma^{-1}(a)^{|N(\mathfrak{p})|} \in \sigma(\mathfrak{P}) = \sigma(\mathfrak{P}) = \mathfrak{P}'.$$

Concretely, we have:

$$\sigma Frob_{\mathfrak{P}}\sigma^{-1}(a) - a^{|N(\mathfrak{p})|} \in \mathfrak{P}'$$

which by definition 35 means that $\sigma Frob_{\mathfrak{P}}\sigma^{-1} \in \left(\frac{L/K}{\mathfrak{P}'}\right)$. □

Definition 36. *Let L/K be a Galois field extension with Galois Group G. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_L$ unramified in L. Then we define:*

$$\left(\frac{L/K}{\mathfrak{p}}\right)$$

as the conjugate class of the Frobenius Symbol in definition 35. This will often be denoted as $Frob_{\mathfrak{p}}$ for it when choice of element does not matter. Now our choice of the Frobenius element is independent of $\mathfrak{P}$ as long as $\mathfrak{P}$ does not ramify.

Remark 9. *When the Galois group is abelian, we get a unique Frobenius symbol because all $\mathfrak{P}$ over $\mathfrak{p}$ are in the same conjugacy class $\left(\frac{L/K}{\mathfrak{p}}\right)$ trivially.*

Example 16. *By example 15 we had that 7 splits into two unique primes $(2+3\zeta_3^2)(2+3\zeta_3) \in \mathbb{Z}[\zeta_3]$. So it is unramified, and we showed that both primes are unramified with inertia degree one, thus:*

$$G_{(2+3\zeta_3^2)} \cong Gal(\kappa((2+3\zeta_3^2)/\kappa(7)) = Gal(F_7/F_7).$$

Same happens for the other prime and here the only Frobenius element is the identity.

We will take a look at the prime 5 now , it remains a prime because if we assume $5 = \mathfrak{P}_1\mathfrak{P}_2$ we get

$$N_{\mathbb{Z}[\zeta_3]} = N_{\mathbb{Z}[\zeta_3]}(\mathfrak{P}_1)N_{\mathbb{Z}[\zeta_3]}(\mathfrak{P}_2)$$

and to not get a unit, one of them must satisfy:

$$N_{\mathbb{Z}[\zeta_3]}(\mathfrak{P}_i) = 5 \iff a^2 + b^2 + ab = 5.$$

But considering this equation modulo 3, we have:

$$\iff a^2 + b^2 + ab \equiv (a^2 + 2ab + b^2) \equiv 5 \equiv 2 \mod 3.$$

But there is no element $x \in F_3$ such that $x^2 = 2$, thus no solution exists and 5 stays inert.

So by 8 , we have that $\sum_{i=1}^{1} e_i f_i = 1 \cdot f = 2$ and so $\kappa(5) \cong F_{5^2}$.

Here we have the Frobenius element $Frob_5 : a + b\zeta_3 \to a + b\zeta_3^5$ for $\sigma \in Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q})$, since

$$\sigma(a + b\zeta_3) \equiv Frob_5(a + b\zeta_3) \equiv a + b\zeta_3^5 \mod 5.$$

We will do one more example, and then we will classify the Frobenius elements for unramified primes p in extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

We will need some more theoretical results.

Corollary 4 ([1, Cor. p. 63])**.** *For an odd prime p,*

$$p \text{ ramifies in } \mathbb{Q}(\zeta_n) \iff p \mid n.$$

Example 17. *For example 7 does not ramify for $\mathbb{Q}(\zeta_5)$ and so it has a unique $Frob_{\mathfrak{p}}$ for some prime $\mathfrak{p}$ lying above it. Splitting here gives the same Frob element because our Galois group is abelian, by proposition 22, and consequently the Frobenius symbol is just the conjugacy class with one element in this case. $Frob_7$ is the element which is precisely $\sigma_a \in Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ which sends $\sigma(\zeta_5) = \zeta_5^a$ for $a = 7$ as we see down below.*

$$Frob_7 : (\zeta_5 \equiv \zeta_5^7 \mod \mathfrak{p}).$$

This comes from us requiring $\zeta_5^a = \zeta_5^7$ and so a must be chosen as the equivalence class in $(Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ such that $a \equiv 7 \mod 5$.

More generally we will deduce the Frobenius element $Frob_{\mathfrak{p}}$ for a general extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ for unramified primes, i.e $p \nmid n$.

Proposition 23 ([5, Ex. p. 34])**.** *For the field extension $(Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, let p be a prime lying under $\mathfrak{p}$ which does not ramify does not ramify in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Then the Frobenius element is:*

$$\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{\mathfrak{p}}\right) = \sigma_{|N(p)|} = \sigma_p.$$

Proof. Let $\mathfrak{p}$ lie above any unramified prime p. Then we have a unique element $\sigma_a \in D_{\mathfrak{p}}$ such that:

$$\sigma_a(x) \equiv x^p \mod \mathfrak{p}.$$

Since we know that $\mathcal{O}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} = \mathbb{Z}[\zeta_n]$ we require,

$$\sigma_a(k\zeta_n) = k^p\zeta_n^a \equiv k\zeta_n^p \mod \mathfrak{p}$$

for $k \in \mathbb{Z}$. This is equivalent to a satisfying:

$$a \equiv p \mod n.$$

And so we know that the Frobenius element is the unique equivalence class $a \in (\mathbb{Z}/n\mathbb{Z})^*$ that satisfies $a \equiv p \mod p$. □

Theorem 20 ([5, Thm . p. 35])**.** *Let L/K be a Galois extension of number fields with group G. For every element $\sigma \in Gal(L/K)$ there exist infinitely many primes $\mathfrak{P} \in \mathcal{O}_L$ such that:*

$$\left(\frac{L/K}{\mathfrak{P}}\right) = \sigma.$$

and $|N(\mathfrak{P})|$ is a prime.

This theorem connects local data about primes to global info, we will see that it contains Dirichlet's theorem on prime progression as a consequence.

Theorem 21 ([5, Ex. p. 45])**.** *Let $a, m \in \mathbb{Z}$ such that $gcd(a, m) = 1$. Then there exists infinitely many primes p such that:*

$$p \equiv a \mod n.$$

Proof. From earlier we derived that for primes p which are unramified in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, the Frobenius symbol was just one element, and more precisely:

$$\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{\mathfrak{p}}\right) = \sigma_p.$$

for p lying under $\mathfrak{p}$. Now using Chebatorev's density theorem 20 we have infinitely many $\mathfrak{p}$ that lie over some prime p such that:

$$\sigma_a \equiv \sigma_{N(\mathfrak{p})} = \sigma_p \mod \mathfrak{p}$$

for our fixed $\sigma_a \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and in particular we have:

$$\zeta_n^a = \zeta_n^p$$

for infinitely many primes p and this is equivalent to having infinitely many primes p satisfying:

$$p \equiv a \mod n.$$

□

8 Brief Rep Theory

We will soon define an object that requires representation theory on Galois groups. We will here go through the necessary background in this section. We will only use the theory over finitely dimensional $\mathbb{C}$ vector-spaces and finite groups G.

Definition 37. *Over a finite group* $\mathbf{G}$*, and a vector space* $\mathbf{V}$*, a complex, finite representation is the group homomorphism:*

$$\rho : G \to GL(V)$$

where $\mathbf{GL(V)}$ *is the group of invertible matrices over* $\mathbf{V}$ *and* V *is a finite dimensional* $\mathbb{C}$ *vector space.*

Each element $g \in \mathbf{G}$ *acts on the underlying vector space* $\mathbf{V}$ *via* $\rho(g)(v)$*.*

We will denote the representations as (ρ, V)*.*

We will also define the notion of a homomorphism between representations.

Definition 38. *For representations* $(\rho_1, \mathbf{V_1})$ *and* $(\rho_2, \mathbf{V_2})$ *of a finite group* $\mathbf{G}$ *we have a morphism of representations defined as:*

$$\varphi : V_1 \to V_2$$

being a $\mathbf{C}$ *linear map and respecting the action of* $\mathbf{G}$ *´via:*

$$\varphi(\rho_1(g)(v_1)) = \rho_2(g)(\varphi(v_1))$$

for $\forall g \in G, \forall v_1 \in \mathbf{V_1}$*.*

It is furthermore an isomorphism if φ is a bijective map of the underlying vector spaces.

Definition 39. *A representation* W *is said to be* G*-invariant if*

$$\rho(g)W \subseteq W, \forall g \in G.$$

Definition 40. *Let G be a finite group and V, W two G representations. We say that W is a subrepresentation of V if $W \subseteq V$ as vector spaces and W is G-invariant.*

Example 18. *Consider $G = S_3$ and $V = \mathbb{C}^3$. The subspace $U \subset V$ such that U contains all elements (x, y, z) such that $x + y + z = 0$ for $x, y, z \in V$. Now any action by $\rho(g)$ on V is via permuting x, y, z but since addition commutes:*

$$\rho(g)U \subseteq U.$$

since the sum $x + y + z = 0$ is invariant under permuting x, y, z.

Definition 41. *If the only invariant subspace that exists are the 0 space or V itself we call our representation irreducible.*

An important function is the functions called characters , which we define down below. Their role in the case we are in, G being finite our vector spaces being over $\mathbb{C}$, these functions are the backbone of the theory.

Definition 42.

$$\chi_\rho : G \to \mathbb{C}, \quad g \to tr(\rho(g)).$$

Lemma 3. *For isomorphisms of* **G** *representations, ρ_1, ρ_2 we have that the character is invariant.*

We use the fact that trace is invariant under conjugation from linear algebra.

Proof. By G-equivariance we have:

$$\rho_1(g) = \varphi^{-1}\rho_2(g)\varphi$$

for φ being a $\mathbb{C}$ linear map. By applying trace on both sides, we get:

$$\begin{aligned} tr(\rho_1(g)) &= tr(\varphi^{-1}\rho_2(g)\varphi) \\ &= tr(\varphi\varphi^{-1}\rho_2(g)) \\ &= tr(\rho_2(g)) \end{aligned}$$

□

We will give a fundamental proof that every representation over a finite group G and over a field with character equal to zero. In particular this works for our field we will work with, which is $\mathbb{C}$.

In this setting it will turn out that the irreducible representations play a role similar to the way prime elements over $\mathbb{Z}$, in a sense that every representation can be broken down uniquely up to order, if we consider the irreducible reps up to isomorphism.

But before we will need slightly more machinery.

Definition 43. *Let $\langle .,. \rangle$ denote a Hermitian inner product on a representation V, we then define a new one as $\langle v_1, v_2 \rangle_{\mathbf{G}} := \frac{1}{|\mathbf{G}|} \sum_{g \in \mathbf{G}} \langle \rho(g)v_1, \rho(g)v_2 \rangle$, $\forall v_1, v_2 \in V$.*

Remark 10. *It's a positive Hermetain inner product.*

Lemma 4. *This product is G invariant, in the sense that*

$$\langle v_1, v_2 \rangle_{\mathbf{G}} = \langle \rho(h)v_1, \rho(h)v_2 \rangle_{\mathbf{G}}$$

for $h \in G$.

Proof.

$$\begin{aligned} < \rho(h)v_1, \rho(h)v_2 > &= \frac{1}{|\mathbf{G}|} \sum_{g \in \mathbf{G}} < \rho(g)\rho(h)v_1, \rho(g)\rho(h)v_2 > \\ &= \frac{1}{|\mathbf{G}|} \sum_{g \in \mathbf{G}} < \rho(gh)v_1, \rho(gh)v_2 > \\ &= \frac{1}{|\mathbf{G}|} \sum_{g \in \mathbf{G}} < \rho(g')v_1, \rho(g')v_2 > \\ &=< v_1, v_2 >_{\mathbf{G}} \end{aligned}$$

They are the same since G acting on itself as $g \mapsto hg$ is just a bijective permutation of its own elements. □

This will help us prove a significant result for our work with representations. First we will prove a lemma that will make the proof of the theorem short.

Proposition 24. *If (W, ρ) is a subrepresentation of (V, ρ) for a finite group $\mathbf{G}$, then there is a complementary invariant subspace W^p of V such that $V = W \oplus W^p$.*

Proof. We will define $W^p = \{v \in V | < v, w >= 0, \forall w \in W\}$ and by the lemma 4 we have $< v_1, v_2 >_{\mathbf{G}} =< \rho(h)v_1, \rho(h)v_2 >_{\mathbf{G}}$ and thus our complementary subspace is also G-invariant. Then using Orthogonal decomposition theorem from linear algebra one gets $V = W \oplus W^p$. □

Now the theorem we wanted follows naturally from the last proposition.

Theorem 22. *Any Representation over a finite group is a direct sum of irreducible representations.*

Theorem 23 (Schurs Lemma)**.** *If (V, ρ_1) and (W, ρ_2) are irreducible non-zero representations of $\mathbf{G}$ and $\varphi : V \to W$ is a G-module morphism, then:*

1) Either φ is an isomorphism or $\varphi = 0$.

2) If $V = W$, then $\varphi = \lambda \cdot 1$ for some $\lambda \in \mathbf{C}$ and 1 is the identity.

Proof. Notice that $(Ker(\varphi), \rho_1) \subset (V, \rho_1)$ and $(Im(\varphi), \rho_2) \subset (W, \rho_2)$. Since V is ireducible $Ker(\varphi)$ is either all of V or 0. For the same reason $im(\varphi)$ is either all of W or 0. Assume that it is V, then by the first isomorphism theorem:

$$V \cong Im(\varphi)$$

, then we know that V cant be isomorphic too 0 and so $im(\varphi) = W$ and we have $V \cong W$.

Assume now that $ker(\varphi) = 0$, then once again by the first isomorphism theorem:

$$0 \cong im(\varphi)$$

and thus $im(\varphi) = 0$ and φ is precisely the zero map. This proves the first part.

In the second part, since $\mathbf{C}$ is algebraic closed we have an eigenvalue λ such that $\varphi - \lambda I$ has a non-zero kernel, and since V is irreducible , it follows that:

$$ker(\varphi - \lambda I) = V,$$

i.e. that $\varphi = \lambda I, \forall v \in V$. □

Notice that every representation (V, ρ), whenever you fix a g you have that $\rho(g) \in End(V)$ as vector spaces because then $\rho(g)$ is just an element in $GL(V)$,so a matrice acting on V which is invertible. But the representation is not necessarily G-equivariant, i.e. it must not lie in $End_G(V)$. But whenever $g \in \mathcal{Z}_G$, i.e the the center we have for any irreducible representation (ρ) over a group G. For a fixed g have that:

$$\rho(g)\rho(h) = \rho(gh) = \rho(hg) = \rho(h)\rho(g), \forall h \in G.$$

So the image of the center $\mathcal{Z}_G$ by ρ are G-equivariant maps, i.e $\rho(\mathcal{Z}_G) \subseteq End_G(V)$ with equality if and only if G is an abelian group.

With the discussion above we get the following classification.

We will build towards more general criterion's of irreducibility, that work even for G not abelian. We will introduce a few notations and theorems.

Definition 44. *For complex valued characters χ, ψ we have:*

$$\langle \chi, \psi \rangle =: \sum_{g \in G} \chi(g)\overline{\psi(g)}.$$

Theorem 24. *If χ is a character of some irreducible representation:*

a) If χ is a character of some irreducible representation, we have:

$$\langle \chi, \chi \rangle = 1.$$

b) If χ, ψ are characters of non-isomorphic irreducible representations , we have:

$$\langle \chi, \psi \rangle = 0.$$

Proposition 25. *For two representations:*

$$\rho_1 \to GL(V_1) \text{ and } \rho_2 \to GL(V_2)$$

we have that that the character of $V1 \oplus V_2$ hhas character $\chi_1 + \chi_2$.

As a consequence of this and the orthogonal relation we have the following relation.

Theorem 25. *Let V be a representation and suppose it decomposes as:*

$$V = W_1 \oplus W_2 ... \oplus W_n.$$

where W_i are all irreducible, not necessarily distinct.

Let Φ be a the character of V and let χ be the representation for a some irreducible Representation W of V.

Then the number of W_i isomorphic to W is equal to $\langle \Phi, \chi \rangle$.

Proof. By proposition 25 we have that:

$$\Phi = \chi_1 + ... + \chi_n$$

where χ_i is the character of W_i.

Further, by bi-linearity of $\langle\rangle$:

$$\langle \Phi, \chi \rangle = \langle \chi_1 + ... + \chi_n, \chi \rangle = \langle \chi_1, \chi \rangle + ... + \langle \chi_n, \chi \rangle.$$

Now using the theorem 24 we know that $\langle \chi_i, \chi \rangle = 1$ and 0 otherwise, we have that:

$$\langle \Phi, \chi \rangle = \sum_{W \cong W_i} 1 = m_i$$

where n_i is the amount of irreducible representations isomorphic to W. □

Corollary 5. *If two representations have the same character they are isomorphic.*

So our rep can be written as:

$$V = m_1 W_1 \oplus ... \oplus m_n W_n$$

with $n_i = \langle \Phi, \chi_i \rangle$.

Then we have that

$$\langle \Phi, \Phi \rangle = \sum_{i=1} \langle \Phi, n_i \chi_i \rangle = \sum_{j=1} \sum_{i=1} \langle n_j \chi_j, n_i \chi_i \rangle.$$

Then by theorem 24 we have that:

$$\sum_{j=1} \sum_{i=1} \langle n_j \chi_j, n_i \chi_i \rangle = \sum_{i=j} n_i^2$$

.

$$\langle \Phi, \Phi \rangle = \sum_{i=1} m_i^2.$$

From the formula $\langle \Phi, \Phi \rangle = \sum_{i=1} m_i^2$ *we acquire a criterion for irreducibility, namely:*

Theorem 26. $\langle \Phi, \Phi \rangle = 1 \iff V$ *is irreducible.*

Proof. We already know that if Φ is irreducible then by theorem 24 , it follows that: $\langle \Phi, \Phi \rangle = 1$.

For the other direction, we assume that $\langle \Phi, \Phi \rangle = 1$.

By our formula above we have:

$$\langle \Phi, \Phi \rangle = \sum_{i=1} m_i^2 = 1$$

and the only way this happens is if $\langle \Phi, \chi_i \rangle = 1$, for some i and zero for the rest, and that $m_i = 1$. In other words that its isomorphic to some irreducible representation. □

We will do an example of a representation that will lead to two more important theorems about characters. And a equality we will see later of our L functions.

Example 19. *Let* ρ_{reg} *be the representation of* G *into* $GL(\mathbb{C}[G])$ *where* $\mathbb{C}[G]$ *is a vector space with bases indexed by* e_g*, for* $g \in G$ *with scalars from* $\mathbb{C}$*.* $\rho_{reg}(h)$ *,* $\forall h \in G$ *acts the following way:*

$$\rho_{reg}(h) e_g = e_{hg}.$$

Definition 45. *We define the representation above as the regular representation.*

Proposition 26. *The character χ_{reg} for the representation ρ_{reg} takes on these following values:*

$$\chi_{reg} = \begin{cases} 0 \text{ if } g \neq e \\ |G| \text{ if } g = e. \end{cases}$$

Proof. We have e_{g_i} in the diagonal of our vector space and our $\rho_{reg}(h)$ fixes it if for some h if $\rho_{reg}(h)e_g = e_{gh} = e_g$, so we require $gh = h$ in the group.

But this gives us that $g = e$ by taking h^{-1} onn both sides and so no basis e_g is fixed under any operation $\rho_{reg}(h)$ except for when $h = e$. Taking the trace now we get what we wanted. □

Corollary 6. *Every irreducible representation is contained m_i times in ρ_{reg} where $Dim(W_i) = m_i$.*

Proof. By theorem 25 we have that the number of times W_i appears in $\mathbb{C}[G]$ is precisely $n_i = \langle \rho_{reg}, \chi_i \rangle$ and then using proposition 26 we get the follwing:

$$\langle \rho_{reg}, \chi_i \rangle = \frac{1}{|G|}(|G|\chi_i(1)) = n_i$$

, since it is well known that the character evaluated at 1, i.e $\chi(1)$, gives the dimension of the rep. □

Corollary 7. *The degrees n_i of the irreducible representations satisfy the following relations:*

a) For $g \in G, g = e$ we have: $\sum_i n_i^2 = 0$.

b) For $g \in G, g \neq e$, we have: $\sum_i n_i^2 = 0$.

Proof. By corollary 6 we have that:

$$\chi_{reg}(g) = \sum_{i=1}^{n} n_i \chi_i(g), \text{ where } n_i \text{ denotes dimension of } n_1.$$

By proposition 26 and setting $g = e$ we get:

$$\chi_{reg}(g) = |G| = \sum_i n_i^2.$$

We also get, that for any $g \in G, g \neq e$, the following:

$$\rho(g) = 0 = \sum_i n_i^2.(i, ind, av, ireps, skriv).$$

□

.

Definition 46. *A class is the set of all functions function f, such that:*

$$f : G \to \mathbb{C}, \quad f(g^{-1}sg) = f(s), \forall s, g \in G.$$

In words, it is invariant under conjugation.

The trace is also known as invariant by basis change matrices, and so this implies that the characters χ are. $\rho(g^{-1})\rho(s)\rho(g)$ .....

Theorem 27. *The characters χ_i make an orthonormal basis for the set of class functions, with a $\mathbb{C}$-Vector space structure.*

Theorem 28. *The number of irreducible representations over a group G, up to isomorphism is equal to the amount of conj classes of G.*

Example 20. *Looking back at our example before of the irreducible representations of S_3 , we can do the example purely algebraically after all of our machinery.*

By corollary 7 and theorem 28 we get the following equation our dimensions must satisfy:

$$n_1^2 + n_2^2 + n_3^2 = 6.$$

We already know that one of these is the trivial rep and so $n_1 = 1$, so our equation is:

$$n_2^2 + n_3^2 = 6 - 1^2.$$

Now the only integer solutions we have left is $n_2 = 1$ and $n_3 = 2$.

Considering $\rho_2 \longmapsto GL_1(\mathbb{C})$ we need that:

$$\begin{aligned} \rho(12)^2 = 1 &\iff \rho(12) = \pm 1 \\ \rho(123)^3 = 1 &\iff \rho(123) = \zeta_3 \\ \rho(12)\rho(123) &= \rho(23). \end{aligned}$$

We also are not interested in $\rho(123) = \rho(12) = 1$ because that's just our trivial representation which we already have. Now by $\rho(12)\rho(123) = \rho(23)$. we get that $\rho(123) = 1$ and thus $\rho(12) = 1$.

We can make a character table with what we have.

	e	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2		

So now we are only missing the two dimensional representation.

Once again:

$$\rho(12)^2 = I_2$$
$$\rho(123)^3 = I_2$$

By theorem 24 we get:

$$\langle \chi_3, \chi_3 \rangle = \frac{1}{6}(2^2 + 3|\chi_3(12)|^2 + 2|\chi_3(123)|^2) = 1.$$

To satisfy $(4 + 3|\chi_3(12)|^2 + 2|\chi_3(123)|^2) = 6$ *we see that* $|\chi_3(12)|^2 = 0$ *and so* $\chi_3(12) = 0$. *And this then also gives us* $|\chi_3(123)| = \pm 1$. *To deduce sign, we will use theorem 24 again, but now as:*

$$\langle \chi_3, \chi_1 \rangle =$$
$$\chi_1(e)\chi_2(e) + 3\chi_1(12)\chi_3(12) + 2\chi_3(123)\chi_1(123) =$$
$$2 + 2\chi_3(123) = 0.$$

This gives us that $\chi_3(123) = -1$ *and this was the last step to get the character table.*

	e	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

8.1 Induced representations

We know basic algebra that restriction gives the opposite direction, i.e if we have a complex representation:

$$\rho : G \to GL(\mathbb{C}),$$

then we can restrict the pre image to elements $h \in (G \cap H = H)$ where H is a subgroup of G and so we get

$$\rho_{res} : H \to GL(\mathbb{C})$$

as a representation on the subgroup H deduced from G.

A natural question to ask is, if you have a known representation on a subgroup H of G, is there a natural way to get a representation on G?

It turns out that this direction requires more work. We will later use this property on Artin L-functions, because they have nice properties under induction.

First note that for a group G and subgroup H we can pick a set of representatives for the left cosets:

$$\mathfrak{N} = \{\mathfrak{g}_1, ..., \mathfrak{g}_n\} \quad \frac{|G|}{|H|} = n.$$

We also have a bijection by G acting on $\mathfrak{N}$ via $g\mathfrak{g}_i H \to \mathfrak{g}_\mathfrak{j} H$. where $\mathfrak{g}_\mathfrak{i}, \mathfrak{g}_\mathfrak{j}$ are unique representatives in $\mathfrak{N}$ and there is a unique h such that $g\mathfrak{g}_i = \mathfrak{g}_\mathfrak{j} h$. We now define an induced representation the following:

Definition 47. *We say that a representation ρ of G in V is induced by a representation ψ of H in W if:*

$$V = \bigoplus_{\mathfrak{g}_i \in \mathfrak{N}} \mathfrak{g}_i W.$$

where

$$\rho(g)\mathfrak{g}_i w := \mathfrak{g}_\mathfrak{j} \psi(h) w$$

and $\rho(g)V$ follows by linearity.

Intuitively, $\rho(g)$ acts by permuting the "coordinates" and $\psi(h)$ acts internally on W. Since W is H invariant we know that $\psi(H)W = W$. And since the g only permutes the $W's$ we see that it is indeed G-invariant.

We will do an example to hopefully make the definition more concrete.

Example 21. *Consider a group G and a subgroup H. We will show that the regular rep ρ_H on H induces the regular rep ρ_G on G, $|\mathfrak{N}| = \frac{|G|}{|H|} = n$.*

By proposition 26 , ρ_H has dimension $|H|$. So the following direct sum :

$$\bigoplus_{g_i \in \mathfrak{N}} g_i W_i$$

has dimension, $\sum_{i=1}^{n} |H| = \frac{|G|}{|H|} \cdot |H| = |G|$.

Since for every $g \in G$ we can be rewritten uniquely as $g = hg_j$ for some g_j, every basis e_g from $\mathbb{C}[g]$ can be written uniquely as $e_{g_j h'}$ and vice versa, every basis in our copies W which are of the form $e_{g_i h}$ can be rewritten as $e_{g_i h} = e_g$ uniquely , because cosets partition G.

This gives a bijection since the sizes are finite.

8.2 Abelinization

Definition 48. *Let G be a group. For any elements $x, y \in G$, we define the commutator of x and y as:*

$$[x, y] := xyx^{-1}y^{-1}.$$

Proposition 27. *We have that $[x, y] = 1 \iff x$ and y commutative.*

Proof. If x, y commute then:

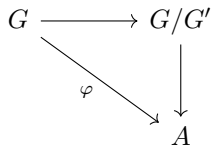
$$[x, y] = xyx^{-1}y^{-1} = yxx^{-1}y^{-1} = yy^{-1} = 1.$$

If $[x, y] = 1$, then $xyx^{-1}y^{-1} = 1 \implies xy = yx$. □

Definition 49. *The commutator subgroup G' of G is the subgroup generated by all commutators:*

$$G' = \langle [x, y] \mid x, y \in G \rangle$$

Proposition 28 ([2, prop . p.169])**.** *If $\varphi : G \to A$ is any homomorphism of G into an abelian group A, then φ factors through G', i.e. $G' \leq \ker \varphi$ and the following diagram commutes:*



Applying this when we have a one dimension representation from G to $\mathbb{C}^*$ we have that every one dimensional representation of G factors through the abelian subgroup $G/G' = G^{AB}$.

This chapter follows the treatment from the books [7] and [6] on representation theory.

9 Artin L functions

Definition 50 ([5, Def. p. 61])**.** *Let L/K be a Galois Extension of number fields with a finite Galois group G. Let $\rho : G \to GL(V)$ be a complex representation over a finite dimensional vector space V. Then for every non-zero prime $\mathfrak{p}$ of $\mathcal{O}_k$ fix a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying over $\mathfrak{p}$ and let $I_{\mathfrak{P}}$ be the corresponding inertia subgroup, then we define the **Artin L-Function** as:*

$$L(\rho, s) = \prod_{\mathfrak{p} \neq 0, \mathfrak{p} \in \mathcal{O}_{\mathbf{K}}} \det\left(id - \rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right) N(\mathfrak{p})^{-s} | V^{I_{\mathfrak{P}}}\right)^{-1}$$

When $\mathfrak{P}$ i ramified over $\mathfrak{p}$ the Frobenius symbol is not well defined and we pick an arbitrary Frobenius element of $\mathfrak{P}$. To be more clear we ill sometimes explicitly write the field extension in the L function as $L(s, \rho, L/K)$ for clarity over what extension we are currently over.

9.1 Invariance for choice of $\mathfrak{P}$

We will work towards proving invariance of choosing $\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right)$ or $\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right)$, where $\mathfrak{P}, \mathfrak{P}'$ both lie over the same prime ideal $\mathfrak{p}$. This is important to show that our local factor is independent of choice, and thus well defined.

Lemma 5. *There exists a $\sigma \in G$ such that:*

$$I_{\mathfrak{P}'} = \sigma I_{\mathfrak{P}} \sigma^{-1}.$$

Proof. By proposition 17 , $\exists \sigma in \mathbf{G}$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Now for any $\psi \in I_{\mathfrak{P}}$. We have:

$$\psi\sigma^{-1}(x) - \sigma^{-1}(x) \in \mathfrak{P} \iff \sigma\psi\sigma^{-1}(x) - x \in \sigma(\mathfrak{P}) = \mathfrak{P}' \iff \sigma\psi\sigma^{-1} \in I'_{\mathfrak{P}}.$$

□

Notice that the element σ had the same property as the one in proposition 22, namely $\sigma(\mathfrak{P}) = \mathfrak{P}'$. This plays a big part in controlling the fixed spaces $V^{I_{\mathfrak{P}}}$ and $V^{I_{\mathfrak{P}'}}$ in the local factor which will be crucial to show independence of choice for $\mathfrak{P}$ over $\mathfrak{p}$.

Proposition 29 ([5, Prop. p. 62-63])**.** *$Dim(V^{I_{\mathfrak{P}}}) = Dim(V^{I'_{\mathfrak{P}}})$ for different choices of primes $\mathfrak{P}, \mathfrak{P}'$ over $\mathfrak{p}$.*

Proof. Take $v \in V^{I'_{\mathfrak{P}}}$ and let $\rho : G \to GL(V)$. By definition of $v \in V^{I_{\mathfrak{P}'}}$:

$$\rho(\psi')v = v, \forall \psi' \in I'_{\mathfrak{P}} = \sigma I_{\mathfrak{P}} \sigma^{-1}.$$

Thus we have:

$$\rho(\psi')v = \rho(\sigma\psi\sigma^{-1})v = v, \forall \psi \in I_{\mathfrak{P}}.$$

Since ρ is a group homomorphism,

$$\rho(\sigma)\rho(\psi)\rho(\sigma^{-1})v = v \iff \rho(\psi)\rho(\sigma^{-1})v = \rho(\sigma^{-1})v, \forall \psi \in I_{\mathfrak{P}}.$$

We thus get that if v is fixed by $\rho(\psi')$ in $V^{I_{\mathfrak{P}'}}$, then $\rho(\sigma^{-1})v$ is fixed by $\rho(\psi)$, $\forall \psi \in I_{\mathfrak{P}}, \forall \psi' \in I_{\mathfrak{P}'}$. So $\rho(\sigma)^{-1}V^{I_{\mathfrak{P}'}} = V^{I_{\mathfrak{P}}} \implies V^{I_{\mathfrak{P}'}} = \rho(\sigma)V^{I_{\mathfrak{P}}}$. Since $\rho(\sigma) \in GL(V)$ it gives an isomorphism of vector the spaces $V^{I_{\mathfrak{P}}}, V^{I_{\mathfrak{P}'}}$ and by the dimension theorem we thus know that,

$$dim(V^{I_{\mathfrak{P}}}) = dim(V^{I_{\mathfrak{P}'}}).$$

□

Proposition 30 ([5, prop. p. 62-63])**.** *We have that*

$$\det\left(id - \rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right) N(\mathfrak{p})^{-s} | V^{I_{\mathfrak{P}}}\right)$$

=

$$\det\left(id - \rho\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right) N(\mathfrak{p})^{-s} | V^{I_{\mathfrak{P}'}}\right)$$

as complex numbers.

Proof. Define the characteristic polynomial $f_{\mathfrak{P}}(t) := \det\left(id - t\rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right)|V^{I_{\mathfrak{P}}}\right)$.

Then we have $\rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right) = \rho(\sigma)\rho\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right)\rho(\sigma)^{-1}$. by proposition 22 and lemma 5. Thus:

$$\begin{aligned} f_{\mathfrak{P}}(t) = \\ \det\left(id - t\rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right)|V^{I_{\mathfrak{P}}}\right) = \\ \det\left(id - t\rho(\sigma)\rho\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right)\rho(\sigma)^{-1}|V^{I_{\mathfrak{P}'}}\right). \end{aligned}$$

Now using the fact that *Det* is a group homomorphism and invariant under conjugation we have:

$$\begin{aligned} \det\left(id - t\rho(\sigma)\rho\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right)\rho(\sigma)^{-1}|V^{I_{\mathfrak{P}'}}\right) = \\ \det(\rho(\sigma))^{-1}\det\left(id - t\rho(\sigma)\rho\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right)\rho(\sigma)^{-1}|V^{I_{\mathfrak{P}'}}\right)\det(\rho(\sigma)) = \\ \det\left(id - t\rho(\sigma)^{-1}\rho(\sigma)\rho\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right)\rho(\sigma)^{-1}\rho(\sigma)|V^{I_{\mathfrak{P}'}}\right) = \\ f_{\mathfrak{P}'}(t). \end{aligned}$$

$\rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right) = \rho(\sigma)\rho\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right)\rho(\sigma)^{-1}$ is a change of basis and our representation goes from acting on $V^{I_{\mathfrak{P}}}$ too $V^{I_{\mathfrak{P}'}}$, which is why it changes in the first line. Evaluated at $t = N(\mathfrak{p})^{-s}$ they are the same. □

Theorem 29 ([5, thm. p. 64-65])**.** *$L(s,\rho)$ converges absolutely for all $\Re(s) > 1$.*

Proof. Every Galois Group we consider is finite with order n, thus every element g has finite order, and since we are over $\mathbb{C}$ the eigenvalues of $\rho(\frac{L/K}{\mathfrak{P}})$ are roots of unity because $\rho(g^n)v = \rho(g)^n v = Iv$. Now consider an eigenvalue λ and we get $v = \rho(g)^n v = \alpha^n v \implies \alpha^n = 1$.

In particular we can write this as a over-triangular matrice over $\mathbb{C}$ where the diagonal is of eigenvalues. Let $\zeta_{\mathfrak{P},i}$ denote the eigenvalues above. We then get that each factor $\det\left(id - t\rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right)|V\right) = \prod_{i=1}^{dim(V)}|1 - t\zeta_{\mathfrak{P},i}|^{-1}$ is none-zero evaluated at $t = \frac{1}{N(\mathfrak{p})^s}$ for $\Re(s) > 1$ since $|\zeta_i| = 1$.

To check convergence we are allowed to remove finitely many terms because it does not affect convergence. Then by proposition [[5, prop. p. 34]] there is only finitely many ramified primes, which we ser aside.

Looking at only the unramified ones, we know that $V^{I_{\mathfrak{P}}} = V$ by proposition 21.

We now have:

$$\det\left(id-\rho\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right)N(\mathfrak{p})^{-s}|V^{I_{\mathfrak{P}'}}\right)=$$
$$\prod_{\mathfrak{p}}\prod_{i=1}^{dim(V)}|1-N(\mathfrak{p})^{-1}\zeta_{\mathfrak{P},i}|^{-1}\leq\prod_{\mathfrak{p}}\prod_{i=1}^{dim(V)}(1-|char(\mathfrak{p})^{-s}|)^{-1}$$

Because $char(\mathfrak{p})=p\leq p^f=N(\mathfrak{p})$ and the reverse triangle inequality. Continuing we get:

$$\prod_{\mathfrak{p}}\prod_{i=1}^{dim(V)}(1-|char(\mathfrak{p})^{-s}|)^{-1}\leq\prod_{i=1}^{dim(V)}\prod_{\mathfrak{p}}(1-char(\mathfrak{p})^{-\Re(s)})^{-1}$$

Because $|n^{-s}|=n^{-\Re(s)}$, and we can switch a finite and infinite product.

$$\prod_{i=1}^{dim(V)}\prod_{\mathfrak{p}}(1-|char(\mathfrak{p})^{-\Re(s)}|)^{-1}=$$
$$\prod_{i=1}^{dim(V)}\prod_{p}\prod_{p|\mathfrak{p}}(1-p^{-\Re(s)})^{-1}.$$

The last equality is because $char(\mathfrak{p})=p$, and the amount of times $(1-p^{-\Re(s)})^{-1}$ amount of $\mathfrak{p}|p$ contributes n times. Now the last inequality is:

$$\prod_{i=1}^{dim(V)}\prod_{p}\prod_{p|\mathfrak{p}}(1-p^{-\Re(s)})^{-1}\leq\zeta(\Re(s))^{dim(V)[K:\mathbb{Q}]}.$$

The $[K:\mathbb{Q}]$ part comes from theorem 18 which says that a prime $p\in\mathbb{Z}$ splits with at most $[K:\mathbb{Q}]$ in $\mathcal{O}_K$. We know the Euler product converges and thus our Artin L function converges. □

Proposition 31 ([5, prop. p. 65])**.** *Consider the definition of an Artin L function, let ρ_{id} to be the identity representation for $Gal(L/K)$, and set $L=K$, then for this setup we get that:*

$$L(\rho_{id},s)=\zeta_K(s)$$

.

Proof.

$$L(s,\rho_{id})=\prod_{\mathfrak{p}}det\left(Id-\rho_{id}\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right)N(\mathfrak{p})^{-s}|V\right)^{-1}=$$
$$\prod_{\mathfrak{p}}det\left(Id-1N(\mathfrak{p})^{-s}\right)^{-1}=\zeta_K(s).$$

Under the trivial representation, $\rho_{id}v = v, \forall g \in G, v \in V$ and thus we get $V^{I_\mathfrak{P}} = V$. □

Notice that $\zeta_K(s) = \zeta(s)$ for $K = \mathbb{Q}$ and so we have shown that the Artin L-function generalizes the Dedekind Zeta function and the Riemann Zeta function. It is also worth mentioning that an abelian class of $L - fucnitons$, denoted as Hecke L-functions, and Dirichlet L-functions are also a special case of the Artin L-function.

We will focus on defining the Hecke L-function due to its important role in saying something about the Artin's Conjecture about Artin's L-functions which we will introduce n the next section.

Definition 51 ([5, Def. p. 67])**.** *Let L/K be a Galois extension, with Galois group G. Then for any one dimensional representations $\rho : G \to GL(\mathbb{C})$, we define the Hecke L-function as the following Artin L-function:*

$$L(s, \rho).$$

They also admit an analytic continuation,

Theorem 30 ([5, thm. p. 65])**.** *Let L/K be a Galois extension with corresponding abelian Galois group G, and let $\chi : G \to \mathbb{C}^*$ be a nontrivial representation. The Hecke L-function $L(\chi, \rho)$ admits an analytic continuation to the full complex plane.*

We will show how our Artin L-functions behave under representation theory. Since we know that over $\mathbb{C}$, our representations are reducible into a unique decomposition by theorem 22 and so a natural question would be is to ask what $L(s, \rho_1 \oplus \rho_2)$ is equal too.

Proposition 32 ([5, Thm. p. 68])**.** *For an extension L/K, and two complex representations ρ_1, ρ_2 from G, we have the following result.*

$$L(s, \rho_1 \oplus \rho_2) = L(s, \rho_1)L(s, \rho_2).$$

Proof. If you have two representations ρ_1, ρ_2 with matrices in $GL_i(\mathbb{C}), GL_j(\mathbb{C})$ then $\rho_1 \oplus \rho_2 \in GL_{i+j}(\mathbb{C})$. With the following form:

$$\rho_1 \oplus \rho_2 = \begin{bmatrix} \rho_1 & 0 \\ 0 & \rho_2 \end{bmatrix}.$$

Now by linear algebra $\det(\rho_1 \oplus \rho_2) = \det(\rho_1)\det(\rho_2)$ and thus:

$$L(t, \rho_1 \oplus \rho_2) = \prod_{\mathfrak{p} \in \mathcal{O}_K} \left(\det(1 - t(\rho_1 \oplus \rho_2) \left(\left(\frac{L/K}{\mathfrak{P}} \right) \right) | V^{I_\mathfrak{P}} \right) =$$

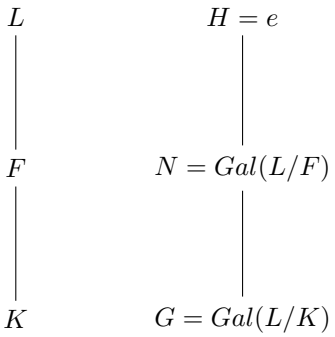
$$\prod_{\mathfrak{p} \in \mathcal{O}_K} \left(\det(1 - t\rho_1 \left(\left(\frac{L/K}{\mathfrak{P}} \right) \right) | V^{I_\mathfrak{P}} \right) \prod_{\mathfrak{p} \in \mathcal{O}_K} \left(\det(1 - t\rho_2 \left(\left(\frac{L/K}{\mathfrak{P}} \right) \right) | V^{I_\mathfrak{P}} \right) =$$

$$L(s, \rho_1)L(s, \rho_2).$$

□

And we will now introduce another property, namely how Artin L-function act via induction.

Considering a tower of galois extensions , $L/F/K$ and the corresponding Galois groups, $G = Gal(L/K)$, $N = Gal(L/F)$ and $H = e$. via theorem 12



One might ask if $L(s, \mathrm{Ind}(\rho)_N^G)$ gives us something interesting, and it turns out it does.

Proposition 33 ([5, thm. p. 68])**.** *Take our setup as above, and let γ be a complex representation of N, then we get:*

$$L(s, \mathrm{Ind}(\gamma)_N^G) = L(s, \gamma).$$

We omit the proof.

Remark 11. *To be clear, this property is not at all trivial. By definition:*

$$L(s, \mathrm{Ind}_N^G(\gamma) = (\prod_{\mathfrak{p} \in \mathcal{O}_K} \left(\det(1 - N(\mathfrak{p})^{-s} \rho_2 \left(\left(\frac{L/K}{\mathfrak{P}} \right) \right) | V^{I_\mathfrak{P}} \right)$$

and,

$$L(s, \gamma) = \prod_{\mathfrak{F} \in \mathcal{O}_F} \left(\det(1 - N(\mathfrak{F})^{-s} \gamma \left(\left(\frac{L/F}{\mathfrak{P}} \right) \right) | V^{I_\mathfrak{P}} \right)$$

and so for this to be true, we would the induction effect to even out, over how prime ideals $\mathfrak{p} \in \mathcal{O}_K$ split over $\mathcal{O}_F$ as prime ideals $\mathfrak{F}$, and the different Frobenius symbols.

This will be used in the next section, which we have built up for.

10 Artins cojecture on the Analytic properties of the Artin L-function

Conjecture 1 ([5, Thm. p. 73])**.** *For a Galois extension over number fields L/K , and a complex irreducible representation ρ for G, $L(s, \rho)$ has an analytic*

continuation to the whole complex plane.

Before we prove this we will now name a theorem, this theorem is the main reason for introducing induction to begin with.

Theorem 31 ([5, Thm. p. 74])**.** *Let G be a finite group and $\rho : G \to GL_n(\mathbb{C})$ be a finite dimensional complex representation. There exists finitely many subgroups $H_1, ..., H_r$ of G with characters $\lambda_i : H_i \to \mathbb{C}^*$ for $i = 1, ..., r$ and integers $n_1, .., n_r$ such that:*

$$\operatorname{tr}(\rho(g)) = \sum_{i=1}^{r} n_i \operatorname{tr}(\operatorname{Ind}_{H_i}^{G}(\lambda_i))(g)$$

$\forall g \in G$.

Theorem 32 ([5, thm. p. 74])**.** *For a Galois extension L/K with finite group G, and for every complex representation ρ of $\mathbf{G}$, the function $L(s, \rho)$ admits a meromorphic continuation on the complex plane.*

Proof. Let $\chi := \operatorname{tr}(\rho)$. Then by theorem 31 :

$$\chi = \sum_{i=1}^{r} n_i \operatorname{tr}(\operatorname{Ind}_{H_i}^{G}(\lambda_i).$$

Now moving our negative coefficients on the right-handside, by adding them on both sides, we get :

$$\chi + \sum n_i \operatorname{tr}(\operatorname{Ind}_{H_i}^{G}(\lambda_i)) = \sum n_j \operatorname{tr}(\operatorname{Ind}_{H_j}^{G}(\lambda_j)$$

where all coefficients are now positive.

By corollary 5 we know that over $\mathbb{C}$, our representations are determined by the character and we thus get:

$$\rho \oplus \bigoplus (\operatorname{Ind}_{H_i}^{G}(\lambda_i))^{\oplus n_i} = \bigoplus Ind_{H_j}^{G}(\lambda_j)^{\oplus n_j} ..$$

Since these representations are equal we get:

$$L(s, \rho \oplus \bigoplus (\operatorname{Ind}_{H_i}^{G}(\lambda_i))^{\oplus n_i}, L/L^{H_i}) = L(s, \bigoplus \operatorname{Ind}_{H_j}^{G}(\lambda_j)^{\oplus n_j}, L/L^{H_j}).$$

By proposition 32 we further get:

$$L(s, \rho) \prod L(s, Ind_{H_i}^{G}(\lambda_i), L/L^{H_i})^{n_i} = \prod L(s, \operatorname{Ind}_{H_j}^{G}(\lambda_j), L/L^{H_j})^{n_j}.$$

To make it explicit, we get: and by proposition 33,

$$L(s, \rho) = \frac{\prod L(s, \operatorname{Ind}_{H_i}^{G}(\lambda_i), L/L^{H_i})^{n_i}}{\prod L(s, \operatorname{Ind}_{Hj}^{G}(\lambda_j), L/L^{H_j})^{n_j}} = \frac{\prod L(s, \lambda_i, L/L^{H_i})^{n_i}}{\prod L(s, \lambda_j, L/L^{H_j})^{n_j}}.$$

Now by proposition 28 we have that all our one dimensional reps factor through an abelian group and thus we can use theorem 30 the left hand-side is a quotient of holomorphic functions, and thus our Artin L-function is meromorphic. □

Remark 12. *If our n_i in the proof above,were positive to begin with, we never would have had to move the negative coefficients to the other side, we would not get a quotient in the end of the proof, but rather a product of holomorphic Hecke L-functions. This would have given us that the corresponding Artin L-function would be holomorphic.*

A version of Brauer's induction theorem but with positive integers does not exist in general.

References

[1] Jürgen Neukrich, *Algebraic Number Thoery*, Springer,

[2] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Wiley

[3] Antoine Chambert-Loir, *(Mostly) Commutative Algebra*, Springer

[4] Kenneth Ireland, Michael rosen, *Modern number theory*,

Springer

[5] Davide Lombardo *L-Functions, an elementary introduction* Springer

[6] J-P. Serre, *Linear Representations of Finite Groups*, Springer

[7] W. Fulton and J. Harris, *Representation Theory: A First Course*, Springer