Realization of Finite Groups as Galois Groups over $\mathbb{Q}$ in $\mathbb{Q}_{tot,p}$

Nantsoina Cynthia Ramiharimanana

Thesis presented for the degree of Master of Science at Stellenbosch University

Supervisors:
Prof. Moshe Jarden
(Tel Aviv University)
Prof. Barry Green
(Stellenbosch University)

December 2013

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the owner of the copyright thereof (unless to the extent explicitly otherwise stated) and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: November 25, 2013

Abstract

For a prime number p, the Henselization $(\mathbb{Q}_p, v_{p,h})$ of the valued field $(\mathbb{Q}, v_p)$ is unique up to isomorphism. The field $\mathbb{Q}_{\mathrm{tot},p} = \bigcap_{\sigma \in \mathrm{Gal}(\mathbb{Q})} \sigma\mathbb{Q}_p$ is the maximal Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_p$ in which p totally splits. The absolute Galois group of $\mathbb{Q}_{\mathrm{tot},p}$ is known, but in contrast, very little is known about the relative group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tot},p}/\mathbb{Q})$. In this work we take first steps toward understanding the latter group. We realize each member of four basic families of finite groups as Galois groups over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$.

Opsomming

Vir enige priemgetal p is die Henselisering $(\mathbb{Q}_p, v_{p,h})$ van die waarderingsliggaam $(\mathbb{Q}, v_p)$ eenduidig bepaal tot en met isomorfisme. Die liggaam $\mathbb{Q}_{\text{tot},p} = \bigcap_{\sigma \in \text{Gal}(\mathbb{Q})} \sigma\mathbb{Q}_p$ is die maksimale Galois uitbreiding van $\mathbb{Q}$ in $\mathbb{Q}_p$ waarin p volledig ontbind. Die absolute Galois groep van $\mathbb{Q}_{\text{tot},p}$ is bekend, maar in teendeel is min bekend oor die relatiewe groep $\text{Gal}(\mathbb{Q}_{\text{tot},p}/\mathbb{Q})$. In hierdie proefskrif word die eerste stappe geneem om die groep beter te verstaan. Die realiserings van elke lid van vier bekende groep-families as Galois groepe oor $\mathbb{Q}$ in $\mathbb{Q}_{\text{tot},p}$ word gegee.

Acknowledgements

I would like to express my deep gratitude to my supervisors Professor Moshe Jarden and Professor Barry Green. They abundantly offered me invaluable assistance, support and guidance throughout this work. Professor Jarden's constructive comments have greatly improved this work. This project would not have been possible without their significant help.
I am also grateful to Professor Peter Roquette, Professor Wulf-Dieter Geyer, and Professor Peter Mueller for important contributions to the work.
Part of this work was done while I was visiting the School of Mathematics at Tel Aviv University. Special thanks go to Dr. Lior Bary-Soroker and Mrs Meira Hillel for their assistance throughout my visit.
My thanks go also to the Faculty of Sciences of Stellenbosch University, the African Institute of Mathematical Sciences (AIMS) in South Africa, and the University of Tel Aviv for their financial and material support.
Finally, I would like to thank my family members, including Yann, for their continuous love, support and encouragement throughout my studies.

This thesis is dedicated to Brilland Ranorovelonalohotsy.

Contents

Notation

$\mathbb{Z} =$ the ring of rational integers.

$\mathbb{Q} =$ the field of rational numbers.

$\mathbb{R} =$ the field of real numbers.

$\zeta_n =$ a primitive n-th root of unity.

$\mathbb{F}_q =$ the field with q elements.

$K^\times =$ the multiplicative group of all nonzero elements of a field K.

$K_s =$ the separable closure of a field K.

$\tilde{K} =$ the algebraic closure of a field K.

$\mathrm{Gal}(L/K) =$ the Galois group of a Galois extension L/K.

$\mathrm{Gal}(f(x), K) =$ the Galois group of the polynomial $f(X)$ over K (By definition it is the Galois group of the splitting field of f over K).

$\mathrm{Gal}(K) =$ $\mathrm{Gal}(K_s/K) =$ the absolute Galois group of a field K.

Introduction

The inverse problem of Galois theory asks if every finite group occurs as a Galois group over $\mathbb{Q}$. This problem has been partially solved, many finite groups and families of finite groups have been realized over $\mathbb{Q}$, but not all of them.

One of the methods for realizing finite groups over $\mathbb{Q}$ is the use of arithmetic tools, like algebraic number theory, Dirichlet's Theorem on arithmetic progressions, reduction of polynomials modulo p, and combinatorics. All finite abelian groups and all symmetric groups are among the groups which have been realized by these tools. Another method of realization applies Hilbert's Irreducibility Theorem. The latter says that if $f \in \mathbb{Q}[t, X]$ is a separable polynomial in X over $\mathbb{Q}(t)$, then there are infinitely many $a \in \mathbb{Q}$ such that $\mathrm{Gal}(f(a, X), \mathbb{Q}) \cong \mathrm{Gal}(f(t, X), \mathbb{Q}(t))$. It follows that all groups that have been realized over $\mathbb{Q}(t)$ also occur as Galois groups over $\mathbb{Q}$. The alternating groups are among those that have been realized over $\mathbb{Q}$ by this method.

One of the central objects in algebraic number theory is the field $\hat{\mathbb{Q}}_p$ of p-adic numbers. We denote the algebraic part of $\hat{\mathbb{Q}}_p$ by $\mathbb{Q}_p$ (Notice the deviation from the classical notation.) The latter is unique up to conjugation over $\mathbb{Q}$. We therefore consider the field

$$\mathbb{Q}_{\mathrm{tot},p} = \bigcap_{\tau \in \mathrm{Gal}(\mathbb{Q})} \tau \mathbb{Q}_p$$

of totally p-adic numbers. It is the maximal Galois extension of $\mathbb{Q}$ in which p totally splits. By Moret-Bailly [Mo-Bal], this field is pseudo p-adically closed. This means that every absolutely irreducible variety V which is definable over $\mathbb{Q}_{\mathrm{tot},p}$ and has a simple $\tau\mathbb{Q}_p$-rational point for every $\tau \in \mathrm{Gal}(\mathbb{Q})$ has a $\mathbb{Q}_{\mathrm{tot},p}$-rational point. The absolute Galois group of $\mathbb{Q}_{\mathrm{tot},p}$ is also known. It is the free product in the sense of Melnikov of groups $\mathrm{Gal}(\tau\mathbb{Q}_p)$ [Po]. This implies in particular that every finite group occurs as a Galois group over $\mathbb{Q}_{\mathrm{tot},p}$.

In contrast, the ralative Galois group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tot},p}/\mathbb{Q})$ has been only scarcely explored. Of course, in the light of the inverse problem of Galois theory, we even do not know the finite quotients of that group. Therefore we make the followig hypotheses:

HYPOTHESIS 1: Every finite group which is realizable over $\mathbb{Q}$ is also realizable over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$.

If L is a Galois extension of $\mathbb{Q}$ which is contained in $\mathbb{Q}_p$, then L is also contained in $\mathbb{Q}_{\mathrm{tot},p}$. Hence, Hypothesis 1 is equivalent to the following one:

HYPOTHESIS 2: Every finite group which is realizable over $\mathbb{Q}$ is realizable over $\mathbb{Q}$ in $\mathbb{Q}_p$.

In this work we verify Hypothesis 2 in four cases: finite abelian groups, certain semi-direct products of groups, symmetric groups, and the alternating groups. The realization ot the first three families uses arithmetical methods, while the construction of the alternating groups over $\mathbb{Q}$ in $\mathbb{Q}_p$ applies Hilbert's irreducibility theorem.

The realization of finite abelian groups in Chapter 2 starts with the special case $\mathbb{Z}/q^k\mathbb{Z}$ for some prime number q and a positive integer k. Then, we

use the fundamental theorem of finite abelian groups for the realization of arbitrary finite abelian groups. We present two methods to realize $\mathbb{Z}/q^k\mathbb{Z}$. The first one applies a result from group theory (Lemma 2.2.6) and Dirichlet's theorem (Lemma 2.1.5). For that, the unramification of p in some linearly disjoint cyclotomic fields $\mathbb{Q}(\zeta_l)$ and $\mathbb{Q}(\zeta_{l'})$, for distinct prime numbers $l, l' \neq p$, implies that the fixed field of the Frobenius at p in a Galois extension N of $\mathbb{Q}$ in $\mathbb{Q}(\zeta_l, \zeta_{l'})$ has a Galois subextension $L \subseteq \mathbb{Q}_{\mathrm{tot},p}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/q^k\mathbb{Z}$. The second method uses an equivalence of the total splitting of a prime number l in $\mathbb{Q}(\zeta_n, \sqrt[n]{p})$ (Lemma 2.2.8) and a special case of the Chebotarev density theorem (Lemma 2.1.6).

In Chapter 3, we deal with the realization of the semi-direct product of a group G which is realisable over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$, and an $\mathbb{F}_2$-vector space of dimension r on which G is acting from the left. The realization is based on Abelian Kummer theory (Section 3.2) and on the Chinese Remainder Theorem for Dedekind domains (Proposition 3.3.2). If K is a Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$, then the Chinese Remainder Theorem for $\mathcal{O}_K$ implies the existence of $x_1, \ldots, x_r \in \mathcal{O}_K$ such that the field $N = K(\sqrt{\sigma x_i} \mid \sigma \in G, 1 \leq i \leq r)$ is a Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$ with Galois group $B \rtimes G$, where B is the free $\mathbb{F}_2[G]$-module of rank r. Since $A \rtimes G$ is a quotient of $B \rtimes G$ (Lemma 3.1.7), $A \rtimes G$ is realisable over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$.

Chapter 4 is devoted to the realization of symmetric groups using reduction modulo some distinct prime numbers $p_1, p_2, p_3 \neq p$, and the continuity of roots (Corollary 4.2.3). One of the consequences of the latter theorem is that there exists a positive integer r such that if $f \in \mathbb{Z}_p[X]$ is of degree n with $f(X)$ congruent to $f_p(X) = X(X-1)\cdots(X-(n-1))$ modulo p^r, then f totally splits in $\mathbb{Q}_p$. The polynomial f is obtained by lifting some polynomials $f_{p_1} \in \mathbb{F}_{p_1}[X], f_{p_2} \in \mathbb{F}_{p_2}[X]$ and $f_{p_3} \in \mathbb{F}_{p_3}[X]$ to polynomials in $\mathbb{Z}[X]$ in such a way that $f \equiv f_p \mod p^r$ and $\mathrm{Gal}(f, \mathbb{Q})$ contains a 2-cycle, an $(n-1)$-cycle, and an n-cycle.

The realization of the alternating groups in Chapter 5 applies a result of Mestre (Proposition 5.3.5) and then Hilbert's irreducibility theorem. The former gives polynomials $f(\mathbf{t}, X) \in \mathbb{Q}(\mathbf{t})[X]$ and $f^*(\mathbf{t}, u, X) \in \mathbb{Q}(\mathbf{t}, u)[X]$ such that $\mathrm{Gal}(f, \mathbb{Q}(\mathbf{t})) \cong A_n$ and $\mathrm{Gal}(f^*, \mathbb{Q}(\mathbf{t}, u)) \cong A_{n-1}$. The specializations of the coefficients of f and f^* allows us to realize these groups over $\mathbb{Q}$. These specializations can be chosen such that the obtained polynomials in $\mathbb{Q}[X]$ are p-close to some polynomials which totally split in $\mathbb{Q}_{\mathrm{tot},p}$. After that, the continuity of roots implies that the splitting fields of the specialized polynomials f and f^* over $\mathbb{Q}$ are contained in $\mathbb{Q}_{\mathrm{tot},p}$.

In the presentation of this thesis most results are cited but occasionally well known result are given without reference. The main original new results in this thesis are Theorem 3.4.3, Theorem 4.3.4, and Theorem 5.5.2. An independent proof has also being given for Theorem 2.3.2, which may be known implicitly from other work, without having been stated explicitly.

Chapter 1

Preliminaries

The goal of this chapter is to give a short description of the field $K_{\mathrm{tot},v}$. For that, we give an introduction to the theory of valuations and point out some useful properties of extensions of valuations to an algebraic extension of the ground field. We are in particular interested in total splitting. After that, we study an important class of valued fields, namely Henselian fields from which we construct $K_{\mathrm{tot},v}$. Finally we concentrate on properties of valuations of $\mathbb{Q}$ and their extensions to number fields. Most of the results in this chapter are presented without proof. For more details, the reader might consult [Jar]

1.1 Valuations

In this section, we define valuations of a field and describe the valuations of $\mathbb{Q}$.

Definition 1.1.1. An abelian group Γ with a total ordering $<$ is called an **ordered group** if $<$ satisfies the following condition: for all $\alpha, \beta, \gamma \in \Gamma$, $\alpha < \beta$ implies $\alpha + \gamma < \beta + \gamma$.

This condition implies that for every positive integer n, $n\alpha < n\beta$ is equivalent to $\alpha < \beta$. In particular the map $\Gamma \longrightarrow \Gamma$: $\alpha \longmapsto n\alpha$ is a monomorphism.

Examples of ordered abelian groups are the additive groups $\mathbb{Z}$ and $\mathbb{R}$. The

group $\mathbb{Z} \times \mathbb{Z}$ is also an ordered group with the lexicographic ordering.

We add an additional element ∞ to Γ that satisfies the following rules, for every $\alpha \in \Gamma$

(1) $\alpha + \infty = \infty + \infty = \infty$,

(2) $\alpha < \infty$.

Definition 1.1.2. Let K be a field and Γ an ordered group. A **valuation** v of K is a map from K to $\Gamma \cup \{\infty\}$ satisfying the following conditions for all $a, b \in K$:

(a) $v(ab) = v(a) + v(b)$.

(b) $v(a + b) \geq \min(v(a), v(b))$.

(c) $v(a) = \infty$ if and only if $a = 0$.

(d) There exists $c \in K$, such that $v(c) \neq 0$.

They imply:

(e) $v(1) = 0$ and $v(-a) = v(a)$ for each $a \in K$.

(f) For all $a, b \in K$, if $v(a) < v(b)$, then $v(a + b) = v(a)$.

We refer to the pair (K, v) as a **valued field**. The subring $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$ of K is the **valuation ring** of v. It has a unique maximal ideal $M_v = \{x \in K \mid v(x) > 0\}$. The field $\bar{K}_v = \mathcal{O}_v/M_v$ is the **residue field** of K at v. The subgroup of Γ defined by $\Gamma_v = v(K^\times)$ is the **value group** of v, it is isomorphic to the quotient $K^\times/\mathcal{O}_v^\times$, where $\mathcal{O}_v^\times$ is the **group of units** of $\mathcal{O}_v$.

Example 1.1.3. *The p-adic valuation.* Consider a unique factorization domain R with quotient field K. Let p be a prime element of R. For every $x \in K^\times$ we can write $x = p^m \frac{a}{b}$, with a unique $m \in \mathbb{Z}$ and relatively prime

elements a, b of R. We define a valuation v_p of K by $v_p(x) = m$. The value group of v_p is $\mathbb{Z}$ and $v_p(p) = 1$ is the smallest positive element in it.

In the case where $R = \mathbb{Z}$ and p is a prime number, the p-adic valuation v_p of $\mathbb{Q}$ has $\mathbb{F}_p$ as its residue field.

Let v be a valuation of a field K and σ an isomorphism of K onto a field K'. Then $v' = v \circ \sigma^{-1}$ is a valuation of K' with $\mathcal{O}_{v'} = \sigma\mathcal{O}_v$ and $\Gamma_{v'} = \Gamma_v$.

Definition 1.1.4 (Equivalence of valuations)**.** Two valuations v_1 and v_2 of a field K with value groups Γ_1 and Γ_2 respectively, are **equivalent** if there exists an ordered preserving isomorphism $f\colon \Gamma_1 \longrightarrow \Gamma_2$ such that $f \circ v_1 = v_2$.

The equivalence of v_1 and v_2 is equivalent to each of the following conditions:

(1) $M_{v_1} = M_{v_2}$.

(2) $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$.

Definition 1.1.5 (Discrete valuation)**.** A valuation v of a field K is **discrete** (sometimes one says **discrete of rank** 1) if the value group Γ_v of v is isomorphic to $\mathbb{Z}$.

In this case, $\mathcal{O}_v$ is a unique factorization domain and M_v is the unique non-zero prime ideal of $\mathcal{O}_v$. If $\alpha \in \Gamma_v$ is the image of 1 under the isomorphism above, then every $\pi \in K^\times$ with $v(\pi) = \alpha$ is a prime element of $\mathcal{O}_v$.

If R is a unique factorization domain, every prime element of R induces a discrete valuation on $\mathrm{Quot}(R)$ as in example 1.1.3.

The next Lemma shows that every valuation of $\mathbb{Q}$ is discrete.

Lemma 1.1.6. Every valuation v of $\mathbb{Q}$ is equivalent to a p-adic valuation v_p, for some prime number p.

Proof. For each $n \in \mathbb{N}$, observe that $v(n) \geq v(1) = 0$. By (d) of Definition 1.1.2, there exists a smallest $p \in \mathbb{N}$ such that $v(p) > 0$. Suppose that $p = ab$ with integers $1 < a, b < p$. Then $v(a) + v(b) = v(p) > 0$. Since $v(a), v(b) \geq 0$, $v(a) > 0$ or $v(b) > 0$. Both cases contradict the minimality of p. Therefore, p is prime number.

Now, consider an integer a such that $p \nmid a$. Then there exist $q \in \mathbb{Z}$ and $1 \leq r < p$ such that $a = qp + r$. By the minimality of p, we have $v(r) = 0$. Hence, by (f) of Definition 1.1.2, $v(a) = v(r)$.

Finally, each nonzero element $x \in \mathbb{Q}$ can be written as $x = p^k \frac{a}{b}$, where $a, b, k \in \mathbb{Z}$ and $p \nmid ab$. By the preceding paragraph, $v(x) = kv(p)$. Since multiplication by $v(p)$ is an isomorphism of $\mathbb{Z}$ onto $v(p)\mathbb{Z}$ that preserves the ordering, v is equivalent to v_p. □

A **valuation ring** of a field K is a proper subring $\mathcal{O}$ of K such that for each $x \in K^\times$, we have $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. It is a local ring with maximal ideal $M = \{x \in \mathcal{O} \mid x^{-1} \notin \mathcal{O}\}$. It is also the valuation ring of a valuation of the field K (See the end of Sect. 2 of [Jar]).

1.2 Extensions of Valuations

There is some ambiguity in the literature about the notion of extensions of valuations. So we start this section by defining what we mean by that notion. Then we introduce places and cite Chevalley's theorem about extensions of places. The latter allows us to extend valuations of given fields to valuations of larger fields.

Definition 1.2.1. [Extension of valuations] Let (K, v) and (L, w) be valued fields. We say that (L, w) **extends** (K, v) and that w is an **extension** of v to L if $K \subseteq L$ and $\mathcal{O}_w \cap K = \mathcal{O}_v$. In this case, $M_w \cap \mathcal{O}_v = M_v$, so $\bar{K}_v = \mathcal{O}_v/M_v$ can be naturally embedded in $\bar{L}_w = \mathcal{O}_w/M_w$, making the following diagram

of short exact sequences commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_w & \longrightarrow & \mathcal{O}_w & \longrightarrow & \bar{L}_w & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \uparrow & & \\ 0 & \longrightarrow & M_v & \longrightarrow & \mathcal{O}_v & \longrightarrow & \bar{K}_v & \longrightarrow & 0 \end{array}$$

Using this embedding, we identify $\bar{K}_v$ as a subfield of $\bar{L}_w$, so that the residue map $\mathcal{O}_w \longrightarrow \bar{L}_w$ extends the residue map $\mathcal{O}_v \longrightarrow \bar{K}_v$. We call $[\bar{L}_w : \bar{K}_v]$ the **residue field degree** of w over v and denote it by $f(w/v)$.

Likewise, $\mathcal{O}_w^\times \cap K^\times = \mathcal{O}_v^\times$, so there is an embedding $\Gamma_v \longrightarrow \Gamma_w$ making the following diagram of short exact sequences commutative:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_w^\times & \longrightarrow & L^\times & \xrightarrow{w} & \Gamma_w & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \uparrow & & \\ 1 & \longrightarrow & \mathcal{O}_v^\times & \longrightarrow & K^\times & \xrightarrow{v} & \Gamma_v & \longrightarrow & 0 \end{array}$$

Using this embedding, we identify Γ_v as an ordered subgroup of Γ_w, so that $w|_K = v$. We call $(\Gamma_w : \Gamma_v)$ the **ramification index** of w over v and denote it by $e(w/v)$.

Lemma 1.2.2. (Cor. 7.2 of [Jar]) If L/K is algebraic, Γ_v is cofinal in Γ_w. In other words, for each $\alpha \in \Gamma_w$ there exists $\beta \in \Gamma_v$ such that $\alpha < \beta$.

If $\Gamma_w = \mathbb{Z}$, then it is customary to normalize v in the following way. By definition, $\Gamma_v = e(w/v)\mathbb{Z}$. Thus, the function v' defined on $K^\times$ by $v'(x) = \frac{1}{e}v(x)$ is a valuation of K with $\Gamma_{v'} = \mathbb{Z}$. Moreover, v' is equivalent to v and $w(x) = v(x) = ev'(x)$ for each $x \in K$.

The residue field degree and the ramification index are multiplicative, that is if $(K, v) \subseteq (L, w) \subseteq (L', w')$ is a tower of valued fields, then $e(w'/v) = e(w'/w)e(w/v)$ and $f(w'/v) = f(w'/w)f(w/v)$ (Prop. 4.7, p. 484 of [La2]).

Let F be a field. We add the symbol ∞ to F and impose the following rules, for each $a \in F$:

(1) $a + \infty = \infty + a = \infty$.

(2) $a \cdot \infty = \infty \cdot a = \infty \cdot \infty = \infty$, if $a \neq 0$.

(3) $\frac{1}{0} = \infty$ and $\frac{1}{\infty} = 0$.

The expressions $\infty + \infty$, $0 \cdot \infty$, ∞/∞ and $0/0$ are not defined.

Definition 1.2.3 (Places)**.** A **place** of a field K is map φ of K into the set $F \cup \{\infty\}$, where F is a field, satisfying the following conditions:

(a) $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$, whenever the right hand side is defined.

(b) There exist $x, y \in K$ with $\varphi(x) = \infty$ and $\varphi(y) \neq 0, \infty$.

These conditions imply that $\varphi(1) = 1, \varphi(0) = 0$ and $\varphi(x^{-1}) = \varphi(x)^{-1}$ if $x \neq 0$. The place φ is **finite** at an element $x \in K$ if $\varphi(x) \neq \infty$, otherwise we say that φ is **infinite** at x. The subring $\mathcal{O}_\varphi = \{x \in K \mid \varphi(x) \neq \infty\}$ of K is the **valuation ring** of φ. It has a unique maximal ideal $M_\varphi = \{x \in K \mid \varphi(x) = 0\}$. The **residue field** $\bar{K}_\varphi = \{\varphi(a) \mid a \in \mathcal{O}_\varphi\}$ of K at φ is isomorphic to the field $\mathcal{O}_\varphi/M_\varphi$.

Two places φ_1 and φ_2 of a field K with residue fields F_1 and F_2 respectively are **equivalent** if there exists an isomorphism $f\colon F_1 \longrightarrow F_2$ such that $\varphi_2 = f \circ \varphi_1$.

There exists a bijective correspondence between valuation classes, place classes, and valuation rings of a field K (see [F-J], page 20).

Places and integrality of an element over an integrally closed domain are related as stated in the following proposition.

Proposition 1.2.4. (p. 12 of [La1]) Let R be an integrally closed domain with quotient field K. Let L be an algebraic extension of K. An element

$x \in L$ is integral over R if and only if every place of L finite on R is finite at x. Thus, the integral closure of R in L is the intersection of all valuation rings of L which contain R. In particular, each valuation ring of L is integrally closed.

Now, Chevalley's theorem guarantees that a valuation v of a field K has at least one extension to each field extension L of K.

Theorem 1.2.5 (Chevalley, see p. 8, Thm. 1 of [La1])**.** *Let φ be a homomorphism of an integral domain R into an algebraically closed filed F. Let L be a field that contains R. Then φ extends to a place of L into F.*

Definition 1.2.6. We say that a valuation v of a field K has **a unique extension** to a field extension L of K if all of the extensions of v to L are equivalent.

Proposition 1.2.7. (Thm. 4, p. 18 of [La1]) Let $(L, w)/(K, v)$ be an algebraic extension of valued fields. Let R be the integral closure of the valuation ring $\mathcal{O}_v$ in L and $\mathfrak{p} = M_w \cap R$. Then $\mathfrak{p}$ is a maximal ideal of R and the valuation ring $\mathcal{O}_w$ is the localization of R at $\mathfrak{p}$. Conversely, if $\mathfrak{p}$ is a prime ideal of R lying over M_v, then $R_{\mathfrak{p}}$ is the valuation ring of a valuation w of L that lies over v and $\mathfrak{p} = M_w \cap R$.

Definition 1.2.8 (Immediate extension)**.** An extension of valued fields $(L, w)/(K, v)$ is **immediate** if the value group and the residue field of (L, w) coincide with those of (K, v).

When L/K is of finite degree, one knows that the ramification index and the residue field degree of an extension to L of a valuation of v of K are finite and bounded by $[L : K]$ (Cor. 3.2.3 of [E-P]). Furthermore, v has at most $[L : K]$ extensions, up to equivalence, to L (Thm. 3.2.9 of [E-P]). Moreover, the sum of all products $e(w_i/v)f(w_i/v)$, for every extension w_i of v to L, is also bounded by $[L : K]$ as stated in the following proposition.

Proposition 1.2.9. (Sec. 8, Chap. 6 of [Bo]) Let (K, v) be a valued field and L a finite extension of K. Suppose $w_1, \ldots, w_g$ are all of the inequivalent extensions of v to L. Then

$$\sum_{i=1}^{g} e(w_i/v) f(w_i/v) \leq [L : K]. \tag{1.2.1}$$

If L/K is Galois, then for every $1 \leq i \leq g$, $e(w_i/v) = e$ and $f(w_i/v) = f$ for some positive integers e and f.

If L/K is separable and v is discrete, then each w_i is discrete and

$$\sum_{i=1}^{g} e(w_i/v) f(w_i/v) = [L : K]. \tag{1.2.2}$$

Definition 1.2.10. Let $(L, w)/(K, v)$ be an extension of discrete valued fields. We say that w is **unramified** over v if $\bar{L}_w/\bar{K}_v$ is a separable extension and $e(w/v) = 1$. The valuation v is unramified in L if each extension of v to L is unramified.

In this case, the condition $e(w/v) = 1$ is equivalent to $M_v\mathcal{O}_w = M_w$. Indeed, using Definition 1.2.1, we may replace v and w by equivalent valuations with $\Gamma_v = \Gamma_w = \mathbb{Z}$ and $w(x) = e(w/v)v(x) = v(x)$ for every $x \in K$. Let $z \in M_w$ and suppose $w(z) = a$. Then there exists $y \in M_v$ such that $v(y) = a$. Hence $w(\frac{z}{y}) = 0$, that is there exists $u \in \mathcal{O}_w^\times$ such that $\frac{z}{y} = u$. Thus, $z = yu \in M_v\mathcal{O}_w$. Conversely, if $M_v\mathcal{O}_w = \mathcal{O}_w$, we choose $\pi \in M_v$ with $M_v = \pi\mathcal{O}_v$. Then $M_w = M_v\mathcal{O}_v = \pi\mathcal{O}_v\mathcal{O}_w = \pi\mathcal{O}_w$. Hence, $\Gamma_w = \Gamma_v$.

Lemma 1.2.11. (Sec. 2.3 of [F-J]) Let $(K, v) \subseteq (L, w) \subseteq (L', w')$ be a tower of discrete valued fields, then the following statements hold.

(a) w'/v is unramified if and only if w'/w and w/v are unramified.

(b) Let L_1 and L_2 be field extensions of K which are contained in a common field. If v is unramified in L_1 and L_2, then v is unramified in L_1L_2.

The next proposition gives a necessary sufficient condition for the unramifiedness of a valuation of $\mathbb{Q}$ in a cyclotomic extension. We will use this result several times in the sequel.

Proposition 1.2.12. (Thm. 9.2, p. 42 of [Jan]) Let n be an integer and p a prime number. Then p is unramified (i.e v_p is unramified) in $\mathbb{Q}(\zeta_n)$ if and only if $p \nmid n$.

1.3 Galois Extensions

In this section, we study the case where the extension of valued fields $(L, w)/(K, v)$ is Galois. We define the decomposition group and the decomposition field of w over K and give some important properties of them.

First, we state a result from Galois theory concerning the decomposition of a prime ideal.

Proposition 1.3.1. (Prop. 2.1, p. 340 of [La2]) Let R be an integrally closed domain with quotient field K. Let L be a finite Galois extension of K and let S be the integral closure of R in L. Let $\mathfrak{p}$ be a prime ideal of R and $\mathfrak{q}$ a prime ideal of S lying over $\mathfrak{p}$. Then a prime ideal $\mathfrak{q}'$ of S is lying over $\mathfrak{p}$ if and only if there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma\mathfrak{q} = \mathfrak{q}'$.

We apply Proposition 1.3.1 to extensions of valuations.

Lemma 1.3.2. Let $(L, w)/(K, v)$ be a Galois extension of valued fields. Then, for each extension w' of v to L there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma\mathcal{O}_w = \mathcal{O}_{w'}$.

Proof. Denote by R the integral closure of $\mathcal{O}_v$ in L. By Proposition 1.2.7, $\mathcal{O}_w$ is the localisation of R at $\mathfrak{p}_w = M_w \cap R$, and $\mathcal{O}_{w'}$ is the localisation of R at $\mathfrak{p}_{w'} = M_{w'} \cap R$. Since $\mathfrak{p}_w$ and $\mathfrak{p}_{w'}$ are prime ideals of R lying over M_v, Proposition 1.3.1 implies that there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma\mathfrak{p}_w = \mathfrak{p}_{w'}$. Therefore $\sigma\mathcal{O}_w = \mathcal{O}_{w'}$. □

It follows from Lemma 1.3.2 that $\{w \circ \sigma^{-1} \mid \sigma \in \mathrm{Gal}(L/K)\}$ is the set of all of the inequivalent extensions of v to L.

Definition 1.3.3 (Decomposition group)**.** The subgroup

$$D_{w/v} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma\mathcal{O}_w = \mathcal{O}_w\}$$

of $\mathrm{Gal}(L/K)$ is the **decomposition group** of w over K (alternatively, over v). The fixed field L_0 of $D_{w/v}$ in L is the **decomposition field** of w over K.

Remark 1.3.4. (Prop. 3.2.16 of [E-P]) The field extension $\bar{L}_w/\bar{K}_v$ is a normal extension and the map $D_{w/v} \longrightarrow \mathrm{Aut}(\bar{L}_w/\bar{K}_v)$ defined by $\sigma \longmapsto \bar{\sigma}$, where $\bar{\sigma}\bar{x} = \overline{\sigma(x)}$ and $\bar{x} = x + M_w$ for each $x \in \mathcal{O}_w$, is an epimorphism.

Lemma 1.3.5. (Cor. 8.3, Prop. 8.6 of [Jar]) Let $(L, w)/(K, v)$ be a Galois extension of valued fields. Let L_0 be the decomposition field of w over K and denote by w_0 the restriction of w to L_0. Then,

(1) w_0 has a unique extension to L,

(2) (L_0, w_0) is an immediate extension of (K, v).

Lemma 1.3.6. Let $(K, v) \subseteq (L, w) \subseteq (L', w')$ be a tower of valued fields such that L/K and L'/K are Galois extension. Then the restriction map res: $\mathrm{Gal}(L'/K) \longrightarrow \mathrm{Gal}(L/K)$ maps $D_{w'/v}$ onto $D_{w/v}$.

Proof. Let $\sigma' \in D_{w'/v}$. Then $\sigma'\mathcal{O}_{w'} = \mathcal{O}_{w'}$, so $\sigma'(\mathcal{O}_{w'} \cap L) = \mathcal{O}_{w'} \cap L$. By assumption, $\mathcal{O}_{w'} \cap L = \mathcal{O}_w$. Hence $\sigma'\mathcal{O}_w = \mathcal{O}_w$, so $\sigma'|_L \in D_{w/v}$. Conversely, consider $\sigma \in D_{w/v}$. Then $\sigma\mathcal{O}_w = \mathcal{O}_w$. Let σ_1' be an arbitrary extension of σ to an element of $\mathrm{Gal}(L'/K)$. Then, $\sigma_1'\mathcal{O}_{w'}$ is a valuation ring of L' that lies over $\mathcal{O}_w$. Hence, by Lemma 1.3.2, there exists $\rho \in \mathrm{Gal}(L'/L)$ such that $\rho\sigma_1'\mathcal{O}_{w'} = \mathcal{O}_{w'}$. Therefore, $\sigma' = \rho\sigma_1' \in D_{w'/v}$ and $\sigma'|_L = \sigma$, as desired. □

Remark 1.3.7. If L_0' is the fixed field of $D_{w'/v}$ in L', Lemma 1.3.6 implies that the fixed field of $D_{w/v}$ in L is $L_0 = L_0' \cap L$.

Proposition 1.3.8. (Cor. 8.5 of [Jar]) Let $(L,w)/(K,v)$ be a finite Galois extension of valued fields and L_0 the decomposition field of w over K. Let $\sigma_1,\ldots,\sigma_m$ be representatives of the left cosets of $\mathrm{Gal}(L/K)$ modulo $\mathrm{Gal}(L/L_0) = D_{w/v}$. The valuations $w\circ\sigma_1^{-1},\ldots,w\circ\sigma_m^{-1}$ are the distinct (up to equivalence) extensions of v to L.

Remark 1.3.9. Let F/E be an algebraic extension.

CLAIM: If w,w' are valuations of F such that $\mathcal{O}_w = \mathcal{O}_{w'}$, $\Gamma_w = \Gamma_{w'}$, and $w|_E = w'|_E$, then $w = w'$. Indeed, we may assume that F/E is finite and let $e = (\Gamma_w : \Gamma_{w|E})$. Let $x \in F$, then there exists $a \in E$ such that $ew(x) = w(a)$. Hence, $w(x^e a^{-1}) = 0$, so $x^e a^{-1} \in \mathcal{O}_w^\times$. Therefore, $x^e a^{-1} \in \mathcal{O}_{w'}^\times$, hence, $w'(x^e a^{-1}) = 0$, so $ew'(x) = w'(a)$. Since $w(a) = w'(a)$, we have $ew(x) = ew'(x)$, consequently $w(x) = w'(x)$ as claimed.

In particular, if F/E is Galois and $\sigma \in \mathrm{Gal}(F/E)$ belongs to the decomposition group D_w of w over E, then $\mathcal{O}_{w\circ\sigma} = \mathcal{O}_w$ and $\Gamma_{w\circ\sigma} = \Gamma_w$. Furthermore, $w\circ\sigma|_E = w|_E$, hence by the claim $w = w\circ\sigma$. $\square$

Proposition 1.3.10. (Prop. 20, p. 21 of [Se]) Let $(L,w)/(K,v)$ be a finite Galois extension of discrete valued fields. Suppose w/v is unramified. Then map defined in Remark 1.3.4 is an isomorphism of $D_{w/v}$ onto $\mathrm{Gal}(\bar{L}_w/\bar{K}_v)$.

Let $(L,w)/(K,v)$ be a finite Galois extension of valued number fields. Then $\bar{K}_v$ is a finite field, so $\bar{L}_w$ is a cyclic extension of $\bar{K}_v$. Suppose w/v is unramified. Then by Proposition 1.3.10, $D_{w/v}$ is isomorphic to $\mathrm{Gal}(\bar{L}_w/\bar{K}_v)$. Since $\mathrm{Gal}(\bar{L}_w/\bar{K}_v)$ is cyclic, so is $D_{w/v}$. Suppose $|\bar{K}_v| = q$, then $\mathrm{Gal}(\bar{L}_w/\bar{K}_v) = \langle\varphi\rangle$ where φ is the Frobenius automorphism defined by $\varphi(x) = x^q$ for $x \in \bar{L}_w$. The image of φ under the isomorphism given by the Proposition 1.3.10 is traditionally denoted by $\left[\frac{L/K}{M_w}\right]$ and is called a **Frobenius element** over v. Then $D_{w/v} = \langle\left[\frac{L/K}{M_w}\right]\rangle$. By Remark 1.3.4, the Frobenius element is defined by the condition $\left[\frac{L/K}{M_w}\right]x \equiv x^q \mod M_w$ for each $x \in \mathcal{O}_w$.

1.4 Total Splitting

In this section, we study some conditions imposed on a valuation of a field K to totally split in an algebraic extension. We need these conditions in the construction of the field $K_{\text{tot},v}$.

Definition 1.4.1. Let (K, v) be a valued field and L a finite extension of K of degree n. We say that v **totally splits** in L if v has exactly n inequivalent extensions to L. Since by Proposition 1.2.9, v has at most n inequivalent extensions to L, v totally splits in L if and only if v has at least n inequivalent extensions to L.

In this case, suppose $w_1, \ldots, w_n$ are all of the inequivalent extensions of v to L. Using the inequalities

$$\sum_{i=1}^{n} e(w_i/v)f(w_i/v) \leq n \text{ and } e(w_i/v)f(w_i/v) \geq 1,$$

we have $e(w_i/v) = f(w_i/v) = 1$. The converse is true for discrete valued fields and separable extensions. Indeed, let $w_1, \ldots, w_g$ be all of the inequivalent extensions of v to L and assume that $e(w_i/v) = f(w_i/v) = 1$ for $i = 1, \ldots, g$. It follows from the equality

$$\sum_{i=1}^{g} e(w_i/v)f(w_i/v) = n$$

that $g = n$, so v totally splits in L.

We give two conditions for total splitting.

Lemma 1.4.2. Let $(L, w)/(K, v)$ be a finite Galois extension of valued fields of degree n. Then v totally splits in L if and only if $D_{w/v} = 1$.

Proof. If $D_{w/v} = 1$, then by Proposition 1.3.8, v totally splits in L.

Conversely, suppose that v totally splits in L, that is v has exactly n inequivalent extensions to L. Let L_0 be the decomposition field of w over

K. Then, by Proposition 1.3.8, $[L_0 : K] = n$, so $L = L_0$. It follows that $\mathrm{Gal}(L/L_0) = D_{w/v} = 1$. $\square$

Lemma 1.4.3. Let (K, v) be a valued field, $f \in \mathcal{O}_v[X]$ a monic irreducible polynomial of degree n, and x a root of f in $\tilde{K}$. Suppose the reduced polynomial $\bar{f}$ with respect to M_v has n distinct roots in $\bar{K}_v$. Then v totally splits in $K(x)$.

Proof. Let $\bar{x}_1, \ldots, \bar{x}_n$ be the distinct roots of $\bar{f}$ in $\bar{K}_v$. For each $1 \leq i \leq n$ we may extend the quotient map $\varphi\colon \mathcal{O}_v \longrightarrow \bar{K}_v$ to a homomorphism $\mathcal{O}_v[X] \longrightarrow \bar{K}_v$ that maps X to $\bar{x}_i$. Since $f(X)$ lies in the kernel of the latter homomorphism, and $\mathcal{O}_v[X]/f(X)\mathcal{O}_v[X] \cong \mathcal{O}_v[x]$, we get a homomorphism $\varphi_i\colon \mathcal{O}_v[x] \longrightarrow \bar{K}_v$ that extends φ. By assumption there exists $a_i \in \mathcal{O}_v$ such that $\varphi(a_i) = \bar{x}_i$. Hence, $\varphi_i(x - a_i) = \varphi_i(x) - \varphi(a_i) = \bar{x}_i - \bar{x}_i = 0$ and $\varphi_j(x - a_i) = \bar{x}_j - \bar{x}_i \neq 0$, if $i \neq j$. Hence $\mathrm{Ker}(\varphi_i) \neq \mathrm{Ker}(\varphi_j)$ if $i \neq j$. By Chevalley, $K(x)$ has a valuation w_i such that $\mathcal{O}_{w_i} \cap K[x] = \mathrm{Ker}(\varphi_i)$, so $\mathcal{O}_{w_i} \cap \mathcal{O}_v = M_v$, hence w_i extends v. Moreover, $\mathcal{O}_{w_1}, \ldots, \mathcal{O}_{w_n}$ are distinct, so $w_1, \ldots, w_n$ are inequivalent. Consequently, v totally splits in $K(x)$. $\square$

Lemma 1.4.4. Let (K, v) be a valued field, L a finite separable extension of K, and $\hat{L}$ the Galois closure of L/K. Suppose v totally splits in L. Then v totally splits in $\hat{L}$.

Proof. Let w be a valuation of $\hat{L}$ lying over v. Using Lemma 1.4.2, it suffices to prove that the decomposition group $D_{w/v}$ of w over v is trivial. Consider $\sigma \in D_{w/v}$. By Remark 1.3.9, $w = w \circ \sigma$.

CLAIM: $\sigma \in \mathrm{Gal}(\hat{L}/L)$. Indeed, let $d = [L : K]$. By assumption, L has d distinct valuations $v_1, \ldots, v_d$ extending v. For each $1 \leq i \leq d$ we extend v_i to a valuation w_i of $\hat{L}$ such that $w_1 = w$. By the Lemma 1.3.2 and Remark 1.3.9, there exists $\sigma_i \in \mathrm{Gal}(\hat{L}/K)$ such that $w_i = w \circ \sigma_i$ and $\sigma_1 = 1$. If some $1 \leq i, j \leq d$ satisfy $\sigma_i \mathrm{Gal}(\hat{L}/L) = \sigma_j \mathrm{Gal}(\hat{L}/L)$, then for each $x \in L$ we have $v_i(x) = w_i(x) = w(\sigma_i x) = w(\sigma_j x) = w_j(x) = v_j(x)$, so

$v_i = v_j$, hence $i = j$. Thus, $\sigma_1\mathrm{Gal}(\hat{L}/L), \ldots, \sigma_d\mathrm{Gal}(\hat{L}/L)$ are distinct cosets of $\mathrm{Gal}(\hat{L}/L)$ in $\mathrm{Gal}(\hat{L}/K)$. Since $(\mathrm{Gal}(\hat{L}/K) : \mathrm{Gal}(\hat{L}/L)) = d$, we have $\mathrm{Gal}(\hat{L}/K) = \bigcup_{i=1}^{d} \sigma_i\mathrm{Gal}(\hat{L}/L)$. In particular, $\sigma = \sigma_i\eta$ for some $1 \leq i \leq d$ and $\eta \in \mathrm{Gal}(\hat{L}/L)$. If $2 \leq i \leq d$, then by the first paragraph of the proof, $v_1 = w|_L = w \circ \sigma|_L = w \circ \sigma_i \circ \eta|_L = w_i|_L = v_i$, which is a contradiction. it follows that $i = 1$, so $\sigma = \eta \in \mathrm{Gal}(\hat{L}/L)$ as claimed.

Now, since v totally splits in L, it totally splits in each of the conjugate L' of L over K. By the claim, σ belongs to $\mathrm{Gal}(\hat{L}/L')$. Since the compositum of all of the fields L' is $\hat{L}$, we conclude that $\sigma = 1$ as asserted. $\square$

Lemma 1.4.5. Let (K, v) be a valued field, $L_1, \ldots, L_n$ linearly disjoint finite extensions of K contained in a common field. Suppose v totally splits in $L_1, \ldots, L_n$. Then v totally splits in $L_1 \cdots L_n$.

Proof. Denote $d_i = [L_i : K]$, for $1 \leq i \leq n$. Let $v_{i,1}, v_{i,2}, \ldots, v_{i,d_i}$ be all of the inequivalent extensions of v to L_i. We choose an extension $v_{i,i(j)}$ for each $1 \leq i \leq n$ and denote by $\varphi_{i,j(i)}$ the corresponding place. The places $\varphi_{1,1(i)}, \varphi_{2,2(i)}, \ldots, \varphi_{n,n(i)}$ coincide on K, then there exists a place φ of $L_1L_2 \cdots L_n$ that extends each $\varphi_{i,j(i)}$ (Lemma 2.5.5 of [F-J]). It follows that v has $d_1d_2 \cdots d_n$ distinct extensions to $L_1L_2 \cdots L_n$, that is v totally splits in $L_1L_2 \cdots L_n$. $\square$

1.5 Henselization

In this section, we define Henselian fields in several equivalent ways. Then we construct Henselian closures for each valued field and prove that all of them are conjugate over the base field.

If (K, v) is a valued field and $a \in \mathcal{O}_v$, we denote the reduction of a modulo M_v by $\bar{a}$.

Definition 1.5.1. [Henselian field] We say that a valued field (K, v) is a Henselian if for each polynomial $f \in \mathcal{O}_v[X]$ and for each $a \in \mathcal{O}_v$ such that $\bar{f}(\bar{a}) = 0$ and $\bar{f}'(\bar{a}) \neq 0$, there exists $x \in \mathcal{O}_v$ such that $f(x) = 0$ and $\bar{x} = \bar{a}$ (Hensel's Lemma).

Proposition 1.5.2. (Def. 11.1 of [Jar]) The following conditions on a valued field (K, v) are equivalent:

(1) (K, v) is Henselian

(2) The valuation v extends uniquely to every algebraic extension of K.

(3) For every monic polynomial $f \in \mathcal{O}_v[X]$, each $a \in \mathcal{O}_v$, and each $\gamma \in \Gamma_v$ such that $\gamma \geq 0$ and $v(f(a)) > 2v(f(a)) + \gamma$, there exists $x \in \mathcal{O}_v$ such that $f(x) = 0$ and $v(x - a) > v(f(a)) + \gamma$ (Hensel-Rychlick).

Corollary 1.5.3. Let (L, w) be a Henselian field and K a subfield of L. Then $L \cap K_s$ is Henselian with respect to the restriction of w to it.

The next proposition states that every valued field has a minimal algebraic extension, unique up to isomorphism, that satisfies Hensel's Lemma.

Proposition 1.5.4. (Prop. 14.1 of [Jar]) Every valued field (K, v) has a separable algebraic extension (K_v, v_h) which has the following properties:

(1) (K_v, v_h) is Henselian.

(2) If (L, w) is a Henselian extension of (K, v), then (K_v, v_h) can be embedded in (L, w) over (K, v).

The valued field (K_v, v_h) defined above is called a **Henselian closure** of the valued field (K, v).

Remark 1.5.5. (1) The proof of Proposition 14.1 in [Jar] shows that if (K, v) is a valued field, v_s is an extension of v to K_s, K_v is the decomposition field of v_s over K, and we set $v_h = v_s|_{K_v}$, then (K_v, v_h) is a Henselian closure of (K, v).

(2) Let N be a Galois extension of K, w the restriction of v_s to N. By Remark 1.3.7, the fixed field of $D_{w/v}$ in N is $N \cap K_v$.

(3) If a Henselian extension (L, w) of (K, v) is contained in (K_v, v_h) then $(L, w) = (K_v, v_h)$. Indeed, by definition, K_v can be embedded in L over K. By Lemma 20.6.2 of [F-J] $L = K_v$.

(4) By Lemma 1.3.2 and by (1), any two Henselizations of (K, v) are K-conjugate.

Lemma 1.5.6. Let (K_v, v_h) be a Henselian closure of a valued field (K, v) and consider a valued field (L, w) that extends (K, v) and is contained in (K_v, v_h). Then (K_v, v_h) is also a Henselian closure of (L, w).

Proof. Let v_s be the unique extension of v_h to K_s, L_w be the decomposition field of v_s over L, and $w_h = v_s|_{L_w}$. Then (L_w, w_h) is a Henselian closure of (L, w). Furthermore, for every $\sigma \in D_{v_s/w}$, $\sigma\mathcal{O}_{v_s} = \mathcal{O}_{v_s}$, hence $\sigma \in D_{v_s/v}$. It follows that $\mathrm{Gal}(L_w) \leq \mathrm{Gal}(K_v)$, so $K_v \subseteq L_w$. By (3) of Remark 1.5.5, $(L_w, w_h) = (K_v, v_h)$. $\square$

In the case where $K = \mathbb{Q}$, we denote a Henselization of $(\mathbb{Q}, v_p)$, for a prime number p, by $(\mathbb{Q}_p, v_{p,h})$ and by $\mathbb{Z}_p$ the valuation ring of $v_{p,h}$ (however, this is a non-standard notation. Usually, $\mathbb{Q}_p$ denotes the completion of $\mathbb{Q}$ with respect to v_p and $\mathbb{Z}_p$ denotes the ring of integers of $\mathbb{Q}_p$, see Sect. 6.5 of [Bo]). Let $\tilde{v}$ be the unique extension of $v_{p,h}$ to $\tilde{\mathbb{Q}}$. If $N/\mathbb{Q}$ is a Galois extension and $w = \tilde{v}|_N$, the field $N_0 = N \cap \mathbb{Q}_p$ is the decomposition field of w over $\mathbb{Q}$ (Remark 1.3.7). Thus, $\mathrm{Gal}(N/N_0)$ is the decomposition group of w over $\mathbb{Q}$. If p is unramified in N, then $D_{w/v_p} = \langle\varphi\rangle$, where φ is a Frobenius element at p (Proposition 1.3.10).

1.6 The Field $K_{\mathbf{tot},v}$

In this section, we construct the field $K_{\mathrm{tot},v}$ and give some of its useful properties.

Let (K_v, v_h) be a Henselization of a valued field (K, v).

Definition 1.6.1. We consider the field $K_{\text{tot},v} = \bigcap_{\sigma \in \text{Gal}(K)} \sigma K_v$.

For all $\tau \in \text{Gal}(K)$, $\tau K_{\text{tot},v} = K_{\text{tot},v}$, so $K_{\text{tot},v}$ is a Galois extension of K. If L is a Galois extension of K which is contained in K_v, then $L \subseteq K_{\text{tot},v}$. Hence, $K_{\text{tot},v}$ is the maximal Galois extension of K in K_v. In other words, if L/K is Galois, then $L \subseteq K_v$ if and only if $L \subseteq K_{\text{tot},v}$.

Lemma 1.6.2. If L is a finite extension of K in $K_{\text{tot},v}$, then v totally splits in L.

Proof. First we consider the case where L/K is a Galois extension. Let v_s be the unique extension of v_h to K_s and w be the restriction of v_h to L. By assumption, $\text{Gal}(K_v) \leq \text{Gal}(L)$. Hence, by Lemma 1.3.6, $D_{w/v} = \text{res}_L(D_{v_s/v}) = \text{res}_L(\text{Gal}(K_v)) = 1$. By Lemma 1.4.2, v totally splits in L.

Next, consider an arbitrary finite extension L of K in $K_{\text{tot},v}$ and let $\hat{L}$ be the Galois closure of L/K. Then $\sigma L \subseteq \sigma K_{\text{tot},v} = K_{\text{tot},v}$ for every $\sigma \in \text{Gal}(K)$. Hence, $\hat{L} = \prod_{\sigma \in \text{Gal}(K)} \sigma L \subseteq K_{\text{tot},v}$. By the preceding paragraph, v totally splits in $\hat{L}$.

Finally, let $v_1, \ldots, v_l$ be all of the inequivalent extensions of v to L. For each $1 \leq i \leq l$, let $(L_i, v_{i,h})$ be a Henselization of (L, v_i). Then $(L_i, v_{i,h})$ is a Henselian extension of (K, v), so L_i contains a K-conjugate of K_v, hence $\hat{L} \subseteq L_i$. Since $\hat{L}/L$ is Galois, $\hat{L} \subseteq L_{\text{tot},v_i}$. Hence by the preceding paragraph applied to (L, v_i), v_i totally splits in $\hat{L}$. Thus, v_i has exactly $[\hat{L} : L]$ inequivalent extensions to $\hat{L}$. It follows that v has exactly $l[\hat{L} : L]$ inequivalent extensions to $\hat{L}$. Moreover, by the preceding paragraph, v has exactly $[\hat{L} : K]$ inequivalent extensions to $\hat{L}$. It follows that $l[\hat{L} : L] = [\hat{L} : K]$, so $l = [L : K]$, that is v totally splits in L. $\square$

Proposition 1.6.3. The field $K_{\text{tot},v}$ is the union of all finite separable extensions of K in which v totally splits.

Proof. Denote the union mentioned in the proposition be N. By Lemma 1.6.2, $K_{\mathrm{tot},v} \subseteq N$. Conversely, if v totally splits in a finite separable extension L of K, then, by Lemma 1.4.4, v totally splits in the Galois closure $\hat{L}$ of L/K. Let v_s be an extension of v to K_s and $w = v_s|_{\hat{L}}$. Then, by Lemma 1.4.2, $D_{w/v} = 1$. Since $\mathrm{Gal}(K_v) = D_{v_s/v}$ (Remark 1.5.5) and the restriction of $D_{v_s/v}$ to $\hat{L}$ is $D_{w/v}$ (Lemma 1.3.6), $\mathrm{Gal}(K_v) \leq \mathrm{Gal}(\hat{L})$. Hence, $L \subseteq \hat{L} \subseteq K_v$, as claimed. $\square$

Chapter 2

Abelian Extensions of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},\boldsymbol{p}}$

The aim of this chapter is to construct a Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$ with a Galois group isomorphic to a given finite abelian group. We start from cyclic groups. Then we use the decomposition of a finite abelian group to a product of cyclic groups to realize that group in $\mathbb{Q}_{\mathrm{tot},p}$.

2.1 Useful Tools

In this section, we describe useful tools for the realization of abelian groups in $\mathbb{Q}_{\mathrm{tot},p}$. We prove that, for a prime number q not dividing an integer n, $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \mathrm{ord}_n(q)$. We also notice that for a prime number l and an integer n such that $l \equiv 1 \mod n$, $\mathbb{Q}(\zeta_l)$ contains a unique cyclic subextension of degree n of $\mathbb{Q}$. At the end of the section we prove a special case of Dirichlet's theorem on primes in arithmetic progressions and state a special case of Chebotarev's Density Theorem.

Let m and n be relatively prime integers. We denote by $\mathrm{ord}_n(m)$ the order of m in the multiplicative group $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$.

Lemma 2.1.1. Let n be a positive integer and q a prime number not dividing n. Then $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \mathrm{ord}_n(q)$.

Proof. For each positive integer k we have the following equivalences:

$$\zeta_n \in \mathbb{F}_{q^k} \iff \zeta_n^{q^k} = \zeta_n \iff q^k \equiv 1 \mod n.$$

The smallest positive integer k satisfying this equivalence is $k = \mathrm{ord}_n(q)$. Therefore, ζ_n belongs to $\mathbb{F}_{q^{\mathrm{ord}_n(q)}}$ and not to any proper subfield. Therefore, ζ_n has degree $\mathrm{ord}_n(q)$ over $\mathbb{F}_q$. □

Remark 2.1.2. (1) Let K be a field and n a positive integer such that $\mathrm{char}(K) \nmid n$. Then the polynomial $X^n - 1$ is separable over K. In the case where $K = \mathbb{Q}$, a primitive n-th root of unity ζ_n has degree $\varphi(n)$ over $\mathbb{Q}$ with irreducible polynomial the n-th cyclotomic polynomial $\Phi_n(X) \in \mathbb{Z}[X]$. The constant term of $\Phi_n(X)$ is ± 1 and we have $X^n - 1 = \prod_{d|n} \Phi_d(X)$. The n-th cyclotomic field $\mathbb{Q}(\zeta_n)$ is the decomposition field of $\Phi_n(X)$ with Galois group over $\mathbb{Q}$ isomorphic to $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ (for more details, see Sec. 13.2 of [I-R]).

(2) If m and n are relatively prime positive integers, then $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_n)$ are linearly disjoint over $\mathbb{Q}$. It follows that if $l_1, l_2, l_3, \ldots$ are distinct prime numbers, then the sequence of fields $\mathbb{Q}(\zeta_{l_1}), \mathbb{Q}(\zeta_{l_2}), \mathbb{Q}(\zeta_{l_3}), \ldots$ is linearly disjoint over $\mathbb{Q}$ (Example 2.5.9 of [F-J]).

Lemma 2.1.3. Let l be a prime number and n a positive integer such that $l \equiv 1 \mod n$. Then $\mathbb{Q}(\zeta_l)$ has a unique cyclic subextension L of degree n over $\mathbb{Q}$.

Proof. We have:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \cong \left(\mathbb{Z}/l\mathbb{Z}\right)^\times \cong \mathbb{Z}/(l-1)\mathbb{Z} \tag{2.1.1}$$

Since $l \equiv 1 \mod n$, there exists a surjective homomorphism:

$$\psi : \mathbb{Z}/(l-1)\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

Hence, by (2.1.1), there exits an epimorphism

$$\phi : \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

By Galois theory, the fixed field L of $\mathrm{Ker}(\phi)$ in $\mathbb{Q}(\zeta_l)$ is a cyclic extension of $\mathbb{Q}$ of degree n. $\square$

Lemma 2.1.4. Let $n \in \mathbb{N}$ and p a prime number such that $p \nmid n$. If y is an integer such that $\Phi_n(y) \equiv 0 \mod p$, then $\mathrm{ord}_p(y) = n$.

Proof. We have $\Phi_1(X) = X - 1$. Hence, if $\Phi_1(y) \equiv 0 \mod p$, then $y \equiv 1 \mod p$, so $\mathrm{ord}_p(y) = 1$. Now assume that $n > 1$ and consider an integer y such that $\Phi_n(y) \equiv 0 \mod p$. Then, $y^n - 1 \equiv 0 \mod p$, that is $y^n \equiv 1 \mod p$. Assume $\mathrm{ord}_p(y) = d < n$. Then, $y^d - 1 \equiv 0 \mod p$ and $d|n$. On the other hand, we have,

$$X^d - 1 \equiv \prod_{j|d} \Phi_j(X) \mod p.$$

Hence, there exists j, $j|d$, such that $\Phi_j(y) \equiv 0 \mod p$.

Since $j|d$ and $d < n$, we have

$$X^n - 1 = \Phi_j(X)\Phi_n(X) \prod_{\substack{h|n \\ h\neq j,\, h\neq n}} \Phi_h(X).$$

Hence, $X^n - 1$ has a double root modulo p which contradicts the assumption that $p \nmid n$. Therefore $\mathrm{ord}_p(y) = n$. $\square$

Dirichlet's theorem states that for any two positive relatively prime integers a and n, there are infinitely many prime numbers p such that $p \equiv a \mod n$. In this work, we use only the case $a = 1$. This case has an elementary proof.

Lemma 2.1.5. For any positive integer n, there are infinitely many prime number p such that $p \equiv 1 \mod n$.

Proof. Assume that there are only finitely many prime numbers p such that $p \equiv 1 \mod n$. List them as $p_1, p_2, \ldots, p_r$. Consider the n-th cyclotomic polynomial Φ_n. Since $\Phi_n(X)$ is a monic polynomial in $\mathbb{Z}[X]$, we have, for a sufficiently large integer y, that

$$h = \Phi_n(ynp_1p_2\cdots p_r) > 1$$

and h is an integer. Let

$$\Phi_n(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0,$$

with $a_0, \ldots, a_{d-1} \in \mathbb{Z}$ and $a_0 = \pm 1$. Hence,

$$h = (ynp_1p_2\cdots p_r)^d + a_{d-1}(ynp_1p_2\cdots p_r)^{d-1} + \cdots \pm 1.$$

Therefore,

$$h \equiv \pm 1 \mod p_i \text{ for all } i = 1, \ldots, r \tag{2.1.2}$$

and

$$h \equiv \pm 1 \mod n. \tag{2.1.3}$$

Since $h > 1$, there exists a prime p such that $p|h$ and, by (2.1.3), $p \nmid n$. Then, we have

$$\Phi_n(ynp_1p_2\cdots p_r) = h \equiv 0 \mod p.$$

It follow from Lemma 2.1.4 that $\mathrm{ord}_p(ynp_1p_2\cdots p_r) = n$. But $|(\mathbb{F}_p)^\times| = p-1$, hence $n|p-1$, so $p \equiv 1 \mod n$. Therefore there exists $i \in \{1, \ldots, r\}$ such that $p = p_i$. This is a contradiction, because by (2.1.2), no p_i divides h. Consequently, there are infinitely many prime numbers p such that $p \equiv 1 \mod n$. □

The following Lemma is a special case of the Chebotarev's Density Theorem.

Lemma 2.1.6. (Lemma 13.3.1 in [F-J]) Let $L/\mathbb{Q}$ be a finite extension. Then there exist infinitely many prime numbers p such that $\bar{L}_w = \mathbb{F}_p$ for every extension w of v_p to L.

Remark 2.1.7. Since there are only finitely many prime numbers p which ramify in a number field, Lemma 2.1.6 implies that for every finite extension $L/\mathbb{Q}$ there exist infinitely many prime numbers p totally splitting in L.

2.2 Cyclic Extensions of $\mathbb{Q}$ in $\mathbb{Q}_{\mathbf{tot},p}$

In this section, we use several methods to construct finite cyclic extensions of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$. We start from the case of $\mathbb{Z}/2\mathbb{Z}$, then move to the case of $\mathbb{Z}/q\mathbb{Z}$ for an arbitrary prime number q, and then we realize the groups $\mathbb{Z}/q^k\mathbb{Z}$ for arbitrary q and k. Indeed, in each case we construct linearly disjoint extensions with those groups. So, we may finally compose extensions with Galois groups $\mathbb{Z}/q^k\mathbb{Z}$ for several q's and k's to a $\mathbb{Z}/n\mathbb{Z}$-extension of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$.

The first case is that of quadratic extensions. To start with, we consider an odd prime number p.

Lemma 2.2.1. Let p an odd prime number and d a square free positive integer such that $p \nmid d$. The following conditions are equivalent:

(1) d is a square in $\mathbb{Q}_p$.

(2) $\left(\frac{d}{p}\right) = 1$

Proof. Suppose there exists $a \in \mathbb{Q}_p$ such that $d = a^2$. Then, $a \in \mathbb{Z}_p$. Reducing with respect to p gives $\bar{d} = \bar{a}^2$. Hence, $\left(\frac{d}{p}\right) = 1$.

Conversely, suppose there exists a positive integer a such that $d \equiv a^2 \mod p$. Then, $a \in \mathbb{Z}_p$ and $f(X) = X^2 - d \in \mathbb{Z}_p[X]$ satisfies $\bar{f}(\bar{a}) = 0$ and $\bar{f}'(\bar{a}) \neq 0$ (since $p \neq 2$). Hence, by Definition 1.5.1, there exists $x \in \mathbb{Z}_p$ such that $f(x) = 0$, so $d = x^2$. □

Lemma 2.2.2. For every odd prime p, $\mathbb{Q}$ has a linearly disjoint sequence $L_1, L_2, \ldots$ of quadratic extensions in $\mathbb{Q}_{\mathrm{tot},p}$.

Proof. First method: By Lemma 2.1.5, there exists an infinite sequence of distinct odd primes $l_1, l_2, \ldots$ such that $l_i \equiv 1 \mod p$. Each of them satisfies $\left(\frac{l_i}{p}\right) = 1$. By Lemma 2.2.1, $\mathbb{Q}(\sqrt{l_i}) \subseteq \mathbb{Q}_p$, for every i and $\mathrm{Gal}(\mathbb{Q}(\sqrt{l_i})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. Since the l_i's are distinct, the $\mathbb{Q}(\sqrt{l_i})$'s are linearly disjoint over $\mathbb{Q}$.

Second method: Consider a sequence of distinct pairs of distinct primes $(l_1', l_1''), (l_2', l_2''), \ldots$ and fix an i. If l_i' is a quadratic residue modulo p, we set $L_i = \mathbb{Q}(\sqrt{l_i'})$. If l_i' is not a quadratic modulo p but l_i'' is, we set $L_i = \mathbb{Q}(\sqrt{l_i''})$. Otherwise, $\left(\frac{l}{p}\right) = \left(\frac{l'}{p}\right) = -1$, so $\left(\frac{ll'}{p}\right) = 1$ and we set $L_i = \mathbb{Q}(\sqrt{l_i' l_i''})$. In all cases, by Lemma 2.2.1, $L_i \subseteq \mathbb{Q}_p$. The choice of the prime numbers implies that the L_i's are linearly disjoint over $\mathbb{Q}$. □

Now, let us consider the case where $p = 2$. We recall:

Lemma 2.2.3. A unit u of $\mathbb{Z}_2$ is a square if and only if $u \equiv 1 \mod 8$.

Proof. The necessity of the Lemma follows from the fact that a square of an odd integer is congruent to 1 modulo 8.

Conversely, the polynomial $f(X) = X^2 - u \in \mathbb{Z}_2[X]$ satisfies $v_2(f(1)) = v_2(1-u) \geq 3$ and $2v_2(f'(1)) = 2v_2(2) = 2$. By (3) of Lemma 1.5.2, there exists $x \in \mathbb{Z}_2$ such that $f(x) = 0$. That is $u = x^2$. □

Lemma 2.2.4. $\mathbb{Q}$ has a linearly disjoint sequence $L_1, L_2, \ldots$ of quadratic extensions in $\mathbb{Q}_{\mathrm{tot},2}$.

Proof. First method: By Lemma 2.1.5, there exists a sequence of distinct primes $l_1, l_2, \ldots$, such that $l_i \equiv 1 \mod 8$. By Lemma 2.2.3, $L_i = \mathbb{Q}(\sqrt{l_i})$ is contained in $\mathbb{Q}_2$ and $L_1, L_2, \ldots$ are linearly disjoint over $\mathbb{Q}$.

Second method: Consider a sequence of disjoint 3-tuples of distinct primes $(l_1, l_1', l_1''), (l_2, l_2', l_2''), \ldots$. For each i, we distinguish between two cases:

Case 1: One of the element l_i, l_i', l_i'', say l_i, is congruent to 1 modulo 8. We set $L_i = \mathbb{Q}(\sqrt{l_i})$.

Case 2: We have $l_i, l_i', l_i'' \not\equiv 1 \mod 8$. If two of them are congruent modulo 8, say $l_i \equiv l_i' \mod 8$, then $l_i l_i' \equiv l_i^2 \equiv 1 \mod 8$ and we set $L_i = \mathbb{Q}(\sqrt{l_i l_i'})$. Otherwise, $l_i l_i' l_i'' \equiv 3 \cdot 5 \cdot 7 \equiv 1 \mod 8$ and we set $L_i = \mathbb{Q}(\sqrt{l_i l_i' l_i''})$.

Therefore, in each case $\mathrm{Gal}(L_i/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ and Lemma 2.2.3 implies that $L_i \subseteq \mathbb{Q}_2$. Moreover, by the choice of the 3-tuples, the L_i's are linearly disjoint over $\mathbb{Q}$. $\square$

Now, we generalise to cyclic extensions of arbitrary prime degree.

Proposition 2.2.5. Let p and q be prime numbers. Then $\mathbb{Q}$ has a linearly disjoint sequence $L_1, L_2, \ldots$ of Galois extensions such that $\mathrm{Gal}(L_i/\mathbb{Q}) \cong \mathbb{Z}/q\mathbb{Z}$ and $L_i \subseteq \mathbb{Q}_{\mathrm{tot},p}$, for all i.

Proof. (Peter Roquette) Let $l_1, l_2 \neq p$ be distinct primes such that $l_1, l_2 \equiv 1 \mod q$. By Lemma 2.1.3, there exist distinct Galois extensions L_1 and L_2 of $\mathbb{Q}$ such that $L_1 \subseteq \mathbb{Q}(\zeta_{l_1})$, $L_2 \subseteq \mathbb{Q}(\zeta_{l_2})$, and $\mathrm{Gal}(L_1/\mathbb{Q}) \cong \mathrm{Gal}(L_2/\mathbb{Q}) \cong \mathbb{Z}/q\mathbb{Z}$. Since $\mathbb{Q}(\zeta_{l_1})$ and $\mathbb{Q}(\zeta_{l_2})$ are linearly disjoint over $\mathbb{Q}$, so are L_1 and L_2. Hence, $N = L_1 L_2$ is a Galois extension of $\mathbb{Q}$ with Galois group $\mathrm{Gal}(N/\mathbb{Q}) \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Now, since $l_1, l_2 \neq p$, the prime p is unramified in $\mathbb{Q}(\zeta_{l_1})$ and $\mathbb{Q}(\zeta_{l_2})$ (Proposition 1.2.12). It follows from Lemma 1.2.11 that p is unramified in L_1, in L_2, and in N. Hence, the fixed field N_0 of the Frobenius φ at p in N is contained in $\mathbb{Q}_p$ (Remark 1.3.7) and the group $\mathrm{Gal}(N/N_0)$ is cyclic.

Since $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ is not cyclic, $|\langle\varphi\rangle|$ is 1 or q. If $|\langle\varphi\rangle| = 1$, then $N \subseteq \mathbb{Q}_p$. Hence, $L_1, L_2 \subseteq \mathbb{Q}_p$. If $|\langle\varphi\rangle| = q$, then $\mathrm{Gal}(N_0/\mathbb{Q}) \cong \mathbb{Z}/q\mathbb{Z}$. Thus, in each case, $\mathbb{Q}$ has a cyclic extension of degree q in $\mathbb{Q}_p$.

Finally, by Lemma 2.1.5, there exists a sequence of distinct pairs of distinct primes $(l_1, l_1'), (l_2, l_2'), \ldots$ such that $l_i, l_i' \equiv 1 \mod q$, $l_i, l_i' \neq p$ and we can construct a field $N_{0,i}$ as in the previous paragraphs. Then the $N_{0,i}$'s are linearly disjoint Galois extensions of $\mathbb{Q}$ in $\mathbb{Q}_p$ with $\mathrm{Gal}(N_{0,i}/\mathbb{Q}) \cong \mathbb{Z}/q\mathbb{Z}$. □

The generalization of Proposition 2.2.5 to cyclic extensions whose degree is a power of a prime number applies the following Lemma from abelian group theory.

Lemma 2.2.6. Let $\bar{V}$ be a free $\mathbb{Z}/n\mathbb{Z}$-module of rank r and $\bar{U}$ a submodule. Then $\bar{V}$ has a $\mathbb{Z}/n\mathbb{Z}$-basis $\bar{v}_1, \ldots, \bar{v}_r$ and there exist $a_1, \ldots, a_r \in \mathbb{Z}$ such that $\bar{V} = \bigoplus_{i=1}^{r} (\mathbb{Z}/n\mathbb{Z})\bar{v}_i$ and $\bar{U} = \bigoplus_{i=1}^{e} (\mathbb{Z}/n\mathbb{Z})\bar{a}_i\bar{v}_i$, where e is the minimal number of generators of $\bar{U}$ as an abelian group. In particular, $(\mathbb{Z}/n\mathbb{Z})^{r-e}$ is a quotient of $\bar{V}/\bar{U}$.

Proof. Let V be a free $\mathbb{Z}$-module of rank r. We choose a $(\mathbb{Z}/n\mathbb{Z})$-basis $\bar{w}_1, \ldots, \bar{w}_r$ for $\bar{V}$ and a $\mathbb{Z}$ basis $w_1, \ldots, w_r$ for V. Then, the map $w_i \longmapsto \bar{w}_i, i = 1, \ldots, r$, extends to an epimorphism $\varphi\colon V \longrightarrow \bar{V}$ such that $\varphi(av) = \bar{a}\varphi(v)$ for all $a \in \mathbb{Z}$ and $v \in V$, where $\bar{a} = a + n\mathbb{Z}$. In particular, $\ker(\varphi) = nV$.

Now we lift generators $\bar{u}_1, \ldots, \bar{u}_e$ of $\bar{U}$ to elements $u_1, \ldots, u_e$ of V and set $U = \sum_{i=1}^{e} \mathbb{Z}u_i$. Then e also is the minimal number of generators of U and $\varphi(U) = \bar{U}$. By the theory of the finitely generated abelian groups, $e \leq r$, V has a $\mathbb{Z}$-basis $v_1, \ldots, v_r$, and there exist $a_1, \ldots, a_e \in \mathbb{Z}$ such that $V = \bigoplus_{i=1}^{r} \mathbb{Z}v_i$ and $U = \bigoplus_{i=1}^{e} \mathbb{Z}a_iv_i$. Applying φ to the latter relations, we get $\bar{V} = \sum_{i=1}^{r} (\mathbb{Z}/n\mathbb{Z})\bar{v}_i$ and $\bar{U} = \sum_{i=1}^{e} (\mathbb{Z}/n\mathbb{Z})\bar{a}_i\bar{v}_i$.

We prove that $\bar{v}_1, \ldots, \bar{v}_r$ are linearly independent over $\mathbb{Z}/n\mathbb{Z}$. Indeed, let $\bar{b}_1, \ldots, \bar{b}_r$ be elements of $\mathbb{Z}/n\mathbb{Z}$ such that $\sum_{i=1}^{r} \bar{b}_i\bar{v}_i = 0$. For each $1 \leq i \leq r$ we lift $\bar{b}_i$ via φ to an integer b_i. Then $\sum_{i=1}^{r} b_iv_i \in nV$. By the first paragraph, there exist $c_1, \ldots, c_r \in \mathbb{Z}$ such that $\sum_{i=1}^{r} b_iv_i = \sum_{i=1}^{r} nc_iv_i$. Since $v_1, \ldots, v_r$ are linearly independent over $\mathbb{Z}$, we have $b_i = nc_i$, so $\bar{b}_i = 0$ for $i = 1, \ldots, r$.

It follows that $\bar{V} = \bigoplus_{i=1}^{r} (\mathbb{Z}/n\mathbb{Z})\bar{v}_i$ and $\bar{U} = \bigoplus_{i=1}^{e} (\mathbb{Z}/n\mathbb{Z})\bar{a}_i\bar{v}_i$. Therefore,

$$\bar{V}/\bar{U} \cong \Big(\bigoplus_{i=1}^{e} (\mathbb{Z}/n\mathbb{Z})/(\mathbb{Z}/n\mathbb{Z})\bar{a}_i\Big) \oplus (\mathbb{Z}/n\mathbb{Z})^{r-e}.$$

Consequently, $(\mathbb{Z}/n\mathbb{Z})^{r-e}$ is a quotient of $\bar{V}/\bar{U}$. □

Proposition 2.2.7. Let p, q be primes and k a positive integer. Then $\mathbb{Q}$ has a sequence of linearly disjoint Galois extensions $L_1, L_2, \ldots$ in $\mathbb{Q}_{\mathrm{tot},p}$ with $\mathrm{Gal}(L_i/\mathbb{Q}) \cong \mathbb{Z}/q^k\mathbb{Z}$, for all i.

Proof. Let $l, l' \neq p$ be distinct prime numbers such that $l, l' \equiv 1 \mod q^k$ (Lemma 2.1.5). Then $\mathbb{Q}(\zeta_l)$ and $\mathbb{Q}(\zeta_{l'})$ are linearly disjoint cyclic extensions of $\mathbb{Q}$. Let L (respectively, L') be the unique subextension of $\mathbb{Q}(\zeta_l)$ (respectively, $\mathbb{Q}(\zeta_{l'})$) such that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/q^k\mathbb{Z}$ (respectively, $\mathrm{Gal}(L'/\mathbb{Q}) \cong \mathbb{Z}/q^k\mathbb{Z}$). Then L and L' are linearly disjoint over $\mathbb{Q}$, so $N = LL'$ is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/q^k\mathbb{Z} \oplus \mathbb{Z}/q^k\mathbb{Z}$.

Since $p \neq l, l'$, it is unramified in both $\mathbb{Q}(\zeta_l)$ and $\mathbb{Q}(\zeta_{l'})$, so p is also unramified in N. Then, the fixed field N_0 of the Frobenius φ at p is a Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_p$ with Galois group $\mathrm{Gal}(N_0/\mathbb{Q}) \cong \mathrm{Gal}(N/\mathbb{Q})/\langle\varphi\rangle$ isomorphic to the quotient of $\mathbb{Z}/q^k\mathbb{Z} \oplus \mathbb{Z}/q^k\mathbb{Z}$ by a cyclic group. By Lemma 2.2.6, $\mathbb{Z}/q^k\mathbb{Z}$ is a quotient of $\mathrm{Gal}(N/\mathbb{Q})/\langle\varphi\rangle$. It follows that $\mathbb{Q}$ has Galois extension L in N_0 with $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/q^k\mathbb{Z}$. Since $N_0 \subseteq \mathbb{Q}_p$, $L \subseteq \mathbb{Q}_p$.

Now consider a sequence of disjoint pairs of distinct primes $(l_1, l_1'), (l_2, l_2'), \ldots$ such that $l_i, l_i' \neq p$ and $l_i, l_i' \equiv 1 \mod q^k$ (Lemma 2.1.5). For each i, construct a field L_i as the field L above. Then $L_1, L_2, \ldots$ are linearly disjoint Galois extensions of $\mathbb{Q}$ in $\mathbb{Q}_p$ with $\mathrm{Gal}(L_i/\mathbb{Q}) \cong \mathbb{Z}/q^k\mathbb{Z}$, for all i. □

We give an alternative proof to Proposition 2.2.7 which handles the case of an arbitrary cyclic extension. The proof is based on the following lemma and on a mild case of the Chebotarev's Density Theorem (Lemma 2.1.6).

Lemma 2.2.8. Let n and a be positive integers and let l be a prime number such that $l \nmid na$. Then the following statements are equivalent:

(1) l totally splits in $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$.

(2) n divides $\dfrac{l-1}{\mathrm{ord}_l(a)}$.

Proof. Assume l totally splits in $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$. Let w be an extension of the l-adic valuation v_l to $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$. Then, $\overline{\mathbb{Q}(\zeta_n, \sqrt[n]{a})}_w = \mathbb{F}_l$ (Definition 1.4.1). Hence $\zeta_n \in \mathbb{F}_l$ and there exists $b \in \mathbb{Z}$ with $a \equiv b^n \mod l$. Thus $l \equiv 1 \mod n$. Furthermore, $a^{\frac{l-1}{n}} \equiv b^{l-1} \equiv 1 \mod l$. Therefore, $\mathrm{ord}_l(a) | \frac{l-1}{n}$.

Now, assume $n | \frac{l-1}{\mathrm{ord}_l(a)}$. On one hand, $l \equiv 1 \mod n$, hence $\zeta_n \in \mathbb{F}_l$. Then the reduction modulo l of the n-th cyclotomic polynomial has exactly $\varphi(n)$ distinct roots in $\mathbb{F}_l$. Hence, by Lemma 1.4.3, v_l totally splits in $\mathbb{Q}(\zeta_n)$. On the other hand, $\mathrm{ord}_l(a) | \frac{l-1}{n}$, so $a^{\frac{l-1}{n}} \equiv 1 \mod l$. We choose $\beta \in \tilde{\mathbb{F}}_l$ such that $\beta = \bar{a}^{\frac{1}{n}}$. Then , $\beta^{l-1} = \bar{a}^{\frac{l-1}{n}} = 1$, so $\beta^l = \beta$. Hence $\beta \in \mathbb{F}_l$ and therefore $\bar{a}^{1/n} \in \mathbb{F}_l$. Hence $X^n - \bar{a}$ has exactly n distinct roots in $\mathbb{F}_l$ namely $\bar{a}^{\frac{1}{n}}, \zeta_n \bar{a}^{\frac{1}{n}}, \ldots, \zeta_n^{n-1} \bar{a}^{\frac{1}{n}}$. Again, by Lemma 1.4.3, v_l totally splits in $\mathbb{Q}(\sqrt[n]{a})$. Therefore, by Lemma 1.4.5, v_l totally splits in $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$, as claimed. □

Proposition 2.2.9. Given a positive integer n and a prime number p, there exists a sequence $l_1, l_2, \ldots$ of distinct prime numbers and for each i there exists a subextension L_i of $\mathbb{Q}(\zeta_{l_i}) \cap \mathbb{Q}_p$ such that $\mathrm{Gal}(L_i/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$.

Proof. We use Lemma 2.1.6 and Remark 2.1.7 to choose a sequence $l_1, l_2, \ldots \neq p$ of prime numbers that totally split in $\mathbb{Q}(\zeta_n, \sqrt[n]{p})$. Then we fix an i and set $l = l_i$. We also choose a valuation w of $\mathbb{Q}(\zeta_l)$ lying over v_p and use bar to denote reduction modulo M_w. Since $l \neq p$, p is unramified in $\mathbb{Q}(\zeta_l)$ (Lemma 1.2.12). Moreover, $\mathbb{Q}(\zeta_l)$ is a cyclic extension of $\mathbb{Q}$ of degree $l-1$. We denote the fixed field of the Frobenius of w/v_p in $\mathbb{Q}(\zeta_l)$ by F_i. By Lemma 1.3.6, $F_i \subseteq \mathbb{Q}_p$. Since the ring of integers of $\mathbb{Q}(\zeta_l)$ is $\mathbb{Z}[\zeta_l]$ (p. 88 of [C-F]), the residue field of $\mathbb{Q}(\zeta_l)$ at w is $\mathbb{F}_p(\zeta_l)$. Hence, by Proposition 1.3.10 and Lemma 2.1.1, $[\mathbb{Q}(\zeta_l) : F_i] = [\mathbb{F}_p(\zeta_l) : \mathbb{F}_p] = \mathrm{ord}_l p$, so F_i is a cyclic extension

of degree $\frac{l-1}{\mathrm{ord}_l p}$.

By the choice of l and Lemma 2.2.8, $l \equiv 1 \mod n$ and $n|\frac{l-1}{\mathrm{ord}_l p}$. Consequently, $\mathbb{Q}$ has a cyclic extension L_i of degree n which is contained in F_i, hence also in $\mathbb{Q}_p$, as desired. $\square$

2.3 Abelian Extensions of $\mathbb{Q}$ in $\mathbb{Q}_{\mathbf{tot},p}$

This section contains the main result of the Chapter. Given a finite abelian group G and a prime p, there is a Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$ with Galois group G.

Lemma 2.3.1. Let p, q be primes, k an integer, and $N/\mathbb{Q}$ a finite separable extension. There exists a Galois extension $L/\mathbb{Q}$ in $\mathbb{Q}_p$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/q^k\mathbb{Z}$ and L is linearly disjoint from N over $\mathbb{Q}$.

Proof. By Lemma 2.2.9, there is a sequence of linearly disjoint Galois extensions $L_1, L_2, \ldots$ of $\mathbb{Q}$ in $\mathbb{Q}_p$ such that $\mathrm{Gal}(L_i/\mathbb{Q}) \cong \mathbb{Z}/q^k\mathbb{Z}$ for every i. Assume for all i, N and L_i are not linearly disjoint over $\mathbb{Q}$. Since the L_i's are Galois, $L_i \cap N = N_i \neq \mathbb{Q}$. Moreover since $L_i \cap L_j = \mathbb{Q}$, for $i \neq j$, we have $N_i \neq N_j$. It follows that N has infinitely many subextensions which is a contradiction. Hence, there exists i such that N is linearly disjoint from L_i over $\mathbb{Q}$. $\square$

We prove our main result by using the decomposition of finite abelian groups into a direct product of cyclic groups.

Theorem 2.3.2. *Let p be a prime number and A a finite abelian group. Then $\mathbb{Q}$ has a Galois extension L in $\mathbb{Q}_{tot,p}$ with $Gal(L/\mathbb{Q}) \cong A$.*

Proof. Let $A = \prod_{i=1}^{n} \mathbb{Z}/q_i^{k_i}\mathbb{Z}$ be the decomposition of A into a direct product of cyclic groups whose orders are prime powers

First method: By Lemma 2.2.7, there exists a cyclic extension $L_1/\mathbb{Q}$ in $\mathbb{Q}_p$ with Galois group $\mathbb{Z}/q_1^{k_1}\mathbb{Z}$. By Lemma 2.3.1, there exists a cyclic extension $L_2/\mathbb{Q}$ in $\mathbb{Q}_p$ such that $\mathrm{Gal}(L_2/\mathbb{Q}) \cong \mathbb{Z}/q_2^{k_2}\mathbb{Z}$ and L_1 is linearly disjoint from L_2. Repeating the latter step, we construct linearly disjoint cyclic extensions $L_1, L_2, \ldots, L_n$ of $\mathbb{Q}$ in $\mathbb{Q}_p$ such that $\mathrm{Gal}(L_i/\mathbb{Q}) \cong \mathbb{Z}/q_i^{k_i}\mathbb{Z}$, for $1 \leq i \leq n$. Then, $L = L_1L_2, \cdots L_n \subseteq \mathbb{Q}_p$ is a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong \prod_{i=1}^{n} \mathbb{Z}/q_i^{k_i}\mathbb{Z} \cong A$.

Second method: Applying induction on n and using Proposition 2.2.9, we find distinct prime numbers $l_1, l_2, \ldots, l_n$ such that for each i, the field $\mathbb{Q}(\zeta_{l_i})$ contains a cyclic extension L_i of $\mathbb{Q}$ in $\mathbb{Q}_p$ with Galois group $\mathbb{Z}/q_i^{k_i}\mathbb{Z}$. Since the l_i's are distinct, the $\mathbb{Q}(\zeta_{l_i})$ are linearly disjoint over $\mathbb{Q}$, hence so are the L_i's. Therefore, $L = L_1L_2 \cdots L_n$ is a Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_p$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong \prod_{i=1}^{n} \mathbb{Z}/q_i^{k_i}\mathbb{Z} \cong G$. $\square$

Chapter 3

Galois extensions of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},\boldsymbol{p}}$ with Galois Group a Semi-direct Product of Groups

Assuming that a finite group G is realizable over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$ and is acting on a finite dimensional vector space A over $\mathbb{F}_2$, we construct in this chapter a Galois extension $L/\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong A \rtimes G$. As an example, we realize A_4 over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$.

3.1 Semi-direct Products

In this section, we introduce semi-direct products in several alternative forms.

Let H and N be groups. Suppose H acts on N from the left by the map

$$\begin{array}{rcl} N \times H: & \longrightarrow & N \\ (n,h) & \longmapsto & hn \end{array}$$

Lemma 3.1.1. The multiplication rule $(n,h)(n',h') = (n \cdot hn', hh')$ defines a group structure on $N \times H$.

Proof. The identity element of the group is $(1,1)$. Let $(n_1,h_1),(n_2,h_2),(n_3,h_3) \in N \times H$. Then,

$$\begin{aligned}(n_1,h_1)\Big((n_2,h_2)(n_3,h_3)\Big) &= (n_1,h_1)(n_2 \cdot h_2n_3, h_2h_3)\\ &= (n_1 \cdot h_1n_2 \cdot h_1h_2n_3, h_1h_2h_3)\\ &= (n_1 \cdot h_1n_2, h_1h_2)(n_3,h_3)\\ &= \Big((n_1,h_1)(n_2,h_2)\Big)(n_3,h_3).\end{aligned}$$

Hence, the operation defined above is associative. Furthermore, for every $(n,h) \in N \times H$,

$$(n,h)(h^{-1}n^{-1},h^{-1}) = (n \cdot hh^{-1}n^{-1}, hh^{-1}) = (1,1).$$

Therefore, every element of $N \times H$ has an inverse. □

Definition 3.1.2. We denote the cartesian product $N \times H$ with the group structure defined in Lemma 3.1.1 by $N \rtimes H$ and call it the **semi-direct product** of N and H.

Remark 3.1.3. The identification of each element $h \in H$ with the pair $(1,h)$ and each element $n \in N$ with the pair $(n,1)$ embeds H and N in $N \rtimes H$ such that N is a normal subgroup of $N \rtimes H$, $H \cap N = 1$, and $NH = N \rtimes H$.

Lemma 3.1.4. Let G be a group, N a normal subgroup of G, and H a subgroup of G such that $H \cap N = 1$. Let H act on N by conjugation from the left $(n,h) \longmapsto nhn^{-1}$. Then $N \rtimes H \cong NH$.

Proof. Consider the map $\psi\colon N \rtimes H \longrightarrow NH$ given by $(n,h) \longmapsto nh$. Then,

$$\begin{aligned}\psi((n_1,h_1)(n_2,h_2)) &= \psi(n_1h_1n_2h_1^{-1}, h_1h_2) = n_1h_1n_2h_1^{-1}h_1h_2\\ &= n_1h_1n_2h_2 = \psi(n_1,h_1)\psi(n_2,h_2).\end{aligned}$$

Hence, ψ is an epimorphism. Furthermore, if $(n,h) \in \mathrm{Ker}(\psi)$, then $nh = 1$. Hence $h = n^{-1}$, and $h \in N$. Since $H \cap N = 1$, $h = 1$. It follows that $n = 1$. Thus $(h,n) = (1,1)$, so ψ is injective. Therefore, ψ is an isomorphism. □

Definition 3.1.5. A short exact sequence

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\alpha} H \longrightarrow 1 \tag{3.1.1}$$

of groups **splits** if there exists a homomorphism $\alpha'\colon H \longrightarrow G$ satisfying $\alpha(\alpha'(h)) = h$ for each $h \in H$. We call α' a **section** of α.

Lemma 3.1.6. Suppose the short exact sequence (3.1.1) splits and let α' be a section of α. Then $G = \mathrm{Ker}(\alpha) \rtimes \mathrm{Im}(\alpha')$.

Proof. Let $g \in \mathrm{Ker}(\alpha) \cap \mathrm{Im}(\alpha')$. Then, $\alpha(g) = 1$ and there exists $h \in H$ such that $\alpha'(h) = g$. Hence $h = \alpha(\alpha'(h)) = \alpha(g) = 1$, so $g = \alpha'(1) = 1$. It follows that $\mathrm{Ker}(\alpha) \cap \mathrm{Im}(\alpha') = 1$. Moreover, for every $g \in G$ we have $\alpha(g) \in H$ and $\alpha\big(\alpha'(\alpha(g))\big) = \alpha(g)$. Thus, $z = \alpha'\alpha(g) \in \mathrm{Im}(\alpha')$ and $\alpha(z) = \alpha(g)$. Hence, $1 = \alpha(g)(\alpha(z))^{-1} = \alpha(gz^{-1})$, so $gz^{-1} \in \mathrm{Ker}(\alpha)$. Since $g = (gz^{-1})z$, we have $g \in \mathrm{Ker}(\alpha)\mathrm{Im}(\alpha')$. Therefore, $G = \mathrm{Ker}(\alpha)\mathrm{Im}(\alpha')$. By Lemma 3.1.4, $G = \mathrm{Ker}(\alpha) \rtimes \mathrm{Im}(\alpha')$. □

Lemma 3.1.7. Let H, N and H', N' be groups such that H acts on N from the left and H' acts on N' from the left. Let $\alpha\colon N \longrightarrow N'$ and $\gamma\colon H \longrightarrow H'$ be homomorphisms that satisfy $\alpha(hn) = \gamma(h)\alpha(n)$ for all $n \in N$ and $h \in H$. Then there exists a unique homomorphism $\beta\colon N \rtimes H \longrightarrow N' \rtimes H'$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & N \rtimes H & \longrightarrow & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & N' & \longrightarrow & N' \rtimes H' & \longrightarrow & H' & \longrightarrow & 1 \end{array} \tag{3.1.2}$$

If α and γ are surjective, then so is β. If α and γ are injective, then so is β. Finally, if α and γ are isomorphisms, then so is β.

Proof. Consider the map $\beta\colon N \rtimes H \longrightarrow N' \rtimes H'$ defined by $\beta(nh) = \alpha(n)\gamma(h)$. With this definition one checks that the diagram 3.1.2 commutes.

Let $n_1h_1, n_2h_2 \in N \rtimes H$, then

$$\begin{aligned}\beta(n_1h_1n_2h_2) &= \beta(n_1h_1n_2h_1^{-1}h_1h_2) = \beta(n_1(h_1n_2)h_1h_2)\\ &= \alpha(n_1(h_1n_2))\gamma(h_1h_2) = \alpha(n_1)\alpha(h_1n_2)\gamma(h_1)\gamma(h_2)\\ &= \alpha(n_1)(\gamma(h_1)\alpha(n_2))\gamma(h_1)\gamma(h_2)\\ &= \alpha(n_1)\gamma(h_1)\alpha(n_2)\gamma(h_1)^{-1}\gamma(h_1)\gamma(h_2)\\ &= \alpha(n_1)\gamma(h_1)\alpha(n_2)\gamma(h_2) = \beta(n_1h_1)\beta(n_2h_2).\end{aligned}$$

Hence, β is a homomorphism. Furthermore, if α and β are surjective (resp. injective, isomorphism), then β is also surjective (resp. injective, isomorphism). By the definition of β and the commutativity of (3.1.2), β is unique. □

Proposition 3.1.8. Let K, E, F, L be fields such that L/K and E/K are Galois, $L = EF$, and $E \cap F = K$. Then $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/E) \rtimes \mathrm{Gal}(L/F)$.

Proof. $L = EF$ implies that $\mathrm{Gal}(L/E) \cap \mathrm{Gal}(L/F) = 1$. Moreover $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/E \cap F) = \langle \mathrm{Gal}(L/E), \mathrm{Gal}(L/F) \rangle$ (p. 263, Cor. 1.4 of [La2]). Then, $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/E)\mathrm{Gal}(L/F)$, since $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/K)$. By Lemma 3.1.4, we have $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/E) \rtimes \mathrm{Gal}(L/F)$. □

3.2 Abelian Kummer Theory

In this section, we give a brief description of Abelian Kummer theory. For more details, the reader may refer to Section 6.8 of [La2].

Let K be a field and n a positive integer such that $\mathrm{char}(K) \nmid n$. A Galois extension L/K is said to be of **exponent** n if $\sigma^n = 1$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Suppose the group μ_n of n-th roots of unity is contained in K. Let $a \in K$ and let $\alpha \in \tilde{K}$ such that $\alpha^n = a$. Then for all $\zeta \in \mu_n$, we have $(\zeta\alpha)^n = a$. We denote by $\sqrt[n]{a}$ any such α and call it the **n-th root** of a. Since $\mu_n \subset K$,

$K(\alpha)$ does not depend on the choice of the n-th root α of a.

Let $(K^\times)^n$ be the subgroup of $K^\times$ consisting of all n-th powers of nonzero elements of K and let G be a subgroup of $K^\times$ containing $(K^\times)^n$. Define $K(G^{1/n})$ to be the compositum of all fields $K(\sqrt[n]{a})$ with $a \in G$. Then $K(G^{1/n})$ is a Galois extension of K of exponent n.

Let $a \in G$ and $\alpha \in \tilde{K}$ with $\alpha^n = a$. If $\sigma \in \mathrm{Gal}(K(G^{1/n})/K)$, then there exists $\zeta_{\sigma,a} \in \mu_n$ such that $\sigma\alpha = \zeta_{\sigma,a}\alpha$ and the map $\sigma \longmapsto \zeta_{\sigma,a}$ is a homomorphism of $\mathrm{Gal}(K(G^{1/n})/K)$ into μ_n. Moreover, $\zeta_{\sigma,a}$ does not depend on the n-th root α of a. Then we have a bilinear map $\mathrm{Gal}(K(G^{1/n})/K) \times G \longrightarrow \mu_n$ given by $(\sigma, a) \longmapsto \zeta_{\sigma,a}$ such that the kernel on the left is 1 and the kernel on the right is $(K^\times)^n$. Therefore, using the duality theorem (Thm. 9.2, p. 49 of [La2]), $K(G^{1/n})/K$ is finite if and only if $(G : (K^\times)^n)$ is finite. In this case, $\mathrm{Gal}(K(G^{1/n})/K) \cong G/(K^\times)^n$, in particular $[K(G^{1/n}) : K] = (G : (K^\times)^n)$.

Proposition 3.2.1. (Thm. 8.2, p. 295 of [La2]) Using the above notation, the map $G \longmapsto K(G^{1/n})$ is a bijection of the set of subgroups of $K^\times$ containing $(K^\times)^n$ and the abelian extensions of K of exponent n.

Remark 3.2.2. We have replaced the condition $\gcd(n, \mathrm{char}(K)) = 1$ of Section 6.8 of [La2] by $\mathrm{char}(K) \nmid n$. Indeed, if $\mathrm{char}(K)$ is a prime number p, then the above condition is equivalent to $p \nmid n$. However, if $\mathrm{Char}(K) = 0$, then $\gcd(n, \mathrm{Char}(K))$ is not defined (see section 2.5 of [La2]). Nevertheless, $0 \nmid n$ and Kummer Theory still works in this case.

3.3 On the Chinese Remainder Theorem for Dedekind Domains

In this section, we prove a sharp form of the Chinese Remainder Theorem for Dedekind domains.

Let R be a Dedekind domain with quotient field K and let $\mathfrak{p}$ be a prime ideal of R. Let $R_\mathfrak{p}$ be the local ring of R at $\mathfrak{p}$. Then, there exists $\pi \in R_\mathfrak{p}$ such that $\mathfrak{p}R_\mathfrak{p} = \pi R_\mathfrak{p}$ and for all $x \in K^\times$, $x = u\pi^k$ for some unit u of $R_\mathfrak{p}$ and $k \in \mathbb{Z}$. The map from K defined by $v_\mathfrak{p}(x) = k$ is a discrete valuation of K whose valuation ring is $R_\mathfrak{p}$.

Let $L/\mathbb{Q}$ be a finite extension of fields and p a prime number. Let $\mathcal{O}_L$ be the ring of integers of L and $\mathfrak{q}$ a prime ideal of $\mathcal{O}_L$ lying over p. Let e be the ramification index of $\mathfrak{p}$ over p. Then, $v_\mathfrak{p}(x) = ev_p(x)$ for each $x \in \mathbb{Q}$.

Proposition 3.3.1. Let R be a Dedekind domain with quotient field K. Let $\mathcal{M}$ be a finite set of maximal ideals of R. For each $\mathfrak{p} \in \mathcal{M}$ let $a_\mathfrak{p} \in R$ and $e_\mathfrak{p} \in \{0\} \cup \mathbb{N}$. Then there exists $x \in R$ such that $v_\mathfrak{p}(x - a_\mathfrak{p}) = e_\mathfrak{p}$ for all $\mathfrak{p} \in \mathcal{M}$.

Proof. Let $\mathfrak{p} \in \mathcal{M}$ and let $\pi \in R$ with $v_\mathfrak{p}(\pi_\mathfrak{p}) = 1$.

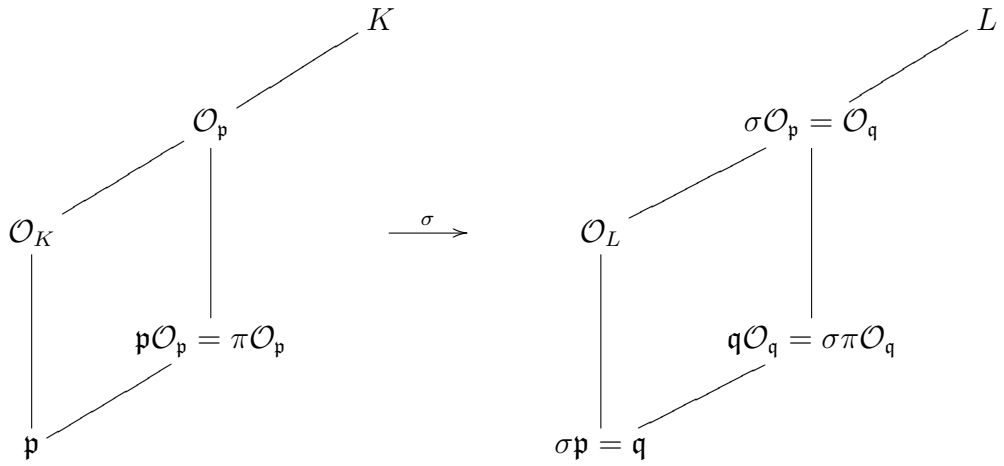
By the Chinese Remainder Theorem, there exists $y \in R$ such that $v_\mathfrak{p}(y - a_\mathfrak{p}) \geq e_\mathfrak{p} + 1$ for each $\mathfrak{p} \in \mathcal{M}$. Another use of this theorem gives $x \in R$ such that $v_\mathfrak{p}(x - \pi_\mathfrak{p}^{e_\mathfrak{p}} - y) \geq e_\mathfrak{p} + 1$ for each $\mathfrak{p} \in \mathcal{M}$. It follows from the identity

$$x - a_\mathfrak{p} = (x - \pi_\mathfrak{p}^{e_\mathfrak{p}} - y) + \pi_\mathfrak{p}^{e_\mathfrak{p}} + (y - a_\mathfrak{p})$$

and from the fact that $v_\mathfrak{p}(\pi_\mathfrak{p}^{e_\mathfrak{p}}) = e_\mathfrak{p} < \min\left(v_\mathfrak{p}(x - \pi_\mathfrak{p}^{e_\mathfrak{p}} - y), v_\mathfrak{p}(y - a_\mathfrak{p})\right)$ that $v_\mathfrak{p}(x - a_\mathfrak{p}) = e_\mathfrak{p}$ for each $\mathfrak{p} \in \mathcal{M}$, as desired. □

Remark 3.3.2. Let K and L be number fields and let $\sigma\colon K \longrightarrow L$ be an isomorphism. Then $\mathcal{O}_L = \sigma\mathcal{O}_K$. If $\mathfrak{p}$ is prime ideal of $\mathcal{O}_K$, then $\mathfrak{q} = \sigma\mathfrak{p}$ is a prime ideal of $\mathcal{O}_L$. Denote the localisation of $\mathcal{O}_K$ at $\mathfrak{p}$ by $\mathcal{O}_\mathfrak{p}$ and the localisation of $\mathcal{O}_L$ at $\mathfrak{q}$ by $\mathcal{O}_\mathfrak{q}$. Then, $\mathcal{O}_\mathfrak{q} = \sigma\mathcal{O}_\mathfrak{p}$ and $\mathfrak{q}\mathcal{O}_\mathfrak{q} = \sigma\mathfrak{p}\mathcal{O}_\mathfrak{p}$. If $\pi \in \mathcal{O}_\mathfrak{p}$

satisfies $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \pi\mathcal{O}_\mathfrak{p}$, then $\mathfrak{q}\mathcal{O}_\mathfrak{q} = \sigma\pi\mathcal{O}_\mathfrak{q}$.



In particular, $v_{\mathfrak{p}'}(\sigma x) = v_\mathfrak{p}(x)$. Indeed, let $x \in K$ with $v_\mathfrak{p}(x) = k$, that is $x = u\pi^k$ with $v_\mathfrak{p}(u) = 0$. Then, $v_{\mathfrak{p}'}(\sigma(x)) = v_{\mathfrak{p}'}(\sigma u)+kv_{\mathfrak{p}'}(\sigma\pi) = 0+k = v_\mathfrak{p}(x)$.

3.4 Realization of $A \rtimes G$

Let G be a finite group and p a prime number. Suppose G is realizable over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$. Let A be a finite dimensional vector space over $\mathbb{F}_2$ on which G is acting from the left. The aim of this section is to realize $A \rtimes G$ over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$. We first recall what is a group ring and state some important remarks.

Group Ring

(a) Let R be a ring and G a finite group. We denote by $R[G]$ the group ring of G over R. Each element of $R[G]$ has a unique representation as a formal sum $\sum_{\sigma\in G} a_\sigma\sigma$, with $a_\sigma \in R$. Addition is defined in $R[G]$ by adding the coefficients and multiplication is given by the formula

$$\sum_{\sigma\in G} a_\sigma\sigma \cdot \sum_{\tau\in G} b_\tau\tau = \sum_{\rho\in G}(\sum_{\sigma\tau=\rho} a_\sigma b_\tau)\rho.$$

The group G naturally embeds in $R[G]$ by $\sigma \longmapsto \sum_{\tau\in G} a_\tau\tau$ where $a_\tau = 1$ if $\tau = \sigma$ and $a_\tau = 0$ otherwise. In particular, G naturally acts

on $R[G]$ by multiplication from the left.

Note that in general the ring $R[G]$ is non-commutative. This is in particular the case if G is a non-abelian group. Nevertheless, whenever we speak about "an $R[G]$-module", we mean "a left $R[G]$-module".

(b) Suppose G is acting from the left on a free R-module A of rank r. Then, one may also consider A as $R[G]$-module. Let $a_1, \ldots, a_r$ be generators of A as an $R[G]$-module. Then $A = \sum_{i=1}^{r} R[G]a_i$ and G acts on A by multiplication from the left. Let B be the free $R[G]$-module of rank r with free generators $b_1, \ldots, b_r$. Thus, each $b \in B$ has a unique presentation as a sum $b = \sum_{i=1}^{r} c_i b_i$, with $c_1, \ldots, c_r \in R[G]$. In other words, we have $B = \bigoplus_{i=1}^{r} R[G]b_i$. The map $b_i \longmapsto a_i, i = 1, \ldots, r$ uniquely extends to an epimorphism φ: $B \longrightarrow A$ of $R[G]$-modules. Hence, by Lemma 3.1.7, φ induces an epimorphism of groups ψ: $B \rtimes G \longrightarrow A \rtimes G$ making the diagram corresponding to (3.1.2) commutative.

Remark 3.4.1. (a) Let K and L be fields and τ: $K \longrightarrow L$ an isomorphism. Let $f \in K[X]$ be an irreducible polynomial and x a root of f in $\tilde{K}$. Set $g = \tau f$ and let y be a root of g in $\tilde{L}$. Then, g is irreducible in $L[X]$ and τ extends to an isomorphism τ': $K(x) \longrightarrow L(y)$ such that $\tau'(x) = y$.

(b) Let $K_1, \ldots, K_n$ be linearly disjoint extensions of K in $\tilde{K}$ and let $L_1, \ldots, L_n$ be linearly disjoint extensions of L in $\tilde{L}$. For each $1 \leq i \leq n$ let τ_i: $K_i \longrightarrow L_i$ be an isomorphism extending τ (of (a)). Set $M = K_1 \cdots K_n$ and $N = L_1 \cdots N_n$. Then, there exists an isomorphism τ': $M \longrightarrow N$ whose restriction to each K_i coincides with τ_i (Lemma 2.5.11 of [F-J]).

(c) Let K/K_0 be a Galois extension with Galois group G, let $\mathcal{F}$ be a family of separable polynomials with coefficients in K, and let N be the

splitting field of $\mathcal{F}$ over K. Suppose that G permutes the polynomials in $\mathcal{F}$. Then N is a Galois extension of K_0.

Lemma 3.4.2. Let K/K_0 be a finite Galois extension with Galois group G of order m. Let n be a positive integer such that $\mathrm{char}(K) \nmid n$ and $\zeta_n \in K$. Let $x_1, \ldots, x_r$ be elements of $K^\times$ such that the mr elements σx_i, with $\sigma \in G$ and $1 \leq i \leq r$ are multiplicatively independent modulo $(K^\times)^n$.

Then $N = K(\sqrt[n]{\sigma x_i} \mid \sigma \in G,\ 1 \leq i \leq r)$ is a Galois extension of K_0 and there is a commutative diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(N/K) & \longrightarrow & \mathrm{Gal}(N/K_0) & \longrightarrow & \mathrm{Gal}(K/K_0) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & B & \longrightarrow & B \rtimes G & \longrightarrow & G & \longrightarrow & 1 \end{array} \tag{3.4.1}$$

where B is a free $(\mathbb{Z}/n\mathbb{Z})[G]$-module of rank r on which G acts from the left and the vertical arrows are isomorphisms.

Proof. By assumption, for all $\sigma \in G$ and $1 \leq i \leq r$ the order of σx_i modulo $(K^\times)^n$ is n. In addition, $\mathrm{char}(K) \nmid n$. Hence, $X^n - \sigma x_i$ is a separable irreducible polynomial of degree n. We fix a root $\sqrt[n]{\sigma x_i}$ of $X^n - \sigma x_i$ in $\tilde{K}$. Since $\mu_n \subseteq K$, $K(\sqrt[n]{\sigma x_i})/K$ is a cyclic extension of order n.

By assumption, $\langle (K^\times)^n, \sigma x_i \mid \sigma \in G \rangle / (K^\times)^n \cong (\mathbb{Z}/n\mathbb{Z})^m$. Hence, $N = K(\sqrt[n]{\sigma x_i} \mid \sigma \in G,\ 1 \leq i \leq r)$ is a Galois extension of K with Galois group $(\mathbb{Z}/n\mathbb{Z})^{mr}$. It follows that the fields $K(\sqrt[n]{\sigma x_i})$ with $\sigma \in G$ and $1 \leq i \leq r$ are linearly disjoint over K. In particular, each of the fields $N_i = K(\sqrt[n]{\sigma x_i} \mid \sigma \in G)$ is a Galois extension of K with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^m$, $N_1, \ldots, N_n$ are linearly disjoint over K, and $N = N_1 \cdots N_r$. Thus $\mathrm{Gal}(N/K) \cong \prod_{i=1}^r \mathrm{Gal}(N_i/K)$.

Next note that N_i is the splitting field over K of the family $\{X^n - \sigma x_i \mid \sigma \in G\}$ and G permutes that family. Hence, by Remark 3.4.1, N_i is also a Galois extension of K_0. Therefore , N is also a Galois extension of K_0.

Again, by Remark 3.4.1, each $\tau \in G$ uniquely extends to an automorphism $\tau' \in \mathrm{Gal}(N/K_0)$ such that $\tau' \sqrt[n]{\sigma x_i} = \sqrt[n]{\tau\sigma x_i}$. The uniqueness implies that $(\tau_1\tau_2)' = \tau_1'\tau_2'$ for all $\tau_1, \tau_2 \in G$. Hence, the map $\tau \longrightarrow \tau'$ is a section of the restriction map $\mathrm{Gal}(N/K_0) \longrightarrow G$.

Finally, observe that $(\mathbb{Z}/n\mathbb{Z})^m$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})[G]$ and $(\mathbb{Z}/n\mathbb{Z})^{mr}$ is isomorphic to B as groups. Moreover, the action of G on $\mathrm{Gal}(N/K)$, defined in the preceding paragraph, is compatible with the action of G from the left on B. This establishes the commutative diagram (3.4.1). □

Theorem 3.4.3. *Let G be a finite group acting on a vector space A over $\mathbb{F}_2$ of dimension r and let p be a prime number. If G is realizable over $\mathbb{Q}$ in $\mathbb{Q}_{tot,p}$, then so is $A \rtimes G$.*

Proof. Let B be the free $\mathbb{F}_2[G]$-module of rank r. By Subsection 3.4 (b), $A \rtimes G$ is a quotient of $B \rtimes G$.

Let K be a Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$ with Galois group G. Thus, p totally splits in K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p. Then, $\sigma\mathfrak{p}$ with $\sigma \in G$, are the distinct prime ideals of $\mathcal{O}_K$ lying over p.

We choose r distinct prime numbers $q_1, q_2, \ldots, q_r$, different from p which totally split in K. For $1 \leq i \leq r$, let $\mathfrak{q}_i$ be a prime ideal of $\mathcal{O}_K$ lying over q_i. Then, $\sigma\mathfrak{q}_i$, with $\sigma \in G$ are the distinct prime ideals of $\mathcal{O}_K$ lying over q_i.

Next we use the Proposition 3.3.1 to find $x_1, x_2, \ldots, x_r \in \mathcal{O}_K$ such that, for $1 \leq i \leq r$

$$v_{\sigma\mathfrak{p}}(x_i - 1) \geq 3 \text{ for } 1 \leq i \leq r \text{ and } \sigma \in G. \tag{3.4.2}$$

$$v_{\mathfrak{q}_i}(x_i) = 1 \text{ for } 1 \leq i \leq r. \tag{3.4.3}$$

$$v_{\sigma\mathfrak{q}_i}(x_j) = 0 \text{ for } i \neq j \text{ or } \sigma \in G \setminus \{1\} \tag{3.4.4}$$

Let $\tau \in G$. Using Remark 3.3.2, and applying (3.4.2) on $\tau^{-1}\sigma$ rather than on σ, we get

$$v_{\sigma\mathfrak{p}}(\tau x_i - 1) = v_{\tau^{-1}\sigma\mathfrak{p}}(x_i - 1) \geq 3 \text{ for } 1 \leq i \leq r \text{ and } \sigma \in G. \tag{3.4.5}$$

Using the same argument on (3.4.3) and (3.4.4), we get

$$v_{\tau\mathfrak{q}_i}(\tau x_i) = 1 \text{ for } 1 \leq i \leq r, \tag{3.4.6}$$

$$v_{\sigma\mathfrak{q}_i}(\tau x_j) = 0 \text{ for } i \neq j \text{ or } \tau \neq \sigma. \tag{3.4.7}$$

Suppose there exist $\alpha_{\sigma,i} \in \{0, 1\}$ for $\sigma \in G$, $1 \leq i \leq r$, and $u \in K$ such that

$$\prod_{\sigma,i} (\sigma x_i)^{\alpha_{\sigma,i}} = u^2. \tag{3.4.8}$$

If there exist τ and l with $\alpha_{\tau,l} = 1$, then applying $v_{\tau\mathfrak{q}_l}$ to both sides of (3.4.8), we get

$$\sum_{\sigma,i} \alpha_{\sigma,i} v_{\tau\mathfrak{q}_l}(\sigma x_i) = 2v_{\tau\mathfrak{q}_l}(u).$$

Since $v_{\tau\mathfrak{q}_l}(\sigma x_i) = 0$ for $(\sigma, i) \neq (\tau, l)$ by (3.4.7) and $v_{\tau\mathfrak{q}_l}(\tau x_l) = 1$ by (3.4.6), we have $1 = 2v_{\tau\mathfrak{q}_l}(u)$, which is a contradiction. Therefore, the σx_i's are multiplicatively independent modulo $(K^\times)^2$. It follows from Lemma 3.4.2 that $N = K(\sqrt{\sigma x_i}, \mid \sigma \in G,\ 1 \leq i \leq r)$ is a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(N/\mathbb{Q}) \cong B \rtimes G$. Since $A \rtimes G$ is a quotient of $B \rtimes G$, N has a subfield L such that $L/\mathbb{Q}$ is Galois and $\mathrm{Gal}(L/\mathbb{Q}) \cong A \rtimes G$.

Finally, since $K \subseteq \mathbb{Q}_p$, Lemma 1.5.6 and (4) of Remark 1.5.5 imply that the $K_{\sigma\mathfrak{p}}$ are henselizations of $\mathbb{Q}$ at p. Therefore, $\mathbb{Q}_{\mathrm{tot},p} = \bigcap_{\sigma\in G} K_{\mathrm{tot},\sigma\mathfrak{p}}$. Moreover, for $\sigma \in G$ and $1 \leq i \leq r$, considering the polynomial $f_{\sigma,i}(X) = X^2 - \sigma x_i$, we get by (3.4.2) that $v_{\tau\mathfrak{p}}(f_{\sigma,i}(1)) \geq 3$ and $v_{\tau\mathfrak{p}}(f'_{\sigma,i}(1)) = v_{\tau\mathfrak{p}}(2)$ is either 0 or 1 for $\tau \in G$. Hence, by Hensel-Rychlick, $\{\sqrt{\sigma x_i}, \mid \sigma \in G,\ 1 \leq i \leq r\} \subseteq \bigcap_{\sigma\in G} K_{\mathrm{tot},\sigma\mathfrak{p}}$. Therefore, $N \subseteq \mathbb{Q}_{\mathrm{tot},p}$, so $L \subseteq \mathbb{Q}_{\mathrm{tot},p}$ as desired. □

3.5 Example: Realization of A_4

In this section, we realize the alternating group A_4 in $\mathbb{Q}_{\mathrm{tot},p}$, for a given prime number p.

Remark 3.5.1. Let $C_2 = \{1, \gamma\}$ be the multiplicative group of order 2, where γ is of order 2. Write $C_2 \times C_2$ as $\{1, \tau, \tau', \tau''\}$, where τ, τ', τ'' are of order 2. Let $C_3 = \langle\sigma\rangle$, where σ is of order 3. The group C_3 acts on $C_2 \times C_2$ by cyclically permuting τ, τ', τ''.

Lemma 3.5.2. The alternating group A_4 is isomorphic to $\big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\big) \rtimes C_3$.

Proof. The subgroup $K_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ is normal in A_4 and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The subgroup $H = \langle(123)\rangle$ is of order 3 and it cyclically permutes the three elements of K_4 of order 2. Since $|K_4|$ and $|H|$ are relatively prime, $K_4 \cap H = \{1\}$. Then, by Lemma 3.1.4, $HK_4 \cong K_4 \rtimes H$. Since $|K_4 \rtimes H| = 12$, $A_4 \cong K_4 \rtimes H \cong \big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\big) \rtimes C_3$. □

Since C_3 is realizable over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$, for every prime number p (Lemma 2.2.5), by Theorem 3.4.3, A_4 is realizable over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$.

Chapter 4

Symmetric Groups in $\mathbb{Q}_{\mathrm{tot},p}$

In this chapter, we construct a Galois extension L of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_n$ for each given positive integer n. To do that, we first establish some useful properties of the Galois group of a polynomial over the residue field of an integrally closed domain, in particular over a finite field. After that, we present the continuity of roots of separable polynomials from valuation theory.

4.1 Galois Groups over Residue Fields

We consider an integrally closed domain R with quotient field K and a prime ideal $\mathfrak{p}$ of R. If $f(X) \in R[X]$ is a monic polynomial, then under some conditions, the group $\mathrm{Gal}(\bar{f}, \mathrm{Quot}(R/\mathfrak{p}))$ is isomorphic to a subgroup of $\mathrm{Gal}(f, K)$. In this section, we are going to present these conditions.

Remark 4.1.1. Let R be an integrally closed domain with quotient field K. Let L/K be a finite Galois extension and S the integral closure of R in L. Then, for every $\sigma \in \mathrm{Gal}(L/K)$, $\sigma S = S$. Let $\mathfrak{p}$ be a prime ideal of R and $\mathfrak{q}$ a prime ideal of S lying over $\mathfrak{p}$. Recall that the decomposition group of $\mathfrak{q}$ over $\mathfrak{p}$ is $D_{\mathfrak{q}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma\mathfrak{q} = \mathfrak{q}\}$. Denote the quotient fields of $R/\mathfrak{p}$ and $S/\mathfrak{q}$ by $\bar{K}$ and $\bar{L}$ respectively. For $x \in S$, denote the equivalence class of x modulo $\mathfrak{q}$ by $\bar{x}$. To each $\sigma \in D_{\mathfrak{q}}$, we associate an automorphism $\bar{\sigma}$ of $\bar{L}$ over

$\bar{K}$ defined for $x \in S$ by $\bar{\sigma}\bar{x} = \overline{\sigma x}$.

(i) $\bar{L}/\bar{K}$ is a normal extension and the map $\sigma \longmapsto \bar{\sigma}$ is an epimorphism of $D_{\mathfrak{q}}$ onto $\mathrm{Aut}(\bar{L}/\bar{K})$ (Prop. 2.5, p. 342 of [La2]).

(ii) If $\bar{L}/\bar{K}$ is separable and $[\bar{L} : \bar{K}] = [L : K]$, then $\bar{L}/\bar{K}$ is Galois, $D_{\mathfrak{q}} = \mathrm{Gal}(L/K)$, and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\bar{L}/\bar{K})$ (Lem. 6.1.1 (b) of [F-J]).

Let f be a monic polynomial with coefficients in R. If $f(X) = \prod_{i=1}^{n}(X - x_i)$ is the factorization of f into linear factors, then the **discriminant** of f is

$$\mathrm{disc}(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(x_i - x_j).$$

This is an element of R and $\mathrm{disc}(f) \neq 0$ if and only if the x_i's are distinct (More detail are in Subsection 5.4).

The discriminant of f plays an important role in the determination of the integral closure of R in some extensions of K containing roots of f, as shown in the following lemmas.

Lemma 4.1.2. (Lemma 6.1.2 of [F-J]) Let R be an integrally closed domain with quotient field K. Let L/K be a finite separable extension and S the integral closure of R in L. Suppose $L = K(x)$ with $x \in S$. If $\mathrm{disc}(f)$ is a unit of R, then $S = R[x]$.

In the case where L is the splitting field of some polynomial over K, we can generalize this Lemma to the following.

Lemma 4.1.3. Let R be an integrally closed domain with quotient field K. Let $f \in R[X]$ be a monic irreducible polynomial of degree n. Suppose $\alpha_1, \ldots, \alpha_n$ are the roots of f in $\tilde{K}$. Denote the splitting field of f over K by $L = K(\alpha_1, \ldots, \alpha_n)$. If $\mathrm{disc}(f)$ is a unit of R, then $S = R[\alpha_1, \ldots, \alpha_n]$ is the integral closure of R in L.

Proof. Fix $0 \leq i \leq n$ and set $R_i = R[\alpha_1, \ldots, \alpha_i]$, and $K_i = K(\alpha_1, \ldots, \alpha_i)$. Since R is integrally closed, we may assume inductively that R_i is the integral closure of R in K_i. Let $g = \mathrm{irr}(\alpha_{i+1}, K_i)$. Then g has its coefficients in

R_i and $g(X)$ divides $f(X)$ in R_i. It follows that $g(X) = \prod_{j\in J}(X - \alpha_j)$ for some $J \subseteq \{1, \ldots, n\}$. Hence $\mathrm{disc}(g)$ divides $\mathrm{disc}(f)$ in R_i. Since $\mathrm{disc}(f)$ is a unit of R, it is a unit of R_i, hence so is $\mathrm{disc}(g)$. Then, by Lemma 4.1.2, $R_{i+1} = R_i[\alpha_{i+1}]$ is the integral closure of R_i in $K_{i+1} = K_i(\alpha_{i+1})$. Therefore, R_{i+1} is the integral closure of R in K_{i+1}.

By induction, R_i is the integral closure of R in K_i for each $0 \leq i \leq n$. In particular, $S = R_n$ is the integral closure of R in $L = K_n$. □

Using this Lemma, we determine the splitting field of $\bar{f}$ over $\bar{K}$.

Lemma 4.1.4. Let R be an integrally closed domain with quotient field K. Let $f(X) \in R[X]$ be a monic irreducible polynomial of degree n and let $\mathfrak{p}$ be a prime ideal of R. Denote the reduction modulo $\mathfrak{p}$ by bar. Let L be the splitting field of f over K and S the integral closure of R in L. Let $\mathfrak{q}$ be a prime ideal of S lying over $\mathfrak{p}$. Set $\bar{K} = \mathrm{Quot}(R/\mathfrak{p})$ and $\bar{L} = \mathrm{Quot}(S/\mathfrak{q})$. Suppose $\mathrm{disc}(f)$ is a unit of R modulo $\mathfrak{p}$. Then $\bar{L}$ is the splitting field of $\bar{f}$ over $\bar{K}$.

Proof. Let $R_\mathfrak{p}$ be the localisation of R at $\mathfrak{p}$. Then $\mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal of $R_\mathfrak{p}$ and $\bar{K} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. Moreover $S_\mathfrak{p} = SR_\mathfrak{p}$ is the integral closure of $R_\mathfrak{p}$ in L, $\mathfrak{q}R_\mathfrak{p}$ is a maximal ideal of $S_\mathfrak{p}$ that lies over $\mathfrak{p}S_\mathfrak{p}$, and $\bar{L} = S_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p}$.

Replacing R by $R_\mathfrak{p}$ and $\mathfrak{p}$ by $\mathfrak{p}R_\mathfrak{p}$, we may assume that R is a local domain and $\mathfrak{p}$ its unique maximal ideal. By assumption, $\mathrm{disc}(f)$ is now a unit of R. Then, Lemma 4.1.3 implies that $S = R[\alpha_1, \ldots, \alpha_n]$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f in L. It follows that $\bar{L} = \bar{K}[\bar{\alpha_1}, \ldots, \bar{\alpha_n}]$, that is $\bar{L}$ is the splitting field of $\bar{f}$ over $\bar{K}$. □

Remark 4.1.5. Consider the case $R = \mathbb{Z}$. Let $f(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial. Let L be the splitting field of f over $\mathbb{Q}$ and $\mathcal{O}_L$ the ring of integers of L. Let p be a prime number and suppose the reduction modulo p of f is separable over $\mathbb{F}_p$. Then, $\mathrm{disc}(\bar{f}) \neq 0$ in $\mathbb{F}_p$. In other words,

disc(f) is a unit of $\mathbb{Z}$ modulo p. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying over p. By Lemma 4.1.4, $\mathcal{O}_L/\mathfrak{P}$ is the splitting field of $\bar{f}$ over $\mathbb{F}_p$.

Now, let us show that, under some assumption, the Galois group of $\bar{f}$ over $\bar{K}$ is a subgroup of the Galois group of f over K.

Lemma 4.1.6. Let R be an integrally closed domain with quotient field K. Let $f(X) \in R[X]$ be a monic irreducible polynomial of degree n and let $\mathfrak{p}$ be a prime ideal of R. Denote the reduction modulo $\mathfrak{p}$ by bar. Let L be the splitting field of f over K and S the integral closure of R in L. Let $\mathfrak{q}$ be a prime ideal of S lying over $\mathfrak{p}$. Set $\bar{K} = \text{Quot}(R/\mathfrak{p})$ and $\bar{L} = \text{Quot}(S/\mathfrak{q})$. Suppose $\bar{f}$ is separable. Then $\bar{L}/\bar{K}$ is a Galois extension and the map $D_\mathfrak{q} \longrightarrow \text{Gal}(\bar{L}/\bar{K})$ given by $\sigma \longmapsto \bar{\sigma}$ is an isomorphism.

Proof. Since $\bar{f}$ is separable, disc(f) is a unit of R modulo $\mathfrak{p}$. Hence by Lemma 4.1.4, $\bar{L}$ is the splitting field of $\bar{f}$ over $\bar{K}$.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in S. Since f is monic, f and $\bar{f}$ have the same degree and $\bar{\alpha_1}, \ldots, \bar{\alpha_n}$ are roots of $\bar{f}$. Since $\bar{f}$ is separable, $\bar{\alpha_1}, \ldots, \bar{\alpha_n}$ are distinct. Hence, the map $\alpha_i \longmapsto \bar{\alpha_i}$, for $i = 1 \ldots n$ is a bijection of the set of roots of f onto the set of roots of $\bar{f}$. Let $\sigma \in D_\mathfrak{q}$ such that $\bar{\sigma} = \text{id}$. Then $\overline{\sigma\alpha_i} = \bar{\sigma}\bar{\alpha_i} = \bar{\alpha_i}$ for $\leq i \leq n$. It follows that $\sigma = \text{id}$. Therefore, the map $\sigma \mapsto \bar{\sigma}$ is injective. By Remark 4.1.1, it is an isomorphism. □

Remark 4.1.7. In this case, since $\bar{L}$ is the splitting field of $\bar{f}$ over $\bar{K}$ and $D_\mathfrak{q}$ is a subgroup of $\text{Gal}(L/K) = \text{Gal}(f, K)$, $\text{Gal}(\bar{f}, \bar{K})$ can be identified as a subgroup of $\text{Gal}(f, K)$.

Now, let us give another property of the Galois group of a polynomial over a finite field.

Lemma 4.1.8. Let q be a power of a prime number. Let $f(X) \in \mathbb{F}_q[X]$ be a separable polynomial. Suppose $f = f_1 f_2 \cdots f_d$, with f_i irreducible polynomials with coefficients in $\mathbb{F}_q$ of degree n_i, for each $1 \leq i \leq d$. Then $\text{Gal}(f, \mathbb{F}_q)$

contains a product of d disjoint cycles $\sigma_1, \ldots, \sigma_d$ of length $n_1, \ldots, n_d$ respectively.

Proof. Let L be the splitting field of f over $\mathbb{F}_q$ and let σ be a generator of $\mathrm{Gal}(L/\mathbb{F}_q)$. For each $1 \leq i \leq d$ we choose a root x_i of f_i in L. Set $\tau_i = \sigma|_{\mathbb{F}_q(x_i)}$. By the Fundamental Theorem of Galois Theory, $\mathrm{Gal}(\mathbb{F}_q(x_i)/\mathbb{F}_q) = \langle \tau_i \rangle$, that is $\mathrm{ord}(\tau_i) = n_i$. If there exists $1 \leq j \leq n_i - 1$ such that $\tau_i^j(x_i) = x_i$, then $\tau_i = 1$ which is a contradiction. Hence, τ_i is a cycle of length n_i. Since f is separable, the presentation of σ as a permutation of the roots of f is the product $\tau_1 \cdots \tau_d$. □

4.2 Continuity of Roots

The aim of this section is to prove that polynomials with coefficients in a Henselian valued field whose coefficients are close to one another have the same splitting field over this field.

If (K, v) is a Henselian valued field, then by Proposition 1.5.2, v extends uniquely to K_s. It follows from Remark 1.3.9 that, for each $\sigma \in \mathrm{Gal}(K)$, $v \circ \sigma = v$.

We start with Krasner's Lemma.

Lemma 4.2.1. (Lem. 12.1 of [Jar]) Let (K, v) be a Henselian valued field. Let $x \in K_s$ and $f(X) = (X - x_1) \cdots (X - x_n) \in K_s[X]$ be the irreducible polynomial of x over K, with $x = x_1$. If $y \in K_s$ satisfies

$$v(y - x) > \max_{x_i \neq x} v(x_i - x),$$

then $K(x) \subseteq K(y)$.

Proof. If $K(x)$ is not contained in $K(y)$, then there exists $\sigma \in \mathrm{Gal}(K)$ such that $\sigma y = y$ and $\sigma x \neq x$. Hence, there exists $2 \leq i \leq n$ such that $\sigma x = x_i$.

The identity $y-x_i = (y-x)+(x-x_i)$ and the inequality $v(y-x) > v(x_i-x)$ imply that $v(x_i-x) = v(y-x_i) = v(\sigma(y-x)) = v(y-x) > v(x_i-x)$, which is a contradiction. Therefore, $K(x) \subseteq K(y)$. $\square$

The next Lemma deals with the continuity of roots of a separable polynomial.

Lemma 4.2.2. (Thm. 2.4.7 of [E-P] or Prop. 12.2 of [Jar]) Let (K, v) be a valued field and let $f(X)$ be a monic polynomial with distinct roots $x_1, \ldots, x_n \in K$. Then for each $\alpha \in \Gamma_v$, there exists $\gamma \in \Gamma_v$ such that if $g(X)$ is a monic separable polynomial of degree n which has all of its roots in K and $v(f-g) > \gamma$, then the roots of g can be enumerated as $y_1, \ldots, y_n$ such that $v(y_i - x_i) > \alpha$, for $1 \leq i \leq n$. Moreover, if $\alpha > \max_{i \neq j} v(x_i - x_j)$, then for each i, y_i is the unique root of g that satisfies $v(y_i - x_i) > \alpha$.

Proof. Suppose $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ and $g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0$. Assume without loss of generality that

$$\alpha > \max_{i \neq j} v(x_i - x_j). \tag{4.2.1}$$

Set

$$\beta = \min_{1 \leq i \leq n} v(x_i). \tag{4.2.2}$$

Then, for $1 \leq i \neq j \leq n$, $\beta \leq \min(v(x_i), v(x_j)) \leq v(x_i - x_j) < \alpha$.

Let $\gamma > \max(n\alpha, n(\alpha - \beta))$ and let $x \in \{x_1, \ldots, x_n\}$. By assumption $g(X) = \prod_{i=1}^{n}(X - y_i)$ with $y_1, \ldots, y_n \in K$. Assume that $v(x - y_i) \leq \alpha$ for all $1 \leq i \leq n$. Then

$$v(g(x)) = \sum_{i=1}^{n} v(x - y_i) \leq n\alpha. \tag{4.2.3}$$

1st case: $v(x) \geq 0$. Since $v(a_k - b_k) > \gamma$ for $0 \leq k \leq n-1$, we have

$$\begin{aligned} v(g(x)) = v(g(x) - f(x)) &= v(\sum_{k=0}^{n-1}(b_k - a_k)x^k) \\ &\geq \min_{0 \leq k \leq n-1}(v(b_k - a_k) + kv(x)) > \gamma. \end{aligned} \tag{4.2.4}$$

It follows from the inequalities (4.2.3) and (4.2.4), and the choice of γ that $n\alpha < \gamma < v(g(x)) \leq n\alpha$ which is a contradiction.

2nd case: $v(x) < 0$. We consider

$$f(x)x^{-n} = a_0x^{-n} + a_1x^{-(n-1)} + \cdots + 1$$

$$g(x)x^{-n} = b_0x^{-n} + b_1x^{-(n-1)} + \cdots + 1$$

Then

$$v(g(x)x^{-n}) = v(g(x)x^{-n} - f(x)x^{-n}) = v(\sum_{k=0}^{n-1}(b_k - a_k)x^{-n+k})$$
$$\geq \min_{0\leq k\leq n-1}(v(b_k - a_k) + (n-k)(-v(x))) > \gamma.$$

Moreover, $v(g(x)x^{-n}) = v(g(x)) - nv(x) \leq n\alpha - nv(x)$. Hence,

$$n(\alpha - \beta) < \gamma < v(g(x)x^{-n}) \leq n\alpha - nv(x). \tag{4.2.5}$$

Therefore, $v(x) < \beta$ which contradicts (4.2.2).

Thus, in both cases we have a contradiction. Therefore, there exists $1 \leq i \leq n$ such that $v(x - y_i) > \alpha$.

If x' is another element of $\{x_1, \ldots, x_n\}$ for which $v(x' - y_i) > \alpha$, then

$$v(x - x') = v((x - y_i) + (y_i - x')) \geq \min(v(x - y_i), v(y_i - x')) > \alpha,$$

in contrast to (4.2.1). Hence, the map φ: $\{x_1, \ldots, x_n\} \longrightarrow \{y_1, \ldots, y_n\}$ which maps each $x \in \{x_1, \ldots, x_n\}$ to y_i with $1 \leq i \leq n$ such that $v(x - y_i) > \alpha$ is injective. Since $x_1, \ldots, x_n$ are distinct, $y_1, \ldots, y_n$ are also distinct and φ is bijective. It follows that $y_1, \ldots, y_n$ can be enumerated such that $v(x_i - y_i) > \alpha$ for $i = 1, \ldots, n$. $\square$

The next corollary combines Krasner's Lemma and the Continuity of Roots.

Corollary 4.2.3. (Prop. 12.3 of [Jar]) Let (K, v) be a Henselian field. Let $f \in K[X]$ be a monic polynomial of degree n with distinct roots $x_1, \ldots, x_n$ in K_s. Then, for each $\alpha \in \Gamma_v$, there exists $\gamma \in \Gamma_v$ such that if $g \in K[X]$ is a monic polynomial of degree n with $v(f-g) > \gamma$, then the roots of g can be enumerated as $y_1, \ldots, y_n$ such that $v(y_i - x_i) > \alpha$ and $K(x_i) = K(y_i)$. In particular, the splitting field of f and g over K coincide, so $\mathrm{Gal}(f, K) \cong \mathrm{Gal}(g, K)$.

Proof. Assume without loss of generality that

$$\alpha > \max_{i \neq j} v(x_i - x_j). \tag{4.2.6}$$

We extend v to a valuation v of K_s. Let $\gamma \in v(K_s^\times)$ as in Lemma 4.2.2. Since $v(K^\times)$ is cofinal in $v(K_s^\times)$ (Lemma 1.2.2), we may assume that $\gamma \in \Gamma_v$. Then, if $g \in K[X]$ is a monic polynomial of degree n such that $v(f-g) > \gamma$, the roots of g are distinct and can be enumerated as $y_1, \ldots, y_n$ such that

$$v(y_i - x_i) > \alpha, \text{for } 1 \leq i \leq n. \tag{4.2.7}$$

In particular, for each i, y_i is the unique root of g satisfying (4.2.7). It follows that $y_1, \ldots, y_n$ are separable over K. If $x_j = \sigma x_i$, for some $\sigma \in \mathrm{Gal}(K)$, then

$$v(\sigma y_i - x_j) = v(\sigma(y_i - x_i)) = v(y_i - x_i) > \alpha.$$

Hence, by the uniqueness of y_j, $\sigma y_i = y_j$. It follows that the number of conjugates of y_i over K is at least the same as those of x_i. Since this holds for each i, y_i and x_i have the same number of conjugates over K, that is $[K(x_i) : K] = [K(y_i) : K]$. By (4.2.6) and (4.2.7) we have

$$v(y_i - x_i) > \max_{k \neq l} v(x_k - x_l).$$

Hence, by Lemma 4.2.1, $K(x_i) \subseteq K(y_i)$. Hence, $K(x_i) = K(y_i)$. Consequently, $K(x_1, \ldots, x_n) = K(y_1, \ldots, y_n)$, as claimed. $\square$

4.3 Realization of the Symmetric Group S_n

In a letter to David Hilbert ([Ba]) Michael Bauer described an elementary method to realize the groups S_n as Galois groups over $\mathbb{Q}$. This method does not use the Hilbert Irreducibility Theorem. B. L. van der Waerden represented that method in his book [Algebra I]. We apply this method to construct for each positive integer n and every prime number p a polynomial $f(X)$ in $\mathbb{Z}[X]$ such that $\mathrm{Gal}(f, \mathbb{Q}) \cong S_n$ and f totally splits in $\mathbb{Q}_{\mathrm{tot},p}$.

First, we state some elementary well known results from group theory and properties of a finite field.

Lemma 4.3.1. Let n be a positive integer.

(1) If a subgroup G of S_n contains an n-cycle (cycle of length n), then G acts transitively on the set $\{1, \ldots, n\}$.

(2) If a transitive subgroup G of S_n contains an $(n-1)$-cycle and a transposition, then $G = S_n$.

(3) If a subgroup G of S_n contains an n-cycle, an $(n-1)$-cycle, and a transposition, then $G = S_n$.

Proof. (1) Let $\sigma = (x_1 x_2 \cdots x_n)$ be an n-cycle in G, with $x_k \in \{1, \ldots, n\}$. Let $x_i, x_j \in \{1, \ldots, n\}$. Suppose $i < j$ and $j = i + r$. Then, $\sigma x_i = x_{i+1}$ and $\sigma^2 x_i = \sigma x_{i+1} = x_{i+2}$. Increasing the power of σ, we get for $k \leq r$, $\sigma^k x_i = x_{i+k}$, in particular $\sigma^r x_i = x_{i+r} = x_j$. Furthermore, $x_i = (\sigma^{-1})^r x_j$. Therefore, G acts transitively on $\{1, \ldots, n\}$.

(2) Let $x, y, x_1, \ldots, x_{n-1}$ be elements of $\{1, \ldots, n\}$. Suppose the transposition (xy) and the $(n-1)$-cycle $\sigma = (x_1 x_2 \cdots x_{n-1})$ are in G. Let z be the unique element of $\{1, \ldots, n\}$ which is not in $\{x_1, \ldots, x_{n-1}\}$. Then, $\sigma z = z$.

CLAIM: For all $x_j \in \{x_1, \ldots, x_{n-1}\}$, $(z x_j) \in G$.

Indeed, since G acts transitively on $\{1,\dots,n\}$, there exists $\delta \in G$ such that $\delta x = z$. Then, $\delta y \neq z$ so there exists $1 \leq k \leq n-1$ such that $\delta y = x_k$. It follows that

$$(zx_k) = (\delta x\ \delta y) = \delta(xy)\delta^{-1},$$

so $(zx_k) \in G$. Moreover,

$$\sigma(zx_k)\sigma^{-1} = \begin{cases} (zx_{k+1}) & \text{if } 1 \leq k \leq n-2 \\ (zx_1) & \text{if } k = n-1. \end{cases}$$

Hence, $(zx_{k+1}) \in G$ if $1 \leq k \leq n-2$ and $(zx_1) \in G$ if $k = n-1$.

A repeated application of σ gives

$$(zx_j) = \begin{cases} \sigma^{j-k}(zx_k)(\sigma^{-1})^{j-k} & \text{for } k < j \leq n-1 \\ \sigma^{(n-1)-k+j}(zx_k)(\sigma^{-1})^{(n-1)-k+j} & \text{for } 1 \leq j \leq k-1. \end{cases}$$

Thus, for every $1 \leq j \leq n-1$, $(zx_j) \in G$, as claimed.

Now, the identity $(x_i x_j) = (zx_i)(zx_j)(zx_i)$, for $1 \leq i < j \leq n-1$, implies that $(x_i x_j) \in G$. Hence, G contains every transpositions of S_n. Since every permutation is a product of transpositions, $G = S_n$.

(3) From (1) and (2)

□

Lemma 4.3.2. For every finite field $\mathbb{F}_q$ and every integer n, there exists a monic irreducible polynomial in $\mathbb{F}_q[X]$ of degree n.

Proof. Let $\mathbb{F}_{q^n}$ be the extension of degree n of $\mathbb{F}_q$. By the primitive element theorem (Thm. 4.6, p.243 of [La2]), there exists $\alpha \in \mathbb{F}_{q^n}$ such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Then the irreducible polynomial of α over $\mathbb{F}_q$ is a monic irreducible polynomial in $\mathbb{F}_q[X]$ of degree n. □

Lemma 4.3.3. If a monic polynomial with coefficients in $\mathbb{Z}$ is irreducible modulo a prime number p, then the polynomial is irreducible over $\mathbb{Z}$.

Theorem 4.3.4. *For every prime number p and positive integer n, $\mathbb{Q}$ has a Galois extension L in $\mathbb{Q}_{tot,p}$, with $Gal(L/\mathbb{Q}) \cong S_n$.*

Proof. For $n = 1$, it is trivial.

For $n = 2, S_2 \cong \mathbb{Z}/2\mathbb{Z}$, this case is proved in Lemma 2.2.2.

Assume $n \geq 3$. Let p_1, p_2, p_3 be distinct prime numbers different from p. Using Lemma 4.3.2, we choose monic separable irreducible polynomials $f_{p_1}, g_{p_2}, g_{p_3}$ with coefficients in $\mathbb{F}_{p_1}, \mathbb{F}_{p_2}, \mathbb{F}_{p_3}$ of degree $n, n-1$, and 2 respectively.

If n is odd, we also choose a monic separable irreducible polynomial $h_{p_3} \in \mathbb{F}_{p_3}[X]$ of degree $n-2$. Otherwise, we choose a monic separable irreducible polynomial $h'_{p_3}[X] \in \mathbb{F}_{p_3}$ of degree $n-3$.

Now, we define $f_{p_2} \in \mathbb{F}_{p_2}[X]$ by $f_{p_2}(X) = (X-1)g_{p_2}(X)$ and $f_{p_3} \in \mathbb{F}_{p_3}[X]$ by $f_{p_3}(X) = g_{p_3}(X)h_{p_3}(X)$ if n is odd, and $f_{p_3}(X) = (X-1)g_{p_3}(X)h'_{p_3}(X)$ if n is even. Then f_{p_2} and f_{p_3} are monic of degree n.

Let $f_p(X) = X(X-1)\cdots(X-(n-1))$. By Corollary 4.2.3, there exists a positive integer r such that if $f \in \mathbb{Z}_p[X]$ of degree n satisfies

$$f(X) \equiv f_p(X) \mod p^r, \tag{4.3.1}$$

then $f(X)$ totally splits in $\mathbb{Q}_{\mathrm{tot},p}$.

Since p_1, p_2, p_3, p^r are pairwise coprime, by Bezout's identity, there exists u, u', v, v',
$s, s' \in \mathbb{Z}$ such that

$$p_1p_3p^ru + p_2p_3p^ru' = p_3p^r \tag{4.3.2}$$

$$p_3 p^r v + p_1 p_2 p^r v' = p^r \tag{4.3.3}$$

$$p_1 p_2 p_3 s + p^r s' = 1. \tag{4.3.4}$$

Substituting $p_3 p^r$ from (4.3.2) in (4.3.3) gives

$$p_1 p_3 p^r uv + p_2 p_3 p^r u' v + p_1 p_2 p^r v' = p^r. \tag{4.3.5}$$

Substituting p^r from (4.3.5) in (4.3.4) gives

$$p_1 p_2 p_3 s + p_1 p_3 p^r uvs' + p_2 p_3 p^r u' vs' + p_1 p_2 p^r v' s' = 1. \tag{4.3.6}$$

Set

$$\alpha_1 = p_2 p_3 s,\ \alpha_2 = p_3 p^r u' vs',\ \alpha_3 = p_1 p^r uvs',\ \alpha_4 = p_1 p_2 v' s'. \tag{4.3.7}$$

By (4.3.6) and (4.3.7)

$$p_1\alpha_1 + p_2\alpha_2 + p_3\alpha_3 + p^r\alpha_4 = 1, \tag{4.3.8}$$

so

$$\begin{aligned}
p_2\alpha_2 &\equiv p_1\alpha_1 + p_2\alpha_2 + p_3\alpha_3 + p^r\alpha_4 \equiv 1 \mod p_1,\\
p_3\alpha_3 &\equiv p_1\alpha_1 + p_2\alpha_2 + p_3\alpha_3 + p^r\alpha_4 \equiv 1 \mod p_2,\\
p^r\alpha_4 &\equiv p_1\alpha_1 + p_2\alpha_2 + p_3\alpha_3 + p^r\alpha_4 \equiv 1 \mod p_3,\\
p_1\alpha_1 &\equiv p_1\alpha_1 + p_2\alpha_2 + p_3\alpha_3 + p^r\alpha_4 \equiv 1 \mod p^r.
\end{aligned} \tag{4.3.9}$$

Now we lift $f_{p_1}, f_{p_2}, f_{p_3}$ to momic polynomials in $\mathbb{Z}[X]$ with the same name, and consider the polynomial $g(X) \in \mathbb{Z}[X]$ defined by

$$g(X) = p_2\alpha_2 f_{p_1}(X) + p_3\alpha_3 f_{p_2}(X) + p^r\alpha_4 f_{p_3} + p_1\alpha_1 f_p(X). \tag{4.3.10}$$

Each of the polynomials appearing on the right hand side of (4.3.10) is monic of degree n. Hence, by (4.3.8), the coefficient of X^n on the right of (4.3.10) is 1. Therefore, $g(X)$ is monic of degree n, and by (4.3.7) and (4.3.9),

$$\begin{aligned}
g(X) &\equiv f_{p_1}(X) \mod p_1,\\
g(X) &\equiv f_{p_2}(X) \mod p_2,\\
g(X) &\equiv f_{p_3}(X) \mod p_3,\\
g(X) &\equiv f_p(X) \mod p^r,
\end{aligned}$$

In particular, since f_{p_1} is a monic separable irreducible polynomial of degree n over $\mathbb{F}_{p_1}$, Lemma 4.3.3 implies that $g(X)$ is irreducible over $\mathbb{Z}$.

Moreover, Lemma 4.1.8 implies that $\mathrm{Gal}(f_{p_1}, \mathbb{F}_{p_1})$ contains an n-cycle. Also, f_{p_2} has an irreducible factor of degree $n-1$, so $\mathrm{Gal}(f_{p_2}, \mathbb{F}_{p_2})$ contains an $(n-1)$-cycle. By Lemma 4.1.6, $\mathrm{Gal}(f_{p_1}, \mathbb{F}_{p_1})$ and $\mathrm{Gal}(f_{p_2}, \mathbb{F}_{p_2})$ are isomorphic, as permutation groups, to subgroups of $\mathrm{Gal}(g, \mathbb{Q})$. Hence, $\mathrm{Gal}(g, \mathbb{Q})$ contains an n-cycle and an $(n-1)$-cycle.

If n is odd, then $n-2$ is also odd. Since f_{p_3} is a product of monic irreducible polynomials of degrees 2 and $n-2$, the group $\mathrm{Gal}(f_{p_3}, \mathbb{F}_{p_3})$ contains a product of disjoint cycles $\sigma\sigma'$, where σ is a 2-cycle and σ' an $(n-2)$-cycle. Since $n-2$ is odd and σ and σ' are disjoint, $\sigma = \sigma^{n-2}(\sigma')^{n-2} = (\sigma\sigma')^{n-2} \in \mathrm{Gal}(f_{p_3}, \mathbb{F}_{p_3})$. Therefore, $\mathrm{Gal}(g, \mathbb{Q})$ contains a 2-cycle.

If n is even, then $n-3$ is odd. In this case f_{p_3} is a product of monic irreducible polynomials of degree $1, 2$, and $n-3$, hence $\mathrm{Gal}(f_{p_3}, \mathbb{F}_{p_3})$ contains a product of disjoint cycles $\eta\eta'$ where η is a 2-cycle and η' is an $(n-3)$-cycle. As before, $\eta = (\eta\eta')^{n-3} \in \mathrm{Gal}(f_{p_3}, \mathbb{F}_{p_3})$. Therefore, $\mathrm{Gal}(g, \mathbb{Q})$ contains a 2-cycle.

In both cases, $\mathrm{Gal}(g, \mathbb{Q})$ contains a 2-cycle. Since $\mathrm{Gal}(g, \mathbb{Q})$ contains an n-cycle, an $(n-1)$-cycle and a transposition, by Lemma 4.3.1, it acts transitively on the set $\{1, \ldots, n\}$ and it follows that $\mathrm{Gal}(g, \mathbb{Q}) \cong S_n$. Denote by L the splitting field of g over $\mathbb{Q}$. Then, $\mathrm{Gal}(L/\mathbb{Q}) \cong S_n$.

Finally, $g(X) \equiv f_p(X) \mod p^r$ implies that all of the roots of $g(X)$ are in $\mathbb{Q}_p$. Consequently, $L \subseteq \mathbb{Q}_{\mathrm{tot},p}$. $\square$

Chapter 5

The Alternating Groups A_n as a Galois Group over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$

For each positive integer $n \geq 4$, we exhibit a polynomial in $\mathbb{Q}[X]$ which totally splits in $\mathbb{Q}_{\mathrm{tot},p}$, whose Galois group over $\mathbb{Q}[X]$ is isomorphic to A_n. The construction goes back to Mestre ([Me]). We begin with some essential tools.

5.1 1-Cocycle for a Group Action

This section shows that every multiplicative 1-cocycle f of a Galois group is determined by an element of the Galois extension, indeed f is a 1-coboundary. This is the content of Hilbert theorem 90.

Let G be a group acting on an abelian group A from the left:

$$\begin{aligned} G \times A &\longrightarrow A \\ (\sigma, a) &\longmapsto \sigma(a). \end{aligned}$$

Definition 5.1.1. A **1-cocycle** of G in A is a map $f\colon G \longrightarrow A$ satisfying

$$f(\sigma_1\sigma_2) = f(\sigma_1) + \sigma_1\big(f(\sigma_2)\big), \quad \text{if } A \text{ is additive,}$$

$$f(\sigma_1\sigma_2) = f(\sigma_1)\sigma_1\big(f(\sigma_2)\big), \quad \text{if } A \text{ is multiplicative.}$$

Lemma 5.1.2. (Thm. 10.1, p. 303 of [La2]) Let L/K be a finite Galois extension of fields with Galois group G. Let $f\colon G \longrightarrow L^\times$ be a cocycle of G with values in $L^\times$. Then, there exists $a \in L^\times$ such that $f(\sigma) = \dfrac{a}{\sigma a}$ for all $\sigma \in G$.

Proof. By Artin's linear independence of automorphisms (Thm. 4.1, p. 283 of [La2]), there exists $b \in L^\times$ such that

$$a = \sum_{\tau \in G} f(\tau)\, \tau b \quad \neq 0. \tag{5.1.1}$$

Let $\sigma \in G$, and now applying σ on both sides of (5.1.1), we get

$$\begin{aligned} \sigma a &= \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau b) = \sum_{\tau \in G} f(\sigma)^{-1} f(\sigma)\sigma(f(\tau))\sigma(\tau b) \\ &= f(\sigma)^{-1} \sum_{\tau \in G} f(\sigma\tau)\sigma(\tau b) = f(\sigma)^{-1} a. \end{aligned}$$

Thus $f(\sigma) = a(\sigma a)^{-1}$, as desired. □

5.2 Hilbertian Fields

Given a Hilbertian field K, there is preservation of Galois groups of polynomials under specialization of variables.

Let K be a field, and let $T_1, \ldots, T_r, X_1, \ldots, X_n$ be variables. Set $\mathbf{T} = (T_1, \ldots, T_r)$ and $\mathbf{X} = (X_1, \ldots, X_n)$. Let $f_1(\mathbf{T}, \mathbf{X}), \ldots, f_m(\mathbf{T}, \mathbf{X})$ be irreducible polynomials in $X_1, \ldots, X_n$ with coefficients in $K(\mathbf{T})$.

Definition 5.2.1. Let $g(\mathbf{T}) \in K[\mathbf{T}]$ be a nonzero polynomial. Let $H_K(f_1, \ldots, f_m; g)$ be the set of all r-tuples $\mathbf{a} = (a_1, \ldots, a_r) \in K^r$ with $g(a_1, \ldots, a_r) \neq 0$ and $f_i(a_1, \ldots, a_r, \mathbf{X})$ is well defined and irreducible in $K[X]$ for $i = 1, \ldots, m$. We call $H_K(f_1, \ldots, f_m; g)$ a **Hilbert subset** of K^r. If $n = 1$ and each f_i is separable in X, then $H_K(f_1, \ldots, f_m; g)$ is a **separable Hilbert subset** of K^r. A **Hilbert set** (resp. separable Hilbert set) of K is a Hilbert subset

(resp. separable Hilbert subset) of K^r for some positive integer r.

The field K is **Hilbertian** if each separable Hilbert set of K is nonempty.

Hilbert's irreducibility theorem says that the field $\mathbb{Q}$ of rational numbers is Hilbertian.

Theorem 5.2.2 (p. 18, Thm. 1.23 of [Vo])**.** *Every number field is Hilbertian.*

The following result appears as Exercise 4 of Chapter 13 of [F-J].

Lemma 5.2.3. Let (K, v) be a Hilbertian valued field and H a separable Hilbert subset of K^r. Then, for each $\mathbf{a} = (a_1, \ldots, a_r) \in K^r$ and for each $\gamma \in \Gamma_v$, there exists $\mathbf{b} = (b_1, \ldots, b_r) \in H$ such that $v(\mathbf{b} - \mathbf{a}) \geq \gamma$.

Proof. Let $f_1, \ldots, f_m \in K(T_1, \ldots, T_r)[X]$ be irreducible separable polynomials with $H = H_K(f_1, \ldots, f_m)$. Let $(a_1, \ldots, a_r) \in K^r$ and $\gamma = v(c)$ for some $c \in K^\times$. Observe that each polynomial in the set $S = \{f_i(a_1 + cT_1^{\epsilon_1}, \ldots, a_r + cT_r^{\epsilon_r}, X) \mid 1 \leq i \leq m \text{ and } \epsilon_1, \ldots, \epsilon_r \in \{\pm 1\}\}$ is separable and irreducible. Since K is Hilbertian, there exist $t_1, \ldots, t_r \in K^r$ such that $f_i(a_1 + ct_1^{\epsilon_1}, \ldots, a_r + ct_r^{\epsilon_r}, X)$ is irreducible in $K[X]$, for $i = 1, \ldots, m$ and $\epsilon_1, \ldots, \epsilon_r \in \{\pm 1\}$. Choose the r-tuple $(\epsilon_1, \ldots, \epsilon_r) \in \{\pm 1\}^r$ such that

$$\epsilon_i = 1 \text{ if } v(t_i) \geq 0, \text{ and } \epsilon_i = -1 \text{ if } v(t_i) < 0. \tag{5.2.1}$$

Set $b_i = a_i + ct_i^{\epsilon_i}$ for $i = 1, \ldots, m$. Then,

$$f_i(b_1, \ldots, b_r, X) = f_i(a_1 + ct_1^{\epsilon_1}, \ldots, a_r + ct_r^{\epsilon_r}, X),$$

so $f_i(b_1, \ldots, b_r, X)$ is irreducible for $i = 1, \ldots, r$. Furthermore, for $i = 1, \ldots, r$

$$v(b_i - a_i) = v(ct_i^{\epsilon_i}) = v(c) + \epsilon_i v(t_i) = \gamma + \epsilon_i v(t_i).$$

By the choice of $\epsilon_i, \ldots, \epsilon_r$ in (5.2.1), $\epsilon_i v(t_i) \geq 0$, so $\gamma + \epsilon_i v(t_i) \geq \gamma$. Thus, $v(b_i - a_i) \geq \gamma$ for $i = 1, \ldots, r$, as desired. □

Proposition 5.2.4. (Prop. 16.1.5 of [F-J]) Let K be a Hilbertian field. Let $h_1, \ldots, h_m \in K[t_1, \ldots, t_r, X]$ be separable polynomials in X. Then, K^r has a separable Hilbert subset H such that for each $\mathbf{a} \in H$, $\mathrm{Gal}(h_j(\mathbf{a}, X)/K) \cong \mathrm{Gal}(h_j(\mathbf{t}, X)/K(\mathbf{t}))$ for $j = 1, \ldots, m$.

5.3 The General Polynomial of Odd Degree

For an odd integer $n \geq 5$, let $g(X) = X^n + s_1 X^{n-1} + \cdots + s_n$ be the general polynomial of degree n with coefficients in a field K. We prove that the equation $g(X)h'(X) - g'(X)h(X) = -q^2(X)$ in the variables $h, q \in K[X]$ is solvable. We may even choose h and q to be separable, and g and h to be relatively prime. First, we recall some essential ingredients.

Circulant Matrices

Let K be a field and n a positive integer. Define the **shift** operator

$$\begin{aligned} S\colon K^n &\longrightarrow K^n \\ (a_1, a_2 \ldots, a_n) &\longmapsto (a_n, a_1, \ldots, a_{n-1}). \end{aligned}$$

The **circulant** matrix $C = \operatorname{circ}(a_1, a_2, \ldots, a_n)$ associated to the vector $(a_1, a_2, \ldots, a_n)$ is the $n \times n$ matrix whose rows are given by the iterations of the shift operator acting on $(a_1, a_2, \ldots, a_n)$: the i-th row of C is $S^{i-1}(a_1, a_2, \ldots, a_n)$ for $1 \leq i \leq n$. Thus, C has the form

$$C = \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_3 & a_4 & \cdots & a_1 & a_2 \\ a_2 & a_3 & \cdots & a_n & a_1 \end{pmatrix}.$$

Let ζ be a primitive n-th root of unity. Set $v_i = (1, \zeta^i, \zeta^{2i}, \ldots, \zeta^{(n-1)i})^T$ (where T is the transpose operation, transferring the row in this case into a column) and $\lambda_i = a_1 + a_2\zeta^i + a_3\zeta^{2i} + \cdots + a_n\zeta^{(n-1)i}$ for $0 \leq i \leq n-1$. Then,

$$C\, v_i = \begin{pmatrix} a_1 + a_2\zeta^i + \cdots + a_{n-1}\zeta^{(n-2)i} + a_n\zeta^{(n-1)i} \\ a_n + a_1\zeta^i + \cdots + a_{n-2}\zeta^{(n-2)i} + a_{n-1}\zeta^{(n-1)i} \\ \vdots \\ a_3 + a_4\zeta^i + \cdots + a_1\zeta^{(n-2)i} + a_2\zeta^{(n-1)i} \\ a_2 + a_3\zeta^i + \cdots + a_n\zeta^{(n-2)i} + a_1\zeta^{(n-1)i} \end{pmatrix},$$

and

$$\lambda_i\ v_i = \begin{pmatrix} a_1 + a_2\zeta^i + \cdots + a_{n-1}\zeta^{(n-2)i} + a_n\zeta^{(n-1)i} \\ a_1\zeta^i + a_2\zeta^{2i} + \cdots + a_{n-1}\zeta^{(n-1)i} + a_n \\ \vdots \\ a_1\zeta^{(n-2)i} + a_2\zeta^{(n-1)i} + a_3 + \cdots + a_n\zeta^{(n-3)i} \\ a_1\zeta^{(n-1)i} + a_2 + a_3\zeta^i + \cdots + a_n\zeta^{(n-2)i} \end{pmatrix}$$

Hence, $C\ v_i = \lambda_i\ v_i$ for each $i = 0, \cdots n-1$. Denote V the matrix whose columns are the vector v_i's:

$$V = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{n-1} \\ 1 & \zeta^2 & (\zeta^2)^2 & \cdots & (\zeta^2)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{n-1} & (\zeta^{n-1})^2 & \cdots & (\zeta^{n-1})^{n-1} \end{pmatrix}.$$

Thus, V is a Vandermonde matrix with determinant

$$\det(V) = \prod_{0 \le i < j \le n-1} (\zeta^j - \zeta^i).$$

Since the ζ^i's are distinct for $i = 0, \ldots, n-1$, $\det(V) \neq 0$, so the v_i's are linearly independent over K. Therefore, v_i's are the eigenvectors of C up to multiplication by nonzero constants and the λ_i's are the corresponding eigenvalues.

Let $p(X) = \det(XI - C)$ be the characteristic polynomial of C, where I is the identity matrix. Then, the roots of $p(X)$ are $\lambda_0, \lambda_2, \ldots, \lambda_{n-1}$, so $p(X) = \prod_{i=0}^{n-1}(X - \lambda_i)$. Furthermore, $\det(-C) = p(0) = \prod_{i=0}^{n-1}(-\lambda_i) = (-1)^n \prod_{i=0}^{n-1} \lambda_i$. Hence, $\det(C) = \prod_{i=0}^{n-1} \lambda_i$. Therefore,

$$\det(C) = \prod_{i=0}^{n-1}(a_1 + a_2\zeta_n^i + \cdots + a_n\zeta_n^{(n-1)i}). \tag{5.3.1}$$

Remark 5.3.1. Let n be a positive integer and let R be a domain. If W is an $n \times n$ skew symmetric matrix with entries in R, then $\det(W) = \det(W^T) = \det(-W) = (-1)^n \det(W)$. Hence, if n is odd then, $\det(W) = 0$.

Traces with respect to Polynomials

Let K be a field and $f \in K[X]$ be a monic separable polynomial of degree m with roots $x_1, \ldots, x_m \in K_s$. Thus, $f(X) = \prod_{i=1}^{m}(X - x_i)$. Set $x = x_1$ and $L = K(x)$. Then, the **trace** of L **with respect to** f is the map tr_f: $L \longrightarrow K$ defined by

$$\mathrm{tr}_f(g(x)) = \sum_{i=1}^{m} g(x_i) \tag{5.3.2}$$

for each $g \in K[X]$. In particular, if $f(X) = X^m + a_1X^{m-1} + \cdots + a_m$ with $a_0, \ldots, a_m \in K$, then

$$\mathrm{tr}_f(x) = x_1 + \cdots + x_m = -a_1. \tag{5.3.3}$$

Now, the right hand side of (5.3.2) is a symmetric polynomial in $x_1, \ldots, x_m$, so the left hand side of (5.3.2) is an element of K, and is unchanged if we choose $x = x_k$ with $2 \leq k \leq m$ rather than $x = x_1$.

The definition of the trace function implies that it is a linear functional of the vector space L over K, that is $\mathrm{tr}_f(ay + bz) = a \cdot \mathrm{tr}_f(y) + b \cdot \mathrm{tr}_f(z)$ for all $a, b \in K$ and $y, z \in L$.

Observe that if f is irreducible, then $\mathrm{tr}_f = \mathrm{tr}_{L/K}$. If $f = \prod_{j\in J} f_j$ is the decomposition of f as a product of irreducible factors in $K[X]$ and x_j a root of f_j for $j \in J$, then $\mathrm{tr}_f(g(x)) = \sum_{j\in J} \mathrm{tr}_{K(x_j)/K}(g(x_j))$.

Equivalent Systems of Equations

Given a field E of characteristic $\neq 2$ and a separable monic polynomial $q \in E[X]$ of degree n, we reduce the solvability of the equation $g(X)h'(X) - g'(X)h(X) = -q(X)^2$ with unknown polynomials $h, q \in E[X]$ of degree at most $n-1$ to the solvability of a linear system of equations over E.

Lemma 5.3.2. Let E be a field with $\mathrm{char}(E) \neq 2$, $n \geq 5$ an odd integer, and $g(X) = X^n + s_1X^{n-1} + \cdots + s_n \in E[X]$ a polynomial with distinct roots

$t_1, \ldots, t_n \in \tilde{E}$. Let F be the splitting field of g over E. We denote by $'$ the differentiation with respect to X. Set $w_{ii} = 0$ and $w_{ij} = \frac{1}{t_i - t_j}$ for $i \neq j$. Let $\mathcal{U}$ be the set of all $(\mathbf{u}, \mathbf{v}) = (u_1, \ldots, u_n, v_1, \ldots, v_n) \in F^{2n}$ that solve the system of equations

$$u_i = v_i^2, \quad v_i \sum_{j=1}^{n} w_{ij} v_j = 0, \quad \text{for } i = 1, \ldots, n. \tag{5.3.4}$$

Let $\mathcal{F}$ be the set of all of the pairs of polynomials $(h, q) \in F[X]^2$ of degree at most $n-1$ that satisfy

$$g(X)h'(X) - g'(X)h(X) = -q(X)^2. \tag{5.3.5}$$

Then

(a) There is a bijective map $\varphi\colon \mathcal{U} \longrightarrow \mathcal{F}$.

(b) Let $(\mathbf{u}, \mathbf{v}) \in \mathcal{U}$, $(h, q) = \varphi(\mathbf{u}, \mathbf{v})$, and $c \in F$. Then $(c^2\mathbf{u}, c\mathbf{v}) \in \mathcal{U}$, $(c^2 h, cq) \in \mathcal{F}$ and $\varphi(c^2\mathbf{u}, c\mathbf{v}) = (c^2 h, cq)$.

(c) Suppose $\varphi(\mathbf{u}, \mathbf{v}) = (h, q)$. Then, $\gcd(g, h) = 1$ if and only if $u_i, v_i \neq 0$ for $i = 1, \ldots, n$. In this case, (5.3.4) reduces to the linear system

$$\sum_{j=1}^{n} w_{ij} v_j = 0 \quad \text{for } i = 1, \ldots, n, \tag{5.3.6}$$

in the variables $v_1, \ldots, v_n$. If in addition, the matrix $W = (w_{ij})_{1 \leq i,j \leq n}$ is of rank $n-1$, then, there exist $(\mathbf{u}_0, \mathbf{v}_0) \in F^{2n}$ and $(h_0, q_0) \in F[X]^2$ such that $\mathcal{U} = \{(c^2\mathbf{u}_0, c\mathbf{v}_0) \mid c \in F\}$ and $\mathcal{F} = \{(c^2 h_0, cq_0) \mid c \in F\}$.

Proof. We start by proving a claim.

CLAIM : The solvability of (5.3.4) is equivalent to the solvability of (5.3.5). Indeed, $\mathcal{F}$ is also the set of all pairs of polynomials $(h, q) \in F[X]^2$ of degree at most $n-1$ that satisfy

$$\left(\frac{h(X)}{g(X)}\right)' = -\left(\frac{q(X)}{g(X)}\right)^2. \tag{5.3.7}$$

For all $h, q \in F[X]$ of degree at most $n-1$, we have the following partial fraction expansions in $F(X)$:

$$\frac{h(X)}{g(X)} = \sum_{i=1}^{n} \frac{u_i}{X - t_i}, \quad \frac{q(X)}{g(X)} = \sum_{i=1}^{n} \frac{v_i}{X - t_i}. \tag{5.3.8}$$

Hence, equation (5.3.7) is equivalent to the equation

$$\sum_{i=1}^{n} \frac{u_i}{(X-t_i)^2} = \sum_{i=1}^{n} \frac{v_i^2}{(X-t_i)^2} + \sum_{i=1}^{n} \Big(\frac{v_i}{X-t_i} \sum_{\substack{j=1 \\ j \neq i}}^{n} \frac{v_j}{X-t_j} \Big). \tag{5.3.9}$$

in the variables $u_1, \ldots, u_n, v_1, \ldots, v_n$.

Now, let $1 \leq k \leq n$. Multiplying both sides of (5.3.9) by $(X-t_k)^2$, we get

$$\begin{aligned} u_k + \sum_{\substack{i=1 \\ i \neq k}}^{n} \frac{u_i (X-t_k)^2}{(X-t_i)^2} = v_k^2 + \sum_{\substack{i=1 \\ i \neq k}}^{n} \frac{v_i^2 (X-t_k)^2}{(X-t_i)^2} + v_k (X-t_k) \sum_{\substack{j=1 \\ j \neq k}}^{n} \frac{v_j}{X-t_j} \\ + \sum_{\substack{i=1 \\ i \neq k}}^{n} \frac{v_i}{X-t_i} \Big(v_k (X-t_k) + \sum_{\substack{j=1 \\ j \neq i, j \neq k}}^{n} \frac{v_j (X-t_k)^2}{X-t_j} \Big). \end{aligned}$$

Substituting t_k for X, we get $u_k = v_k^2$. It follows from (5.3.9) that

$$\sum_{i=1}^{n} \Big(\frac{v_i}{X-t_i} \sum_{\substack{j=1 \\ j \neq i}}^{n} \frac{v_j}{X-t_j} \Big) = 0. \tag{5.3.10}$$

Again, let $1 \leq k \leq n$ and multiply both sides of (5.3.10) by $X - t_k$. Then,

$$\begin{aligned} &\frac{v_1}{X-t_1} \Big(v_k + \sum_{\substack{j=1 \\ j \neq 1, j \neq k}}^{n} \frac{v_j (X-t_k)}{X-t_j} \Big) + \cdots + v_k \sum_{\substack{j=1 \\ j \neq k}}^{n} \frac{v_j}{X-t_j} + \cdots \\ &+ \frac{v_n}{X-t_n} \Big(v_k + \sum_{\substack{j=1 \\ j \neq n, j \neq k}}^{n} \frac{v_j (X-t_k)}{X-t_j} \Big) = 0. \end{aligned}$$

Substituting t_k for X, we get

$$\frac{v_1}{t_k - t_1} v_k + \cdots + v_k \sum_{\substack{j=1 \\ j \neq k}}^{n} \frac{v_j}{t_k - t_j} + \cdots + \frac{v_n}{t_k - t_n} v_k = 0,$$

so

$$v_k \sum_{\substack{j=1 \\ j\neq k}}^{n} \frac{v_j}{t_k - t_j} + v_k \sum_{\substack{j=1 \\ j\neq k}}^{n} \frac{v_j}{t_k - t_j} = 0.$$

Since $\mathrm{char}(E) \neq 2$, (5.3.7) is equivalent to

$$u_i = v_i^2 \quad \text{and} \quad v_i \sum_{j=1}^{n} w_{ij} v_j = 0, \ 1 \leq i \leq n, \tag{5.3.11}$$

as claimed.

Proof of (a). Let $\varphi\colon \mathcal{U} \longrightarrow \mathcal{F}$ be the map given by $(\mathbf{u}, \mathbf{v}) \longmapsto (h, q)$ such that $\frac{h(X)}{g(X)} = \sum_{i=1}^{n} \frac{u_i}{X - t_i}$ and $\frac{q(X)}{g(X)} = \sum_{i=1}^{n} \frac{v_i}{X - t_i}$. By the claim, φ is well defined and surjective. If $\varphi(\mathbf{u}, \mathbf{v}) = \varphi(\mathbf{u}', \mathbf{v}')$, then by the uniqueness of the partial fraction expansions of $\frac{h}{g}$ and $\frac{q}{g}$, $(\mathbf{u}, \mathbf{v}) = (\mathbf{u}', \mathbf{v}')$, so φ is injective.

Proof of (b). Set $\mathbf{u}^* = c^2\mathbf{u}, \mathbf{v}^* = c\mathbf{v}$, $h^* = c^2 h$, and $q^* = c\, q$. Then $u_i^* = (v_i^*)^2$ and $v_i^* \sum_{j=1}^{n} w_{ij} v_j^* = c^2 v_i \sum_{j=1}^{n} w_{ij} v_j = 0$ for $i = 1, \ldots, n$. Hence, $(\mathbf{u}^*, \mathbf{v}^*) \in \mathcal{U}$. Moreover, $g(X)(h^*)'(X) - g'(X)h^*(X) = c^2(g(X)h'(X) - g'(X)h(X)) = -c^2\, q^2(X) = -(q^*)^2(X)$, so $(h^*, q^*) \in \mathcal{F}$. Let $(h_1, q_1) = \varphi(\mathbf{u}^*, \mathbf{v}^*)$. Then,

$$\frac{h_1(X)}{g(X)} = \sum_{i=1}^{n} \frac{u_i^*}{X - t_i} = c^2 \sum_{i=1}^{n} \frac{u_i}{X - t_i} = c^2 \frac{h(X)}{g(X)},$$

and

$$\frac{q_1(X)}{g(X)} = \sum_{i=1}^{n} \frac{v_i^*}{X - t_i} = c \sum_{i=1}^{n} \frac{v_i}{X - t_i} = c \frac{q(X)}{g(X)}.$$

Hence, $h_1 = c^2 h$ and $q_1 = c\, q$, as claimed.

Proof of (c). Suppose $\gcd(g, h) = 1$. If there is $1 \leq i \leq n$ such that $v_i = 0$, then $u_i = 0$ and

$$h(X) = (X - t_i) \sum_{\substack{j=1 \\ j\neq i}}^{n} u_j \Big(\prod_{\substack{k=1 \\ k\neq i,j}}^{n} (X - t_k) \Big).$$

Thus, t_i is a root of h in F, which contradicts the coprimeness of h and g.

Conversely, suppose there exists $1 \leq k \leq n$ such that $h(t_k) = g(t_k) = 0$. Then, the partial fraction decomposition of $\dfrac{h(X)}{g(X)}$ in $F[X]$ has the form

$$\frac{h(X)}{g(X)} = \sum_{\substack{i=1 \\ i \neq k}}^{n} \frac{u_i'}{X - t_i}.$$

Since $\sum_{i=1}^{n} \frac{u_i}{X - t_i}$ is a partial fraction decomposition of $\frac{h(X)}{g(X)}$, by the its uniqueness, $u_i' = u_i$ for all $i = 1, \ldots, n$. Hence, $u_k = 0$, so $v_k = 0$.

We conclude that in the case where $\gcd(g, h) = 1$, (5.3.4) is reduced to (5.3.6).

Now, suppose $W = (w_{ij})_{i,j}$ is of rank $n - 1$. Then, the eigenvector of W with the eigenvalue 0 is uniquely determined up to constants in $F^\times$. In other words, there exists $\mathbf{v}_0 \in F^n$ such that $\{c\mathbf{v}_0 \mid c \in F\}$ is the set of solutions of (5.3.6). Set $\mathbf{u}_0 = \mathbf{v}_0^2$. Then, $(\mathbf{u}_0, \mathbf{v}_0) \in \mathcal{U}$. By (b), $(c^2\mathbf{u}_0, c\mathbf{v}_0) \in \mathcal{U}$ for all $c \in F$. Let $(\mathbf{u}, \mathbf{v}) \in \mathcal{U}$. Then, $\mathbf{u} = \mathbf{v}^2$ and $\mathbf{v}$ is an eigenvector of W with the eigenvalue 0. Hence, there exists $c \in F^\times$ with $\mathbf{v} = c\mathbf{v}_0$, so $\mathbf{u} = c^2\mathbf{v}_0^2 = c^2\mathbf{u}_0$. Therefore, $\mathcal{U} = \{(c^2\mathbf{u}_0, c\mathbf{v}_0) \mid c \in F\}$.

Let $(h_0, q_0) = \varphi(\mathbf{u}_0, \mathbf{v}_0)$. By (b), $(c^2\ h_0, c\ q_0) \in \mathcal{F}$ for all $c \in F$. Let $(h, q) \in \mathcal{F}$ and $(\mathbf{u}, \mathbf{v}) = \varphi^{-1}(h, q)$. By the preceding argument, there exists $c \in F$ such that $\mathbf{u} = c^2\mathbf{u}_0$ and $\mathbf{v} = c\mathbf{v}_0$. Again by (b), $(h, q) = \varphi(\mathbf{u}, \mathbf{v}) = (c^2\ h_0, c\ q_0)$. Therefore $\mathcal{F} = \{(c^2\ h_0, c\ q_0) \mid c \in F\}$. $\square$

Example

We give an example of polynomials $\bar{g}$, $\bar{h}$, $\bar{q} \in \mathbb{Q}[X]$ that satisfy all of the assumptions of Lemma 5.3.2, hence all of its consequences.

Let $n \geq 3$ be a positive odd integer, and let $\bar{g}(X) = X^n - X$, $\bar{h}(X) = n^2X^{n-1} - (n-2)^2$, and $\bar{q}(X) = nX^{n-1} + n - 2 \in \mathbb{Q}[X]$. Let ζ be a primitive $(n-1)$th root of unity. Then $0, 1, \zeta, \ldots, \zeta^{n-2}$ are the roots of $\bar{g}$ in $\tilde{\mathbb{Q}}$. Let

$\bar{W} = (\bar{w}_{ij})_{i,j}$ be the $n \times n$ matrix given by

$$\bar{W} = \begin{pmatrix} 0 & -1 & -\frac{1}{\zeta} & \cdots & -\frac{1}{\zeta^{n-2}} \\ 1 & 0 & \frac{1}{1-\zeta} & \cdots & \frac{1}{1-\zeta^{n-2}} \\ \frac{1}{\zeta} & \frac{1}{\zeta-1} & 0 & \cdots & \frac{1}{\zeta-\zeta^{n-2}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\zeta^{n-2}} & \frac{1}{\zeta^{n-2}-1} & \frac{1}{\zeta^{n-2}-\zeta} & \cdots & 0 \end{pmatrix}. \tag{5.3.12}$$

Lemma 5.3.3. (App.1 of [Me]) The polynomials $\bar{g}$ and $\bar{h}$ are relatively prime, and $\bar{h}$ and $\bar{q}$ are separable. Taking $g(X) = \bar{g}(X)$ in Lemma 5.3.2, the pair $(\bar{h}, \bar{q})$ satisfies the equation (5.3.5). The matrix $\bar{W}$ is the coefficient matrix of the linear system corresponding to the system (5.3.6), and it is of rank $n-1$. In other words, $\bar{h}$ and $\bar{q}$ are the unique polynomials, up to a constant, of degree $\leq n-1$ which satisfy the equation (5.3.5).

Proof. Since $\bar{h}(0) \neq 0$ and $\bar{h}(\zeta^i) = n^2 - (n-2)^2 \neq 0$, for $i = 0, \ldots, n-2$, $\bar{g}$ and $\bar{h}$ are relatively prime. Furthermore, $\bar{h}$ (resp. $\bar{q}$) and $\bar{h}'$ (resp. $\bar{q}'$) have no common root, so $\bar{h}$ (resp. $\bar{q}$) is separable.

For the equality (5.3.5), we have

$$\begin{aligned} \bar{g}(X)\bar{h}'(X) - \bar{g}'(X)\bar{h}(X) &= (X^n - X)n^2(n-1)X^{n-2} \\ &\quad - (nX^{n-1} - 1)(n^2X^{n-1} - (n-2)^2) \\ &= \Big(n^2(n-1) - n^3\Big)X^{2n-2} \\ &\quad + \Big(-n^2(n-1) + n(n-2)^2 + n^2\Big)X^{n-1} - (n-2)^2 \\ &= -n^2X^{2n-2} + (-2n^2 + 4n)X^{n-1} - (n-2)^2 \\ &= -\Big(n^2X^{2n-2} + 2n(n-2)X^{n-1} + (n-2)^2\Big) = -\bar{q}(X)^2. \end{aligned}$$

Since $\gcd(\bar{g}, \bar{h}) = 1$, by (c) of Lemma 5.3.2, the solvability of

$$\bar{g}h'(X) - \bar{g}'(X)h(X) = -q(X)^2 \tag{5.3.13}$$

in the polynomial variables $h, q \in \mathbb{Q}[X]$ is equivalent to the solvability of the system of equations

$$\sum_{i=1}^{n} \bar{w}_{ij} v_j = 0 \text{ for } i = 1, \ldots, n \tag{5.3.14}$$

with the variables $v_1, \ldots, v_n$ and with coefficient matrix $\bar{W} = (\bar{w}_{ij})_{i,j}$ as the matrix in (5.3.12).

Let $\overline{\mathcal{F}}$ be the set of all pairs of polynomials $(h, q) \in \mathbb{Q}(\zeta)[X]$ of order at most $n-1$ that satisfy (5.3.13). Observe that $(\bar{h}, \bar{q})$ is a nonzero pair in $\overline{\mathcal{F}}$. Hence, if $\bar{W}$ is of rank $n-1$, by (c) of Lemma 5.3.2, $\overline{\mathcal{F}} = \{(c^2\bar{h}, c\bar{q}) \mid c \in \mathbb{Q}(\zeta)\}$. Thus, it remains to prove that $\bar{W}$ is of rank $n-1$.

To this end observe that $\bar{W}$ is an $n \times n$ skew symmetric matrix. Since n is odd, Remark 5.3.1 implies that $\det(\bar{W}) = 0$. Thus, $\bar{W}$ is of rank $\leq n-1$. For the equality, we divide the rest of the proof into several parts.

PART A: *The matrix A.*
Consider the matrix A obtained from $\bar{W}$ by removing the 1st row and the 1st column:

$$A = \begin{pmatrix} 0 & \frac{1}{1-\zeta} & \cdots & \frac{1}{1-\zeta^{n-2}} \\ \frac{1}{\zeta-1} & 0 & \cdots & \frac{1}{\zeta-\zeta^{n-2}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\zeta^{n-2}-1} & \frac{1}{\zeta^{n-2}-\zeta} & \cdots & 0 \end{pmatrix}.$$

Set $a_1 = 0, a_2 = \dfrac{1}{1-\zeta}, a_3 = \dfrac{1}{1-\zeta^2}, \ldots, a_{n-1} = \dfrac{1}{1-\zeta^{n-2}}$. Using the identity $\frac{1}{\zeta^j - \zeta^i} = \frac{1}{\zeta^j(1-\zeta^{n-1-j+i})}$ for all i, j with $0 \leq i < j \leq n-2$, we find that the matrix A is formed by the row vectors: $(a_1, a_2, \ldots, a_{n-1})$, $\dfrac{1}{\zeta}(a_{n-1}, a_1, a_2, \ldots, a_{n-2})$, $\dfrac{1}{\zeta^2}(a_{n-2}, a_{n-1}, a_1, a_2, \ldots), \ldots$. Consider the circulant matrix

$$A' = \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}.$$

Then, the determinant of A is the product of an $(n-1)$-th root of unity and the determinant of A'. That is, there exists an integer k, such that

$$\det(A) = \zeta^k \det(A') \tag{5.3.15}$$

By (5.3.1),

$$\det(A') = \prod_{i=1}^{n-2} \Big(\frac{\zeta^i}{1-\zeta} + \frac{\zeta^{2i}}{1-\zeta^2} + \cdots + \frac{\zeta^{(n-2)i}}{1-\zeta^{n-2}} \Big). \tag{5.3.16}$$

PART B: *The ith factor of* $\det(A')$.

Consider the separable polynomial $f(X) = \dfrac{X^{n-1}-1}{X-1} = \prod_{i=1}^{n-2}(X-\zeta^i)$. Thus, in the notation of Subsection 5.3, the ith factor on the right hand side of (5.3.16) is $\mathrm{tr}_f(\dfrac{\zeta^i}{1-\zeta})$, so

$$\det(A') = \prod_{i=1}^{n-2} \mathrm{tr}_f\Big(\frac{\zeta^i}{1-\zeta} \Big). \tag{5.3.17}$$

Since $f(X) = X^{n-2} + X^{n-3} + \cdots + X + 1$, $\zeta^{i(n-2)} + \zeta^{i(n-3)} + \cdots + \zeta^i = -1$. Hence,

$$\mathrm{tr}_f(\zeta^i) = -1 \ \text{ for each } 1 \leq i \leq n-2. \tag{5.3.18}$$

It follows from the linearity of the trace that for each $2 \leq i \leq n-1$

$$\text{(5.3.19)} \qquad \mathrm{tr}_f\Big(\frac{\zeta^i}{1-\zeta}\Big) - \mathrm{tr}_f\Big(\frac{\zeta^{i-1}}{1-\zeta}\Big) = \mathrm{tr}_f\Big(\frac{\zeta^i - \zeta^{i-1}}{1-\zeta}\Big) = \mathrm{tr}_f(-\zeta^{i-1}) = 1.$$

CLAIM C : $\mathrm{tr}_f\Big(\dfrac{1}{1-\zeta}\Big) = \dfrac{n-2}{2}$.

Indeed, since $\zeta^{n-1} - 1 = 0$, we have

$$0 = \big((\zeta-1)+1\big)^{n-1} - 1$$

$$= (\zeta-1)^{n-1} + (n-1)(\zeta-1)^{n-2} + \cdots$$

$$+ \frac{(n-1)(n-2)}{2}(\zeta-1)^2 + (n-1)(\zeta-1) + 1 - 1.$$

Hence,

$$(\zeta-1)^{n-2} + (n-1)(\zeta-1)^{n-3} + \cdots + \frac{(n-1)(n-2)}{2}(\zeta-1) + (n-1) = 0.$$

Dividing the latter identity by $(\zeta-1)^{n-2}(n-1)$, we get

$$\frac{1}{n-1} + \frac{1}{\zeta-1} + \cdots + \frac{n-2}{2}\Big(\frac{1}{\zeta-1}\Big)^{n-3} + \Big(\frac{1}{\zeta-1}\Big)^{n-2} = 0.$$

Now, since n is odd, $n-3$ is even. Multiplying the latter equality by -1 and reversing the order of its left hand side, we get

$$\Big(\frac{1}{1-\zeta}\Big)^{n-2} - \frac{n-2}{2}\Big(\frac{1}{1-\zeta}\Big)^{n-3} + \cdots + \frac{1}{1-\zeta} + \frac{1}{1-n} = 0.$$

Similar equality hold if we replace ζ by ζ^i for $i = 1, \ldots, n-2$. Since $\zeta, \ldots, \zeta^{n-2}$ are distinct, we get

$$X^{n-2} - \frac{n-2}{2}X^{n-3} + \cdots + X + \frac{1}{1-n} = \prod_{i=1}^{n-2}\Big(X - \frac{1}{1-\zeta^i}\Big).$$

Hence,

$$\text{(5.3.20)} \qquad \mathrm{tr}_f\big(\frac{1}{1-\zeta}\big) = \sum_{i=1}^{n-2}\frac{1}{1-\zeta^i} = \frac{n-2}{2},$$

as claimed.

PART D: *The value of the ith factor of* $\det(A')$.
The equalities (5.3.19) and (5.3.20) imply that each $1 \leq i \leq n-2$ satisfies

$$\begin{aligned}\mathrm{tr}_f\Big(\frac{\zeta^i}{1-\zeta}\Big) &= \mathrm{tr}_f\Big(\frac{\zeta^i}{1-\zeta}\Big) - \mathrm{tr}_f\Big(\frac{\zeta^{i-1}}{1-\zeta}\Big) \\ &+ \mathrm{tr}_f\Big(\frac{\zeta^{i-1}}{1-\zeta}\Big) - \mathrm{tr}_f\Big(\frac{\zeta^{i-2}}{1-\zeta}\Big) \\ &\cdots \\ &+ \mathrm{tr}_f\Big(\frac{\zeta}{1-\zeta}\Big) - \mathrm{tr}_f\Big(\frac{1}{1-\zeta}\Big) \\ &+ \mathrm{tr}_f\Big(\frac{1}{1-\zeta}\Big) = i + \frac{n-2}{2}.\end{aligned}$$

PART E: $\bar{W}$ *is of rank* $n-1$.
Since $n \geq 3$, $i + \dfrac{n-2}{2} > 0$ for $1, \ldots, n-2$. Thus, by (5.3.17) and by Part D, $\det(A') \neq 0$. It follows from the equality (5.3.15) that $\det(A) \neq 0$. Since A is a $(n-1) \times (n-1)$ submatrix of $\bar{W}$ and $\mathrm{rank}(\bar{W}) \leq n-1$, $\bar{W}$ is of rank $n-1$. $\square$

The General Equation of degree n

We deal with the solutions of the general case.

Remark 5.3.4. Let R be an integral domain with quotient field E. Let φ be a homomorphism of R into an algebraically closed field F and use a bar to denote the images of elements of R and polynomials with coefficients in R.

If $d \in R[X]$ is a nonconstant common divisor in $E[X]$ of polynomials $f, g \in$

$R[X]$, and $\deg(\bar{d}) = \deg(d)$, then $\bar{d}$ is a nonconstant common divisor of $\bar{f}$ and $\bar{g}$ in $F[X]$.

Let $f \in R[X]$ be a polynomial of degree n whose leading coefficient is a unit of R. Suppose that f has a multiple root, $\gcd(f, f') \in R[X]$, and $\deg(\varphi(\gcd(f, f'))) = \deg(\gcd(f, f'))$. Then by the preceding paragraph, $\bar{f}$ and $\bar{f}'$ have a common root in $F[X]$, hence $\bar{f}$ has a multiple root in F. □

Let $n \geq 5$ be an odd integer and let $t_1, \ldots, t_n$ be indeterminates. For each $i = 1, \ldots, n$, set $s_i = (-1)^i \sum_{1 \leq k_1 < k_2 < \cdots < k_i \leq n} t_{k_1} t_{k_2} \cdots t_{k_i}$. Set $K = \mathbb{Q}(s_1, \ldots, s_n)$ and $L = \mathbb{Q}(t_1, \ldots, t_n)$. Then $g(X) = X^n + s_1 X^{n-1} + \cdots + s_n$ is the general polynomial of degree n. It factors over L as $g(X) = \prod_{i=1}^{n} (X - t_i)$. Moreover, L/K is a Galois extension whose Galois group is S_n (p. 272 of [La2]).

Lemma 5.3.5. (Chap. 4, Lem. 5.11 of [Mal-Mat] or Sec. 3, Prop. 1 of [Me]) There exist separable polynomials $h, q \in K[X]$ both of degree $n - 1$, such that h and g are relatively prime and

$$g(X)h'(X) - g'(X)h(X) = -q(X)^2. \tag{5.3.21}$$

Proof. The group S_n acts on $t_1, \ldots, t_n$ by the law

$$\sigma t_i = t_{\sigma i}, \quad \sigma \in S_n \text{ and } 1 \leq i \leq n. \tag{5.3.22}$$

Assuming the coprimeness of g and h, by (c) of Lemma 5.3.2, the solvability of (5.3.21) in $L[X]$ is equivalent to the solvability of the linear system of equations

$$\sum_{j=1}^{n} w_{ij} v_j = 0 \text{ for } 1 \leq i \leq n \tag{5.3.23}$$

in the variables $v_1, \ldots, v_n$ with $w_{ii} = 0$ and $w_{ij} = \dfrac{1}{t_i - t_j}$ if $i \neq j$.

Let $\mathcal{U}$ be the set all pairs $(\mathbf{u}, \mathbf{v}) \in L^{2n}$ such that $\mathbf{v}$ satisfies (5.3.23) and

$\mathbf{u} = \mathbf{v}^2$. Extend the specialization $(s_1, \ldots, s_n) \longmapsto (0, \ldots, 0, -1, 0)$ to a homomorphism φ: $\mathbb{Q}[s_1, \ldots, s_n] \longrightarrow \mathbb{Q}$. In particular, φ maps g onto $\bar{g} = X^n - X$.

PART A: *The set* $\mathcal{U}$.
The coefficient matrix $W = (w_{ij})_{i,j}$ of (5.3.23) is a skew symmetric matrix of odd dimension. By Remark 5.3.1, $\det(W) = 0$, so W is of rank $< n$. On the other hand, φ maps W onto $\bar{W}$ of (5.3.12). By Lemma 5.3.3, $\bar{W}$ is of rank $n-1$, so the rank of W is also $n-1$. By (c) of Lemma 5.3.2, there exists $(v_1, \ldots, v_n) \in L^n$ such that $\mathcal{U} = \{(c^2\mathbf{u}, c\mathbf{v}) \mid c \in L\}$ where $\mathbf{u} = \mathbf{v}^2$.

PART B: *1-Cocycle of* S_n *in* $L^\times$.
Let $\mathbf{v} = (v_1, \ldots, v_n)$ be as in PART A. By (5.3.23), $W\mathbf{v}^T = 0$. Each $\sigma \in \mathrm{Gal}(L/K)$ permutes the rows of W in the same way as it permutes $\{1, \ldots, n\}$. Hence ,

$$\sigma W \begin{pmatrix} v_{\sigma 1} \\ \vdots \\ v_{\sigma n} \end{pmatrix} = 0 \tag{5.3.24}$$

On the other hand, σ acts on the entries of W and on the v_i's as an automorphism of L. Hence,

$$\sigma W \begin{pmatrix} \sigma v_1 \\ \vdots \\ \sigma v_n \end{pmatrix} = 0 \tag{5.3.25}$$

The eigenvectors of σW appearing in (5.3.24) and (5.3.25) need not be the same. However, since the eigenvectors of W of the eigenvalue 0 are uniquely determined up to a factor from $L^\times$, so are the eigenvectors of σW of the eigenvalue 0. It follows that there exists a unique $a_\sigma \in L^\times$ such that

$$\sigma v_i = a_\sigma v_{\sigma i} \quad \text{for } 1 \leq i \leq n. \tag{5.3.26}$$

For $\tau \in S_n$, we have

$$\tau v_i = a_\tau v_{\tau i}$$
$$\sigma(\tau v_i) = \sigma a_\tau \cdot \sigma(v_{\tau i}) = (\sigma a_\tau) a_\sigma v_{\sigma\tau i}.$$

It follows by $\sigma(\tau v_i) = a_{\sigma\tau} v_i$ and by the uniqueness that $a_{\sigma\tau} = (\sigma a_\tau) a_\sigma$. Therefore, the map $f\colon S_n \longrightarrow L^\times$ given by $\sigma \longmapsto a_\sigma$ is a 1-cocycle of S_n. By Lemma 5.1.2, there exists $b \in L^\times$ such that $a_\sigma = b/\sigma b$ for each $\sigma \in S_n$. Substitution in (5.3.26) gives

$$\sigma(b\, v_i) = b\, v_{\sigma i}, \quad \text{for all } \sigma \in S_n \text{ and } 1 \le i \le n. \tag{5.3.27}$$

PART C: *Solutions of (5.3.21).*

We set $z_i = b\ v_i$ for $i = 1, \ldots, n$. Since $(v_1, \ldots, v_n)^T$ is an eigenvector of W of the eigenvalue 0, so is $(z_1, \ldots, z_n)^T$. In other words, $W(z_1, \ldots, z_n)^T = 0$, which means that $z_1, \ldots, z_n$ solves the linear system (5.3.23). For $i = 1, \ldots, n$, set $u_i = z_i^2$. It follows from (a) of Lemma 5.3.2 that there exist $h(X), q(X) \in L[X]$ that satisfy (5.3.21) with

$$\frac{h(X)}{g(X)} = \sum_{i=1}^{n} \frac{u_i}{X - t_i}, \quad \text{and} \quad \frac{q(X)}{g(X)} = \sum_{i=1}^{n} \frac{v_i}{X - t_i}.$$

For $\sigma \in S_n$ and $i = 1, \ldots, n$, by (5.3.22) and (5.3.27), $\sigma u_i = \sigma(z_i)^2 = (z_{\sigma(i)})^2 = u_{\sigma(i)}$. Hence

$$\sigma\Big(\frac{h(X)}{g(X)}\Big) = \sum_{i=1}^{n} \frac{\sigma(z_i)}{X - \sigma(t_i)} = \sum_{i=1}^{n} \frac{u_{\sigma i}}{X - t_{\sigma i}} = \frac{h(X)}{g(X)}.$$

Hence, $\frac{q(X)}{g(X)} \in K(X)$. It follows that $h(X) \in K(X) \cap L[X] = K[X]$. For the same reason, $q(X) \in K[X]$.

PART D: *Properties of h and g.*

Let h_1 and q_1 be the images in $\mathbb{Q}[X]$ of h and q under φ. By Lemma 5.3.3, h_1 and q_1 are obtained from $\bar{h} = n^2 X^{n-1} - (n-2)^2$ and $\bar{q} = nX^{n-1} + n - 2$ respectively by multiplication with nonzero constants. Hence h_1 and q_1 are separable with $\deg(h_1) = \deg(q_1) = n - 1$ and h_1 and $\bar{g}$ are relatively prime. It follows from Remark 5.3.4 that h and q are separable, each of degree $n-1$ and h and g are relatively prime. $\square$

5.4 Polynomials with Galois Group A_n

Assuming that polynomials $g(X), h(X)$ and $q(X) \in K[X]$ satisfy the equation (5.3.21) of Lemma 5.3.5 and $\mathrm{Gal}(g(X), K) \cong S_n$, for indeterminates t and u, we define polynomials $f(t, X)$ and $f^*(u, X)$ with Galois group A_n over $L(t)$ and A_{n-1} over $L(u)$ respectively, for an odd integer $n \geq 5$, where L the splitting field of g over K.

First, we recall the notions of resultant and discriminant of polynomials.

Resultants and Discriminants

(For more details, see Chap. 4, Sec. 8 of [La2]) Let R be an integral domain with quotient field E. Let $f_1(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ and $f_2(X) = b_mX^m + b_{m-1}X^{n-1} + \cdots + b_0$ be polynomials in $R[X]$. Consider the $(n+m) \times (n+m)$ matrix

$$M = \begin{pmatrix} \overbrace{\begin{matrix} a_n & a_{n-1} & \cdots & \cdots & a_0 \end{matrix}}^{n+1} & \overbrace{\begin{matrix} 0 & \cdots & \cdots & 0 \end{matrix}}^{m-1} \\ \begin{matrix} 0 & a_n & a_{n-1} & \cdots & \cdots \end{matrix} & \begin{matrix} a_0 & 0 & \cdots & 0 \end{matrix} \\ \begin{matrix} \vdots & \vdots & \vdots & \vdots & \vdots \end{matrix} & \begin{matrix} \vdots & \vdots & \vdots & \vdots \end{matrix} \\ \begin{matrix} 0 & \cdots & \cdots & 0 & \cdots \end{matrix} & \begin{matrix} \cdots & \cdots & a_1 & a_0 \end{matrix} \\ \begin{matrix} b_m & b_{m-1} & \cdots & b_0 & 0 \end{matrix} & \begin{matrix} \cdots & \cdots & \cdots & 0 \end{matrix} \\ \begin{matrix} \vdots & \vdots & \vdots & \vdots & \vdots \end{matrix} & \begin{matrix} \vdots & \vdots & \vdots & \vdots \end{matrix} \\ \begin{matrix} 0 & \cdots & 0 & b_m & b_{m-1} \end{matrix} & \begin{matrix} b_{m-2} & \cdots & \cdots & b_0 \end{matrix} \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \\ a \end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \\ a \end{matrix}}\right\} n \end{matrix}.$$

The **resultant** $\mathrm{Res}(f_1, f_2)$ of f_1 and f_2 is the element of R defined by $\mathrm{Res}(f_1, f_2) = \det(M)$.

We may consider $a_n, \cdots, a_0, b_m, \cdots b_0$ as variables and set $\mathrm{Res}(a_n, \cdots, a_0, b_m, \cdots b_0) = \det(M)$. If z is a new variable, then

$$\mathrm{Res}(za_n, \cdots, za_0, b_m, \cdots b_0) = z^m \mathrm{Res}(a_n, \cdots, a_0, b_m, \cdots b_0),$$

and

$$\mathrm{Res}(a_n, \cdots, a_0, zb_m, \cdots zb_0) = z^n \mathrm{Res}(a_n, \cdots, a_0, b_m, \cdots b_0).$$

Indeed, in $\mathrm{Res}(za_n, \cdots, za_0, b_m, \cdots b_0)$ (resp. in $\mathrm{Res}(a_n, \cdots, a_0, zb_m, \cdots zb_0)$), z is a factor of the m first rows (reps. n last rows) of the corresponding matrix M. Hence, $\mathrm{Res}(f_1, f_2)$ is homogeneous of degree m in the coefficients of f_1, and homogenous of degree n in the coefficients of f_2. Furthermore, if $f_1(X) = a_n \prod_{i=1}^{n}(X - x_i)$ and $f_2(X) = b_m \prod_{j=1}^{m}(X - y_j)$ then

$$\text{(5.4.1)} \quad \mathrm{Res}(f_1, f_2) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(x_i - y_j) \quad \text{(p. 202, Prop. 8.3 of [La2])}.$$

Consider the above polynomial $f_1(X) \in E[X]$. The **discriminant** $\mathrm{disc}(f_1)$ is given by

$$\text{(5.4.2)} \qquad \mathrm{disc}(f_1) = a_n^{2n-2} \prod_{i<j}(x_i - x_j)^2 = (-1)^{n(n-1)/2} a_n^{2n-2} \prod_{i \neq j}(x_i - x_j)$$

The discriminant can be also expressed by $\mathrm{Res}(f_1, {f_1}')$ (see p. 204, Prop. 8.5 of [La2]):

$$\text{(5.4.3)} \qquad \mathrm{disc}(f_1) = (-1)^{n(n-1)/2} \frac{1}{a_n} \mathrm{Res}(f_1, f_1').$$

Suppose ${f_1}'(X) = c(X - x_1') \cdots (X - x_{n-1}')$ with $c = na_n$. Then, by (5.4.1),

$$\begin{aligned} \mathrm{Res}(f_1, {f_1}') &= a_n^{n-1}\ n^n\ a_n^n \prod_{i=1}^{n}\prod_{j=1}^{n-1}(x_i - x_j') \\ &= a_n^{n-1} \prod_{i=1}^{n} na_n \prod_{j=1}^{n-1}(x_i - x_i') \\ &= a_n^{n-1} \prod_{i=1}^{n} f'(x_i) \end{aligned}$$

Hence, from (5.4.3)

$$\text{(5.4.4)} \qquad \mathrm{disc}(f_1) = (-1)^{n(n-1)/2} a_n^{n-2} \prod_{i=1}^{n} {f_1}'(x_i)$$

Remark 5.4.1. The Galois group $\mathrm{Gal}(f_1(X), E)$ is a subgroup of A_n if and only if $\mathrm{disc}(f_1)$ is a square in E. First, we define $\mathrm{sgn}(\sigma)$, for each $\sigma \in S_n$, to be $\mathrm{sgn}(\sigma) = (-1)^\eta$, where η is the number of pairs (i, j) with $1 \leq i < j \leq n$ such that $\sigma(i) > \sigma(j)$. We let S_n acts on $\mathbb{Z}[X_1, \ldots, X_n]$ by the rule $\sigma(X_i) = X_{\sigma i}$. Then, for $\Delta = \prod_{1 \leq i < j \leq n}(X_i - X_j)$, $\sigma(\Delta) = \mathrm{sgn}(\sigma)\Delta$. In particular, if $\sigma = (k\ l)$ with $k < l$, we get $\mathrm{sgn}(\sigma) = -1$, so $\sigma(\Delta) = -\Delta$. Indeed, in this case the number of elements of the set

$$\{(i,j) \in \{1,\ldots,n\}^2 \mid i < j \text{ and } \sigma i > \sigma j\} = \{(k,k+1),(k,k+2),\ldots,(k,l-1)\} \dot\cup \{(k+1,l),(k+2,l),\ldots,(l-1,l)\} \dot\cup \{(k,j)\}$$

is $2(l-k-1)+1$, so this number is odd. Furthermore, $\mathrm{sgn}(\tau\tau') = \mathrm{sgn}(\tau)\mathrm{sgn}(\tau')$, for $\tau, \tau' \in S_n$. It follows that $\sigma(\Delta) = \Delta$ if and only if σ is an even permutation.

Now, embed $\mathrm{Gal}(f_1, E)$ into S_n by defining $\sigma(x_i) = x_{\sigma i}$ for each $\sigma \in S_n$. For $\delta = \prod_{i<j}(x_i - x_j)$, by the preceding paragraph, $\sigma(\delta) = \delta$ if and only if $\sigma \in A_n$. It follows that $\mathrm{Gal}(f_1, E) \leq A_n$ if and only if $\delta \in E$, hence if and only if δ^2 is a square in E.

Next, observe that

$$\begin{aligned}\prod_{i \neq j}(x_i - x_j) &= \prod_{i<j}(x_i - x_j) \cdot \prod_{i>j}(x_i - x_j) = \prod_{i<j}(x_i - x_j) \cdot (-1)^{\frac{n(n-1)}{2}} \prod_{j<i}(x_j - x_i) \\ &= (-1)^{\frac{n(n-1)}{2}}\delta^2.\end{aligned}$$

It follows from (5.4.2) that $\mathrm{disc}(f_1) = a_n^{2n-2}\delta^2$. By the preceding paragraph, this implies that $\mathrm{Gal}(f_1, E) \leq A_n$ if and only if $\mathrm{disc}(f_1)$ is a square in E, as claimed. $\square$

Setup

Now, let K be a field of characteristic 0, $n \geq 5$ an integer, and $g \in K[X]$ a monic irreducible polynomial of degree n. We denote the splitting field

of g over K by L and assume that $\mathrm{Gal}(L/K) \cong S_n$. we also assume that there exist polynomials $h, q \in K[X]$ of degree $n-1$ such that q is separable, $\gcd(g,h) = 1$ and

$$gh' - g'h = -q^2 \tag{5.4.5}$$

Further let t and u be indeterminates and set

$$f(t,X) = g(X) - t \cdot h(X) \tag{5.4.6}$$

and

$$f^*(u,X) = \frac{g(X)h(u) - g(u)h(X)}{X-u} \tag{5.4.7}$$

Remark 5.4.2. Since g is a monic polynomial of degree n and h is a polynomial of degree $n-1$, both with coefficients in K, the polynomial f is monic of degree n with coefficients in $K[t]$. Moreover, since g and h are relatively prime and g is irreducible,

(i) $f(t,X)$ is irreducible in $\tilde{K}(t)[X]$ (Gauss' lemma), so f is separable as a polynomial in X.

Thus, $f(t,X) = \prod_{i=1}^{n}(X - x_i)$, where each x_i is transcendental over K, $x_1, \ldots, x_n$ are distinct and conjugate to each other. Hence

(ii) every symmetric rational function in $x_1, \ldots, x_n$ with coefficients in $K(t)$ belongs to $K(t)$.

Moreover, $x_1, \ldots, x_n$ are integral over $K[t]$, so

(iii) every symmetric polynomial in $x_1, \ldots, x_n$ with coefficients in $K[t]$ belongs to $K[t]$.

The following Lemma is due to Peter Müller (private communication).

Lemma 5.4.3. There exist $c \in K^\times$ and $p(t) \in K[t]$ such that $\mathrm{disc}(f) = cp(t)^2$

Proof. By (5.4.4), the discriminant of $f(t,X)$ is

$$\operatorname{disc}(f) = \pm \prod_{i=1}^{n} \frac{\partial f}{\partial X}(t, x_i). \tag{5.4.8}$$

In the following calculation, we use $'$ to denote derivation of polynomials in $\tilde{K}[t,X]$ with respect to X and omit X. By (5.4.5)

$$f'h - fh' = (g' - th')h - (g - th)h' = g'h - th'h - gh' + thh' = g'h - gh' = q^2.$$

Substituting x_i for X gives $f'(x_i)h(x_i) = q^2(x_i)$ for $1 \leq i \leq n$. Hence, by (5.4.8),

$$\operatorname{disc}(f) = \pm \frac{\left(\prod_{i=1}^{n} q(x_i)\right)^2}{\prod_{i=1}^{n} h(x_i)}. \tag{5.4.9}$$

By (iii) of Remark 5.4.2, both $p(t) = \prod_{i=1}^{n} q(x_i)$ and $\prod_{i=1}^{n} h(x_i)$ belong to $K[t]$.

CLAIM: $\prod_{i=1}^{n} h(x_i)$ lies in K. Indeed, we write $g(X) = \prod_{r=1}^{n}(X - t_r)$ and $h(X) = \eta \prod_{s=1}^{n-1}(X - u_s)$ with $\eta \in K^\times$ and $t_r, u_s \in \tilde{K}$ for all r and s. Using that $n-1$ is even, we get

$$\begin{aligned}
\prod_{i=1}^{n} h(x_i) &= \prod_{i=1}^{n} \Big(\eta \prod_{s=1}^{n-1} (x_i - u_s) \Big) \\
&= \eta^n \prod_{s=1}^{n-1} \prod_{i=1}^{n} (u_s - x_i) = \eta^n \prod_{s=1}^{n-1} f(u_s) \\
&= \eta^n \prod_{s=1}^{n-1} \big(g(u_s) - t\, h(u_s) \big) = \eta^n \prod_{s=1}^{n-1} g(u_s) \\
&= \eta^n \prod_{s=1}^{n-1} \prod_{r=1}^{n} (u_s - t_r) \\
&= \prod_{r=1}^{n} \Big(\eta \prod_{s=1}^{n-1} (t_r - u_s) \Big) = \prod_{r=1}^{n} h(t_r).
\end{aligned} \tag{5.4.10}$$

The right hand side of (5.4.10) is fixed by $\operatorname{Gal}(K)$, so it belongs to $K^\times$. Hence, $\prod_{i=1}^{n} h(x_i) \in K^\times$, as claimed.

We conclude that

$$\text{disc}(f) = c\, p(t)^2, \tag{5.4.11}$$

for some $c \in K^\times$. $\square$

The proof of the following Proposition is due to Wulf-Dieter Geyer (private communication). It is an essential simplification of Mestre's proof (as appears in Chap. 4, Prop. 5.12 of [Mal-Mat]). Among others, Geyer's proof avoids the calculation of inertia groups, the use of Dedekind discriminant theorem, an application of the Riemann-Hurwitz formula (which is implicit in [Mal-Mat]), and a theorem of Jordan.

Proposition 5.4.4. In the notation of Setup 5.4, $\text{Gal}(f(t,X), K(t)) \cong S_n$ and $\text{Gal}(f(t,X), L(t)) \cong A_n$.

Proof. Set $x = x_1$. Then, $g(x) - t\, h(x) = f(t,x) = 0$. Since x is transcendental over K, $h(x) \neq 0$. Hence, $t = \frac{g(x)}{h(x)}$, so

(a) $K(x)$ is a separable extension of $K(t)$ of degree n.

Since x is transcendental over K,

(b) $K(x)$ is a regular extension of K (Cor. 10.2.2 of [F-J]).

We denote the Galois closure of $K(x)/K(t)$ by F. Then, $F = K(x_1, \ldots, x_n)$. Let S be the integral closure of $K[t]$ in F. Since $K[t]$ is integrally closed, the map $t \longmapsto 0$ extends to a K-homomorphism φ of S onto a Galois extension $\bar{F}$ of K (Lem. 6.1.1 of [F-J]). Furthermore,

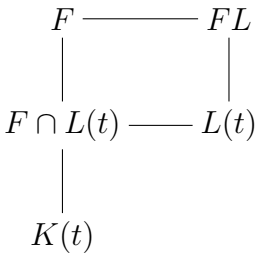
(c) φ maps $f(t,X)$ onto $g(X)$, so φ maps $x_1, \ldots, x_n$ bijectively onto $t_1, \ldots, t_n$. Hence $\varphi(\text{disc}(f)) = \text{disc}(g)$

(d) By Lemma 5.4.3, $\text{disc}(f) = c \cdot p(t)^2$, with $p \in K[t]$. Hence, by (c), $\text{disc}(g) = cp(0)^2$.

The rest of the proof breaks up into two parts.

PART A: Proof of $\mathrm{Gal}(f(t,X),K(t)) \cong S_n$.
Since $F = K(x_1,\ldots,x_n)$, $\mathrm{Gal}(F/K(t))$ is isomorphic to $\mathrm{Gal}(f(t,X),K(t))$. In particular, $\mathrm{Gal}(F/K(t))$ is isomorphic to a subgroup of S_n. The elements $x_1,\ldots,x_n$ are integral over $K[t]$, so they belong to S. It follows by (c) that $L \subseteq \bar{F}$, so $\mathrm{Gal}(L/K)$ is a quotient of $\mathrm{Gal}(\bar{F}/K)$. Since $\mathrm{Gal}(L/K) \cong S_n$, we have $|\mathrm{Gal}(\bar{F}/K)| \geq [L:K] = n!$. On the other hand, $\mathrm{Gal}(\bar{F}/K)$ is a quotient of the decomposition group D_φ of φ. Since $D_\varphi \leq \mathrm{Gal}(F/K(t))$, $|\mathrm{Gal}(F/K(t))| \geq n!$. It follows that $\mathrm{Gal}(F/K(t)) \cong S_n$.

PART B: Proof of $\mathrm{Gal}(f(t,X),L(t)) \cong A_n$. The field $FL = L(x_1,\ldots,x_n)$ is the splitting field of $f(t,X)$ over $L(t)$. Thus, $\mathrm{Gal}(FL/L(t)) \cong \mathrm{Gal}(f(t,X),L(t))$ and $\mathrm{Gal}(FL/L(t)) \cong \mathrm{Gal}(F/F\cap L(t))$.



Since L/K is Galois, $\mathrm{Gal}(F/F\cap L(t))$ is a normal subgroup of $\mathrm{Gal}(F/K(t))$. Since $n \geq 5$ odd integer, it follows from PART A that $\mathrm{Gal}(F/F\cap L(t))$ is either trivial, or $\mathrm{Gal}(F/F\cap L(t)) \cong A_n$, or $\mathrm{Gal}(F/F\cap L(t)) \cong S_n$.

By (d) and (5.4.2), $\mathrm{disc}(g) = c\,p(0)^2 = \prod_{i<j}(t_i - t_j)^2$ is a square in L, hence so is c. Hence $\mathrm{disc}(f) = c\,p(t)^2$ is a square in $L(t)$. It follows from Remark 5.4.1 that $\mathrm{Gal}(FL/L(t))$ is a subgroup of A_n. By (a) and (b) $[L(x):L(t)] = n > 1$, so $\mathrm{Gal}(FL/L(t)) \neq 1$. We conclude that $\mathrm{Gal}(FL/L(t)) = A_n$. $\square$

Remark 5.4.5. Let $i \in \{1,\ldots,n\}$ and denote $\mathrm{Stab}_{S_n}(i) = \{\sigma \in S_n \mid \sigma(i) = i\}$ the stabilizer of i in S_n. Then, $\mathrm{Stab}_{S_n}(i)$ is the group of all permutations

of $\{1,\dots,n\} \setminus \{i\}$. That is, $\mathrm{Stab}_{S_n}(i) \cong S_{n-1}$. It follows that $\mathrm{Stab}_{A_n}(i)$ is the group of even permutation in S_{n-1} which is A_{n-1}.

Corollary 5.4.6. $\mathrm{Gal}(f^*(u,X),K(u)) \cong S_{n-1}$ and $\mathrm{Gal}(f^*(u,X),L(u)) \cong A_{n-1}$.

Proof. Since u is transcendental over K, $h(u) \neq 0$ and the element $t^* = \frac{g(u)}{h(u)}$ is also transcendental over K. Moreover, $K(t^*) \subseteq K(u)$ and $L(t^*) \subseteq L(u)$. Let $\widetilde{f(t^*,X)} = \prod_{i=1}^{n}(X - x_i^*)$ be the factorization of $f(t^*,X)$ into linear factors in $\widetilde{K(t^*)}$. By Proposition 5.4.4,

$$\mathrm{Gal}(f(t^*,X),K(t^*)) \cong S_n \text{ and } \mathrm{Gal}(f(t^*,X),L(t^*)) \cong A_n. \tag{5.4.12}$$

Furthermore,

$$\begin{aligned}\prod_{i=1}^{n}(X - x_i^*) = f(t^*,X) = f\Big(\frac{g(u)}{h(u)},X\Big) &= g(X) - \frac{g(u)}{h(u)}h(X) \\ &= \frac{g(X)h(u) - g(u)h(X)}{h(u)}.\end{aligned} \tag{5.4.13}$$

Hence, u is a root of the right hand side of (5.4.13), that is u is equal to one of the roots of the left hand side, say $u = x_1^*$. Moreover

$$f^*(u,X) = \frac{g(X)h(u) - g(u)h(X)}{X - u} = h(u)\prod_{i=2}^{n}(X - x_i^*).$$

Thus, by (5.4.12), $\mathrm{Gal}(f^*(u,X),K(u))$ (resp. $\mathrm{Gal}(f^*(u,X),L(u))$) is the stabilizer of x_1^* in S_n (resp. A_n). Hence, by Remark 5.4.5, $\mathrm{Gal}(f^*(u,X),K(u)) \cong S_{n-1}$ and $\mathrm{Gal}(f^*(u,X),L(u)) \cong A_{n-1}$ as desired. □

The Case of the General Polynomial

For an odd integer $n \geq 5$, let $t_1,\dots,t_n$ be indeterminates, and $s_i = (-1)^i \sum_{1\leq k_1<k_2<\cdots<k_i\leq n} t_{k_1}t_{k_2}\cdots t_{k_i}$, for $i = 1,\dots,n$. Set $K = \mathbb{Q}(s_1,\dots,s_n)$, and $L = \mathbb{Q}(t_1,\dots,t_n)$. Then, L is the splitting field of the general polynomial $g(X) = X^n + s_1X^{n-1} + \cdots + s_n$ over K, and $\mathrm{Gal}(L/K) \cong S_n$

(p. 272 of [La2]). By Lemma 5.3.5, there exist separable polynomials $h, q \in K[X]$ each of degree $n-1$ such that g and h are relatively prime, and $g(X)h'(X) - g'(X)h(X) = -q(X)^2$. Thus g, h and q satisfy the conditions of Setup 5.4. Using Proposition 5.4.4 and Corollary 5.4.6, we summarize the result as follows.

Proposition 5.4.7. Let $n \geq 5$ be an odd integer and $\mathbf{t} = (t_1, \ldots, t_n)$ be a n-tuple of indeterminates. Set

$$g(\mathbf{t}, X) = (X - t_1)(X - t_2) \cdots (X - t_n).$$

Then, there exists a polynomial $h \in \mathbb{Q}(\mathbf{t})[X]$ of degree $n-1$ such that, for an indeterminate u

$$\text{Gal}(g(\mathbf{t}) - u\, h(\mathbf{t}, X), \mathbb{Q}(\mathbf{t}, u)) \cong A_n. \tag{5.4.14}$$

Moreover,

$$\text{Gal}\Big(\frac{g(\mathbf{t}, u)h(\mathbf{t}, X) - g(\mathbf{t}, X)h(\mathbf{t}, u)}{X - u}, \mathbb{Q}(\mathbf{t}, u)\Big) \cong A_{n-1}. \tag{5.4.15}$$

5.5 Realization of A_n

We use Proposition 5.4.7 and the results from Section 5.2 to realize A_n over $\mathbb{Q}$ in $\mathbb{Q}_{\text{tot},p}$.

Lemma 5.5.1. Let $f \in \mathbb{Q}(t_1, \ldots, t_r)[X]$ be a separable polynomial of degree ≥ 1 in X and p a prime number. Set $G = \text{Gal}(f(\mathbf{t}, X), \mathbb{Q}(\mathbf{t}))$. Suppose there exist $a_1, \ldots a_r \in \mathbb{Q}$ such that $\deg(f(\mathbf{a}, X)) = \deg_X(f(\mathbf{t}, X))$, and $f(\mathbf{a}, X)$ is separable and totally splits over $\mathbb{Q}_p$. Then G can be realized over $\mathbb{Q}$ in $\mathbb{Q}_p$.

Proof. Dividing $f(\mathbf{t}, X)$ by its leading coefficient, we may assume that $f(\mathbf{t}, X)$ is a monic polynomial in $\mathbb{Q}(\mathbf{t})[X]$. Using Proposition 5.2.4, there exits a separable Hilbert subset H of $\mathbb{Q}^r$ such that $\text{Gal}(f(\mathbf{b}, X), \mathbb{Q}) \cong G$ for all $\mathbf{b} \in H$. If $\mathbf{b} \in H$ is p-adically close to $\mathbf{a}$, then $f(\mathbf{b}, X)$ is p-adically close to $f(\mathbf{a}, X)$. By Corollary 4.2.3, $f(\mathbf{b}, X)$ totally splits over $\mathbb{Q}_p$. By Lemma 5.2.3, there

exists $\mathbf{b}_0 \in H$ which is p-adically closed to $\mathbf{a}$. Hence, $f(\mathbf{b}_0, X)$ is irreducible separable over $\mathbb{Q}[X]$ with $\mathrm{Gal}(f(\mathbf{b}_0, X), \mathbb{Q}) \cong G$ and totally splits in $\mathbb{Q}_p$. It follows that the splitting field L of $f(\mathbf{b}, X)$ over $\mathbb{Q}$ is a Galois extension of $\mathbb{Q}$ which is contained in $\mathbb{Q}_p$ with Galois group G. $\square$

Theorem 5.5.2. *Each alternating group can be realized as a Galois group over $\mathbb{Q}$ in $\mathbb{Q}_{tot,p}$ for every prime number p.*

Proof. The group A_3 can be realized over $\mathbb{Q}$ in $\mathbb{Q}_p$ by Proposition 2.2.5, since $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Hence, it suffices to prove that for every odd integer $n \geq 5$ both A_n and A_{n-1} can be realized over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$. To this end, let g, h, and $f(\mathbf{t}, u, X) = g(\mathbf{t}, X) - u\ h(\mathbf{t}, X)$ be as in Proposition 5.4.7. Then $\mathrm{Gal}(f(\mathbf{t}, u, X), \mathbb{Q}(\mathbf{t}, u)) \cong A_n$. Choose $a_1, \ldots, a_n \in \mathbb{Z}$ such that $h(a_1, \ldots a_n, X)$ is well defined. Since $g(\mathbf{t}) = (X - t_1) \cdots (X - t_n)$, $f(\mathbf{a}, 0, X) = (X - a_1) \cdots (X - a_n)$ totally splits in $\mathbb{Q}$, hence also in $\mathbb{Q}_p$. By Lemma 5.5.1, A_n can be realized over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$.

Next, set

$$f^*(\mathbf{t}, u, X) = \frac{g(\mathbf{t}, u)h(\mathbf{t}, X) - g(\mathbf{t}, X)h(\mathbf{t}, u)}{X - u}.$$

By Proposition 5.4.7, $\mathrm{Gal}(f^*(\mathbf{t}, u, X), \mathbb{Q}(\mathbf{t}, u)) \cong A_{n-1}$. Moreover

$$f^*(\mathbf{a}, a_n, X) = \Big(\prod_{i=1}^{n}(a_n - a_i)\Big)\frac{h(\mathbf{a}, X)}{X - a_n} - \frac{\prod_{i=1}^{n}(X - a_i)}{X - a_n}h(\mathbf{a}, a_n)$$

$$= -\Big(\prod_{i=1}^{n-1}(X - a_i)\Big)h(\mathbf{a}, a_n)$$

totally splits in $\mathbb{Q}$, hence also in $\mathbb{Q}_p$. Again by Lemma 5.5.1, A_{n-1} can be realized over $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},p}$, as desired. $\square$

Bibliography

[Ba] M. Bauer, *Ganzzahlige Gleichungen ohne Affekt*, Mathematische Annalen **64** (1907), 325-327.

[Bo] N. Bourbaki, *Commutative Algebra*, Springer, Berlin (1989).

[C-F] J. W. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London (1967).

[E-P] A.J. Engler and A. Prestel, *Valued Fields*, Springer-Verlag, Berlin (2005).

[F-J] M. D. Fried and M. Jarden, *Field Arithmetic* (Third Edition), Springer-Verlag, Berlin (2008).

[I-R] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Secon Edition), Springer-Verlag Graduate Texts in Mathematics **84** (1990).

[Jan] G. Janusz, *Algebraic Number Fields*, Academic Press, New York (1973).

[Jar] M. Jarden, *Intersection of local algebraic extensions of a Hilbertian field*, NATO ASI Series C **333** (1991), 343-405.

[La1] S. Lang, *Introduction to Algebraic Geometry*, Interscience Publishers, New York (1958).

[La2] S. Lang, *Algebra* (Third Edition), Springer-Verlag Graduate Texts in Mathematics **211** (2002).

[Mal-Mat] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer-Verlag, Berlin (1999).

[Me] J. F. Mestre, *Extension régulière de $\mathbb{Q}(T)$ de groupe de Galois de A_n*, Journal of Algebra **131** (1990), 483-495.

[Mo-Bal] L. Moret-Bailly, *Groups de Picard et problémes de Skolem II*, Annals Scientifiques de l'Ecole Normale Superieure **22** (1989), 181-194.

[Po] F. Pop, *Embedding problems over large fields*, Annals of Mathematics **144** (1996), 1-34.

[Se] J. P. Serre, *Local Fields*, Springer, New York (1979).

[Vo] H. Völklein, *Groups as Galois Groups*, Cambridge University Press (1996).