Inverse Galois Problem

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Abhishek Kumar Shukla

IISER PUNE

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

April, 2016

Supervisor: Steven Spallone

This is to certify that this dissertation entitled Inverse Galois Problem towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents original research carried out by Abhishek Kumar Shukla at Indian Institute of Science Education and Research under the supervision of Steven Spallone, Associate Professor, Department of Mathematics, during the academic year 2015-2016.

Steven Spallone

Committee:
Steven Spallone
Michael D.Fried

Declaration

I hereby declare that the matter embodied in the report entitled Inverse Galois Problem are the results of the investigations carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Steven Spallone and the same has not been submitted elsewhere for any other degree.

Abhishek

Abhishek Kumar Shukla

Acknowledgments

I would like to extend my sincere and heartfelt gratitude towards Dr. Steven Spallone for his constant encouragement and able guidance at every step of my project. He has invested a great deal of time and effort in my project, and this thesis would not have been possible without his mentorship. I would like to thank my thesis committee member Prof. Michael D.Fried for his guidance and valuable inputs throughout my project.

I am grateful to Dr. Vivek Mallick, Dr. Krishna Kaipa and Dr. Supriya Pisolkar for patiently answering my questions.

Abstract

In this thesis, motivated by the Inverse Galois Problem, we prove the occurence of S_n as Galois group over any global field. While Hilbert's Irreducibility Theorem, the main ingredient of this proof, can be proved(for $\mathbb{Q}$) using elementary methods of complex analysis, we do not follow this approach. We give a general form of Hilbert's Irreducibility Theorem which says that all global fields are Hilbertian. Proving this takes us to Riemann hypothesis for curves and Chebotarev Density Theorem for function fields. In addition we prove the Chebotarev Density Theorem for Number Fields. The main reference for this thesis is [1] and the proofs are borrowed from the same.

Contents

Chapter 1

Introduction

Given a field K and a finite group G, the **Inverse Galois Problem** is to find a Galois extension L of K such that $\mathrm{Gal}(L/K) \cong G$. While the problem is still open over $\mathbb{Q}$, it has an affirmative solution over $\mathbb{C}(t)$. We are interested in extensions of $\mathbb{Q}$. It is easy to see that IGP has a solution over $\mathbb{Q}$ for any finite abelian group G. Indeed, if G is a finite abelian group, then by the structure theorem for finitely generated abelian groups,

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z} \tag{1.1}$$

where $m_1 \mid m_2 \mid \ldots \mid m_k$.

By Dirichlet's theorem, which we will prove in the next chapter, there are infinitely many primes congruent to $1 \mod m_i$ for each $1 \leq i \leq k$. Choose primes $p_1, \ldots, p_k$ such that $p_i \equiv 1 \mod m_i$. Thus, corresponding to each m_i we obtain a subgroup H_i of $(\mathbb{Z}/p_i\mathbb{Z})^*$ of index m_i.

We know that

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1 \ldots p_k})/\mathbb{Q}) &\cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_2})/\mathbb{Q}) \times \ldots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k})/\mathbb{Q}) \\ &\cong (\mathbb{Z}/p_1\mathbb{Z})^* \times (\mathbb{Z}/p_2\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_k\mathbb{Z})^* \end{aligned} \tag{1.2}$$

Since $H_1 \times H_2 \times \ldots \times H_k$ is a subgroup of the RHS of index $m_1 \ldots m_k$, there exists H a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_1 \ldots p_k})/\mathbb{Q})$ of the same index. Being an abelian extension, every subgroup is normal and hence

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}^H/\mathbb{Q}) &\cong \frac{\mathrm{Gal}(\mathbb{Q}(\zeta_{p_1\dots p_k})/\mathbb{Q})}{H}\\ &\cong \frac{\mathbb{Z}/(p_1-1)\mathbb{Z}}{H_1} \times \frac{\mathbb{Z}/(p_2-1)\mathbb{Z}}{H_2} \times \dots \times \frac{\mathbb{Z}/(p_k-1)\mathbb{Z}}{H_k}\\ &\cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}\\ &\cong G.\end{aligned} \tag{1.3}$$

In following chapters we will build enough theory to show that IGP can be solved over $\mathbb{Q}$ for S_n for any positive integer n.

Chapter 2

Chebotarev Density Theorem for Number Fields

In this chapter we will give an elementary proof of the Chebotarev Density Theorem. In particular we do not assume any knowledge of class field theory. All fields occuring in this chapter are number fields. The exposition follows more or less Chapter 6 of [1].

Let L/K be a finite Galois extension of fields. By fixing an unramified prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, we know that the Frobenius elements living over $\mathfrak{p}$ form a conjugacy class $\mathcal{C}$ in $\mathrm{Gal}(L/K)$.

Suppose we start with an arbitrary conjugacy class $\mathcal{C}$ in $\mathrm{Gal}(L/K)$ and ask whether we can find an unramified prime ideal $\mathfrak{p}$ such that its associated conjugacy class is $\mathcal{C}$. The Chebotarev Density Theorem answers this question in the affirmative and moreover also proves that there are infinitely many such prime ideals.

Let $P(K)$ be the set of prime ideals in $\mathcal{O}_K$ and $A \subset P(K)$, we define

$$\delta(A) = \lim_{s \to 1^+} \frac{\Sigma_{\mathfrak{p} \in A} (N\mathfrak{p})^{-s}}{\Sigma_{\mathfrak{p} \in P(K)} (N\mathfrak{p})^{-s}} \tag{2.1}$$

whenever the limit exists.

Remark 2.0.1. 1. For every $\mathfrak{p} \in P(K)$ there lies a prime $p \in \mathbb{Z}$ such that $\mathfrak{p} \mid p$

and there can be at most $[K:\mathbb{Q}]$ prime ideals above a give prime $p \in \mathbb{Z}$. Thus,

$$\begin{aligned} \sum_{\mathfrak{p} \in P(K)} (N\mathfrak{p})^{-x} &= \sum_{p \in P(\mathbb{Z})} \sum_{\mathfrak{p}|p} (N\mathfrak{p})^{-x} \\ &\leq \sum_{p \in P(\mathbb{Z})} \sum_{\mathfrak{p}|p} p^{-x} \\ &\leq [K:\mathbb{Q}] \sum_{p \in P(\mathbb{Z})} p^{-x} \\ &\leq [K:\mathbb{Q}]\zeta(x) < \infty, \end{aligned} \tag{2.2}$$

where $x \in \mathbb{R}$ such that $x > 1$ and $\zeta(x)$ is the Riemann-Zeta function.

2. We observe that for x as above

$$\frac{1}{1+(N\mathfrak{p})^{-x}} < \frac{1}{1-(N\mathfrak{p})^{-x}} \leq 1 + 2(N\mathfrak{p})^{-x}. \tag{2.3}$$

Thus we may conclude that $\prod_{\mathfrak{p} \in P(K)} (1-(N\mathfrak{p})^{-x})^{-1}$ converges.

3. We also note that

$$|A_k| = |\{\mathfrak{p} \in P(K); N\mathfrak{p} \leq k\}| < \infty. \tag{2.4}$$

4. Thus,

$$\prod_{\mathfrak{p} \in P(K); N\mathfrak{p} < k} (1-(N\mathfrak{p})^{-x})^{-1} = \sum_{\mathfrak{a} \in T} (N\mathfrak{a})^{-x} \tag{2.5}$$

where T is the set of all ideals in $\mathcal{O}_K$ such that only primes in A_k occur in its factorization.

5. Taking $k \to \infty$, we get that

$$\sum_{\mathfrak{a}} (N\mathfrak{a})^{-x} = \prod_{\mathfrak{p} \in P(K)} (1-(N\mathfrak{p})^{-x})^{-1}, \tag{2.6}$$

where $\mathfrak{a}$ runs over all non-zero ideals in $\mathcal{O}_K$. This is also referred to as **Euler factorization**.

6. If $\delta(A)$ exists and is non-zero, then A is infinite. Moreover, whenever the limit exists it is a real number lying between 0 and 1.

Theorem 2.0.2 (**Chebotarev Density Theorem**)**.** Let L/K be a finite Galois extension and suppose $\mathcal{C}$ is a conjugacy class in $\mathrm{Gal}(L/K)$ and let

$$A = \left\{ \mathfrak{p} \in P(K), \left(\frac{L/K}{\mathfrak{p}} \right) = \mathcal{C} \right\}. \tag{2.7}$$

Then $\delta(A)$ exists and equals $\frac{|\mathcal{C}|}{[L:K]}$.

The proof of the above theorem is given in steps. Sequentially, we prove the CDT for:

1. Cyclotomic extensions.
2. Abelian extension by Chebotarev's field crossing argument.
3. Arbitrary Galois extension by reducing to the cylic case.

We mention a lemma which will be used a couple of times.

Lemma 2.0.3. Let $a, b, n \in \mathbb{N}$ such that $(a, n) = (b, n) = 1$. Then $\zeta^a = \zeta^b \Leftrightarrow \zeta^a \equiv \zeta^b$ in $\mathcal{O}_{\mathbb{Q}(\zeta)}/\mathfrak{p}$, where $\mathfrak{p}$ is a prime lying over $p \in \mathbb{Z}$ such that $(p, n) = 1$ and ζ is a primitive n^{th} root of unity.

Proof. The direction $\Rightarrow$ is clear.
$\Leftarrow$ Let $K = \mathbb{Q}(\zeta)$ and if $\zeta^a \neq \zeta^b$ and $\zeta^a \equiv \zeta^b \mod \mathfrak{p}$ where $\mathfrak{p}$ is as in the Lemma. Then $\zeta^a - \zeta^b \in \mathfrak{p}$.
But

$$\begin{gathered} \prod_{1 \leq i,j \leq n, i \neq j} (\zeta^i - \zeta^j) = (-1)^{n-1} n^n \\ \prod_{1 \leq i,j \leq n, i \neq j, (i,n)=1, (j,n)=1} (\zeta^i - \zeta^j) = \mathrm{disc}(K/\mathbb{Q}). \end{gathered} \tag{2.8}$$

Thus,

$$\begin{gathered} n^n \mathcal{O}_K \subset \mathrm{disc}(K/\mathbb{Q}) \mathcal{O}_K \subset (\zeta^a - \zeta^b) \mathcal{O}_K \subset \mathfrak{p} \\ n^n \mathcal{O}_K \subset \mathfrak{p} \Rightarrow n \mathcal{O}_K \subset \mathfrak{p} \Rightarrow n \mathcal{O}_K \cap \mathbb{Z} \subset \mathfrak{p} \cap \mathbb{Z} \Rightarrow p \mid n. \end{gathered} \tag{2.9}$$

This is a contradiction. □

2.1 Cyclotomic extension

Now we begin our proof of the density theorem for cyclotomic extensions. An extension L/K is called **cyclotomic** if $L \subset K(\zeta_n)$ for some primitive n^{th} root of unity ζ_n. Let $\mathfrak{c} \subset \mathcal{O}_K$ be a non-zero ideal and define

$$J(\mathfrak{c}) := \{\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k} \mid e_i \in \mathbb{Z}, \mathfrak{p}_i \nmid \mathfrak{c}\}. \tag{2.10}$$

In other words, $J(\mathfrak{c})$ is the multiplicative subgroup of all fractional ideals coprime to $\mathfrak{c}$.

For L/K an abelian extension, we define an integral ideal $\mathfrak{c} \subset \mathcal{O}_K$ to be admissible if the following holds:

If $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$ and $\mathfrak{p}$ ramifies in $\mathcal{O}_L$ then $\mathfrak{c} \subset \mathfrak{p}$.

The ideal generated by the discriminant of the extension is an example of an admissible ideal. For $\mathfrak{c}$ an admissible ideal, we define the **Artin map** as follows:

$$\omega_{\mathfrak{c}} : J(\mathfrak{c}) \to \mathrm{Gal}(L/K), \tag{2.11}$$

where $\omega_{\mathfrak{c}}(\mathfrak{p}) = \left[\frac{L/K}{\mathfrak{p}}\right]$. The symbol $\left[\frac{L/K}{\mathfrak{p}}\right]$ is the corresponding Frobenius element in $\mathrm{Gal}(L/K)$. Note that it is unique since the conjugacy classes are singleton.

Also, $J(\mathfrak{c})$ is free on prime ideals which do not occur in the prime factorization of $\mathfrak{c}$ and hence a map defined on primes extends uniquely to all of $J(\mathfrak{c})$.

If M/L is also an abelian extension and $\mathfrak{c}$ is admissible for M/K, then $\mathfrak{c}$ is also admissible for L/K, and thus we have the following maps and the diagram commutes (since the restriction of a Frobenius is still a Frobenius).

$$\begin{tikzcd}
J(\mathfrak{c}) \arrow[r, "\omega_{\mathfrak{c},L/K}"] \arrow[d, "\omega_{\mathfrak{c},M/K}"] & \mathrm{Gal}(M/K) \arrow[d, "\mathrm{res}"] \\
\mathrm{Gal}(L/K) \arrow[r, "Id"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

For a cyclotomic extension, we will show that the Artin map is surjective. To this end, we define the following.

Let $K_{\mathfrak{c}} \subset K^*$ be the subgroup of all elements $x \in K^*$ which satisfy:

1. If $\mathfrak{p} \mid \mathfrak{c}$, then $x \in \mathcal{O}_{K,\mathfrak{p}}$ and $x \equiv 1$ in $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{c}\mathcal{O}_{K,\mathfrak{p}}$.

2. For all real embeddings $\sigma : K \to \mathbb{R}$, we have $\sigma(x) > 0$.

Let $P(\mathfrak{c}) = \{x\mathcal{O}_K \mid x \in K_\mathfrak{c}\}$. It is easy to see that $P(\mathfrak{c}) \subset J(\mathfrak{c})$. We denote $G(\mathfrak{c}) = J(\mathfrak{c})/P(\mathfrak{c})$ and note that $G(\mathfrak{c})$ is finite (Theorem 1, Chapter 6, [2]).
For $\mathcal{K} \in G(\mathfrak{c})$, we denote $j(\mathcal{K}, n) = \{\mathfrak{a}$ an integral ideal, $[\mathfrak{a}] = \mathcal{K}, N(\mathfrak{a}) \leq n\}$.
We note that

$$|j(\mathcal{K}, n)| = \rho_\mathfrak{c} n + O(n^{1-\frac{1}{[K:\mathbb{Q}]}}), \tag{2.12}$$

where $\rho_\mathfrak{c}$ is a constant which is independent of $\mathcal{K}$. (Theorem 3, Chapter 6, [2])

Lemma 2.1.1. Suppose $K \subset L \subset K(\zeta_m)$ where ζ_m is a primitive m^{th} root of 1 and $\mathfrak{c}$ an ideal in $\mathcal{O}_K$ such that $\mathfrak{c} \subset m\mathcal{O}_K$. Then $\mathfrak{c}$ is admissible and $\omega_\mathfrak{c}$ factors through $G(\mathfrak{c})$.

Proof. We need to show that $P(\mathfrak{c}) \subset \ker(\omega_{\mathfrak{c},L/K})$.
Since the above diagram commutes, it is enough to show that $P(\mathfrak{c}) \subset \ker(\omega_{\mathfrak{c},K(\zeta_m)/K})$.
Also, if a prime $\mathfrak{p}$ ramifies in $K(\zeta_m)$ then $\mathfrak{p} \mid \operatorname{disc}(K(\zeta_m)/K)$ and we know that $\operatorname{disc}(K(\zeta_m)/K) \mid m^m$. Hence $\mathfrak{p} \mid m$. Thus, we have $\mathfrak{p} \mid \mathfrak{c}$. Thus, $\mathfrak{c}$ is admissible.
We know that

$$i : \operatorname{Gal}(K(\zeta_m)/K) \to (\mathbb{Z}/m\mathbb{Z})^* \tag{2.13}$$

defined by $i(\sigma) = a \mod m$ where $\sigma(\zeta_m) = \zeta_m^a$ is an injection.
For a prime ideal $\mathfrak{p} \in J(\mathfrak{c})$, we see that

$$\omega_{\mathfrak{c},K(\zeta_m)/K}(\mathfrak{p})(\zeta_m) \equiv \zeta_m^{N\mathfrak{p}} \mod \mathfrak{b}, \tag{2.14}$$

where $\mathfrak{b}$ is any prime ideal lying above $\mathfrak{p}$. By Lemma(2.0.3), we get that the same relation holds in $K(\zeta_m)$ and hence

$$i \circ \omega_{\mathfrak{c},K(\zeta_m)/K}(\mathfrak{p}) \equiv N\mathfrak{p} \mod m. \tag{2.15}$$

Thus, for any fractional ideal $\mathfrak{a} \in P(\mathfrak{c})$, we have

$$i \circ \omega_{\mathfrak{c},K(\zeta_m)/K}(\mathfrak{a}) \equiv N\mathfrak{a} \mod m. \tag{2.16}$$

For $x = \frac{a}{b} \in K_{\mathfrak{c}}$, such that $a, b \in \mathcal{O}_K$, we see that $a - b \in \mathfrak{c}\mathcal{O}_{K,\mathfrak{p}} \cap \mathcal{O}_K = \mathfrak{c}$ (this is true for Dedekind domains). Thus, $a - b \in \mathfrak{c} \subset m\mathcal{O}_K$.
To compute $N_{K/\mathbb{Q}}(x)$, we can take the normal closure of $K/\mathbb{Q}$ say as T, then $N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in H} \sigma(x)$ where H contains the coset representatives of $\operatorname{Gal}(T/\mathbb{Q})/\operatorname{Gal}(T/K)$.
Since $a - b \in m\mathcal{O}_K \Rightarrow a - b \in m\mathcal{O}_T$ and hence $\sigma(a) - \sigma(b) \in m\mathcal{O}_T$. But then

$$\sigma(a) \equiv \sigma(b) \ in \ \mathcal{O}_T/m\mathcal{O}_T. \tag{2.17}$$

Hence

$$\prod_{\sigma \in H} \sigma(a) \equiv \prod_{\sigma \in H} \sigma(b) \ in \ \mathcal{O}_T/m\mathcal{O}_T. \tag{2.18}$$

Thus,

$$N_{K/\mathbb{Q}}(a) \equiv N_{K/\mathbb{Q}}(b) \ in \ \mathcal{O}_T/m\mathcal{O}_T. \tag{2.19}$$

But both LHS and RHS lie in $\mathbb{Z}$ and hence

$$N_{K/\mathbb{Q}}(a) \equiv N_{K/\mathbb{Q}}(b) \ in \ \mathbb{Z}/m\mathbb{Z}. \tag{2.20}$$

Thus, we have

$$N_{K/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}(\frac{a}{b}) \equiv 1 \ in \ \mathbb{Z}/m\mathbb{Z}. \tag{2.21}$$

Then,

$$N(x\mathcal{O}_K) = N_{K/\mathbb{Q}}(x) \equiv 1 \mod m. \tag{2.22}$$

(here we use the 2^{nd} defining condition of $K_{\mathfrak{c}}$).
Thus,

$$P(\mathfrak{c}) \subset \ker(\omega_{\mathfrak{c},K(\zeta_m)/K}). \tag{2.23}$$

□

Our next aim is to show that the above map $\overline{\omega}_{\mathfrak{c}} : G(\mathfrak{c}) \to \operatorname{Gal}(L/K)$ is surjective. In order to do this, we define L-series and analytically continue it to a larger space and make some observations.

Let G be a finite abelian group. A character χ of G is a group homomorphism from G to $\mathbb{C}^*$. The set of all characters on a group G is represented by $\hat{G}$ and it is easy to see that $|G| = |\hat{G}|$. We also note the following **orthogonality relations** are satisfied by the characters:

1. $\sum_{\chi\in\hat{G}}\chi(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases}$

2. $\sum_{g\in G}\chi(g) = \begin{cases} |G| & \chi = 1 \\ 0 & \chi \neq 1 \end{cases}$

3. $\prod_{\chi\in\hat{G}}(1-\chi(g)Y) = (1-Y^t)^{|G|/t}$ where $t = \mathrm{ord}(g)$.

In order to prove the last relation, suppose $G = \widehat{\langle g\rangle}$, then polynomial on LHS is separable and

$$\begin{aligned} \text{Roots of LHS} &= \{\chi(g)^{-1}|\chi\in\hat{G}\} \\ \text{Roots of LHS} &\subset \text{Roots of RHS} \\ |\hat{G}| = |\text{Roots of LHS}| &\leq |\text{Roots of RHS}| \leq |G| \end{aligned} \tag{2.24}$$

Thus identity follows in cyclic case.
For any G and $g\in G$, if $\chi\in\widehat{\langle g\rangle}$, then we observe that since $\mathbb{C}^*$ is divisible abelian group, it is injective $\mathbb{Z}$-module and hence

$$\chi : \langle g\rangle \to \mathbb{C}^* \tag{2.25}$$

can be lifted to a map

$$\chi_1 : G \to \mathbb{C}^* \tag{2.26}$$

As a result there exists a split exact sequence

$$\begin{gathered} 1 \to H \to \hat{G} \to \widehat{\langle g\rangle} \to 1 \\ \text{where } H = \{\chi\in\hat{G}|\chi(g) = 1\}. \end{gathered} \tag{2.27}$$

Thus, $\hat{G} = \widehat{\langle g\rangle}H$ and

$$\hat{G} = \chi_1 H \ \cup \chi_2 H \cup \ldots \cup \chi_{t-1}H \cup H \tag{2.28}$$

is the coset decomposition, where

$$\widehat{\langle g\rangle} = \{1, \chi_1, \ldots, \chi_{t-1}\} \tag{2.29}$$

We observe that

$$\begin{aligned}\prod_{\chi\in\hat{G}}(1-\chi(g)Y) &= \prod_{i=1}^{t}\prod_{\chi\in\chi_i H}(1-\chi(g)Y)\\ &= \prod_{i=1}^{t}(1-\chi_i(g)Y)^{|H|}\\ &= (\prod_{\chi\in\widehat{\langle g\rangle}}(1-\chi(g)Y))^{|G|/t}\\ &= (1-Y^t)^{|G|/t}.\end{aligned} \tag{2.30}$$

The last equality follows from the cyclic case.

For $\mathfrak{c}$ as above and χ a character on $G(\mathfrak{c})$, we define

$$L_{\mathfrak{c}}(s,\chi) = \sum_{(\mathfrak{a},\mathfrak{c})=1}\frac{\chi([\mathfrak{a}])}{(N\mathfrak{a})^s}, \Re(s) > 1 \tag{2.31}$$

The summation runs over all integral ideals coprime to $\mathfrak{c}$.

Remark 2.1.2. 1. For defining an L-series and its convergence we do not require $\mathfrak{c}$ to be admissible.

2. Convergence of the L-series can be seen by comparing with equation 6.

3. L-series for the trivial character is called **Dedekind zeta function** of K with respect to the ideal $\mathfrak{c}$ and denoted by $\zeta_{\mathfrak{c}}(s,K)$.

$$\zeta_{\mathfrak{c}}(s,K) = \sum_{(\mathfrak{a},\mathfrak{c})=1}\frac{1}{(N\mathfrak{a})^s}, \Re(s) > 1 \tag{2.32}$$

The function χ is multiplicative on $J(\mathfrak{c})$ and by using the argument similar to (6), we derive an **Euler factorization**

$$L_{\mathfrak{c}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{c}}\frac{1}{1-\frac{\chi([\mathfrak{p}])}{(N\mathfrak{p})^s}}, \Re(s) > 1 \tag{2.33}$$

We take the following Lemma (Chapter 5, [2]) for granted.

Lemma 2.1.3. Let $\{a_i\}_{i\in\mathbb{N}}$ be a sequence of complex numbers for which there is a

$0 \leq \sigma < 1$ and a complex number ρ such that

$$\sum_{i=1}^{n} a_i = \rho n + O(n^{\sigma}), n \to \infty. \tag{2.34}$$

Then

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s} \tag{2.35}$$

defined for $\Re(s) > 1$ analytically continues to $\Re(s) > \sigma$ except for a simple pole at $s = 1$ with residue ρ.

Corollary 2.1.4. The L-series $L_{\mathfrak{c}}(s, \chi)$ has an analytic continuation to $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$.
Moreover, if $\chi = 1$, then it has a simple pole with residue $h_{\mathfrak{c}}\rho_{\mathfrak{c}}$ and if $\chi \neq 1$, it is analytic on whole of $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$.

Proof. Define $a_n := \sum_{a \in J(\mathfrak{c}), N\mathfrak{a}=n} \chi([\mathfrak{a}])$ and observe that $|a_n| < \infty$. Then,

$$\begin{aligned}
\sum_{i=1}^{n} a_i &= \sum_{a \in J(\mathfrak{c}), N\mathfrak{a} \leq n} \chi([\mathfrak{a}]) \\
&= \sum_{\mathcal{K} \in G(\mathfrak{c})} \sum_{\mathfrak{a} \in j(\mathcal{K}, n)} \chi([\mathfrak{a}]) \\
&= \sum_{\mathcal{K} \in G(\mathfrak{c})} \chi(\mathcal{K}) \sum_{\mathfrak{a} \in j(\mathcal{K}, n)} 1 \\
&= \sum_{\mathcal{K} \in G(\mathfrak{c})} \chi(\mathcal{K}) j(\mathcal{K}, n).
\end{aligned} \tag{2.36}$$

By plugging in the estimates of $j(\mathcal{K}, n)$ in the above equation we get
For $\chi = 1$,

$$\sum_{i=1}^{n} a_i = h_{\mathfrak{c}}\rho_{\mathfrak{c}} n + O(n^{1-\frac{1}{[K:\mathbb{Q}]}}). \tag{2.37}$$

For $\chi \neq 1$, by using the orthogonality relations,

$$\sum_{i=1}^{n} a_i = 0 + O(n^{1-\frac{1}{[K:\mathbb{Q}]}}). \tag{2.38}$$

Hence, by above lemma, $L_{\mathfrak{c}}(s, 1)$ analytically extends to $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ with a simple pole at $s = 1$ with residue $h_{\mathfrak{c}}\rho_{\mathfrak{c}}$ and $L_{\mathfrak{c}}(s, \chi)$, for $\chi \neq 1$, can be analytically continued to the entire half plane $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$.

□

Recalling the context we are in i.e $K \subset L \subset K(\zeta_m)$ and $\mathfrak{c}$ an admissible ideal (since it was divisible by $m\mathcal{O}_K$) we will relate the Dedekind zeta function of $\mathfrak{c}\mathcal{O}_L$ to L-series over K.
Denote $G := \overline{\omega}_{\mathfrak{c}}(G(\mathfrak{c}))$ and denote $n := [\mathrm{Gal}(L/K) : G]$. We observe that any character χ of G lifts to a character $\chi \circ \overline{\omega}_{\mathfrak{c}}$ on $G(\mathfrak{c})$.

Lemma 2.1.5. Let $\mathfrak{C} := \mathfrak{c}\mathcal{O}_L$ and n as above. Then

$$\zeta_{\mathfrak{C}}(s, L) = \prod_{\chi \in \hat{G}} L_{\mathfrak{c}}(s, \chi \circ \overline{\omega}_{\mathfrak{c}})^n. \tag{2.39}$$

Proof. We will use orthogonality relation 3 with $Y = \frac{1}{(N\mathfrak{p})^s}$ and group G as above. We observe that, any prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \nmid \mathfrak{c}$, is unramified and hence splits into g primes in $\mathcal{O}_L$ each with inertia f. Thus, $[L:K] = fg$.
But

$$\begin{aligned} \mathrm{ord}(\overline{\omega}_{\mathfrak{c}}(\mathfrak{p})) &= \mathrm{ord}(\omega_{\mathfrak{c}}(\mathfrak{p})) \\ &= \mathrm{ord}([\frac{L/K}{\mathfrak{p}}]) \\ &= |D_{\mathfrak{B}}| = f, \end{aligned} \tag{2.40}$$

where $\mathfrak{B}$ is any prime lying above $\mathfrak{p}$. Using 3 with $Y = \frac{1}{(N\mathfrak{p})^s}$, we get

$$\prod_{\chi \in \hat{G}} (1 - \frac{\chi(\overline{\omega}_{\mathfrak{c}}(\mathfrak{p}))}{(N\mathfrak{p})^s}) = (1 - \frac{1}{(N\mathfrak{p})^{sf}})^{|G|/f}. \tag{2.41}$$

Taking n^{th} powers,

$$\prod_{\chi \in \hat{G}} (1 - \frac{\chi(\overline{\omega}_{\mathfrak{c}}(\mathfrak{p}))}{(N\mathfrak{p})^s})^n = (1 - \frac{1}{(N\mathfrak{p})^{sf}})^{|G|n/f} = (1 - \frac{1}{(N\mathfrak{p})^{sf}})^g = \prod_{\mathfrak{B}|\mathfrak{p}} (1 - \frac{1}{(N\mathfrak{B})^s}). \tag{2.42}$$

But then

$$\begin{aligned}\zeta_{\mathfrak{C}}(s,L)^{-1} &= \prod_{\mathfrak{B}\nmid\mathfrak{C}}(1-\frac{1}{(N\mathfrak{B})^s})^{-1} \\ &= \prod_{\mathfrak{p}\nmid\mathfrak{c}}\prod_{\mathfrak{B}|\mathfrak{p}}(1-\frac{1}{(N\mathfrak{B})^s})^{-1} \\ &= \prod_{\mathfrak{p}\nmid\mathfrak{c}}\prod_{\chi\in\hat{G}}(1-\frac{\chi(\overline{\omega}_{\mathfrak{c}}(\mathfrak{p}))}{(N\mathfrak{p})^s})^{-n} \\ &= \prod_{\chi\in\hat{G}}\prod_{\mathfrak{p}\nmid\mathfrak{c}}(1-\frac{\chi(\overline{\omega}_{\mathfrak{c}}(\mathfrak{p}))}{(N\mathfrak{p})^s})^{n} \\ &= \prod_{\chi\in\hat{G}} L_{\mathfrak{c}}(s,\chi\circ\overline{\omega}_{\mathfrak{c}})^{-n}.\end{aligned} \tag{2.43}$$

□

Now we will show surjectivity of the map $\overline{\omega}_{\mathfrak{c}}$ by showing $n = 1$ by using above lemma.

Lemma 2.1.6. Let χ be a nontrivial character of G, then:

1. $L_{\mathfrak{c}}(1,\chi\circ\overline{\omega}_{\mathfrak{c}}) \neq 0$.
2. $\log\zeta_{\mathfrak{c}}(s,K) = -\log(s-1) + O(1), s \to 1^+$.
3. $n = 1$.

Proof.

1. If χ is nontrivial, so is $\chi\circ\overline{\omega}_{\mathfrak{c}}$, thus if $L_{\mathfrak{c}}(1,\chi\circ\overline{\omega}_{\mathfrak{c}}) = 0$, then Lemma(2.1.5) product on the RHS would be analytic at $s = 1$. Indeed, since the n^{th} power of Dedekind zeta function on RHS has a pole of order n which is cancelled by zero of order n of $L_{\mathfrak{c}}(s,\chi\circ\overline{\omega}_{\mathfrak{c}})^n$. Every other term on RHS is analytic at $s = 1$ and hence it is forced that the LHS is also analytic at $s = 1$ which contradicts our earlier assertion about Dedekind zeta function always having a pole at $s = 1$.
2. This is basically the restatement that Dedekind zeta function has a pole at $s = 1$.
3. Since the RHS has a pole of order n at $s = 1$, so should the LHS. Thus, $n = 1$.

□

Suppose we prove that

$$\log \zeta_{\mathfrak{c}}(s, K) = \sum_{\mathfrak{p}} \frac{1}{(N\mathfrak{p})^s} + O(1), s \to 1^+. \tag{2.44}$$

Then we make the observation that

$$\begin{aligned}\left| \frac{\frac{\sum_{\mathfrak{p}\in A}(N\mathfrak{p})^{-s}}{-\log(s-1)}}{\frac{\sum_{\mathfrak{p}\in A}(N\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}}(N\mathfrak{p})^{-s}}} - 1 \right| &= \left| \frac{\sum_{\mathfrak{p}(N\mathfrak{p})^{-s}}}{\log(s-1)} + 1 \right| \\ &= \frac{\left|\sum_{\mathfrak{p}}(N\mathfrak{p})^{-s} + \log(s-1)\right|}{|\log(s-1)|} \\ &\leq \frac{\left|\sum_{\mathfrak{p}}(N\mathfrak{p})^{-s} - \log\zeta_{\mathfrak{c}}(s,K)\right|}{|\log(s-1)|} \\ &\quad + \frac{|\log\zeta_{\mathfrak{c}}(s,K) + \log(s-1)|}{|\log(s-1)|}.\end{aligned} \tag{2.45}$$

As $s \to 1^+$, we see that numerators of both the sums are bounded and since denominators tends to infinity, we get that

$$\delta(A) = \frac{\sum_{\mathfrak{p}\in A}(N\mathfrak{p})^{-s}}{-\log(s-1)}. \tag{2.46}$$

Lemma 2.1.7. If χ is a character of $G = \mathrm{Gal}(L/K)$, then

$$\log L_{\mathfrak{c}}(s, \chi \circ \overline{\omega}_{\mathfrak{c}}) = \sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi \circ \overline{\omega}_{\mathfrak{c}}(\mathfrak{p})}{(N\mathfrak{p})^s} + O(1), s \to 1^+. \tag{2.47}$$

Proof. Using the Euler factorization of L-series,

$$L_{\mathfrak{c}}(s, \chi) = \prod_{\mathfrak{p}\nmid\mathfrak{c}} \frac{1}{1 - \frac{\chi([\mathfrak{p}])}{(N\mathfrak{p})^s}} \tag{2.48}$$

converges on the right side of 1.

Taking logarithm on both sides we get,

$$\log L_{\mathfrak{c}}(s,\chi) = -\sum_{\mathfrak{p}\nmid\mathfrak{c}} \log(1 - \frac{\chi([\mathfrak{p}])}{(N\mathfrak{p})^s}). \tag{2.49}$$

Close to 1, we can use the power series expansion of complex logarithm i.e

$$\log(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}. \tag{2.50}$$

Thus,

$$\begin{aligned}\log L_{\mathfrak{c}}(s,\chi) &= \sum_{\mathfrak{p}\nmid\mathfrak{c}} \sum_{n=1}^{\infty} \frac{\chi([\mathfrak{p}])^n}{n(N\mathfrak{p})^{sn}} \\ &= \sum_{n=1}^{\infty} \sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi([\mathfrak{p}])^n}{n(N\mathfrak{p})^{sn}} \qquad (2.51)\\ &= \sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi([\mathfrak{p}])}{(N\mathfrak{p})^s} + \sum_{n=2}^{\infty} \sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi([\mathfrak{p}])^n}{n(N\mathfrak{p})^{sn}}.\end{aligned}$$

Hence, it is enough to show that close to 1

$$\sum_{n=2}^{\infty} \sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi([\mathfrak{p}])^n}{n(N\mathfrak{p})^{sn}} \tag{2.52}$$

is bounded. We let $\sigma = \Re(s)$

$$\begin{aligned}
\left|\sum_{n=2}^{\infty}\sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi([\mathfrak{p}])^n}{n(N\mathfrak{p})^{sn}}\right| &= \left|\sum_{\mathfrak{p}\nmid\mathfrak{c}}\sum_{n=2}^{\infty} \frac{\chi([\mathfrak{p}])^n}{n(N\mathfrak{p})^{sn}}\right| \\
&\leq \sum_{\mathfrak{p}\nmid\mathfrak{c}}\sum_{n=2}^{\infty} \frac{1}{n(N\mathfrak{p})^{\sigma n}} \\
&\leq \sum_{\mathfrak{p}\in P(K)}\sum_{n=2}^{\infty} \frac{1}{n(N\mathfrak{p})^{\sigma n}} \\
&\leq \sum_{p\in P(\mathbb{Q})}\sum_{\mathfrak{p}|p}\sum_{n=2}^{\infty} \frac{1}{(N\mathfrak{p})^{\sigma n}} \\
&\leq \sum_{p\in P(\mathbb{Q})}[K:\mathbb{Q}]\sum_{n=2}^{\infty} \frac{1}{(N\mathfrak{p})^{\sigma n}} \qquad (2.53)\\
&\leq [K:\mathbb{Q}]\sum_{p\in P(\mathbb{Q})}\sum_{n=2}^{\infty} \frac{1}{p^{\sigma n}} \\
&\leq [K:\mathbb{Q}]\sum_{p\in P(\mathbb{Q})} \frac{1}{p^{2\sigma}}\frac{1}{1-p^{-\sigma}} \\
&\leq [K:\mathbb{Q}]\sum_{p\in P(\mathbb{Q})} \frac{1}{p^{2\sigma}} \\
&\leq [K:\mathbb{Q}]\sum_{p\in P(\mathbb{Q})} \frac{1}{p^{2}} \\
&< \infty.
\end{aligned}$$

Hence we are done.

□

Using the above Lemma(2.1.7) for the trivial character we get

$$\log\zeta_{\mathfrak{c}}(s,K) = \sum_{\mathfrak{p}\nmid\mathfrak{c}}(N\mathfrak{p})^{-s} + O(1), s \to 1^+. \qquad (2.54)$$

Thus,

$$\log\zeta_{\mathfrak{c}}(s,K) = \sum_{\mathfrak{p}\in P(K)}(N\mathfrak{p})^{-s} + O(1), s \to 1^+. \qquad (2.55)$$

Hence, we can say that

$$\delta(A) = \frac{\sum_{\mathfrak{p}\in A}(N\mathfrak{p})^{-s}}{-\log(s-1)}. \tag{2.56}$$

Now, we observe that for a given $\sigma \in \mathrm{Gal}(L/K)$

$$A = \left\{\mathfrak{p} \in P(K), \left[\frac{L/K}{\mathfrak{p}}\right] = \sigma\right\} = \{\mathfrak{p} \in P(K), \overline{\omega}_{\mathfrak{c}}(\mathfrak{p}) = \sigma\}. \tag{2.57}$$

Consider

$$f(s) := \sum_{\chi\in\hat{G}} \chi(\sigma^{-1})\log(L_{\mathfrak{c}}(s, \chi\circ\overline{\omega}_{\mathfrak{c}})), \Re(s) > 1 \tag{2.58}$$

In this expression,

$$f(s) = \log(\zeta_{\mathfrak{c}}(s,K)) + \sum_{\chi\in\hat{G},\chi\neq 1} \chi(\sigma^{-1})\log(L_{\mathfrak{c}}(s, \chi\circ\overline{\omega}_{\mathfrak{c}})). \tag{2.59}$$

We observe that the $L_{\mathfrak{c}}(s,\chi)$ is analytic at 1 for all $\chi \neq 1$ and hence is bounded close to 1. We also know that

$$\log(\zeta_{\mathfrak{c}}(s,K)) = -\log(s-1) + O(1) \tag{2.60}$$

in a suitable neighbourhood of 1. Thus,

$$f(s) = -\log(s-1) + O(1), s \to 1^{+}. \tag{2.61}$$

On the other hand, using the Lemma(2.1.5), close to 1

$$\begin{aligned} f(s) &= \sum_{\chi\in\hat{G}} \chi(\sigma^{-1})(\sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi\circ\overline{\omega}_{\mathfrak{c}}(\mathfrak{p})}{(N\mathfrak{p})^{s}} + O(1)) \\ &= \sum_{\chi\in\hat{G}}\sum_{\mathfrak{p}\nmid\mathfrak{c}} \chi(\sigma^{-1})\frac{\chi\circ\overline{\omega}_{\mathfrak{c}}(\mathfrak{p})}{(N\mathfrak{p})^{s}} + O(1) \\ &= \sum_{\chi\in\hat{G}}\sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi(\sigma^{-1}\overline{\omega}_{\mathfrak{c}}(\mathfrak{p}))}{(N\mathfrak{p})^{s}} + O(1) \\ &= \sum_{\mathfrak{p}\nmid\mathfrak{c}}\sum_{\chi\in\hat{G}} \frac{\chi(\sigma^{-1}\overline{\omega}_{\mathfrak{c}}(\mathfrak{p}))}{(N\mathfrak{p})^{s}} + O(1) \end{aligned} \tag{2.62}$$

But orthogonality relation2 dictate that the sum will always be zero for $\mathfrak{p} \notin A$ and for $\mathfrak{p} \in A$ we will get $[L : K]$, thus we get

$$f(s) = [L : K] \sum_{\mathfrak{p} \in A} (N\mathfrak{p})^{-s} + O(1) \tag{2.63}$$

Thus,

$$\begin{aligned} \left| \frac{\sum_{\mathfrak{p}\in A}(N\mathfrak{p}^{-s})}{-\log(s-1)} - \frac{1}{[L:K]} \right| &= \left| \frac{[L:K]\sum_{\mathfrak{p}\in A}(N\mathfrak{p}^{-s}) + \log(s-1)}{[L:K]\log(s-1)} \right| \\ &\leq \frac{\left|[L:K]\sum_{\mathfrak{p}\in A}(N\mathfrak{p}^{-s}) - f(s)\right|}{|[L:K]\log(s-1)|} + \frac{|f(s)+\log(s-1)|}{|[L:K]\log(s-1)|}. \end{aligned} \tag{2.64}$$

Both of the terms in the above sum are bounded and hence as $s \to 1^+$,we get that

$$\delta(A) = \frac{1}{[L : K]}. \tag{2.65}$$

Thus, we have proved CDT for the special case of cyclotomic extensions.

Corollary 2.1.8 (Dirichlet's theorem)**.** Let a, n be positive integers such that $(a, n) = 1$, then there exist infintely many rational primes p in the arithmetic progession $\{a + tn \mid t \in \mathbb{Z}\}$.

Proof. Consider the sets

$$A = \{p \in P(\mathbb{Q}) \mid p \equiv a \mod n\} \tag{2.66}$$

$$B = \left\{ p \in P(\mathbb{Q}) \mid \left[\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p}\right] \equiv a \mod n \right\}. \tag{2.67}$$

Since $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$, where the isomorphism is decided after fixing a primitive n^{th} root of unity (but here we do have a canonical choice which we represent by $\zeta_n = e^{2\pi i/n}$ and it sends $\sigma \to c$ where $\sigma(\zeta_n) = \zeta_n^c$ and it is through this identification that we write Frobenius elements as elements of $(\mathbb{Z}/n\mathbb{Z})^*$.
It is obvious that $B \subset A$ and the other inclusion follows from Lemma(2.0.3) for abelian extensions, thus $A = B$.
But CDT for cycltomic extensions gives that $\delta(A) = \delta(B) = \frac{1}{\phi(n)}$ and hence A is infinite. □

2.2 Abelian extension

Lemma 2.2.1. Let L/K be a finite abelian extension and m be a positive integer. Then there exists a cyclotomic field M of degree m such that $M \cap L = K$.

Proof. Suppose $K = \mathbb{Q}$, then let L' be the maximal cyclotomic extension contained in L. Then $L' \subset \mathbb{Q}(\zeta_k)$ for some positive integer k.

Then, find a prime q such that $q > k$ and $q \equiv 1 \mod m$ by Dirichlet's theorem. Thus, $m \mid q-1$ and hence there is a unique subfield $M \subset \mathbb{Q}(\zeta_q)$ such that $[M : \mathbb{Q}] = m$ and the Galois group is cyclic. Also, $\mathbb{Q} \subset M \cap L' \subset \mathbb{Q}(\zeta_q) \cap \mathbb{Q}(\zeta_k) = \mathbb{Q}(\zeta_{\gcd(q,k)}) = \mathbb{Q}$. Thus, $M \cap L' = \mathbb{Q}$ and since $L \cap M \subset M \subset \mathbb{Q}(\zeta_q)$, we infer that $L \cap M \subset L'$ as L' is maximal cyclotomic. Thus $L \cap M = \mathbb{Q}$.
Now for the general case,
We find M' which is cyclotomic and cyclic of degree m, then choose $M = KM'$. Since $L \cap M' = \mathbb{Q}$, we have that $K \cap M' = \mathbb{Q}$ and hence $[KM' : K] = [M' : \mathbb{Q}] = m$ and their Galois groups are isomorphic.

$$\begin{tikzcd}
L & & KM' & \\
& K \arrow[ul, dash] \arrow[ur, dash] & & M' \\
& & \mathbb{Q} \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

Since, L and M' are linearly disjoint over $\mathbb{Q}$, by Theorem 20.12 in [3], K and M' are linearly disjoint over $\mathbb{Q}$ and L and KM' are linearly disjoint over K. Since, L and KM' are linearly disjoint over K, we get that $L \cap KM' = K$. □

For each M as above $\mathrm{Gal}(M/K) = \langle \tau \rangle$ and $\tau^m = 1$.
Now, we begin the proof of CDT for abelian extension.
Suppose L/K is an abelian extension and $\sigma \in \mathrm{Gal}(L/K)$ and we know that $\mathrm{ord}(\sigma) \mid \mathrm{ord}(\tau)$. In other words, if $\mathrm{ord}(\tau) = m = p_1^{b_1} \dots p_k^{b_k}$ and $\mathrm{ord}(\sigma) = n = p_1^{a_1} \dots p_k^{a_k}$ we have $a_i \leq b_i$.

Consider the set

$$T(M/K) = \{\tau^i, \mathrm{ord}(\sigma) \mid \mathrm{ord}(\tau^i)\} \tag{2.68}$$

Then we calculate the size of $T(M/K)$.
Let $l = m/n$ and $A = \{1 \leq i \leq m, \gcd(i,m)|l\}$. We get a bijection from $T(M/K)$ to A by sending $\tau^i \to i$.
Let $B = \{1 \leq i \leq l, i|l\}$.
Then we get a surjective map $\theta : A \to B$ by sending $i \to \gcd(i,m)$.
The cardinality of each fibre can be computed easily. More precisely, for $d \in B$, $|\theta^{-1}(d)| = \phi(m/d)$.
Thus, $|T(M/K)| = |A| = \Sigma_{d|l}\phi(m/d)$.
But $\phi(m/d) = \frac{m}{d}\prod_{i=1}^{k}\frac{p_i-1}{p_i}$.
We get

$$\begin{aligned}|A| = \sum_{d|l}\phi(m/d) &= \Sigma_{d|l}\frac{m}{d}\prod_{i=1}^{k}\frac{p_i-1}{p_i}\\ &= m\prod_{i=1}^{k}\frac{p_i-1}{p_i}(\sum_{d|l}\frac{1}{d}) \qquad (2.69)\\ &= \frac{m}{l}\prod_{i=1}^{k}\frac{p_i-1}{p_i}(\sum_{d|l}\frac{l}{d}).\end{aligned}$$

But if $x = p_1^{y_1}\dots p_l^{y_l}$, then sum of its divisors is given by $\prod_{i=1}^{l}\frac{p_i^{y_i+1}-1}{p_i-1}$.
Hence,

$$|A| = \frac{m}{l}\prod_{i=1}^{k}\frac{p_i-1}{p_i}\prod_{i=1}^{k}\frac{p_i^{b_i-a_i+1}-1}{p_i-1} = \prod_{i=1}^{k}(p_i^{b_i} - p_i^{a_i-1}). \qquad (2.70)$$

Fix $\gamma \in \mathrm{Gal}(M/K)$.
Let $F = LM$ and find $\rho_\gamma \in \mathrm{Gal}(F/K)$ such that $\rho_\gamma|_M = \gamma$ and $\rho_\gamma|_L = \sigma$ and consider $E = F^{<\rho_\gamma>} = \{x \in F \mid \rho_\gamma(x) = x\}$.

$$\begin{tikzcd}
& F \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & E \arrow[d, dash] & M \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

Then we claim that F/E is a cyclotomic extension. Indeed, since

$$E \cap M = F^{<\rho_\gamma>} \cap M = M^{<\rho_\gamma>} = M^\gamma = K \tag{2.71}$$

and hence $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(F/E)$.
But

$$\mathrm{ord}(\gamma) = [F:E] = [F:ME][ME:E] = [F:ME][M:K] = [F:ME]\,\mathrm{ord}(\gamma). \tag{2.72}$$

Thus, $F = ME$.
As $K \subset M \subset K(\zeta) \Rightarrow KE \subset ME \subset K(\zeta)E \Rightarrow E \subset F \subset E(\zeta)$.
Thus, F/E is a cyclotomic extension.
Thus,

$$A_\gamma = \{\mathfrak{q} \in P(E) \mid [\frac{F/E}{\mathfrak{q}}] = \rho_\gamma\} \tag{2.73}$$

has a density by the CDT for cyclotomic extensions and $\delta(A_\gamma) = \frac{1}{[F:E]}$.
We also note that if $\gamma \neq \beta$, then $A_\gamma \cap A_\beta = \emptyset$.
We will show that primes in A_γ with non-trivial inertia do not count from a density perspective, they form a "thin" set.
Let $A'_\gamma = \{\mathfrak{q} \in A_\gamma \mid \mathfrak{p} := \mathfrak{q} \cap K$ is unramified for E/K and $N\mathfrak{p} = N\mathfrak{q}\}$.

$$\begin{aligned}\sum_{\mathfrak{q} \in A_\gamma \setminus A'_\gamma} (N\mathfrak{q})^{-s} &\leq \alpha + \sum_{\mathfrak{q} \in B} (N\mathfrak{q})^{-s} \\ &\leq \alpha + \sum_{\mathfrak{q} \in B, p \mid \mathfrak{q}} p^{-2s} \\ &\leq \alpha + [E:\mathbb{Q}] \sum_{p \in P(\mathbb{Q})} p^{-2} < \infty.\end{aligned} \tag{2.74}$$

In above inequalties α is the sum of all $N\mathfrak{q}^{-s}$ for which $\mathfrak{q} \cap K$ ramifies in E and there are finitely many such.
Let

$$B = \{\mathfrak{q} \in A_\gamma, \mathfrak{q} \cap K \text{is unramified and} N\mathfrak{q} > N(\mathfrak{q} \cap K)\}. \tag{2.75}$$

Thus, $\delta(A_\gamma) = \delta(A'_\gamma) + \delta(A_\gamma \setminus A'_\gamma) = \delta(A'_\gamma)$.

We know that

$$A'_\gamma = \{\mathfrak{q} \in P(E) \mid \mathfrak{p} := \mathfrak{q} \cap K \text{ is unramified for } E/K \text{ and } N\mathfrak{p} = N\mathfrak{q}, \left[\frac{F/E}{\mathfrak{q}}\right] = \rho_\gamma\}. \tag{2.76}$$

Let $B'_\gamma = \{\mathfrak{p} \in P(K) \mid \mathfrak{p} \text{ is unramified }, \left[\frac{F/K}{\mathfrak{p}}\right] = \rho_\gamma\}$.
Again, $B_\gamma \cap B_\beta = \emptyset$ whenever $\gamma \neq \beta$.
Consider the restriction map $res : A'_\gamma \to B'_\gamma$ which sends $\mathfrak{q} \to \mathfrak{q} \cap K$.
Since $\mathfrak{q} \cap K$ is unramified for E/K and $\mathfrak{q}$ is unramified for F/E, we have $\mathfrak{q} \cap K$ is unramified for F/K and since $N\mathfrak{q} = N(\mathfrak{q} \cap K)$, the Frobenius for F/E is also the Frobenius for F/K as the inertia of E/K is trivial and hence the residue fields are same.
Moreover, if $\mathfrak{p} \in B'_\gamma$, then there exists a prime $\mathfrak{b} \in P(L)$ lying above $\mathfrak{p}$ such that $[\frac{F/K}{\mathfrak{b}}] = \rho_\gamma$, then it is easy to see that $\mathfrak{b} \cap E \in A'_\gamma$.
We calculate the cardinality of the fibres in the above restriction map.
If $\mathfrak{p} \in B'_\gamma$, then it splits into r primes in E such that $ref = [E : K]$ but since $\mathfrak{p}$ is unramified we have $e = 1$. Thus, for each prime $\mathfrak{p}$ in B' there are exactly r primes lying above $\mathfrak{p}$ such that $\mathfrak{p}\mathcal{O}_E = \mathfrak{q}_1 \dots \mathfrak{q}_r$. Also, for each such $\mathfrak{q}_i$, we see that $[\frac{E/K}{\mathfrak{p}}] = [\frac{F/K}{\mathfrak{p}}]|_E = \rho_\gamma|_E = 1_E$ and hence $f = |D_{\mathfrak{q}_i}| = \text{ord}([\frac{E/K}{\mathfrak{p}}]) = 1$. Thus, $N\mathfrak{p} = N\mathfrak{q}$ for each $\mathfrak{q}$ which lies above $\mathfrak{p}$, we get that $f = 1$ and hence $r = [E : K]$.
Thus, $A'_\gamma = \coprod_{\mathfrak{p} \in B'_\gamma} A_\mathfrak{p}$ where $A_\mathfrak{p}$ contains $[E : K]$ primes which lie above $\mathfrak{p}$.
Pick a representative from each fibre and form the set D (which is bijective to B'_γ).

$$\sum_{\mathfrak{q} \in D} (N\mathfrak{q})^{-s} = \sum_{\mathfrak{q} \in D} (N(\mathfrak{q} \cap K))^{-s} = \sum_{\mathfrak{p} \in B'_\gamma} (N\mathfrak{p})^{-s}. \tag{2.77}$$

But $A'_\gamma = \bigcup_{\sigma \in \text{Gal}(E/K)} \sigma D$ and the union is disjoint. Thus,

$$\begin{aligned} \frac{1}{[F : E]} = \delta(A'_\gamma) = \sum_{\sigma \in \text{Gal}(E/K)} \delta(\sigma D) = [E : K]\delta(D) = [E : K]\delta(B'_\gamma) \\ \delta(B'_\gamma) = \frac{1}{[E : K][F : E]} = \frac{1}{[F : K]}. \end{aligned} \tag{2.78}$$

Now, consider

$$\begin{aligned}\delta(\cup_{\gamma\in T(M/K)}B'_\gamma) &= \sum_{\gamma\in T(M/K)}\delta(B'_\gamma)\\ &= \sum_{\gamma\in T(M/K)}\frac{1}{[F:K]}\\ &= |T(M/K)|[F:K]\\ &= \prod_{i=1}^{k}(p_i^{b_i}-p_i^{a_i-1})[F:K]\\ &= \frac{1}{[F:K]}[M:K]\prod_{i=1}^{k}(1-p_i^{a_i-1-b_i}).\end{aligned}\tag{2.79}$$

If $T=\{\mathfrak{p}\in P(K)\mid \frac{L/K}{\mathfrak{p}}=\sigma\}$, then since the restriction of a Frobenius is also a Frobenius, we get that $\bigcup_{\gamma\in T(M/K)}B'_\gamma\subset T$.
Thus,

$$\begin{aligned}\delta(T)\geq\delta(\cup_{\gamma\in T(M/K)}B'_\gamma)\geq\frac{1}{[F:K]}[M:K]\prod_{i=1}^{k}(1-p_i^{a_i-1-b_i})\\ =\frac{1}{[L:K][M:K]}[M:K]\prod_{i=1}^{k}(1-p_i^{a_i-1-b_i})\\ =\frac{1}{[L:K]}\prod_{i=1}^{k}(1-p_i^{a_i-1-b_i}).\end{aligned}\tag{2.80}$$

But as

$$m=|\,\mathrm{Gal}(M/K)\to\infty\Rightarrow(1-p_i^{a_i-1-b_i})\to 1.\tag{2.81}$$

Thus,

$$\delta(T)\geq\frac{1}{[L:K]}.\tag{2.82}$$

But since

$$\delta(\cup_{\sigma\in\mathrm{Gal}(L/K)}T_\sigma)=1,\tag{2.83}$$

we must have

$$\delta(T)=\frac{1}{[L:K]}.\tag{2.84}$$

Remark 2.2.2. This proof is not entirely correct as we have assumed $\delta(T)$ exists.

To do away with that, show that the equations above for $\delta(T)$ are valid for partial sums and take limit.

Thus, we have proved CDT for the abelian case.

2.3 Arbitrary extension

Now we will prove CDT for arbitrary Galois extensions.
Suppose L/K is a finite Galois extensions and $\mathcal{C} \subset \operatorname{Gal}(L/K)$ is a conjugacy class and $A = \{\mathfrak{p} \in P(K) \mid (\frac{L/K}{\mathfrak{p}}) = \mathcal{C}\}$.
Consider $\tau \in \mathcal{C}$, and look at $E := L^{<\tau>} = \{x \in L \mid \tau(x) = x\}$.

$$\begin{tikzcd} L \arrow[d, dash] \\ E \arrow[d, dash] \\ K \end{tikzcd}$$

Then L/E is an abelian (in fact cyclic) extension and hence we know that for

$$D' = \{\mathfrak{q} \in P(E) \mid [\frac{L/E}{\mathfrak{q}}] = \tau\}, \tag{2.85}$$

we have

$$\delta(D') = \frac{1}{[L:E]}. \tag{2.86}$$

For a prime Q above $\mathfrak{q} \in D'$, we have $ref = [L:E] = \operatorname{ord}(\tau)$. But $e = 1$ and $f = |D_Q| = |<\tau>| = \operatorname{ord}(\tau)$ and hence $r = 1$. Thus, there is a one to one correspondence between primes in L having τ as their Frobenius element and primes lying below such primes.
Consider the set

$$D = \{\mathfrak{q} \in D' \mid (\mathfrak{q} \cap K) \text{ unramified for} E/K, N\mathfrak{q} = N(\mathfrak{q} \cap K)\}. \tag{2.87}$$

Then, we claim that the set $D' \setminus D$ does not contribute to the density.

$$\begin{aligned}\sum_{\mathfrak{q}\in D'\setminus D} (N\mathfrak{q})^{-s} &\leq \sum_{\mathfrak{q}\in P(E), N(\mathfrak{q}\cap K)<N(\mathfrak{q})} (N\mathfrak{q})^{-s} \\ &\leq \sum_{\mathfrak{q}\in P(E), N(\mathfrak{q}\cap K)<N(\mathfrak{q})} (N(\mathfrak{q}\cap K))^{-s} \\ &\leq \sum_{\mathfrak{q}\in P(E), N(\mathfrak{q}\cap \mathbb{Q})<N(\mathfrak{q})} (N(\mathfrak{q}\cap \mathbb{Q}))^{-s} \\ &\leq \sum_{p\in P(\mathbb{Q})} \sum_{p|\mathfrak{q}, p^2\leq N(\mathfrak{q})} (N(\mathfrak{q}\cap \mathbb{Q}))^{-s} \\ &\leq [E:K] \sum_{p\in P(\mathbb{Q})} p^{-2} < \infty.\end{aligned} \tag{2.88}$$

Thus,

$$\delta(D') = \delta(D) = \frac{1}{[E:K]}. \tag{2.89}$$

Now, for the set

$$B = \{\mathfrak{p} \in P(K) \mid (\frac{L/K}{\mathfrak{p}}) = \mathcal{C}\}, \tag{2.90}$$

consider the restriction map $\theta : D \to B$.

Note that if τ is the Frobenius element over $\mathfrak{q} \in D$ for L/E, it is also the Frobenius element over $\mathfrak{q} \cap K$ of L/K, since residue of E/K is trivial for $\mathfrak{q} \in D$. Thus, the map θ makes sense.

Moreover, given $\mathfrak{p} \in B$, there exists $\mathfrak{b} \in P(L)$ such that $[\frac{L/K}{\mathfrak{b}}] = \tau$ and take $\mathfrak{q} := \mathfrak{b} \cap E$ and observe that $\mathfrak{q} \in D$ as restriction of a Frobenius is also a Frobenius and in this case $\tau|_E = 1$ which means that the inertia is one and $N\mathfrak{p} = N(\mathfrak{b} \cap E)$.

We compute the cardinality of the fibres in the above map.

If $\mathfrak{q}$ and $\mathfrak{t}$ are elements of D such that they lie over the same prime in B. Then find unique primes Q and T in $P(L)$ such that they lie over $\mathfrak{q}$ and $\mathfrak{t}$ respectively. Then their exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(Q) = T$ and

$$[\frac{L/K}{Q}] = \tau = [\frac{L/K}{T}] = [\frac{L/K}{\sigma(Q)}] = \sigma[\frac{L/K}{Q}]\sigma^{-1} \Rightarrow \sigma \in C_G(\tau), \tag{2.91}$$

where $G = \mathrm{Gal}(L/K)$.

The group $C_G(\tau)$ acts transitively on $\theta^{-1}(\mathfrak{p}) = \{\mathfrak{b} \in D, \mathfrak{p} \mid \mathfrak{b}\}$. Thus, the orbit size, the cardinality of $\theta^{-1}(\mathfrak{p})$, is $|\frac{C_G(\tau)}{D_\mathfrak{q}}| = \frac{|G|}{\mathrm{ord}(\tau)|\mathcal{C}|}$ where $\mathfrak{q}$ is any prime lying above $\mathfrak{p}$ with

τ as the Frobenius element.

Thus,

$$D = \coprod_{\mathfrak{p} \in B} \theta^{-1}(\mathfrak{p}). \tag{2.92}$$

Pick a representative from each fibre and call that set R. Then R is bijective to B and

$$\sum_{\mathfrak{q} \in R} (N\mathfrak{q})^{-s} = \sum_{\mathfrak{q} \in R} (N(\mathfrak{q} \cap K))^{-s} = \sum_{\mathfrak{p} \in B} (N\mathfrak{p})^{-s}. \tag{2.93}$$

Thus,

$$\begin{gathered} \frac{1}{\operatorname{ord}\tau} = \frac{1}{[E:K]} = \delta(D) = \frac{|G|}{\operatorname{ord}(\tau)|\mathcal{C}|}\delta(B) \\ \delta(B) = \frac{|\mathcal{C}|}{[L:K]}. \end{gathered} \tag{2.94}$$

Hence, we have proved CDT for an arbitrary Galois extension.

Now we will see some cool applications of the CDT.

Lemma 2.3.1. Suppose L/K is a finite Galois extension of number fields. Then there are infinitely many primes $\mathfrak{p} \in P(K)$ such that for any prime $\mathfrak{b}$ lying above $\mathfrak{p}$ we have $N\mathfrak{p} = N\mathfrak{b}$.

Proof. Consider

$$C = \{\mathfrak{p} \in P(K); [\frac{L/K}{\mathfrak{p}}] = 1\}. \tag{2.95}$$

Then $\delta(C) = \frac{1}{[L:K]}$. For any $\mathfrak{p} \in C, e_{\mathfrak{p}} f_{\mathfrak{p}} = D_{\mathfrak{b}} = 1$. Thus, $N\mathfrak{p} = N\mathfrak{b}$. Thus, there are infinitely many primes $\mathfrak{p} \in P(K)$ such that $N\mathfrak{p} = N\mathfrak{b}$ where $\mathfrak{b}$ is any prime lying above $\mathfrak{p}$. □

Lemma 2.3.2. Suppose L/K is a finite Galois extension of number fields and $\mathcal{C}$ a conjugacy class of $\mathrm{Gal}(L/K)$. Then there are infinitely many primes $\mathfrak{p} \in P(K)$ such that for any prime $N\mathfrak{p}$ is a prime number and $\frac{[L/K]}{\mathfrak{p}} = \mathcal{C}$.

Proof. For

$$A = \{\mathfrak{p} \in P(K); N\mathfrak{p} > p, \mathfrak{p} \mid p\}, \tag{2.96}$$

we have

$$\begin{aligned}\sum_{\mathfrak{p}\in A}(N\mathfrak{p})^{-x} &= \sum_{\mathfrak{p}\in A}(p^{f_\mathfrak{p}})^{-x}\\ &\leq \sum_{\mathfrak{p}\in A} p^{-2x}\\ &\leq \sum_{\mathfrak{p}\in P(K)} p^{-2x}\\ &\leq [L:\mathbb{Q}]\sum_{p\in P(\mathbb{Q})} p^{-2x}\\ &\leq [L:\mathbb{Q}]\sum_{p\in P(\mathbb{Q})} p^{-2} < \infty.\end{aligned} \tag{2.97}$$

Hence, $\delta(A) = 0$. For $\mathcal{C}$, any conjugacy class in $\mathrm{Gal}(L/K)$, and

$$C = \{\mathfrak{p} \in P(K); (\frac{L/K}{\mathfrak{p}}) = \mathcal{C}\}. \tag{2.98}$$

By CDT, we know that $\delta(C) = \frac{|\mathcal{C}|}{[L:K]}$.
But

$$\frac{|\mathcal{C}|}{[L:K]} = \delta(C) = \delta(C \cap A) + \delta(C \cap A^{\mathrm{c}}) = 0 + \delta(C \cap A^{\mathrm{c}}). \tag{2.99}$$

Thus, there are infinitely many primes $\mathfrak{p}$ such that there corresponding conjugacy class is $\mathcal{C}$ and $N\mathfrak{p} = p$. □

Lemma 2.3.3. Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $n > 1$. Then there are infinitely many primes p such that $\overline{f}$ has no root in $\mathbb{Z}/p\mathbb{Z}$.

Proof. Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ where α_i are distinct roots of $f(x)$ in $\mathbb{C}$. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on roots $\{\alpha_i\}$ and each permutation specifies the element of the Galois group uniquely.

Hence we may think of $\mathrm{Gal}(K/\mathbb{Q})$ as a subgroup of S_n. For $T_1 = \mathbb{Q}(\alpha_1)$ we see that $\mathrm{Gal}(K/T_1)$ is a proper subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ and its conjugates $\sigma\,\mathrm{Gal}(K/T_1)\sigma^{-1} = \mathrm{Gal}(K/T_i)$ where $\sigma(\alpha_1) = \alpha_i$. As a finite group cannot be written as union of conjugates of a proper subgroup, find $\sigma \notin \bigcup \mathrm{Gal}(K/T_i)$. By CDT, there are infinitely many primes $p \in \mathbb{Z}$ such that there exists a prime $\mathfrak{p}$ above p and $[\frac{K/\mathbb{Q}}{\mathfrak{p}}] = \sigma$. The cycle type of σ tells us the irreducible decomposition of $\overline{f}$ in the quotient field. For p as above, if there was a root of $\overline{f}$ in the residue field of p, then σ must fix a root of f i.e for some i we must have $\sigma(\alpha_i) = \alpha_i$, which implies $\sigma \in \mathrm{Gal}(K/T_i)$. This contradicts our choice of σ. □

Chapter 3

Chebotarev Density Theorem for Function Fields

In this chapter we formulate and give an elementary proof of the Chebotarev Density Theorem for function fields of one variable defined over finite fields.
We assume familiarity with Theory of function fields over one variable and Riemann hypothesis for finite fields. A good reference is [4] and we assume knowledge of Chapter 1,3,5.
Over function fields, role of primes is played by places and hence we will use the term prime/place interchangeably.
Let q be a power of a prime and K be function field of $\mathbb{F}_q$. Given a divisor $A \in \mathrm{Div}(K)$, we define $\mathcal{N}A = q^{\deg(A)}$. For a place P, this turns out to be $\mathcal{N}P = q^{\deg(P)}$ which is the cardinality of the residue field $\overline{K}_P = \mathcal{O}_P/P$.
A special consequence of Riemann hypothesis is the **Hasse-Weil bound** on the number of places of degree 1.

Theorem 3.0.4 (**Hasse-Weil bound**). Let F be a function field and $N(F)$ be the number of places $F/\mathbb{F}_q$ of degree 1 and g be the genus of the function field. Then

$$\left|N(F) - (q+1)\right| \leq 2gq^{1/2}. \tag{3.1}$$

Proof. Refer to Theorem 5.2.3 [4]. □

Suppose L/K is a Galois extension and $\mathbb{F}_{q^n}$ is the constant field inside L. By fixing an unramified place P in K, we know that the Frobenius elements living over

P form a conjugacy class $\mathcal{C}$ in $\mathrm{Gal}(L/K)$.

Let $\mathbb{P}(K)$ be the set of places in K and $A \subset P(K)$, we define

$$\delta(A) = \lim_{s \to 1^+} \frac{\sum_{P \in A} (\mathcal{N}P)^{-s}}{\sum_{P \in \mathbb{P}(K)} (\mathcal{N}P)^{-s}}, \tag{3.2}$$

whenever the limit exists.

Remark 3.0.5. 1. The convergence of numerator (a subseries of denominator) and denominator is seen as follows:

$$\begin{aligned}
\sum_{P \in \mathbb{P}(K)} (\mathcal{N}P)^{-s} &= \sum_{\mathfrak{p} \in \mathbb{P}(\mathbb{F}_q(t))} \sum_{P|\mathfrak{p}} (\mathcal{N}P)^{-s} \\
&= \sum_{\mathfrak{p} \in \mathbb{P}(\mathbb{F}_q(t))} \sum_{P|\mathfrak{p}} q^{-s\deg(P)} \\
&\leq \sum_{\mathfrak{p} \in \mathbb{P}(\mathbb{F}_q(t))} \sum_{P|\mathfrak{p}} q^{-s\deg(\mathfrak{p})} \\
&\leq [K : \mathbb{F}_q(t)] \sum_{\mathfrak{p} \in \mathbb{P}(\mathbb{F}_q(t))} q^{-s\deg(\mathfrak{p})} \\
&\leq [K : \mathbb{F}_q(t)] \sum_{\substack{f \in \mathbb{F}_q[t] \\ f \text{irreducible,monic}}} q^{-s\deg(f)} + [K : \mathbb{F}_q(t)] q^{-s} \\
&\leq [K : \mathbb{F}_q(t)] \sum_{\substack{f \in \mathbb{F}_q[t], \\ f \text{monic}}} q^{-s\deg(f)} + [K : \mathbb{F}_q(t)] q^{-s} \\
&\leq [K : \mathbb{F}_q(t)] \frac{1}{1 - q^{1-s}} + [K : \mathbb{F}_q(t)] q^{-s} < \infty.
\end{aligned} \tag{3.3}$$

2. We may assume that $K/\mathbb{F}_q(t)$ is a separable extension.

Theorem 3.0.6 (**Chebotarev Density Theorem**)**.** Let L/K be a finite Galois extension of function fields and $\mathcal{C}$ be a conjugacy class in $\mathrm{Gal}(L/K)$ and consider the set

$$A = \left\{ P \in \mathbb{P}(K) \mid \left(\frac{L/K}{P} \right) = \mathcal{C} \right\}. \tag{3.4}$$

Then $\delta(A)$ exists and equals $\frac{|\mathcal{C}|}{[L:K]}$.

We set up the notation as follows:

Let $\tau \in \mathrm{Gal}(L/K)$ and we assume the set up to be inside some algebraically closed field Ω.

$$\mathbb{P}'(K) = \{P \in \mathbb{P}(K) \mid P \text{is unramified below and above}\} \tag{3.5}$$

$$\mathbb{P}_k(K) = \{P \in \mathbb{P}(K) \mid \deg(P) = k\} \tag{3.6}$$

$$\mathbb{P}'_k(K) = \mathbb{P}'(K) \cap \mathbb{P}_k(K) \tag{3.7}$$

$$A_k(L/K, \mathcal{C}) = \{P \in \mathbb{P}'_k(K) \mid (\frac{L/K}{P}) = \mathcal{C}\} \tag{3.8}$$

$$B_k(L/K, \tau) = \{Q \in \mathbb{P}(L) \mid Q \cap K \in \mathbb{P}_k(K), [\frac{L/K}{Q}] = \tau\} \tag{3.9}$$

$$A' = \bigcup_{k=1}^{\infty} A_k(L/K, \mathcal{C}) \tag{3.10}$$

$$g_k = \text{genus of K} \tag{3.11}$$

$$\mathrm{Frob}_q = \text{ Frobenius endomorphism of} \, \mathrm{Gal}(\mathbb{F}_q) \tag{3.12}$$

We know that $\mathbb{P}'(K)$ is cofinite subset of $\mathbb{P}(K)$ and hence A' is a cofinite subset of A and it is enough to show that the density of A' is $\frac{|\mathcal{C}|}{[L:K]}$.

We introduce some new degrees as the following:

$$\begin{tikzcd}
 & & L \arrow[dl, dash, "m"'] \arrow[d, dash] \\
K \arrow[r, dash, "n"] \arrow[d, dash, "d"'] & K\mathbb{F}_{q^n} \arrow[d, dash] & \mathbb{F}_{q^n}(t) \arrow[dl, dash] \\
\mathbb{F}_q(t) \arrow[r, dash, "n"] & \mathbb{F}_{q^n}(t) &
\end{tikzcd}$$

Lemma 3.0.7. Let k be a positive integer and $P \in A_k(L/K, \mathcal{C})$ and $\tau \in \mathcal{C}$.

1. There are $\frac{[L:K]}{\mathrm{ord}(\tau)}$ places of $\mathbb{P}(L)$ living over P.

2. If $A_k \subset A_k(L/K, \mathcal{C})$ and $B_k(\tau) = \{Q \in B_k(L/K, \tau) \mid Q \cap K \in A_k\}$, then

$$|A_k| = \frac{|\mathcal{C}| \, \mathrm{ord}(\tau) |B_k(\tau)|}{[L : K]}. \tag{3.13}$$

Proof. 1. For Q any place above P, we know that $\operatorname{ord}(\tau) = |D_Q| = f_{Q/P}$. Since P is unramified $ref = [L : K]$ and $r = \frac{[L:K]}{\operatorname{ord}(\tau)}$.

2. We observe that $\sigma B_k(L/K, \tau) = B_k(L/K, \sigma\tau\sigma^{-1})$. Moreover, if $\tau_1 \neq \tau_2$, then

$$B_k(L/K, \tau_1) \cap B_k(L/K, \tau_2) = \emptyset \tag{3.14}$$

The same is true for $B_k(\tau)$, hence $|B_k(\tau)| = |B_k(\sigma\tau\sigma^{-1})|$. The restriction map

$$\bigcup_{\tau \in \mathcal{C}} B_k(\tau) \to A_k \tag{3.15}$$

$$Q \to Q \cap K \tag{3.16}$$

is surjective and each fibre has cardinality $\frac{[L:K]}{\operatorname{ord}(\tau)}$. Thus,

$$|\bigcup_{\tau \in \mathcal{C}} B_k(\tau)| = |A_k| \frac{[L : K]}{\operatorname{ord}(\tau)}, \tag{3.17}$$

$$|\mathcal{C}||B_k(\tau)| = |A_k| \frac{[L : K]}{\operatorname{ord}(\tau)}. \tag{3.18}$$

□

Lemma 3.0.8. Let $K \subset M \subset L$ and $\tau \in \operatorname{Gal}(L/M)$. Suppose $\mathbb{F}_{q^r}$ is the full constant field of M and $r \mid k$. Then

$$B_k(L/K, \tau) = B_{k/r}(L/M, \tau) \cap \{Q \in \mathbb{P}(L) \mid \deg(Q \cap K) = k\}. \tag{3.19}$$

Proof. We see that since $\tau \in \operatorname{Gal}(L/M)$, we have $\tau(x) = x$ for all $x \in \overline{K}_{P'}$ where $P' = Q \cap M$.

$$\begin{tikzcd}
& \overline{K}_Q \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{F}_{q^n} \arrow[d, dash] & \overline{K}_{P'} \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{F}_{q^r} \arrow[d, dash, "r"'] & \overline{K}_P \arrow[dl, dash, "k"'] \\
\mathbb{F}_q &
\end{tikzcd}$$

If $Q \in B_k(L/K, \tau)$, then $\tau(x) = x^{q^k} \forall x \in \overline{K}_Q$.
Since, $\overline{K}_{P'} \subset \overline{K}_Q$, $x^{q^k} = \tau(x) = x$.
Thus, $\overline{K}_{P'} \subset \mathbb{F}_{q^k}$.
Also, $\deg(Q \cap K) = k$, hence $\overline{K}_P = \mathbb{F}_{q^k}$.
But, $\mathbb{F}_{q^k} = \overline{K}_P \subset \overline{K}_{P'} \subset \mathbb{F}_{q^k}$.
Thus, $\mathbb{F}_{q^k} = \overline{K}_{P'} = \mathbb{F}_{q^{r \deg(P')}}$.
Hence, $\deg(P') = \frac{k}{r}$.

Thus, $Q \in B_{k/r}(L/M, \tau)$.

On the other hand, if $Q \in B_{k/r}(L/M, \tau) \cap \{Q \in \mathbb{P}(L) \mid \deg(Q \cap K) = k\}$, then $\deg(P') = \frac{k}{r}$, due to which $\overline{K}_P = \overline{K}_{P'}$ and hence $Q \in B_k(L/K, \tau)$.

□

Lemma 3.0.9. Let $K \subset M \subset L$ and $\tau \in \mathrm{Gal}(L/M)$. Suppose $\mathbb{F}_{q^r}$ is the full constant field of M and $r \mid k$. Suppose $\mathcal{C}$ and $\mathcal{C}'$ are the conjugacy classes of τ in $\mathrm{Gal}(L/K), \mathrm{Gal}(L/M)$, respectively. Then, consider the set

$$A'_{k/r} = A_{k/r}(L/M, \mathcal{C}') \setminus \{P' \in \mathbb{P}(M) \mid \deg(P' \cap K) \leq \frac{k}{2}.\} \tag{3.20}$$

Then we have

$$|A_k(L/K, \mathcal{C})| = \frac{|\mathcal{C}||A'_{k/r}|}{|\mathcal{C}'|[M:K]}. \tag{3.21}$$

Proof. Consider the set

$$B'_k(\tau) = B_{k/r}(L/M, \tau) \cap \{Q \in \mathbb{P}(L) \mid \deg(Q \cap K) = k\}. \tag{3.22}$$

Then, by Lemma(5.0.11)

$$B'_k(\tau) = B_k(L/K, \tau). \tag{3.23}$$

Also, places in L which lie over $A'_{k/r}$ and have τ as their Frobenius elements are precisely members of $B'_k(\tau)$. More precisely,

$$B'_k(\tau) = \{Q \in B_{k/r}(L/M, \tau) \mid Q \cap M \in A'_{k/r}\}. \tag{3.24}$$

Thus, we can use Lemma(5.0.10) to get

$$|A'_{k/r}| = \frac{|\mathcal{C}'| \operatorname{ord}(\tau) |B'_k(\tau)|}{[L : M]}, \tag{3.25}$$

$$|B'_k(\tau)| = |B_k(L/K, \tau)| = \frac{|A_k(L/K, \mathcal{C})| [L : K]}{|\mathcal{C}| \operatorname{ord}(\tau)}, \tag{3.26}$$

$$\text{Thus, } |A_k(L/K, \mathcal{C})| = \frac{|\mathcal{C}||A'_{k/r}}{|\mathcal{C}'|[M : K]}. \tag{3.27}$$

□

Theorem 3.0.10. Suppose L/K is Galois extension and $\mathbb{F}_{q^n}$ is the constant field of L. Let k be a positive integer such that

$$\tau|_{\mathbb{F}_{q^n}} = \operatorname{Frob}|_{\mathbb{F}_{q^n}}^k. \tag{3.28}$$

For $n' \in \mathbb{N}$ such that $n \mid n'$, we consider the constant field extension $L' = \mathbb{F}_{q^n} L$. Then, for each $\tau \in \mathcal{C}$, we can find a unique $\tau' \in \operatorname{Gal}(L'/K)$ such that $\tau'|_L = \tau$ and $\tau'|_{\mathbb{F}_{q^{n'}}} = \operatorname{Frob}|_{\mathbb{F}_{q^{n'}}}^k$.
Moreover,

1. $\mathcal{C}' = \{\tau' \mid \tau \in \mathcal{C}\}$ is a conjugacy class of $\operatorname{Gal}(L'/K)$
2. $\operatorname{ord}(\tau') = lcm(\operatorname{ord}(\tau), [\mathbb{F}_{q^{n'}} : \mathbb{F}_{q^{n'}} \cap \mathbb{F}_{q^k}])$
3. $A_k(L'/K, \mathcal{C}') = A_k(L/K, \mathcal{C})$

Proof. Let $n' = nt$. We first show how to extend τ to L'.

$$\begin{tikzcd}
& & L' \arrow[d, dash] \\
& L \arrow[ur, dash] \arrow[d, dash] & \mathbb{F}_{q^{n'}} \\
K \arrow[ur, dash] \arrow[d, dash] & \mathbb{F}_{q^n} \arrow[ur, dash] & \\
\mathbb{F}_q \arrow[ur, dash] & &
\end{tikzcd}$$

We know that $\langle \mathrm{Frob}\,|^{n}_{\mathbb{F}_{q^{n'}}} \rangle = \mathrm{Gal}(\mathbb{F}_{q^{n'}}/\mathbb{F}_{q^n}) \cong \mathrm{Gal}(L'/L) = \langle \phi \rangle$ where the isomorphism is given by the restriction map. Moreover, τ can be extended to $\overline{\tau} \in \mathrm{Gal}(L'/K)$ and all other extensions are related by elements of $\mathrm{Gal}(L'/L)$. More precisely,

$$\{\overline{\tau}\phi^i \mid 1 \leq i \leq t\} \tag{3.29}$$

are all the extensions of τ to L'. We need to pick the right one. Suppose

$$\overline{\tau}|_{\mathbb{F}_{q^{n'}}} = \mathrm{Frob}\,|^{l}_{\mathbb{F}_{q^{n'}}}. \tag{3.30}$$

But we also know that

$$\mathrm{Frob}\,|^{l}_{\mathbb{F}_{q^n}} = \overline{\tau}|_{\mathbb{F}_{q^n}} = \mathrm{Frob}\,|^{k}_{\mathbb{F}_{q^n}}. \tag{3.31}$$

Thus, we must have $k \equiv l \mod n$. Suppose $nr = l - k$ then

$$\overline{\tau}\phi^{-r}|_{\mathbb{F}_{q^{n'}}} = \overline{\tau}|_{\mathbb{F}_{q^{n'}}} \mathrm{Frob}\,|^{-nr}_{\mathbb{F}_{q^{n'}}} = \mathrm{Frob}\,|^{l}_{\mathbb{F}_{q^{n'}}} \mathrm{Frob}\,|^{-nr}_{\mathbb{F}_{q^{n'}}} = \mathrm{Frob}\,|^{l-nr}_{\mathbb{F}_{q^{n'}}} = \mathrm{Frob}\,|^{k}_{\mathbb{F}_{q^{n'}}}. \tag{3.32}$$

Hence choose $\tau' := \overline{\tau}\phi^{-r}$.
Moreover such a τ' is unique. Indeed, since $L' = \mathbb{F}_{q^{n'}}L$, any extension which agrees on $\mathbb{F}_{q^{n'}}$ and L, neccesarily agrees on L'.
Now we show other properties.

1. If τ_1' and τ_2' are extensions of τ_1, τ_2, respectively such that $\sigma\tau_1\sigma^{-1} = \tau_2$, then τ_2' and $\sigma'\tau_1'\sigma'^{-1}$ agree on L where σ' is any lift of σ. Also, τ_2' and $\sigma'\tau_1'\sigma'^{-1}$ agree on

$\mathbb{F}_{q^{n'}}$ since the $\mathrm{Gal}(\mathbb{F}_{q^{n'}}/\mathbb{F}_q)$ is abelian. Hence, by uniqueness $\tau_2' = \sigma'\tau_1'\sigma'^{-1}$.

$$\begin{tikzcd}
\mathbb{F}_{q^{n'}} \arrow[dr, dash] \arrow[drr, dash] & & & \mathbb{F}_{q^k} \arrow[dl, dash] \arrow[ddl, dash] \\
& \mathbb{F}_{q^n} \arrow[dr, dash] & \mathbb{F}_{q^{\gcd(n',k)}} \arrow[d, dash] & \\
& & \mathbb{F}_q &
\end{tikzcd}$$

2. $\mathrm{ord}(\tau') = lcm(\mathrm{ord}(\tau), \mathrm{ord}(\mathrm{Frob}\,|^k_{\mathbb{F}_{q^{n'}}}))$.
   But $\mathrm{ord}(\mathrm{Frob}\,|^k_{\mathbb{F}_{q^{n'}}}) = \frac{lcm(n',k)}{k}$.
   Thus, $\mathrm{ord}(\tau') = lcm(\mathrm{ord}(\tau), \frac{lcm(n',k)}{k}) = lcm(\mathrm{ord}(\tau), [\mathbb{F}_{q^{n'}} : \mathbb{F}_{q^{n'}} \cap \mathbb{F}_{q^k}])$.

3. $A_k(L'/K, \mathcal{C}') = A_k(L/K, \mathcal{C})$
   Fix a $\tau \in \mathcal{C}$. If $P \in A_k(L'/K, \mathcal{C}')$, then for some $Q \in \mathbb{P}(L')$, we have $[\frac{L'/K}{Q}] = \tau'$, thus restricting both sides to L, we get $[\frac{L/K}{Q \cap L}] = \tau$, and hence $P \in A_k(L/K, \mathcal{C})$. On the other hand, if $P \in A_k(L/K, \mathcal{C})$, then $[\frac{L/K}{Q}] = \tau$ and for Q' a lift of place Q in $\mathbb{P}(L')$, we have $\tau'|_{\overline{K}_Q}(x) = x^{q^k}$ and $\tau'|_{\mathbb{F}_{q^{n'}}}(x) = x^{q^k}$ and since $\overline{K}_{Q'} = \mathbb{F}_{q^{n'}}\overline{K}_Q$ we must have $\tau'(x) = x^{q^k}$ for all $x \in \overline{K}_{Q'}$. Thus, $[\frac{L'/K}{Q'}] = \tau'$ and hence $P \in A_k(L'/K, \mathcal{C}')$.

□

Corollary 3.0.11. Let $L = \mathbb{F}_{q^n}K$ and $\tau \in \mathrm{Gal}(L/K)$ such that

$$\tau|_{\mathbb{F}_{q^n}} = \mathrm{Frob}\,|^k_{\mathbb{F}_{q^n}} \tag{3.33}$$

then

$$A_k(K/K, \{1\}) = A_k(L/K, \{\tau\}). \tag{3.34}$$

Proof. We apply the above Theorem(3.0.10) to the set up where $L = K$ and $L' = \mathbb{F}_{q^n}K$. □

Theorem 3.0.12. Suppose $L = \mathbb{F}_{q^n}K$ and $\mathcal{C} = \{\tau\}$ and $\tau|_{\mathbb{F}_{q^n}} = \mathrm{Frob}\,|_{\mathbb{F}_{q^n}}$, then

$$\Big| |A_1(L/K, \mathcal{C})| - q \Big| < 2(g_L\sqrt{q} + g_L + d). \tag{3.35}$$

Proof. We observe that $A_1(L/K, \mathcal{C}) = \mathbb{P}'_1(K)$. Indeed, since L/K is a constant field extension, for any place $P \in \mathbb{P}(K)$ and Q a place above P in L, we have $\overline{K}_Q = \mathbb{F}_{q^n}\overline{K}_P$

$$\begin{tikzcd}
 & \overline{K}_Q \arrow[dd, no head] \\
\mathbb{F}_{q^n} \arrow[ur, no head] \arrow[dd, no head, "n"'] & \\
 & \overline{K}_P \\
\mathbb{F}_q \arrow[ur, no head, "1"] &
\end{tikzcd}$$

Thus, if P is a place in K and Q is any place in L lying over P, we have $\tau|_{\overline{K}_P}(x) = \tau|_{\mathbb{F}_q}(x) = x^q$ and $\tau|_{\mathbb{F}_{q^n}}(x) = x^q$. Thus, $\tau(x) = x^q$ for all $x \in \overline{K}_Q$ and hence $\tau = [\frac{L/K}{Q}]$. Consequently, $Q \in A_1(L/K, \mathcal{C})$.
Moreover, $\mathbb{P}_1(K) \setminus \mathbb{P}'_1(K)$ is the set of all primes of degree 1 ramified over $\mathbb{F}_q(t)$ as there is no ramification over a constant field extension. But, the set of ramified primes is precisely the support of the Different i.e $\mathrm{Diff}(K/\mathbb{F}_q(t))$.
Recalling Hurwitz genus formula,

$$2g_K - 2 = -2[K : \mathbb{F}_q(t)] + \deg(\mathrm{Diff}(K/\mathbb{F}_q(t))). \tag{3.36}$$

For our case the above equation can be re-written as

$$\deg(\mathrm{Diff}(K/\mathbb{F}_q(t))) = 2(g_K + d - 1). \tag{3.37}$$

By Hasse-Weil(3.0.4), we have a bound on places of degree 1 given by

$$|\mathbb{P}_1(K) - q - 1| < 2g_K\sqrt{q}. \tag{3.38}$$

Thus, we get $q-1-2g_K\sqrt{q} < |\mathbb{P}_1(K)| < q-1+2g_K\sqrt{q}$,
$q-1-2g_K\sqrt{q} < |\mathbb{P}_1(K)\cap \mathrm{Supp}(\mathrm{Diff}(K/\mathbb{F}_q(t)))| + |\mathbb{P}_1'(K)| < q-1+2g_K\sqrt{q}$,
But,
$q-1-2g_K\sqrt{q} < |\mathbb{P}_1(K)\cap \mathrm{Supp}(\mathrm{Diff}(K/\mathbb{F}_q(t)))| + |\mathbb{P}_1'(K)|$
$< \deg(\mathrm{Diff}(K/\mathbb{F}_q(t))) + |\mathbb{P}_1'(K)|$,
$q-1-2g_K\sqrt{q} < 2g_K+2d-2+|\mathbb{P}_1'(K)|$,
$q-2(g_K\sqrt{q}+g_K+d) < q+1-2g_K\sqrt{q}-2g_K-2d < |\mathbb{P}_1'(K)|$.

$$\text{Also } |\mathbb{P}_1'(K)| \le |\mathbb{P}_1(K)| < q-1+2g_K\sqrt{q} \le q+2g_K\sqrt{q}+2g_K+2d. \tag{3.39}$$

But since the genus does not change for constant field extensions, we have $g_K = g_L$ and hence we are done. □

Lemma 3.0.13. Let $[K':K]=km$ such that $\mathbb{F}_{q^k}\subset K'$.Then

$$|\{Q\in\mathbb{P}(K'); \deg(Q\cap K)\mid k; \deg(Q\cap K)\neq k\}| \le 2m(q^{k/2}+(2g_K+1)q^{k/4}). \tag{3.40}$$

Proof.

$$\{Q\in\mathbb{P}(K'); \deg(Q\cap K)\mid k; \deg(Q\cap K)\neq k\} = \{Q\in\mathbb{P}(K'); \deg(Q\cap K)\mid k; \deg(Q\cap K)\le \frac{k}{2}\}. \tag{3.41}$$

Note that equation is trivially true when $k=1$ so we may assume $k\ge 2$.
The main ingredient of this proof is Lemma(5.1.9) [4] which tells us the ramification of place in a constant field extension over a finite field.
For any $j|k$, we have $\mathbb{F}_{q^j}\subset\mathbb{F}_{q^k}$.

$$\begin{tikzcd}
& & & K' \arrow[dl, dash, "m"'] \arrow[d, dash] \\
& & K\mathbb{F}_{q^k} \arrow[dl, dash, "k/m"'] \arrow[d, dash] & \mathbb{F}_{q^k} \arrow[dl, dash] \\
& K\mathbb{F}_{q^j} \arrow[dl, dash, "j"'] \arrow[d, dash] & \mathbb{F}_{q^k} \arrow[dl, dash] & \\
K \arrow[d, dash] & \mathbb{F}_{q^j} \arrow[dl, dash] & & \\
\mathbb{F}_q & & &
\end{tikzcd}$$

If $P \in \mathbb{P}_j(K)$, then there are $\gcd(j,j) = j$ places lying above P in $\mathbb{P}(K\mathbb{F}_{q^j})$ and each of them has degree $j/j = 1$.
For any prime $P' \in \mathbb{P}(K\mathbb{F}_{q^j})$ lying above $P \in \mathbb{P}_j(K)$, remains prime of degree 1 in $\mathbb{P}(K\mathbb{F}_{q^k})$ since $\gcd(j,k) = j$ and there can be at most m lifts of P' in K'. Thus,

$$\begin{aligned}
&|\{Q \in \mathbb{P}(K'); \deg(Q \cap K) \mid k; \deg(Q \cap K) \leq \frac{k}{2}\}| \\
&\leq m|\{Q \in \mathbb{P}(K\mathbb{F}_{q^k}); \deg(Q \cap K) \mid k; \deg(Q \cap K) \leq \frac{k}{2}\}| \\
&\leq m|\bigcup_{j|k, j \leq k/2} \{Q \in \mathbb{P}(K\mathbb{F}_{q^k}); \deg(Q \cap K) = j\}| \\
&\leq m \sum_{j|k, j \leq k/2} |\{Q \in \mathbb{P}(K\mathbb{F}_{q^k}); \deg(Q \cap K) = j\}| \\
&\leq m \sum_{j|k, j \leq k/2} |\{Q \in \mathbb{P}(K\mathbb{F}_{q^j}); \deg(Q \cap K) = j\}| \\
&\leq m \sum_{j|k, j \leq k/2} |\mathbb{P}_1(K\mathbb{F}_{q^j})| \\
&\leq m \sum_{j|k, j \leq k/2} (q^j + 1 + 2g_K q^{j/2}).
\end{aligned} \tag{3.42}$$

The last inequality is a consequence of Theorem(3.0.4) applied to $K\mathbb{F}_{q^j}$.

$$\begin{aligned}\sum_{j|k,j\leq k/2}(q^j+1+2g_Kq^{j/2}) &\leq \sum_{j\leq k/2}q^j+\sum_{j\leq k/2}1+\sum_{j\leq k/2}2g_Kq^{j/2}) \\ &\leq 2q^{k/2}+k/2+4g_Kq^{k/4} \qquad (3.43)\\ &\leq 2q^{k/2}+2q^{k/4}+4g_Kq^{k/4} \\ &= 2(q^{k/2}+q^{k/4}(1+2g_K)).\end{aligned}$$

The last inequality follows from $\sum_{j\leq k/2}q^j\leq 2q^{k/2}$, $k/2\leq 2q^{k/4}$ and $\sum_{j\leq k/2}q^{j/2}\leq 2q^{k/4}$, all of which can be proved easily.

□

Theorem 3.0.14. Suppose L/K is finite Galois extension such that $m=[L:K\mathbb{F}_{q^n}]$ and $d=[K:\mathbb{F}_q(t)]$. Let $a\in\mathbb{N}$ such that

$$\tau|_{\mathbb{F}_{q^n}}=\mathrm{Frob}\,|^a_{\mathbb{F}_{q^n}}. \qquad (3.44)$$

for each $\tau\in\mathcal{C}$. For $k\in\mathbb{N}$, if $k\not\equiv a \mod n$, then $A_k(L/K,\mathcal{C})=\emptyset$, otherwise

$$\left||A_k(L/K,\mathcal{C})|-\frac{|\mathcal{C}|}{km}q^k\right|<\frac{2|\mathcal{C}|}{km}[(m+g_L)q^{k/2}+m(2g_K+1)q^{k/4}+g_L+dm]. \qquad (3.45)$$

Proof. If $P\in A_k(L/K,\mathcal{C})$, then there exists a place Q lying over P such that $[\frac{L/K}{Q}]=\tau$. But

$$\mathrm{Frob}\,|^a_{\mathbb{F}_{q^n}}=\tau|_{\mathbb{F}_{q^n}}=\mathrm{Frob}\,|^k_{\mathbb{F}_{q^n}}. \qquad (3.46)$$

Thus, $k\equiv a \mod n$.
Let $n'=n\,\mathrm{ord}(\tau)k$ and consider $L'=L\mathbb{F}_{q^{n'}}$.
Now suppose $k\equiv a \mod n$, then τ is an in Theorem(3.0.10). Extend τ to get τ' such that $\tau'|_L=\tau$ and $\tau'|_{\mathbb{F}_{q^{n'}}}=\mathrm{Frob}\,|^k_{\mathbb{F}_{q^{n'}}}$. Consider the subfield fixed field of τ' in L' and call it L_1 i.e $L_1=L'^{\langle\tau'\rangle}$.
We observe that $L_1\cap\mathbb{F}_{q^{n'}}=\mathbb{F}_{q^k}$ almost by definition and hence $\mathbb{F}_{q^k}$ is the full constant subfield of L_1. Moreover,

$$[L:L_1]=\mathrm{ord}(\tau')=lcm(\mathrm{ord}(\tau),\frac{n'}{k})=lcm(\mathrm{ord}(\tau),n\,\mathrm{ord}(\tau))=n\,\mathrm{ord}(\tau). \qquad (3.47)$$

Thus,

$$n\,\mathrm{ord}(\tau) = [L' : L_1] = [L' : L_1\mathbb{F}_{q^{n'}}][L_1\mathbb{F}_{q^{n'}} : L_1] = [L' : L_1\mathbb{F}_{q^{n'}}][\mathbb{F}_{q^{n'}} : \mathbb{F}_{q^k}] = [L' : L_1\mathbb{F}_{q^{n'}}]\frac{n'}{k}. \tag{3.48}$$

Thus, $L' = L_1\mathbb{F}_{q^{n'}}$. By Corollary 3.6.7 of [4], we get that $[L_1 : K\mathbb{F}_{q^k}] = [L' : K\mathbb{F}_{q^{n'}}]$. Also, by same Corollary, we get $[L' : K\mathbb{F}_{q^{n'}}] = [L : K\mathbb{F}_{q^n}]$. Thus, $[L_1 : K\mathbb{F}_{q^k}] = [L : K\mathbb{F}_{q^n}] = m$. Thus, $[L_1 : K] = km$.

Applying Lemma(3.0.9), where $M = L_1$ $\mathcal{C} := \mathcal{C}'$ is the conjugacy class of τ' and $\mathcal{C}' := \{\tau'\}$ and $r = k$, we get

$$|A_k(L'/K, \mathcal{C}')| = \frac{|\mathcal{C}'||A_1'|}{[L_1 : K]} = \frac{|\mathcal{C}||A_1'|}{[L_1 : K]}. \tag{3.49}$$

But

$$A_1' = A_1(L'/L_1, \{\tau'\}) \setminus \{P' \in \mathbb{P}(L_1) \mid \deg(P' \cap K) \leq \frac{k}{2}\}. \tag{3.50}$$

Since,

$$\begin{aligned} A_1(L'/L_1, \{\tau'\}) = (A_1(L'/L_1, \{\tau'\}) \setminus \{P' \in \mathbb{P}(L_1) \mid \deg(P' \cap K) \leq \frac{k}{2}\}) \bigcup \\ (A_1(L'/L_1, \{\tau'\}) \cap \{P' \in \mathbb{P}(L_1) \mid \deg(P' \cap K) \leq \frac{k}{2}\}). \end{aligned} \tag{3.51}$$

We get that

$$\begin{aligned} |A_1(L'/L_1, \{\tau'\})| = |A_1(L'/L_1, \{\tau'\}) \setminus \{P' \in \mathbb{P}(L_1) \mid \deg(P' \cap K) \leq \frac{k}{2}\}| \\ + |A_1(L'/L_1, \{\tau'\}) \cap \{P' \in \mathbb{P}(L_1) \mid \deg(P' \cap K) \leq \frac{k}{2}\}|. \end{aligned}$$

$$|A_1(L'/L_1, \{\tau'\})| \leq \frac{[L_1 : K]|A_k(L'/K, \mathcal{C}'|)}{|\mathcal{C}|} + \left|\{P' \in \mathbb{P}(L_1) \mid \deg(P' \cap K) \leq \frac{k}{2}; \deg(P' \cap K) = 1\}\right|.$$

$$\left|\frac{|\mathcal{C}|}{[L_1 : K]}|A_1(L'/L_1, \{\tau'\})| - |A_k(L'/K, \mathcal{C}')|\right| \leq$$
$$\frac{|\mathcal{C}|}{[L_1 : K]}\left|\{P' \in \mathbb{P}(L_1) \mid \deg(P' \cap K) \leq \frac{k}{2}; \deg(P' \cap K) = 1\}\right|.$$

But then we can apply Lemma(3.0.13) to get an upper bound of the set on right side.

Take $K' := L_1$, then we get

$$\begin{aligned}
&\frac{|\mathcal{C}|}{[L_1 : K]}\left|\{P' \in \mathbb{P}(L_1) \mid \deg(P' \cap K) \leq \frac{k}{2}; \deg(P' \cap K) = 1\}\right| \\
\leq &\frac{|\mathcal{C}|}{[L_1 : K]}\left|\{P' \in \mathbb{P}(L_1) \mid \deg(P' \cap K)\right| \leq \frac{k}{2}; \deg(P' \cap K) \mid k\}\right| \\
&\qquad \leq \frac{|\mathcal{C}|}{[L_1 : K]} 2m(q^{k/2} + (2g_K + 1)q^{k/4}) \\
&\qquad = \frac{2|\mathcal{C}|}{k}(q^{k/2} + (2g_K + 1)q^{k/4}).
\end{aligned} \tag{3.52}$$

By Theorem(3.0.12), where $K = L_1$ and $L = L'$, we get that

$$\left||A_1(L'/L_1, \{\tau'\})| - q^k\right| < 2(g_{L'}q^{k/2} + g_{L'} + dm). \tag{3.53}$$

Now, using both the above equations

$$\begin{aligned}
\left||A_k(L/K, \mathcal{C})| - \frac{|\mathcal{C}|}{km}q^k\right| &= \left||A_k(L'/K, \mathcal{C}')| - \frac{|\mathcal{C}|}{km}q^k\right| \\
&\leq \left||A_k(L'/K, \mathcal{C}')| - \frac{|\mathcal{C}|}{km}|A_1(L'/L_1, \{\tau'\})|\right| \\
&+ \left|\frac{|\mathcal{C}|}{km}|A_1(L'/L_1, \{\tau'\})| - \frac{|\mathcal{C}|}{km}q^k\right| \\
&\leq \frac{2|\mathcal{C}|}{k}(q^{k/2} + (2g_K + 1)q^{k/4}) \\
&+ \frac{|\mathcal{C}|}{km}2(g_{L'}q^{k/2} + g_{L'} + dm).
\end{aligned} \tag{3.54}$$

But $g_L = g_{L'}$ being a constant field extension.
Rearranging the right side gives us the proposition.

□

Lemma 3.0.15. Let $a, n \in \mathbb{N}$,then

$$\sum_{j=0}^{\infty} \frac{x^{a+jn}}{a + jn} = -\frac{1}{n}\log(1 - x) + O(1), \ x \to 1^-. \tag{3.55}$$

Proof. Consider ζ a primitive n^{th} root of unity. For $|x| < 1$, we have

$$\begin{aligned}
\sum_{i=0}^{n-1} \log(1-\zeta^i x)\zeta^{-ia} &= -\sum_{i=0}^{n-1}\Big(\sum_{k=0}^{\infty}\frac{\zeta^{ki}x^k}{k}\Big)\zeta^{-ia} \\
&= -\sum_{i=0}^{n-1}\Big(\sum_{k=0}^{\infty}\frac{\zeta^{(k-a)i}x^k}{k}\Big) \\
&= -\sum_{k=0}^{\infty}\Big(\sum_{i=0}^{n-1}\frac{\zeta^{(k-a)i}}{k}\Big)x^k \qquad (3.56)\\
&= -n\sum_{k\equiv a \mod n}\frac{x^k}{k} \\
&= -n\sum_{j=0}^{\infty}\frac{x^{a+jn}}{a+jn}.
\end{aligned}$$

But

$$\log(1-x) + n\sum_{j=0}^{\infty}\frac{x^{a+jn}}{a+jn} = -\sum_{i=1}^{n-1}\log(1-\zeta^i x)\zeta^{-ia}. \qquad (3.57)$$

But $\log(1-\zeta^i x)$ for $i \neq 0$ is holomorphic(at 1) and hence bounded close to 1.

□

Assuming the set up as in the beginning of the chapter we have the following theorem.

Theorem 3.0.16. Suppose L/K is finite Galois extension such that $m = [L : K\mathbb{F}_{q^n}]$ and $d = [K : \mathbb{F}_q(t)]$. If $a \in \mathbb{N}$ such that $a \leq n$ and

$$\tau|_{\mathbb{F}_{q^n}} = \text{Frob}\,|_{\mathbb{F}_{q^n}}^{a}, \qquad (3.58)$$

for each $\tau \in \mathcal{C}$. Then,

$$\sum_{P\in A}(\mathcal{N}P)^{-s} = -\frac{|\mathcal{C}|}{[L:K]}\log(1-q^{1-s}) + O(1),\ \ s \to 1^+. \qquad (3.59)$$

Proof. Since A' and A differ by only finitely many elements, equation about A' would imply the same equation about A. Moreover, $A_k(L/K, \mathcal{C}) = \emptyset$ whenever $k \not\equiv a$ mod n.

Now

$$\begin{aligned}\sum_{P\in A'}(\mathcal{N}P)^{-s} &= \sum_{k=0}^{\infty}\sum_{P\in A_k(L/K,\mathcal{C})}(\mathcal{N}P)^{-s}\\ &= \sum_{k=0}^{\infty}|A_k(L/K,\mathcal{C})|q^{-sk} \qquad (3.60)\\ &= \sum_{j=0}^{\infty}|A_{a+jn}(L/K,\mathcal{C})|q^{-s(a+jn)}.\end{aligned}$$

Moreover for $s \to 1^+$, we have $|q^{1-s}| < 1$ and hence we can use above Lemma3.0.15 Now

$$\begin{aligned}\Big|\sum_{P\in A'}(\mathcal{N}P)^{-s}+\frac{|\mathcal{C}|}{[L:k]}\log(1-q^{1-s})\Big| \leq \Big|\sum_{j=0}^{\infty}|A_{a+jn}(L/K,\mathcal{C})|q^{-s(a+jn)}-n\frac{|\mathcal{C}|}{[L:k]}\sum_{j=0}^{\infty}\frac{q^{(1-s)(a+jn)}}{a+jn}\Big|+\\ \frac{|\mathcal{C}|}{[L:k]}\Big|\log(1-q^{1-s})+n\sum_{j=0}^{\infty}\frac{q^{(1-s)(a+jn)}}{a+jn}\Big|. \qquad (3.61)\end{aligned}$$

Close to 1 and s such that $\Re(s) > 1$, we have $|q^{1-s}| < 1$ and hence by above Lemma3.0.15 the second term is bounded. Hence it is enough to show that the first term is bounded.

$$\begin{aligned}\Big|\sum_{j=0}^{\infty}|A_{a+jn}(L/K,\mathcal{C})|q^{-s(a+jn)}-n\frac{|\mathcal{C}|}{[L:k]}\sum_{j=0}^{\infty}\frac{q^{(1-s)(a+jn)}}{a+jn}\Big| =\\ \Big|\sum_{j=0}^{\infty}\Big(|A_{a+jn}(L/K,\mathcal{C})|-n\frac{|\mathcal{C}|}{[L:k](a+jn)}q^{(a+jn)}\Big)q^{-s(a+jn)}\Big| \leq \qquad (3.62)\\ \sum_{j=0}^{\infty}\Big|\Big(|A_{a+jn}(L/K,\mathcal{C})|-\frac{|\mathcal{C}|}{m(a+jn)}q^{(a+jn)}\Big)\Big||q^{-s(a+jn)}|.\end{aligned}$$

Using Theorem(3.0.14)

$$\begin{aligned}\sum_{j=0}^{\infty}\bigg|\bigg(|A_{a+jn}(L/K,\mathcal{C})| - \frac{|\mathcal{C}|}{m(a+jn)}q^{(a+jn)}\bigg)\bigg||q^{-s(a+jn)}| \\ \leq \sum_{j=0}^{\infty} c_1\bigg|\frac{q^{(1/2-s)(a+jn)}}{a+jn}\bigg| + \\ \sum_{j=0}^{\infty} c_2\bigg|\frac{q^{(1/4-s)(a+jn)}}{a+jn}\bigg| + \\ \sum_{j=0}^{\infty} c_3\bigg|\frac{q^{(-s)(a+jn)}}{a+jn}\bigg| \\ = -\bigg(\log(1-q^{1/4-x}) + \\ c_2\log(1-q^{1/2-x}) + \\ c_3\log(1-q^{-x})\bigg). \end{aligned} \tag{3.63}$$

where $x = \Re(s)$. But all the three terms are bounded as $s \to 1^+$. □

Corollary 3.0.17. If $L = K$,then

$$\sum_{P\in\mathbb{P}(K)} (\mathcal{N}P)^{-s} = -\log(1-q^{1-s}) + O(1),\ \ s \to 1^+. \tag{3.64}$$

Corollary 3.0.18.

$$\delta(A) = \lim_{s\to 1^+} \frac{\sum_{P\in A}(\mathcal{N}P)^{-s}}{-\log(1-q^{1-s})}. \tag{3.65}$$

Proof.

$$\begin{aligned}\left|\frac{\frac{\sum_{P\in A}(\mathcal{N}P)^{-s}}{-\log(1-q^{1-s})}}{\frac{\sum_{P\in A}(\mathcal{N}P)^{-s}}{\sum_{P\in\mathbb{P}(K)}(\mathcal{N}P)^{-s}}} - 1\right| &= \left|\frac{\sum_{P\in\mathbb{P}(K)}(\mathcal{N}P)^{-s}}{-\log(1-q^{1-s})} - 1\right| \\ &= \left|\frac{\sum_{P\in\mathbb{P}(K)}(\mathcal{N}P)^{-s} + \log(1-q^{1-s})}{-\log(1-q^{1-s})}\right|.\end{aligned} \tag{3.66}$$

As $s \to 1^+$ the numerator is bounded and denominator becomes arbitarily large. □

Theorem 3.0.19 (Chebotarev Density Theorem). Let L/K be a finite Galois extension of function fields and $\mathcal{C}$ be a conjugacy class in $\mathrm{Gal}(L/K)$ and consider the set

$$A = \left\{ P \in \mathbb{P}(K) \mid \left(\frac{L/K}{P} \right) = \mathcal{C} \right\}. \tag{3.67}$$

Then $\delta(A)$ exists and equals $\frac{|\mathcal{C}|}{[L:K]}$.

Proof.

$$\begin{aligned} &\left| \frac{\sum_{P \in A} (\mathcal{N}P)^{-s}}{-\log(1-q^{1-s})} - \frac{|\mathcal{C}|}{[L:K]} \right| \\ &\qquad \leq \frac{1}{[L:K]} \left| \frac{[L:K] \sum_{P \in A} (\mathcal{N}P)^{-s} + |\mathcal{C}| \log(1-q^{1-s})}{\log(1-q^{1-s})} \right| \\ &\qquad \leq \frac{|\sum_{P \in A} (\mathcal{N}P)^{-s} + \frac{|\mathcal{C}|}{[L:K]} \log(1-q^{1-s})|}{\log(1-q^{1-s})}. \end{aligned} \tag{3.68}$$

The numerator of the first term is bounded by the previous theorem and as $s \to 1^+$, the denominator increases arbitarily and hence we get

$$\delta(A) = \lim_{s \to 1^+} \frac{\sum_{P \in A} (\mathcal{N}P)^{-s}}{-\log(1-q^{1-s})} = \frac{|\mathcal{C}|}{[L:K]}. \tag{3.69}$$

□

Chapter 4

Nullstellensatz and Bertini-Noether Theorem

In this chapter we give a model theoretic proof of Hilbert's Nullstellensatz and a theorem of Bertini and Noether. We assume familiarity with Chapter 2 and Chapter 3 of [5]. We write ACF for the theory of algebraically closed fields.

4.1 Introduction

Theorem 4.1.1. Let $A = \{a_1, \ldots, a_n\}$ and $p \in \text{Prop}(A)$, then there exists $k \geq 1$ such that $\models p \leftrightarrow p_1 \vee \ldots \vee p_k$ where $p_i = a_1^{e_{i1}} \wedge \ldots \wedge a_n^{e_{ni}}$ where $e_{ij} \in \{1, -1\}$ where $a_i^{-1} := \neg a_i$.
This form of proposition p is known as **disjunctive normal form** or **DNF**.

Before proving the above we prove a lemma.

Lemma 4.1.2. Assuming the set up as in the above theorem. If p is in DNF, then so is $\neg p$.

Proof. Assuming p is a proposition in DNF i.e

$$\models p \leftrightarrow \vee_{i=1}^{k} p_i. \tag{4.1}$$

Then applying negation operation and de Morgan's law we get,

$$\models \neg p \leftrightarrow \neg(\vee_{i=1}^{k} p_i) \leftrightarrow \wedge_{i=1}^{k} \neg p_i. \tag{4.2}$$

But expanding out the proposition p we get,

$$\neg p_i = \neg(a_1^{e_{i1}} \wedge \ldots \wedge a_n^{e_{ni}}) \leftrightarrow \vee_{j=1}^{n}(a_j^{e'_{ij}}), \text{ where } e'_{ij} = -e_{ij}. \tag{4.3}$$

Thus we observe that,

$$\begin{aligned} \neg p &\leftrightarrow \neg(\vee_{i=1}^{k} p_i) \\ &\leftrightarrow \wedge_{i=1}^{k} \neg p_i \\ &\leftrightarrow \wedge_{i=1}^{k} \neg(a_1^{e_{i1}} \wedge \ldots \wedge a_n^{e_{ni}}) \\ &\leftrightarrow \wedge_{i=1}^{k}(\vee_{j=1}^{n}(a_j^{e'_{ij}})) \\ &\leftrightarrow \vee_{l=1}^{n^k}(\wedge_{i=1}^{k} b_{il}), \end{aligned} \tag{4.4}$$

$$\text{where } b_{il} \in \{a_j^{e'_{ij}}\}_{j=1}^{n}.$$

Now it is enough to show that $\wedge_{i=1}^{k} b_{il}$ can be brought into the form $a_1^{t_{i1}} \wedge \ldots \wedge a_n^{t_{in}}$ for suitable t_{ij}.
In order to do that we refer to the following procedure:

1. Eliminating the proposition containing both an atomic formula and its negation as it can never hold.

2. Removing an extra atomic formula if it occurs multiple times.

3. Whichever $a_i's$ do not occur we take all combinations of it and its negation.

For example if we have

$$a_1^1 \wedge a_1^{-1} \wedge a_n$$

we remove this as it can never hold and if we have

$$a_1^1 \wedge a_1 \wedge a_n$$

we take

$$\vee_{i\neq 1, i\neq n}(a_1 \wedge a_2^{e_2} \wedge \ldots \wedge a_i^{e_i} \wedge \ldots \wedge a_{n-1}^{e_{n-1}} \wedge a_n),$$

where $(e_2, \ldots, e_i, \ldots, e_n) \in [0,1]^{n-2}$.
Hence we get that the negation of a proposition in DNF is also in DNF. □

Proof. We prove the above by induction on length of proposition.
If $k = 1, p = a_i$ or $p = \top$ or $p = \bot$.

For $p = a_i$, let $p_j = a_1^{e_{j1}} \wedge a_{i-1}^{e_{j(i-1)}} \wedge a_i^1 \wedge a_{i+1}^{e_{j(i+1)}} \wedge \ldots a_n^{e_{jn}}$ where we take each of the 2^{n-1} possible such propositions and note that $\models a_i \leftrightarrow \vee_{i=1}^{2^{n-1}} p_i$.
For $p = \top$, take all possible 2^n propositions and observe that $\top \leftrightarrow \vee_{i=1}^{2^n} p_i$.
For $p = \bot$ then $p \leftrightarrow \neg\top$ and $\top$ is in DNF.
Assuming the induction hypothesis, p can be $q \wedge r$ or $q \vee r$ or $\neg q$ where q, r can be written in DNF.
If $p = q \vee r$, then it is obvious that p is also in DNF.
If $p = \neg q$, then we have done it above.
If $p = q \wedge r$, where $q \leftrightarrow \vee_{i=1}^m q_i$ and $r \leftrightarrow \vee_{j=1}^n r_j$, then

$$p \leftrightarrow (\vee_{i=1}^m q_i) \wedge (\vee_{j=1}^n r_j) \leftrightarrow \vee_{i,j} q_i \wedge r_j. \tag{4.5}$$

But $q_i \wedge r_j = (a_1^{e_1} \wedge \ldots \wedge a_n^{e_n}) \wedge (a_1^{f_1} \wedge \ldots \wedge a_n^{f_n})$. This can also be brought into the desired form by the same argument in the proof of converting $\neg p$ in DNF. □

Lemma 4.1.3. For every quantifier free formula ϕ we have a set of atomic formulas $A = \{\phi_1, \ldots, \phi_k\}$ such that $\phi \in \text{Prop}(A)$.

Proof. We induct on the number of connectives n in the formula ϕ.
If $n = 0$, then ϕ is an atomic formula and it is a proposition on itself. Assuming the induction hypothesis, if $\phi = \psi \wedge \theta$ or $\phi = \psi \vee \theta$ or $\phi = \neg\psi$ then these are propositions on atomic formulas. Note that we are done since ϕ cannot be of the form $\exists x \psi$ or $\forall x \psi$ as it is quantifier free. □

By Lemma 2.7.2 in [5], we have that if $p(\alpha_1, \ldots, \alpha_n) \in \text{Prop}(\{\alpha_1, \ldots, \alpha_n\})$ is a tautology then $p(\phi_1, \ldots, \phi_n)$ is valid in all L-structures $\mathcal{A}$ for any formulas $\phi_1, \ldots, \phi_n$. Thus, given any quantifier free formula ϕ, by the above lemma $\phi = p(\phi_1, \ldots, \phi_n) \in \text{Prop}(\phi_1, \ldots, \phi_n)$ where ϕ_i are atomic formulas. By Theorem(4.1.1), we have that $\models \phi \leftrightarrow p_1 \vee \ldots \vee p_k$ where $p_i = \phi_1^{e_{i1}} \wedge \ldots \wedge \phi_n^{e_{in}}$.
Thus, $\phi \leftrightarrow \vee_{i=1}^k p_i$ is valid in all L-structures $\mathcal{A}$ by Lemma 2.7.2.

4.2 Model completeness

Definition 4.2.1. Let $\mathcal{A}$ and $\mathcal{B}$ be two L-structures, and $h : A \to B$ be a set theoretic map between the underlying sets. We say h is an **embedding** if

(a) For each m-ary relation symbol R, $(a_1, \ldots, a_m) \in R^A \subset A^m \Leftrightarrow (ha_1, \ldots, ha_m) \in R^B \subset B^m$.

(b) For each m-ary function symbol f, we have $hf^A(a_1, \ldots, a_m) = f^B(ha_1, \ldots, ha_m)$.

(c) h is injective.

Lemma 4.2.1. For any term $t(x_1, \ldots, x_m)$ of the language, and any embedding $h : \mathcal{A} \to \mathcal{B}$ and $(a_1, \ldots, a_m) \in A^m$, we have $ht^A(a_1, \ldots, a_m) = t^B(ha_1, \ldots, ha_m)$.

Proof. Induct on the length of the term t. □

Definition 4.2.2. Given a theory Σ, we say that Σ is **model complete** if for every embedding $h : \mathcal{A} \to \mathcal{B}$ between models $\mathcal{A}, \mathcal{B}$ of Σ and given any formula $\phi(x_1, \ldots, x_m)$ and any collection $(a_1, \ldots, a_m) \in A^m$, we have

$$\mathcal{A} \models \phi(a_1, \ldots, a_m) \Leftrightarrow \mathcal{B} \models \phi(ha_1, \ldots, ha_m).$$

Let $L_{Ab} = (0, +, -)$ be the language of abelian groups and Σ be the theory of abelian groups. Then for models $\mathbb{Z}$ and $\mathbb{Q}$ and the natural injective map between them is an embedding as is easy to see, but for the formula $\phi(y) = \exists x(x + x = y)$ and $y = 3$, we have $\mathbb{Z} \not\models \phi(3)$ but $\mathbb{Q} \models \phi(3)$ for $x = 3/2$. Hence we see that the theory of abelian groups is not model complete.

Definition 4.2.3. Given a theory Σ, we say that Σ has **quantifier elimination** if for any formula $\phi(x_1, \ldots, x_m)$ there exists a quantifier free formula ϕ' such that $\Sigma \models \phi \leftrightarrow \phi'$.

Theorem 4.2.2. If Σ has quantifier elimination, then Σ is model complete.

Proof. Let $\mathcal{A}, \mathcal{B}$ be models of Σ, and h an embedding between them. Let $\phi(x_1, \ldots, x_m)$ be a formula and fix $(a_1, \ldots, a_m) \in A^m$, we need to show that

$$\mathcal{A} \models \phi(a_1, \ldots, a_m) \Leftrightarrow \mathcal{B} \models \phi(ha_1, \ldots, ha_m). \tag{4.6}$$

We will do this by induction on the number of connectives in ϕ.
If $n = 0$, then ϕ is an atomic formula,

Case 1: $\phi(x_1, \ldots, x_m) = Rt_1 \ldots t_k$

$$\begin{aligned} \mathcal{A} \models \phi(a_1, \ldots, a_m) &\iff (a_1, \ldots, a_m) \in R^A \\ \mathcal{B} \models \phi(ha_1, \ldots, ha_m) &\iff (ha_1, \ldots, ha_m) \in R^B. \end{aligned} \tag{4.7}$$

But the equations on RHS are equivalent by the definition of embedding.

Case 2: $\phi(x_1, \ldots, x_m) = (t_1(x_1, \ldots, x_m) = t_2(x_1, \ldots, x_m))$

$$\begin{aligned} \mathcal{A} \models \phi(a_1, \ldots, a_m) &\iff t_1^A(a_1, \ldots, a_m) = t_2^A(a_1, \ldots, a_m) \\ &\iff ht_1^A(a_1, \ldots, a_m) = ht_2^A(a_1, \ldots, a_m) \\ &\iff t_1^B(ha_1, \ldots, ha_m) = t_2^B(ha_1, \ldots, ha_m) \\ &\iff \mathcal{B} \models \phi(ha_1, \ldots, ha_m). \end{aligned} \tag{4.8}$$

Assuming the induction hypothesis,

(a) If $\phi = \psi \vee \theta$ then,

$$\begin{aligned} \mathcal{A} \models \phi(a_1, \ldots, a_m) &\iff \mathcal{A} \models \psi(a_1, \ldots, a_m) \; or \; \mathcal{A} \models \theta(a_1, \ldots, a_m) \\ &\iff \mathcal{B} \models \psi(ha_1, \ldots, ha_m) \; or \; \mathcal{B} \models \theta(ha_1, \ldots, ha_m) \\ &\iff \mathcal{B} \models \phi(ha_1, \ldots, ha_m). \end{aligned} \tag{4.9}$$

(b) If $\phi = \psi \wedge \theta$
Similar to (a)

(c) If $\phi = \neg\psi$,

$$\begin{aligned} \mathcal{A} \models \phi(a_1, \ldots, a_m) &\iff \mathcal{A} \not\models \psi(a_1, \ldots, a_m) \\ &\iff \mathcal{B} \not\models \psi(ha_1, \ldots, ha_m) \\ &\iff \mathcal{B} \models \phi(ha_1, \ldots, ha_m). \end{aligned} \tag{4.10}$$

(d) If $\phi = \exists x\psi$,
As Σ has quantifier elimination, there exists quantifier free ψ' equivalent to ψ.
Thus,

$$\begin{aligned} \Sigma \models \phi \leftrightarrow \exists x\psi' &\iff \mathcal{A} \models \phi(a_1, \ldots, a_m, x) \\ &\iff \mathcal{A} \models \psi(a_1, \ldots, a_m, b) \; for \; some \; b \in A \\ &\iff \mathcal{A} \models \psi'(a_1, \ldots, a_m, b). \end{aligned} \tag{4.11}$$

But ψ' being quantifier independent is a proposition on some atomic formulas, and we have already dealt with that case.

(d) Similarly for the case where $\phi = \forall x\psi$.
Note that we have used the fact that Σ has quantifier elimination in only the last two cases. □

4.3 Quantifier elimination

Lemma 4.3.1. If K is a model of ACF, and $p(x), q(x) \in K[x]$,then $p(x)$ divides $q(x)^{\deg p}$ iff every root of $p(x)$ is also a root of $q(x)$.

Proof. If $p|q^{\deg p}$ and $(x-\alpha)$ is a root of p, then $(x-\alpha)|p|q^{\deg p}$, thus $(x-\alpha)|q$ and is root of q.
If every root of p is also a root of q and let $p = \prod_{i=1}^{r}(x-\alpha_i)^{l_i}$, where$\alpha_i$ are distinct roots of multiplicity l_i.
Since $(x-\alpha_i)$ is a root of q, $(x-\alpha_i) \mid q \Rightarrow (x-\alpha_i)^{l_i}|q^{l_i} \mid q^n$, where $n = \deg p$.
Thus, $\prod_{i=1}^{r}(x-\alpha_i)^{l_i} \mid q^n \Rightarrow p \mid q^n$ □

Henceforth, R always stands for an integral domain. We will show that the theory of ACF is model complete but more can be said. We extend the language L_{Ring} to $L_{Ring}(R)$ where we include one constant for each element in R (elements of R become constants) and consider theory ACF(R) in which we include the following sentences:
(i) $a+b=c$ where $a, b, c \in R$ and the same relation holds in R
(ii) $a.b=c$ where $a, b, c \in R$ and the same relation holds in R
Then models of ACF(R) are algebraically closed fields which contain a homomorphic copy of R. Note that this is not same as ACF. If $R=\mathbb{Z}$, then models of ACF(R) are same as models of ACF. On the other hand if $R = \mathbb{Z}/p\mathbb{Z}$, then models of ACF(R) contain algebraically closed fields of characteristic p while those of char 0 are not models of ACF(R). Thus, we are clearly dealing with a more general situation. We will show that ACF(R) is model complete.

Theorem 4.3.2. ACF(R) has quantifier elimination. In particular, ACF(R) is model complete.

Proof. We want to show that given any $L_{Ring}(R)$-formula ϕ, we can find ϕ' which is quantifier free and $\Sigma \models \phi \leftrightarrow \phi'$. We will proof this by induction on the number of quantifiers in the formula ϕ.
If $n=0$, then ϕ is an atomic formula and is quantifier free.
Suppose $n=k\geq 1$, then ϕ can be one of the following:

(a) $\phi = \psi \wedge \theta$ and $\psi \leftrightarrow \psi'$ and $\theta \leftrightarrow \theta'$, where ψ' and θ' are quantifier free. Then $\phi \leftrightarrow \psi' \wedge \theta'$.

(b) $\phi = \psi \vee \theta$ and we have quantifier free ψ' and θ' as in the above case. Then $\phi \leftrightarrow \psi' \vee \theta'$.

(c) $\phi = \neg\psi$ and quantifier free ψ', then $\phi \leftrightarrow \neg\psi'$.

(d) $\phi = \exists x\psi$, where $\psi \leftrightarrow \psi'$ with ψ' quantifier free. Then $\phi \leftrightarrow \exists x\psi'$.
We have $\psi' \leftrightarrow p_1 \vee \ldots \vee p_k$ where $p_i = \phi_1^{e_{i1}} \wedge \ldots \wedge \phi_n^{e_{in}}$, where ϕ_i are atomic L-formulas. Thus, $\phi \leftrightarrow \exists x(p_1 \vee \ldots \vee p_k) \leftrightarrow \exists x p_1 \vee \ldots \exists x p_n$.
It is enough to show that each $\exists x p_i$ is equivalent to a quantifier free formula.
Let $p = p_i = \psi_1^{e_{i1}} \wedge \ldots \wedge \psi_n^{e_{in}}$ but we know that any atomic formula ψ in $L_{Ring}(R)$ is equivalent to $p(x_1, \ldots, x_l) = 0$ where $p(x_1, \ldots, x_l) \in R[x_1, \ldots, x_l]$. Consequently

$$\exists xp \leftrightarrow \exists x((\wedge_{i=1}^n p_i = 0) \wedge (\wedge_{j=1}^m q_j \neq 0)) \tag{4.12}$$

But $\wedge_{j=1}^m q_j \neq 0 \leftrightarrow q \neq 0$ where $q = \prod_{j=1}^m q_j$. Thus

$$\exists xp \leftrightarrow \exists x((\wedge_{i=1}^n p_i = 0) \wedge q \neq 0) \tag{4.13}$$

We may assume $p_i \in R[x_1, \ldots, x_l, x]$ for each p_i and if some p_j is independent of x, then

$$\exists x((\wedge_{i=1}^n p_i = 0) \wedge q \neq 0) \leftrightarrow p_j \wedge \exists x((\wedge_{i=1, i\neq j}^n p_i = 0) \wedge q \neq 0) \tag{4.14}$$

Thus it is enough to show that formula appearing on right side of above wedge is equivalent to a quantifier free forumla. In that sense, we may assume that each p_i is a polynomial in x. Suppose $\Sigma_{i=1}^n \deg_x(p_i)$.
Suppose,

$$\begin{aligned} p_1 &= a_{10} + \ldots + a_{1m_1}x^{m_1} \\ p_2 &= a_{20} + \ldots + a_{2m_2}x^{m_2}. \end{aligned} \tag{4.15}$$

We define

$$p_{1j} = a_{10} + \ldots + a_{1j}x^j \ for\ 1 \leq j \leq m_1. \tag{4.16}$$

WLOG we may assume $\deg_x(p_2) \geq \deg_x(p_1) \geq \deg(p_{1j}) \geq 1$.
We observe that

$$a_{1j}p_2 = a_{2m_2}x^{m_2-j}p_{1j} + (a_{1j}p_2 - a_{2m_2}x^{m_2-j}p_{1j}) = t_j(x)p_{1j}(x) + r_j(x), \tag{4.17}$$

where $\deg_x(r_j) < \deg_x(p_{1j})$.

We observe that in any model of ACF(R),

$$p_1 = 0 \wedge p_2 = 0 \leftrightarrow \vee_{j=1}^{m_1}(\wedge_{k>j} a_{1k} = 0 \wedge a_{1j} \neq 0 \wedge p_{1j} = 0 \wedge r_j = 0) \vee (\wedge_{j=0}^{m_1} a_{1j} = 0 \wedge p_2 = 0). \tag{4.18}$$

Thus, the equation (9) above can be simplied so as to reduce the degree by at least 1 Let

$$\begin{aligned} w_j &:= (\wedge_{k>j} a_{1k} = 0 \wedge a_{1j} \neq 0 \wedge p_{1j} = 0 \wedge r_j = 0) \\ w_0 &:= (\wedge_{j=0}^{m_1} a_{1j} = 0 \wedge p_2 = 0). \end{aligned} \tag{4.19}$$

$$\begin{aligned} \exists x((\wedge_{i=1}^{n} p_i = 0) \wedge q \neq 0) &\leftrightarrow \exists x((p_1 = 0 \wedge p_2 = 0) \wedge (\wedge_{j>2} p_j = 0 \wedge q \neq 0)) \\ &\leftrightarrow \exists x((\vee_j w_j = 0) \wedge (\wedge_{j>2} p_j = 0 \wedge q \neq 0)) \\ &\leftrightarrow \vee_j \exists x(w_j = 0 \wedge (\wedge_{j>2} p_j = 0) \wedge q \neq 0). \end{aligned} \tag{4.20}$$

Thus we see that we have reduced equation on the left to mutiple equations with fewer number of polynomials.

Hence we may assume that the problem is of the following kind.

$$\exists x(p = 0 \wedge q \neq 0). \tag{4.21}$$

Let

$$p = a_0 + \ldots + a_d x^d, \tag{4.22}$$

And define

$$\begin{aligned} p_j &= a_0 + \ldots + a_j x^j \ for\ 0 \leq j \leq d \\ a_j q^j &= h p_j + r_j \ where\ \deg_x(r_j) < \deg_x(p_j). \end{aligned} \tag{4.23}$$

For any ACF model $\mathcal{A}$ and $\vec{a} \in \mathcal{A}^l$,

1. If $p(\vec{a}, x) = 0$ then the validity of $\exists x(p(\vec{a}, x) = 0 \wedge q(\vec{a}, x) \neq 0)$ is equivalent to finding a non-root of $q(\vec{a}, x)$. This is always possible when $q(\vec{a}, x) \neq 0$ i.e some coefficient of $q(\vec{a}, x)$ is non-zero.

2. If $p(\vec{a}, x) \neq 0$ then there exists j such that some $a_j(\vec{a}) \neq 0$ and $a_k(\vec{a}) = 0$ for all $k > j$. We have $p(\vec{a}, x_0) = 0$ and $q(\vec{a}, x_0) \neq 0$ for some $x_0 \in \mathcal{A}$ iff $p(\vec{a}, x)$ does not divide $q(\vec{a}, x)^j$ iff $a_j(\vec{a}) \neq 0$ and $r_j(\vec{a}, y_0) \neq 0$ for some $y_0 \in \mathcal{A}$.
   Indeed, if $p(\vec{a}, x)$ does not divide $q(\vec{a}, x)^j$, then $p = p_j$ and $a_j(\vec{a}) \neq 0$ and

$r_j(\vec{a}, x_0) \neq 0$.
If $r_j(\vec{a}, y_0) \neq 0$ and $p_j \mid q^j$, then $p_j(\vec{a}, x)t(x) = q^j(\vec{a}, x)$. But then $a_j(\vec{a}, x)p_j(\vec{a}, x)t(x) = a_j(\vec{a})q^j(\vec{a}, x) = h(\vec{a}, x)p_j(\vec{a}, x) + r_j(\vec{a}, x)$. Thus, we get $p_j(\vec{a}, x)(a_j(\vec{a}, x)t(x) - h(\vec{a}, x)) = r_j(\vec{a}, x)$. By comparing the degrees w.r.t x on both sides we get that the equation in brackets must be zero, which forces $r_j(\vec{a}, x) = 0$ for all x. This is a contradiction.

Thus,

$$\begin{aligned}\exists x(p = 0 \wedge q \neq 0) \leftrightarrow \vee_{j=1}^{l}(a_l = 0 \wedge a_{l-1} = 0 \wedge \ldots \wedge a_{j+1} = 0 \wedge a_j \neq 0 \wedge \exists x r_j \neq 0)\\ \vee(a_0 = 0 \wedge a_1 = 0 \wedge \ldots \wedge a_{l-1} = 0 \wedge a_l = 0 \wedge (\vee_j q_j \neq 0))\end{aligned} \tag{4.24}$$

where q_j are coefficients of q.

Thus, we can reduce the case $\exists x(p = 0 \wedge q \neq 0)$ to a quantifier free formula.

(e) For $\phi = \forall x\psi$, we may assume that ψ is quantifier free.

$$\neg\forall x\psi \leftrightarrow \exists x\neg\psi \tag{4.25}$$

As the above equation is a tautology and since ψ is quantifier free, so is $\neg\psi$ and hence we can find by (d), a quantifier free formula θ such that

$$\exists x\neg\psi \leftrightarrow \theta. \tag{4.26}$$

Hence,

$$\begin{aligned}\forall x\psi &\leftrightarrow \neg\neg\forall x\psi\\ &\leftrightarrow \neg\theta.\end{aligned} \tag{4.27}$$

□

Corollary 4.3.3. Let R be an integral domain and θ be a sentence in $L_{Ring}(R)$, then there exists a constant $c \in R$ such that ACF$(R) \cup \{c \neq 0\} \models \theta$ or ACF$(R) \cup \{c \neq 0\} \models \neg\theta$.

Proof. A sentence does not contain any free variables but it might contain bound occurences of variables. But since ACF(R) has quantifier elimination we may assume that θ does not contain any variables and hence $\theta \leftrightarrow \vee_{j=1}^{m}((\wedge_{i=1}^{n} p_{ij} = 0) \wedge q_i \neq 0)$ where p_{ij} and q_i are constants in R(this is obvious from the above proof technique).

Let $c = \prod p_{ij} \prod q_i$ where $p_{ij}, q_i \in R$ are non-zero elements in R and if all of the them are zero take $c = 1$.
If θ holds in R then θ holds in $\tilde{K}$ where K is the fraction field of R. For any model $\mathcal{A}$ of ACF(R) in which $c \neq 0$, θ is valid in the homomorphic image $\overline{R}$ of R contained in $\mathcal{A}$ as the equation θ is imported as is in $\overline{R}$. Consequently $\mathcal{A} \vDash \theta$ and ACF$(R) \cup \{c \neq 0\} \vDash \theta$.
On the other hand, if θ is not valid in R, then it is not valid in $\tilde{K}$ and hence $\tilde{K} \vDash \neg\theta$. Since $\neg\theta$ is valid in R, then by above paragraph $\neg\theta$ is valid in all models $\mathcal{A}$ of ACF(R) for which $c \neq 0$ holds.

□

Theorem 4.3.4 (**Nullstellensatz).** Let k be a field, $\tilde{k}$ an algebraic closure of k and $p_1, \ldots, p_r$ a collection of polynomials in $k[x_1, \ldots, x_n]$. Suppose that the ideal $(p_1, \ldots, p_r)$ generated by them is a proper ideal in $k[x_1, \ldots, x_n]$, then there exists $\overline{a} = (a_1, \ldots, a_n) \in \mathbb{A}^n(\tilde{k})$ such that $p_i(\overline{a}) = 0$ for all $1 \leq i \leq r$.

Proof. Let $\phi = \exists x_1 \exists x_2 \ldots \exists x_n (\wedge_{i=1}^{r} p_i(x_1, \ldots, x_n) = 0)$ and $\mathfrak{m}$ be a maximal ideal containing $(p_1, \ldots, p_r)$ and denote $L = k[x_1, \ldots, x_n]/\mathfrak{m}$ and $\overline{L}$ be its algebraic closure, then we have an embedding $k \to k[x_1, \ldots, x_n] \to L \to \overline{L}$. But we know that $\tilde{k} \to \overline{L}$ is an embedding and $\overline{L} \models \phi(\overline{x})$. By model completeness of ACF, we have $\tilde{k} \models \phi$. □

We say that $f(x_1, x_2, \ldots, x_m) \in R[x_1, x_2, \ldots, x_m]$ is of degree d if the maximum total degree of monomials is d. We know that f is irreducible if it is not possible to write $f = gh$ where g and h are polynomials of degree strictly less than that of f.
For any polynomial $f(x_1, x_2, \ldots, x_m) \in R[x_1, x_2, \ldots, x_m]$, we can express the irreducibility of f as a sentence in $L_{Ring}(R)$.
Indeed, it is enough to produce a sentence which gives the reducibility of f. We know that f is reducible if there exist polynomials g, h of degree strictly less than that of f and $f = gh$. If f, g, h are as below:

$$f = \sum_{p=0}^{n} \left(\sum_{i_1 + \ldots + i_s = p} a_{i_1 \ldots i_s} X_1^{i_1} \ldots X_s^{i_s} \right). \tag{4.28}$$

$$g = \sum_{q=0}^{m} \left(\sum_{j_1 + \ldots + j_s = q} b_{j_1 \ldots j_s} X_1^{j_1} \ldots X_s^{j_s} \right). \tag{4.29}$$

$$h = \sum_{r=0}^{t} \left(\sum_{k_1 + \ldots + k_s = r} c_{k_1 \ldots k_s} X_1^{k_1} \ldots X_s^{k_s} \right). \tag{4.30}$$

And $f = gh$, then by comparing coefficients we infer that for each s-tuple $(i_1, \ldots, i_s)$ where $0 \leq i_u \leq p$ and $\sum_u i_u = p$, we must have

$$a_{i_1 \ldots i_s} = \sum b_{j_1 \ldots j_s} c_{k_1 \ldots k_s}, \tag{4.31}$$

where sum on the right side runs over all indices j_u for which $\sum_u j_u = q$ and k_w for which $\sum_w k_w = r$ and $q + r = p$ and $i_1 = j_1 + k_1, \ldots, i_s = j_s + k_s$.
This can be expressed as

$$f = gh \leftrightarrow \bigwedge_{0 \leq p \leq n} \bigwedge_{\{q,r \mid q+r=p, q \geq 0, r \geq 0\}} \left(\prod \exists b_{j_1 \ldots j_s} \prod \exists c_{k_1 \ldots k_s} \left(\sum b_{j_1 \ldots j_s} c_{k_1 \ldots k_s} = a_{i_1 \ldots i_s} \right) \right), \tag{4.32}$$

where $\prod \exists b_{j_1 \ldots j_s}$ and $\prod \exists c_{k_1 \ldots k_s}$ represents writing $\exists b_{j_1 \ldots j_s}$ and $\exists c_{k_1 \ldots k_s}$ for all indices $(j_1, \ldots, j_s)$ and $(k_1, \ldots, k_s)$ for which $j_1 + k_1 = i_1, j_2 + k_2 = i_2, \ldots, j_s + k_s = i_s$.

We take θ as the conjuction of above statement for g and h, where $(\deg(g), \deg(h)) \in \{(i,j) \in \mathbb{N} \times \mathbb{N} \mid i \geq 0, j \geq 0, i < n, i + j = n\}$. This gives a statement θ to express reducibility of f.

Definition 4.3.1. Let R be an integral domain, K its fraction field and suppose $f \in R[x_1, \ldots, x_n]$. Then f is called **absolutely irreducible** if f is irreducible as an element of $\tilde{K}[x_1, \ldots, x_n]$ where $\tilde{K}$ is an algebraic closure of K.

Theorem 4.3.5 (**Bertini-Noether**)**.** Assuming the notation as in the above definition let $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ be an absolutely irreducible polynomial. Then there exists a non-zero element $c \in R$ such that for any homomorphism of domains $\phi : R \to S$ for which $\phi(c) \neq 0$, $\phi(f)$ remains absolutely irreducible.

Proof. Let θ_1 be the statement that f is irreducible in R. Let $c \in R$ be as in the Lemma(4.3.3) for the sentence θ_1. Since $\tilde{K} \vDash \theta$ and $c \neq 0$ in $\tilde{K}$, by Lemma(4.3.3) we get $\mathrm{ACF}(R) \cup \{c \neq 0\} \vDash \theta_1$. Also, since $\phi(c) \neq 0$, we get that $\tilde{F}$, where F is the fraction field of S, is a model of $\mathrm{ACF}(R)$ and hence $\tilde{F} \vDash \theta_1$. This means that $\phi(f)$ is absolutely irreducible. □

Corollary 4.3.6. Let $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be an absolutely irreducible polynomial. Then there exists a non-zero integer c such that for all p which do not divide c, $f(x_1, \ldots, x_n)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x_1, \ldots, x_n]$

The above corollary can be stated in a more general context of global fields.

Theorem 4.3.7. Let $f_1, f_2, \ldots, f_r, g \in K[X_1, \ldots, X_n]$ and suppose g vanishes on on each point $\mathbf{a}$ of $\tilde{K}^n$ for which $f_1(\mathbf{a}) = \ldots = f_r(\mathbf{a}) = 0$. Then there exists $r \in \mathbb{N}$ such that $g^r \in (f_1, \ldots, f_r) \subset K[X_1, \ldots, X_n]$.

Proof. We may assume $g \neq 0$. Consider the ring $K[X_1, \ldots, X_n, Y]$ and the polynomial $h(\mathbf{X}, Y) = 1 - g(\mathbf{X})Y$. We observe that there is no point $(\mathbf{a}, b) \in \tilde{K}^{n+1}$ for which $f_1(\mathbf{a}) = \ldots = f_n(\mathbf{a}) = h(\mathbf{a}, b) = 0$.
Hence by (4.3.4) we must have that $(f_1, \ldots, f_n, h) = K[X_1, \ldots, X_n, Y]$.
Thus, we have a relation:

$$1 = \sum_{i=1}^{n} a_i(\mathbf{X}, Y) f_i(\mathbf{X}) + b(\mathbf{X}, Y) h(\mathbf{X}, Y)$$

Consider the ring $K[X_1, \ldots, X_n]_{(g)}$ which is $K[X_1, \ldots, X_n]$ localised at $S = \{g(\mathbf{X})^i \mid i \geq 0\}$. Now define the evaluation map $K[X_1, \ldots, X_n, Y] \to K[X_1, \ldots, X_n]_{(g)}$ sending $f(\mathbf{X}, Y)$ to $f(\mathbf{X}, g(X)^{-1})$.
Then under this map, above equation becomes:

$$1 = \sum_{i=1}^{n} a_i(\mathbf{X}, g(\mathbf{X})^{-1}) f_i(\mathbf{X}) \tag{4.33}$$

We can find $r \in \mathbb{N}$ large enough so that

$$g^r = \sum_{i=1}^{n} a_i'(\mathbf{X}) f_i(\mathbf{X}), \tag{4.34}$$

where $a_i'(\mathbf{X}) \in K[X_1, \ldots, X_n]$. Thus, the above relation also holds in $K[X_1, \ldots, X_n]$.

□

Chapter 5

Conjugate Lemma

For any ideal $I \subset K[X_1, \ldots, X_n]$, we associate a K-algebraic set $V(I)$ defined as

$$V(I) := \{\mathbf{a} \in \tilde{K}^n \mid f(\mathbf{a}) = 0 \ \forall \ f \in I\} \tag{5.1}$$

A subset V of $\tilde{K}^n$ is called K-defined if $V = V(I)$ for some ideal I in $K[X_1, \ldots, X_n]$. On the other hand, given a subset $A \subset \tilde{K}^n$ we define:

$$I(A) := \{f \in K[X_1, \ldots, X_n] \mid f(\mathbf{a}) = 0 \ \forall \mathbf{a} \in A\} \tag{5.2}$$

On the space $\tilde{K}^n$, the set $\{V(I)\}$ satisfy axioms of a closed sets and hence they form a topological space. We call the topology **Zariski K-topology**.

It is easy to see the following properties:

1. If $I \subset J$, then $V(J) \subset V(I)$.
2. $I(A)$ is a radical ideal.
3. $I(V(I)) = \sqrt{I}$ (by (4.3.7)).
4. $V(I(A)) = \overline{A}$ (by above)

We call a K-algebraic set V a K-variety if it is irreducible as a toplogical space. We observe that V is a K-variety iff $I(V)$ is a prime ideal.

We define the $\dim(V)$ as the dimension of it as a topological space. Closed irreducible subsets in V correspond to prime ideals in the coordinate ring $\Gamma(V) :=$

$K[X_1, \ldots, X_n]/I(V)$ and hence we get that $\dim(V) = \dim(\Gamma(V))$. If V is a variety then the coordinate ring is a domain and then we have that dimension of the coordinate ring is same as the transcendence degree of fraction field of $\Gamma(V)$ over K.
Any K-closed set V can be written as $V = \bigcup V_i$ where V_i are irreducible closed sets. Moreover, this decomposition is unique. It is easy to show that $\dim(V) = \max(\dim(V_i))$.

Lemma 5.0.8. If $V_1 \subset V_2$ are K-varieties of the same dimension, then $V_1 = V_2$.

Proof. For any chain of prime ideals in $\Gamma(V_2)$ can be pulled back to a chain in $K[X_1, \ldots, X_n]$, we know that dimension is bounded by n.
Let $\mathfrak{p}_1 := I(V_1)$ and $\mathfrak{p}_2 := I(V_2)$. Since $V_1 \subset V_2$, we have $\mathfrak{p}_2 \subset \mathfrak{p}_1$ and there is a canonical surjection

$$\phi : K[X_1, \ldots, X_n]/\mathfrak{p}_2 \twoheadrightarrow K[X_1, \ldots, X_n]/\mathfrak{p}_1 \tag{5.3}$$

We claim that the above canonical map is injective. Indeed, for any chain of prime ideals in $\Gamma(V_1)$;

$$(0) \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_t,$$

we get a chain in $\Gamma(V_2)$;

$$(0) \subset \phi^{-1}((0)) \subsetneq \phi^{-1}(\mathfrak{q}_1) \subsetneq \ldots \subsetneq \phi^{-1}(\mathfrak{q}_t)$$

But since $\phi^{-1}((0)) = \ker(\phi)$ is a prime ideal, the chain length increases by 1 if and only if the map is not injective. We know that $\dim(V_1) = \dim(V_2)$ and hence it is forced that ϕ is injective.
Thus, if $\mathfrak{p}_2 \subsetneq \mathfrak{p}_1$, then there exists $f \in \mathfrak{p}_1$ such that $f \notin \mathfrak{p}_2$. But then $\overline{f} \neq 0$ in $\Gamma(V_2)$ but $\phi(\overline{f}) = \overline{f} = 0$ in $\Gamma(V_1)$. This contradicts the fact that ϕ is an isomorphism. Hence $\mathfrak{p}_1 = \mathfrak{p}_2$, we have $V_1 = V(\mathfrak{p}_1) = V(\mathfrak{p}_2) = V_2$.

□

Lemma 5.0.9. If V and W are K-varieties such that $V \not\subseteq W$ and $W \not\subseteq V$. Then $\dim(V \cap W) < \min(\dim(V), \dim(W))$.

Proof. Suppose $\dim(V \cap W) = \dim(V)$. Decompose $V \cap W$ into irreducible components and let T be an irreducible component with maximum dimension. Then. $T \subset V \cap W \subset V$ and $\dim(T) = \dim(V)$.

By (5.0.8) we get that $T = V$. Thus $V = T \subset V \cap W \subset W$. This is a contradiction. $\square$

We denote $\mathrm{Gal}(\tilde{K}/K)$ as G. Given $\gamma \in G$ we get an K-linear bijection

$$\gamma' : \mathbb{A}^n(\tilde{K}) \to \mathbb{A}^n(\tilde{K}), \tag{5.4}$$

where $\gamma'((a_1, \ldots, a_n)) = (\gamma a_1, \ldots, \gamma a_n)$.
Moreover, for an ideal $I \subset \tilde{K}[x_1, \ldots, x_n], V(\gamma(I)) = \gamma'(V(I))$ we get that the map is continuous and closed. Thus a homeomorphism. Since the association between γ and γ' is unique we will refer to γ' as γ too.

Lemma 5.0.10. Let $K \subset L$ be a Galois extension with Galois group G and W be a G-stable L-subspace of L-space V. If $W^G = 0$ then $W = 0$.

Proof. Suppose $W \neq 0$, and let $\{e_i\}$ be an L-basis of W which we extend to a basis of V.Choose $u \in W$ such that it has minimum number of non-zero coefficients. Then, $u = \Sigma_{i=1}^{k} c_i e_i$ where $c_i \in L$ and $c_i \neq 0$ and we may assume $c_1 = 1$. But $gu = \Sigma_{i=1}^{k} g c_i e_i \Rightarrow u - gu = (1-g)c_2 e_2 + \ldots (1-g)c_n e_n$. By minimality, we get that $c_i = gc_i$ for all i and since g was arbitrary, $c_i \in K$. We thus get $u = gu$ for all g. Thus $u \in W^G = 0$. This is a contradiction.

$\square$

Lemma 5.0.11. If $K \subset L$ is a Galois extension of with Galois group G and J an ideal of $K[x_1, \ldots, x_n]$, then $(J^e)^G = J$ where J^e is the extension of the ideal in $L[x_1, \ldots, x_n]$.

Proof. It is easy to see that $J^e \cong J \otimes_K L$. Let $\{e_i\}$ be a K-basis of J, then $\{e_i \otimes 1\}$ is a L-basis of $J \otimes_K L$, and hence $\{e_i\}$ is an L-basis of J^e. It is obvious that $J \subset (J^e)^G$. If $u \in (J^e)^G$, then $u = \Sigma_{i=1}^{k} c_i e_i$ and $gu = \Sigma_{i=1}^{k} g c_i e_i$. But $gu = u \Rightarrow c_i = gc_i$ for all $g \in G$, then $c_i \in K$ and hence $u \in J$.

$\square$

Let V be a K-variety in $\mathbb{A}^n(\tilde{K})$. Suppose $V = \bigcup_{i=1}^{k} U_i$ is the decomposition of V into $\tilde{K}$-components i.e U_i are $\tilde{K}$-closed and irreducible subset in $\mathbb{A}^n(\tilde{K})$.
For V is invariant under the action of G, then $V = \gamma(V) = \gamma(\bigcup_{i=1}^{k} U_i) = \bigcup_{i=1}^{k} \gamma(U_i)$. By uniqueness of decomposition, we get that G acts on $\{U_i \mid 1 \leq i \leq k\}$ by permuting them.

Lemma 5.0.12. U_i as above are G conjugates i.e $V = \bigcup_{\gamma \in G} \gamma(U_1)$. In other words, the action is transitive.

Proof. We sketch the outline of the proof.

1. Write $V = W_1 \cup W_2 \cup \ldots \cup W_n$ where $W_i = \bigcup_{g \in G} gU_i$ and observe that each W_i is invariant under the G-action.

2. Observe that only finitely many unions appear in W_i as there are only finitely many $\tilde{K}$-irreducible components.

3. Now it is enough to show that each W_i is defined over K, as we know V is K-irreducible which will force $V = W_i$ for some i.

4. Fix a W_i and call it W. Since W is $\tilde{K}$-closed we get that $W = V(I)$ for some ideal $I \subset \tilde{K}[x_1, \ldots, x_n]$. We note that $V(gI) = gV(I) = gW = W = V(I)$. Thus, $gI = I$ and hence I is invariant under the action of the Galois group.

5. Let J be the complementary subspace of $I^c := I \cap K[x_1, \ldots, x_n]$ i.e
$$K[x_1, \ldots, x_n] = I^c \oplus J. \tag{5.5}$$
By Lemma(5.0.11) we have $(J^e)^G = J$. Thus,
$$\{0\} \subset (I \cap J^e)^G \subset I^G \cap (J^e)^G = I \cap J = \{0\} \tag{5.6}$$

6. By Lemma(5.0.10), $I \cap J^e = 0$.

7. Extending ideals in $\tilde{K}[x_1, \ldots, x_n]$, we see that
$$\tilde{K}[x_1, \ldots, x_n] = K[x_1, \ldots, x_n]^e = (I^c \oplus J)^e = (I^c)^e + J^e = (I^c)^e \oplus J^e. \tag{5.7}$$

8. But $I \cap J^e = 0$, which means that $I = \tilde{K}[x_1, \ldots, x_n](I \cap K[x_1, \ldots, x_n]) = (I^c)^e$.

9. Thus, $W = V(I) = V(\tilde{K}[x_1, \ldots, x_n](I \cap K[x_1, \ldots, x_n])) = V(I \cap K[x_1, \ldots, x_n])$ and is defined over K.

□

Chapter 6

Hilbert Irreducibility Theorem

In this chapter, we define what it means for a field to be Hilbertian. We prove that all global fields are Hilbertian.

6.1 Hilbertian fields

Let $f_1, f_2, \ldots, f_m \in K(T_1, \ldots, T_r)[X_1, \ldots, X_n]$ be a collection of irreducible polynomials and $g \in K[T_1, \ldots, T_r]$ is a non-zero polynomial, then define $H_r(f_1, \ldots, f_m; g)$ as the subset of $\mathbb{A}^r(K)$ for which $f_i(a_1, \ldots, a_r, X_1, \ldots, X_n)$ is defined and irreducible in $K[X_1, \ldots, X_n]$ and $g(a_1, \ldots, a_r) \neq 0$. $H_r(f_1, \ldots, f_m; g)$ is called a **Hilbert set** of $\mathbb{A}^r(K)$. If $n = 1$ and each f_i is separable in X, then call $H_r(f_1, \ldots, f_m; g)$ a **separable Hilbert set** of $\mathbb{A}^1(K)$.

A field K is called **Hilbertian** if every separable Hilbert set of $\mathbb{A}^r(K)$ is non-empty.

Lemma 6.1.1. Each separable Hilbert set $H(f_1, \ldots, f_m; g)$ contains $H(h_1, \ldots, h_m; g')$ where h_i is irreducible in $K[T_1, \ldots, T_r, X]$, separable in X and $h_i \notin K[T_1, \ldots, T_r]$.

Proof. Suppose

$$f_i = \sum_{j=0}^{n_j} \frac{a_j(\mathbf{T})}{b_j(\mathbf{T})} X^j,$$

where $\mathbf{T} = (T_1, \ldots, T_r)$. Multiply by $b_i(\mathbf{T}) = \prod_j b_j(\mathbf{T})$ on both sides to get

$$b(\mathbf{T}) f_i = \sum_{j=0}^{n_j} a_j(\mathbf{T}) X^j$$

Now let $d_i(\mathbf{T}) = \gcd(a_j(\mathbf{T}); 0 \leq j \leq n_j)$. Then

$$b(\mathbf{T})f_i = d_i(\mathbf{T}) \sum_{j=0}^{n_j} a'_j(\mathbf{T})X^j = d(\mathbf{T})h_i. \tag{6.1}$$

such that $h_i = \sum_{j=0}^{n_j} a'_j(\mathbf{T})X^j$ is primitive (has 1 as the gcd of coefficients)

Now it is easy to see that $\{h_i\}$ are irreducible polynomials in $K[T_1, \ldots, T_r, X]$. Take $g' = \prod_i b_i(\mathbf{T})d_i(\mathbf{T})g(\mathbf{T})$ and observe that $H(h_1, \ldots, h_m; g') \subset H(f_1, \ldots, f_m; g)$. Also, h_i are separable in X as root of f_i and h_i are same over $K(\mathbf{T})$ by equation 1. □

Before proving the next theorem we recall a lemma from Lang[3,9.1]

Lemma 6.1.2. Let K be a field and $n \geq 2, a \in K^*$. Suppose for all primes $p \mid n$, a does not have a p^{th} root in K and if $4 \mid n$, then $a \notin -4K^4$, then $X^n - a$ is irreducible in $K[X]$.

Theorem 6.1.3. Let $H = H_K(f_1, \ldots, f_m; g)$ be a Hilbert subset of $\mathbb{A}^r(K)$ with f_i irreducible in $K[T_1, \ldots, T_r, X]$ and $\deg_X(f_i) \geq 1$. Then H contains a Hilbert set of the form $H(h_1, \ldots, h_m)$ in which h_i are monic, irreducible polynomials in $K[T_1, \ldots, T_r, X]$ such that $\deg_X(h_i) \geq 2$.
Moreover, if f_i are separable then so is h_i.

Proof. Let $c_i(\mathbf{T})$ be the leading coefficients of f_i as polynomial over X and $n_i = \deg_X(f_i)$. Consider $q(\mathbf{T}) = \prod_i c_i(\mathbf{T})g(\mathbf{T})$.

If $\deg_{T_i}(q) = 0$ for all i, then $c_i \in K^*$ and $g \in K^*$. Then $H_K(f_1, \ldots, f_m; g) = H_K(f_1, \ldots, f_m)$. Since $c_i \in K^*$, we may assume f_i are monic. Moreover, if for some i, we have $\deg_X(f_i) = 1$, then $f_i = X - a_i(\mathbf{T})$ for some $a_i \in K[\mathbf{T}]$, then it is also true that $H_K(f_1, \ldots, f_m) = H_K(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m)$. Hence by this reduction, we may assume all $\deg_X(f_i) \geq 2$ for all i and f_i are monic, irreducible polynomials. Take $h_i = f_i$

On the other hand, if $\deg_{T_i}(q) \geq 1$ for some i, then take b, a prime such that $b > \deg_{T_i}(q)$ and note that $X^b - q(T)$ has no solution in $K[\mathbf{T}]$. Indeed, if for some $p(\mathbf{T}) \in K[\mathbf{T}]$, we have $p(\mathbf{T})^b = q(\mathbf{T})$. But then, $\deg_{T_i}(p(\mathbf{T})^b) = b \deg_{T_i}(p(\mathbf{T})) = \deg_{T_i}(q(\mathbf{T}))$, which implies $b \leq \deg_{T_i}(q(\mathbf{T}))$. Thus, from above lemma we get that

$X^b - q(T)$ is irreducible in $K[T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_r][T_i]$ but being monic it is irreducible in $K[\mathbf{T}]$.

Now for $\deg_X(f_i) = 1$, take $h_i = X^b - q(\mathbf{T})$ and for $\deg_X(f_i) \geq 2$, take

$$h_i = q(\mathbf{T})^{n_i} c_i(\mathbf{T})^{-1} f_i(\mathbf{T}, q(\mathbf{T})^{-1}X). \tag{6.2}$$

Then, by expanding out h_i, it is easy to see that h_i is monic. Moreover, if $h_i = a(\mathbf{T}, X)b(\mathbf{T}, X)$ then

$$\frac{c_i(\mathbf{T})}{q(\mathbf{T})^{n_i}} a(\mathbf{T}, q(\mathbf{T})X) b(\mathbf{T}, q(\mathbf{T})X) = f_i(\mathbf{T}, X)$$

It is evident that $\deg_X(a(\mathbf{T}, q(\mathbf{T})X)) = \deg_X(a(\mathbf{T}, X))$.

By comparing above equation, we get that WLOG $\deg_X(a(\mathbf{T}, q(\mathbf{T})X)) \geq 1$. If $\deg_X(a(\mathbf{T}, q(\mathbf{T})X)) < n_i$, then $\deg_X(b(\mathbf{T}, q(\mathbf{T})X)) \geq 1$ which would imply a non-trivial factorization of f in the polynomial ring $K(\mathbf{T})[X]$ which can be brought to a non-trivial facotrization in $K[\mathbf{T}][X]$ by Gauss Lemma. This contradicts irreducibility of f. Thus h_i is irreducible.

Now we see that $H(h_1, \ldots, h_m) \subset H(f_1, \ldots, f_m; g)$.

Suppose $\mathbf{a} \in H(h_1, \ldots, h_m)$, then

If $n_i = 1$, then $X^b - q(\mathbf{a})$ is irreducible, then $q(\mathbf{a}) \neq 0$. As a result $c_i(\mathbf{a}) \neq 0$ and $f_i = c_i(\mathbf{a})X - d$ is irreducible.

If $n_i \geq 2$, then

$$h_i(\mathbf{a}, X) = q(\mathbf{a})^{n_i} c_i(\mathbf{a})^{-1} f_i(\mathbf{a}, q(\mathbf{a})^{-1}X)$$

then $q(\mathbf{a}) \neq 0, c_i(\mathbf{a}) \neq 0$ and $f_i(\mathbf{a}, q(\mathbf{a})^{-1}X)$ is defined and irreducible.

In either case, $q(\mathbf{a}) \neq 0$ and hence $g(\mathbf{a}) \neq 0$.

The claim about separability is obvious from equation (2). □

Lemma 6.1.4. Let H be a separable Hilbert set in $\mathbb{A}^r(K)$, then there exists an irreducible polynomial $f \in K[T_1, \ldots, T_r, X]$ such that $H(f) \subset H$, where f is monic, separable in X and $\deg_X(f) \geq 2$.

Proof. By lemma 1, we may assume that $H = H(f_1, \ldots, f_k; g)$ where $f_i \in K[T_1, \ldots, T_r, X]$ is irreducible,separable in X and $f_i \notin K[T_1, \ldots, T_r]$ and $g \neq 0$. Let $r_i(\mathbf{T})$ be the leading term of f_i as polynomial over X.

Let x_i be roots of f_i as polynomial in $K(\mathbf{T})[X]$ and consider $L' = K(\mathbf{T})(x_1, \ldots, x_k)$. If $\deg_X(f_i) = 1$ for all $i \in \{1, \ldots, k\}$, then $[L' : K] = 1$. Then choose a prime

$l \neq char(K)$, and consider $L := K(\mathbf{T})(T_1^{1/l})$, then $[L : K] > 1$ and is a separable extension.

Otherwise $[L' : K] > 1$ and let $L := L'$. Since $L/K(\mathbf{T})$ is a finite separable extension,we may assume $L = K(\mathbf{T})(z)$ for some z separable and integral over $K[\mathbf{T}]$. Let $h \in K[\mathbf{T}, X]$ be the monic, irreducible polynomial for which $h(z) = 0$.

Since $K(\mathbf{T})(z) = K(\mathbf{T})[z]$, we may write $x_i = \sum_{j=0}^{n_i} \frac{a_{ij}(\mathbf{T})}{b_{ij}(\mathbf{T})} z^j = \frac{p_i(\mathbf{T},z)}{p_0(\mathbf{T})}$.

Let $h_i \in K(\mathbf{T})[x_i][X]$ be the monic, irreducible polynomial such that $h_i(z) = 0$. We note that h_i is separable in X. Then $h_i = q_i(\mathbf{T})g_i$ where $g_i \in K[\mathbf{T}, x_i, X]$ and $q_i(\mathbf{T}) \neq 0$.

Now let $b = g(\mathbf{T}) \prod q_i(\mathbf{T}) p_0(\mathbf{T}) \prod_i r_i(\mathbf{T})$ and we observe that $\deg_X(f_i) = \deg_X(f_i(\mathbf{a}, X))$ and $\deg_X(h) = \deg_X h(\mathbf{a}, X)$.

Now we prove that $H(h; b) \subset H(f_1, \ldots, f_k; g)$.

Suppose $\mathbf{a} \in H(h; b)$ and suppose $c \in \tilde{K}$ is a root of $h(\mathbf{a}, X)$. Let $\phi : K[\mathbf{T}] \to K(\mathbf{a})$ be the evaluation map i.e $\phi(T_i) = a_i$. By (**??**) extend ϕ to a place $\phi : K(\mathbf{T}) \to K(\mathbf{a}) \cup \{\infty\}$. By (4.1) we can extend this place, also denoted by ϕ, from $K(\mathbf{T})(z)$ where $\phi(z) = c$.

$$\begin{tikzcd}
K(\mathbf{T})(z) \arrow[r] \arrow[d, dash] & K(\mathbf{a})(c) \cup \{\infty\} \arrow[d, dash] \\
K(\mathbf{T}) \arrow[r] & K(\mathbf{a}) \cup \{\infty\}
\end{tikzcd}$$

Thus, $\phi(f(\mathbf{T}, X)) = f(\mathbf{a}, X)$ and hence $\frac{p_i(\mathbf{a},c)}{p_0(\mathbf{a})}$ is a root of $f(\mathbf{a}, X)$.

$[K(c) : K] = \deg_X(h) = [K(\mathbf{T})(z) : K(\mathbf{T})]$. Moreover, $[K(\frac{p_i(\mathbf{a},c)}{p_0(\mathbf{a})}) : K] \leq \deg_X(f_i)$ and $[K(c) : K(\frac{p_i(\mathbf{a},c)}{p_0(\mathbf{a})})] \leq \deg_X(h_i)$.

We infer that above inequalities are actually equalities and hence $f_i(\mathbf{a}, X)$ is irreducible.

Now, use above lemma to eliminate b.

□

Given $f_1, \dots, f_n \in K[T, X]$ be irreducible elements such that $\deg_X(f_i) \geq 2$, f_i is separable in X and $g \in K[T]$ be a non zero polynomial. Then define

$$G(f_1, \dots, f_n; g) = \{a \in K \mid \prod_i f_i(a, b) \neq 0 \ \forall\ b \in K, g(a) \neq 0\}.$$

Theorem 6.1.5. Let $G := G(f_1, \dots, f_m; g)$ be a subset of $\mathbb{A}^r(K)$ with f_i absolutely irreducible in $K[T_1, \dots, T_r, X]$, $\deg_X(f_i) \geq 2$ and separable in X. Then G contains a set of the form $G(h_1, \dots, h_m)$ in which h_i are monic, absolutely irreducible polynomials in $K[T_1, \dots, T_r, X]$ such that $\deg_X(h_i) \geq 2$ and h_i separable in X.

Proof. Let $c_i(\mathbf{T})$ be the leading coefficients of f_i as polynomial over X and $n_i = \deg_X(f_i)$. Consider $q(\mathbf{T}) = \prod_i c_i(\mathbf{T}) g(\mathbf{T})$.

We give a prescription for h_i as follows:

$$h_i = q(\mathbf{T})^{n_i} c_i(\mathbf{T})^{-1} f_i(\mathbf{T}, q(\mathbf{T})^{-1} X). \tag{6.3}$$

Then, by expanding out h_i, it is easy to see that h_i is monic. Moreover, if $h_i = a(\mathbf{T}, X) b(\mathbf{T}, X)$ with constant from $\tilde{K}$ then

$$\frac{c_i(\mathbf{T})}{q(\mathbf{T})^{n_i}} a(\mathbf{T}, q(\mathbf{T})X) b(\mathbf{T}, q(\mathbf{T})X) = f_i(\mathbf{T}, X)$$

It is evident that $\deg_X(a(\mathbf{T}, q(\mathbf{T})X)) = \deg_X(a(\mathbf{T}, X))$.
By comparing above equation, we get that WLOG $\deg_X(a(\mathbf{T}, q(\mathbf{T})X)) \geq 1$. If $\deg_X(a(\mathbf{T}, q(\mathbf{T})X)) < n_i$, then $\deg_X(b(\mathbf{T}, q(\mathbf{T})X)) \geq 1$ which would imply a non-trivial factorization of f in the polynomial ring $K(\mathbf{T})[X]$ which can be brought to a non-trivial facotrization in $\tilde{K}[\mathbf{T}][X]$ by Gauss Lemma. This contradicts absolute irreducibility of f_i. Thus h_i is absolutely irreducible.
Now we see that $G(h_1, \dots, h_m) \subset G(f_1, \dots, f_m; g)$.
Suppose $\mathbf{a} \in G(h_1, \dots, h_m)$, then

$$q(\mathbf{a})^{n_i} c_i(\mathbf{a})^{-1} f_i(\mathbf{a}, q(\mathbf{a})^{-1} b) = h_i(\mathbf{a}, b) \neq 0$$

then $q(\mathbf{a}) \neq 0, c_i(\mathbf{a}) \neq 0$ and $f_i(\mathbf{a}, q(\mathbf{a})^{-1} b) \neq 0$
In either case, $q(\mathbf{a}) \neq 0$ and hence $g(\mathbf{a}) \neq 0$.
The claim about separability is obvious from equation (5). □

If K is Hilbertian then $H(f_1, \ldots, f_n; g)$ is non-empty which implies $G(f_1, \ldots, f_n; g)$ is non-empty. We prove the converse.

Lemma 6.1.6. Suppose $f \in K[T_1, \ldots, T_r, X]$ be an irreducible polynomial, monic and separable in X such that $\deg_X(f) \geq 2$. Then there exists $f_1, \ldots, f_r \in K[T_1, \ldots, T_r, X]$ where f_i is absoutely irreducible, monic and separable in X and $\deg_X(f_i) \geq 2$ such that $G(f_1, \ldots, f_n) \subset H(f)$.

Proof. Let $\{x_i\}$ be roots of f as a polynomial over the field $K(\mathbf{T})$. Then $E = K(\mathbf{T})(x_1, \ldots, x_n)$ is a finite separable extension of $K(\mathbf{T})$ and $f(\mathbf{T}, X) = \prod_{i=1}^{n}(X - x_i)$. For any non-empty proper subset $I \subset \{1, \ldots, n\}$, we know that $f_I = \prod_{i \in I}(X - x_i)$ is not an element of $K(\mathbf{T})[X]$, otherwise f is reducible. Thus, there exists a coefficient y_I of f_I such that $y_I \notin K(\mathbf{T})$. Let $g_I \in K(\mathbf{T})[X]$ be the monic, irreducible polynomial such that $g_I(\mathbf{T}, y_I) = 0$. Since y_I is a polynomial in x_i and x_i are integral over $K[\mathbf{T}]$, we may assume that $g_I \in K[\mathbf{T}][X]$. For the same reason, g_I is separable polynomial in X and $\deg_X(g_I) \geq 2$.
Suppose g_I is reducible in $\tilde{K}[\mathbf{T}, X]$, i.e $g_I = \prod_j h_j$ where h_j are monic, irreducible polynomials in $\tilde{K}[\mathbf{T}, X]$. Note that since g_I is separable, each h_j is distinct.
Since $h_i \neq h_j \Rightarrow V(h_i) \nsubseteq V(h_j)$. This is because $I(V(\mathfrak{p})) = \mathfrak{p}$ if $\mathfrak{p}$ is a prime ideal in $K[\mathbf{T}, X]$. Let $W_I = \bigcap_i V(h_i) = V(h_1, \ldots, h_k)$.
For any i, we must have $\dim(V(h_i)) = \dim(K[\mathbf{T}, X]/(h_i)) \leq r$ since height of (h_i) is at least 1 because of the chain $(0) \subset (h_i)$.

By Lemma5.0.8, $\dim(W_I) \leq r-1$. For all proper non-empty subsets of I for which g_I is reducible in $\tilde{K}[\mathbf{T}, X]$ let $W := \bigcup W_I$ where W_I is as above. Since $\dim(W) = \max(\dim(W_I))$ we get that $\dim(W) \leq r-1$.
Project $\pi : W \to \mathbb{A}^r(\tilde{K})$ and let A be the K-closure of $\pi(W)$. Since $\pi' : W \to A$ is a dominant map, the induced map between function fields $K(A) \to K(W)$ is a injection and hence $\dim(A) \leq \dim(W) \leq r-1$ and hence $(0) \subsetneq I(A)$.

Thus, there exists $g \in K[\mathbf{T}]$ such that g is non-zero and vanishes on A. For I non-empty proper subsets of $\{1, \ldots, n\}$ for which g_I is absolutely irreducible, denote them by h_I. Then we claim that

$$G(h_I; g) \subset G(g_I \mid I \subsetneq \{1, \ldots, n\})$$

Indeed, if $\mathbf{a} \in \mathbb{A}^r(K)$ such that $h_I(\mathbf{a}, b) \neq 0$ for all $b \in K$ and $g(\mathbf{a}) \neq 0$. Suppose

$g_I(\mathbf{a}, b) = 0$ for some I a non-empty proper subset of $\{1, \ldots, n\}$.

Suppose $g_I = \prod_j h_j$, then $0 = g_I(\mathbf{a}, b) = \prod_j h_j(\mathbf{a}, b)$. Thus, WLOG $h_1(\mathbf{a}, b) = 0$. Thus, $(\mathbf{a}, b) \in V(h_1)$.

By Lemma(5.0.12), we know that $V(h_j) = \sigma(V(h_1))$ for some $\sigma \in \mathrm{Gal}(\tilde{K}/K)$ and hence $(\mathbf{a}, b) \in V(h_i)$ for all i. Consequently, $(\mathbf{a}, b) \in W_I$ and hence $\mathbf{a} \in A$. By choice of g, we have $g(\mathbf{a}) = 0$. This is a contradiction.

Now we show that

$$G(g_I \mid I \subsetneq \{1, \ldots, n\}) \subset H(f) \tag{6.4}$$

Suppose $\mathbf{a} \in LHS$ and $f(\mathbf{a}, X)$ is reducible i.e $f(\mathbf{a}, X) = f_1(X)f_2(X)$.

Consider the place $\phi : K(\mathbf{T}) \to K(\mathbf{a}) \cup \{\infty\}$ generated by application of (**??**) to the ring map $K[\mathbf{T}] \to K(\mathbf{a})$ where T_i is sent to a_i. By (**??**) we can extend ϕ to a place $\phi* : K(\mathbf{T})(x_1, \ldots, x_n) \to K(\mathbf{a})(c_1, \ldots, c_n) \cup \{\infty\}$ where c_i are roots of $\phi(f(\mathbf{T}, X)) = f(\mathbf{a}, X)$. Note that since $\deg_X(\phi(f(\mathbf{T}, X))) = \deg_X(f(\mathbf{T}, X))$ no root is sent to ∞. Since $f(\mathbf{a}, X) = \prod(X - c_i)$ we infer that there exists a proper non-empty subset I of $\{1, \ldots, n\}$ such that $f_1 = \prod_{i \in I}(X - c_i)$.

Let $\phi^*(y_I) = d$ for I as in above line. Then since $g_I(\mathbf{T}, y_I) = 0$, by applying ϕ^* we infer that $g_I(\mathbf{a}, d) = 0$. But since $c_i \in K$ and y_I is a polynomial combination of x_i, it is true that d is a polynomial combination of c_i and hence $d \in K$. But it contradicts our choice of $\mathbf{a}$. Thus, $G(h_I; g) \subset H(f)$. Use (6.1.5) to eliminate g.

□

6.2 Global fields are Hilbertian

Lemma 6.2.1. A finite group G cannot be union of conjugates of its proper subgroup.

Lemma 6.2.2. For L/K a finite separable extension of global fields, there are infinitely many places $\mathfrak{p} \in \mathbb{P}(K)$ for which $\overline{L}_{\mathfrak{P}} = \overline{K}_{\mathfrak{p}}$ where $\mathfrak{P}$ is any prime lying above $\mathfrak{p}$.

Proof. WLOG we may assume L/K is finite Galois. Consider $A = \{\mathfrak{p} \mid (\dfrac{L/K}{\mathfrak{p}}) = \{1\}\}$ and we know by CDT A is infinite. Primes in A exactly correspond to primes which split completely in L. □

Lemma 6.2.3. Let q be a prime power and $\overline{K} = \mathbb{F}_q$ and consider $\overline{E} = \overline{K}(T)$ where T is an indeterminate. Consider a Galois extension $\overline{F} = \overline{K}(T)(z)$ where $\overline{g}(T, X)$ is the monic irreducible polynomial for z and suppose $\overline{K}$ is algebraically closed in $\overline{F}$. Let $d = \deg(\overline{g}), m = \deg_X(\overline{g})$ and $\mathcal{C}$ be a conjugacy class in $\mathrm{Gal}(\overline{F}/\overline{K})$. Then the number N of degree 1, unramified primes $\mathfrak{p} \in \mathbb{P}(K)$ such that $(\frac{\overline{F}/\overline{K}}{\mathfrak{p}}) = \mathcal{C}$ satisfies

$$\left| N - \frac{|\mathcal{C}|q}{m} \right| < 10d^2|\mathcal{C}|\sqrt{q}. \tag{6.5}$$

Proof. We use Theorem(3.0.14) coupled with the inequality $g_{\overline{F}} \leq \frac{(d-1)(d-2)}{2}$. □

Lemma 6.2.4. Let K be a global field and $f \in K[T, X]$ be an absolutely irreducible polynomial such that f is monic, separable in in the variable X and $\deg_X(f) > 1$. Then there are infinitely many primes $\mathfrak{p} \in \mathbb{P}(K)$ such that there exists $a_{\mathfrak{p}} \in \mathcal{O}_K$ with the following property:
If $a \in \mathcal{O}_K$ such that $a \equiv a_{\mathfrak{p}} \mod \mathfrak{p}$, then $f(a, b) \neq 0 \ \forall \ b \in K$.

Proof. In case K is a function field over $\mathbb{F}_q$, choose $t \in K$ such that $K/\mathbb{F}_q(t)$ is a separable extension.
Let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ or $\mathbb{F}_q[t]$(depending on K) in the field K. Almost all primes/places lie in $\mathcal{O}_K$ and since fraction field of $\mathcal{O}_K$ is K, by changing X to cX for some $c \in \mathcal{O}_K$, we may reduce the problem to $f \in \mathcal{O}_K[T, X]$.
Considering f as polynomial over $K(T)$, let $\{X_1, \ldots, X_n\}$ be roots of f and define $F := K(T)(\{X_i\})$. Let L be the algebraic closure of K in F. Since $[F : K(T)] < \infty$, we must have $[L : K] < \infty$. Hence, $\mathrm{tr}(L/\mathbb{F}_q(t)) = 1$. Thus, by Lemma 2.7.5(c)[1], we have that F/L is a regular extension.

$$\begin{tikzcd}
 & & F = K(T, x_1, \ldots, x_n) \arrow[dl, dash] \arrow[d, dash] \\
 & L(T) \arrow[dl, dash] \arrow[d, dash] & L \arrow[dl, dash] \\
E = K(T) \arrow[d, dash] & L \arrow[dl, dash] & \\
K & &
\end{tikzcd}$$

Let $F = L(T)(z)$ and $g \in L(T)[X]$ be the irreducible polynomial of z. We may assume that z is integral over $\mathcal{O}_L[T]$. Thus, $g \in \mathcal{O}_L[T][X]$. By regularity g is absolutely irreducible.
By Lemma last one of CDT, the set of places $A \subset \mathbb{P}(K)$ such that $\overline{L}_{\mathfrak{P}} = \overline{K}_{\mathfrak{p}}$ is infinite.

After carefully choosing a set $B \subset A$, we consider $\overline{f}(T,X) \in \overline{K}_{\mathfrak{p}}[T,x]$ where $\mathfrak{p} \in B$. We want B to consist of primes such that

1. $\overline{f}(T,X)$ is defined.
2. $\overline{f}(T,X)$ remains absolutely irreducible
3. $\overline{f}(T,X)$ remains separable in X.
4. $\overline{g}(T,X)$ is defined.
5. $\overline{g}(T,X)$ remains absolutely irreducible
6. $\overline{g}(T,X)$ remains separable in X.
7. $\{\overline{X}_i\}$ is defined.
8. $\overline{z}$ is defined.

Suppose there exist such a set B which is infinite.

$$\begin{tikzcd}
\overline{F} = \overline{K}_{\mathfrak{p}}(T)(\overline{x}_1, \ldots, \overline{x}_n) \arrow[d, dash] \\
\overline{E} = \overline{K}_{\mathfrak{p}}(T) \arrow[d, dash] \\
\overline{K}_{\mathfrak{p}}
\end{tikzcd}$$

Let $\{\overline{x}_i\}$ be roots of $\overline{f}$ in some algebraic closure. Then $\overline{g}(T,X)$ is the irreducible polynomial for $\overline{z}$ and $\overline{F} = \overline{E}(\overline{z})$. Since $\overline{g}(T,X)$ is absolutely irreducible, hence we have that $\overline{K}_{\mathfrak{p}}$ is algebraically closed in $\overline{F}$.
Since $\mathrm{Gal}(\overline{F}/\overline{E}(\overline{x}_1)) \subsetneq \mathrm{Gal}(\overline{F}/\overline{E})$, we can find $\sigma \in \mathrm{Gal}(\overline{F}/\overline{E})$ such that $\sigma(\overline{x}_i) \neq \overline{x}_i$ for all i.

Since $q = |\overline{K}_{\mathfrak{p}}|$, for almost all prime $\mathfrak{p} \in B$, we can ensure that $10d^2 \deg_X(g) < \sqrt{q}$ and hence by Lemma 0.1, we can find $\alpha \in \overline{K}_{\mathfrak{p}}$, such that $(\frac{\overline{F/E}}{\mathfrak{p}_\alpha}) = \mathcal{C}_\sigma$. Call the set $C \subset B$ for which above is valid.
Thus for any element $\mathfrak{p}_\alpha \in C$, we have $\sigma(\overline{x}) \equiv \overline{x}^q$ and $\overline{x}_i \not\equiv \overline{x}_j$. Moreover, this implies that $\overline{x}_i \not\equiv \overline{x}_i^q$. Thus, $\overline{f}(\alpha, X)$ has no roots in $\overline{K}_{\mathfrak{p}}$.
Choose $\alpha_{\mathfrak{p}}$ as a lift of α in $\mathcal{O}_K$. For $\alpha \equiv \alpha_{\mathfrak{p}}$ in $\mathcal{O}_K/\mathfrak{p}$, we must have that $f(\alpha, X)$ has no root in $\mathcal{O}_K$ and hence in K, otherwise we would get a root in $\overline{K}_{\mathfrak{p}}$. Thus we are done after showing the existence of set B as above.

For choosing the set B as above,

1. Since $f \in \mathcal{O}_K[T, X]$ and $\mathcal{O}_K \subset \mathcal{O}_{\mathfrak{p}}$ for all most all primes,$\overline{f}$ is defined for almost all primes $\mathfrak{p} \in \mathbb{P}(K)$. Moreover, $A_1 = \{\mathfrak{p} \in \mathbb{P}(K) \mid \overline{f}$ is defined and is absolutely irreducible $\}$ is cofinite by Bertini-Noether Lemma. If $\text{disc}(f(T)) = \prod_{i\neq j}(x_i - x_j) = N_{F/E}(f_X(x_1)) \in \mathcal{O}_K[T]$, we have $\text{disc}(\overline{f}(T)) = \prod_{i\neq j}(\overline{x}_i - \overline{x}_j) \in \overline{K}_{\mathfrak{p}}[T]$. For primes $\mathfrak{p} \in A_1$ which do not divide $\text{disc}(\overline{f}(T))$, we get that $\overline{f}$ is separable. Thus, the set of primes A_1' for which $\overline{f}$ is defined, absolutely irreducible, separable is a cofinite set.

2. Almost similar argument as above gives that the set A_2' of primes in $\mathbb{P}(L)$ for which $\overline{g}$ is defined, absolutely irreducible, separable is a cofinite set.

3. $\{x_i\}$ are polynomial combinations over z with coefficients as ratio of elements in $\mathcal{O}_L[T]$. Let A_3 be the set of primes $\mathfrak{p}$ which do not divide any of the denomiators, and they are also cofinite.

4. z can be written as polynomial combination of $\{x_i\}$ with coefficients as ratios of elements in $\mathcal{O}_K[T]$. Let A_3' be the set of primes $\mathfrak{p} \in \mathbb{P}(L)$ which do not divide any of the denominators, and this set is also cofinite.

5. Let $B = A \cap A_1' \cap A_2' \cap A_3 \cap A_3'$ and observe that B is infinite.

Theorem 6.2.5. Let K be a global field and H a separable Hilbert subset of K, then H contains infinitely many elements. In particular, K is Hilbertian.

Proof. By Lemma(6.1.4), we may assume $H(f) \subset H$ where $f \in K[T, X]$ where f is monic, separable in X and $\deg_X(f) \geq 2$. By (6.1.6), we may assume $G(h_1, \ldots, h_k) \subset H(f)$ where $h_i \in K[T, X]$ are absolutely irreducible, monic and separable in X such that $\deg_X(h_i) \geq 2$. Hence, it is enough to show that $G(h_1, \dots, h_k)$ contains infinitely many points.

For each h_i, by Lemma (6.2.4), choose a prime ideal $\mathfrak{p}_i \in \mathcal{O}_K$ for which there exists $a_{\mathfrak{p}_i} \in \mathcal{O}_K$ such that $h_i(a_{\mathfrak{p}_i}, X)$ has no zero in K. Thus, $a_{\mathfrak{p}_i} \in G(h_i)$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ be distinct such primes. By Chinese remainder , choose an element $a \in \mathcal{O}_K$ such that $a \equiv a_{\mathfrak{p}_i} \mod \mathfrak{p}_i$ and hence we get that $a \in G(h_1, \dots, h_k)$. In particular all elements $b \in \mathcal{O}_K$ such that $b - a \in \prod_{i=1}^{t} \mathfrak{p}_i$ lie in $G(h_1, \dots, h_k)$.

□

Lemma 6.2.6. Let K/F be a finite Galois extension with Galois group G. Let R be a subring of F with fraction field as F. Suppose $K = F(\alpha)$ and $f(x) \in R[x]$ is the monic, irreducible polynomial of degree $n = [K : F]$ such that $f(\alpha) = 0$. Let A be a finite subset of K containing α such that it is G-invariant. Let $S = R[A]$.

There exists $u \in R$ such that, for each ring homomorphism $\omega : R \to F'$,:

If $\omega(u) \neq 0$, ω extends to $\omega' : S \to K'$ where K' is a finite Galois extension of F'. Moreover,

1. $K' = F'(\alpha')$ where $\alpha' = \omega'(\alpha)$.
2. The polynomial $f' = \omega(f)$ is such that $f'(\alpha') = 0$.
3. Suppose f' is irreducible, then $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K'/F')$.

Proof. Suppose $R[A] = R[\alpha]$ and $f' = \omega(f)$, then it is easy to see that $R[\alpha] \cong R[x]/(f)$.

Let g' be an irreducible factor of f'. Then there exists a map :

$$R[\alpha] \cong R[x]/(f) \to F'[x]/(g') \tag{6.6}$$

Let ω' be the composition of above maps.

Take $K' = F'[x]/(g)$ and then it is clear that $K' = F'(\alpha')$.

Let $u = \mathrm{disc}(f)$ and we observe that if $\omega(u) \neq 0$ then $\omega(f)$ has distinct roots and hence so does g. Thus, K'/F' is separable.

Since $K' = F'(\alpha')$ and conjugates of g are contained in the conjugates of f' which are contained in K'. Hence K' is normal over F'.

If f' is irreducible, then $g' = f'$.

For any $\sigma' \in \mathrm{Gal}(K'/F')$ is uniquely determined by its action on α'. If $\alpha_1, \alpha_2, \dots, \alpha_n$

are roots of f in $R[A]$, then $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$ are roots of f' in K'.
Given a $\sigma' \in \mathrm{Gal}(K'/F')$ such that $\sigma'(\alpha) = \alpha'_i$, send σ' to σ which sends $\alpha \to \alpha_i$. This map is an isomorphism.

If $R[A] \neq R[\alpha]$, then we use the following trick.
Each element $x \in A$ can be written as $x = \sum_{i=0}^{m} a_i \alpha^i$ where $a_i \in F$. Hence, we can find a $b \in R$ such that $bx \in R[\alpha]$ for all $x \in A$.
Now consider $R' = R_{(b)}$ (localising at $\{b^i \mid i \in \mathbb{N}\}$). Then for $u = b\,\mathrm{disc}(f) \in R$ such that $\omega(u) \neq 0$, we can extend ω to $\tilde{\omega} : R' = R_{(b)} \to F'$.
We observe that $R[A] \subset R'[A]$ and $R'[A] = R'[\alpha]$. Now use the above case for $\tilde{\omega} : R' \to F'$. □

Lemma 6.2.7. Let K be a Hilbertian field. If G can be represented as Galois group over $K(x_1, \ldots, x_n)$ then there exists a finite Galois extension L of K for which G is the Galois group.

Proof. Suppose $L = K(x_1, \ldots, x_n)(\alpha)$ such that $\mathrm{Gal}(L/K(x_1, \ldots, x_n)) = G$. Suppose $R = K[x_1, \ldots, x_n]$ and we may assume that α is integral over R. Consider $A = \{$ conjugates of $\alpha\}$.
Suppose the irreducible polynomial of α is $f \in K[x_1, \ldots, x_n][Y]$ and let $u \in R$ be as in the Lemma(6.2.6). Consider the set $H_n(f; u)$, which is non-empty by Hilbertianity of K. Then there exists $\mathbf{b} \in K^n$ such that $f(\mathbf{b})(Y)$ is irreducible in $K[Y]$ and $u(\mathbf{b}) \neq 0$.
Consider $\omega : R \to K$ which sends $g(\mathbf{x}) \to g(\mathbf{b})$. By Lemma(6.2.6) we get that there exists F a Galois extension of K such that $G \cong \mathrm{Gal}(F/K)$.

□

Lemma 6.2.8. S_n is a Galois group over $\mathcal{K}$ where $\mathcal{K}$ is Hilbertian field.

Proof. If $\mathcal{K}$ is a Hilbertian field, then consider

$$f(y) = y^n + x_1 y^{n-1} + \ldots + x_{n-1} y + x_n \tag{6.7}$$

a polynomial in $\mathcal{K}(x_1, \ldots, x_n)[y]$ where x_i are indeterminates, we look at the splitting field of $f(y)$, that is $\mathcal{K}(t_1, t_2, \ldots, t_n)$ where $f(y) = \prod_{i=1}^{n}(y - t_i)$.
Thus,

$$[\mathcal{K}(t_1, \ldots, t_n) : \mathcal{K}(x_1, \ldots, x_n)] \leq n!. \tag{6.8}$$

Since S_n, the symmetric group on n letters acts on $\{t_1, \ldots, t_n\}$, it extends to an action of S_n on $\mathcal{K}(t_1, \ldots, t_n)$. We observe that x_i, for each $1 \leq i \leq n$, is a symmetric polynomial in $t_1, \dots, t_n$ and hence it is contained in the fixed field of S_n. We observe that

$$\mathcal{K}(x_1, \dots, x_n) \subset \mathcal{K}(t_1, \dots, t_n)^{S_n}, \tag{6.9}$$

due to which we get that

$$[\mathcal{K}(t_1, \dots, t_n) : \mathcal{K}(x_1, \dots, x_n)] \geq [\mathcal{K}(t_1, \dots, t_n) : \mathcal{K}(t_1, \dots, t_n)^{S_n}]. \tag{6.10}$$

We also know that $[\mathcal{K}(t_1, \dots, t_n) : \mathcal{K}(t_1, \dots, t_n)^{S_n}] =\mid S_n \mid= n!$, by Artin's theorem. Hence $[\mathcal{K}(t_1, \dots, t_n) : \mathcal{K}(x_1, \dots, x_n)] = n!$. Consequently

$$S_n = \mathrm{Gal}(\mathcal{K}(t_1, \dots, t_n)/\mathcal{K}(t_1, \dots, t_n)^{S_n}) = \mathrm{Gal}(\mathcal{K}(t_1, \dots, t_n)/\mathcal{K}(x_1, \dots, x_n)). \tag{6.11}$$

Hence by Lemma(6.2.7),we can get S_n as Galois group over $\mathcal{K}$.

□

Corollary 6.2.9. S_n is a Galois group over $\mathbb{Q}$.

We showed that for $G = S_n$ the field $K(\mathbf{x})^G$ is a purely transcendental function field and hence the Galois group could be transferred to that over K. Emmy Noether asked whether this is true for all groups G and field $\mathbb{Q}(\mathbf{x})$. If this was true then the Inverse Galois Problem would have been solved. In 1969, Richard Swan came up with a counterexample.

Theorem 6.2.10 (Swan)**.** Let G be the cyclic group of order p acting transitively on the indeterminates $x_1, \dots, x_p$. Let L be the fixed field $\mathbb{Q}(x_1, \dots, x_p)^G$. Then L is not a purely transcendental extension of $\mathbb{Q}$ for $p = 47$.

Proof. Refer [7]. □

Bibliography

[1] M.Fried, M. Jarden, *Field Arithmetic*; 3rd edition, Springer.

[2] S. Lang, *Algebraic Number Theory*; 2nd edition, Springer.

[3] P. Morandi, *Field and Galois Theory*; Springer.

[4] H. Stichtenoth, *Algebraic Function Fields and Codes*; Springer.

[5] L.V Dries, *Mathematical Logic(Math 570) Lecture Notes.*

[6] Helmut Volklein, *Groups as Galois Groups*; Cambridge Studies in Advanced Mathematics.

[7] Richard G.Swan, *Invariant Rational Functions and a Problem of Steenrod*; Inventiones mathematicae(1969).