Inverse Galois Problem & Root Clusters

विद्यावाचस्पति की
उपाधि की अपेक्षाओं की आंशिक पूर्ति में प्रस्तुत शोधप्रबंध

A thesis submitted in partial fulfilment of the requirements of the degree of Doctor of Philosophy

द्वारा / By
शुभम् जयस्वाल / Shubham Jaiswal

पंजीकरण सं. / Registration No.:
20182006

शोधप्रबंध पर्यवेक्षक / Thesis Supervisor:

Dr Chandrasheel Bhagwat

भारतीय विज्ञान शिक्षा एवं अनुसंधान संस्थान पुणे
INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH PUNE
2024

Certificate

This is to certify that this dissertation entitled Inverse Galois Problem & Root Clusters towards the partial fulfilment of the degree of Doctor in Philosophy at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Shubham Jaiswal at Indian Institute of Science Education and Research under the supervision of Dr. Chandrasheel Bhagwat , Associate Professor at IISER Pune, during the academic year 2018-2024 .

28/02/2025

Dr. Chandrasheel Bhagwat

Declaration by Student

Name of Student: Shubham Jaiswal

Reg. No.: 20182006

Thesis Supervisor(s): Dr Chandrasheel Bhagwat

Department: Mathematics

Date of joining program: Aug 1st 2018

Date of Pre-Synopsis Seminar : July 29th 2024

Title of Thesis : Inverse Galois Problem & Root Clusters

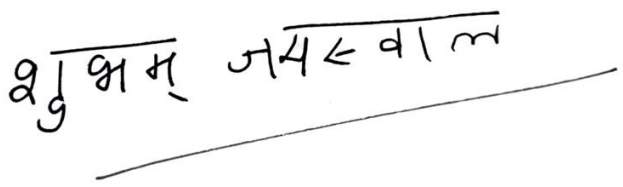
I declare that this written submission represents my idea in my own words and where others' ideas have been included; I have adequately cited and referenced the original sources. I declare that I have acknowledged collaborative work and discussions wherever such work has been included. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

The work reported in this thesis is the original work done by me under the guidance of

Dr./Prof. Dr Chandrasheel Bhagwat

Date: Oct 29th 2024

Signature of the student



Acknowledgments

First and foremost I offer my humble obeisances unto the lotus-feet of my Iṣṭa Hanumān Bhagavān. I am grateful for everything to God Hanumān, and to the presiding God Someshwara of Someshwarawādī Mandira in Pune and to Goddess Mātā Karajā Devī of Vaḷṇaī in Mumbai and to the Great Mathematical Traditions of the World!

I would like to express my deepest gratitude to my Math PhD Guide, Research Supervisor and Academic Advisor Dr. Chandrasheel Bhagwat for his exceptional and insightful guidance and advice, unwavering and invaluable commitment and support and constructive critiques and suggestions that have been instrumental in shaping this research. Your dedication, scholarly prowess, experience and expertise have profoundly influenced and enhanced my academic and personal growth and development. I am incredibly grateful for your patience, encouragement and the time you devoted to help me navigate the complexities of this research. May the Garden of our Mathematics be Everblossoming!

My sincere thanks to Prof. P Vanchinathan for introducing their beautiful paper on Cluster Magnification to us by email which had inspired the second part of this work. I also thank Prof. Vanchinathan and Prof. B. Sury for appreciating our work and motivating us to continue further. I would also like to thank Prof. Joachim König for a prompt reply and useful discussion over email about the results in their paper on IGP for general linear groups over prime order finite fields which had inspired the first part of this work.

I give my heartfelt thanks to my IISER Pune Int PhD Math RAC members Dr. Vivek Mohan Mallick and Dr. Baskar Balasubramanyam and to my IISER Pune Math professors Dr. Amit Hogadi, Dr. Debargha Banerjee and Dr. Krishna Kaipa and to my CMI Chennai BSc Honours Math professors Prof. Krishna Hanumanthu, Prof. Govind Krishnaswami and Prof. Ramaiyengar Sridharan for contributing immensely in my mathematical journey.

I am thankful to my institute IISER Pune for all the resources and facilities and IISER Pune Institute Scholarship for supporting my academic pursuits without which the endeavour would have been impossible. The environment in the institute was an enriching one with both an academic and an extracurricular exposure, which wonderfully nurtured the artist in me who could express himself creatively through math, poetry and music!

I offer my obeisances to the great Srinivasa Ramanujan, whose life and work has always inspired me. I am extremely grateful to my Junior College mentor Siddhesh Naik Sir for identifying the mathematical spark in me and giving the mathematical direction to my life and Ashutosh Chauhan Sir for making mathematics as interesting as challenging! I thank my batchmate Darshan Nasit for helping me with this thesis format. I thank Dr. Sazzad Ali Biswas and Dr. Venketeswara Pai and also thank my IISER batchmates P Narayanan, Dhruv Bhasin, Ajinkya Gaikwad and friend Hiren Dhameliya and seniors Visakh Narayanan, Jewel Mahajan and juniors Paramananda Das, Sushant Maske, Devesh Giri, Eshwar, Harshal and my CMI batchmates Neelarnab Raha, Prabhat Jha and friend Ashwin Bhaskar and seniors Aritriya Mukhapadhyay and Soumyadip Sahu for being a part of my journey.

I am deeply indebted to my mother Sangeeta Jaiswal, my father Shravan Jaiswal and my sister Shreya Jaiswal and my grandparents. Your belief in me, your sacrifices, your patience and understanding and your continuous love and emotional support have been my greatest source of strength. I am forever grateful to my mother for nurturing my potential since my childhood. I am also thankful to all my school and college teachers for contributing to my mathematical journey. May God Gaṇesha and Goddess Saraswatī reveal more unexplored realms of aesthetic knowledge in the years ahead! Namaskāra to All!

Shubham Jaiswal

Abstract

The first part of the thesis is on right splitting, Galois correspondence, Galois representations and Inverse Galois problem. The famous 'Inverse Galois problem' IGP asks whether every finite group appears as the Galois group of some finite Galois extension of $\mathbb{Q}$. Using Galois representations attached to elliptic curves, Arias-de-Reyna and König in [1] have proved the IGP for $\mathrm{GL}_2(\mathbb{F}_p)$ over $\mathbb{Q}$ for all primes $p \geq 5$. Through Galois correspondence and right splitting of some exact sequences of groups, we obtain some general results and apply these to the case in König and obtain interesting occurrences of IGP. The IGP for $\mathrm{PSL}_2(\mathbb{F}_p)$ over $\mathbb{Q}$ for all primes $p \geq 5$ was established by Zywina in [23] using the results of Ribet in [19] about the Deligne's Galois representations associated to certain newforms. Using algebraic operations on Galois representations and right splitting of some exact sequences of groups, we obtain the main results and then apply these to the case in Zywina and obtain equally interesting occurrences of IGP.

The second part of the thesis is on Root Clusters, Magnification, Capacity, Unique chains, Base change and Ascending Index. Inspired from the the work of M Krithika and P Vanchinathan in [13] on Cluster Magnification and the work of Alexander Perlis in [18] on Cluster Size, we establish the existence of polynomials for given degree and cluster size over number fields which generalises a result of Perlis. We state the Strong cluster magnification problem and establish an equivalent criterion for that. We also discuss the notion of weak cluster magnification and prove some properties. We provide an important example answering a question about Cluster Towers. We introduce the concept of Root capacity and prove some of its properties. We also introduce the concept of unique descending and ascending chains for extensions and establish some properties and explicitly compute some interesting examples. Finally we establish results about all these phenomena under a particular type of base change. The thesis concludes with results about strong cluster magnification and unique chains and some properties of the ascending index for a field extension.

Contents

Chapter 1

Introduction

Inverse Problems in Mathematics especially Algebra tend to intrigue me more than often. Like the Inverse problem in Galois theory or Inverse problems in Root Cluster Theory. This thesis deals with such Inverse Problems and attempts to bring to light aesthetically interesting new results and organically develops the theories further.

1.1 Right Splitting, Galois Correspondence, Galois Representations and Inverse Galois Problem

The famous 'Inverse Galois problem' asks whether every finite group appears as the Galois group of some finite Galois extension of $\mathbb{Q}$. Many families of simple groups are known instances of this problem but the general question is still open.

Using Galois representations attached to elliptic curves, Arias-de-Reyna and König have proved the following (Thm 1.1 in [1])

Theorem 1.1.1. *(Arias-de-Reyna, König)*

For a prime $p \geq 5$, there are infinitely many locally cyclic Galois extensions of $\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_p)$, which are pairwise linearly disjoint over $\mathbb{Q}(\sqrt{p^*})$ where $p^* = (-1)^{(p-1)/2}\, p$.

Using the results of Ribet [19] about the Deligne's Galois representations associated to certain newforms, Zywina established the following (Thm 1.4 in [23]),

Theorem 1.1.2. *(Zywina)*

$\mathrm{PSL}_2(\mathbb{F}_p)$ *can be realized as a Galois group over* $\mathbb{Q}$ *for all primes* $p \geq 5$.

1.1.1 Our Contribution

We establish some instances of Inverse Galois problem. These results are a part of the manuscript [4] by Bhagwat and Jaiswal. In Chapter 2, through Galois correspondence and right splitting of some exact sequences of groups, we obtain the main results Thm. 2.2.1, Thm. 2.4.1. We then apply these general results to the case in [1] and obtain interesting consequences as corollaries which are as follows.

Theorem 1.1.3. *(Bhagwat, Jaiswal)*

1. *For a prime* $p \geq 5$, $(\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)) \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$ *(with semidirect product group law as in Thm 2.4.1) is realizable as Galois group over* $\mathbb{Q}$.

2. *For a prime* $p \geq 5$ *with* $p \equiv 3 \, mod \, 4$, *let* H *be the unique index-*2 *(hence normal) subgroup of* $\mathrm{GL}_2(\mathbb{F}_p)$. *Then* $(H \times H) \rtimes \mathrm{GL}_2(\mathbb{F}_p)/H$ *(with semidirect product group law as in Thm 2.4.1) is realizable as Galois group over* $\mathbb{Q}$.

3. *For a prime* $p \geq 5$, $(\mathrm{PSL}_2(\mathbb{F}_p) \times \mathrm{PSL}_2(\mathbb{F}_p)) \rtimes \mathbb{Z}/2\mathbb{Z}$ *(with semidirect product group law as in Thm 2.2.1) is realizable as Galois group over* $\mathbb{Q}$.

In Chapter 3, using the algebraic operation induction on Galois representations and right splitting of some exact sequences of groups, we obtain Thm. 3.1.7, Thm. 3.1.8 as the main results. We then apply these general results to the case in [23] and obtain following interesting consequence as Thm. 3.4.3.

Theorem 1.1.4. *(Bhagwat, Jaiswal)*

1. *For* $p \geq 5$, $\mathrm{PSL}_2(\mathbb{F}_p) \rtimes \mathbb{Z}/2\mathbb{Z}$ *is realizable as Galois Group over* $\mathbb{Q}$ *(for semidirect product group law in Thm 3.1.7).*

2. *This semidirect product in part (1) is direct* $\iff \tilde{\pi}(s) = I$.

3. *Automorphism* $\phi_{\tilde{\rho}(s)}$ *of* $\tilde{\rho}(H)$*, by conjugation by* $\tilde{\rho}(s)$*, is inner.*

4. *The group obtained here is not isomorphic to* $\mathrm{PGL}_2(\mathbb{F}_p)$.

Remark 1.1.4.1. *In Sections* 4 *and* 5 *of the undergraduate Thesis [16] by Joris Nieuwveld, they have constructed explicit algorithm that computes polynomials over any hilbertian base field of characteristic 0 (in particular over rationals) with Galois group isomorphic to a semidirect product with abelian kernel (that is the normal subgroup being abelian).*

Note that all the families of groups that we have proved to be realizable as Galois groups over rationals in Thm 1.1.3 and Thm 1.1.4 are semidirect products with non-abelian kernels (that is the normal subgroup being non-abelian).

Then for the algebraic operations direct sum and tensor products on Galois representations we obtain an unanticipated and interersting result Prop 3.2.2.

Then by using the algebraic operations direct sum and tensor products on Galois representations and right splitting of some exact sequences of groups, we obtain Thm. 3.2.7 as the main result. We then apply this general result to the case in [23] and obtain that $\mathrm{PSL}_2(\mathbb{F}_p) \times \mathbb{Z}/2\mathbb{Z}$ is realizable as Galois Group over $\mathbb{Q}$ for $p \geq 5$.

Right Splitting of exact sequences of groups is the common thread that runs through Chapter 2 and Chapter 3.

1.2 Root Clusters, Magnification, Capacity, Unique Chains, Base Change and Ascending Index

For an irreducible polynomial over a perfect field, we have the notion of root clusters with combinatorial relation between degree of the polynomial, cluster size and number of clusters. For notations refer to Sec. 4.1.

Perlis has proved in [17] and [18] the following.

Theorem 1.2.1. *(Perlis)*

1. *The cluster size $r_K(f)$ is independent of the choice of α.*
2. $r_K(f)\ s_K(f) = \deg(f)$. *In particular,* $r_K(f) \mid \deg(f)$.
3. $r_K(f) =$ *number of roots of f fixed by* $H = |\mathrm{Aut}(K(\alpha)/K)| = [N_G(H) : H]$.

All these notions carry forward to field extensions over the perfect field.

Krithika and Vanchinathan proved the Cluster Magnification theorem (Thm 1 in [13]).

Cluster Magnification Theorem

Theorem 1.2.2. *(Krithika, Vanchinathan)*

Let $\deg(f) = n > 2$ over K with cluster size $r_K(f) = r$. Assume that there is a Galois extension F of K, say of degree d, which is linearly disjoint with K_f over K. Then there exists an irreducible polynomial g over K of degree nd with cluster size rd.

They reformulate the theorem for field extensions as well.

1.2.1 Our Contribution

The results discussed here are a part of the manuscript [3] by Bhagwat and Jaiswal. In Chapter 4, after setting up some notations and reviewing the results by Perlis in [17] [18] and Krithika-Vanchinathan in [13] in Sec. 4.1, we generalise a result of Perlis for number fields that also improves on the generalisation proved previously by Krithika and Vanchinathan in [13]. The generalisation Thm. 4.3.1 is as follows.

Inverse Cluster Size Problem for Number Fields

Theorem 1.2.3. *(Perlis, Krithika and Vanchinathan, A generalisation by Bhagwat, Jaiswal)*

Let K be a number field. Let $n > 2$ and $r|n$. Then there exists an irreducible polynomial over K of degree n with cluster size r.

In the same chapter, we also present a simple lemma about number of clusters, Lemma 4.4.1, which is very useful in giving alternate proofs of results by Perlis and Krithika-Vanchinathan as well as in proving further results.

In Chapter 5, we state the Strong cluster magnification problem and establish the following equivalent criterion for that in Thm. 5.2.3 in terms of Galois groups. For all notations, see Chapter 5.

Theorem 1.2.4. *(Bhagwat, Jaiswal)*

An extension M/K is obtained by nontrivial strong cluster magnification from some subextension L/K if and only if

$$\mathrm{Gal}(\tilde{M}/K) \cong A \times B$$

for nontrivial groups A and B and

$$\mathrm{Gal}(\tilde{M}/M) \cong A' \times 1$$

(under the same isomorphism) for a subgroup $A' \subset A$ with $[A : A'] > 2$.

We also reformulate the Strong cluster magnification problem for irreducible polynomials. We then state the Weak cluster magnification problem and demonstrate how the notions for strong cluster magnification and weak cluster magnification are actually different.

In Chapter 6, we provide an important example, Example 6.1.3, answering a question in [13] about Cluster Towers. We also give a group theoretic formulation for cluster towers.

In Chapter 7, we introduce the concept of Root capacity as a generalisation of cluster size. We begin the chapter with some observations about group of automorphisms of finite extensions in Prop. 7.1.1 & Prop. 7.1.2 & its corollaries. Then we prove some properties of root capacity in Propositions 7.2.1, 7.2.2, 7.2.4, 7.2.7 and 7.2.9. We conclude the chapter with Thm. 7.2.10 which is as follows. For notations, see Sec 4.1 and Chapter 7.

Theorem 1.2.5. *(Bhagwat, Jaiswal)*

Consider extensions $M/L/K$ and let $\tilde{L}$ be Galois closure of L/K. If $M \cap \tilde{L} = L$ and $[M : L] = r_K(M)/r_K(L)$, then M/L is Galois.

In Chapter 8, we introduce the concept of unique descending and ascending chains for extensions. Thm. 8.1.1 and Thm. 8.2.1 encapsulate the important properties of unique chains. Prop. 8.2.2 links unique ascending and descending chain under certain conditions. We prove an interesting result Prop. 8.1.2 that describes the field N_1 in unique descending chain in terms of the sums of elementary symmetric functions. In Sec. 8.3, we compute unique ascending/ descending chains for some interesting examples (see Example 8.3.1, Thm. 8.3.3 and Thm. 8.3.4).

In Chapter 9, we establish Theorems 9.1.1, 9.1.5, 9.2.2 and 9.3.1 about strong cluster magnification, weak cluster magnification, root capacity and unique chains respectively under a particular type of base change.

Then we prove results Thm. 9.4.1 and Thm. 9.4.2 about strong cluster magnification and unique chains which are as follows.

Theorem 1.2.6. *(Bhagwat, Jaiswal)*

- *Let M/K be obtained by strong cluster magnification from L/K with $r_K(L) \neq 1$. Then we have that $M \supsetneq N_1 \supsetneq \cdots \supsetneq N_k$ is the unique descending chain for $M/K \iff L \supsetneq N_1 \supsetneq \cdots \supsetneq N_k$ is the unique descending chain for L/K.*
- *Let M/K be obtained by strong cluster magnification from L/K through F/K as in Def 5.2.0.1 with $t_K(L) \neq 1$. Then we have*
  1. *F' is unique intermediate field for M/K as in Thm. 8.2.1 $\iff$ $F' = F_1F$ where F_1 is unique intermediate field for L/K.*
  2. *$K \subsetneq F_1 \subsetneq \cdots \subsetneq F_k$ is the unique ascending chain for $L/K \iff$ $K \subsetneq F_1F \subsetneq \cdots \subsetneq F_kF$ is the unique ascending chain for M/K for $F_i \subset L$ for all i.*

The thesis concludes with Chapter 10 with some properties of the ascending index $t_K(L)$ defined in Thm. 8.2.1 in the context of unique ascending chain for an extension L/K. The ascending index has many properties similar to the cluster size $r_K(L)$ but has no immediate description in terms of roots of the minimal polynomial of α over K when $L = K(\alpha)$. In Chapter 10, Prop. 10.1.2 establishes a base change property for $t_K(L)$.

Thm. 10.1.3 establishes an analogue of Cluster Magnification Theorem (Thm. 5.1.2) for $t_K(L)$ which is as follows. For notations, see Chapter 8.

Ascending Index Magnification Theorem

Theorem 1.2.7. *(Bhagwat, Jaiswal)*

Let M/K be obtained by strong cluster magnification with magnification factor d. Then

$$t_K(M) = d\, t_K(L) \text{ and } u_K(M) = u_K(L).$$

Finally, Thm. 10.1.4 is an analogue of Thm. 4.3.1 and is as follows.

Inverse Ascending Index Problem for Number Fields

Theorem 1.2.8. *(Bhagwat, Jaiswal)*

Let K be a number field. Let $n > 2$ and $t|n$. Then there exists an extension L/K of degree n with ascending index $t_K(L) = t$.

In the last section of the thesis, we talk about future directions.

1.3 Research Articles

The following two research articles of ours have resulted as part of the work carried out for this PhD thesis.

1. Chandrasheel Bhagwat and Shubham Jaiswal. Right Splitting, Galois Correspondence, Galois Representations and Inverse Galois Problem. Accepted for publication in Journal of the Ramanujan Mathematical Society (2025).

   https://arxiv.org/abs/2403.14316, 2024.

2. Chandrasheel Bhagwat and Shubham Jaiswal. Cluster Magnification, Root Capacity, Unique Chains, Base Change and Ascending Index. Accepted for publication in Proceedings Mathematical Sciences (2025).

   https://arxiv.org/abs/2405.06825, 2024

Chapter 2

Galois Correspondence, Right Splitting & Inverse Galois Problem

In this chapter, we describe some group theoretic results and then through these results as well as Galois correspondence and right splitting of some exact sequences, we obtain some general Galois theoretic results. Then we apply these general results to the cases described in [1] and obtain interesting consequences.

2.1 Right Splitting and Group Theoretic Preliminaries

Proposition 2.1.1. *Let G be a finite group. Then the condition $G/[G,G]$ is cyclic of order m is equivalent to the condition that for any $n|m$, G has a unique index-n normal subgroup such that the quotient is abelian (the quotient with that subgroup is in fact cyclic). This unique subgroup is given by*

$$H = \{x \in G \mid \pi(x) \text{ is an } n\text{-th power in } G/[G,G]\}$$

where π is the quotient homomorphism $G \to G/[G,G]$.

Proof. Suppose $G/[G,G]$ is a cyclic group of order m and $n \mid m$. Hence $G/[G,G]$ has a

unique index-n cyclic subgroup, call it H', which is precisely given by $H' = \{z^n \mid z \in G/[G,G]\}$, which is generated by y^n, where y is a generator of $G/[G,G]$.

Since π is surjective, we have one to one correspondence between subgroups of $G/[G,G]$ and subgroups of G containing $[G,G]$. Let $H = \pi^{-1}(H') = \{x \in G | \pi(x)$ is an n-th power in $G/[G,G]\}$. Hence it is the unique index-n normal subgroup of G containing $[G,G]$.

Let K be any index-n normal subgroup of G such that the quotient is abelian. Consider the quotient map $\rho : G \to G/K$. Since $\mathrm{Image}(\rho)$ is abelian, hence $[G,G] \subset Ker(\rho) = K$. Hence $K = H$.

Also we have that G/H is isomorphic to $(G/[G,G])/H'$. Hence it is cyclic.

Conversely, suppose $G/[G,G]$ is not cyclic. Hence, by structure theorem for abelian groups (Thm 14.7.3 in [2]),

$$G/[G,G] \cong \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times G'$$

for some group G', $a_1 \mid a_2$ and $a_1 > 1$. Since $\mathbb{Z}/a_2\mathbb{Z}$ is cyclic and $a_1 \mid a_2$, we get a unique index-a_1 subgroup G'' of $\mathbb{Z}/a_2\mathbb{Z}$. Hence $\mathbb{Z}/a_2\mathbb{Z} \times G'$ and $\mathbb{Z}/a_1\mathbb{Z} \times G'' \times G'$ are distinct index-a_1 subgroups of $G/[G,G]$. Hence we don't get a unique index-a_1 subgroup H' of $G/[G,G]$. By the one to one correspondence between subgroups of $G/[G,G]$ and subgroups of G containing $[G,G]$, we get two distinct index-a_1 subgroups such that the quotients are abelian.

□

Corollary 2.1.1.1. *Let $n, r \in \mathbb{N}$ and p be an odd prime. For a prime power $q = p^r$, if $q \equiv 1 \ mod\ n$, then $\mathrm{GL}_2(\mathbb{F}_q)$ has a unique index-n normal subgroup such that the quotient is abelian. (The quotient with that subgroup is in fact cyclic). This unique subgroup is given by*

$$H = \{x \in \mathrm{GL}_2(\mathbb{F}_q) \mid det(x) \text{ is an } n\text{-th power in } \mathbb{F}_q^\times\}.$$

Proof. Let $G = \mathrm{GL}_2(\mathbb{F}_q)$. Then $[G,G] = \mathrm{SL}_2(\mathbb{F}_q)$ and $G/[G,G] \cong \mathbb{F}_q^\times$ (isomorphism being through the surjective determinant map) which is cyclic of order $m = q - 1$. Now since $q \equiv 1 \ mod\ n$, we have $n \mid m$. Now consider the determinant map $det : G \to \mathbb{F}_q^\times$ (which is a homomorphism) with kernel $\mathrm{SL}_2(\mathbb{F}_q)$. By applying similar argument to det map as applied

to π map in previous proposition, we are done.

□

Remark 2.1.1.1. *Above corollary holds for* $\mathrm{GL}_k(\mathbb{F}_q)$ *as well for any* $k \in \mathbb{N}$.

Corollary 2.1.1.2. *Let* G *be a group. If* $[G,G]$ *has index* m *in* G*, then* $[G,G]$ *is the unique index-*m *subgroup of* G *such that the quotient is abelian.*

Corollary 2.1.1.3. *Let* $r \in \mathbb{N}$ *and* p *be an odd prime. For a prime power* $q = p^r$*,* $\mathrm{SL}_2(\mathbb{F}_q)$ *is the unique index-*$(q-1)$ *subgroup of* $\mathrm{GL}_2(\mathbb{F}_q)$ *such that the quotient is abelian.*

Proposition 2.1.2. *(Bhagwat, Jaiswal) (Prop 2.2 in [4])*

Let $n \in \mathbb{N}$ *and let* G *be a group such that* $G/[G,G]$ *is cyclic of order* m*. Let* $n|m$ *and let* H *be the unique index-*n *normal subgroup of* G *such that the quotient is abelian. Then the following holds.*

1. *If there exists* $x \in G$ *such that* $x^n = 1$ *and* $\{1, x, x^2, ..., x^{n-1}\}$ *is a set of representatives for* H*-cosets in* G*, then*
$$(n, m/n) = gcd(n, m/n) = 1.$$
2. *If* $(n, m/n) = 1$ *and the exact sequence*
$$1 \to [G,G] \to G \to G/[G,G] \to 1$$
is right split, then there exists $x \in G$ *such that* $x^n = 1$ *and* $\{1, x, x^2, ..., x^{n-1}\}$ *is a set of representatives for* H*-cosets in* G*.*
3. *Let* $n = m$ *(hence* $[G,G]$ *is the unique index-*m *subgroup of* G *such that quotient is abelian). Then the above exact sequence is right split if and only if there exists* $x \in G$ *such that* $x^m = 1$ *and* $\{1, x, x^2, ..., x^{m-1}\}$ *is a set of representatives for* $[G,G]$*-cosets in* G*.*

Proof.

1. Suppose we have a set of representatives for H-cosets in G of the form $\{1, x, x^2, ..., x^{n-1}\}$ with $x \in G$ such that $x^n = 1$. Let y be a generator of cyclic group $G/[G,G]$ and let

$0 \leq l \leq m-1$ be such that $\pi(x) = y^l$. As $x^n = 1$, we have $1 = \pi(x)^n = y^{ln}$ and hence $m \mid ln$. Thus we have

$$j = ln/m \in \mathbb{Z} \text{ and } 1 \leq j \leq (n-1).$$

Now assume on the contrary that $(n, m/n) \neq 1$. Then for $k = n/(n, m/n) \leq n-1$, we have $n \mid km/n$, hence $n \mid kl$, and therefore $\pi(x^k) = y^{lk}$ is an n-th power in $G/[G,G]$, hence $x^k \in H$. Hence we get a contradiction. Furthermore, if $(j, n) \neq 1$ then for $k = n/(j, n)$ we have $n \mid lk$, which gives a contradiction. Hence $(j, n) = 1$.

2. If $(n, m/n) = 1$, then we clearly have that $n \nmid km/n$ for all $1 \leq k \leq (n-1)$. Consider the quotient map $\pi : G \to G/[G,G]$. Since given exact sequence is right split, we have an injective homomorphism $\iota : G/[G,G] \to G$ such that $\pi \circ \iota = id_{G/[G,G]}$. Let $x = \iota(y^{jm/n}) \in G$ where $1 \leq j \leq (n-1)$ and $(j, n) = 1$. Hence $\pi(x) = y^{jm/n}$. Since ι is injective, x will be an element of order n. Now since $n \nmid km/n$ for all $1 \leq k \leq (n-1)$ and since $(j, n) = 1$, we have $n \nmid jkm/n$ for all $1 \leq k \leq (n-1)$. Hence for all $1 \leq k \leq (n-1)$, $\pi(x^k) = y^{jkm/n}$ is not an n-th power in $G/[G,G]$. Hence $x^k \notin H$. Therefore we get a set of representatives for H-cosets in G of the form $\{1, x, x^2, ..., x^{n-1}\}$ with $x \in G$ such that $x^n = 1$.

3. Let us assume that the exact sequence is right split. Since $n = m$, we have $(n, m/n) = (m, 1) = 1$. Hence from (2), we get the required set of representatives for $[G,G]$-cosets in G.

   Conversely, if there exists a set of representatives for $[G,G]$-cosets in G of the form $\{1, x, x^2, ..., x^{m-1}\}$ with $x \in G$ such that $x^m = 1$. Then clearly $\pi(x) = x[G,G]$ is a generator of cyclic group $G/[G,G]$. Define $\iota : G/[G,G] \to G$ by

   $$\iota(\pi(g)) := x^r \text{ if } \pi(g) \in G/[G,G] \text{ is of the form } \pi(x)^r, r \geq 0.$$

   Hence ι is an injective homomorphism satisfying $\pi \circ \iota = id_{G/[G,G]}$ and consequently the exact sequence is right split.

□

Remark 2.1.2.1. *If G is abelian, then it satisfies the hypothesis of above proposition if and only if it is cyclic.*

Remark 2.1.2.2. *The condition that $G/[G,G]$ is cyclic is important in statement (3) above. If G is a non-cyclic abelian group, then $[G,G]=1$ and so exact sequence $1\to 1\to G\to G\to 1$ is clearly right split, but we can never have required representatives for $[G,G]$-cosets because of non-cyclicity of G.*

Corollary 2.1.2.1. *(Bhagwat, Jaiswal) (Corollary 2.2.1 in [4])*

Let $n,r\in\mathbb{N}$. Consider a prime power $q=p^r$ such that $q\equiv 1$ mod n. Let H be the unique index-n subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$ such that the quotient is abelian. Then the following are equivalent.

- $(n,(q-1)/n)=1$.
- *There exists a set of representatives for H-cosets in $\mathrm{GL}_2(\mathbb{F}_q)$ of the form $\{1,x,x^2,...,x^{n-1}\}$ with $x\in\mathrm{GL}_2(\mathbb{F}_q)$ such that $x^n=I$.*

Proof. Let $G=\mathrm{GL}_2(\mathbb{F}_q)$ then $[G,G]=\mathrm{SL}_2(\mathbb{F}_q)$ and $G/[G,G]\cong\mathbb{F}_q^\times$ (isomorphism is defined through the determinant map) is cyclic of order $m=q-1$. Since $q\equiv 1\ mod\ n$, we have $n\mid m$. Consider the exact sequence given by the determinant map

$$1\to[G,G]\to G\xrightarrow{det}\mathbb{F}_q^\times\to 1.$$

Let $\iota:\mathbb{F}_q^\times\to G$ be the map defined by

$$\iota(a)=\begin{pmatrix}1&0\\0&a\end{pmatrix}\ \text{ for all } a\in\mathbb{F}_q^\times.$$

This is a homomorphism satisfying $det\circ\iota=id_{\mathbb{F}_q^\times}$. Hence we conclude that the exact sequence is right split.

By applying similar argument to det map as applied to π map in previous proposition, we are done.

□

Remark 2.1.2.3. *Above corollary holds for* $\mathrm{GL}_k(\mathbb{F}_q)$ *as well for any* $k \in \mathbb{N}$*. This can be proved using the map*

$$\iota(a) = \begin{pmatrix} I_{k-1\times k-1} & 0 \\ 0 & a \end{pmatrix}_{k\times k} \quad \textit{for all } a \in \mathbb{F}_q^{\times}.$$

Proposition 2.1.3. *For given* $n, r \in \mathbb{N}$ *such that* $(r, n) = 1$*, there are infinitely many primes satisfying the two conditions*

$$p^r \equiv 1 \; mod \; n,$$
$$(n, (p^r - 1)/n) = 1.$$

Proof. Suppose a prime p satisfies the given conditions. Let $q = p^r$. Choose $0 \leq k \leq (n-1)$ such that

$$\frac{q-1}{n} \equiv k \; mod \; n.$$

Observe that $(k, n) = 1$ since $(n, (q-1)/n) = 1$. Hence $q \equiv kn + 1 \; mod \; n^2$.

Conversely, each p satisfying $p^r \equiv kn+1 \; mod \; n^2$ for some $0 \leq k \leq (n-1)$ with $(k, n) = 1$, satisfies given conditions.

Now for each $0 \leq k \leq (n-1)$ with $(k, n) = 1$, we have $(kn + 1, n^2) = 1$. Hence by Dirichlet's theorem on primes in arithmetic progression, we conclude that for each such k, there are infinitely many primes such that

$$p \equiv kn + 1 \; mod \; n^2,$$
$$\text{and hence } \; p^r \equiv (kn+1)^r \; mod \; n^2.$$

Now for each such k, $(rk, n) = 1$, because $(k, n) = (r, n) = 1$. Hence there are infinitely many primes satisfying given conditions. □

2.2 Galois correspondence, Right splitting and Galois theoretic results

We discuss a result here that establishes the occurrence of certain semidirect product of groups as a Galois group.

Theorem 2.2.1. *(Bhagwat, Jaiswal) (Thm 2.4 in [4]).*

Let $l \geq 2$. Let K be a finite extension of $\mathbb{Q}$ and let $E_1, E_2, ..., E_l$ be finite Galois extensions of $\mathbb{Q}$ contained in $\bar{\mathbb{Q}}$. Let G_i be the Galois group of E_i over $\mathbb{Q}$ for all i. Suppose

1. *$E_1 \cdots E_k \cap E_{k+1} = K$ for all $1 \leq k \leq l-1$,*

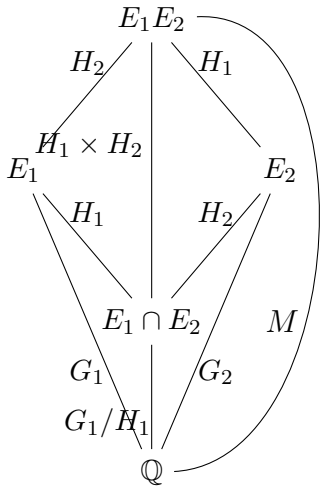
2. *for every i, there exists a set of representatives of H_i-cosets in respective G_i that is closed under multiplication, where H_i is Galois group of E_i over K.*

Then for each $1 \leq i \leq l$, H_i is a normal subgroup of respective G_i and the group $(H_1 \times H_2 \times \cdots \times H_l) \rtimes G_1/H_1$ (for some semidirect product group law) is realizable as the Galois Group of $E_1 \cdots E_l$ over $\mathbb{Q}$.

Proof. We will prove by induction that $\mathrm{Gal}(E_1E_2 \cdots E_k/K) \cong (H_1 \times H_2 \times \cdots \times H_k)$ and $\mathrm{Gal}(E_1E_2 \cdots E_k/\mathbb{Q}) \cong (H_1 \times H_2 \times \cdots \times H_k) \rtimes G_1/H_1$ (for some semidirect product group law) for all $2 \leq k \leq l$.

For base case $k = 2$, see the following diagram.

Since, E_1, E_2 are Galois over $\mathbb{Q}$ and are contained in $\bar{\mathbb{Q}}$, E_1E_2 and $E_1 \cap E_2$ are defined and are Galois over Q and $K = E_1 \cap E_2$. We have $\mathrm{Gal}(E_i/\mathbb{Q}) = G_i$ and $\mathrm{Gal}(E_i/K) = H_i$ for $i = 1, 2$. Since K is Galois over $\mathbb{Q}$, H_is are normal in respective G_is. $\mathrm{Gal}(K/\mathbb{Q}) \cong G_1/H_1 \cong G_2/H_2$. Fix an isomorphism θ from G_2/H_2 to G_1/H_1.



Let $\mathrm{Gal}(K/\mathbb{Q}) = \{x_iH_1 | 1 \leq i \leq n\}$ where $x_iH_1 = \theta(y_iH_2)$ for all i. Here $\{x_i \in G_1 | 1 \leq i \leq n\}$ and $\{y_i \in G_2 | 1 \leq i \leq n\}$ are sets of representatives of H_1 and H_2 cosets in G_1 and G_2 respectively, which are closed under multiplication.

By Galois Correspondence Theorems 2.1 and 2.6 in [5], we have $\mathrm{Gal}(E_1E_2/E_1) \cong H_2$, $\mathrm{Gal}(E_1E_2/E_2) \cong H_1$ and $\mathrm{Gal}(E_1E_2/K) \cong H_1 \times H_2$.

Let $\mathrm{Gal}(E_1E_2/\mathbb{Q}) = M$. We have

$$\begin{aligned} |M| &= [E_1E_2 : K]\,[K : \mathbb{Q}] = |H_1 \times H_2|\,|G_1/H_1| \\ &= |H_1 \times H_2|\,|G_2/H_2| = |G_1|\,|H_2| = |G_2|\,|H_1|. \end{aligned}$$

Consider map $\sigma : M \to G_1 \times G_2$ given by $\sigma(g) = (g_1, g_2)$, where $g_i = g|_{E_i}$ for $i = 1, 2$. The map σ is clearly a well defined injective group homomorphism (see Thm 1.1 [5]).

If $g \in M$ and $g|_K = x_iH_1 = g_1|_K$, then $(x_i^{-1}g_1)|_K = id_K$. Hence $x_i^{-1}g_1 \in H_1$, thus $g_1 \in x_iH_1$. Similarly, by $g|_K = x_iH_1 = \theta(g_2|_K) = \theta(y_iH_2)$, $g_2 \in y_iH_2$.

Hence $\mathrm{Image}(\sigma) \subset \bigsqcup_{i=1}^{n}(x_iH_1 \times y_iH_2)$. Since $|\bigsqcup_{i=1}^{n}(x_iH_1 \times y_iH_2)| = |H_1 \times H_2||G_1/H_1| = |M|$ and σ is injective, we get $\mathrm{Image}(\sigma) = \bigsqcup_{i=1}^{n}(x_iH_1 \times y_iH_2)$. Hence, $M \cong \bigsqcup_{i=1}^{n}(x_iH_1 \times y_iH_2)$.

Consider a map $\psi : \bigsqcup_{i=1}^{n}(x_iH_1 \times y_iH_2) \to (H_1 \times H_2) \rtimes G_1/H_1$ given by $\psi((x_ih_1, y_ih_2)) =$

$((h_1, h_2), x_i H_1)$ where we define a semidirect product group law for $(H_1 \times H_2) \rtimes G_1/H_1$ by

$$((h_1, h_2), x_i H_1).((k_1, k_2), x_j H_1) = ((x_j^{-1} h_1 x_j k_1, y_j^{-1} h_2 y_j k_2), x_i x_j H_1).$$

This group law is well defined and associative since H_i are normal in G_i for $i = 1, 2$ and sets of their respective coset representatives are closed under multiplication. We observe that

$$(x_i h_1, y_i h_2).(x_j k_1, y_j k_2) = (x_i h_1 x_j k_1, y_i h_2 y_j k_2) = ((x_i x_j)(x_j^{-1} h_1 x_j k_1), (y_i y_j)(y_j^{-1} h_2 y_j k_2)).$$

Hence we conclude that ψ is a group isomorphism and hence $M \cong (H_1 \times H_2) \rtimes G_1/H_1$.

Alternatively, consider the sequence

$$1 \to (H_1 \times H_2) \xrightarrow{i} \bigsqcup_{i=1}^{n} (x_i H_1 \times y_i H_2) \xrightarrow{\pi} G_1/H_1 \to 1$$

where $i(h_1, h_2) = (x_1 h_1, y_1 h_2)$ ($x_1 \in H_1, y_1 \in H_2$) and $\pi(x_i h_1, y_i h_2) = x_i H_1$. Because of our multiplicatively closed assumption, x_1 and y_1 are identities of G_1 and G_2 respectively. Hence i is injective. Also π is surjective and $\pi \circ i$ is trivial homomorphism. Thus the sequence is exact.

Now consider $\iota : G_1/H_1 \to \bigsqcup_{i=1}^{n} (x_i H_1 \times y_i H_2)$ with $\iota(x_i H_1) = (x_i, y_i)$. The map ι is clearly a group homomorphism because of our multiplicatively closed assumption and also $\pi \circ \iota = id_{G_1/H_1}$. Hence the sequence is right split. Thus $M \cong (H_1 \times H_2) \rtimes G_1/H_1$.

Now assume that the statement is true for $k = m$, where $2 \leq m \leq l - 1$, that is,

$$\mathrm{Gal}(E_1 E_2 \cdots E_m / K) \cong (H_1 \times H_2 \times \cdots \times H_m),$$

$$\text{and}, \mathrm{Gal}(E_1 E_2 \cdots E_m / \mathbb{Q}) \cong (H_1 \times H_2 \times \cdots \times H_m) \rtimes G_1/H_1,$$

we will prove the statement for $k = m + 1$.

Let $F_1 = E_1 \cdots E_m$ and $F_2 = E_{m+1}$. Hence

$$\begin{aligned}
\mathrm{Gal}(F_1/\mathbb{Q}) &= \mathrm{Gal}(E_1E_2\cdots E_m/\mathbb{Q}) \cong (H_1 \times H_2 \times \cdots \times H_m) \rtimes G_1/H_1, \\
\mathrm{Gal}(F_2/\mathbb{Q}) &= \mathrm{Gal}(E_{m+1}/\mathbb{Q}) \cong G_{m+1}, \\
\mathrm{Gal}(F_1/K) &= \mathrm{Gal}(E_1E_2\cdots E_m/K) \cong (H_1 \times H_2 \times \cdots \times H_m), \\
\mathrm{Gal}(F_2/K) &= \mathrm{Gal}(E_{m+1}/K) \cong H_{m+1} \text{ since} F_1 \cap F_2 = E_1 \cdots E_m \cap E_{m+1} = K.
\end{aligned}$$

Hence F_1 and F_2 satisfy conditions of base case and thus we have

$$\begin{aligned}
\mathrm{Gal}(E_1E_2\cdots E_{m+1}/K) = \mathrm{Gal}(F_1F_2/K) &\cong \mathrm{Gal}(F_1/K) \times \mathrm{Gal}(F_2/K) \\
&\cong (H_1 \times H_2 \times \cdots \times H_m) \times H_{m+1} = H_1 \times H_2 \times \cdots \times H_{m+1}
\end{aligned}$$

and,

$$\begin{aligned}
\mathrm{Gal}(E_1E_2\cdots E_{m+1}/\mathbb{Q}) = \mathrm{Gal}(F_1F_2/\mathbb{Q}) &\cong \mathrm{Gal}(F_1F_2/K) \rtimes G_1/H_1 \\
&\cong (H_1 \times H_2 \times \cdots \times H_{m+1}) \rtimes G_1/H_1.
\end{aligned}$$

□

Remark 2.2.1.1.

1. *If $[G : H]$ is finite, then a set of representatives for H-cosets in G satisfies the condition of closed under multiplication if and only if it is a subgroup of G.*

   In particular, A set of representatives $\{1, x, x^2, ..., x^{n-1}\}$ for H-cosets in G which forms a cyclic subgroup of G, satisfies the condition. We get a criterion for existence of such a set of representatives in Prop 2.1.2.

2. *The second condition assumed in the theorem is equivalent to exact sequences*

$$1 \to H_i \to G_i \to G_i/H_i \to 1$$

   being right split, that is $G_i \cong H_i \rtimes G_i/H_i$ for some semidirect product group law.

Remark 2.2.1.2. *Let d_i be distinct primes for $i = 1, 2$ and $d_3 = d_1d_2$. Let $K = \mathbb{Q}$ and consider quadratic extensions $E_i = \mathbb{Q}\sqrt{d_i}$ for $1 \leq i \leq 3$.*

Clearly $E_i \cap E_j = K$ for all $i \neq j$, but we have $E_iE_j \cap E_k = E_k \neq K$ where i, j, k are a permutation of $1, 2, 3$. So the assumed condition in the above theorem is not always satisfied and hence it is important.

Remark 2.2.1.3. *In the above theorem, we could have assumed a symmetric but stronger condition $E_1...E_{i-1}E_{i+1}...E_n \cap E_i = K$ for all $1 \leq i \leq n$ which implies the condition that we have assumed $E_1...E_k \cap E_{k+1} = K$ for all $1 \leq k \leq n-1$ since $E_1...E_k \cap E_{k+1} \subset E_1...E_kE_{k+2}...E_n \cap E_{k+1} = K$. But it would have made our theorem weaker. (Note: Condition for $i = 1$ is not required, it is written for symmetry).*

Remark 2.2.1.4.

1. *Under the conditions of above theorem, we have $(H_1 \times H_2 \times \cdots \times H_l) \rtimes G_1/H_1 \hookrightarrow G_1 \times G_2 \times \cdots \times G_l$ from Thm 1.1 [5].*
2. *If all G_is are abelian in above theorem that is each E_i is an abelian extension of $\mathbb{Q}$, then the compositum is an abelian extension over $\mathbb{Q}$ and the semidirect product that we defined is in fact the direct product.*
3. *However to the best of our knowledge, one doesn't know in general whether $(H_1 \times H_2 \times \cdots \times H_l) \times G_1/H_1$ is realizable as a Galois group over $\mathbb{Q}$.*

We now describe an independently interesting consequence of the Galois Correspondence (see Theorems 2.1 and 2.6 in [5].)

Proposition 2.2.2. *(Bhagwat, Jaiswal) (Prop 2.5 in [4])*

Let finite groups $H_1, H_2, ..., H_n$ be Galois groups over K of extensions $E_1, E_2, ..., E_n$ respectively which are contained in $\bar{\mathbb{Q}}$. Fix $k \leq n-1$ and suppose $E_{i_1} \cdots E_{i_j} \cap E_{i_{j+1}} = K$ for all $1 \leq j \leq k-1$ where i_l are distinct elements from 1 to k. Then the following statements are equivalent.

1. $E_1 \cdots E_k \cap E_{k+1} = K$.
2. $E_{i_1} \cdots E_{i_k} \cap E_{i_{k+1}} = K$ *where i_l are distinct elements from 1 to $k+1$.*
3. $E_1 \cdots E_{i-1}E_{i+1} \cdots E_{k+1} \cap E_1 \cdots E_{j-1}E_{j+1} \cdots E_{k+1} = E_1 \cdots E_{i-1}E_{i+1} \cdots E_{j-1}E_{j+1} \cdots E_{k+1}$ *for any $1 \leq i < j \leq k+1$.*

Proof. Because of given conditions and induction we get,

$$\mathrm{Gal}(E_{i_1} \cdots E_{i_j}/K) \cong H_{i_1} \times ... \times H_{i_j}$$

for all $j \leq k$ where i_l are distinct elements from 1 to k and

$$\mathrm{Gal}(E_{i_1} \cdots E_{i_j}/E_{i_1} \cdots E_{i_{m-1}} E_{i_{m+1}} \cdots E_{i_j}) \cong H_{i_m}$$

for all $j \leq k$ and $1 \leq m \leq j$ where i_l are distinct elements from 1 to k.

Equivalence of (1) and (2): For i_l distinct elements from 1 to $k+1$,

$$\begin{aligned} & E_1 ... E_k \cap E_{k+1} = K. \\ \iff & \mathrm{Gal}(E_1 \cdots E_{k+1}/K) \cong H_1 \times \cdots \times H_{k+1}. \\ \iff & E_{i_1} \cdots E_{i_k} \cap E_{i_{k+1}} = K. \end{aligned}$$

Equivalence of (1) and (3): For any $1 \leq i < j \leq k+1$, let

$$\begin{aligned} D &= E_1 \cdots E_{k+1}, \\ D_i &= E_1 \cdots E_{i-1} E_{i+1} \cdots E_{k+1}, \\ D_j &= E_1 \cdots E_{j-1} E_{j+1} \cdots E_{k+1}, \\ D_{ij} &= E_1 ... E_{i-1} E_{i+1} ... E_{j-1} E_{j+1} ... E_{k+1}. \end{aligned}$$

Now since $\mathrm{Gal}(D_i/D_{ij}) \cong H_j$ and $\mathrm{Gal}(D_j/D_{ij}) \cong H_i$, we have by Thm 1.1 [5],

$$\mathrm{Gal}(D/D_{ij}) \hookrightarrow H_i \times H_j.$$

We also have

$$\begin{aligned} \mathrm{Gal}(D/K)/\mathrm{Gal}(D/D_{ij}) &\cong \mathrm{Gal}(D_{ij}/K) \\ &\cong H_1 \times \cdots \times H_{i-1} \times H_{i+1} \times \cdots \times H_{j-1} \times H_{j+1} \times \cdots \times H_{k+1}. \end{aligned}$$

Hence,

$$\begin{aligned} & \mathrm{Gal}(D/K) \cong H_1 \times \cdots \times H_{k+1} \\ \implies & \mathrm{Gal}(D/D_{ij}) \cong H_i \times H_j \\ \implies & D_i \cap D_j = D_{ij}. \end{aligned}$$

Conversely,

$$\begin{aligned} & D_i \cap D_j = D_{ij} \\ \implies & D_i \cap E_i \subset D_i \cap D_j = D_{ij} \\ \implies & D_i \cap E_i \subset D_{ij} \cap E_i = K \\ \implies & D_i \cap E_i = K \\ \implies & \mathrm{Gal}(D/K) \cong H_1 \times \cdots \times H_{k+1}. \end{aligned}$$

□

2.3 Cases of IGP in work of Arias-de-Reyna & König

We begin with definition of linear disjointness.

Definition 2.3.1. *Let E_1 and E_2 be extensions of a fields K contained in an algebraic closure $\bar{K}$ of K. Then E_1 and E_2 are linearly disjoint over K if every K-linearly independent subset of E_1 is also linearly independent over E_2.*

We note the following basic fact from Galois theory.

Remark 2.3.1.1. *Let E_1 and E_2 be finite extensions over K contained in $\bar{K}$ and suppose one of them is Galois. Then E_1 and E_2 are linearly disjoint over $K \iff E_1 \cap E_2 = K$ (see [15, Def 20.1 and Example 20.6]).*

Definition 2.3.2. *Let K'/K be a Galois extension of number fields. We say that K'/K is locally cyclic, if its decomposition group at every prime is cyclic.*

Using Galois representations attached to elliptic curves, Arias-de-Reyna and König have proved the following (Thm 1.1 in [1])

Theorem 2.3.3. *(Arias-de-Reyna, König)*

For a prime $p \geq 5$, there are infinitely many locally cyclic Galois extensions of $\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_p)$, which are pairwise linearly disjoint over $\mathbb{Q}(\sqrt{p^*})$ where $p^* = (-1)^{(p-1)/2}\, p$.

Consequently one also has the following.

Corollary 2.3.3.1. *For a prime $p \geq 5$, there are infinitely many locally cyclic Galois extensions of $\mathbb{Q}$ with Galois group $\mathrm{PGL}_2(\mathbb{F}_p)$, which are pairwise linearly disjoint over $\mathbb{Q}(\sqrt{p^*})$.*

One also has the following from Remark 4.4 and Corollary 4.3 of [1].

Proposition 2.3.4. *There are two Galois extensions L_1, L_2 over $\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_p)$ which are linearly disjoint over $\mathbb{Q}(\zeta_p)$.*

2.4 New Cases of IGP through the Cases in work of Arias-de-Reyna & König

Theorem 2.4.1. *(Bhagwat, Jaiswal) (Thm 2.6 in [4]).*

Let $n, r \in \mathbb{N}$. For a prime power $q = p^r$, suppose the following hold.

1. *$q \equiv 1 \; mod \; n$ and $(n, (q-1)/n) = 1$.*
2. *$\mathrm{GL}_2(\mathbb{F}_q)$ is realizable as Galois group over $\mathbb{Q}$ of extensions E_1, E_2 which are contained in $\bar{\mathbb{Q}}$ such that $E_1 \cap E_2 = K$ is a degree n abelian extension of $\mathbb{Q}$.*

Then $(H \times H) \rtimes \mathrm{GL}_2(\mathbb{F}_q)/H$ (with semidirect product group law as in Thm 2.2.1) is realizable as Galois group over $\mathbb{Q}$ where H is the unique index-n subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$ such that the quotient is abelian.

Proof. We have for $l = 2$, E_1, E_2 satisfying conditions of Thm 2.2.1 with $G_1 = G_2 = \mathrm{GL}_2(\mathbb{F}_q)$, and $[G_1 : H_1] = n$ and G_1/H_1 is abelian group and $q \equiv 1 \ mod \ n$. Therefore $H_1 = H_2 = H$. Since $q \equiv 1 \ mod \ n$ and $(n, (q-1)/n) = 1$, from Corollary 2.1.2.1, we get the required set of representatives for H-cosets in $\mathrm{GL}_2(\mathbb{F}_q)$. □

Remark 2.4.1.1. *Because of the conditions on p and n in above theorem, we actually get that K is a cyclic extension (not just abelian).*

Corollary 2.4.1.1. *(Bhagwat, Jaiswal) (Corollary 2.6.1 in [4])*

For a prime $p \geq 5$, $(\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p)) \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$ (with semidirect product group law as in above theorem) is realizable as Galois group over $\mathbb{Q}$.

Proof. From Prop 2.3.4, we get E_1, E_2 satisfying conditions of previous theorem with $n = p-1$, $K = \mathbb{Q}(\zeta_p)$ and $\mathrm{GL}_2(\mathbb{F}_p)/H$ is cyclic group of order $p-1$. Moreover from Corollary 2.1.1.3, we have $H = \mathrm{SL}_2(\mathbb{F}_p)$. □

Corollary 2.4.1.2. *(Bhagwat, Jaiswal) (Corollary 2.6.2 in [4])*

For a prime $p \geq 5$ with $p \equiv 3 \ mod \ 4$, let H be the unique index-2 (hence normal) subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Then $(H \times H) \rtimes \mathrm{GL}_2(\mathbb{F}_p)/H$ (with semidirect product group law as in above theorem) is realizable as Galois group over $\mathbb{Q}$.

Proof. From Thm 2.3.3, we get E_1, E_2 satisfying conditions of previous theorem with $n = 2$. Since $p \equiv 1 \ mod \ 2$, the conditions $p \equiv 3 \ mod \ 4$ and $(2, (p-1)/2) = 1$ are equivalent. Hence we are done. □

Remark 2.4.1.2. *If $p \equiv 1 \ mod \ 4$ then $(2, (p-1)/2) = 2$. Hence by Corollary 2.1.2.1 there is no $x \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $x \in H$ and $order(x) = 2$.*

Corollary 2.4.1.3. *For a prime $p \geq 5$ with $p \equiv 3 \ mod \ 4$, let H be the unique index-2 subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Then H and $H \times H$ are realizable as Galois groups over $\mathbb{Q}\sqrt{-p}$.*

Proof. From previous corollary and proof of Thm 2.2.1, we have that $H \times H$ is realizable as Galois group over $\mathbb{Q}\sqrt{p^*} = \mathbb{Q}\sqrt{-p}$ (since $p \equiv 3 \ mod \ 4$). Since H is normal in $H \times H$ (where embedding is given by $h \mapsto (h, 1)$), the quotient H is also realizable as Galois group over $\mathbb{Q}\sqrt{-p}$.

□

Proposition 2.4.2. *(Bhagwat, Jaiswal) (Prop 2.7 in [4])*

For a prime $p \geq 5$, $(\mathrm{PSL}_2(\mathbb{F}_p) \times \mathrm{PSL}_2(\mathbb{F}_p)) \rtimes \mathbb{Z}/2\mathbb{Z}$ (with semidirect product group law as in Thm 2.2.1) is realizable as Galois group over $\mathbb{Q}$.

Proof. Consider $H = \{x \in \mathrm{GL}_2(\mathbb{F}_p) \mid det(x) \text{ is a square in } \mathbb{F}_p^\times\}$, which is the unique index-2 subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$ by Corollary 2.1.1.1. We have $\mathrm{SL}_2(\mathbb{F}_p) \subset H \subset \mathrm{GL}_2(\mathbb{F}_p)$. Let $h \in H$ and $det(h) = \Delta_h^2$. Then $h = \Delta_h I \Delta_h^{-1} h$ where $\Delta_h I \in Z(\mathrm{GL}_2(\mathbb{F}_p))$ and $\Delta_h^{-1} h \in \mathrm{SL}_2(\mathbb{F}_p)$. Hence $PH \cong \mathrm{PSL}_2(\mathbb{F}_p)$ where isomorphism is given by the map sending $hZ(\mathrm{GL}_2(\mathbb{F}_p))$ to $(\Delta_h^{-1}h)Z(\mathrm{SL}_2(\mathbb{F}_p))$. Since H is the unique index-2 subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ containing $Z(\mathrm{GL}_2(\mathbb{F}_p))$, we have that $PH \cong \mathrm{PSL}_2(\mathbb{F}_p)$ is the unique index-2 subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ by one to one correspondence between subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ containing $Z(\mathrm{GL}_2(\mathbb{F}_p))$ and subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$.

We have $p > 3$. Let $r \neq p-1$ be a non-square element in $\mathbb{F}_p$. Consider $x = \begin{pmatrix} 1 & r+1 \\ -1 & -1 \end{pmatrix} \notin H$ with $x^2 = 1$ $(Z(\mathrm{GL}_2(\mathbb{F}_p)))$.

From Corollary 2.3.3.1 of Thm 2.3.3 for $\mathrm{PGL}_2(\mathbb{F}_p)$, we get E_1, E_2 satisfying conditions of Thm 2.2.1 for $l = 2$ with $G_1 = G_2 = \mathrm{PGL}_2(\mathbb{F}_p)$, and $[G_1 : H_1] = 2$. Therefore $H_1 = H_2 = \mathrm{PSL}_2(\mathbb{F}_p)$. We observe that $\{1, xZ(\mathrm{GL}_2(\mathbb{F}_p))\}$ is required set of representatives of $\mathrm{PSL}_2(\mathbb{F}_p)$-coset in $\mathrm{PGL}_2(\mathbb{F}_p)$. □

Corollary 2.4.2.1. *For a prime $p \geq 5$, $\mathrm{PSL}_2(\mathbb{F}_p)$ and $\mathrm{PSL}_2(\mathbb{F}_p) \times \mathrm{PSL}_2(\mathbb{F}_p)$ are realizable as Galois groups over $\mathbb{Q}\sqrt{p^*}$.*

Proof. Proof is similar to proof of Corollary 2.4.1.3.

□

Chapter 3

Galois Representations, Right Splitting & Inverse Galois Problem

In this chapter, by using the algebraic operations induction, direct sums and tensor products on Galois representations and right splitting of some exact sequences of groups, we establish occurrence of some groups as Galois groups over $\mathbb{Q}$.

3.1 Induced Galois Representations and Galois groups

Definition 3.1.1. *Let $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ with Krull topology. Let E be a number field and Λ be a prime in its ring of integers $\mathcal{O}$. Let E_Λ be the completion of E with respect to Λ and $\mathcal{O}_\Lambda$ be its ring of integers. Let $\mathbb{F}_\Lambda = \mathcal{O}_\Lambda/\Lambda\mathcal{O}_\Lambda$. (π, V) is called a Galois Representation if*

1. *V is a finite dimensional vector space over E_Λ and*

2. *$\pi : G \to \mathrm{GL}(V)$ is a continuous homomorphism where GL(V) has the topology inherited from the topology of the topological field E_Λ which has the Λ-adic topology.*

Remark 3.1.1.1. *In place of $\mathbb{Q}$, we can have a similar definition for any number field K with $G = \mathrm{Gal}(\bar{K}/K)$.*

Remark 3.1.1.2. *Let $dim_{E_\Lambda}(V) = m$. Now from Prop 9.3.5 in [6], there is a basis of V such that $\pi(G) \subset \mathrm{GL}_m(\mathcal{O}_\Lambda)$ for all $g \in G$. Let us consider the maps $\pi' : G \to \mathrm{GL}_m(\mathbb{F}_\Lambda)$ and $\tilde{\pi} : G \to \mathrm{PGL}_m(\mathbb{F}_\Lambda)$ obtained from π through the quotients maps $\mathcal{O}_\Lambda \to \mathbb{F}_\Lambda$ and $\mathrm{GL}_m(\mathbb{F}_\Lambda) \to \mathrm{PGL}_m(\mathbb{F}_\Lambda)$.*

Definition 3.1.2. *A finite group C is said to be realizable as Galois group over $\mathbb{Q}$ through a Galois Representation (π, V) if $C \cong \mathrm{Image}(\tilde{\pi})$.*

Remark 3.1.2.1. *We have a similar definition for π' in place of $\tilde{\pi}$.*

Let K be a finite extension of $\mathbb{Q}$ contained in $\bar{\mathbb{Q}}$. Then $\bar{K} = \bar{\mathbb{Q}}$. Let $H = \mathrm{Gal}(\bar{K}/K) \subset G$. Let (π, W) be a Galois representation with $dim_{E_\Lambda}(W) = m$.

Let $\sigma = \pi|_H : H \to \mathrm{GL}(W)$. Then $\sigma' : H \to \mathrm{GL}_m(\mathbb{F}_\Lambda)$ and $\tilde{\sigma} : H \to \mathrm{PGL}_m(\mathbb{F}_\Lambda)$ and $\mathrm{Image}(\tilde{\sigma}) = \tilde{\pi}(H)$. Also, $[\tilde{\pi}(G) : \tilde{\pi}(H)] \leq [G : H]$.

Let us consider the induced representation $\rho = Ind_H^G(\sigma)$ on the induced space over E_Λ, defined by

$$V = \{f : G \to W \mid f(hg) = \sigma(h)f(g) \; for \; all \; h \in H, g \in G\}$$

and $\rho : G \to \mathrm{GL}(V)$ is given by $\rho(g)f(x) = f(xg)$, for all $g, x \in G, f \in V$. Thus (ρ, V) is a Galois representation.

Let $\{s_i\}_{1 \leq i \leq n}$ be a set of representatives of right cosets in $H\backslash G$ and $\{w_j\}_{1 \leq j \leq m}$ be a basis of W. Then we know that $\{\phi_{s_i,w_j}\}_{1 \leq i \leq n, 1 \leq j \leq m}$ is a basis for V where

$$\phi_{s,w}(g) = \begin{cases} \sigma(gs^{-1})w, & \text{if } gs^{-1} \in H \\ 0 & \text{otherwise.} \end{cases}$$

and $dim(V) = dim(W)[G : H]$.

Let H be a normal subgroup of G (i.e., K is Galois over $\mathbb{Q}$) such that $[G : H] = n$. Since $dim(W) = m$, we have $dim(V) = mn$. Without loss of generality, let $s_1 = 1$. We label the basis of V as

$$f_1 = \phi_{1,w_1}, \;\; f_2 = \phi_{1,w_2}, \;\; \ldots, \;\; f_m = \phi_{1,w_m},$$
$$f_{m+1} = \phi_{s_2,w_1}, \;\; \ldots, \;\; f_{2m} = \phi_{s_2,w_m}, \;\; \ldots,$$
$$f_{(n-1)m+1} = \phi_{s_n,w_1}, \;\; \ldots, \;\; f_{nm} = \phi_{s_n,w_m}.$$

We write down the matrix of $\rho(g)$ with respect to the above basis. Observe that

$$\rho(g)f_i(x) = f_i(xg) = \sum_{j=1}^{mn} a_{ji} f_j(x)$$

By taking $x = s_k$, we get that

$$\rho(g) = \begin{bmatrix} (f_1(g)) & (f_2(g)) & \dots & (f_{nm}(g)) \\ (f_1(s_2g)) & (f_2(s_2g)) & \dots & (f_{nm}(s_2g)) \\ \dots & \dots & \dots & \dots \\ (f_1(s_ng)) & (f_2(s_ng)) & \dots & (f_{nm}(s_ng)) \end{bmatrix}_{nm\times nm}$$

where $(f_i(s_kg))$ are treated as $m \times 1$ column matrices (matrices with respect to given basis $\{w_j : 1 \leq j \leq m\}$ of W).

The $nm \times nm$ matrix for $\rho(hs_i)$: The p, q-th $m \times m$ block where $1 \leq p, q \leq n$ and q is such that $s_ps_i \in s_qH$ is $\pi(s_phs_is_q^{-1})$, since $\phi_{s_q,w}(s_phs_i) = \pi(s_phs_is_q^{-1})w$, since $s_phs_i \in s_qH$.

Since $\pi(G) \subset \mathrm{GL}_m(\mathcal{O}_\Lambda)$, we conclude that $\rho(G) \subset \mathrm{GL}_{nm}(\mathcal{O}_\lambda)$ and $\rho' : G \to \mathrm{GL}_{nm}(\mathbb{F}_\Lambda)$ and $\tilde{\rho} : G \to \mathrm{PGL}_{nm}(\mathbb{F}_\Lambda)$ can be defined.

Remark 3.1.2.2. *All the following results for ρ and π in this section also hold for ρ' and π' as well as $\tilde{\rho}$ and $\tilde{\pi}$.*

Lemma 3.1.3. *Images $\rho(H)$ and $\pi(H)$ are isomorphic.*

Proof. If $g = h \in H$, then

$$\rho(h) = \begin{bmatrix} \pi(h) & 0 & \dots & \\ 0 & \pi(s_2hs_2^{-1}) & & \\ \vdots & & \ddots & \\ & & & \pi(s_nhs_n^{-1}) \end{bmatrix}_{nm\times nm}.$$

Define a map from $\rho(H)$ to $\pi(H)$ by first block projection sending $\rho(h)$ to $\pi(h)$. This is clearly a surjective group homomorphism onto $\pi(H)$. If $\pi(h) = 1$, then $\pi(s_khs_k^{-1}) = \pi(s_k)\pi(h)\pi(s_k)^{-1} = 1$ for all k. Hence, this map is injective too. □

Lemma 3.1.4. *We get an exact sequence*

$$1 \to \rho(H) \to \rho(G) \to G/H \to 1.$$

Proof. If $g = hs_j \in Hs_j$, $(f_{(j-1)m+1}(g)) = \pi(h)w_1, (f_{(j-1)m+2}(g)) = \pi(h)w_2, \ldots, (f_{jm}(g)) = \pi(h)w_m$ and for other k, $(f_k(g)) = 0$. We have

$$\rho(G) = \rho(H) \bigsqcup \rho(Hs_2) \bigsqcup \cdots \bigsqcup \rho(Hs_n) = \rho(H) \bigsqcup \rho(H)\rho(s_2) \bigsqcup \cdots \bigsqcup \rho(H)\rho(s_n)$$

hence $[\rho(G) : \rho(H)] = n$.

Now, since H is normal in G, its left and right cosets coincide. Hence we can define a map $\gamma : \rho(G) \to G/H$ with $\gamma(\rho(hs_k)) = s_kH$ for any h, s_k. Now γ is well defined surjective homomorphism because $\rho(Hs_i)$ for $1 \leq i \leq n$ are disjoint. The kernel of γ is precisely $\rho(H)$. □

Remark 3.1.4.1. *We do not necessarily get a similar exact sequence involving $\pi(H)$, $\pi(G)$ and G/H a similar well defined surjective map from $\pi(G)$ to G/H may not exist since $\pi(Hs_i)$ need not be disjoint.*

Example 3.1.5. *Let G/H be cyclic with representatives of H-cosets in G of the form $\{1, s, s^2, \ldots, s^{n-1}\}$. If $g = hs^i \in H$ for $0 \leq i \leq n-1$, the matrix $\rho(hs^i)$ is given by*

$$\begin{bmatrix}
0 & \cdots & 0 & \pi(h) & 0 & \cdots & \\
\vdots & & & 0 & \pi(shs^{-1}) & 0 & \cdots \\
 & \ddots & & \vdots & & \ddots & \\
 & & & & & & \pi(s^{n-1-i}hs^{-(n-1-i)}) \\
\pi(s^{n-i}hs^i) & & & & & & 0 \\
0 & \pi(s^{n-(i-1)}hs^{(i-1)}) & & & & & \vdots \\
\vdots & 0 & \ddots & & & & \\
 & & 0 & \pi(s^{n-1}hs) & & &
\end{bmatrix}.$$

In particular,

$$\rho(s) = \begin{bmatrix} 0 & I_2 & 0 & \dots & \\ 0 & 0 & I_2 & 0 & \dots \\ \vdots & \vdots & & \ddots & \\ & & & & I_2 \\ \pi(s^n) & & & & 0 \end{bmatrix}.$$

Lemma 3.1.6. *Suppose we have a set of representatives of H-cosets in G, $\{s_1, s_2, \dots, s_n\}$ with $s_1 \in H$, then $\rho(s_i)\rho(s_j) = \rho(s_k) \iff (\pi(s_i)\pi(s_j) = \pi(s_k)$ and $s_i s_j \in s_k H)$.*

Proof. We compute matrices $\rho(s_i), \rho(s_j)$, $\rho(s_k)$ nd $\rho(s_i)\rho(s_j)$.

The p, q-th $m \times m$ block of $\rho(s_i)$ is $\pi(s_p s_i s_q^{-1})$, where $1 \leq p, q \leq n$ and q is such that $s_p s_i \in s_q H$.

The q, r-th $m \times m$ block of $\rho(s_j)$ is $\pi(s_q s_j s_r^{-1})$, where $1 \leq q, r \leq n$ and r is such that $s_q s_j \in s_r H$.

The p, l-th $m \times m$ block of $\rho(s_k)$ is $\pi(s_p s_k s_l^{-1})$, where $1 \leq l \leq n$ and l is such that $s_p s_k \in s_l H$.

The p, r-th $m \times m$ block of $\rho(s_i)\rho(s_j)$ is $\pi(s_p s_i s_q^{-1})\pi(s_q s_j s_r^{-1}) = \pi(s_p s_i s_j s_r^{-1})$.

Since $s_p s_i \in s_q H$, $s_q s_j \in s_r H$, we get $s_p s_i s_j \in s_r H$.

Hence $\rho(s_i)\rho(s_j) = \rho(s_k) \iff (\pi(s_p s_i s_j s_r^{-1}) = \pi(s_p s_k s_l^{-1})$ and $r = l) \iff (\pi(s_i)\pi(s_j) = \pi(s_k)$ and $s_i s_j \in s_k H)$.

□

Remark 3.1.6.1. *$\pi(s_i)$ need not be distinct even though $\rho(s_i)$ are distinct. In fact even if all $\pi(s_i)$ are same, $\rho(s_i)$ will be distinct.*

Corollary 3.1.6.1. *Let G/H be cyclic with representatives of H-cosets in G of the form $\{1, s, s^2, \dots, s^{n-1}\}$. Then $\rho(s)^n = 1$ if and only if $\pi(s)^n = 1$.*

Theorem 3.1.7. *(Bhagwat, Jaiswal) (Thm 3.7 in [4])*

Let G and H be as above, then the exact sequence

$$1 \to \rho(H) \to \rho(G) \to G/H \to 1$$

is right split (that is $\rho(G) \cong \rho(H) \rtimes G/H$ for some semidirect product group law) if and only if there exists a set of representatives of H-cosets in G, $\{s_1, s_2, \ldots, s_n\}$ with $s_1 \in H$ such that $\{\rho(s_i)\}_i$ forms a multiplicatively closed subset of $\rho(G)$. (In fact it is a subgroup with same group structure as $\{s_iH\}_i = G/H$)

Proof. Let $\{r_1, r_2, ..., r_n\}$ be a set of representatives of H-cosets in G. If the exact sequence is right split, let ι be splitting with $\gamma \circ \iota = id_{G/H}$. Hence $\gamma \circ \iota(r_iH) = r_iH$ for each i. Thus for each i, $\iota(r_iH) = \rho(h_ir_i)$ for some $h_i \in H$. Let $s_i = h_ir_i$ for each i. Hence $\{s_1, s_2, ..., s_n\}$ also forms a set of representatives for H-cosets in G with $s_iH = r_iH$ and $\iota(s_iH) = \rho(s_i)$ for each i. Since ι is a homomorphism, we have $\iota(s_iH)\iota(s_jH) = \iota(s_is_jH)$ for any i, j. Let $s_is_jH = s_kH$ for some k. Hence $\iota(s_iH)\iota(s_jH) = \iota(s_kH)$ that is $\rho(s_i)\rho(s_j) = \rho(s_k)$. Hence $\{\rho(s_i)\}_i$ forms a multiplicatively closed subset of $\rho(G)$.

Conversely, suppose there exists a set of representatives of H-cosets in G, $\{s_1, s_2, \ldots, s_n\}$ with $s_1 \in H$ and $\{\rho(s_i)\}_i$ forming a multiplicatively closed subset of $\rho(G)$. Let $i \neq 1$. Then $\rho(s_1)\rho(s_i) = \rho(s_k)$ for some k. Hence, $\rho(s_1s_i) = \rho(s_k)$. Since $s_1 \in H$, we have $s_1s_i \in s_iH$. Hence by matrix calculation done above, $\rho(s_1s_i) = \rho(s_k)$ is not true unless $k = i$. Hence $\rho(s_1)\rho(s_i) = \rho(s_i)$. Thus $\rho(s_1) = 1$. For any i, consider the set $\{\rho(s_j)\rho(s_i)\}_j$ which is a permutation of the set $\{\rho(s_j)\}_j$. Hence there is a j such that $\rho(s_j)\rho(s_i) = 1$. Hence $\{\rho(s_i)\}_i$ forms a subgroup of $\rho(G)$.

Now by assumption $\rho(s_i)\rho(s_j) = \rho(s_l)$ for some l. Hence $\rho(s_is_j) = \rho(s_l)$. Suppose $s_iHs_jH = s_is_jH = s_kH$. Then by matrix calculation done above, $\rho(s_is_j) = \rho(s_l)$ is not true unless $l = k$. Hence $\rho(s_is_j) = \rho(s_k)$. Hence $\{\rho(s_i)\}_i$ is a group with the same group structure as $\{s_iH\}_i = G/H$.

Then we can define $\iota(s_iH) = \rho(s_i)$. Hence, $\iota(s_iH)\iota(s_jH) = \rho(s_i)\rho(s_j) = \rho(s_k) = \iota(s_kH) = \iota(s_iHs_jH)$. Hence ι is a homomorphism. Also, $\gamma(\iota(s_iH)) = \gamma(\rho(s_i)) = s_iH$ hence $\gamma \circ \iota = id_{G/H}$. Hence the exact sequence is right split. □

Remark 3.1.7.1. *We can similarly prove Remark 2.2.1.1 in previous section.*

Corollary 3.1.7.1. *If there exists a set of coset representatives of H in G which forms a multiplicatively closed set, then the above exact sequence is right split.*

Corollary 3.1.7.2. *Let K be a cyclic extension of $\mathbb{Q}$ and let G and H be as above. Then the above exact sequence is right split if and only if there exists a set of representatives of H-cosets in G of the form $\{1, s, s^2, \ldots, s^{n-1}\}$ with $\rho(s)^n = 1$. Also, if these statements are true then $order(\rho(s)) = n$ and $s^n \in H$.*

Proof. From the above theorem, we get coset representatives of H, $\{s_i\}_i$ with $\{\rho(s_i)\}_i$ forming a subgroup with same group structure as $\{s_iH\}_i = G/H =< sH >$ for some $s \in G$ with $s_1 \in H$. Hence without loss of generality, let $s_iH = s^{i-1}H$ for all i. Now let $r_i = s_2^{i-1}$. Hence $r_iH = s_iH$. Now since $s_2^nH = (s_2H)^n = H$, we have $\tilde{\rho}(s_2)^n = 1$. Hence we are done. Other assertions are clear.

□

Applying above discussion to $\tilde{\rho}$ and $\tilde{\pi}$ we have the following.

Theorem 3.1.8. *(Bhagwat, Jaiswal) (Thm 3.8 in [4])*

Let H be a finite index normal subgroup of $G = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. Suppose there exists a set of coset representatives of H in G which form a multiplicatively closed subset of G. Then if a finite group M is realizable as a Galois group over $\mathbb{Q}$ through a Galois Representation (π, W) such that $M \cong \tilde{\pi}(G) = \tilde{\pi}(H)$, then $M \rtimes G/H$ is realizable as a Galois group over $\mathbb{Q}$ (for semidirect product group law as in Thm 3.1.7).

Observation : $G = H \iff ker(\pi) \subset H \; and \; \pi(G) = \pi(H)$.

We can generalize Lemma 3.1.4 and Thm 3.1.7. Consider a closed subgroup H' of G. We have $H'/(H' \cap H) \hookrightarrow G/H$.

Theorem 3.1.9.

1. *We get an exact sequence*

$$1 \to \rho(H' \cap H) \to \rho(H') \to H'/(H' \cap H) \to 1.$$

2. *This exact sequence is right split (that is $\rho(H') \cong \rho(H' \cap H) \rtimes H'/(H' \cap H)$ for some semidirect product group law) if and only if there exists a set of representatives of $(H' \cap H)$-cosets in H', $\{s_1, s_2, \ldots, s_l\}$ with $s_1 \in H' \cap H$ such that $\{\rho(s_i)\}_i$ forms a multiplicatively closed subset of $\rho(H')$.*

3. *$H \subset H'$ if and only if $\rho(H) \subset \rho(H')$ and $ker(\pi) \cap H \subset H'$*

4. *Let $H \subset H'$. Then the exact sequence is*

$$1 \to \rho(H) \to \rho(H') \to H'/H \to 1.$$

If there exists a set of representatives of H-cosets in G, $\{s_1, s_2, \ldots, s_n\}$ with $s_1 \in H$ such that $\{\rho(s_i)\}_i$ forms a multiplicatively closed subset of $\rho(G)$, then this exact sequence is right split. That is $\rho(H') \cong \rho(H) \rtimes H'/H$ for some semidirect product group law.

3.2 Direct Sum / Tensor Product of Representations and Galois Groups

Consider Galois representations $(\pi_i, V_i) : 1 \leq i \leq n$ and their direct sum Galois representation $\pi = \bigoplus_{1 \leq i \leq n} \pi_i : G \to \mathrm{GL}(\bigoplus_{1 \leq i \leq n} V_i)$.

Lemma 3.2.1. *If for each $1 \leq i \leq n$, finite group H_i is realizable as a Galois group over $\mathbb{Q}$ through Galois representation (π_i, V_i) for m_i-dimensional vector spaces V_i over E_Λ, then $\{(\tilde{\pi}_1(g), \ldots, \tilde{\pi}_n(g)) \mid g \in G\} \subset H_1 \times H_2 \times \cdots \times H_n$ is realizable as Galois group over $\mathbb{Q}$.*

Proof. We have $\pi_i : G \to \mathrm{GL}(V_i)$ with $\pi_i(G) \subset \mathrm{GL}_{m_i}(\mathcal{O}_\Lambda)$ and $\tilde{\pi}_i : G \to \mathrm{PGL}_{m_i}(\mathbb{F}_\Lambda)$ such that $H_i \cong \mathrm{Image}(\tilde{\pi}_i)$.

Now the direct sum Galois representation, $\pi(g) = \mathrm{diag}(\pi_1(g), \ldots, \pi_n(g))_{m \times m}$ where $m = m_1 + m_2 + \ldots + m_n$. Hence $\pi(G) \subset \mathrm{GL}_m(\mathcal{O}_\Lambda)$ and $\tilde{\pi} : G \to \mathrm{PGL}_m(\mathbb{F}_\Lambda)$ with $\mathrm{Image}(\tilde{\pi}) \cong \{(\tilde{\pi}_1(g), \ldots, \tilde{\pi}_n(g)) \mid g \in G\} \subset H_1 \times H_2 \times \cdots \times H_n$.

□

We consider the tensor product Galois representation $\Pi = \bigotimes_{1\le i\le n} \pi_i$ of G on $\bigotimes_{1\le i\le n} V_i$.

Proposition 3.2.2. *(Bhagwat, Jaiswal) (Prop 3.15 in [4])*

The groups realized as Galois groups over $\mathbb{Q}$ through Galois representations π and Π are isomorphic, i.e.,

$$\mathrm{Image}(\tilde{\pi}) \cong \mathrm{Image}(\tilde{\Pi}).$$

Proof. Let V_1 and V_2 be finite dimensional vector spaces over a field $\mathbb{F}$ with dimensions m_1 and m_2 respectively. Given $T_i \in \mathrm{GL}(V_i)$ for each $i = 1, 2$, we consider the natural $\mathbb{F}$-linear map $(T_1 \otimes T_2) : V_1 \otimes V_2 \to V_1 \otimes V_2$ that is also invertible.

Fix bases of V_1 and V_2 and the corresponding basis of $V_1 \otimes V_2$. Let A_1, A_2, A be the matrices representing $T_1, T_2, T_1 \otimes T_2$, respectively with respect to these bases. Then

$$A = A_1 \otimes A_2 = \begin{bmatrix} a_{11}A_2 & \dots & a_{1m_1}A_2 \\ \vdots & \ddots & \vdots \\ a_{m_11}A_2 & \dots & a_{m_1m_1}A_2 \end{bmatrix}_{m_1m_2},$$

where $A_1 = \begin{bmatrix} a_{11} & \dots & a_{1m_1} \\ \vdots & \ddots & \vdots \\ a_{m_11} & \dots & a_{m_1m_1} \end{bmatrix}$ and $A_2 = \begin{bmatrix} a'_{11} & \dots & a'_{1m_2} \\ \vdots & \ddots & \vdots \\ a'_{m_21} & \dots & a'_{m_2m_2} \end{bmatrix}$.

If the map $T_1 \otimes T_2$ is given by the scalar multiplication by $\lambda \in \mathbb{F}^\times$, then it follows that $A_i = \mu_i I$ for some scalars $\mu_1, \mu_2 \in \mathbb{F}^\times$ such that $\lambda = \mu_1\mu_2$. Thus the map $T_1 \otimes T_2$ descends to a injective group homomorphism

$$\tilde{\tau} : \mathrm{PGL}(V_1) \times \mathrm{PGL}(V_2) \to \mathrm{PGL}(V_1 \otimes V_2).$$

Let $\mathbb{F} = E_\Lambda$. Then $\Pi(g) = \pi_1(g) \otimes \pi_2(g) \otimes \cdots \otimes \pi_n(g)$. Hence $\Pi(G) \subset \mathrm{GL}_m(\mathcal{O}_\Lambda)$ where $m = m_1m_2 \cdots m_n$ and $\tilde{\Pi} : G \to \mathrm{PGL}_m(\mathbb{F}_\Lambda)$.

Let $\mathbb{F} = \mathbb{F}_\Lambda$. We observe that $\tilde{\tau}((\tilde{\pi}_1(g), \tilde{\pi}_2(g))) = \pi_1(g) \tilde{\otimes} \pi_2(g) = (\pi_1 \tilde{\otimes} \pi_2)(g)$. Hence, $\tilde{\tau}(\{(\tilde{\pi}_1(g), \tilde{\pi}_2(g)) \mid g \in G\}) = \mathrm{Image}(\pi_1 \tilde{\otimes} \pi_2)$. Since $\tilde{\tau}$ is injective, we get $\{(\tilde{\pi}_1(g), \tilde{\pi}_2(g)) \mid g \in G\} \cong \mathrm{Image}((\pi_1 \tilde{\otimes} \pi_2))$.

By induction on n, we get a well defined injective homomorphism from $\mathrm{PGL}(V_1) \times \mathrm{PGL}(V_2) \times \cdots \times \mathrm{PGL}(V_n)$ to $\mathrm{PGL}(\bigotimes_{1 \leq i \leq n} V_i)$ such that $\mathrm{Image}(\tilde{\Pi}) \cong \{(\tilde{\pi}_1(g), \ldots, \tilde{\pi}_n(g)) \mid g \in G\}$. By Lemma 3.2.1 we are done.

□

Proposition 3.2.3. *Suppose for each $1 \leq i \leq n$, finite group H_i is realizable as a Galois group over $\mathbb{Q}$ through Galois representation (π_i, V_i). Let $|H_i| = r_i$. Suppose we have $g_{i1}, \ldots, g_{ir_i} \in G$ for each i, such that for all i, $H_i = \{\tilde{\pi}_i(g_{i1}), \ldots, \tilde{\pi}_i(g_{ir_i})\}$ and such that for each i, $\tilde{\pi}_i(g_{jk}) = 1$ for all $1 \leq k \leq r_j$ and for all $j \neq i$. Then $H_1 \times H_2 \times \cdots \times H_n$ is realizable as Galois group over $\mathbb{Q}$.*

Proof. Any element of $H_1 \times H_2 \times \cdots \times H_n$ is of the form $(\tilde{\pi}_1(g_{1l_1}), \ldots, \tilde{\pi}_n(g_{nl_n}))$ for some $1 \leq l_i \leq r_i$ for each $1 \leq i \leq n$.

Now, $(\tilde{\pi}_1(g_{1l_1}), \ldots, \tilde{\pi}_n(g_{nl_n})) = (\tilde{\pi}_1(g_{1l_1}), 1, \ldots, 1)(1, \tilde{\pi}_2(g_{2l_2}), \ldots, 1) \cdots (1, \ldots, 1, \tilde{\pi}_n(g_{nl_n}))$

$= (\tilde{\pi}_1(g_{1l_1}), \ldots, \tilde{\pi}_n(g_{1l_1}))(\tilde{\pi}_1(g_{2l_2}), \ldots, \tilde{\pi}_n(g_{2l_2})) \cdots (\tilde{\pi}_1(g_{nl_n}), \ldots, \tilde{\pi}_n(g_{nl_n}))$

$= (\tilde{\pi}_1(g_{1l_1} g_{2l_2} \ldots g_{nl_n}), \ldots, \tilde{\pi}_n(g_{1l_1} g_{2l_2} \ldots g_{nl_n})) \in \{(\tilde{\pi}_1(g), \ldots, \tilde{\pi}_n(g)) \mid g \in G\}$.

Hence $\{(\tilde{\pi}_1(g), ..., \tilde{\pi}_n(g)) \mid g \in G\} = H_1 \times H_2 \times \cdots \times H_n$. By Lemma 3.2.1 we are done.

□

Let $L = \{(\pi(g), \rho(g)) | g \in G\}$. Thus $\tilde{L} = \{(\tilde{\pi}(g), \tilde{\rho}(g)) | g \in G\}$ is realizable as a Galois group over $\mathbb{Q}$ through the Galois representation $(\pi \oplus \rho, W \oplus V)$ where ρ is induced representation as before.

Remark 3.2.3.1. *All following results for ρ and π also hold for ρ' and π' as well as $\tilde{\rho}$ and $\tilde{\pi}$.*

Lemma 3.2.4.

1. *The projection $\Psi : L \to \rho(G)$ is an isomorphism.*
2. *The kernel $ker(\Phi)$ of the projection $\Phi : L \to \pi(G)$ is isomorphic to $ker(\pi)/(ker(\pi) \cap H)$ and isomorphic to a subgroup of G/H.*

Proof. (1) If $\rho(g) = I$, then $g \in H$. By matrix of $\rho(g)$, we get $\pi(g) = I$ since $g \in H$. Hence Ψ is also injective.

(2) Suppose $\pi(h_i s_i) = \pi(h_j s_j) = I_m$ for some $h_i, h_j \in H$. Then in the matrix of $\rho(h_i s_i)$, the p, q-th $m \times m$ block matrix, where $1 \leq p, q \leq n$ and q is such that $s_p s_i \in s_q H$, is $\pi(s_p s_q^{-1})$. Hence it is independent of $h_i \in H$. Let $\rho(h_i s_i) = \theta_i$. Similarly, $\rho(h_j s_j) = \theta_j$.

Let $s_i s_j H = s_k H$ for some k, that is $s_i s_j = h s_k$ for some $h \in H$. Now, $\pi(h_i s_i)\pi(h_j s_j) = \pi(h_i s_i h_j s_j) = \pi(h_i h'_j s_i s_j)$ where $s_i h_j = h'_j s_i$ since H is normal in G. Hence $\pi(h_i s_i)\pi(h_j s_j) = \pi(h_i h'_j h s_k)$. Let $h_k = h_i h'_j h$. Hence $\pi(h_i s_i)\pi(h_j s_j) = \pi(h_k s_k)$. Similarly, $\rho(h_i s_i)\rho(h_j s_j) = \rho(h_k s_k)$.

Hence $\pi(h_k s_k) = I_m$ for above h_k. Let $\rho(h_k s_k) = \theta_k$. Then $\theta_i \theta_j = \theta_k$. Hence $\{\theta_i\}_{1 \leq i \leq n}$ form a group with same group law as $\{(s_i H)\}_{1 \leq i \leq n}$. Also, for any i, $\rho(h_i s_i) = \theta_i$ if and only if $\pi(h_i s_i) = I_m$. Let $J = \{i \in \{1, 2, ..., n\} \mid ker(\pi) \cap H s_i \neq \emptyset\}$. Hence $ker(\Phi) = \{(I, \theta_i)\}_{i \in J}$. Thus we have $\Omega : ker(\Phi) \hookrightarrow G/H$ sending (I, θ_i) to $s_i H$.

Now, since $H \trianglelefteq G$, we have $(ker(\pi) \cap H) \trianglelefteq ker(\pi)$. We also have usual maps $ker(\pi) \hookrightarrow G \to G/H$. Hence $ker(\pi)/(ker(\pi) \cap H) \hookrightarrow G/H$. Since $G = \bigsqcup_{1 \leq i \leq n} H s_i$, we have $ker(\pi) = \bigsqcup_{i \in J}(ker(\pi) \cap H s_i)$. Now for $i \in J$ there exists an $h_i \in H$ such that $\pi(h_i s_i) = I_m$. Hence for $i \in J$, it is easy to see that, $(ker(\pi) \cap H s_i) = (ker(\pi) \cap H)(h_i s_i)$. Hence $ker(\pi) = \bigsqcup_{i \in J}(ker(\pi) \cap H) h_i s_i$. Thus $ker(\pi)/(ker(\pi) \cap H) \cong \{(s_i H)\}_{i \in J} \cong ker(\Phi)$. □

Example 3.2.5. *Let G/H be cyclic with representatives of H-cosets in G of the form $\{1, s, s^2, \ldots, s^{n-1}\}$. Suppose $\pi(h s^i) = I_m$. Then,*

$$\rho(h s^i) = \begin{bmatrix} 0 & \cdots & & 0 & \pi(s^{-i}) & 0 & \cdots & \\ \vdots & & & & 0 & \pi(s^{-i}) & 0 & \cdots \\ & \ddots & & & \vdots & & \ddots & \\ & & & & & & & \pi(s^{-i}) \\ \pi(s^{n-i}) & & & & & & & 0 \\ 0 & \pi(s^{n-i}) & & & & & & \vdots \\ \vdots & 0 & \ddots & & & & & \\ & & 0 & \pi(s^{n-i}) & & & & \end{bmatrix} = \theta^i.$$

Corollary 3.2.5.1. $\tilde{L} \cong \tilde{\pi}(G) \iff ker(\tilde{\pi}) \subset H$.

Proof. Now $\tilde{L}/ker(\tilde{\Phi}) \cong \tilde{\pi}(G)$ where $\tilde{\Phi} : \tilde{L} \to \tilde{\pi}(G)$ is the projection map. Since $\tilde{L}$ is finite group, we have $\tilde{L} \cong \tilde{\pi}(G) \iff ker(\tilde{\Phi})$ is trivial $\iff ker(\tilde{\pi}) = (ker(\tilde{\pi}) \cap H) \iff ker(\tilde{\pi}) \subset H$.

□

We have remarked earlier (Lemma 3.2.4) that $ker(\Phi) \hookrightarrow G/H$ via an injective homomorphism say Ω. Let G' be the unique subgroup of G such that $H \subset G' \subset G$ and $ker(\Phi) = G'/H$.

In fact, we have a more precise statement.

Lemma 3.2.6. *Let $H \subset G' \subset G$. Then*

$ker(\Phi) = G'/H$ under $\Omega \iff G'$ is the largest subgroup of G such that $\pi(G') = \pi(H)$.

In particular, $ker(\Phi) = G/H$ under $\Omega \iff \pi(G) = \pi(H)$.

Proof. Now $H \subset G' \subset G$. Since $G = \bigsqcup_{1 \le i \le n} Hs_i$, we have $G' = \bigsqcup_{i \in I}(G' \cap Hs_i)$ where $I = \{i \in \{1, 2, ..., n\} \mid G' \cap Hs_i \neq \emptyset\}$. Since $H \subset G'$, we have $(G' \cap Hs_i) \neq \emptyset \iff s_i \in G'$. Hence $I = \{i \in \{1, 2, ..., n\} \mid s_i \in G'\}$. Now for $i \in I$, it is easy to see that, $(G' \cap Hs_i) = (G' \cap H)(s_i) = Hs_i$. Hence $G' = \bigsqcup_{i \in I} Hs_i$ and $G'/H = \{s_iH\}_{i \in I}$. Now the following argument completes the proof.

$$
\begin{aligned}
& ker(\Phi) = G'/H \text{ under } \Omega \\
\iff & \{s_iH\}_{i \in J} = \{s_iH\}_{i \in I}, \text{that is } I = J \\
\iff & s_i \in G' \text{ iff } ker(\pi) \cap Hs_i \neq \emptyset. \\
\iff & s_i \in G' \text{ iff there is } h_i \in H \text{ such that } \pi(h_is_i) = I. \\
\iff & s_i \in G' \text{ iff } \pi(s_i) \in \pi(H) \\
\iff & g \in G' \text{ iff } \pi(g) \in \pi(H) \\
\iff & G' \text{ is the largest subgroup of } G \text{ such that } \pi(G') = \pi(H).
\end{aligned}
$$

□

Theorem 3.2.7. *(Bhagwat, Jaiswal) (Thm 3.19 in [4])*

Suppose $\pi(G) = \pi(H)$. *Then the exact sequence*

$$1 \to ker(\Phi) \hookrightarrow L \to \pi(G) \to 1$$

is right split. $L \cong \pi(G) \ltimes G/H$ *for some semidirect product group law.*

Proof. Since $\pi(G) = \pi(H)$, $ker(\Phi) = G/H$ under Ω.

Consider $\iota : \pi(G) \to L$ given by $\iota(x) = (\pi(h), \rho(h))$ where $x = \pi(h)$ for some $h \in H$.

If $x = \pi(h) = \pi(h')$ for some $h, h' \in H$ then $\pi(hh'^{-1}) = I$. Hence by matrix calculation above, $\rho(hh'^{-1}) = I$. Hence $\rho(h) = \rho(h')$. Thus ι is well defined.

Now, for $x, y \in \pi(G)$, let $h, h' \in H$ such that $x = \pi(h), y = \pi(h')$. Then

$$\iota(x)\iota(y) = (\pi(h), \rho(h))(\pi(h'), \rho(h')) = (\pi(hh'), \rho(hh')) = \iota(\pi(hh')) = \iota(\pi(h)\pi(h')) = \iota(xy).$$

Hence ι is a homomorphism. Also since, $\Phi \circ \iota = id_{\tilde{\pi}(G)}$, the exact sequence splits.

□

Corollary 3.2.7.1. *Let* G/H *be cyclic* $< sH >$. *Then if* $ker(\pi) \cap Hs \neq \emptyset$ *then the above exact sequence is right split.*

Proof. Since $ker(\pi) \cap Hs \neq \emptyset$, there is an $h_1 \in H$ such that $\pi(h_1 s) = 1$. Since H is normal in G, $(h_1 s)^i = h_i s^i$ for some $h_i \in H$. Hence $\pi(h_i s^i) = \pi(h_1 s)^i = 1$. Hence for all i, $ker(\pi) \cap Hs^i \neq \emptyset$. Thus $ker(\Phi) \cong G/H$.

□

Corollary 3.2.7.2. *Let* $\{\rho(s_i)\}_i$ *form a multiplicatively closed subset of* $\rho(G)$ *and let* $(n, |\pi(G)|) = 1$. *Then above exact sequence is right split.*

Proof. Since $|G/H| = n$, for any i, $(s_iH)^n = H$. Thus $\rho(s_i)^n = I$. Hence $\pi(s_i)^n = I$. Since $\pi(s_i) \in \pi(G)$, we have $\pi(s_i)^{|\pi(G)|} = I$. Now $(n, |\pi(G)|) = 1$. Hence, $\pi(s_i) = 1$ for all i. Thus $\pi(H) = \pi(G)$. □

We can generalize Lemma 3.2.4, Corollary 3.2.5.1, Lemma 3.2.6 and Thm 3.2.7. Consider a closed subgroup H' of G. We have $H'/(H' \cap H) \hookrightarrow G/H$.

Theorem 3.2.8. *Let* $N = \{(\pi(h'), \rho(h'))|h' \in H'\}$ *and* $\tilde{N} = \{(\tilde{\pi}(h'), \tilde{\rho}(h'))|h' \in H'\}$.

1. *The surjective projection* $N \to \rho(H')$ *is an isomorphism.*
2. *Consider the surjective projection* $\xi : N \to \pi(H')$. *We have* $\omega : ker(\xi) \hookrightarrow H'/(H' \cap H)$ *and* $ker(\xi) \cong (ker(\pi) \cap H')/(ker(\pi) \cap H' \cap H)$.
3. $\tilde{N} \cong \tilde{\pi}(H') \iff ker(\tilde{\pi}) \cap H' \subset H$.
4. *Let* $(H' \cap H) \subset G' \subset H'$ *then*
   $ker(\xi) = G'/(H' \cap H)$ *under* $\omega \iff G'$ *is largest subgroup of* H' *such that* $\pi(G') = \pi(H' \cap H)$.
   In particular, $ker(\xi) = H'/(H' \cap H)$ *under* $\omega \iff \pi(H') = \pi(H' \cap H)$.
5. *Suppose* $\pi(H') = \pi(H' \cap H)$. *Then the exact sequence*
   $$1 \to ker(\xi) \to N \to \pi(H') \to 1$$
   is right split. $N \cong \pi(H') \ltimes H'/(H' \cap H)$ *for some semidirect product group law.*
6. *Let* $H \subset H'$. *Suppose* $\pi(G) = \pi(H)$. *Then the above exact sequence is right split.* $N \cong \pi(H') \ltimes H'/H$ *for some semidirect product group law.*

3.3 Cases of IGP in work of Zywina

Using the results of Ribet [19] about the Deligne's Galois representations associated to certain newforms, Zywina established the IGP for $PSL_2(F_p)$ over $\mathbb{Q}$ for all primes $p \geq 5$. (For a discussion on newforms refer to 16.8 in [21]).

It is easy to prove IGP directly for the group $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$ over $\mathbb{Q}$. So for the other cases, Zywina considered a non-CM newform $f = \sum_{n=1}^{\infty} a_n q^n$ on $\Gamma_1(N)$ of weight $k = 3$, level $N = 27$ and nebentypus $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ with $\varepsilon(a) = \left(\frac{-3}{a}\right)$ where the a_n are complex numbers and $q = e^{2\pi i\tau}$ with τ a variable of the complex upper-half plane. He chose f so that

$$f = q + 3iq^2 - 5q^4 - 3iq^5 + 5q^7 - 3iq^8 + 9q^{10} - 15iq^{11} - 10q^{13} + \cdots;$$

the other possibility for f is its complex conjugate $\sum_n \bar{a}_n q^n$.

The subfield E of $\mathbb{C}$ generated by the coefficients a_n is $\mathbb{Q}(\iota)$. All the a_n are known to lie in E's ring of integers $\mathcal{O}$ which is $\mathbb{Z}[\iota]$. The subfield K of E generated by the algebraic integers $r_p := a_p^2/\varepsilon(p)$ for primes $p \nmid N$ is $\mathbb{Q}$; and its ring of integer R is $\mathbb{Z}$ and we also have $L = \mathbb{Q}$ where $L \subseteq \mathbb{C}$ is the extension of K generated by the square roots of the values $r_p = a_p^2/\varepsilon(p)$ with $p \nmid N$.

Take any non-zero prime ideal Λ of $\mathcal{O}$ and denote by $\ell = \ell(\Lambda)$ the rational prime lying under Λ. Let E_Λ and $\mathcal{O}_\Lambda$ be the completions of E and $\mathcal{O}$, respectively, at Λ. There is a continuous representation $\pi_\Lambda\colon G \to \mathrm{GL}_2(\mathcal{O}_\Lambda)$ such that for each prime $p \nmid N\ell$, the representation π_Λ is unramified at p and satisfies $tr(\pi_\Lambda(Frob_p)) = a_p$ & $\det(\pi_\Lambda(Frob_p)) = \varepsilon(p)p^{k-1}$.

The representation π_Λ is uniquely determined by the above conditions up to conjugation by an element of $\mathrm{GL}_2(E_\Lambda)$. By composing ρ_Λ with the natural projection arising from the reduction map $\mathcal{O}_\Lambda \to \mathbb{F}_\Lambda := \mathcal{O}/\Lambda$, we obtain representation $\pi'_\Lambda\colon G \to \mathrm{GL}_2(\mathbb{F}_\Lambda)$. Composing π'_Λ with the natural quotient map $\mathrm{GL}_2(\mathbb{F}_\Lambda) \to \mathrm{PGL}_2(\mathbb{F}_\Lambda)$, we obtain a homomorphism $\tilde{\pi}_\Lambda\colon G \to \mathrm{PGL}_2(\mathbb{F}_\Lambda)$. Define the field $\mathbb{F}_\lambda := R/\lambda$, where $\lambda := \Lambda \cap R$. The natural injective homomorphisms $\mathrm{PSL}_2(\mathbb{F}_\lambda) \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_\lambda) \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_\Lambda)$ and $\mathrm{PSL}_2(\mathbb{F}_\Lambda) \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_\Lambda)$ are viewed as inclusions.

The following is a general result of Ribet [19].

Theorem 3.3.1. *(Ribet)*

There is a finite set S of non-zero prime ideals of R such that if Λ is a non-zero prime ideal of $\mathcal{O}$ with $\lambda := R \cap \Lambda \notin S$, then the group $\tilde{\pi}_\Lambda(G)$ is conjugate in $\mathrm{PGL}_2(\mathbb{F}_\Lambda)$ to either $\mathrm{PSL}_2(\mathbb{F}_\lambda)$ or $\mathrm{PGL}_2(\mathbb{F}_\lambda)$.

Zywina verified that above general theorem holds with $S = \{2, 3, 5\}$ for the case he has considered. The following is a part of a general result Thm 1.2 of Zywina [23].

Theorem 3.3.2. *(Zywina)*

Let Λ be a non-zero prime ideal of $\mathcal{O}$ such that $\tilde{\pi}_\Lambda$ is conjugate to $\mathrm{PSL}_2(\mathbb{F}_\lambda)$ or $\mathrm{PGL}_2(\mathbb{F}_\lambda)$, where $\lambda = \Lambda \cap R$. After conjugating π'_Λ, we may assume that $\tilde{\pi}_\Lambda(G) \subseteq \mathrm{PGL}_2(\mathbb{F}_\lambda)$. Let ℓ be the rational prime lying under Λ. If weight k is odd, then $\tilde{\pi}_\Lambda(G) = \mathrm{PSL}_2(\mathbb{F}_\lambda)$ if and only if λ splits completely in L.

By taking any prime $\ell \geq 7$ and prime $\Lambda \subseteq \mathbb{Z}[i]$ dividing ℓ. Since in the case that Zywina has considered, $L = K = \mathbb{Q}$ and λ splits completely in L, $\tilde{\pi}_\Lambda(G)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_\ell)$.

The following is Thm 1.4 in [23].

Theorem 3.3.3. *(Zywina)*

$\mathrm{PSL}_2(\mathbb{F}_p)$ can be realized as a Galois group over $\mathbb{Q}$ for all primes $p \geq 5$.

3.4 New Cases of IGP through the Cases in work of Zywina and Galois Representations for Newforms

Consider the case in previous section with $\pi = \pi_\Lambda$, $p = l \geq 5$ and $W = E_\Lambda^2$ and $\pi : G \to \mathrm{GL}(W)$ with $\pi(G) \subset \mathrm{GL}_2(\mathcal{O}_\Lambda)$ and $\tilde{\pi} : G \to \mathrm{PGL}_2(\mathbb{F}_\Lambda)$. Then $\mathrm{Image}(\tilde{\pi}) = \tilde{\pi}(G) = \mathrm{PSL}_2(\mathbb{F}_p)$. The representations $\sigma = \pi|_H : H \to \mathrm{GL}(W)$ and $\tilde{\sigma} : H \to \mathrm{PGL}_2(\mathbb{F}_\Lambda)$ are defined, and $\mathrm{Image}(\tilde{\sigma}) = \tilde{\pi}(H) \subset \tilde{\pi}(G)$.

Lemma 3.4.1. *Let $p \geq 5$ and H be normal in G (K is Galois) and $[G : H] = n < |\mathrm{PSL}_2(\mathbb{F}_p)|$. Then $\tilde{\pi}(H) = \mathrm{PSL}_2(\mathbb{F}_p)$.*

Proof. Now, $[\mathrm{PSL}_2(\mathbb{F}_p) : \tilde{\pi}(H)] = [\tilde{\pi}(G) : \tilde{\pi}(H)] \leq [G : H] = n < |\mathrm{PSL}_2(\mathbb{F}_p)|$. Hence $\tilde{\pi}(H)$ is not trivial. Since H is normal in G, $\tilde{\pi}(H)$ is normal in $\tilde{\pi}(G)$. Now since $\mathrm{PSL}_2(\mathbb{F}_p)$ is simple we have that $\mathrm{PSL}_2(\mathbb{F}_p) = \tilde{\pi}(H)$ otherwise $\tilde{\pi}(H)$ will become non-trivial normal subgroup in $\mathrm{PSL}_2(\mathbb{F}_p)$.

□

Remark 3.4.1.1. *If $n \geq |\mathrm{PSL}_2(\mathbb{F}_p)|$ then either $\tilde{\pi}(H) = \mathrm{PSL}_2(\mathbb{F}_p)$ or $\tilde{\pi}(H)$ is trivial. If latter case happens, then $\tilde{\rho}(H)$ is also trivial. Hence $\tilde{\rho}(G) \cong G/H$ in that case.*

Proposition 3.4.2.

1. *For $p \geq 5$, $\mathrm{PGL}_2(\mathbb{F}_p) \cong \mathrm{PSL}_2(\mathbb{F}_p) \rtimes \mathbb{Z}/2\mathbb{Z}$ for some semidirect product group law and the semidirect product is not direct product.*
2. *Let $p \geq 5$. For any semidirect product group law such that $\mathrm{PGL}_2(\mathbb{F}_p) \cong \mathrm{PSL}_2(\mathbb{F}_p) \rtimes \mathbb{Z}/2\mathbb{Z}$, the semidirect product is not direct product. Furthermore, the automorphism of $\mathrm{PSL}_2(\mathbb{F}_p)$, given by conjugation by image of generator of $\mathbb{Z}/2\mathbb{Z}$ in $\mathrm{PGL}_2(\mathbb{F}_p)$, is not inner.*

Proof. (1) From proof of Prop 2.4.2, we have an exact sequence

$$1 \to \mathrm{PSL}_2(\mathbb{F}_p) \to \mathrm{PGL}_2(\mathbb{F}_p) \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

Let $\iota : \mathbb{Z}/2\mathbb{Z} \to \mathrm{PGL}_2(\mathbb{F}_p)$ be given by $\iota(\bar{1}) = xZ(\mathrm{GL}_2(\mathbb{F}_p))$ where x is as in Prop 2.4.2. ι is a right splitting. Hence above exact sequence is right split. Hence $\mathrm{PGL}_2(\mathbb{F}_p) \cong \mathrm{PSL}_2(\mathbb{F}_p) \rtimes \mathbb{Z}/2\mathbb{Z}$ for some semidirect product group law. Now since, $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} Z(\mathrm{GL}_2(\mathbb{F}_p)) \in PH$ doesn't commute with $xZ(\mathrm{GL}_2(\mathbb{F}_p))$, the semidirect product is not direct product.

(2) Let $xZ(\mathrm{GL}_2(\mathbb{F}_p))$ be the image of generator of $\mathbb{Z}/2\mathbb{Z}$ in $\mathrm{PGL}_2(\mathbb{F}_q)$ for $x \in \mathrm{GL}_2(\mathbb{F}_p)$. Then $x \notin H$, $xZ(\mathrm{GL}_2(\mathbb{F}_p)) \notin PH$ and $x^2 \in Z(\mathrm{GL}_2(\mathbb{F}_p))$. Suppose the semidirect product was direct product. Then for some $\nu_h \in Z(\mathrm{GL}_2(\mathbb{F}_p))$, $xhx^{-1} = h\nu_h$ for all $h \in H$. Now, $\mathrm{PGL}_2(\mathbb{F}_p) = PH \bigsqcup (xZ(\mathrm{GL}_2(\mathbb{F}_p)))PH$. Hence, $xZ(\mathrm{GL}_2(\mathbb{F}_p)) \in Z(\mathrm{PGL}_2(\mathbb{F}_p)) = \{1\}$. Hence $x \in H$, which gives a contradiction.

Now, suppose automorphism of $\mathrm{PSL}_2(\mathbb{F}_p)$, given by conjugation by $xZ(\mathrm{GL}_2(\mathbb{F}_p))$, is inner. Then for some $h' \in H$ and $\mu_h \in Z(\mathrm{GL}_2(\mathbb{F}_p))$, $xhx^{-1} = h'hh'^{-1}\mu_h$ for all $h \in H$. Hence $(h'^{-1}x)h(h'^{-1}x)^{-1} = h\mu_h$ for all $h \in H$. Now, $\mathrm{PGL}_2(\mathbb{F}_p) = PH \bigsqcup ((h'^{-1}x)Z(\mathrm{GL}_2(\mathbb{F}_p)))PH$. Hence, $(h'^{-1}x)Z(\mathrm{GL}_2(\mathbb{F}_p)) \in Z(\mathrm{PGL}_2(\mathbb{F}_p)) = \{1\}$. Hence $x \in H$, which gives a contradiction.

□

Theorem 3.4.3. *(Bhagwat, Jaiswal) (Thm 3.12 in [4])*

1. *For $p \geq 5$, $\mathrm{PSL}_2(\mathbb{F}_p) \rtimes \mathbb{Z}/2\mathbb{Z}$ is realizable as Galois Group over $\mathbb{Q}$ (for semidirect product group law in Thm 3.1.7).*
2. *This semidirect product in part (1) is direct $\iff \tilde{\pi}(s) = I$.*
3. *Automorphism $\phi_{\tilde{\rho}(s)}$ of $\tilde{\rho}(H)$, by conjugation by $\tilde{\rho}(s)$, is inner.*
4. *The group obtained here is not isomorphic to $\mathrm{PGL}_2(\mathbb{F}_p)$.*

Proof. (1) Let $[G : H] = 2$. Then H is normal in G (K is Galois). Also $2 < |\mathrm{PSL}_2(\mathbb{F}_p)|$. Hence by previous lemma, $\tilde{\pi}(H) = \mathrm{PSL}_2(\mathbb{F}_p)$.

We could have chosen $K = \mathbb{Q}(i)$ and $s \in G$ as complex conjugation so that $s^2 = 1$ and $\{1, s\}$ become representatives of right cosets of H in G. Then by Thm 3.1.8 we are done.

(2) Now, $\tilde{\pi}(G) = \tilde{\pi}(H) = \mathrm{PSL}_2(\mathbb{F}_p)$.

Above semidirect product is direct.

$\iff \tilde{\rho}(s) = \begin{bmatrix} 0 & I_2 \\ I_2 & 0 \end{bmatrix}$ commutes with every $\tilde{\rho}(h) = \begin{bmatrix} \tilde{\pi}(h) & 0 \\ 0 & \tilde{\pi}(shs^{-1}) \end{bmatrix}$.

$\iff \tilde{\pi}(s)$ commutes with every $\tilde{\pi}(h)$.

$\iff \tilde{\pi}(s) \in Z(\mathrm{PSL}_2(\mathbb{F}_p))$.

$\iff \tilde{\pi}(s) = I$.

Since $Z(\mathrm{PSL}_2(\mathbb{F}_p))$ is trivial as $\mathrm{PSL}_2(\mathbb{F}_p)$ is non-abelian and simple.

(3) Now $\tilde{\pi}(G) = \tilde{\pi}(H)$. Hence $\tilde{\pi}(s) = \tilde{\pi}(h')$ for some $h' \in H$.

So, $\phi_{\tilde{\rho}(s)}(\tilde{\rho}(h)) = \tilde{\rho}(s)\tilde{\rho}(h)\tilde{\rho}(s)^{-1} = \begin{bmatrix} \tilde{\pi}(shs^{-1}) & 0 \\ 0 & \tilde{\pi}(h) \end{bmatrix} = \tilde{\rho}(h')\tilde{\rho}(h)\tilde{\rho}(h')^{-1}$.

(4) This follows from (3) and Prop 3.4.2.

□

We have results similar to (1), (2) and (3) of Thm 3.4.3 for certain simple groups of the form $\mathrm{PSL}_2(\mathbb{F}_q)$.

Theorem 3.4.4. *$\mathrm{PSL}_2(\mathbb{F}_q) \rtimes \mathbb{Z}/2\mathbb{Z}$ is realizable as Galois Group over $\mathbb{Q}$ (for semidirect product group law in Thm 3.1.7) for following q.*

1. *$q = p$ for $p \geq 5$ (From 1.2 [23]).*
2. *$q = p^2$ for $p \equiv \pm 2 \ mod \ 5, \ p \geq 7$ (From Corollary 3.6 [7]).*
3. *$q = p^2$ for $p \equiv \pm 3 \ mod \ 8, \ p \geq 5$ (From Corollary 3.8 [7]).*
4. *$q = p^3$ for odd prime $p \equiv \pm 2, \pm 3, \pm 4, \pm 6 \ mod \ 13$ (From 1.3 [23]).*
5. *$q = 5^3, 3^5, 3^4$ (From 2.2, 2.5, 3 [8] respectively).*

Remark 3.4.4.1. *One has even more general conditions for $q = p^2$ (See Thm 3.1 [9]) and $q = p^4$ (See 3.3 [9]).*

Recall the results from [23] that we discussed earlier. In this case, we have

Proposition 3.4.5. *(Corollary 3.19.3 in [4]). For $p \geq 5$, $\mathrm{PSL}_2(\mathbb{F}_p) \times \mathbb{Z}/2\mathbb{Z}$ is realizable as Galois Group over $\mathbb{Q}$.*

Proof. Since $\tilde{\pi}(H) = \tilde{\pi}(G)$ as in Thm 3.4.3, we have from Thm 3.2.7 that $\mathrm{PSL}_2(\mathbb{F}_p) \ltimes \mathbb{Z}/2\mathbb{Z}$ is realizable as Galois Group over $\mathbb{Q}$ (for semidirect product group law as in 3.2.7). Since $Aut(\mathbb{Z}/2\mathbb{Z})$ is trivial, we have that semidirect product is indeed direct. □

Chapter 4

Root Cluster Size

Perlis proved some properties of cluster size in [17] and [18]. In this chapter, we generalise a result of Perlis for number fields that also improves on the generalisation proved previously by Krithika and Vanchinathan in [13]. We also present a simple lemma about number of clusters which is very useful in giving alternate proofs of results by Perlis and Krithika-Vanchinathan as well as in proving further results.

4.1 Root Clusters in work of Perlis

A perfect field is such that every irreducible polynomial over that field is separable (Equivalently every finite extension of that field is separable). In particular, number fields are perfect.

Let K be a perfect field. We fix an algebraic closure $\bar{K}$ once and for all and work with finite extensions of K contained in $\bar{K}$. All the fields henceforth will be finite extensions of K contained in $\bar{K}$.

Let $f \in K[t]$ be an irreducible polynomial and let α be a root of f in $\bar{K}$. Since K is perfect, it follows that f has $\deg(f)$ distinct roots in $\bar{K}$. The cluster of α is defined as the set of roots of f in the field $K(\alpha)$ and its cardinality $r_K(f)$ is called the cluster size of α over K.

Let K_f be the splitting field of f over K and let $G := \mathrm{Gal}(K_f/K)$. Let $H = \mathrm{Gal}(K_f/K(\alpha))$ be the subgroup of G such that $K(\alpha)$ is the fixed field of H.

Let $s_K(f)$ be the number of distinct fields of the form $K(\alpha_j)$, with α_j a root of f in K_f for all $1 \leq j \leq \deg(f)$.

The following result is proved in [17] and [18].

Theorem 4.1.1. *(Perlis)*

1. $r_K(f)$ *is independent of the choice of* α.
2. $r_K(f)\ s_K(f) = \deg(f)$. *In particular,* $r_K(f) \mid \deg(f)$.
3. $r_K(f) =$ *number of roots of* f *fixed by* $H = |\mathrm{Aut}(K(\alpha)/K)| = [N_G(H) : H]$.

Proof.

1. Let α_i's for $1 \leq i \leq n$ be roots of f in $\bar{K}$. Consider fields $K(\alpha_i)$ for all i. Each of this field is K-isomorphic to $K[x]/(f(x))$. Hence they are K-isomorphic to each other. Since roots map to roots under isomorphism, we have that $r_K(f)$ is independent of the choice of α.

2. Now any root α_j lies in exactly one of the above fields which is precisely $K(\alpha_j)$. This is because, suppose $\alpha_j \in K(\alpha_i)$ then $K(\alpha_j) \subset K(\alpha_i)$. Since both these fields have same degree over K, we have $K(\alpha_j) = K(\alpha_i)$.

   Thus one observes that α_i's are partitioned by corresponding fields $K(\alpha_i)$'s into $s_K(f)$ collections with $r_K(f)$ many in each collection. Therefore $r_K(f)\ s_K(f) = \deg(f)$. In particular, $r_K(f) \mid \deg(f)$.

3. Since $H = \mathrm{Gal}(K_f/K(\alpha))$, the roots of f fixed by H are precisely the roots of f contained in $K(\alpha)$. Hence $r_K(f) =$ number of roots of f fixed by H.

   Now any K-automorphism of $K(\alpha)$ maps α to one of the roots of f contained in $K(\alpha)$. Conversely mapping α to one of the roots of f contained in $K(\alpha)$ gives us a K-automorphism of $K(\alpha)$. Thus $r_K(f) = |\mathrm{Aut}(K(\alpha)/K)|$.

   One can show that the group $\mathrm{Aut}(K(\alpha)/K)$ is isomorphic to $N_G(H)/H$ (See Corollary 7.1.0.2). Thus $r_K(f) = [N_G(H) : H]$.

□

Remark 4.1.1.1. *By the proof of part (2) in above theorem it can be seen that $s_K(f)$ is the number of clusters of roots of f in K_f.*

Let L/K be a finite extension of degree n contained in $\bar{K}$ and $\tilde{L}$ be its Galois closure inside $\bar{K}$. Since K is perfect, by primitive element theorem, $L = K(\alpha)$ with f over K a degree n irreducible polynomial with α as a root in $\bar{K}$. The cluster size of L/K is defined as $r_K(L) := r_K(f)$ which is well defined because of part (3) of Thm. 4.1.1 (Corollary 1 in [13]). Similarly one can define $s_K(L) := s_K(f)$. Thus we have

$$r_K(L)\, s_K(L) = [L : K].$$

Remark 4.1.1.2. *The cluster size is preserved under isomorphism over K. If M/K and M'/K contained in $\bar{K}$ are isomorphic over K, then $r_K(M) = r_K(M')$.*

4.2 Hilbertian Fields

We will state some important results about hilbertian fields in this section. For a detailed discussion one can refer to Völklein [22].

Definition 4.2.1. *If K' is a field with subfield K, we say K' is regular over K if K is algebraically closed in K'.*

Definition 4.2.2. *(Def 1.9 in [22]). A field K is called hilbertian if for each irreducible polynomial $f(x, y)$ in two variables over K, of degree ≥ 1 in y, there are infinitely many $b \in K$ such that the specialised polynomial $f(b, y)$ (in one variable) is irreducible.*

Remark 4.2.2.1. *For equivalent definitions of hilbertian fields see Corollary 1.8 in [22].*

Proposition 4.2.3. *(Corollary 1.11 in [22]). If K is hilbertian then so is every finitely generated extension field of K.*

Definition 4.2.4. *(Def 1.14 in [22]). Let G be a finite group. We say G occurs regularly over K if for some $m \geq 1$ there is a Galois extension of $K(x_1, \ldots, x_m)$, regular over K, with Galois group isomorphic to G.*

Proposition 4.2.5. *(Corollary 1.15 in [22]). Suppose G occurs regularly over K. Then G occurs regularly over every extension field K' of K. Thus G is a Galois group over K' if K' is hilbertian.*

Proposition 4.2.6. *(Example 1.17 in [22]). The symmetric group $\mathfrak{S}_n$ occurs regularly over every field K.*

Theorem 4.2.7. *(Hilbert's irreducibility theorem) (Thm 1.23 in [22]). The field $\mathbb{Q}$ is hilbertian.*

4.3 Existence of Polynomials for given Degree and Cluster Size over Number Fields

We present the following theorem which is generalisation of a result in an unpublished note of Perlis [17, Exercise 4], which was for $K = \mathbb{Q}$. This theorem includes even the excluded cases in generalisation done by Krithika and Vanchinathan (without using Shafarevich's theorem) in [13, Thm. 2] namely $n = 2r$ where r is odd for $\mathbb{Q}$ and $n = 2r$ for any number field $K \neq \mathbb{Q}$.

Inverse Cluster Size Problem for Number Fields

Theorem 4.3.1. *(Perlis, Krithika and Vanchinathan, A generalisation by Bhagwat, Jaiswal) (Thm 3.1.1 in [3])*

Let K be a number field. Let $n > 2$ and $r|n$. Then there exists an irreducible polynomial over K of degree n with cluster size r.

Before proving Thm. 4.3.1, we state some results which we will use in the proof of the theorem.

Lemma 4.3.2. *The group $\mathfrak{S}_n$ is realizable as Galois group over any number field.*

Proof. The field $\mathbb{Q}$ is hilbertian by Thm 4.2.7. Furthermore, every finitely generated extension of a hilbertian field is hilbertian by Prop 4.2.3, and thus we conclude that every number field is hilbertian.

Let K be a number field. We know that the group $\mathfrak{S}_n$ occurs regularly over every field by Prop 4.2.6. In particular, $\mathfrak{S}_n$ occurs regularly over K. The result Prop 4.2.5 says that if a group occurs regularly over a hilbertian field, then it is realizable as a Galois group over that field. Hence finally we conclude that $\mathfrak{S}_n$ is realizable as Galois group over K.

□

The following lemma is the final proposition in Perlis [17]. We write the proof given by Perlis for the sake of completion.

Lemma 4.3.3. *Let G be a transitive subgroup of $\mathfrak{S}_n$ for some n. If there exists a finite Galois extension of a field K with Galois group isomorphic to G, then there exists an irreducible polynomial f over K of degree n and a labelling of the roots of f so that the Galois group of f, viewed as a group permuting roots of f, is precisely G.*

Proof. Let G act transitively on n symbols $\{1, 2, \ldots, n\}$. Let $H \subset G$ be the stabiliser of the symbol 1. Then there is a canonical labelling of the n cosets in G/H so that G acts on G/H exactly the same way G acts on the original n symbols that is $\{x_1H, x_2H, \ldots, x_nH\}$ with $x_j \cdot 1 = j$ and $g \cdot (x_jH) = x_{g\cdot j}H$ for all $g \in G$ and all $1 \leq j \leq n$. The action is faithful and transitive. We have $\mathrm{Stab}(x_jH) = x_jHx_j^{-1}$. Since the action is faithful, it follows that $\bigcap\limits_{1\leq j\leq n}(x_jHx_j^{-1}) = \bigcap\limits_{1\leq j\leq n}(\mathrm{Stab}(x_jH)) = \{1\}$.

Let K_G/K be finite Galois extension with Galois group isomorphic to G. We identify it with G. Let L be the subfield of K_G fixed by H. The Galois closure of L/K in K_G is the subfield of K_G corresponding to the intersection of the conjugates of H in G and that intersection is trivial because of argument in previous paragraph. Hence K_G is the Galois closure of L/K. Let f over K be the minimal (hence irreducible) polynomial for a primitive element of L/K. We can identify the n roots of f with the n cosets in G/H. This is the required polynomial f. □

Lemma 4.3.4. *Let K be a perfect field and K'/K be a finite extension. If for a group G, direct products G^n are realizable as Galois group over K for each $n \in \mathbb{N}$ then they are realizable as Galois groups over K'.*

As a corollary, we get arbitrarily large finite families of Galois extensions of K inside a fixed $\bar{K}$ which are pairwise non-isomorphic over K and are pairwise linearly disjoint over K

with each having Galois group G over K. This corollary also holds for G^n in place of G for any $n \in \mathbb{N}$ as well as for K'.

Proof. We will mimic the proof of Thm. 4.2 in [5] which states that if every finite group can be realized as a Galois group over $\mathbb{Q}$ then every finite group can be realized as a Galois group over any finite extension of $\mathbb{Q}$.

Since K is perfect and K'/K is finite, we have that K'/K is separable. Hence, K'/K has finitely many intermediate fields. Let n be the number of these intermediate fields (including K' and K). Now G^n is realizable over K by assumption, say for E/K Galois, we have $\mathrm{Gal}(E/K) \cong G^n$. We have normal subgroups $N_i = G \times G \times \cdots \times 1 \times \cdots \times G$ of G^n for $1 \leq i \leq n$ where the ith coordinate is trivial and there is no restriction in other coordinates. So $N_i \cong G^{n-1}$. Let E_i be the subfield of E corresponding to N_i, so E_i/K is Galois with $\mathrm{Gal}(E_i/K) \cong G^n/N_i \cong G$.

Now for $i \neq j$, $E_i \cap E_j$ corresponds to subgroup generated by N_i and N_j which is G^n. Hence $E_i \cap E_j = K$. Suppose for some $i \neq j$ we have $E_i \cap K' = E_j \cap K'$. Since $E_i \cap E_j = K$, we get $E_i \cap K' = E_j \cap K' = K$. Now suppose that all $E_i \cap K'$ are distinct. Since we have n intermediate fields of K'/K, $E_i \cap K' = K$ for some i. In either case we get an i such that $E_i \cap K' = K$. Hence $\mathrm{Gal}(E_iK'/K') \cong \mathrm{Gal}(E_i/K) \cong G$. This realizes G as a Galois group over K'. By replacing G with G^m for any $m \in \mathbb{N}$ in the above argument, we can realize G^m over K' for any m.

For the proof of the corollary, we observe that for any n we have some E/K Galois with Galois group G^n and N_i normal subgroups of G^n and E_i subfield of E corresponding to N_i. We observe that N_i are not conjugate to each other in G^n and they pairwise generate G^n. Hence E_i are not isomorphic to each other over K and are pairwise linearly disjoint over K with G as Galois group of each E_i/K. □

Now we prove Thm. 4.3.1.

Proof. Suppose $r = 1$. By Lemmas 4.3.2 and 4.3.3, there exists an irreducible polynomial f over K of degree n with Galois group $\mathfrak{S}_n$. This f satisfies $r_K(f) = 1$.

Now suppose $r > 1$. In solutions of Exercises 3 and 4 in [17], a solvable group $G \subseteq \mathfrak{S}_n$

is constructed with the properties that its action is transitive on n points, and a point stabiliser fixes precisely r points. The construction is as follows: We divide the n points into $n/r = s$ packets of size r. Let G be the group of permutations on these n points generated by independent cyclic permutations on each packet, together with a cyclic permutation on the overall set of packets. Hence G is transitive. This construction of G has the explicit description of a semidirect product of an s-fold direct product of cyclic groups $\mathbb{Z}/r\mathbb{Z}$ and a cyclic group $\mathbb{Z}/s\mathbb{Z}$. A semidirect product group law on G is given by

$$((a_1, \ldots, a_s), b) \cdot ((c_1, \ldots, c_s), d) = ((a_1, \ldots, a_s) + (b \cdot (c_1, \ldots, c_s)), b + d),$$

where $b \cdot (c_1, \ldots, c_s) = (c_{b+1}, \ldots, c_s, c_1, \ldots, c_b)$ for $b \neq 0$ & $0 \cdot (c_1, \ldots, c_s) = (c_1, \ldots, c_s)$.

Thus, $G = (\mathbb{Z}/r\mathbb{Z})^s \rtimes \mathbb{Z}/s\mathbb{Z}$.

Suppose the n points are $\{1, 2, \ldots, n\}$ and the s many packets are $\{1, 2, \ldots, r\}$, $\{r+1, r+2, \ldots, 2r\}$, ..., $\{(s-1)r+1, (s-1)r+2, \ldots, sr\}$. The above group G has the following action on the set of these points. For $1 \leq j \leq s$ and $1 \leq k \leq r$,

$$((a_1, \ldots, a_s), b) \cdot ((j-1)r + k) := ((j'-1)r + k')$$

where $j' \equiv j - b \pmod{s}$ and $1 \leq j' \leq s$ and $k' \equiv k + a_{j'} \pmod{r}$ and $1 \leq k' \leq r$. Thus we can see that each $\mathbb{Z}/r\mathbb{Z}$ permutes points in a packet and action of $\mathbb{Z}/s\mathbb{Z}$ permutes s copies of $\mathbb{Z}/r\mathbb{Z}$.

It is easy to see that any point stabiliser is isomorphic to $(\mathbb{Z}/r\mathbb{Z})^{s-1}$. The group G is solvable since the following chain has successive cyclic quotients (See definition on Page 105 in [10]).

$$1 \subseteq \mathbb{Z}/r\mathbb{Z} \subseteq (\mathbb{Z}/r\mathbb{Z})^2 \subseteq \cdots \subseteq (\mathbb{Z}/r\mathbb{Z})^s \subseteq G.$$

Since direct product of solvable groups is solvable, direct products G^i for $i \in \mathbb{N}$ are solvable. By Shafarevich's theorem ([20]), G^i for $i \in \mathbb{N}$ are realizable as Galois groups over $\mathbb{Q}$. Hence by Lemma 4.3.4, G is realizable as Galois group over number field K. By Lemma 4.3.3, there exists an irreducible polynomial f over K of degree n and a labelling of the roots so that the Galois group of f, viewed as a group permuting roots of f, is precisely G. This f satisfies $r_K(f) = r$.

□

4.4 A Simple Lemma about $s_K(L)$

We begin this section by giving an alternate proof for last equality in (3) of Thm.4.1.1, which is stated in [18] and proved in first Proposition in unpublished note of Perlis [17]. The equality states: $r_K(f) = [N_G(H) : H]$.

Proof. We observe that a field is isomorphic to $K(\alpha)$ over K if and only if it is of the form $K(\alpha')$ for some root α' of f. All these fields are contained in K_f. By Galois correspondence, K-isomorphic subfields of a Galois extension over K correspond to conjugate subgroups of its Galois group.

Hence, $s_K(f) =$ number of distinct $K(\alpha') =$ number of distinct subgroups of G that are conjugate to H in $G = [G : N_G(H)]$. The last equality follows from orbit-stabiliser theorem for the conjugation action of G on the set of its subgroups. By Thm. 4.1.1 (2), we are done. □

We state the simple observation used above, as a lemma.

Lemma 4.4.1. *Let K be perfect field. For finite L/K, $s_K(L)$ (as defined in Sec. 4.1) is the number of distinct fields inside $\bar{K}$ isomorphic to L over K.*

Proof. By primitive element theorem, $L = K(\alpha)$ with α root of some irreducible polynomial f over K. Now, L' is isomorphic with L over $K \iff L' = K(\alpha')$ for some root α' of f. Thus $s_K(L) = s_K(f) =$ number of distinct $K(\alpha')$ for α' root of f= number of distinct fields isomorphic to L over K. □

Remark 4.4.1.1. *Let $L_1, L_2, \ldots, L_{s_K(L)}$ be the distinct fields as in above Lemma 4.4.1. Hence we have $\tilde{L} = L_1 L_2 \ldots L_{s_K(L)}$, that is the Galois closure of L/K is compositum of distinct fields isomorphic to L over K.*

Using Lem. 4.4.1, we will give an alternate proof for Cluster Magnification theorem Thm. 5.1.2, Thm. 1 in [13] in Sec. 9.

Remark 4.4.1.2. *Let K be a number field. Note that ${}^nP_k$ and ${}^nC_k$ are integers with ${}^nP_k = k!\,{}^nC_k$. By Thm. 4.3.1, we get irreducible polynomial over the field with degree ${}^nP_k$ and cluster size $k!$. The following theorem says that this is also true under some condition for a general perfect field.*

By using the above Lemma 4.4.1, we give an alternate proof for Thm. 3 in [13].

Theorem 4.4.2. *Let K be a perfect field. Let f over K be irreducible of degree n with Galois group $\mathfrak{S}_n$ (For a number field K, such f always exists. See $r = 1$ case in Proof of Thm. 4.3.1).*

For $1 \leq k \leq n-2$, let L_k be an extension of K obtained by adjoining any k roots of f in $\bar{K}$. Let g be the irreducible polynomial over K for a primitive element of L_k. This polynomial has degree ${}^nP_k$ and cluster size $k!$.

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be roots of f in $\bar{K}$. Let $L_k = K(\alpha_1, \alpha_2, \ldots, \alpha_k)$. We have that degree of L_k/K is $n(n-1)\ldots(n-k+1) = {}^nP_k$. Since Galois group of f is $\mathfrak{S}_n$, we have L' is isomorphic to L_k over $K \iff L' = K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k})$ for k roots $\alpha_{i_j} : 1 \leq j \leq k$ of f. By Lemma 4.4.1, $s_K(L_k)$ is number of distinct fields inside $\bar{K}$ isomorphic to L_k over K which is precisely the number of ways of choosing k roots from n roots which is ${}^nC_k$. By Thm. 4.1.1 (2), $r_K(L_k) = k!$. □

Chapter 5

Cluster Magnification

Krithika and Vanchinathan proved the Cluster Magnification theorem in [13]. In this chapter we state the Strong cluster magnification problem and establish an equivalent criterion for that in terms of Galois groups. We also reformulate the Strong cluster magnification problem for irreducible polynomials. We then state the Weak cluster magnification problem and demonstrate how the notions for strong cluster magnification and weak cluster magnification are actually different.

5.1 Cluster Magnification Theorem in work of Krithika & Vanchinathan

Recall the notion of two extensions of a field being linearly disjoint over that field from Def 2.3.1 and Rem 2.3.1.1. The following lemma can be deduced from [12, Lem. 1, Chap. 8.15] in combination with Remark 2.3.1.1.

Lemma 5.1.1. *Let E/K be any extension and F/K be Galois extension and let $E' \subset E$. Then*

$$E \cap F = K \iff E \cap E'F = E' \text{ and } E' \cap F = K.$$

The following result proved in [13, Sec. 3.1] is referred to as the Cluster Magnification

theorem. The theorem is reformulated in [13, Sec. 4].

Cluster Magnification Theorem

Theorem 5.1.2. *[Krithika, Vanchinathan] Let K, f and α be as above. Let $\deg(f) = n > 2$ over K with cluster size $r_K(f) = r$. Assume that there is a Galois extension F of K, say of degree d, which is linearly disjoint with K_f over K. Then there exists an irreducible polynomial g over K of degree nd with cluster size rd. (F can be chosen to be $K(\beta)$ for some β in $\bar{K}$ so that $K(\alpha, \beta) = K(\alpha + \beta)$ and the irreducible polynomial of $\alpha + \beta$ over K, has degree nd with cluster size rd; d is the magnification factor).*

Reformulation : Let K be a perfect field as above and L/K be an extension of degree $n > 2$ contained in $\bar{K}$ with cluster size $r_K(L) = r$. Let F/K be any finite Galois extension of degree d contained in $\bar{K}$, which is linearly disjoint with $\tilde{L}$ over K. Then the compositum LF/K has degree nd with cluster size $r_K(LF) = rd$. (d is the magnification factor).

Proof. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of f in $\bar{K}$. By relabeling we can assume that $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ is the cluster of α. We have a Galois extension $K(\beta)/K$ such that $K(\beta)$ and K_f are linearly disjoint over K that is $K_f \cap K(\beta) = K$. Hence by Lemma 5.1.1, $K_f \cap K(\alpha, \beta) = K(\alpha)$ and $K(\alpha) \cap K(\beta) = K$. Since $K(\beta)/K$ is Galois and $K(\alpha) \cap K(\beta) = K$. Hence $K(\alpha, \beta)/K(\alpha)$ is Galois of degree $[K(\beta) : K] = d$. Hence degree of $K(\alpha, \beta)/K$ is nd.

Since K is perfect, we have that $K(\alpha, \beta)$ is a simple extension of K generated by a primitive element of the form $\alpha + c\beta$ for a suitable $c \in K$. By using $c\beta$ as primitive element of $K(\beta)$ over K we can assume $\alpha + \beta$ is a primitive element over K for $K(\alpha, \beta)$. Let conjugates of β over K be $\beta = \beta_1, \beta_2, \ldots, \beta_d$ all of which lie in $K(\beta)$.

Consider the minimal polynomial $g(x)$ of $\alpha + \beta$. Since degree of g over K is nd. Hence the conjugates of $\alpha + \beta$ over K are $\alpha_i + \beta_j$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, d$. Since α_i for $1 \leq i \leq r$ are in $K(\alpha)$, we have that $\alpha_i + \beta_j \in K(\alpha + \beta) = K(\alpha, \beta)$ for $i = 1, 2, \ldots, r$ and $j = 1, 2, \ldots, d$. The cluster of $\alpha + \beta$ has at least rd.

Suppose that the cluster has more than these rd roots. Thus we have $\alpha_i + \beta_j \in K(\alpha + \beta)$ for some $i \neq 1, 2, \ldots, r$ and for some j. As $\beta_j \in K(\beta) \subset K(\alpha + \beta)$, we have $\alpha_i \in K(\alpha + \beta)$. Now $\alpha_i \in K_f$ as well. So $\alpha_i \in K(\alpha + \beta) \cap K_f = K(\alpha)$. This is a contradiction. Thus the cluster size of $g(x)$ is rd.

□

5.2 Strong Cluster Magnification

A natural question arises: When is the hypothesis of Cluster Magnification Theorem Thm 5.1.2 true? This leads us to defining the following. One would appreciate the usage of 'strong' in Sec 5.4.

Let M/K be a finite extension of degree m with $r_K(M) = k$.

Definition 5.2.0.1. (Bhagwat, Jaiswal) (Def 4.1.1 in [3])

M/K is said to be obtained by strong cluster magnification from a subextension L/K if we have the following:

1. $[L : K] = n > 2$,
2. there exists a finite Galois extension F/K such that the Galois closure $\tilde{L}$ of L in $\bar{K}$ and F are linearly disjoint over K.
3. $LF = M$.

The number $[F : K]$ is called the magnification factor and denoted by d. The magnification is called trivial if $F = K$ and nontrivial otherwise.

Remark 5.2.0.1. *Suppose we have an extension L/K,and a Galois extension F/K such that $\tilde{L} \cap F = L \cap F$. Then $LF/(L \cap F)$ is obtained by strong cluster magnification from $L/(L \cap F)$.*

Remark 5.2.0.2. *Let LF/K be obtained by strong cluster magnification from L/K through F/K. If $K \subset L' \subset L$. Then $L'F/K$ is obtained by strong cluster magnification from L'/K through F/K.*

We prove the following hereditary property for strong cluster magnification.

Proposition 5.2.1. *Let M/K be obtained by strong cluster magnification from L/K through F/K as in Def 5.2.0.1. Then for any $K \subset K' \subset L$ the extension M/K' is obtained by strong cluster magnification from L/K' through $K'F/K'$ with same magnification factor.*

Proof. We check that the conditions in Def. 5.2.0.1 hold.

Let L_1 be Galois closure of L/K'. So $L_1 \subset \tilde{L}$. Since $\tilde{L}$ and F are linearly disjoint over K, we conclude that L_1 and F are linearly disjoint over K. Hence by Lemma 5.1.1 we have

$$L_1 \cap F = K \iff L_1 \cap K'F = K' \text{ and } K' \cap F = K.$$

Hence $K'F/K'$ is Galois and L_1 and $K'F$ are linearly disjoint over K'. Also $M = LF = LK'F$ and hence we are done. The magnification factor is same since $[F : K] = [K'F : K']$.

□

Let $\tilde{M}$ be Galois closure of M/K inside $\bar{K}$. Let $G' = \mathrm{Gal}(\tilde{M}/K)$. Let $H' = \mathrm{Gal}(\tilde{M}/M)$ be the subgroup of G' with fixed field M. Hence H' is normal in G' if and only if H' is trivial.

Proposition 5.2.2. *Suppose M/K is obtained by strong cluster magnification from L/K. Let $\tilde{L}$ and F/K be as in the Def. 5.2.0.1 and let $R := \mathrm{Gal}(F/K)$. Let $G = \mathrm{Gal}(\tilde{L}/K)$ and $H = \mathrm{Gal}(\tilde{L}/L)$. Then the following hold.*

1. $r_K(M) = r_K(L)\,[F : K], \quad s_K(M) = s_K(L) = [G : N_G(H)]$.
2. $\tilde{L}F = \tilde{M}$.
3. $G' \cong G \times R$ *where isomorphism is given by* $\lambda \in G' \mapsto (\lambda|_{\tilde{L}}, \lambda|_F)$.
4. *Furthermore* $H' \cong H \times \{e\} \subset G \times R$ *under the above isomorphism.*
5. F *is uniquely determined by* L *and* M.

Proof.

1. From (2) and (3) in Thm. 4.1.1, we have $s_K(L) = [G : N_G(H)]$. Now from Thm. 5.1.2, $[M : K] = [L : K]\,[F : K]$ and $r_K(M) = r_K(L)\,[F : K]$.

   Also from Thm. 4.1.1, $[M : K] = r_K(M)\,s_K(M)$ and $[L : K] = r_K(L)\,s_K(L)$. Hence $s_K(M) = s_K(L)$.

2. Since $M = LF$, we have $\tilde{L}F \subset \tilde{M}$. Since $\tilde{L}/K$ and F/K are Galois it follows that $\tilde{L}F/K$ is Galois. Thus, $\tilde{L}F = \tilde{M}$.

3. $\tilde{L}$ and F are linearly disjoint over K. Since F/K is Galois, it follows that $\tilde{L} \cap F = K$. Therefore, by (2) and [5, Thm. 2.1], we conclude that $G' \cong G \times R$ under the given isomorphism.

4. Let $\lambda \in G'$. We have

$$\lambda \in H' \iff \lambda|_M = id_M \iff \lambda|_L = id_L \text{ and } \lambda|_F = id_F$$

$$\iff \lambda|_{\tilde{L}} \in H \subset G \text{ and } \lambda|_F = 1 \in R.$$

5. We have isomorphism $G' \cong G \times R$. Hence $G' = G_0 R_0$ where $G_0, R_0 \subset G'$ with $G_0 \cong G \times 1$ and $R_0 \cong 1 \times R$ under above isomorphism. Furthermore, $\tilde{L} = \tilde{M}^{R_0}$ and $F = \tilde{M}^{G_0}$. Now if a subextension L of M is given, then $\tilde{L}$ is uniquely determined inside $\tilde{M}$. Thus R_0 is uniquely determined inside G' which implies that G_0 is uniquely determined inside G'. Hence F is uniquely determined from L and M.

□

In view of property (1) in Prop. 5.2.2, we see that $r_K(L)|r_K(M)$ and the ratio $r_K(M)/r_K(L)$ is indeed same as the degree $d = [F : K]$, which is the magnification factor for M/L over K as defined earlier.

A criterion for strong cluster magnification: We now establish an equivalent criterion for strong cluster magnification for a field extension in terms of Galois groups.

Theorem 5.2.3. *(Bhagwat, Jaiswal) (Thm 4.1.6 in [3])*

An extension M/K is obtained by nontrivial strong cluster magnification from some subextension L/K if and only if

$$\mathrm{Gal}(\tilde{M}/K) \cong A \times B$$

for nontrivial groups A and B and

$$\mathrm{Gal}(\tilde{M}/M) \cong A' \times 1$$

(under the same isomorphism) for a subgroup $A' \subset A$ with $[A : A'] > 2$.

Proof. Suppose M/K is obtained by nontrivial strong cluster magnification from a subextension L/K. From Prop. 5.2.2 (3) and (4), we get $A = G, B = R$ and $A' = H$ with the required conditions since, $d = |R| > 1, n = [G : H] > 2$.

Conversely, suppose $G' \cong A \times B$ for nontrivial subgroups A and B and $H' \cong A' \times \{e\}$ (under the same isomorphism) for a subgroup $A' \subset A$ with $[A : A'] > 2$. We identify G' and H' with their images under the isomorphism. Now we check the three conditions of Def. 5.2.0.1 for M/K.

1. Since $1 \times B$ is normal in G', we conclude that $\tilde{M}_B := \tilde{M}^{1\times B}$ is Galois over K with Galois group A. Let $L := \tilde{M}^{A'\times B}$. Hence L/K has degree $n = [A : A'] > 2$.
2. Since $A \times 1$ is normal in G', we conclude that $F := \tilde{M}^{A\times 1}$ is Galois over K with Galois group B and degree $d = |B|$. Let $\tilde{L}$ be Galois closure of L in $\bar{K}$. Since, $L \subset \tilde{M}_B$, we have $\tilde{L} \subset \tilde{M}_B$. The intersection of fields $\tilde{M}_B \cap F$ corresponds to the subgroup generated by $A \times 1$ and $1 \times B$ which is G'. Hence $\tilde{M}_B \cap F = K$. Thus $\tilde{L} \cap F = K$. So $\tilde{L}$ and F are linearly disjoint over K.
3. Now, $M = \tilde{M}^{A'\times 1}$. Hence $L, F \subset M$, thus $LF \subset M$. Since $\tilde{L} \cap F = K$, we conclude $L \cap F = K$. Hence $[LF : K] = [L : K]\,[F : K] = nd$. Also, $[M : K] = [G' : H'] = [A : A']\,|B| = nd$. Hence $LF = M$.

The magnification is nontrivial since B is nontrivial subgroup. □

Remark 5.2.3.1. *In the above proof of the converse part, we can additionally conclude $\tilde{M}_B = \tilde{L}$. Since, $\tilde{M}_B \cap F = \tilde{L} \cap F = K$ we get $[F : K] = [\tilde{M}_B F : \tilde{M}_B] = [\tilde{L}F : F]$. Now, $\tilde{M}_B F \subset \tilde{M}$ corresponds to intersection of the groups $A \times 1$ and $1 \times B$ which is trivial. Hence $\tilde{M}_B F = \tilde{M}$. From prop. 5.2.2 (2), $\tilde{M} = \tilde{L}F$. Hence, $[\tilde{M}_B : K] = [\tilde{L} : K]$. Thus, $\tilde{M}_B = \tilde{L}$.*

Corollary 5.2.0.2. Let M/K be Galois. Then M/K is obtained by nontrivial strong cluster magnification from some subextension L/K if and only if $\mathrm{Gal}(M/K) \cong A \times B$ for nontrivial groups A and B with $|A| > 2$. If this happens then, L/K is also Galois.

Proof. Since M/K is Galois, $\tilde{M} = M$, $G' = \mathrm{Gal}(M/K)$ and H' is trivial. So A' is trivial and $[A : A'] = |A|$. Also $\tilde{L} = \tilde{M}_B = L$. Hence, L/K is Galois. □

We end this section with a result that the strong cluster magnification behaves well with respect to K-isomorphisms.

Proposition 5.2.4. *Let M'/K be contained in $\bar{K}$ and $\sigma : M \to M'$ be an isomorphism over K. If M/K is obtained by strong cluster magnification from L/K, then M'/K is obtained by strong cluster magnification from $\sigma(L)/K$.*

Proof. Suppose M/K is obtained by strong cluster magnification from L/K. We have L/K, n, r, F/K, d as above. Now we check the three conditions of Def. 5.2.0.1 for M'/K.

1. $\sigma(L) \cong L$ has degree $n > 2$ over K with $r_K(\sigma(L)) = r_K(L) = r$.

2. $F = \sigma(F)$ since F/K is Galois. It is easy to prove that $\tilde{L}$ is Galois closure of $\sigma(L)$ in $\bar{K}$. $\tilde{L}$ and F are linearly disjoint over K.

3. $\sigma(L)F = \sigma(M) = M'$.

Alternatively, we can use the criterion in Thm. 5.2.3. The isomorphism between M and M' extends to isomorphism between their Galois closures. Hence we also get an isomorphism between G', H' and corresponding groups of M'.

□

Remark 5.2.4.1. *From the proof of Thm. 5.2.3, we get the following way to construct all fields M/K which are obtained by nontrivial strong cluster magnification from some subextension L/K.*

Suppose $A \times B$ is realizable as a Galois group over K for nontrivial groups A and B with a subgroup $A' \subset A$ with $[A : A'] > 2$ such that $\bigcap_{a \in A} aA'a^{-1} = 1$. Let P be such that $\mathrm{Gal}(P/K) = A \times B$. Then our required fields are $M = P^{A' \times 1}$ and $L = P^{A' \times B}$.

5.3 Strong Cluster Magnification Problem for Irreducible Polynomials

Let g be an irreducible polynomial over K with degree m and $r_K(g) = k$.

Definition 5.3.0.1. We have the following equivalent definitions:

1. The polynomial g is said to be obtained by strong cluster magnification from a polynomial f over K if we have the following:

   (a) an extension $K(\alpha)/K$ of degree $n > 2$ with f as the minimal polynomial of α over K and $r_K(f) = r$,

   (b) there exists a Galois extension F/K of degree d such that K_f and F are linearly disjoint over K, and

   (c) $K(\alpha)F = K(\gamma)$ where γ is some root of g in $\bar{K}$.

   The magnification is called trivial if $d = 1$ and nontrivial otherwise. (d is the magnification factor).

2. The polynomial g over K is said to be obtained by strong cluster magnification from a polynomial f over K, if for some root γ of g in $\bar{K}$, the field extension $M = K(\gamma)$ over K is obtained by strong cluster magnification from L/K with $L = K(\alpha)$, where α is a root of the irreducible polynomial f.

Remark 5.3.0.1. *Let $s_K(g) = s$. Let $\{\gamma_1, \gamma_2, \ldots, \gamma_s\}$ be a complete set of representatives of the clusters of roots of g in $\bar{K}$. Let $M_i = K(\gamma_i)$ for $1 \leq i \leq s$.*

1. *All M_i's are mutually isomorphic by mapping γ_i's to each other. For every i, M_i/K is an extension of degree m contained in $\bar{K}$ with $r_K(M_i) = r_K(g) = k$.*

2. *By Prop. 5.2.4, if for some i, M_i/K is obtained by strong cluster magnification from L_i/K then for each $1 \leq j \leq s$, M_j/K is obtained by strong cluster magnification from some subextension L_j/K.*

3. *More precisely, if $L_i = K(\alpha_i)$ for a root α_i of the irreducible polynomial f then, by isomorphism of M_i and M_j, we get $L_j = K(\alpha_j)$ where α_j is a root of f.*

Because of the above remark, if strong cluster magnification holds for some root of g, then it holds for every root of g. Hence we can work with any root γ of g in $\bar{K}$. Let $M = K(\gamma)$. Let K_g be splitting field of g over K inside $\bar{K}$. Let $G' = \mathrm{Gal}(K_g/K)$. Let $H' \subset G'$ be subgroup with $K(\gamma)$ as the fixed field that is $H' = \mathrm{Gal}(K_g/K(\gamma))$.

By Thm. 5.2.3, we get an equivalent criterion for strong cluster magnification of an irreducible polynomial.

Theorem 5.3.1. *g over K is obtained by nontrivial cluster magnification from an f over K if and only if*

$$\mathrm{Gal}(K_g/K) \cong A \times B$$

for nontrivial groups A and B and (for γ as above)

$$\mathrm{Gal}(K_g/K(\gamma)) \cong A' \times 1$$

(under the same isomorphism) for a subgroup $A' \subset A$ with $[A : A'] > 2$ and f is the minimal polynomial for a primitive element of $(K_g)^{A' \times B}$ over K.

Definition 5.3.0.2. An irreducible polynomial g over K is called primitive if it is not obtained by a nontrivial strong cluster magnification over K. (this notion occurs in [13] as well).

Example 5.3.2. *Some simple examples / cases of primitive polynomials g over K follow from Thm. 5.1.2 and Thm. 5.3.1.*

1. $\deg g = 4$ *or a prime* $p > 2$.

2. $|\mathrm{Gal}(K_g/K)| = 4$.

3. $\mathrm{Gal}(K_g/K)$ *is not a direct product of two nontrivial groups. In particular, the case when* $\mathrm{Gal}(K_g/K)$ *is simple. In particular, the case* $|\mathrm{Gal}(K_g/K)|$ *is a prime* $p > 2$.

5.4 Weak Cluster Magnification

Another natural question arises: Is the hypothesis of Cluster Magnification Theorem Thm 5.1.2 necessary for cluster size to magnify? Example 5.4.1 and other examples in this section answer this negatively. This leads us to defining the following. The definition is not vacuous which will be demonstrated later in Remark 8.3.3.1.

Definition 5.4.0.1. (Bhagwat, Jaiswal) (Def 4.3.1 in [3])

M/K is said to be obtained by weak cluster magnification from a subextension L/K if $r_K(L)|r_K(M)$.

We call $d = r_K(M)/r_K(L)$ as the magnification factor. The magnification is called trivial if $d = 1$ and nontrivial otherwise.

Remark 5.4.0.1. *From Def 5.2.0.1 and Thm. 5.1.2, if M/K is obtained by strong cluster magnification from L/K then M/K is obtained by weak cluster magnification from L/K. This together with the following example justify the usage of 'weak' in above definition and 'strong' in Sec 5.2.*

Example 5.4.1. *Consider $M/L/K$ where M/K is Galois and L/K is not Galois (a particular case is $M = \tilde{L}$ for L/K not Galois). So $r_K(L) \neq [L : K]$ and $r_K(M) = [M : K]$. Now $r_K(L) \mid [L : K]$ and $[L : K] \mid [M : K]$. Hence $r_K(L) \mid r_K(M)$ and $r_K(L) \neq r_K(M)$. Thus M/K is obtained by nontrivial weak cluster magnification from L/K.*

We claim that M/K is not obtained by strong cluster magnification from L/K. Assume the contrary. Then we must have by Def. 5.2.0.1 and Lem. 5.1.1 that $M \cap \tilde{L} = L$ which is a contradiction since L/K is not Galois. Moreover M/K is not obtained by strong cluster magnification of L_1/K for any $\tilde{L} \supsetneq L_1 \supset L$.

Example 5.4.2. *Let L_k be as in proof of Thm. 4.4.2. Then for $j < k$, L_k/K is obtained by nontrivial weak cluster magnification from L_j/K but is not obtained by nontrivial strong cluster magnification from L_j/K since $\tilde{L_j} \cap L_k = L_k \neq L_j$.*

One can also verify that $[L_k : L_j] = r_K(L_k)/r_K(L_j) \iff k > n/2$ and $j = n - k$.

Example 5.4.3. *Let $K = \mathbb{Q}$ and ξ_n be n-th primitive root of unity.*

1. *Let* $M = \mathbb{Q}(\xi_{2^k})$ *and* $L = \mathbb{Q}(\xi_{2^{k-1}})$ *for* $k \geq 4$. *Now* M/K, L/K *and* M/L *are Galois. Hence* M/K *is obtained by nontrivial weak cluster magnification from* L/K *with magnification factor* $[M : L] = 2$. *Also* $\mathrm{Gal}(M/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2^{k-2})\mathbb{Z}$ *and* $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2^{k-3})\mathbb{Z}$. *By uniqueness in structure theorem for finite abelian groups* $\mathrm{Gal}(M/K) \ncong \mathbb{Z}/2\mathbb{Z} \times \mathrm{Gal}(L/K)$. *Hence by Corollary 5.2.0.2, we conclude that* M/K *is not obtained by nontrivial strong cluster magnification from* L/K.

   We can use a similar argument as above to conclude that for integers $k > j \geq 3$ *for prime* $p = 2$ *and integers* $k > j \geq 2$ *for prime* $p \neq 2$, $M = \mathbb{Q}(\xi_{p^k})$ *is not obtained by nontrivial strong cluster magnification from* $L = \mathbb{Q}(\xi_{p^j})$.

2. *Let* n, l *be integers such that* $6 < l < n$, $l|n$ *such that* $n = lm$ *and gcd*$(l, m) = 1$. *Let* $M = \mathbb{Q}(\xi_n)$ *and* $L = \mathbb{Q}(\xi_l)$. *We have*

$$\begin{aligned}\mathrm{Gal}(M/K) &\cong \prod_{p|n} (\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^\times = \prod_{p|l} (\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^\times \times \prod_{p|m} (\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^\times \\ &\cong \mathrm{Gal}(L/K) \times \prod_{p|m} (\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^\times.\end{aligned}$$

   Hence by Corollary 5.2.0.2, M/K *is obtained by nontrivial strong cluster magnification from* L/K *through* F/K *where* $F = \mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_{n/l})$.

Chapter 6

Cluster Towers

In this chapter, we provide an important example answering a question in [13] about Cluster Towers. We also give a group theoretic formulation for cluster towers.

6.1 Cluster Tower of a Polynomial

Let f be an irreducible polynomial over K. Consider a complete set of representatives of clusters of roots of f in $\bar{K}$. Let $(\beta_1, \beta_2, \ldots, \beta_s)$ be an ordering of this set where $s = s_K(f)$. Now consider the following cluster tower of fields terminating at the splitting field K_f.

Write the tower as

$$K \subseteq K(\beta_1) \subseteq K(\beta_1, \beta_2) \subseteq \cdots \subseteq K(\beta_1, \beta_2, \ldots, \beta_s) = K_f.$$

In [13], the notions of degree sequence and length of such tower are defined as follows.

The length of tower is number of distinct fields in the tower and the degrees of these distinct fields over K form the degree sequence.

Example 6.1.1. *As noted in [13], if the Galois group of f over K is $\mathfrak{S}_n$ for $n > 2$, we have*

$s = n$ *and the cluster tower is given by*

$$K \subsetneq K(\beta_1) \subsetneq K(\beta_1, \beta_2) \subsetneq \cdots \subsetneq K(\beta_1, \beta_2, \ldots, \beta_{n-1}) = K(\beta_1, \beta_2, \ldots, \beta_n) = K_f,$$

with degree sequence $(n, n(n-1), n(n-1)(n-2), \ldots, n!/2, n!) = ({}^nP_1, {}^nP_2, \ldots, {}^nP_{n-1})$*. So in this case the degree sequence is independent of ordering of* β_i *'s. The length of the tower is* n*.*

An important example: A question was asked by Krithika and Vanchinathan in [13]: Is the degree sequence in general independent of the ordering of the representatives of the clusters of roots? We describe the following example that answers this question negatively.

First we mention some easy to verify properties of Euler's totient function ϕ.

Proposition 6.1.2. *Suppose* l *and* n *are positive integers such that* $l|n$ *with* $n = lm$*. Consider their prime factorisations* $n = \prod_p p^{v_p(n)}$ *and* $l = \prod_p p^{v_p(l)}$ *with* $v_p(l) \leq v_p(n)$ *for every prime* p *(here* v_p *is usual* p*-adic valuation). Then*

1. $\phi(n)/\phi(l) = m\phi(k)/k$ *where* $k = \prod_{p \nmid l} p^{v_p(n)}$*.*
2. $k|m$ *and hence,* $\phi(l)|\phi(n)$*.*
3. $\phi(n) = \phi(l)$ *if and only if* $n = l$*, or* l *is odd and* $n = 2l$*.*
4. $\phi(n)/\phi(l) = m$ *if and only if* n *and* l *have same prime factors.*

Example 6.1.3. *(Bhagwat, Jaiswal) (Example 5.1.3 in [3])*

Let $n \geq 6$*. Fix* $\bar{\mathbb{Q}}$ *to be an algebraic closure of* $\mathbb{Q}$*. Fix* b *to be a primitive* n*-th root of unity in* $\bar{\mathbb{Q}}$*. Let* c *be a positive rational number such that* $f = x^n - c$ *is an irreducible polynomial over* $\mathbb{Q}$*. (In particular,* $c = p$*, a prime works for any* n *by Eisenstein criterion). Let* $a = c^{1/n}$ *be the positive real root of* f*. Hence the roots of* f *are given by* $a, ab, \ldots, ab^j, ab^{j+1}, \ldots, ab^{n-1}$*. We observe that, when* n *is odd,* $r = 1, s = n$*. When* n *is even, the roots appear in pairs* $\{\alpha, -\alpha\}$ *and thus* $r = 2, s = n/2$*.*

By [11, Prop. 1 and Thm. A], the Galois group G of splitting field of f is isomorphic to $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if n is odd or, n is even with $\sqrt{c} \notin \mathbb{Q}(b)$ if and only if $\mathbb{Q}(c^{1/n}) \cap \mathbb{Q}(b) = \mathbb{Q}$. Assume n to satisfy these conditions. Hence, in particular the order of G is $n\phi(n)$.

Further, assume that n is composite and $l|n$ with $n = ml$, where for the cases n odd or $n \equiv 0 \pmod 4$, we assume $2 < l < n$; and for the case $n \equiv 2 \pmod 4$ we assume $2 < l < n/2$. Because of our assumptions, $ab^m \neq \pm a, \pm ab$ and $1 < \phi(l) < \phi(n)$ by (3) of Prop. 6.1.2. Also, $\phi(l)|\phi(n)$ by (2) of Prop. 6.1.2. Since $\mathbb{Q}(b)/\mathbb{Q}$ is Galois, by Thm. 2.6 in [5], we get

$$\mathrm{Gal}(\mathbb{Q}(a, b^m)/\mathbb{Q}(a)) \cong \mathrm{Gal}(\mathbb{Q}(b^m)/\mathbb{Q}) \cong (\mathbb{Z}/l\mathbb{Z})^\times.$$

(For example, $c = 2, n = 9, l = 3$ and $c = 3, n = 8, l = 4$ work.)

Because of our assumptions, we have $m+1 \leq s$. Let the representatives of clusters of roots of f be given by

$$\beta_3 = ab^m, \beta_{m+1} = ab^2, \beta_i = ab^{i-1} \text{ for other } 1 \leq i \leq s.$$

Consider the following cluster towers:

$$\mathbb{Q} \subsetneq \mathbb{Q}(\beta_1) \subsetneq \mathbb{Q}(\beta_1, \beta_2) = \mathbb{Q}_f,$$

with degrees n and $n\phi(n)$ and length of tower $= 3$ and

$$\mathbb{Q} \subsetneq \mathbb{Q}(\beta_1) \subsetneq \mathbb{Q}(\beta_1, \beta_3) \subsetneq \mathbb{Q}(\beta_1, \beta_3, \beta_2) = \mathbb{Q}_f,$$

with degrees $n, n\phi(l)$ and $n\phi(n)$ and length of tower $= 4$.

This example shows us that not only the degree sequence is not independent of the ordering of the β_i's but length of tower is also not independent of the ordering of the β_i's.

6.2 Group Theoretic Formulation of Cluster Towers

Let the notations be as earlier in Sec. 5.2. Let $(\beta_1, \beta_2, \ldots, \beta_s)$ be a fixed ordering of a complete set of representatives of the clusters of roots of an irreducible polynomial f over K in $\bar{K}$, where $s = s_K(f)$. We have the cluster tower:

$$K \subset K(\beta_1) \subset K(\beta_1, \beta_2) \subset \cdots \subset K_f.$$

Let $G = \mathrm{Gal}(K_f/K)$. For each $1 \leq i \leq s$, let H_i be the subgroup of G that fixes $K(\beta_i)$. Let $\beta_1 = \beta$ and $H_1 = H$. Let σ_i be isomorphism from $K(\beta)$ to $K(\beta_i)$ mapping β to β_i (hence $\sigma_1 = id$). Then $H_i = \sigma_i H \sigma_i^{-1}$.

Let $K_m = K(\beta_1, \beta_2, \ldots, \beta_m)$ and $J_m := (\bigcap_{1 \leq i \leq m} H_i)$ be the subgroup of G that fixes K_m.

Let $m_1 < m_2 < \cdots < m_l$ be all the indices $i > 1$ such that $J_i \neq J_{i-1}$. The length of above cluster tower is $l + 2$. Here, m_l is smallest index i such that $K_i = K_f$.

The degree sequence is $a_0 = n, a_1, a_2, \ldots, a_l = |G|$ with $a_i = [G : J_{m_i}]$ for all $i \geq 1$.

Since $\dfrac{a_i}{a_{i-1}} \leq (n - (m_i - 1)r)$, for all $i \geq 1$ (where $r = r_K(f)$), we have

$$|G| \leq n \prod_{1 \leq i \leq l} (n - (m_i - 1)r)\,.$$

Remark 6.2.0.1. *We have $a_1 = n(n-1) \implies r_K(f) = 1$. The converse is not true. Consider Example 6.1.3 for n odd and composite. Then $r_K(f) = 1$ and $a_1 \leq n\phi(n) < n(n-1)$.*

Now since $H_i = \sigma_i H \sigma_i^{-1}$ for all i, we have that $N_G(H_i) = \sigma_i N_G(H) \sigma_i^{-1}$. From Thm. 4.1.1 (3), we have $r_K(K_m) = [N_G(J_m) : J_m]$.

Example 6.2.1. *Let f be an irreducible polynomial such that $|G| = np$ and $|H| = p$ where $p \nmid n$. Then length of cluster tower is 3 and degree sequence is n, np. Both degree sequence and length of cluster tower are independent of the ordering of the β_i's. As a particular case, $G = \mathfrak{A}_4$ for a degree-4 irreducible polynomial f.*

Chapter 7

Root Capacity

In this chapter, we introduce the concept of Root capacity as a generalisation of cluster size. We begin the chapter with some observations about the group of automorphisms of finite extensions. Then we prove some properties of root capacity. We conclude the chapter with an interesting theorem.

7.1 The Group of Automorphisms of Finite Extensions

Let F_1/F_2 be a finite extension of fields. Let $\mathrm{Aut}(F_1/F_2)$ denote the group of F_2-automorphisms of F_1. In this section, we describe some of the facts about this group and later use it to prove some results about root clusters.

Proposition 7.1.1. *(Bhagwat, Jaiswal) (Prop 6.1.1 in [3])*

Let L/K and M/L be extensions. Then

1. $\mathrm{Aut}(M/L)$ *is a subgroup of* $\mathrm{Aut}(M/K)$. *Hence,* $r_L(M) \mid r_K(M)$.

2. *Suppose* $\sigma|_L \in \mathrm{Aut}(L/K)$ *for any* $\sigma \in \mathrm{Aut}(M/K)$. *Then* $\mathrm{Aut}(M/L) \trianglelefteq \mathrm{Aut}(M/K)$ *and* $r_K(M) \mid (r_L(M)\, r_K(L))$.

3. *Suppose* $\sigma|_L \in \mathrm{Aut}(L/K)$ *for any* $\sigma \in \mathrm{Aut}(M/K)$. *Then any* $\lambda \in \mathrm{Aut}(L/K)$ *can be extended to* $\tilde{\lambda} \in \mathrm{Aut}(M/K) \iff r_K(M) = r_L(M) r_K(L)$. *In this case* M/K *is obtained by weak cluster magnification of* L/K *with magnification factor* $r_L(M)$.

Proof. From Thm. 4.1.1 (3), $r_K(L) = |\mathrm{Aut}(L/K)|$. Now (1) is easy to see.

Proof of (2): Suppose we have $\sigma|_L \in \mathrm{Aut}(L/K)$ for any $\sigma \in \mathrm{Aut}(M/K)$. Then we can define the a homomorphism $\Phi : \mathrm{Aut}(M/K) \to \mathrm{Aut}(L/K)$ by mapping σ to $\sigma|_L$. Hence, $\ker(\Phi) = \mathrm{Aut}(M/L)$ and so $\mathrm{Aut}(M/L) \trianglelefteq \mathrm{Aut}(M/K)$. Also, $\mathrm{Aut}(M/K)/\mathrm{Aut}(M/L) \hookrightarrow \mathrm{Aut}(L/K)$. Thus $r_K(M) \mid (r_L(M)\, r_K(L))$.

Proof of (3): This corresponds to the homomorphism Φ being surjective.

□

Remark 7.1.1.1. *The homomorphism* Φ *in above proof is not surjective in general. For example, when* $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}), M = \mathbb{Q}(\sqrt[4]{2})$, *then* Φ *is not surjective.*

Proposition 7.1.2. *(Bhagwat, Jaiswal) (Prop 6.1.3 in [3])*

Consider extensions L/K *and* M/L. *Then for* $\sigma \in \mathrm{Aut}(M/K)$ *we have*

$$\sigma \in N_{\mathrm{Aut}(M/K)}(\mathrm{Aut}(M/L)) \iff \sigma|_{M^{\mathrm{Aut}(M/L)}} \in \mathrm{Aut}(M^{\mathrm{Aut}(M/L)}/K).$$

Hence also

$$N_{\mathrm{Aut}(M/K)}(\mathrm{Aut}(M/L))/\mathrm{Aut}(M/L) \hookrightarrow \mathrm{Aut}(M^{\mathrm{Aut}(M/L)}/K).$$

Proof. We will mimic Perlis' proof of Thm. 4.1.1 (3) (see [17, first proposition]).

For notational simplicity, (just for this proof) let G_1, G_2 denote the groups $\mathrm{Aut}(M/K)$ and $\mathrm{Aut}(M/L)$, respectively.

If $\sigma \in N_{G_1}(G_2)$, then $\sigma\, G_2\, \sigma^{-1} = G_2$. Let $x \in M^{G_2}$. Since $\sigma\, G_2 x = G_2 \sigma x$, we have $\sigma x = G_2 \sigma x$. Hence $\sigma x \in M^{G_2}$.

Conversely, suppose $\sigma \notin N_{G_1}(G_2)$. Then there exists $\lambda \in G_2$ such that $\sigma^{-1}\lambda\sigma \notin G_2$. We know $\mathrm{Aut}(M/L) = \mathrm{Aut}(M/M^{G_2})$. Hence there exists $x \in M^{G_2}$ such that $\sigma^{-1}\lambda\sigma x \neq x$. That is $\lambda\sigma x \neq \sigma x$. Hence $\sigma x \notin M^{G_2}$. Thus $\sigma|_{M^{G_2}} \notin \mathrm{Aut}(M^{G_2}/K)$.

Then we can define the map $\Phi : N_{G_1}(G_2) \to \mathrm{Aut}(M^{G_2}/K)$ by mapping σ to $\sigma|_{M^{G_2}}$. Hence, $\ker(\Phi) = G_2$ and also we have

$$N_{G_1}(G_2)/G_2 \hookrightarrow \mathrm{Aut}(M^{G_2}/K).$$

□

Corollary 7.1.0.1. Suppose M/L is Galois. Then we can replace $M^{\mathrm{Aut}(M/L)}$ by L in above Prop. 7.1.2. If additionally we have $\mathrm{Aut}(M/L) \trianglelefteq \mathrm{Aut}(M/K)$, then $\sigma|_L \in \mathrm{Aut}(L/K)$ for any $\sigma \in \mathrm{Aut}(M/K)$. This is converse to Prop. 7.1.1 (2) under the condition M/L is Galois.

We will also give a direct proof of second part of this corollary without referring to above Prop. 7.1.2.

Proof. Let $\sigma \in \mathrm{Aut}(M/K)$. Now $\mathrm{Aut}(M/\sigma(L)) = \sigma\mathrm{Aut}(M/L)\sigma^{-1}$. Since $\mathrm{Aut}(M/L) \trianglelefteq \mathrm{Aut}(M/K)$, we have $\mathrm{Aut}(M/\sigma(L)) = \mathrm{Aut}(M/L)$. Also $|\mathrm{Aut}(M/\sigma(L))| = |\mathrm{Aut}(M/L)| = [M : L]$ since M/L is Galois. Since $\sigma(L)$ is isomorphic to L, $[M : L] = [M : \sigma(L)]$. Hence, $M/\sigma(L)$ is also Galois. Thus $L = M^{\mathrm{Aut}(M/L)} = M^{\mathrm{Aut}(M/\sigma(L))} = \sigma(L)$. Therefore $\sigma|_L \in \mathrm{Aut}(L/K)$. □

By letting $M = \tilde{L}$ we have the following corollary, i.e., [17, first Prop.].

Corollary 7.1.0.2. Let $G = \mathrm{Gal}(\tilde{L}/K)$ and $H = \mathrm{Gal}(\tilde{L}/L)$. Then we have $\sigma \in N_G(H) \iff \sigma|_L \in \mathrm{Aut}(L/K)$. Hence $\sigma H \mapsto \sigma|_L$ defines an isomorphism $N_G(H)/H \to \mathrm{Aut}(L/K)$.

Proof. Now $\tilde{L}^H = L$ and the injective map $N_G(H)/H \hookrightarrow \mathrm{Aut}(L/K)$ is surjective because any automorphism of L/K extends to an automorphism of $\tilde{L}/K$. □

Remark 7.1.2.1. *There is an interesting result about automorphism groups. Although the Inverse Galois Problem is still not solved for every finite group over rationals, the Inverse Automorphism Group Problem is solved for every group not just over rationals but also over a bigger class of fields.*

Recall Def 4.2.2 of Hilbertian fields. In a recent work in 2018, Francois Legrand and Elad Paran have proved in Thm 1.1 [14] that, every finite group G occurs as the automorphism group of infinitely many distinct finite extensions of any given Hilbertian field K.

7.2 Root Capacity

We saw that the cluster size counts the number of roots appearing in the root cluster of α that is the number of roots of minimal polynomial of α over K which are contained in $K(\alpha)$. We can ask for an analogous quantity associated to an extension M/K. We introduce the following concept as a generalisation of cluster size. One can easily appreciate the usage of 'capacity'.

Definition 7.2.0.1. (Bhagwat, Jaiswal) (Def 6.2.1 in [3])

Let $\alpha \in \bar{K}$ and let f be minimal polynomial of α over K. For an extension M/K, let $\rho_K(M, \alpha)$ be the number of roots of f that are contained in M. We call this quantity as the root capacity of M with respect to α (with base field K fixed).

Let L/K be an extension. By primitive element theorem $L = K(\alpha)$ for some $\alpha \in \bar{K}$. We define $\rho_K(M, L) := \rho_K(M, \alpha)$ which is well defined by the following proposition. We call this quantity as the root capacity of M with respect to L (with base field K fixed).

Proposition 7.2.1. *(Bhagwat, Jaiswal) (Prop 6.2.2 in [3])*

Let $\alpha, \beta \in \bar{K}$ and let $K(\alpha) = K(\beta)$. Then for any M/K, we have $\rho_K(M, \alpha) = \rho_K(M, \beta)$.

Proof. Let the degree-n minimal polynomials of α and β over K be f and g respectively. Let $\{\alpha_i\}_{1 \le i \le n}$ and $\{\beta_i\}_{1 \le i \le n}$ be all the roots of f and g in $\bar{K}$ with $\alpha_1 = \alpha, \beta_1 = \beta$. Since $K(\alpha) = K(\beta)$, we have polynomials μ and λ over K with degrees $\le (n-1)$ such that $\alpha = \lambda(\beta)$ and $\beta = \mu(\alpha)$. Now, $g(\beta) = 0$. Hence $g(\mu(\alpha)) = 0$. Thus $f | g \circ \mu$. Hence $g(\mu(\alpha_i)) = 0$ for all i. Hence each $\mu(\alpha_i) = \beta_j$ for some j.

We also have $\alpha = \lambda \circ \mu(\alpha)$. Hence $f(x) | (\lambda \circ \mu(x) - x)$. Thus $\lambda \circ \mu(\alpha_i) = \alpha_i$ for all i. Hence μ is a bijection from the set of roots of f to set of roots of g. By relabelling we can assume $\mu(\alpha_i) = \beta_i$ for all i. Thus $\lambda(\beta_i) = \alpha_i$ for all i. Hence for any i, we have $\alpha_i \in M \iff \beta_i \in M$.

□

Remark 7.2.1.1. *Let α and f be as in Def. 7.2.0.1. Now, $\rho_K(K(\alpha), \alpha) = r_K(f)$. Thus the above proposition proves that given an extension L/K, the cluster size is the same for all irreducible polynomials that are the minimal polynomials of primitive elements of L over K (Corollary 1 in [13]). This proof is independent of Thm. 4.1.1 (3).*

We prove some properties of root capacity.

Proposition 7.2.2. *(Bhagwat, Jaiswal) (Prop 6.2.4 in [3])*

Let M/K be extension of L/K. Then the following hold.

1. $\rho_K(L,K) = 1$ *and* $\rho_K(L,L) = r_K(L)$ *and* $\rho_K(M,L) \geq r_K(L)$ *and* $\rho_K(\tilde{L},L) = [L:K]$.
2. $\rho_K(M,L) = r_K(L) \implies \sigma|_L \in \mathrm{Aut}(L/K)$ *for any* $\sigma \in \mathrm{Aut}(M/K)$.

Proof. The property (1) is easy to see.

Proof of (2): Let $L = K(\alpha)$ for $\alpha \in \bar{K}$ with f as the minimal polynomial of α over K with roots $\{\alpha_i\}_{1\leq i\leq n}$. Then $\rho_K(M,L) = r_K(L)$ is equivalent to the statement $\alpha_i \in M \iff \alpha_i \in L$. If $\sigma \in \mathrm{Aut}(M/K)$, then $\sigma|_L$ maps α to an $\alpha_i \in M$. Hence, $\sigma|_L(\alpha) \in L$. Thus $\sigma|_L \in \mathrm{Aut}(L/K)$.

□

The following lemma is reformulation of [18, Thm. 2] for a perfect base field K.

Lemma 7.2.3. *Let $\alpha \in \bar{K}$. Then for any M/K we have $r_K(f)|\rho_K(M,\alpha)$. Hence for any L/K, we have $r_K(L)|\rho_K(M,L)$. That is $\rho_K(M,L) = a.r_K(L)$ where $0 \leq a \leq s_K(L)$.*

Proof. The proof of Theorem 4.1.1 (2) gives a partition of the set of roots of f into $s_K(f)$ many subsets of equal size $r_K(f)$, where each subset satisfies the property that in any extension of K, one of the roots being present implies the presence of the remaining ones. □

The integer a obtained in Lem. 7.2.3 can be described as follows.

Proposition 7.2.4. *(Bhagwat, Jaiswal) (Prop 6.2.6 in [3]). We have*

1. *a is number of distinct fields inside $M \cap \tilde{L}$ isomorphic to L over K.*
2. *$a = |Z|$ with $Z = \{1 \leq i \leq s \mid$ there exists $\sigma \in \sigma_i N_G(H)$ with $\sigma(L) \subseteq M \cap \tilde{L}\}$ where σ_i are coset representatives of $N_G(H)$ in G.*

Proof.

1. In Lemma 7.2.3, we have that the set of roots of f in M is union of a clusters of roots of f. From proof of Lemma 4.4.1, we are done.

2. From the proof at the beginning of Sec. 4.4, we have that $s_K(L)$ is number of distinct subgroups conjugate to $H = \mathrm{Gal}(\tilde{L}/L)$ in $G = \mathrm{Gal}(\tilde{L}/K)$ which is $[G : N_G(H)]$. From (1), we are done.

□

Example 7.2.5. *Let L_k be as in proof of Thm. 4.4.2. Let $L = L_1$. So $r_K(L) = 1, s_K(L) = n$ and $\tilde{L} = L_{n-1}$. Also $\rho_K(L_k, L) = k$ for $1 \leq k \leq (n-2)$. Also $\rho_K(L_2, L) = r_K(L_2) = 2$.*

Example 7.2.6. *Let notation be as in section 6.2. Let $L = K_1$ and $m_0 = 1$. Then for $i \geq 0$ and $m_i \leq m < m_{i+1}$, we have $\rho(K_m, L) = \rho(K_{m_i}, L) \geq (m_{i+1} - 1)r_K(L)$.*

Proposition 7.2.7. *(Bhagwat, Jaiswal) (Prop 6.2.9 in [3]) Let M_1/K and M_2/K be extensions of L/K contained in $\bar{K}$. Then*

$$\rho_K(M_1M_2, L) \geq \rho_K(M_1, L) + \rho_K(M_2, L) - \rho_K(M_1 \cap M_2, L).$$

Proof. Consider the set of s many representatives of clusters of minimal polynomial of a primitive element of L/K. Consider the subsets of representatives contained in M_1 and M_2 and let a and b be their respective cardinalities. Hence $\rho_K(M_1) = a.r_K(L)$ and $\rho_K(M_2) = b.r_K(L)$. Let i be cardinality of intersection of these two sets. Hence $\rho_K(M_1 \cap M_2, L) \geq i.r_K(L)$. Also since cardinality of union of these two sets is $a + b - i$. Hence $\rho_K(M_1M_2, L) \geq (a + b - i).r_K(L)$. Hence we are done.

□

Example 7.2.8. *Let p be a prime and let $a = \sqrt[12]{p}$ and $b = \xi_{12}$. Let $L = \mathbb{Q}(a)$ and $M_1 = \mathbb{Q}(a, ab^2)$ and $M_2 = \mathbb{Q}(a, ab^3)$. Thus $M_1M_2 = \tilde{L}$. So $\rho_K(M_1M_2, L) = 12, \rho_K(M_1, L) = 6, \rho_K(M_2, L) = 4$. Hence $\rho_K(M_1M_2, L) > \rho_K(M_1, L) + \rho_K(M_2, L) - \rho_K(M_1 \cap M_2, L)$. The inequality is strict here.*

Let M/K be an extension of L/K and $\rho_K(M,L) = a.r_K(L)$ for some $0 \leq a \leq s_K(L)$. Let $L = K(\alpha)$ for some $\alpha \in \bar{K}$ with f as the minimal polynomial over K. Relabel the roots $\{\alpha_i\}_{1\leq i\leq n}$ such that $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ forms a set of representatives of the clusters of roots of f such that $\alpha_i \in M \iff 1 \leq i \leq a$. Let $L_M := K(\alpha_1, \alpha_2, \ldots, \alpha_a)$. The roots of f in L_M and M are same. We can observe that $L_M = \tilde{L}^T$ where $T = \bigcap_{i\in Z} \sigma_i H \sigma_i^{-1}$ with notations as in Prop. 7.2.4.

Proposition 7.2.9. *(Bhagwat, Jaiswal) (Prop 6.2.11 in [3])*

Let M/K be extension of L/K. Let L_M be as above. Then the following hold.

1. *L_M is independent of choice of primitive root for L/K that is L_M is well defined for a given M and L.*
2. *$L_M \subseteq M \cap \tilde{L}$.*
3. *$\rho_K(L_M, L) = \rho_K(M, L)$. For $K \subset P \subset M$, we have $\rho_K(M,L) = \rho_K(P,L)$ if and only if $L_M \subset P$.*
4. *$\rho_K(M,L) = r_K(L) \iff L = L_M$.*
5. *$\rho_K(M, L_M) = r_K(L_M)$. Thus we have $\sigma|_{L_M} \in \mathrm{Aut}(L_M/K)$ for any $\sigma \in \mathrm{Aut}(M/K)$.*
6. *$M \cap \tilde{L} = L \implies \rho_K(M,L) = r_K(L)$. Also $M \cap \tilde{L} = K \implies \rho_K(M,L) = 0$.*
7. *If M/K is obtained by strong cluster magnification from L/K then $\rho_K(M,L) = r_K(L)$.*

Proof. Proof of (1): From the proof of Prop. 7.2.1 it follows that if $K(\alpha) = K(\beta)$ then there is a relabelling of $\{\beta_i\}_{1\leq i\leq n}$ such that $K(\alpha_i) = K(\beta_i)$. Hence, for the above labelling of $\{\beta_i\}_{1\leq i\leq n}$, we have $K(\alpha_1, \alpha_2, \ldots, \alpha_a) = K(\beta_1, \beta_2, \ldots, \beta_a)$.

Proofs of (2), (3), (4) follow from definition of L_M.

Proof of (5): From Lem. 7.2.3, $\rho(M, L_M) = a.r_K(L_M)$ for $a \leq s_K(L_M)$. From Prop. 7.2.4 (1), a is number of distinct fields inside $M \cap \tilde{L}$ isomorphic to L_M over K. By definition of L_M, we have $a = 1$. The second assertion follows from Prop. 7.2.2 (2).

Proof of (6): Since $M \cap \tilde{L} = L$, we use (2) to conclude that $L = L_M$. Hence by (4), we are done.

Proof of (7): If the extension M/K is obtained by strong cluster magnification from L/K, then we have $M \cap \tilde{L} = L$ (see Def. 5.2.0.1 and Lem. 5.1.1). □

Remark 7.2.9.1. *The statement $L_M = M \cap \tilde{L}$ and the statement $\rho_K(M, L) = 0 \implies M \cap \tilde{L} = K$ are not true in general. Let $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[4]{2})$ and $M = \mathbb{Q}(\sqrt[6]{2})$. Hence $\tilde{L} = \mathbb{Q}(\sqrt[4]{2}, \iota)$ and $M \cap \tilde{L} = \mathbb{Q}(\sqrt{2})$ and $L_M = \mathbb{Q}$.*

Theorem 7.2.10. *(Bhagwat, Jaiswal) (Thm 6.2.13 in [3])*

If $M \cap \tilde{L} = L$ and $[M : L] = r_K(M)/r_K(L)$, then M/L is Galois.

Proof. Suppose $M \cap \tilde{L} = L$. Hence from Prop. 7.2.9 (6), Prop. 7.2.2 (2) and Prop. 7.1.1 (2), we have $r_K(M)|(r_L(M)r_K(L))$. Since $r_K(M) = [M : L]r_K(L)$, we conclude that $r_L(M) = [M : L]$ and M/L is Galois.

□

Chapter 8

Unique Chains for Extensions

In this chapter, we introduce the concept of unique descending and ascending chains for extensions and prove the important properties of unique chains. We also compute unique ascending/ descending chains for some interesting examples.

8.1 Unique Descending Chains

Theorem 8.1.1. *(Bhagwat, Jaiswal) (Thm 7.1.1 in [3])*

Let L/K be a nontrivial finite extension. Let $G = \mathrm{Gal}(\tilde{L}/K)$ and $H = \mathrm{Gal}(\tilde{L}/L)$.

1. *The extension $N = \tilde{L}^{N_G(H)}$ is the unique intermediate extension N/K such that L/N is Galois with degree $[L : N] = r_K(L)$. Hence the degree $[N : L] = s_K(L)$.*

2. *There is a unique strictly descending chain of subextensions*

$$L = N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_k$$

such that for all $i \geq 1$, N_{i-1}/N_i is Galois extension with degree $[N_{i-1} : N_i] = r_K(N_{i-1})$, with the chain terminating at N_k for which $r_K(N_k) = 1$. Hence the degree $[N_i : K] = s_K(N_{i-1})$ for all $i \geq 1$ and $s_K(N_{k-1}) = s_K(N_k)$.

This unique strictly descending chain of subextensions corresponds to the unique strictly ascending chains of subgroups of G

$$H = H_0 \trianglelefteq N_G(H_0) = H_1 \trianglelefteq N_G(H_1) = H_2 \trianglelefteq \cdots \trianglelefteq N_G(H_{k-1}) = H_k$$

such that $N_G(H_k) = H_k$. *Hence* $r_K(N_i) = [H_{i+1} : H_i]$ *and* $s_K(N_i) = [G : H_{i+1}]$.

3. L/K *is obtained by weak cluster magnification from* N_k/K *with magnification factor* $r_K(L)$.
4. $N_k = K \iff N_{k-1}/K$ *is Galois.*
5. $r_K(L) = 1 \iff N_G(H) = H \iff$ *the unique descending chain is singleton* L.
6. L/K *is Galois* $\iff N_G(H) = G \iff$ *the unique descending chain is* $L \supsetneq K$.
7. $N_G(H) \trianglelefteq G \iff$ *the unique descending chain is* $L \supsetneq N \supsetneq K$.

Proof.

Proof of (1): Let $N = \tilde{L}^{N_G(H)}$. Thus L/N is Galois as $H \trianglelefteq N_G(H)$. We have $[L : N] = [N_G(H) : H]$. Hence by Thm. 4.1.1 (3), $[L : N] = r_K(L)$. Suppose N'/K is another intermediate extension such that L/N' is Galois and $[L : N'] = r_K(L)$. Since L/N' is Galois, we have $H \trianglelefteq \mathrm{Gal}(\tilde{L}/N') \subseteq G$. Thus $\mathrm{Gal}(\tilde{L}/N') \subseteq N_G(H)$. Hence $N \subseteq N'$. Since $[L : N] = [L : N']$, we have $N = N'$.

Proof of (2): Let $N_0 = L$, From (1), we can inductively choose N_i for each $i \geq 1$. Let N_i/K be the unique intermediate extension of N_{i-1}/K such that N_{i-1}/N_i is Galois with degree $[N_{i-1} : N_i] = r_K(N_{i-1})$. The chain terminates since L/K is finite.

Proofs of (3)-(6) are easy to see.

Proof of (7): We have $N_G(H) = G \iff H \trianglelefteq G \iff H = 1$. We also have $N_G(H) \trianglelefteq G \implies N_G(H) \neq H$. Since if $N_G(H) = H$, then by assumption, $H \trianglelefteq G$. Hence $H = 1$, so $N_G(H) = G$ which contradicts the assumption. Hence, $N_G(H) \trianglelefteq G \iff N_G(H) \neq H$ and $H \neq 1$ and $N_G(H) \trianglelefteq G \iff r_K(L) \neq 1$ and L/K is not Galois and N/K is Galois $\iff$ the unique descending chain is $L \supsetneq N \supsetneq K$.

□

Remark 8.1.1.1. *Alternate proof for Thm. 8.1.1 (1).*

Let $N = L^{\mathrm{Aut}(L/K)}$. Hence L/N is Galois and $[L : N] = |\mathrm{Aut}(L/K)|$. Hence by Thm. 4.1.1 (3), $[L : N] = r_K(L)$. Suppose N'/K is another intermediate extension such that L/N' is Galois and $[L : N'] = r_K(L)$. Since L/N' is Galois, we have $N' = L^{\mathrm{Aut}(L/N')}$ and $[L : N'] = |\mathrm{Aut}(L/N')|$. Hence $|\mathrm{Aut}(L/N')| = |\mathrm{Aut}(L/K)|$. By Prop. 7.1.1 (1), $\mathrm{Aut}(L/N') \subset \mathrm{Aut}(L/K)$. Thus $\mathrm{Aut}(L/N') = \mathrm{Aut}(L/K)$. Hence $N' = N$.

Because of uniqueness, $\tilde{L}^{N_G(H)} = L^{\mathrm{Aut}(L/K)}$. This can also be seen in this way. Since $\tilde{L}^{N_G(H)} \subset \tilde{L}^H = L$ and $L^{\mathrm{Aut}(L/K)} \subset L$, by identifying $N_G(H)/H$ and $\mathrm{Aut}(L/K)$ through the map in Cor. 7.1.0.2, we have $\tilde{L}^{N_G(H)} = L^{\mathrm{Aut}(L/K)}$.

Remark 8.1.1.2. *Equivalently we can state Thm. 8.1.1 (1) as follows: There exists a unique intermediate extension N/K such that L/N is Galois of maximum possible degree. This is because, since L/N is Galois, we have $[L : N] = |\mathrm{Aut}(L/N)|$ and we also have $\mathrm{Aut}(L/N) \subset \mathrm{Aut}(L/K)$. Hence $[L : N]$ is bounded by $r_K(L)$.*

This also gives an equivalent definition of $r_K(L)$ as the maximum possible degree of L/N where N is intermediate field of L/K such that L/N is Galois.

Proposition 8.1.2. *(Bhagwat, Jaiswal) (Prop 7.1.4 in [3])*

Let L/K be a nontrivial finite extension and N be the unique intermediate extension for L/K as in Thm. 8.1.1 (1). Suppose $L = K(\alpha)$ for a primitive element $\alpha \in \bar{K}$ with minimal polynomial f over K such that $r_K(f) = r$ and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ be the roots of f contained in L. Then

$$N = K(t_1, t_2, \ldots, t_r)$$

where t_i are elementary symmetric sums of α_i for $1 \leq i \leq r$.

Proof. Let h be the minimal polynomial of α over N. The degree of h is $r = |Aut(L/N)|$. Since $Aut(L/N) = Aut(L/K)$, it follows that $h = \Pi_{1 \leq i \leq r}(x - \alpha_i) = x^r - t_1 x^{r-1} + \cdots + (-1)^r t_r$. Now $K(t_1, t_2, \ldots, t_r) \subset N$. Since h is a polynomial over $K(t_1, t_2, \ldots, t_r)$ which α satisfies. we conclude that h is the minimal polynomial of α over $K(t_1, t_2, \ldots, t_r)$. Thus $N = K(t_1, t_2, \ldots, t_r)$. □

8.2 Unique Ascending Chains

We mention an analogue of Thm. 8.1.1 in this section. The proof is similar.

First some notations: For any subgroup H of a group G, we denote by H^G, the normal closure of H in G, i.e., the intersection of all normal subgroups of G that contain H.

Theorem 8.2.1. *(Bhagwat, Jaiswal) (Thm 7.2.1 in [3])*

Let L/K be a nontrivial finite extension. Let $G = \mathrm{Gal}(\tilde{L}/K)$ and $H = \mathrm{Gal}(\tilde{L}/L)$ be as earlier.

1. *The extension $F = \tilde{L}^{H^G}$ is the unique intermediate extension F/K such that F/K is Galois with maximum possible degree.*
2. *We define the ascending index $t_K(L)$ of L/K by $t_K(L) := [F : K]$. Let $u_K(L) := [L : F]$. Thus $t_K(L)\, u_K(L) = [L : K]$. We have $t_K(L) = [G : H^G]$ and $u_K(L) = [H^G : H]$. We also have $r_K(L) \mid t_K(L)\, r_F(L)$.*
3. *There exists a unique strictly ascending chain inside L, i.e.,*

$$K = F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_k$$

   such that for all $i \geq 1$, we have F_i/F_{i-1} is Galois with maximum possible degree with the chain terminating at F_k where $t_{F_k}(L) = 1$.

   This unique strictly ascending chain of subextensions corresponds to the unique strictly descending chains of subgroups of G

$$G = G_0 \supsetneq H^{G_0} = G_1 \supsetneq H^{G_1} = G_2 \supsetneq \cdots \supsetneq H^{G_{k-1}} = G_k$$

   such that $H^{G_k} = G_k$. Hence $t_{F_i}(L) = [G_i : G_{i+1}]$ and $u_{F_i}(L) = [G_{i+1} : H]$.
4. *$F_k = L \iff L/F_{k-1}$ is Galois.*
5. *$t_K(L) = 1 \iff H^G = G \iff$ the unique ascending chain is singleton K.*
6. *L/K is Galois $\iff H^G = 1 \iff H^G = H \iff$ the unique ascending chain is $K \subsetneq L$.*

7. $H \trianglelefteq H^G \iff H^G \neq G$ *and* $H^G \neq H$ *and* $H \trianglelefteq H^G \iff$ *the unique ascending chain is* $K \subsetneq F \subsetneq L$.

The following result connects the unique descending chain and unique ascending chain for a nontrivial finite extension L/K.

Proposition 8.2.2. *(Bhagwat, Jaiswal) (Prop 7.2.2 in [3])*

Let L/K *be a nontrivial finite extension. Let* N *be as in Thm. 8.1.1 and* F *be as in Thm. 8.2.1.*

1. $N_G(H) = G \iff r_K(L) = [L : K] \iff t_K(L) = [L : K] \iff H^G = H$.
2. $H \trianglelefteq H^G \iff H^G \subset N_G(H) \iff N \subset F$.
3. $N_G(H) \trianglelefteq G \implies H^G \subset N_G(H)$.
4. $H^G = N_G(H) \implies N_G(H) \trianglelefteq G$ *and* $H \trianglelefteq H^G$.
5. $H^G = N_G(H) \iff N = F \iff$ *the unique descending chain is* $L \supsetneq N \supsetneq K$ *and the unique ascending chain is* $K \subsetneq F \subsetneq L$ *and they both coincide. In this case we have* $r_K(L)\, t_K(L) = [L : K]$ *and* $t_K(L) = s_K(L)$.

Example 8.2.3. *For a degree* 4 *non-Galois extension* L/K*, we have* $N = F$*. In particular,* $K = \mathbb{Q}$*,* $L = \mathbb{Q}(\sqrt[4]{2})$ *and hence* $N = F = \mathbb{Q}(\sqrt{2})$.

8.3 Interesting Examples

In this section, we will compute the unique ascending /descending chains for some examples.

Example 8.3.1. *(Bhagwat, Jaiswal) (Prop 7.3.1 in [3])*

Let the notation and conditions be as in Example 6.1.3. Let $L = \mathbb{Q}(a)$ *and* $K = \mathbb{Q}$ *and let* v_2 *be the standard* 2*-adic valuation.*

1. *Let* $N_i = \mathbb{Q}(a^{2^i})$. *Then the unique descending chain is* $L = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_{v_2(n)}$.

2. *Let* $F_i = \mathbb{Q}(a^{n/2^i})$. *Then the unique ascending chain is* $K = F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_{v_2(n)}$.

Proof. Identifying $G = \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ with $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ we have $H = \{0\} \times (\mathbb{Z}/n\mathbb{Z})^\times \subseteq G$. Now G has the semidirect product group law

$$(\alpha, u) \cdot (\beta, v) = (\alpha + u \cdot \beta, uv)$$

as in [11] where $u \cdot \beta$ is usual multiplication $u\beta$ in the ring $\mathbb{Z}/n\mathbb{Z}$. Thus $(\alpha, u)^{-1} = (-u^{-1}\alpha, u^{-1})$ and

$$(\alpha, u) \cdot (0, v) \cdot (\alpha, u)^{-1} = (\alpha - v\alpha, v)$$

Proof of (1):

If $(\alpha, u) \in N_G(H)$ then $\alpha = v\alpha$ for all $v \in (\mathbb{Z}/n\mathbb{Z})^\times$.

If n is odd then $2 \in (\mathbb{Z}/n\mathbb{Z})^\times$ and in particular $2\alpha = \alpha$. Thus $\alpha = 0$ and $N_G(H) = H$. Hence $r_K(L) = 1$. Hence by Thm. 8.1.1(5), the unique descending chain is singleton L.

If n is even, then $(n/2)(1 - v) = 0$ for all $v \in (\mathbb{Z}/n\mathbb{Z})^\times$ as all these v are given by odd integers mod n. Since $-1 \in (\mathbb{Z}/n\mathbb{Z})^\times$, we get $2\alpha = 0$. Hence $\alpha = 0$ or $n/2$. Thus $N_G(H)$ can be identified with the set $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times$ where $\mathbb{Z}/2\mathbb{Z}$ is generated by the element $(n/2, 1)$ of G mapping a to $-a$ and b to b. Also $r_K(L) = 2$. Hence $\tilde{L}^{N_G(H)} = \mathbb{Q}(a^2) = N_1$.

Let $\tilde{N}_1$ be Galois closure of N_1/K. Hence $\tilde{N}_1 = \mathbb{Q}(a^2, b^2)$. Also since $\mathbb{Q}(a) \cap \mathbb{Q}(b) = \mathbb{Q}$. Hence $\mathbb{Q}(a^2) \cap \mathbb{Q}(b^2) = \mathbb{Q}$. Hence $\mathrm{Gal}(\tilde{N}_1/K)$ can be identified with $\mathbb{Z}/(n/2)\mathbb{Z} \rtimes (\mathbb{Z}/(n/2)\mathbb{Z})^\times$. If $n/2$ is even, we can repeat the process for N_1 and get N_2. The process will terminate at $N_{v_2(n)}$ as $n/v_2(n)$ is odd.

Proof of (2):

Now H^G is generated by elements of the form $(\alpha - v\alpha, v)$ with $\alpha \in \mathbb{Z}/n\mathbb{Z}, v \in (\mathbb{Z}/n\mathbb{Z})^\times$.

If n is odd then $2 \in (\mathbb{Z}/n\mathbb{Z})^\times$. Thus $(\alpha - 2\alpha, v) = (-\alpha, v) \in H^G$ for any α, v. Thus $H^G = G$. Hence $t_K(L) = 1$. Hence by Thm. 8.2.1(5), the unique ascending chain is singleton K.

If n is even then all $v \in (\mathbb{Z}/n\mathbb{Z})^\times$ are given by odd integers mod n. Thus all $\alpha - v\alpha$

are even mod n. Since $-1 \in (\mathbb{Z}/n\mathbb{Z})^\times$, we get $(2\alpha, v) \in H^G$ for any α, v. Thus $H^G = \mathbb{Z}/(n/2)\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ where $\mathbb{Z}/(n/2)\mathbb{Z}$ is generated by the element $(2,1)$ of G mapping a to ab^2 and b to b. Also $t_K(L) = 2$. Hence $\tilde{L}^{H^G} = \mathbb{Q}(a^{n/2}) = F_1$.

Let L_1 be Galois closure of L/F_1. Hence $L_1 = \mathbb{Q}(a, b^2)$. Also since $\mathbb{Q}(a) \cap \mathbb{Q}(b) = \mathbb{Q}$. Hence $L \cap \mathbb{Q}(b^2) = \mathbb{Q}$. By Lemma 5.1.1, $L \cap F_1(b^2) = F_1$. Hence $\mathrm{Gal}(L_1/F_1)$ can be identified with $\mathbb{Z}/(n/2)\mathbb{Z} \rtimes (\mathbb{Z}/(n/2)\mathbb{Z})^\times$. If $n/2$ is even, we can repeat the process for F_1 and get F_2. The process will terminate at $F_{v_2(n)}$ as $n/v_2(n)$ is odd.

□

Remark 8.3.1.1. *The Part (1) above is also true for the case not covered, that is n is even and $\sqrt{c} \in \mathbb{Q}(b)$. The following proof works in general. We know that $N_1 = L^{\mathrm{Aut}(L/K)}$. Since n is even, $\mathrm{Aut}(L/K)$ has 2 elements mapping a to a and a to $-a$. Hence $\mathbb{Q}(a^2) \subset L^{\mathrm{Aut}(L/K)}$. Now since $x^n - c$ is minimal polynomial for a over $\mathbb{Q}$. Hence a^2 satisfies $x^{n/2} - c$. We claim that it is indeed the minimal polynomial for a^2 over $\mathbb{Q}$. If not, then let $f(x)$ be minimal polynomial for a^2 with degree $< n/2$. Then a satisfies the polynomial $f(x^2)$ which has degree $< n$ which gives a contradiction. Hence $[\mathbb{Q}(a^2) : \mathbb{Q}] = n/2$. Thus $N_1 = \mathbb{Q}(a^2)$. Proceeding similarly we get the unique descending chain.*

Example 8.3.2. *Consider the case in Example 8.3.1 with $n \equiv 2$ mod 4. Hence for $L = \mathbb{Q}(a)$ and $K = \mathbb{Q}$, we have $L \supsetneq N$ to be the unique descending chain with $N = \mathbb{Q}(a^2)$ and $K \subsetneq F$ to be the unique descending chain with $F = \mathbb{Q}(a^{n/2})$. We can show that L/K is obtained by strong cluster magnification from N/K through F/K.*

Now F/K is clearly Galois. Since $(n/2, 2) = 1$. Hence $NF = L$. Thus $N \cap F = K$. Since $\mathbb{Q}(a) \cap \mathbb{Q}(b) = K$. Hence $\mathbb{Q}(a) \cap \mathbb{Q}(b^2) = K$. Thus by Lemma 5.1.1, $\mathbb{Q}(a) \cap \mathbb{Q}(a^2, b^2) = \mathbb{Q}(a^2)$. That is $\tilde{N} \cap L = N$. Hence $\tilde{N} \cap F = K$.

Theorem 8.3.3. *(Bhagwat, Jaiswal) (Thm 7.3.4 in [3])*

Let f be an irreducible polynomial over number field K with given $n > 2$ and $1 < r < n$ with $r|n$ as in proof of Thm. 4.3.1 and $s = n/r$. Let L/K be extension formed by adjoining a root of f to K. Then the unique descending chain is $L \supsetneq N \supsetneq K$ and the unique ascending chain is $K \subsetneq F \subsetneq L$ and they both coincide.

Proof. Let $G = \mathrm{Gal}(\tilde{L}/K)$ and $H = \mathrm{Gal}(\tilde{L}/L)$. By construction, $G = (\mathbb{Z}/r\mathbb{Z})^s \rtimes \mathbb{Z}/s\mathbb{Z}$ and $H = (\mathbb{Z}/r\mathbb{Z})^{s-1} \times \{0\} \times \{0\}$. Now G has the semidirect product group law given by

$$((a_1, \ldots, a_s), b) \cdot ((c_1, \ldots, c_s), d) = ((a_1, \ldots, a_s) + (b \cdot (c_1, \ldots, c_s)), b + d),$$

where $b \cdot (c_1, \ldots, c_s) = (c_{b+1}, \ldots, c_s, c_1, \ldots, c_b)$ for $b \neq 0$ & $0 \cdot (c_1, \ldots, c_s) = (c_1, \ldots, c_s)$.

Also $((a_1, \ldots, a_s), b)^{-1} = ((-a_{s-b+1}, \ldots, -a_s, -a_1, \ldots, -a_{s-b}), -b)$ for $b \neq 0$ & $((a_1, \ldots, a_s), 0)^{-1} = ((-a_1, \ldots, -a_s), 0)$. One can verify that

$$((a_1, \ldots, a_s), b) \cdot ((c_1, \ldots, c_{s-1}, 0), 0) \cdot ((a_1, \ldots, a_s), b)^{-1} = ((c_{b+1}, \ldots, c_{s-1}, 0, c_1, \ldots, c_b), 0).$$

Thus for $r < n$ (that is $s > 1$), one can compute and show that $N_G(H) = H^G = (\mathbb{Z}/r\mathbb{Z})^s \times \{0\}$. Hence by Prop. 8.2.2 (5), we are done.

□

Remark 8.3.3.1. *For $M/L/K$, the statements $r_K(M) \geq r_K(L)$ and $r_K(L) | r_K(M)$ (weak cluster magnification) are not true in general. Consider $L/N/K$ as in Thm. 8.3.3. Here, $r_K(L) \geq r_K(N) \iff r^2 \geq n$ and $r_K(N) | r_K(L) \iff n | r^2$. Thus in particular $n = 6, r = 2$ and $n = 6, r = 3$ give us counterexamples for the two statements.*

Theorem 8.3.4. *(Bhagwat, Jaiswal) (Thm 7.3.6 in [3])*

Let f over K be irreducible of deg n with Galois group $\mathfrak{S}_n$ with roots $\alpha_i \in \bar{K}$ for $1 \leq i \leq n$. For $1 \leq k \leq n-2$, let $L_k = K(\alpha_1, \ldots, \alpha_k)$.

- *Let N_k be the unique intermediate extension for L_k/K as in Thm. 8.1.1 (1). Then we have the following.*

  1. *$N_k = K(t_1, t_2, \ldots, t_k)$ where t_i are elementary symmetric sums of α_i for $1 \leq i \leq k$.*
  2. *Case (a): Characteristic of $K \neq 2$. For $k < n-1$, we have*

$$N_k = K(t_1) = K(\alpha_1 + \alpha_2 \cdots + \alpha_k).$$

Case (b) Characteristic of $K = 2$. For $k < n - 1$ but $k \neq n/2$, we have

$$N_k = K(t_1) = K(\alpha_1 + \alpha_2 \cdots + \alpha_k).$$

3. *for $k \neq 1, n/2$, the unique descending chain is $L_k \supsetneq N_k$. Also $r_K(L_1) = 1$.*
4. *for $k = n/2$ and for field K with characteristic $\neq 2$, the cluster size $r_K(N_k) = 2$. The unique intermediate field for N_k/K is $K(t_1(a - t_1))$ where $\alpha_1 + \alpha_2 + \cdots + \alpha_n = a$.*

- *The unique ascending chain is singleton K. And $t_K(L_k) = 1$.*

Proof.

- 1. Now, $\tilde{L_k} = L_{n-1} = L_n$. As noted in proof of Thm 4.4.2 in [13], the subgroup $H_k \subseteq \mathfrak{S}_n$ fixing L_k is isomorphic to $\mathfrak{S}_{n-k}$ as it consists of all permutations of the remaining $n - k$ roots. We have that $N_{\mathfrak{S}_n}(H_k) \cong \mathfrak{S}_{n-k} \times \mathfrak{S}_k$ where $\mathfrak{S}_k$ permutes the k roots $\alpha_1, \alpha_2, \ldots, \alpha_k$ and $\mathfrak{S}_{n-k}$ permutes the other $n - k$ roots as we have that $N_{\mathfrak{S}_n}(H_k)$ is a subgroup of $\mathfrak{S}_n$ which preserves the set of first k roots and hence also preserves the set of other $n - k$ roots. (Also follows from Lemma 3 in [13]). Now $N_k = \tilde{L_n}^{N_{\mathfrak{S}_n}(H_k)}$. Hence $\mathrm{Gal}(L_k/N_k) \cong \mathfrak{S}_k$ and $[L_k : N_k] = k!$ and $[N_k : K] = {}^nC_k$.

  Now $K(t_1, t_2, \ldots, t_k) \subseteq N_k$. Also L_k is splitting field of polynomial $x^k - t_1x^{k-1} + \cdots + (-1)^k t_k$ over $K(t_1, t_2, \ldots, t_k)$. Hence $[L_k : K(t_1, t_2, \ldots, t_k)] \leq k!$. Thus $K(t_1, t_2, \ldots, t_k) = N_k$.

  2. We give a proof for case (a) only. The proof in the other case follows similarly. Now for any $l < n - 1$, we have $\alpha_{i_{l+1}} \notin K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_l})$ and we also have $\alpha_{i_n} \in K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{n-1}})$ for distinct $i_m \leq n$. Since $t_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_k$. Hence t_1 has at most ${}^nC_k$ conjugates inside $\tilde{L_k}$ of the form $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_k}$ for distinct $i_m \leq n$.

  We claim that number of conjugates is exactly ${}^nC_k$ that is, if $\{i_1, i_2, \ldots, i_k\}$ and $\{j_1, j_2, \ldots, j_k\}$ are distinct sets of k numbers $\leq n$ then $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_k} \neq \alpha_{j_1} + \alpha_{j_2} + \cdots + \alpha_{j_k}$. Assume on the contrary $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_k} = \alpha_{j_1} + \alpha_{j_2} + \cdots + \alpha_{j_k}$.

  Case 1 : Let $k < n/2$. Hence number of distinct α_i in the equation is at most $n - 1$. After cancelling the common terms on both sides and then by taking all

α_i on one side except say α_{i_l}, we get α_{i_l} lies in field generated over K by other $\leq n-2$ many α_i. This gives a contradiction.

Case 2 : Let $k > n/2$. Now before cancelling we have $\leq n-k$ terms on RHS distinct than terms on LHS. Hence we have $\geq 2k-n$ common terms on both sides. Cancelling these common terms out leaves us with $\leq n-k$ terms on both sides. Since $k > n/2$, we have $n-k < n/2$. So we are back to Case 1.

Case 3 : Let n be even and $k = n/2$. We assume characteristic is not 2 in this case. If we can cancel out even one term from both sides then we are back to Case 1. So assume that $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_{n/2}} = \alpha_{j_1} + \alpha_{j_2} + \cdots + \alpha_{j_{n/2}}$ where all i_m, j_m are distinct. We know that $\alpha_1 + \alpha_2 + \cdots + \alpha_n = a \in K$. Hence $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_{n/2}} + \alpha_{j_1} + \alpha_{j_2} + \cdots + \alpha_{j_{n/2}} = a$. Thus $2(\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_{n/2}}) = a$. Since characteristic is not 2, we have $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_{n/2}} \in K$. Thus $\alpha_{i_{n/2}} \in K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{n/2-1}})$ which is a contradiction.

Hence $[K(t_1) : K] = {}^nC_k$. Now $K(t_1) \subset N_k$. Hence $K(t_1) = N_k$.

3. Case 1 : Let $k < n/2$. We claim that $r_K(N_k) = 1$. Suppose $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_k} \in K(t_1)$ for at least one $i_j \geq k+1$. By similar argument as in Case 1 of (2), we get a contradiction. Hence the unique descending chain is $L_k \supsetneq N_k$.

   Case 2 : Let $k > n/2$. Thus $n-k < n/2$. So $r_K(N_{n-k}) = 1$. Hence $N_{\mathfrak{S}_n}(\mathfrak{S}_k \times \mathfrak{S}_{n-k}) = \mathfrak{S}_k \times \mathfrak{S}_{n-k}$. By symmetry $N_{\mathfrak{S}_n}(\mathfrak{S}_{n-k} \times \mathfrak{S}_k) = \mathfrak{S}_{n-k} \times \mathfrak{S}_k$. Thus $r_K(N_k) = 1$.

4. Suppose $k = n/2$ and characteristic of $K \neq 2$. Clearly

$$(\alpha_{n/2+1} + \alpha_{n/2+2} + \cdots + \alpha_n) \in K(\alpha_1 + \alpha_2 + \cdots + \alpha_{n/2}).$$

   Suppose any other $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_k} \in K(t_1)$. Thus at least one i_l satisfies $1 \leq i_l \leq k$. Hence we get that at least one of the α_i lies in field generated over K by other $\leq n-2$ many α_j, which is a contradiction. Hence $r_K(N_k) = 2$. By Prop. 8.1.2, unique intermediate field for N_k/K as in Thm. 8.1.1 (1) will be $K((t_1 + a - t_1), t_1(a - t_1)) = K(t_1(a - t_1))$.

- Proof of last assertion: We have that the smallest normal subgroup of $\mathfrak{S}_n$ containing $\mathfrak{S}_{n-k}$ is $\mathfrak{S}_n$ itself. This is because $k \leq n-2$ that is $n-k \geq 2$. We know that for $n = 3$ and $n \geq 5$, the only proper non trivial normal subgroup of $\mathfrak{S}_n$ is $\mathfrak{A}_n$ and $\mathfrak{A}_n$ cannot contain $\mathfrak{S}_{n-k}$ for any $k \leq n-2$. We also know that for $n = 4$, the only proper non

trivial normal subgroups of $\mathfrak{S}_4$ are $\mathfrak{A}_4$ and V_4 (Klein four-subgroup) and $\mathfrak{A}_4$ and V_4 cannot contain $\mathfrak{S}_{4-k}$ for both $k = 1, 2$.

Hence by Thm. 8.2.1 (5), we are done.

□

Remark 8.3.4.1. *From the above theorem, in the case $k \neq 1, n/2$, the unique descending chain is $L_k \supsetneq N_k$. Hence L_k/K is obtained by nontrivial weak cluster magnification from N_k/K with magnification factor $[L_k : N_k]$. But L_k/K is not obtained by nontrivial strong cluster magnification from N_k/K, since the last assertion of above theorem implies that there doesn't exist a Galois F/K contained in L_k as in Def 5.2.0.1 with $[F : K] = [L_k : N_k]$.*

Remark 8.3.4.2. *In view of the examples discussed in Sec. 8.3, we can see that the converse of Thm. 7.2.10 is not true.*

1. *Let $M = \tilde{L}$ where L/K is not a Galois extension. Then M/L is Galois but $M \cap \tilde{L} \neq L$ and $[M : L] \neq r_K(M)/r_K(L)$.*
2. *Consider the case in Thm. 8.3.3. We have L/N is Galois and $L \cap \tilde{N} = N$ but $[L : N] \neq r_K(L)/r_K(N)$.*
3. *Consider the case in Thm. 8.3.4 for $n \geq 5$ and $k = 2$ and Characteristic of $K \neq 2$. Since $N_k = K(\alpha_1 + \alpha_2)$. Thus $\alpha_1 + \alpha_3, \alpha_2 + \alpha_3 \in \tilde{N_k}$. Hence $\alpha_1 - \alpha_2 \in \tilde{N_k}$ and thus $\alpha_1, \alpha_2 \in \tilde{N_k}$. That is $L_k \subset \tilde{N_k}$. So L_k/N_k is Galois and $[L_k : N_k] = r_K(L_k)/r_K(N_k)$ but $\tilde{N_k} \cap L_k \neq N_k$.*

On a similar note, the conclusion of Thm. 7.2.10 does not hold if we remove any one of the two conditions in its hypothesis.

1. *Let M/K be a nontrivial non Galois extension. Let $L = K$. Then $M \cap \tilde{L} = L$ but $[M : L] \neq r_K(M)/r_K(L)$ and M/L is not Galois.*
2. *Consider the case in Ex 5.4.2 for odd $n \geq 5$ and $k = (n+1)/2$ and $j = n - k$. Hence $j = (n-1)/2 = k - 1$. Thus $L_k = L_j(\alpha_k)$. One can verify that the minimal polynomial of α_k over L_j has degree $n - k + 1$ and has the roots $\alpha_k, \alpha_{k+1}, \ldots, \alpha_n$. Also $\alpha_i \notin L_k$ for $i > k$. Thus $[L_k : L_j] = r_K(L_k)/r_K(L_j)$ but $\tilde{L_j} \cap L_k \neq L_j$ and L_k/L_j is not Galois.*

Chapter 9

Base Change Theorems

In this chapter, we establish theorems about strong cluster magnification, weak cluster magnification, root capacity and unique chains under a particular type of base change. Then we prove results about strong cluster magnification and unique chains.

First we see a result about field extensions. The following lemma is a special case of Prop. 2.2.2 [4, Prop. 2.5].

Lemma 9.0.1. *Let E_1, E_2, E_3 be Galois over K contained in $\bar{K}$. Suppose each pairwise intersections of E_is is K, i.e.,*

$$E_1 \cap E_2 = E_2 \cap E_3 = E_3 \cap E_1 = K.$$

Then

$$E_1E_2 \cap E_3 = K \iff E_1E_3 \cap E_2E_3 = E_3.$$

Throughout this chapter, let L/K be a finite extension and let K'/K be a finite Galois extension such that $\tilde{L}$ and K' are linearly disjoint over K. We consider base change by such extensions K'.

9.1 A Base Change Theorem for Strong and Weak Cluster Magnification

Theorem 9.1.1. *(Bhagwat, Jaiswal) (Thm 8.1.1 in [3])*

Suppose M/K is obtained by nontrivial strong cluster magnification from an L/K with magnification factor d. Let $\tilde{M}$ and K' be also linearly disjoint over K. Then MK'/K' is obtained by nontrivial strong cluster magnification from LK'/K' with the same magnification factor d.

Furthermore, MK'/K is obtained by strong cluster magnification from M/K and LK'/K is obtained by strong cluster magnification from L/K and these are non trivial if $[K' : K] > 1$.

Proof. Proof of second assertion essentially follows from definition of cluster magnification. We prove the first assertion. Suppose M/K is obtained by strong cluster magnification from an L/K. We have L/K and F/K as in Def. 5.2.0.1. Let $M' := MK'$. Since $\tilde{M}$ and K' are linearly disjoint over K, we have $\tilde{M} \cap K' = K$. Since $\tilde{M} = \tilde{L}F$, we have $\tilde{L} \cap K' = K$, $L \cap K' = K$ and $F \cap K' = K$.

Now we check the three conditions of Def. 5.2.0.1 for M'/K'.

1. Let $L' := LK'$. Since K'/K Galois and $L \cap K' = K$, we have $[L' : K'] = [L : K] = n > 2$.

2. Let $F' := FK'$. Since, F/K is Galois, F'/K' is Galois. Also, $[F' : K'] = [F : K] = d > 1$. Let $\tilde{L'}$ be Galois closure of L' over K' in $\bar{K}$. Now, $N := \tilde{L}K'$ is Galois over K' and $L' \subset N$. Hence, $\tilde{L'} \subset N$. Since F is linearly disjoint with $\tilde{L}$ over K, we have $\tilde{L} \cap F = K$. Also $\tilde{L} \cap K' = K$ and $F \cap K' = K$. Since $\tilde{L}, F$ and K' are Galois over K. From Lem. 9.0.1 for $E_1 = \tilde{L}, E_2 = F, E_3 = K'$, we have $\tilde{L}F \cap K' = K \iff \tilde{L}K' \cap FK' = K'$. So we have $N \cap F' = K'$. Thus, $\tilde{L'} \cap F = K'$. Hence $\tilde{L'}$ and F' are linearly disjoint over K'.

3. $L'F' = (LK')(FK') = (LF)K' = MK' = M'$.

□

Remark 9.1.1.1. *The above theorem can be reformulated in this way: If M/K is obtained by strong cluster magnification from L/K through F/K and M'/K is obtained by strong cluster magnification from M/K through K'/K, then M'/K' is obtained by strong cluster magnification from LK'/K' through FK'/K'.*

We also have $\rho_K(M', L) = r_K(L)$. This is because $M' \cap \tilde{M} = M$ and $M \cap \tilde{L} = L$ which imply $M' \cap \tilde{L} = L$.

Lemma 9.1.2. *The extension M/K' is K'-isomorphic to $LK'/K' \iff M = L_1K'$ where L_1/K is K-isomorphic to L/K. Further in this case, the extension L_1 is unique and is given by $L_1 = M \cap \tilde{L}$.*

Proof. Suppose M/K' is isomorphic to LK'/K'. Let $\sigma : LK' \to M$ be the isomorphism such that $\sigma|_{K'} = id_{K'}$. Let $\sigma(L) = L_1$. Hence $M = L_1K$. Since $\sigma|_K = id_K$, it follows that L_1/K is isomorphic to L/K.

Conversely, suppose L_1/K is isomorphic to L/K. Let $\lambda : L \to L_1$ be the isomorphism such that $\lambda|_K = id_K$. Let $\tilde{\lambda} : LK' \to L_1K'$ be such that $\tilde{\lambda}(l) = \lambda(l)$ for all $l \in L$ and $\tilde{\lambda}(k') = k'$ for all $k' \in K'$. Let $\{l_i\}_{1 \leq i \leq [L:K]}$ be a K-basis for L. Hence any element of LK' is of the form $\sum_i l_i k'_i$ for $k'_i \in K'$.

Suppose $\sum_i l_i k'_i = 0$. Since $l_i \in L \subset \tilde{L}$ are linearly independent over K, and $\tilde{L}$ and K' are linearly disjoint over K; it follows by [15, Def. 20.1], we have that $\{l_i\}_{1 \leq i \leq [L:K]}$ are linearly independent over K'. Thus $k'_i = 0$ for all i. Now $\tilde{\lambda}(\sum_i l_i k'_i) = \sum_i \lambda(l_i)k'_i = 0$. Hence $\tilde{\lambda}$ is well defined field isomorphism with $\tilde{\lambda}|_{K'} = id_{K'}$.

As $L_1 \subset \tilde{L}$ and by Lemma 5.1.1, we have $\tilde{L} \cap L_1K' = L_1$. Thus the uniqueness of L_1 follows. □

Corollary 9.1.0.1. M/K is K-isomorphic to $LK'/K \iff M = L_1K'$ where L_1/K is K-isomorphic to L/K. (In this case such L_1 is unique).

(In particular, M/K is isomorphic to $LK'/K \iff M/K'$ is isomorphic to LK'/K'.)

Proof. Suppose M/K is isomorphic to LK'/K. Let $\sigma : LK' \to M$ be the isomorphism such that $\sigma|_K = id_K$. Since K'/K is Galois, it follows that $\sigma(K') = K'$. Let $\sigma(L) = L_1$. Hence $M = L_1K$ and L_1/K is isomorphic to L/K.

Conversely, suppose L_1/K is isomorphic to L/K. Hence by Lemma 9.1.2, L_1K'/K' is isomorphic to LK'/K'. Thus L_1K'/K is isomorphic to LK'/K. □

An alternate proof for Cluster Magnification theorem Thm. 5.1.2 [13, Thm. 1]:

Proof. By Lemma 5.1.1, since F/K is Galois, we have

$$\tilde{L} \cap F = K \iff \tilde{L} \cap LF = L \text{ and } L \cap F = K.$$

So $[LF : K] = [L : K][F : K] = nd$. Since F/K is Galois, we have by Corollary 9.1.0.1,

M is isomorphic to LF over $K \iff M = L'F$ where L' is isomorphic to L over K.

Since such L' is unique. Hence by Lemma 4.4.1, $s_K(LF) = s_K(L)$. Hence by Thm. 4.1.1 (2), we have

$$[LF : K]/r_K(LF) = [L : K]/r_K(L).$$

Thus we get $r_K(LF) = r_K(L)[F : K] = rd$. □

Corollary 9.1.0.2. The extension $\tilde{L}K'$ is the Galois closure of LK'/K'.

Proof. By Lemma 9.1.2, the fields isomorphic to LK'/K' are L_iK'/K' where L_i/K are distinct fields isomorphic to L/K. From remark 4.4.1.1, $\tilde{L} = L_1L_2 \dots L_{s_K(L)}$. Hence the Galois Closure of LK'/K' is $L_1K'L_2K' \dots L_{s_K(L)}K' = \tilde{L}K'$.

□

Lemma 9.1.3. *The degrees and Galois groups are preserved under base change. Hence the cluster sizes satisfy*

$$r_K(L) = r_{K'}(LK').$$

Proof. By Lemma 5.1.1, since K'/K is Galois, we have

$$\tilde{L} \cap K' = K \iff \tilde{L} \cap LK' = L \text{ and } L \cap K' = K.$$

Since, $L \cap K' = K$, we have $[L : K] = [LK' : K']$. Also $[\tilde{L} : K] = [\tilde{L}K' : K']$. Hence also $[\tilde{L} : L] = [\tilde{L}K' : LK']$.

Let $G_1 = \mathrm{Gal}(\tilde{L}K'/K')$. Let $H_1 \subset G_1$ be subgroup with LK' as the fixed field that is $H_1 = \mathrm{Gal}(\tilde{L}K'/LK')$. By [5, Thm. 2.6], since $\tilde{L} \cap K' = K$, we have G_1 is isomorphic to G by restriction. And since $\tilde{L} \cap LK' = L$, we have H_1 is isomorphic to H under same isomorphism.

Now the last assertion follows from Thm. 4.1.1 (3). □

Remark 9.1.3.1. *Lem. 9.1.3 gives an alternate proof for Thm. 9.1.1 by using the criterion in Thm. 5.2.3.*

We conclude the following result for the strong cluster magnification of polynomials from Thm. 9.1.1.

Theorem 9.1.4. *(Bhagwat, Jaiswal) Suppose g over K is obtained by nontrivial strong cluster magnification from an f over K with magnification factor d. Let K'/K, contained in $\bar{K}$, be Galois and linearly disjoint with K_g over K. Then g over K' is obtained by nontrivial strong cluster magnification from f over K' with same magnification factor d.*

Now we state a base change theorem for weak cluster magnification.

Theorem 9.1.5. *(Bhagwat, Jaiswal) (Thm 8.1.9 in [3])*

Suppose M/K is obtained by weak cluster magnification from an L/K with magnification factor d. Let K'/K, contained in $\bar{K}$, be Galois and let $\tilde{M}$ and K' be linearly disjoint over K. Then MK'/K' is obtained by weak cluster magnification from LK'/K' with the same magnification factor d.

Proof. Follows from last assertion in Lemma 9.1.3.

□

9.2 Base Change and Root Capacity

Lemma 9.2.1. *$K' \subset M \subset LK' \iff M = NK'$ for a field $K \subset N \subset L$. This N is unique and given by $N = \tilde{L} \cap M$.*

Proof. From Lemma 9.1.3, number of subgroups of $\mathrm{Gal}(\tilde{L}/K)$ containing $\mathrm{Gal}(\tilde{L}/L) =$ number of intermediate extensions for $L/K =$ number of intermediate extensions for LK'/K'. The uniqueness follows from Lemma 5.1.1. □

Theorem 9.2.2. *(Bhagwat, Jaiswal) (Thm 8.2.2 in [3])*

Let M/K be extension of L/K such that $\tilde{M}$ and K' are also linearly disjoint over K. Then $\rho_K(M, L) = \rho_{K'}(MK', LK')$.

Proof. Let $\rho_K(M, L) = a_K \cdot r_K(L)$ and $\rho_{K'}(MK', LK') = a_{K'} \cdot r_{K'}(LK')$ where $a_K, a_{K'}$ are as in Lem. 7.2.3. From Lem. 9.1.3, we have $r_K(L) = r_{K'}(LK')$.

By Prop. 7.2.4 (1), a_K is number of distinct fields inside $M \cap \tilde{L}$ isomorphic to L over K and $a_{K'}$ is number of distinct fields inside $MK' \cap \tilde{L}K'$ isomorphic to LK' over K'. By Lem. 9.2.1, $K' \subset P \subset \tilde{L}K' \iff P = L_1K'$ for a unique field $K \subset L_1 \subset \tilde{L}$.

Now for $L_1 \subset \tilde{L}$, we claim $L_1 \subset M \cap \tilde{L} \iff L_1K' \subset MK' \cap \tilde{L}K'$. Suppose $L_1K' \subset MK' \cap \tilde{L}K'$. Thus $L_1K' \cap \tilde{M} \subset (MK' \cap \tilde{M}) \cap (\tilde{L}K' \cap \tilde{M})$. By Lemma 5.1.1, we have $L_1 \subset M \cap \tilde{L}$. The other implication is clear. Hence by Lem. 9.1.2, we are done.

□

9.3 Base Change and Unique Chains

We study how the unique chains are related to the base change to K'.

Theorem 9.3.1. *(Bhagwat, Jaiswal) (Thm 8.3.1 in [3])*

1. *$L \supsetneq N_1 \supsetneq \cdots \supsetneq N_k$ is unique descending chain for $L/K \iff$ $LK' \supsetneq N_1K' \supsetneq \cdots \supsetneq N_kK'$ is unique descending chain for LK'/K' for $N_i \subset L$ for all i.*

2. *$K \subsetneq F_1 \subsetneq \cdots \subsetneq F_l$ is unique ascending chain for $L/K \iff K' \subsetneq F_1K' \subsetneq \cdots \subsetneq F_lK'$ is unique ascending chain for LK'/K' for $F_i \subset L$ for all i.*

Proof. We use Lemma 9.1.3 here.

Proof of (1): Since $\tilde{L}$ and K' are linearly disjoint over K and $N_i \subset L$ for all i, we have that $\tilde{N}_i$ and K' are linearly disjoint over K for all i. It is enough to show that the unique N for LK'/K' is N_1K'.

Since $\mathrm{Gal}(\tilde{L}K'/K') \cong \mathrm{Gal}(\tilde{L}/K) = G$ through restriction and $\mathrm{Gal}(\tilde{L}K'/LK') \cong \mathrm{Gal}(\tilde{L}/L) = H$ under same map. Hence by identifying the groups, we have

$$\tilde{L}^{N_G(H)} = N_1 \iff (\tilde{L}K')^{N_G(H)} = N_1K'.$$

Proof of (2): Let L_i/F_i be the Galois closure of L/F_i for all $i \geq 1$. Since $\tilde{L}$ and K' are linearly disjoint over K, we have that L_i and K' are linearly disjoint over K. Hence by Lemma 5.1.1, L_i and F_iK' are linearly disjoint over F_i for all i.

It is enough to show that the unique F for LK'/K' is F_1K'. Similar to proof of part (1), we have
$\tilde{L}^{H^G} = F_1 \iff (\tilde{L}K')^{H^G} = F_1K'$.

□

9.4 Strong Cluster Magnification and Unique Chains

Theorem 9.4.1. *(Bhagwat, Jaiswal) (Thm 8.4.1 in [3])*

Let M/K be obtained by strong cluster magnification from L/K with $r_K(L) \neq 1$. Then we have that $M \supsetneq N_1 \supsetneq \cdots \supsetneq N_k$ is the unique descending chain for $M/K \iff$ $L \supsetneq N_1 \supsetneq \cdots \supsetneq N_k$ is the unique descending chain for L/K.

Proof. It is enough to show that $\tilde{M}^{N_{G'}(H')} = \tilde{L}^{N_G(H)}$ where $G' = \mathrm{Gal}(\tilde{M}/K)$ and

$H' = \mathrm{Gal}(\tilde{M}/M)$. After identifying the groups in Prop. 5.2.2, we have $G' = G \times R$ and $H' = H \times 1$. Hence $N_{G'}(H') = N_G(H) \times R$. Now $\tilde{L} = \tilde{M}^{1\times R}$. Hence $\tilde{M}^{N_G(H)\times R} \subseteq \tilde{L}$ and $\mathrm{Gal}(\tilde{L}/\tilde{M}^{N_{G'}(H')}) = N_G(H)$. Thus we are done.

We could also see the last fact in the following way. By Lemma 5.1.1, $\tilde{L} \cap F = K \iff N \cap F = K$ and $\tilde{L} \cap NF = N$. We also have $(\tilde{L})(NF) = \tilde{L}F = \tilde{M}$. Hence $Gal(NF/N) \cong Gal(F/K)$ and $Gal(\tilde{M}/N) = Gal(\tilde{L}/N) \times Gal(NF/N) = N_G(H) \times R$. □

Remark 9.4.1.1. *If $r_K(L) = 1$ in above theorem. Then the unique descending chain for M/K is $M \supsetneq L$.*

Theorem 9.4.2. *(Bhagwat, Jaiswal) (Thm 8.4.3 in [3])*

Let M/K be obtained by strong cluster magnification from L/K through F/K as in Def 5.2.0.1 with $t_K(L) \neq 1$. Then we have

1. *F' is unique intermediate field for M/K as in Thm. 8.2.1 $\iff$ $F' = F_1F$ where F_1 is unique intermediate field for L/K.*
2. *$K \subsetneq F_1 \subsetneq \cdots \subsetneq F_k$ is the unique ascending chain for $L/K \iff K \subsetneq F_1F \subsetneq \cdots \subsetneq F_kF$ is the unique ascending chain for M/K for $F_i \subset L$ for all i.*

Proof. (1) Let $G' = \mathrm{Gal}(\tilde{M}/K)$ and $H' = \mathrm{Gal}(\tilde{M}/M)$. After identifying the groups in Prop. 5.2.2, we have $G' = G \times R$ and $H' = H \times 1$. Hence $H'^{G'} = H^G \times 1$. Now $F = \tilde{M}^{G\times 1}$. Let $F_1 = \tilde{L}^{H^G}$. Hence $F_1 = \tilde{M}^{H^G\times R}$. Since $(G\times 1)\cap(H^G\times R) = (H^G\times 1)$, we get $\tilde{M}^{H^G\times 1} = F_1F$.

(2) Since $\tilde{L} = \tilde{M}^{1\times R}$. Thus $\tilde{L} \cap F_1F = F_1$. Since $M = LF$, by Thm. 9.3.1 (2), we have $F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_k$ is unique ascending chain for $L/F_1 \iff F_1F \subsetneq F_2F \subsetneq \cdots \subsetneq F_kF$ is unique ascending chain for M/F_1F for $F_i \subset L$ for all $i \geq 2$. □

Remark 9.4.2.1. *If $t_K(L) = 1$ in the above theorem. Then the unique ascending chain for M/K is $K \subsetneq F$.*

Chapter 10

Ascending Index and Future Directions

The thesis concludes with this chapter with some properties of the ascending index. The ascending index has many properties similar to the cluster size. In the last section we talk about future directions.

10.1 Properties of Ascending Index

Recall that the ascending index $t_K(L)$ of L/K was defined to be the degree $[F : K]$ in Thm. 8.2.1.

Proposition 10.1.1. *(Bhagwat, Jaiswal) (Prop 9.0.1 in [3])*

If $M/L/K$ are extensions, then $t_K(L)|t_K(M)$.

Proof. Let F/K and F'/K be the unique intermediate extensions as in Thm. 8.2.1 for L/K and M/K respectively. Since F'/K is Galois with maximum possible degree contained in M, we conclude that $F \subset F'$. Thus $[F : K] \mid [F' : K]$. □

Remark 10.1.1.1. *The above proposition tells that the analogue of the notion of weak magnification always holds for ascending index.*

From Lemma 9.1.3, we have the following base change result for ascending index.

Proposition 10.1.2. *(Bhagwat, Jaiswal) (Prop 9.0.3 in [3])*

Let L/K be a finite extension and let K'/K be a finite Galois extension such that $\tilde{L}$ and K' are linearly disjoint over K. Then

$$t_K(L) = t_{K'}(LK').$$

By proof of Thm. 9.4.2 (1) and Thm. 8.2.1 (2), we have the following analogue of the Cluster Magnification Theorem Thm. 5.1.2.

Ascending Index Magnification Theorem

Theorem 10.1.3. *(Bhagwat, Jaiswal) (Thm 9.0.4 in [3])*

Let M/K be obtained by strong cluster magnification with magnification factor d. Then

$$t_K(M) = d\, t_K(L) \text{ and } u_K(M) = u_K(L).$$

The following theorem is an analogue of Thm. 4.3.1.

Inverse Ascending Index Problem for Number Fields

Theorem 10.1.4. *(Bhagwat, Jaiswal) (Thm 9.0.5 in [3])*

Let K be a number field. Let $n > 2$ and $t|n$. Then there exists an extension L/K of degree n with ascending index $t_K(L) = t$.

Proof. Suppose $t = 1$. By Lemmas 4.3.2 and 4.3.3 and Thm. 4.4.2 and Thm. 8.3.4 we have $L = L_1$ which satisfies $t_K(L) = 1$.

Now suppose $t = n$. By Thm. 4.3.1 for $r = n$, there exists an L/K of degree n with $r_K(L) = n$. For that L/K we have $t_K(L) = n$.

Now suppose $1 < t < n$. Hence $1 < n/t < n$. By Thm. 4.3.1 for $r = n/t$ and Thm. 8.3.3, there exists an L/K of degree n with $r_K(L) = n/t$ and $t_K(L) = t$.

□

Remark 10.1.4.1. *Since we have Thm. 10.1.3, we could have approached Thm. 10.1.4 in a similar way as Thm. 4.3.1 was approached in [13] using Thm. 5.1.2. This approach would have left us with some cases not covered as in Thm. 2 in [13].*

The following result is Lemma 2 in [13].

Lemma 10.1.5. *Given a finite extension of algebraic number field L/K and a positive integer $d \geq 2$, there exist infintely many Galois extensions of F/K of degree d such that L and F are linearly disjoint over K.*

Proof. Case 1 : $K = \mathbb{Q}$: Let $\Delta_L \in \mathbb{Z}$ be the discriminant of the number field L. For a prime p not dividing Δ_L, consider the cyclotomic extension $M = \mathbb{Q}(\xi_p)$ where ξ_p is primitive p-th root of unity. Now p is the only prime ramified in M but it remains unramified in L. Hence discriminant of $L \cap M$ has absolute value 1. So $L \cap M = \mathbb{Q}$. As M is Galois over $\mathbb{Q}$, L and M are linearly disjoint over $\mathbb{Q}$.

Now for a given $d \geq 2$ we can find infinitely many primes p such that $p > \Delta_L$ and $p \equiv 1 \pmod{d}$ by Dirichlet's theorem on arithmetic progressions. For such p the cyclotomic fields M will have a cyclic Galois extension of degree d as a subfield F such that L and F are linearly disjoint over $\mathbb{Q}$.

Case 2 : For any number field K : For given extension L/K, we get extensions $F_1/\mathbb{Q}$ by Case 1 such that L and F_1 are linearly disjoint over $\mathbb{Q}$. Now by the Lemma 5.1.1, the extensions L and $F = KF_1$ will be linearly disjoint over K. Also F/K is Galois and has the same degree as $F_1/\mathbb{Q}$.

□

The following theorem is an analogue of Thm. 2 in [13].

Theorem 10.1.6. *(Bhagwat, Jaiswal) (Thm 9.0.7 in [3])*

1. *Let K be a number field. For any integers $u \geq 3, t \geq 1$ there exists L/K of degree ut and $t_K(L) = t$.*
2. *Let $K = \mathbb{Q}$. For t an even number, there exists L/K of degree $2t$ and $t_K(L) = t$.*

Proof. (1) For $n = u$, we have L_1/K with degree u and satisfying $t_K(L_1) = 1$ as in first case of Thm. 10.1.4. By Lemma 10.1.5, there exists F/K Galois of degree t such that $\tilde{L_1}$ and F are linearly disjoint over K. Hence by Thm. 10.1.3, $L = L_1F$ has degree ut over K and $t_K(L) = t$.

(2) Consider $P = \mathbb{Q}(\sqrt[4]{2})$ which has degree 4 over $K = \mathbb{Q}$ and $t_K(P) = 2$. For t an even number, by Lemma 10.1.5, there exists F/K Galois of degree $t/2$ such that $\tilde{P}$ and F are linearly disjoint over K. Hence by Thm. 10.1.3, $L = PF$ has degree $2t$ over K and $t_K(L) = t$.

□

10.2 Future Directions

The following are certain problems which are some of the future directions that we plan to explore.

10.2.1 Problems based on Chapters 2 and 3.

Problem 10.2.1. *Can we apply Theorems 2.2.1, 2.4.1, 3.1.7, 3.1.8 and 3.2.7 to more special cases to get new cases of IGP?*

Problem 10.2.2. *Can we realize the group $\mathrm{SL}_2(\mathbb{F}_p)$ as a Galois group over $\mathbb{Q}$ for all primes $p \geq 5$ through the methods discussed in Chapters 2 and 3?*

Problem 10.2.3. *Can we find special cases satisfying hypothesis of Prop 3.2.3 and thus realize over $\mathbb{Q}$, some direct products of groups which are realizable as a Galois group over $\mathbb{Q}$ through Galois representation?*

Can we have some general approach to realize over $\mathbb{Q}$, direct products of groups which are realizable as a Galois group over $\mathbb{Q}$?

10.2.2 Problems based on Chapters 4 to 10.

Problem 10.2.4. *Can we generalise the Inverse cluster size problem for number fields (Thm 4.3.1) and the Inverse ascending index problem for number fields (Thm 10.1.4) from number fields to a bigger class of fields?*

Problem 10.2.5. *Given K, can we classify all L/K with cluster size $r_K(L) = 1$ & $r_K(L) = 2$?*

Problem 10.2.6. *Let M/K be obtained by nontrivial strong cluster magnification from some L/K (see Def 5.2.0.1).*

1. *Let $K \subset K' \subset M$. Is M/K' obtained by nontrivial strong cluster magnification from some subextension over K'?*
2. *Let $K \subset M' \subset M$. Is M'/K obtained by nontrivial strong cluster magnification from some subextension over K?*

Similar questions can be asked for M/K obtained by nontrivial weak cluster magnification from some L/K (see Def 5.4.0.1).

Problem 10.2.7. *Is the hereditary property, which is true for strong cluster magnification (Prop 5.2.1), also true for weak cluster magnification? Let M/K be obtained by weak cluster magnification from L/K. Let $K \subset K' \subset L$. Is the extension M/K' obtained by weak cluster magnification from L/K'?*

Problem 10.2.8. *What are the minimal additional conditions that we require so that M/K which is obtained by nontrivial weak cluster magnification from some L/K is also obtained by nontrivial strong cluster magnification from L/K?*

Problem 10.2.9. *(Refer to Sections 6.1 and 6.2). What are the necessary and sufficient conditions on an irreducible polynomial over K, for degree sequence of cluster tower of the polynomial to be independent of the ordering of the representatives of the clusters of roots? Can we get the conditions in terms of Galois group of splitting field of the polynomial?*

Under the above conditions, can we find general formula for the length of cluster tower in terms of other invariants of the irreducible polynomial?

Problem 10.2.10. *Is the Inverse degree sequence problem true for number fields? Suppose we have a number field and positive integers $a_0, a_1, a_2, \ldots, a_l$. What are the necessary and sufficient conditions (if they exist) on these a_i's so that there exists an irreducible polynomial over the given number field such that, for an ordering of the representatives of clusters of its roots, we have the cluster tower having degree sequence $a_0, a_1, a_2, \ldots, a_l$?*

Problem 10.2.11. *Given L/K, we define the descending dimension of L/K as the length of the unique descending chain in Thm 8.1.1 (similarly ascending dimension of L/K as the length of the unique ascending chain in Thm 8.2.1) which is the number of distinct fields in the chain except the first field.*

Can we find general formula for the descending and ascending dimensions in terms of other invariants of the extension L/K?

Problem 10.2.12. *(Refer to Thm 8.2.1 (2)). Given L/K, can the ascending index $t_K(L)$ have a description in terms of roots of the minimal polynomial of α over K where α is a primitive element for L/K?*

Can we have an analogous result to Prop 8.1.2 for the unique intermediate extension F/K for L/K as in Thm. 8.2.1 (1)? That is, can we describe F in terms of the roots of the minimal polynomial of α?

Problem 10.2.13. *Consider L/K.*

1. *We define the cluster size sequence of L/K as*

$$r_K(N_0), r_K(N_1), \ldots, r_K(N_{k-1})$$

where N_i's are the fields in the unique descending chain as in Thm 8.1.1.

Is the Inverse cluster size sequence problem true for number fields? Suppose we have a number field K and positive integers $n, r_1, r_2, \ldots, r_k$. What are the necessary and sufficient conditions (if they exist) on these positive integers so that there exists an extension L/K such that $[L : K] = n$ and the cluster size sequence of L/K is $r_1, r_2, \ldots, r_k$?

2. *We define the ascending index sequence of L/K as*

$$t_{F_0}(L), t_{F_1}(L), \ldots, t_{F_{k-1}}(L)$$

where F_i's are the fields in the unique ascending chain as in Thm 8.2.1.

Is the Inverse ascending index sequence problem true for number fields? Suppose we have a number field K and positive integers $n, t_1, t_2, \ldots, t_k$. What are the necessary and sufficient conditions (if they exist) on these positive integers so that there exists an extension L/K such that $[L : K] = n$ and the ascending index sequence of L/K is $t_1, t_2, \ldots, t_k$?

Problem 10.2.14. *Can we find the unique descending chains in the remaining cases of Thm 8.3.4?*

Bibliography

[1] Sara Arias-de Reyna and Joachim König. Locally cyclic extensions with Galois group $\mathrm{GL}_2(p)$. *International Journal of Number Theory, 20(03):781–796*, 2024.

[2] Michael Artin. *Algebra*. Pearson, Noida, 2nd ed. edition, c2015.

[3] Chandrasheel Bhagwat and Shubham Jaiswal. Cluster Magnification, Root Capacity, Unique Chains, Base Change and Ascending Index. Accepted for publication in Proceedings Mathematical Sciences (2025). *https://arxiv.org/abs/2405.06825*, 2024.

[4] Chandrasheel Bhagwat and Shubham Jaiswal. Right Splitting, Galois Correspondence, Galois Representations and Inverse Galois Problem. Accepted for publication in Journal of the Ramanujan Mathematical Society (2025). *https://arxiv.org/abs/2403.14316*, 2024.

[5] Keith Conrad. The Galois correspondence at work. *https://kconrad.math.uconn.edu/blurbs/galoistheory/galoiscorrthms.pdf*, 2023.

[6] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[7] Luis Dieulefait. *Galois realizations of families of Projective Linear Groups via cusp forms*, page 85–92. Cambridge University Press, 2008.

[8] Luis Dieulefait, Enric Florit, and Núria Vila. Seven small simple groups not previously known to be Galois over $\mathbb{Q}$. *Mathematics*, 10(12):2048, 2022.

[9] Luis Dieulefait and Núria Vila. Projective Linear Groups as Galois Groups over $\mathbb{Q}$ via Modular Representations. *Journal of Symbolic Computation*, 30(6):799–810, 2000.

[10] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.

[11] Eliot T Jacobson and William Y Vélez. The Galois group of a radical extension of the rationals. *Manuscripta Mathematica*, 67:271–284, 1990.

[12] Nathan Jacobson. *Basic Algebra II*. Dover publications, Inc., 2nd edition, 1989.

[13] M Krithika and P Vanchinathan. An elementary problem in Galois theory about the roots of irreducible polynomials. *Proc. Indian Acad. Sci. (Math. Sci.) (2024) 134:28*, 2024.

[14] François Legrand and Elad Paran. Automorphism groups over hilbertian fields. *Journal of Algebra*, 503:1–7, 2018.

[15] Patrick Morandi. *Field and Galois theory*, volume 167. Springer Science & Business Media, 2012.

[16] Joris Nieuwveld. Explicit constructions for semidirect products in Inverse Galois Theory. *Thesis BSc Mathematics, Radboud University Nijmegen*, 2019.

[17] Alexander R Perlis. Roots appear in quanta: exercise solutions. *https://www.math.lsu.edu/ aperlis/publications/rootsinquanta/*, 2003.

[18] Alexander R Perlis. Roots appear in quanta. *The American Mathematical Monthly*, 111(1):61–63, 2004.

[19] Kenneth A Ribet. On l-adic representations attached to modular forms ii. *Glasgow Mathematical Journal*, 27:185–194, 1985.

[20] Igor Shafarevich. Factors of decreasing central series. *Mat. Zametki*, 45, no.3, 128, 1989.

[21] Goro Shimura. *Modular forms: basics and beyond*. Springer Science & Business Media, 2011.

[22] Helmut Völklein. *Groups as Galois groups: an introduction*. Number 53. Cambridge University Press, 1996.

[23] David Zywina. Modular forms and some cases of the Inverse Galois Problem. *Canadian Mathematical Bulletin*, 66(2):568–586, 2023.