TOPLOGICAL METHODS IN GALOIS THEORY

by

Yuri Burda

A thesis submitted in conformity with the requirements for the degree of Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto

Copyright © 2012 by Yuri Burda
Abstract

Topological Methods in Galois Theory

Yuri Burda

Doctor of Philosophy

Graduate Department of Mathematics

University of Toronto

2012

This thesis is devoted to application of topological ideas to Galois theory. In the first part we obtain a characterization of branching data that guarantee that a regular mapping from a Riemann surface to the Riemann sphere having this branching data is invertible in radicals. The mappings having such branching data are then studied with emphasis on those exceptional properties of these mappings that single them out among all mappings from a Riemann surface to the Riemann sphere. These results provide a framework for understanding an earlier work of Ritt on rational functions invertible in radicals. In the second part of the thesis we apply topological methods to prove lower bounds in Klein’s resolvent problem, i.e. the problem of determining whether a given algebraic function of \(n\) variables is a branch of a composition of rational functions and an algebraic function of \(k\) variables. The main topological result here is that the smallest dimension of the base-space of a covering from which a given covering over a torus can be induced is equal to the minimal number of generators of the monodromy group of the covering over the torus. This result is then applied for instance to prove the bounds \(k \geq \lceil \frac{n}{2} \rceil\) in Klein’s resolvent problem for the universal algebraic function of degree \(n\) and the answer \(k = n\) for generic algebraic function of \(n\) variables of degree \(m \geq 2n\).
Acknowledgements

I would like to thank my family (and especially my parents Andrey and Irina) for their unlimited love and support.

I would like to thank my dear advisor, Askold Khovanskii, for showing me how beautiful mathematics can be.

I would like to thank Edward Bierstone, Ida Bulat, Yael Karshon, Boris Khesin, Stephen Kudla, Misha Mazin, Pierre Milman, Lev and Vladimir Radzivilovskii, Zinovy Reichstein and Sergei Yakovenko for providing valuable advice when it was much needed.

I would like to thank my friends (and especially Konstantin Livanov) for making writing this thesis so much more enjoyable.

I would like to thank my angel Liudmyla Kadets for being what she is.

I would like to thank my teachers and my students for providing me the opportunity to learn so many valuable lessons.
Contents

1 Introduction .................................................. 1
   1.1 The subject of topological Galois theory .................. 1
   1.2 Rational functions invertible in radicals ................. 3
   1.3 Simplifying algebraic equations ......................... 5
      1.3.1 Simplification of the quintic ..................... 5
      1.3.2 Hilbert’s 13th problem — a short history .......... 6
      1.3.3 Arnold’s work on an algebraic version of Hilbert’s 13th problem ... 8
      1.3.4 Klein’s resolvent problem ....................... 10
      1.3.5 Methods for obtaining bounds in Klein’s resolvent problem .... 11
      Low-dimensional birational geometry .................. 11
      Essential dimension of groups ....................... 13
      Topological methods .................................. 16
   1.4 Main results of the thesis .............................. 17

2 Local branching and rational functions invertible in radicals .... 19
   2.1 Conventions .......................................... 22
   2.2 Non-hyperbolic Galois branched coverings over the Riemann sphere ... 22
   2.3 Auxiliary definitions and results ...................... 24
   2.4 Characterization by local branching ................... 25
   2.5 When branching data implies global properties .......... 30
3.7.1 Algebraic functions on the algebraic torus ........................................ 73
3.7.2 Application to Universal Algebraic Function ................................... 76
3.7.3 Lower Bound from Local Monodromy Around a Flag ..................... 79
3.7.4 Essential dimension at a prime $p$ ................................................. 83
3.7.5 Generic algebraic function of $k$ parameters and degree $\geq 2k$ can’t
be simplified .......................................................................................... 84

Bibliography ............................................................................................ 90
Chapter 1

Introduction

1.1 The subject of topological Galois theory

This thesis deals with applications of topological methods and ideas to problems in Galois theory.

One of the classical questions that Galois theory is whether it is possible to solve a given irreducible algebraic equation \( x^n + a_1 x^{n-1} + \ldots + a_n = 0 \) with coefficients in a field \( K \) of characteristic zero by radicals. To formalize this question the following definitions can be used:

**Definition 1.** A field extension \( L/K \) is radical if there exists a tower of extensions \( K = K_0 \subset K_1 \subset \ldots \subset K_n \) such that \( L \subset K_n \) and for any \( i \), \( K_{i+1} \) is obtained from \( K_i \) by adjoining an element \( a \) satisfying \( a^n = b \) for some \( b \in K_i \).

**Definition 2.** An equation \( x^n + a_1 x^{n-1} + \ldots + a_n = 0 \) is solvable in radicals over a field \( K \) containing its coefficients if the field extension \( K(x)/K \) is radical.

To treat the question of solvability of an equation in radicals one introduces the notion of Galois group of a field extension:

**Definition 3.** Fix an algebraic closure \( \overline{K} \) of \( K \). Let \( \overline{L} \) be the normal closure of \( L \) in \( \overline{K} \). The Galois group of a field extension \( L/K \) is the group of automorphisms of \( \overline{L} \) over \( K \).
Chapter 1. Introduction

One proves in Galois theory that the Galois group of any radical extension is solvable. Thus an equation $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ with coefficients in a field $K$ with non-solvable Galois group over $K$ (i.e. the Galois group of the extension $K(x)/K$) is not solvable in radicals.

In the case when $K$ is a function field of a complex algebraic variety $X$, one can approach the problem differently. Namely one considers the monodromy group of the algebraic function defined by the equation $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ and the monodromy group of any algebraic function defined using rational functions on $X$, arithmetical operations and extracting radicals. One shows that the latter monodromy group is always solvable, so an algebraic function with non-solvable monodromy group is not representable in radicals (see [1] and [18] where this approach is being made precise).

These two approaches are parallel to each other as one can prove that the monodromy group of an algebraic function is isomorphic to the Galois group of the equation that defines it over the field of rational functions in the parameters of the function.

The advantage of the latter approach is that it can be applied even if one steps outside the realm of algebraic extensions. For instance one can prove the following result by topological methods [18]:

**Theorem 1.** If an algebraic function has a non-solvable monodromy group, then it can’t be represented using arithmetic operations, radicals, single-valued analytic mappings with at most countably many singular points, differentiation and integration.

This theorem shows that in some situation topological reasons for impossibility of representation of a function using some allowed operations give stronger results than algebraic reasons.

The second part of this thesis is devoted to describing a topological reason for non-representability of some algebraic functions of $n$ variables as compositions of rational functions and one algebraic function of $k$ variables for a certain $k \leq n$. The fact that the reason is topological in nature allows one to extend the results to the case when “one
algebraic function of $k$ parameters" in question is replaced by “one multivalued function of $k$ parameters with finitely or infinitely many values whose values are all distinct outside an algebraic subvariety in the space of parameters” \(^1\).

The author of this thesis has learned about theorem \(^1\) from a course of A. G. Khovanskii called “Galois theory and Riemann surfaces”. Another impressive theorem that the author has learned from that course is as follows \(^2\):

**Theorem 2.** Let $f : R \to \mathbb{CP}^1$ be any regular function of degree 23 from a Riemann surface $R$ of genus 1, 2, 3, 6, 7, 12, 17 or 23 to the Riemann sphere. The mapping $f$ is not invertible in radicals \(^2\).

The results presented in the first part of this thesis have flavour similar to the theorem mentioned above. For instance we can prove: a rational mapping of prime degree with at least 5 critical values is not invertible in radicals.

An additional reason for citing Theorems \(^1\) and \(^2\) above is the profound effect that the course by A. G. Khovanskii has had on the author and its influence on the choice of subject for the research undertaken during author’s PhD program.

### 1.2 Rational functions invertible in radicals

**Example 1.** The function $w = R(z) = z^n$ is invertible in radicals for any $n$: $z = \sqrt[n]{w}$.

**Example 2.** The Chebyshev polynomial $w = T_n(z)$ defined by the formula $T_n(\cos \alpha) = \cos n\alpha$ is invertible in radicals for any $n$:

$$w = \frac{1}{2} \left( \sqrt[w]{w + \sqrt{w^2 - 1}} + \sqrt[w]{w - \sqrt{w^2 - 1}} \right)$$

(see \(^2\).10 below).

---

\(^1\)Since this generality seems to be unnecessary at this point, we formulate our theorems for algebraic functions

\(^2\)A function $f : R \to S$ between Riemann surfaces $R$ and $S$ is invertible in radicals if the field extension $\mathbb{C}(R)/f^*(\mathbb{C}(S))$ is radical
It is natural to ask whether it is possible to describe all the rational functions on the Riemann sphere that are invertible in radicals. Unfortunately this question seems to be too hard to be approachable. However some classes of rational functions invertible in radicals can be described explicitly. Especially noteworthy is the following result of Ritt:

**Theorem 3.** Let $f : \mathbb{CP}^1 \to \mathbb{CP}^1$ be a polynomial invertible in radicals. Then $f$ is a composition of linear polynomials, polynomials $z \to z^n$, Chebyshev polynomials and polynomials of degree 4.

More generally, a rational function can always be written as a composition of rational functions which are indecomposable in the sense of composition. Moreover, the composition of functions is invertible in radicals if and only if each one of the functions appearing in the composition is invertible in radicals. Thus to study rational functions invertible in radicals, it is enough to study only those rational functions invertible in radicals which are indecomposable in the sense of composition.

A group-theoretic result of Burnside can be used to show that the degree of a rational function invertible in radicals that is indecomposable in the sense of composition is a power of a prime number.

Ritt has studied the case of rational functions invertible in radicals of prime degree. Remarkably, Ritt has found that a rational function of prime degree is invertible in radicals if and only if it is one of the functions related to multiplication theorems for exponential, trigonometric or certain elliptic functions (see section 2.4 for a precise description).

The results of the first part of this thesis provide a framework that explains and generalizes Ritt’s results for rational functions of prime degree invertible in radicals. It turns out that sometimes the local branching of the rational mapping guarantees that the mapping with such local branching is invertible in radicals. **Theorem 26** classifies all possible such branching types. In particular all rational functions of prime degree...
invertible in radicals have this branching type. The rest of the first part of the thesis deals with the question of explicit description of the functions having such branching types, their characterizations in other terms and their possible multidimensional generalizations.

1.3 Simplifying algebraic equations

1.3.1 Simplification of the quintic

Galois theory can be used to show that generic algebraic equation of degree 5 or higher is not solvable in radicals. One can ask whether such equation can be solved using other multivalued functions, rather than radicals. Questions of this type have been studied by classics such as Hermite:

**Theorem 4.** One can make a rational change of variables \( y = R(z, a_1, \ldots, a_5) \) in the equation \( z^5 + a_1 z^4 + \ldots + a_5 = 0 \) so that \( y \) satisfies an equation of the form

\[
y^5 + ay^3 + by + b = 0
\]

with \( a, b \) which are rational functions of \( a_1, \ldots, a_5 \). Moreover, \( z \) can be expressed as a rational function of \( y \) and \( a_1, \ldots, a_5 \).

More generally we say that an algebraic equation \( E_1 \) in \( z \) with parameters \( a_1, \ldots, a_n \) can be reduced to an algebraic equation \( E_2 \) in \( y \) by means of a rational change of variables if the parameters of the equation \( E_2 \) are rational functions in \( a_1, \ldots, a_n \) and the function \( z \) is (perhaps a branch of) a rational function of \( y \) and \( a_1, \ldots, a_n \).

We also say that the algebraic equation \( E_1 \) in \( z \) can be reduced to an algebraic equation \( E_2 \) in \( y \) by means of a change of variables involving a given collection of algebraic functions \( A \) if the parameters of the equation \( E_2 \) are (branches of) rational functions in \( a_1, \ldots, a_n \) and functions from \( A \) and the function \( z \) is (a branch of) a rational function of \( y, a_1, \ldots, a_n \) and functions from the collection \( A \).
Bring has shown that if one allows changes of variables involving radicals, the general quintic equation can be reduced to a form that depends on one parameter only:

**Theorem 5.** The equation $z^5 + a_1 z^4 + \ldots + a_5 = 0$ can be reduced to an equation of the form

$$y^5 + y + a = 0$$

by means of a change of variables involving radicals.

The algebraic equation $z^n + a_1 z^{n-1} + \ldots + a_n = 0$ can be reduced by means of a rational substitution to an equation that depends on $n - 3$ algebraically independent parameters. The question about possibility to reduce this equation to an equation depending on even smaller number of parameters has been considered by classical mathematicians like Klein and Kronecker. Following Chebotarev, we will be referring to this problem as "Klein’s resolvent problem”.

### 1.3.2 Hilbert’s 13th problem — a short history

Hilbert was interested in the question about the possibility to simplify an algebraic equation by means of solving auxiliary equations that depend on a small number of parameters. Problem 13 in his famous list of 21 problems asks whether it is possible to express the algebraic function of 3 variables defined by the equation

$$z^7 + a z^3 + b z^2 + c z + 1 = 0$$

as a composition of continuous functions of two parameters.

In this formulation the question has been successfully resolved by Kolmogorov and Arnold. They proved the following surprising result:

**Theorem 6.** Any continuous function $f$ on $[0,1]^n$ can be written as composition of functions of one variable and the operation of addition.
This result shows that a germ of the algebraic function defined by the equation $z^7 + \alpha z^3 + \beta z^2 + \gamma z + 1 = 0$ can indeed be written as a composition of continuous functions of two variables, but it doesn’t tell whether it is possible to represent it as a composition of smooth, analytic or algebraic functions. It is known in fact that there are functions that cannot be written as such a composition [35]:

**Theorem 7.** There exists a germ of analytic function of $n$ variables that is not a composition of analytic functions of smaller number of variables.

In fact it can be proved that the set of analytic functions of $n$ variables representable as compositions of analytic functions of smaller number of variables is very small.

The situation is a bit better with representations of algebraic functions as compositions of entire algebraic functions of one variable. The following theorem is due to A. Khovanskii [19]:

**Theorem 8.** Suppose that an algebraic function is representable as a branch of a composition of entire algebraic functions of one variable and entire functions of several variables. Then the local monodromy group of this function at any point is solvable.

**Corollary 9.** The algebraic function defined by the equation $z^5 + \alpha z + \beta = 0$ is not a branch of a composition of entire algebraic functions of one variable and analytic functions of several variables.

The proof of the theorem is based on the observation that the local monodromy of an algebraic function of one variable at any point is a cyclic group. Moreover, the notion of local monodromy is preserved by means of continuous mappings, and hence the local monodromy of a composition of continuous functions and entire algebraic functions of one variable must be a solvable group. The local monodromy of the function defined by $z^5 + \alpha z + \beta = 0$ at the origin is isomorphic to the symmetric group $S_5$ and hence isn’t solvable.
1.3.3 Arnold’s work on an algebraic version of Hilbert’s 13th problem

Arnold has noticed that usual formula

$$z = \sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}}$$  (1.1)

for the solution of the cubic equation \(z^3 + 3pz + 2q = 0\) in radicals doesn’t use the operation of division. He also noticed that the actual solution is only one branch of the 18-valued function defined by the formula (1.1). This has motivated him to ask whether a given algebraic function can be written as an exact composition (i.e. a composition taking all branches into account) of algebraic functions of small number of variables and polynomial functions. He proved the following results [2]:

**Theorem 10.** If an algebraic function on an irreducible algebraic variety \(X\) with a primitive monodromy group can be written over a Zariski open subset of \(X\) as an exact composition of algebraic and rational functions, then only one of the functions in the composition is multivalued, while the rest are single-valued rational functions.

**Theorem 11.** The algebraic function defined by the equation \(z^n + a_1z^{n-1} + \ldots + a_n = 0\) cannot be written as an exact composition of polynomial functions of any number of variables and algebraic functions of \(<\phi(n)\) variables, where \(\phi(n)\) is \(n\) minus the number of ones appearing in the binary representation of the number \(n\).

The first result uses only two simple facts:

1. The monodromy group of an algebraic function over an irreducible variety \(X\) coincides with its monodromy group over any of the Zariski open subsets of \(X\).

2. The monodromy group of a composition of algebraic functions acts imprimitively on a generic fiber of the composition.
This result serves as one of the motivations for studying Klein’s resolvent problem later in this thesis.

The bound $\phi(n)$ from theorem 11 has been later improved to $n - 1$ by Lin. The answer $n - 1$ is in fact the exact answer, as one can get rid of the coefficient at $z^{n-1}$ in $z^n + a_1 z^{n-1} + \ldots + a_n = 0$ by means of a polynomial change of variables $w = z + \frac{a_1}{n}$.

What interests us in theorem 11 is its proof. The proof is based on the idea of associating with any unramified algebraic function a characteristic cohomology class on the parameter space of the function. The word “characteristic” here means that it behaves naturally with respect to pull-backs: the cohomology class associated to the pullback of a function is the pullback of the class associated to the function. Thus if the cohomology class associated to a given function doesn’t vanish in degree $k$, then the function can’t be induced from any algebraic function on a space of dimension smaller than $k$.

To make this idea work one has to do two things: construct some characteristic classes for unramified algebraic functions and compute their values for the algebraic functions of interest (the most interesting of these functions being the universal algebraic function $z^n + a_1 z^{n-1} + \ldots + a_n = 0$).

For both tasks it is necessary to study the cohomology groups of the complement to the discriminant hypersurface of the equation $z^n + a_1 z^{n-1} + \ldots + a_n = 0$. Indeed, the universal algebraic function defined by this equation has the property that every unramified algebraic function can be induced from it. Thus the cohomology classes in the base-space of this function are in fact all possible characteristic classes for unramified algebraic functions.

Computation of the cohomology groups of this space (which turns out to be also the Eilenberg-Maclane $K(\pi, 1)$ space for the braid group of $n$ strands) with coefficients in $\mathbb{Z}_2$ has been carried out by D. Fuchs in 13 and it turns out that the highest degree of a non-vanishing cohomology class is $\phi(n)$. The bound $\phi(n)$ can be improved somewhat by computing the cohomology groups of the braid group with coefficients other than $\mathbb{Z}_2$ as
Chapter 1. Introduction

has been done in [33] and [32].

1.3.4 Klein’s resolvent problem

While Lin’s theorem tells that it is impossible to reduce the equation $z^n + a_1 z^{n-1} + \ldots + a_n = 0$ to an equation depending on less than $n - 1$ parameters by means of a polynomial change of variables, it is possible when $n \geq 5$ to reduce this equation to an equation that depends on $n - 3$ parameters by means of a rational change of variables. This reduction is of course only valid outside of the set where the rational functions in question are not defined, i.e. it is valid on a Zariski open subset of the space of parameters.

In a similar fashion the function defined by the equation $z^5 + az + b = 0$ can’t be written as a composition of entire algebraic functions of one variable and entire functions of any number of variables by Corollary 9. However the substitution $w = \frac{b}{a} z$ reduces the equation $z^5 + az + b = 0$ to the equation $w^5 + c z + c = 0$ depending on one parameter $c = \frac{a^5}{b^4}$. The reduction is valid on the set defined by the inequalities $a \neq 0, b \neq 0$.

The reason the local monodromy group fails to be an obstruction to representation of an algebraic function as a composition of algebraic functions of one variable and rational functions is that the notion of locality is not preserved by discontinuous rational mappings.

Thus it is of great interest to study whether a given algebraic function can be written as an exact composition of algebraic functions of $k$ variables and rational functions. By the result of theorem 10 for algebraic functions with primitive monodromy group it is equivalent to the following question:

**Question 1.** (Klein’s resolvent problem) Given an algebraic function $z$ on an irreducible variety $X$ what is the smallest number $k$ such that the function $z$ can be written as a composition of rational functions and one algebraic function $w$ on some variety $Y$ of dimension $\leq k$?
Chapter 1. Introduction

The second part of this thesis is devoted to a topological method of proving estimates in this question and some of its variants:

Question 2. (*Klein’s resolvent problem, non-exact representation*) Given an algebraic function $z$ on an irreducible variety $X$ what is the smallest number $k$ such that the function $z$ can be written as a branch of a composition of rational functions and one algebraic function $w$ on some variety $Y$ of dimension $\leq k$?

Question 3. (*Klein’s resolvent problem with auxiliary irrationalities*) Given an algebraic function $z$ on an irreducible variety $X$ and a collection $A$ of algebraic functions, what is the smallest number $k$ such that the function $z$ can be written as a branch of a composition of rational functions of the coordinates on $X$ and functions from the collection $A$ and one algebraic function $w$ on some variety $Y$ of dimension $\leq k$?

1.3.5 Methods for obtaining bounds in Klein’s resolvent problem

Low-dimensional birational geometry

The first interesting results in Klein’s resolvent problem belong to Hermite and Kronecker. As we mentioned above, Hermite has proved that the general quintic equation $z^5 + a_1z^4 + \ldots + a_5 = 0$ can be reduced by means of a rational change of variables to an equation $y^5 + ay^3 + by + b = 0$ depending on two parameters. Kronecker has contemplated the problem whether this equation can be further reduced to an equation depending on one parameter only. He was able to prove the following:

Theorem 12. *The algebraic equation* $z^5 + a_1z^4 + \ldots + a_5 = 0$ *can’t be reduced to an equation depending on one parameter by means of a change of variables that involves rational functions of the parameters* $a_1, \ldots, a_5$ *and square root of the discriminant.*

To demonstrate the main idea from the proof of this theorem, we prove here a simpler version of the theorem:
Theorem 13. The algebraic equation $z^5 + a_1z^4 + \ldots + a_5 = 0$ can’t be reduced to an equation depending on one parameter by means of a rational change of variables.

Proof. Suppose that we can write $z$ as $z = R(y(c(a)), a)$ where $a = (a_1, \ldots, a_5)$, while $c(a)$ and $R(y, a)$ are rational functions. Since coefficients of an equation are symmetric functions of its parameters, we get a rational mapping $r : \mathbb{C}^5 \to C \subset \mathbb{C}^5$ mapping 5-tuples $z_1, \ldots, z_5$ of the roots of the equation $z^5 + a_1z^4 + \ldots + a_5 = 0$ to 5-tuples $y_1, \ldots, y_5$ of the values of the function $y$. The image of this mapping is an algebraic curve $C$, and the mapping itself is equivariant with respect to the $S_5$ action on the source and target spaces: if $r(z_1, \ldots, z_5) = (y_1, \ldots, y_5)$, then for any permutation $\sigma \in S_5$, $r(z_{\sigma(1)}, \ldots, z_{\sigma(5)}) = (y_{\sigma(1)}, \ldots, y_{\sigma(5)})$.

The domain of the mapping $r$ contains at least one line which is not mapped to a point by means of $r$. The restriction of $r$ to this line is a rational mapping of the Riemann sphere to the curve $C$ whose image is dense in $C$. This implies that $C$ is a curve of genus zero. It is known however that any algebraic action of the group $S_5$ on a curve of genus zero has a non-trivial kernel. This contradicts the fact that the function $z$ is a rational function of $y$ and the parameters $a_1, \ldots, a_5$, because when the parameters $a_1, \ldots, a_5$ are generic, the corresponding values $z_1, \ldots, z_5$ are all distinct.

The proof presented above uses knowledge of algebraic actions of the group $S_5$ on a rational curve. Kronecker’s proof of theorem [12] relies on classification of algebraic actions of the group $A_5$. In fact there is essentially only one action of the group $A_5$ on a rational curve and it is the action of $A_5$ on the Riemann sphere by the rotational symmetries of a regular icosahedron. Additional considerations are then employed to show that it is impossible to find an $A_5$-equivariant mapping from $\mathbb{C}^5$ to the Riemann sphere with this particular $A_5$ action (see [21]).

Recently Serre has proved the following theorem relying on Manin-Iskovskih classification of minimal rational $G$-surfaces:
Theorem 14. The universal degree 6 algebraic function is not a composition of one algebraic function of 2 parameters and rational functions of the original parameters and square root of the discriminant.

Very recently Duncan has proved the following theorem [11]:

Theorem 15. The universal algebraic function of degree 7 is not a composition of algebraic functions of three variables and rational functions of the original parameters and square root of the discriminant.

The proofs of Duncan and Serre follow the same general outline that Kronecker’s proof uses, but they are much more complicated because the theory of two- and three-dimensional algebraic varieties is substantially more complicated than the theory of algebraic curves.

Essential dimension of groups

Buhler and Reichstein have proved the following result about the universal algebraic function of degree $n$ by completely different methods:

Theorem 16. The universal algebraic function of degree $n$ is not a composition of rational functions and an algebraic function of less than $\lfloor \frac{n}{2} \rfloor$ variables.

The general algebraic function of degree $n$ is not a composition of rational functions of the parameters and square root of the discriminant and an algebraic function of less than $2\lfloor \frac{n}{3} \rfloor$ variables.

To prove this theorem they introduced the notion of essential dimension of a finite group:

Definition 4. The essential dimension of an algebraic action of a finite group $G$ on an algebraic variety $X$ is the minimal dimension of an algebraic $G$-variety $Y$ with a
generically-free action of the group $G$ for which there exists a dominant $G$-equivariant rational morphism $X \to Y$.

The essential dimension of a finite group is the essential dimension of any of its faithful linear representations.

Hidden in the definition of essential dimension is the following theorem:

**Theorem 17.** Let $G$ be a finite group and let $G \to GL(V)$, $G \to GL(W)$ be two faithful linear representations of $G$. The essential dimensions of the $G$-varieties $V$ and $W$ coincide.

In terms of essential dimensions, Klein’s resolvent problem for the universal algebraic function of degree $n$ is equivalent to the problem of finding the essential dimension of the group $S_n$. The version of the same problem with square root of the discriminant added to the domain of rationality is equivalent to finding the essential dimension of the group $A_n$. To see these equivalences, it is enough to pass from the formulation of Klein’s problem in terms of rational mappings between the parameter spaces of the equations defining the algebraic functions in question to the version with equivariant rational mappings between the spaces of their roots as we have done in the proof of a version of Kronecker’s result (theorem 13).

For the proof of theorem 16, Reichstein uses the following corollary of theorem 17:

**Theorem 18.** The essential dimension of a group is greater than or equal to the essential dimension of any of its subgroups.

**Definition 5.** Let $G$ be a finitely generated abelian group. Its rank $r(G)$ is the smallest number of its generators.

The group $S_n$ contains a subgroup isomorphic to the group $Z_2^{[n/2]}$, namely the group

$$\langle (1, 2), (3, 4), \ldots, (2[n/2] - 1, 2[n/2]) \rangle$$
Chapter 1. Introduction

The bound $\lfloor n/2 \rfloor$ for the essential dimension of the group $S_n$ follows from theorem 18 and the following result:

**Theorem 19.** The essential dimension of an abelian group is equal to its rank.

In a similar manner the bound $2\lfloor n/4 \rfloor$ on the essential dimension of the group $A_n$ can be deduced from the fact that the group $A_n$ contains a subgroup

$$\langle (1,2)(3,4), (1,3)(2,4), (5,6)(7,8), (5,7)(6,8), \ldots \rangle$$

isomorphic to the group $\mathbb{Z}_2^{2\lfloor n/4 \rfloor}$ of rank $2\lfloor n/4 \rfloor$.

There have been many developments recently in the field of computing essential dimensions of finite groups. For instance Karpenko and Mekurjev have computed the essential dimensions of all the $p$-groups [17]:

**Theorem 20.** The essential dimension of a $p$-group is equal to the smallest dimension among the dimensions of its faithful linear representations.

Theorem 16 has been reproved by Serre [7]. His proof uses algebraic version of Stiefel-Whitney characteristic classes constructed by Delzant [10]. These characteristic classes are associated to finite algebraic extensions and their values lie in Galois cohomology. Serre showed that for the extension of the field of parameters $\mathbb{C}(a_1, \ldots, a_n)$ by the universal degree $n$ algebraic function $z = z(a_1, \ldots, a_n)$ the degree $\lfloor n/2 \rfloor$ Delzant’s Stiefel-Whitney class doesn’t vanish.

This theorem of Serre can be also used to give another proof of the fact that the essential dimension of an abelian 2-group is equal to its rank. A modified version of Delzant’s Stiefel-Whitney classes can be used to compute the essential dimension of other abelian $p$-groups.

Serre’s proof of theorem 16 can be thought of as an algebraic analogue of Arnold’s proof of theorem 11: both proofs use a version of Stiefel-Whitney characteristic classes and rely on the fact that these characteristic classes don’t vanish in certain degree for
the field extension/branched covering associated with the universal algebraic function of degree $n$.

**Topological methods**

The first attempt to apply topological methods to Klein’s resolvent problem has been made by Chebotarev in [9]. Unfortunately this work contained uncorrectable mistakes which have been pointed out in [27] (at the time of writing Chebotarev was critically ill and decided to publish a result that he didn’t have time to verify completely).

The method of Chebotarev was based on the notion of local monodromy around a point. Unfortunately this notion is not applicable in Klein’s resolvent problem because rational mappings don’t preserve locality.

The methods employed by Arnold for obtaining bounds in polynomial version of Klein’s resolvent problem also don’t seem to survive the passage to rational mappings because the topology of the parameter space of an algebraic function changes completely once one removes a subvariety where some rational function is not defined.

In this thesis we present a topological method for obtaining bounds in Klein’s resolvent problem that is based on the notion of local monodromy around a flag of subvarieties. This notion turns out to be better adapted to dealing with rational mappings as we explain in §3.7.3. It turns out that one can associate with a flag of subvarieties a family of neighbourhoods which are all homotopically equivalent to each other and such that for any hypersurface one can find a neighbourhood in this family which is completely disjoint from this hypersurface. Thus the notion of monodromy on any one of these neighbourhoods survives the removal of any hypersurface from the space of parameters of the algebraic function.

Each of the neighbourhoods in the family described above is homotopically equivalent to a topological torus. Our method for obtaining bounds in Klein’s resolvent problem is based on considering the covering realized by an algebraic function over such torus and
using the following topological result proved in section 3.5:

**Theorem 21.** A covering over a topological torus $(S^1)^n$ can be induced from a covering over a $k$-dimensional space if and only if the monodromy group of this covering has rank $\leq k$.

The proof of the prohibitive part of the theorem (i.e. the fact that if the monodromy group has rank $k$, then the covering can’t be induced from a space of dimension $< k$) uses characteristic classes, like the proof of Arnold’s theorem 11. However our proof employs characteristic classes for the category of coverings with a given monodromy group. The usual characteristic classes for the category of all coverings turn out to be too coarse to prove theorem 21.

### 1.4 Main results of the thesis

This thesis has two main parts. The first part deals with questions arising from attempts to classify rational functions invertible in radicals. The second part deals with questions about whether it is possible to reduce algebraic equations depending on many parameters to algebraic equations depending on a smaller number of parameters.

The main results obtained in this thesis are as follows:

- We give a complete description of branching data that guarantee that an algebraic function with such branching data is expressible in radicals (section 2.5).
- We give a complete description of branching data that guarantee that an algebraic function with such branching data defines a Riemann surface of bounded genus (section 2.5).
- We provide explicit formulas for the algebraic functions that have branching data as described above (section 2.8).
- We describe the moduli spaces of such algebraic functions (section 2.7).
We prove that a covering over a topological torus can be induced from a space of dimension $k$ if and only if the rank of the monodromy group of this covering is at most $k$ (section 3.5).

We show that an algebraic function unramified over the algebraic torus is a composition of rational functions and one algebraic function of $k$ variables (over a Zariski open subset of the torus where all the functions in question are defined) if and only if its monodromy group has rank $k$ (section 3.7.1).

We show that the equation $z^n + a_1 z^{n-1} + \ldots + a_n = 0$ can’t be reduced to an equation depending on less than $\lfloor \frac{n}{2} \rfloor$ parameters by means of a rational change of variables. Even if square root of the discriminant is used in the formulas for the change of variables, we show that one can’t reduce this equation to an equation depending on less than $2 \lfloor \frac{n}{4} \rfloor$ parameters (sections 3.7.2, 3.7.3).

We show that a generic algebraic equation depending on $k$ parameters and having degree $\geq 2k$ can’t be reduced to an equation depending on less than $k$ parameters by means of a rational change of variables (section 3.7.5).
Chapter 2

Local branching and rational functions invertible in radicals

In this part of the thesis we study a family of rational functions characterized by several wonderful properties. These functions appeared, for instance, in the work \[30\] of J.F. Ritt, where the following question has been asked:

**Question 4.** What rational functions \(R : \mathbb{C}P^1 \rightarrow \mathbb{C}P^1\) of prime degree are invertible in radicals (i.e. when can the equation \(w = R(z)\) be solved for \(z\) in radicals)?

Using somewhat ad hoc arguments Ritt has shown that the answer to question 4 can be formulated as follows:

**Theorem 22.** A rational function \(R\) of prime degree invertible in radicals if and only if it fits into the diagram

\[
\begin{array}{ccc}
A_1 & \longrightarrow & A_2 \\
\downarrow & & \downarrow \\
S & \underset{R}{\longrightarrow} & S
\end{array}
\]

where the arrow between \(A_1\) and \(A_2\) is an isogeny of algebraic groups of dimension 1 (i.e. either \(\mathbb{C}^*\) or elliptic curves) and the vertical arrows are quotients by the action of
a non-trivial finite group of automorphisms of the algebraic group \( A_i \) (\( S \) in this case is isomorphic either to \( \mathbb{C}^* \), if \( A_i \) is \( \mathbb{C}^* \), or to \( \mathbb{CP}^1 \), if \( A_i \) is an elliptic curve).

One can also show that the rational functions from theorem 22 appear among the rational functions that constitute the answer to the following question:

**Question 5.** What are the rational functions \( R \) having the property that the total space of the minimal Galois branched covering that dominates the branched covering \( R : \mathbb{CP}^1 \to \mathbb{CP}^1 \) is non-hyperbolic (i.e. has genus 0 or 1).

The full answer to question 5 contains also rational functions with icosahedral symmetry of the associated minimal Galois branched covering that dominates \( R : \mathbb{CP}^1 \to \mathbb{CP}^1 \).

One can also provide a local topological description. More precisely, an algebraic function on the Riemann sphere has a very simple invariant — the branching orders at all its branching points. The branching orders of an algebraic function give very limited information about the function. Knowing them doesn’t guarantee knowing the local monodromy around the branching points, to say nothing of the global monodromy group! Nevertheless for some particular branching data one can know a priori that the monodromy group of an algebraic function with such branching satisfies some properties (e.g. is solvable). More precisely the functions from theorem 22 are also the functions that appear in the answer to the following question:

**Question 6.** Let \( w_1, \ldots, w_b \in \mathbb{CP}^1 \) be a given collection of points and let \( d_1, \ldots, d_b \in \mathbb{N} \cup \{0\} \) be some given natural numbers. Consider the collection of holomorphic functions \( R \) from some compact Riemann surface to \( \mathbb{CP}^1 \) that are branched over the points \( w_1, \ldots, w_b \) with the local monodromy \( \sigma_i \) around the point \( w_i \) satisfying \( \sigma_i^{d_i} = 1 \). Suppose that all the functions in this collection have inverses expressible in radicals. What are the rational functions in this collection?

Another question whose answer turns out to be the same as the answer to question 5.
with “rational functions” replaced by “regular functions from a Riemann surface to $\mathbb{C}P^1$ is as follows:

**Question 7.** Let $w_1, \ldots, w_b \in \mathbb{C}P^1$ be a given collection of points and let $d_1, \ldots, d_b \in \mathbb{N} \cup \{0\}$ be some given natural numbers. Consider the collection of holomorphic functions $R$ from some compact Riemann surface (it may be different for different $R$’s) to $\mathbb{C}P^1$ that are branched over the points $w_1, \ldots, w_b$ with the local monodromy $\sigma_i$ around the point $w_i$ satisfying $\sigma_i^{d_i} = 1$. Suppose that the functions in this collection have bounded topological complexity in the following sense: the genus of their source Riemann surface is bounded. **What are the rational functions in this collection?**

The results of this part of the thesis are mainly concerned with the questions outlined above. However the functions we will be discussing appear in arithmetic applications as well. Namely these functions appear as a part of the answer to the following question:

**Question 8.** What are the rational functions $R$ defined over a number field $K$ so that for infinitely many places the map induced by $R$ on the projective line defined over the corresponding residue field is a bijection?

This question (inspired by conjecture of Schur) has been answered in a works of M. Fried [12] and R.Guralnick, P. Muller and J. Saxl [15].

It seems that there are some multidimensional generalizations of the family of rational functions that appear as answers to the questions above. For instance some polynomial analogues of the rational functions that are studied in this part of the thesis have been explored in works of Hoffmann and Withers [16] and Veselov [34]. These polynomials satisfy some multidimensional analogues of properties mentioned in questions 22 and 8 but not 6.
Chapter 2. Local branching and rational functions invertible in radicals

2.1 Conventions

A branched covering over a compact Riemann surface $S$ is a non-constant holomorphic map $f : \tilde{S} \to S$ from a compact Riemann surface $\tilde{S}$ to $S$. For any point $z_0 \in \tilde{S}$ there exist holomorphic coordinate charts around $z_0$ and $f(z_0)$ so that in these coordinates $f(z) = z^{d_{z_0}}$. The integer $d_{z_0}$ is called the multiplicity of $f$ at $z_0$.

The local monodromy at a point $w \in S$ is the conjugacy class inside the monodromy group of the permutation induced by going along a small loop in the base around $w$.

A branched covering $f : \tilde{S} \to S$ is called Galois if there exists a group $G$ of automorphisms of $\tilde{S}$ that are compatible with $f$ (i.e. $f \circ g = f$ for any $g \in G$) that acts transitively on all fibers of $f$. For Galois branched coverings the multiplicities of all points in a fiber over a fixed point $w$ in $S$ are the same. This common multiplicity will be called the multiplicity of the Galois branched covering $f$ at $w$.

2.2 Non-hyperbolic Galois branched coverings over the Riemann sphere

In this section we describe the Galois branched coverings over the Riemann sphere, whose total space has genus 0 or 1, i.e. is topologically a sphere or a torus. Equivalently it is a description of all non-free actions of a finite group on a sphere or a torus.

We provide a short proof of this classical result to remind the reader the branching orders of the functions realizing quotients by these actions.

Let $f : T \to \mathbb{CP}^1$ be a Galois branched covering of degree $d$. Let $w_1, \ldots, w_b \in \mathbb{CP}^1$ be all the branching points of $f$ and let $d_{w_i}$ denote the local multiplicity at $w_i$.

Riemann-Hurwitz formula for $f$ states that

$$
\chi(T) = \chi(\mathbb{CP}^1)d - \sum_{i=1}^{b}(d - \frac{d}{d_{w_i}})
$$
or

\[
b - 2 + \frac{\chi(T)}{d} = \frac{1}{d_1} + \ldots + \frac{1}{d_b}
\]

If the surface \( T \) is a sphere then \( \chi(T) = 2 \) and the formula specializes to

\[
b - 2 + \frac{2}{d} = \frac{1}{d_1} + \ldots + \frac{1}{d_b}
\]

If there are only two branching points, the local monodromies around them must be the same, since the product of small loops around the two branching points is contractible in the compliment to the branching locus. In this case we have then a family of solutions

\[
b = 2; d_1 = d_2 = d
\]

In the case \( b = 3 \) we have the following solutions:

case \( (2,2,\ast) \):

\[
b = 3, d_1 = 2, d_2 = 2, d_3 = d
\]

case \( (2,3,3) \):

\[
b = 3, d_1 = 2, d_2 = 3, d_3 = 3; d = 12
\]

case \( (2,3,4) \):

\[
b = 3, d_1 = 2, d_2 = 3, d_3 = 4; d = 24
\]

case \( (2,3,5) \):

\[
b = 3, d_1 = 2, d_2 = 3, d_3 = 5; d = 60
\]

For \( b \geq 4 \) there are no solutions.

If the surface \( T \) is the torus, then \( \chi(T) = 0 \) and the formula specializes to

\[
b - 2 = \frac{1}{d_1} + \ldots + \frac{1}{d_b}
\]

The solutions of this equation are

case \( (2,3,6) \):

\[
b = 3, d_1 = 2, d_2 = 3, d_3 = 6
\]
case (2,4,4):

\[ b = 3, d_1 = 2, d_2 = 4, d_3 = 4 \]

case (3,3,3):

\[ b = 3, d_1 = 3, d_2 = 3, d_3 = 3 \]

case (2,2,2,2):

\[ b = 4, d_1 = 2, d_2 = 2, d_3 = 2, d_4 = 2 \]

We see that there are only few possibilities for such Galois coverings and they all have very simple branching data. In section 2.4 we will see that this simple local picture characterizes these coverings uniquely.

### 2.3 Auxiliary definitions and results

To prove the results of section 2.4 we will need the following two lemmas.

**Lemma 23.** If a branched covering over \( \mathbb{C}P^1 \) is branched at most at two points, then the total space of the covering is the Riemann sphere. Moreover, if the degree of the covering is \( d \), then a holomorphic coordinate on source and target spheres can be chosen so that the covering is given by \( z \to z^d \).

If a covering over a genus one curve is unbranched, then the total space of the covering has genus one.

**Lemma 24.** (Local picture of pull-back) Let \( D \) denote the unit disc in \( \mathbb{C} \). Let \( f : D \to D \) denote the branched covering \( z \to z^n \) and \( g : D \to D \) denote the branched covering \( z \to z^m \). Let \( \tilde{f}, \tilde{g}, X \) fit into the pullback diagram

\[
\begin{array}{ccc}
X & \xrightarrow{\tilde{f}} & D \\
\downarrow{\tilde{g}} & & \downarrow{g} \\
D & \xrightarrow{f} & D
\end{array}
\]

Then \( X \) is a disjoint union of \( \gcd(m, n) \) discs, \( \tilde{f} \) restricted to each of the discs is of the form \( z \to z^{\frac{m}{\gcd(m, n)}} \), \( \tilde{g} \) restricted to each of the discs is of the form \( z \to z^{\frac{n}{\gcd(m, n)}} \).
For the purposes of section 2.4 we will also need the Galois coverings $T \to T/G$, where the Riemann surface $T$ and the group $G$ acting on it are as following:

Case $(2,2,\ast)$: $T = \mathbb{CP}^1$, $G = \mathbb{Z}_2$, $G$ acts by an involution fixing two points on $\mathbb{CP}^1$.

Case $(2,3,3)$: $T = \mathbb{CP}^1$, $G = A_4$ acting on the sphere by rotations of a regular tetrahedron.

Case $(2,3,4)$: $T = \mathbb{CP}^1$, $G = S_4$ acting on the sphere by rotations of an octahedron.

Case $(2,3,5)$: $T = \mathbb{CP}^1$, $G = A_5$ acting on the sphere by rotations of an icosahedron.

Case $(2,4,4)$: $T = \mathbb{C}/\langle 1, i \rangle$, $G = \mathbb{Z}_4$ with generator acting by $z \to iz$.

Case $(2,3,6)$: $T = \mathbb{C}/\langle 1, \omega \rangle$, $G = \mathbb{Z}_6$ with generator acting by $z \to -\omega z$, $\omega^2 + \omega + 1 = 0$.

Case $(3,3,3)$: $T = \mathbb{C}/\langle 1, \omega \rangle$, $G = \mathbb{Z}_3$ with generator acting by $z \to \omega z$, $\omega^2 + \omega + 1 = 0$.

Case $(2,2,2,2)$: $T$ is any elliptic curve, $G = \mathbb{Z}_2$, with the nontrivial element acting by $z \to -z$.

In each case the quotient space $T/G$ can be identified with $\mathbb{CP}^1$. For any of the nontrivial subgroups $H$ of $G$ the quotient space by the action of $H$ can also be identified with $\mathbb{CP}^1$.

### 2.4 Characterization by local branching

In this section we will prove the following result:

**Theorem 25.** Let $f : S \to \mathbb{CP}^1$ be a branched covering over the Riemann sphere and suppose it is branched at $b$ points $w_1, \ldots, w_b$ with local monodromies $\sigma_1, \ldots, \sigma_b$ around them satisfying $\sigma_i^{d_i} = 1$ for one of the following cases:

- **case $(\ast, \ast)$**: $b = 2, d_1 = d_2 = 0$ (i.e. we are given that it is branched at two points)
- **case $(2,2,\ast)$**: $b = 2, d_1 = d_2 = 2, d_3 = 0$ (i.e. we are given that it is branched at most at three points and local monodromies around two of them square to identity)

- **case $(2,3,3)$**: $b = 3, d_1 = 2, d_2 = 3, d_3 = 3$
• case (2,3,4): \(b = 3, d_1 = 2, d_2 = 3, d_3 = 4\)
• case (2,3,5): \(b = 3, d_1 = 2, d_2 = 3, d_3 = 5\)
• case (2,3,6): \(b = 3, d_1 = 2, d_2 = 3, d_3 = 6\)
• case (2,4,4): \(b = 3, d_1 = 2, d_2 = 4, d_3 = 4\)
• case (3,3,3): \(b = 3, d_1 = 3, d_2 = 3, d_3 = 3\)
• case (2,2,2,2): \(b = 4, d_1 = 2, d_2 = 2, d_3 = 2, d_4 = 2\)

Then the function \(f\) fits into one of the following diagrams:

\(\text{case } (\ast, \ast):\)

\[
\begin{array}{c}
\mathbb{CP}^1 \\ \downarrow \cong \\
S \quad f \\
\downarrow \cong \\
\mathbb{CP}^1
\end{array}
\]

\(\text{case } (2,2, \ast):\)

\[
\begin{array}{c}
\mathbb{CP}^1 \\ \downarrow \\
\mathbb{CP}^1/\mathbb{H} \quad \cong \\
\downarrow \\
\mathbb{CP}^1/G \\
\downarrow \cong \\
S \quad f \\
\downarrow \cong \\
\mathbb{CP}^1
\end{array}
\]

where \(G = \mathbb{Z}_2\) and \(H\) is one of its subgroups - either \(\mathbb{Z}_2\) or the trivial group.

\(\text{cases } (2,3,3),(2,3,4),(2,3,5):\)

\[
\begin{array}{c}
\mathbb{CP}^1 \\
\downarrow \\
\mathbb{CP}^1/\mathbb{H} \quad \cong \\
\downarrow \\
\mathbb{CP}^1/G \\
\downarrow \cong \\
S \quad f \\
\downarrow \cong \\
\mathbb{CP}^1
\end{array}
\]

where \(G\) is the group for the corresponding case from section 2.3 and \(H\) is any of its subgroups.
cases \((2,4,4), (2,3,6), (3,3,3), (2,2,2,2)\):

\[
\begin{array}{c}
T_1 \xrightarrow{\tilde{f}} T \\
\downarrow \quad \downarrow \\
T_1/H \xrightarrow{\sim} T/G \\
\downarrow \quad \downarrow \\
S \xrightarrow{f} \mathbb{CP}^1
\end{array}
\]

where \(T_1\) and \(T\) are curves of genus \(1\), \(\tilde{f}\) is an unramified covering of tori, \(G\) is the group for the corresponding case from section 2 and \(H\) is one of its subgroups (the automorphism group of the curve \(T_1\) should contain \(H\)).

In particular the Riemann surface \(S\) is either the Riemann sphere or (in the cases \((2,4,4), (2,3,6), (3,3,3), (2,2,2,2)\) when \(H\) is the trivial group) a torus.

**Remark.** By identifying the quotient spaces by the actions of the groups \(G\) and \(H\) with \(\mathbb{CP}^1\) when possible (i.e. except the cases when \(H\) is trivial and acts on a torus) and choosing an appropriate holomorphic coordinate on this \(\mathbb{CP}^1\) we get very explicit description of the rational function \(f\) (up to change of coordinate in the source and in the target):

In case \((2,2,*)\) the quotient by action of \(\mathbb{Z}_2\) can be realized in appropriate coordinates by \(z \to \frac{z + z^{-1}}{2}\), so the rational function \(f\) is the Chebyshev polynomial: \(f\left(\frac{z + z^{-1}}{2}\right) = \frac{z^d + z^{-d}}{2}\).

In case \((2,2,2,2)\) the quotient by the action of \(\mathbb{Z}_2\) can be realized by the Weierstrass \(\wp\)-function, and thus \(f\) is the rational function that expresses the \(\wp\)-function of a lattice and in terms of the \(\wp\)-function of its sublattice.

In case \((3,3,3)\) the quotient by the action of \(\mathbb{Z}_3\) can be realized by \(\wp'\).

In case \((2,4,4)\) the quotient by the action of \(\mathbb{Z}_4\) can be realized by \(\wp''\).

In case \((2,3,6)\) the quotient by the action of \(\mathbb{Z}_6\) can be realized by \(\wp^{(4)}\).

**Proof.** In case \((*,*)\) the claim is the content of lemma 23.

In case \((2,2,*)\) identify \(T/\mathbb{Z}_2\) (for \(T = \mathbb{CP}^1\) and action of \(\mathbb{Z}_2\) as in section 2.3) with \(\mathbb{CP}^1\) in such a way that the two branching points of the quotient map \(q_G : \mathbb{CP}^1 \to \mathbb{CP}^1/\mathbb{Z}_2 \simeq \mathbb{CP}^1\) coincide with points \(w_1\) and \(w_2\).
In other cases choose the identification of $T/G$ from section 2.3 with $\mathbb{CP}^1$ so that the branching points $w_i$ and the numbers $d_i$ attached to them (i.e. the numbers so that the local monodromy to the power $d_i$ is the identity) coincide with the branching points for the quotient mapping $q_G : T \to T/G \simeq \mathbb{CP}^1$ and their local multiplicities.

Consider the pullback of the map $q_G$ by the map $f$. Let the pullback maps be called as in the diagram below

$$
\begin{array}{c}
\tilde{T} \\
\downarrow \tilde{q}_G \\
S \\
\end{array} \quad \begin{array}{c}
f \\
\downarrow q_G \\
\mathbb{CP}^1 \\
\end{array} \quad \begin{array}{c}
f \\
\downarrow q_G \\
\mathbb{CP}^1 \\
\end{array}
$$

The map $\tilde{q}_G$ realizes the quotient map by the action of $G$ on a possibly reducible curve $\tilde{T}$.

Let $H$ be the subgroup of $G$ fixing some component of $\tilde{T}$ and let $T_1$ denote this component. Then we can restrict the diagram to this component:

$$
\begin{array}{c}
T_1 \\
\downarrow q_H \\
S \\
\end{array} \quad \begin{array}{c}
\tilde{f} \\
\downarrow \tilde{q}_G \\
\mathbb{CP}^1 \\
\end{array} \quad \begin{array}{c}
f \\
\downarrow q_G \\
\mathbb{CP}^1 \\
\end{array}
$$

(The map $q_H$ is the restriction of $\tilde{q}_G$ to the connected component $T_1$; it realizes the quotient map by the action of $H$).

Now we can use lemma 24 to investigate how the map $\tilde{f}$ is branched.

For every point $w_i$ in $\mathbb{CP}^1$ for which we know that the local $f$-monodromy $\sigma$ satisfies $\sigma^{d_i} = 1$ with $d_i > 0$ we know also that the local monodromy of $q_G$ at this point is a disjoint unit of cycles of length $d_i$. Hence $\tilde{f}$ is unramified over any $q_G$-preimage of such points.

In case (2,2,*) this means that $\tilde{f}$ is branched over at most at two points — the two preimages of the point $w_3$ under $q_G$.

In other cases this means that $\tilde{f}$ is unramified.

In case (2,2,*) lemma 23 implies that $T_1$ is the Riemann sphere and by changing identification of $T$ and $T_1$ with $\mathbb{CP}^1$ and choosing an appropriate holomorphic coordinate,
we can make it be given by $z \rightarrow z^d$.

Hence $f$ fits into the diagram

\[
\begin{array}{c}
\mathbb{C}P^1 \xrightarrow{z \rightarrow z^d} \mathbb{C}P^1 \\
\downarrow \quad \downarrow \\
\mathbb{C}P^1/H \xrightarrow{\simeq} \mathbb{C}P^1/G \\
\downarrow \simeq \downarrow \simeq \\
S \xrightarrow{f} \mathbb{C}P^1
\end{array}
\]

as required.

In cases (2,3,3),(2,3,4),(2,3,5) the covering $\tilde{f}$ is unramified covering over the Riemann sphere, hence $\tilde{f}$ is the identity map.

Thus in this case $f$ fits into the diagram

\[
\begin{array}{c}
\mathbb{C}P^1 \\
\downarrow \\
\mathbb{C}P^1/H \xrightarrow{\simeq} \mathbb{C}P^1/G \\
\downarrow \simeq \\
S \xrightarrow{f} \mathbb{C}P^1
\end{array}
\]

In cases (2,4,4),(2,3,6),(3,3,3),(2,2,2,2) the covering $\tilde{f}$ is an unramified covering of a torus over a torus. In the diagram

\[
\begin{array}{c}
T_1 \xrightarrow{\tilde{f}} T \\
\downarrow q_H \\
T/G \\
\downarrow \simeq \\
S \xrightarrow{f} \mathbb{C}P^1
\end{array}
\]

the map $q_H$ must be one of the quotient maps by the action of a finite group of automorphisms of the genus 1 curve $T_1$ as described in section 2.3 because the action of $H$ (if $H$ is not trivial) has fixed points and all the actions with this property appeared in section 2.3. In this case $S$ is either a torus (if $H$ is trivial) or the Riemann sphere (if it is not).
Finally \( f \) fits into the diagram

\[
\begin{array}{ccc}
T_1 & \xrightarrow{f} & T \\
\downarrow & & \downarrow \\
T_1/H & \xrightarrow{} & T/G \\
\downarrow & \simeq & \downarrow \\
S & \xrightarrow{f} & \mathbb{CP}^1
\end{array}
\]

as required.

\[\square\]

### 2.5 When branching data implies global properties

In this section we will answer questions 7 and 6. The answers to these questions explain why the branching data that appear in the formulation of theorem 25 are in some sense optimal. The result we will be proving is the following.

**Theorem 26.** Let \( w_1, \ldots, w_b \in \mathbb{CP}^1 \) be a given collection of points and let \( d_1, \ldots, d_b \in \mathbb{N} \cup \{0\} \) be some given natural numbers. Consider the collection of holomorphic functions \( R \) from some compact Riemann surface to \( \mathbb{CP}^1 \) that are branched over the points \( w_1, \ldots, w_b \) with the local monodromy \( \sigma_i \) around the point \( w_i \) satisfying \( \sigma_i^{d_i} = 1 \).

The genus of the source Riemann surface for all functions in this collection is bounded if and only if the numbers \( (d_1, \ldots, d_b) \) are the ones that appear in theorem 25.

All the functions in this collection have inverses expressible in radicals if and only if the numbers \( (d_1, \ldots, d_b) \) are the ones that appear in theorem 25, with the exception of case \((2, 3, 5)\).

**Proof.** For the proof we make two observations: the first one is that if the function \( R : S \to \mathbb{CP}^1 \) belongs to this collection, then the minimal branched Galois covering \( \tilde{R} : \tilde{S} \to \mathbb{CP}^1 \) that dominates \( R \) also belongs to it. The second observation is that if \( S_1 \to S \) is an unramified covering and \( R : S \to \mathbb{CP}^1 \) is a function from the collection, then the composite function \( S_1 \to S \to \mathbb{CP}^1 \) also belongs to the collection.
Chapter 2. Local branching and rational functions invertible in radicals

Now suppose that for given \( w_1, \ldots, w_b \) and \( d_1, \ldots, d_b \) as above, the collection contains some function that is not one of those mentioned in theorem 25. Then it also contains its ”Galois closure” - the minimal Galois branched covering that dominates it, and the source space of this Galois closure has genus at least 2. Hence we can find an unramified covering over it with total space of arbitrary high genus, contradicting the assumption of the first claim. Also we can find an unramified covering over it with unsolvable monodromy group, so that the inverse to this mapping can’t be expressed in radicals, contradicting the assumptions of the second claim.

Finally for the branching data appearing in theorem 25 the genus of the source Riemann surface is either 0 or 1. Similarly the possible monodromy groups for all the branching data from theorem 25 are all solvable, with the exception of the group \( A_5 \) in case (2,3,5).

2.6 Applications to Ritt’s problem

In this section we prove Theorem 22 that has been proved differently in 30.

Describing rational functions with complex coefficients that are invertible in radicals is equivalent to describing rational functions with solvable monodromy group.

If we are interested in rational functions that can’t be expressed as compositions of other rational functions, we should only consider those branched coverings of \( \mathbb{CP}^1 \) over \( \mathbb{CP}^1 \) with solvable primitive monodromy group (see section 2.9).

Result 28 of Burnside tells that a primitive action of a solvable group on a finite set can be identified with an irreducible action of a subgroup of the group of affine motions of the vector space \( F_p^n \).

In case \( n = 1 \) above, i.e. when the degree of the rational function is a prime number, the action can be identified with action of a subgroup of \( AGL_1(F_p) = \{ x \to ax + b \} \) on
Now let $w_1, \ldots, w_b$ be the branching points and let the local monodromies around these points be given by $x \to a_i x + b_i \mod p$ in the above identification. A simple application of Riemann-Hurwitz formula shows

$$\sum \frac{1}{\text{ord } a_i} = b - 2$$

with the convention that $\text{ord } 1 = \infty$.

This equation has the following solutions for $\text{ord } a_i$:

1. $\frac{1}{\infty} + \frac{1}{\infty} = 2 - 2$
2. $\frac{1}{2} + \frac{1}{2} + \frac{1}{\infty} = 3 - 2$
3. $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 3 - 2$
4. $\frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 3 - 2$
5. $\frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 3 - 2$
6. $\frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} = 4 - 2$

It is easy to check that if $\text{ord } a_i \neq \infty$ then the $\text{ord } a_i$th power of the permutation $x \to a_i x + b_i$ is the identity.

Thus we are exactly in the situation described in theorem 25 and the results thereof apply here.

Moreover, since the degree of our covering is prime, and degree considerations force the subgroup $H$ from theorem 25 to be equal to the group $G$. Indeed, the degree of the function $f$ fitting into diagram

$$
\begin{array}{ccc}
X & \xrightarrow{j} & Y \\
\downarrow & & \downarrow \\
X/H & \xrightarrow{f} & Y/H
\end{array}
$$

is equal to the degree of $\tilde{f}$ multiplied by $|G|/|H|$. If the degree of $f$ is prime, the index of $H$ in $G$ must be equal to 1.

Thus we get immediately that we can change coordinates in the source and the target $\mathbb{CP}^1$ so that our function $f$ becomes either the map $z \to z^p$ or fits into one of the following
diagrams

\[
\begin{array}{c}
\mathbb{CP}^1 \xrightarrow{z \mapsto z^p} \mathbb{CP}^1 \\
\downarrow_{z \mapsto z^{1/2}} & \downarrow_{z \mapsto z^{1/2}} \\
\mathbb{CP}^1 \xrightarrow{f} \mathbb{CP}^1 \\
\end{array}
\]

\[
\begin{array}{c}
T_1 \xrightarrow{\bar{f}} T_2 \\
\downarrow_{QC} & \downarrow_{QC} \\
\mathbb{CP}^1 \xrightarrow{f} \mathbb{CP}^1 \\
\end{array}
\]

where \(T_1\) and \(T_2\) are tori on which the same group \(G\) acts with fixed points, \(\bar{f}\) is an unbranched covering of tori, the vertical arrows are quotients by the action of \(G\) and \(G\) is \(\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4\) or \(\mathbb{Z}_6\).

## 2.7 Three classifications of Ritt’s functions

Here we would like to obtain slightly more precise results, that show how many rational functions invertible in radicals there are up to equivalence. We will consider three equivalence relations: left analytical equivalence (\(f_1\) and \(f_2\) are equivalent if there exists a Mobius transformation \(\mathbb{CP}^1 \sim \mathbb{CP}^1\) so that the diagram

\[
\begin{array}{c}
\mathbb{CP}^1 \xrightarrow{\sim} \mathbb{CP}^1 \\
\downarrow_{f_1} & \downarrow_{f_2} \\
\mathbb{CP}^1 \\
\end{array}
\]

commutes), left-right analytical equivalence (\(f_1\) and \(f_2\) are equivalent if there exist two Mobius transformations \(\mathbb{CP}^1 \sim \mathbb{CP}^1\) so that the diagram

\[
\begin{array}{c}
\mathbb{CP}^1 \xrightarrow{\sim} \mathbb{CP}^1 \\
\downarrow_{f_1} & \downarrow_{f_2} \\
\mathbb{CP}^1 \\
\end{array}
\]

commutes), and topological equivalence (which is defined by the same diagram, but instead of Mobius transformations we have orientation-preserving homeomorphisms of the sphere).
We start with the easiest of these, the left-analytical equivalence.

We will consider the case $(2,2,2,2)$ in some details and only state the result for other cases.

Let $w_1, w_2, w_3, w_4$ be four branching points in $\mathbb{CP}^1$. We want to count how many rational functions of prime degree $p$ there are up to left analytical equivalence with branching points $w_1, w_2, w_3, w_4$ so that their inverses are expressible in radicals.

Consider the two-sheeted covering $q : T \rightarrow \mathbb{CP}^1$ branched over $w_1, w_2, w_3, w_4$. Let $O \in T$ denote the preimage of $w_1$. We can identify the space $T$ with an elliptic curve with zero at $O$.

Now we claim that the set of left equivalence classes of degree $p$ isogenies from some elliptic curve to $T$ is in bijection with the set of left analytical equivalence classes of rational functions we are interested in.

The bijection is constructed in the following way.

Take the left equivalence class of an isogeny $s : T_1 \rightarrow T$. The composition $q \circ s$ satisfies $q \circ s(z) = q \circ s(-z)$ for every $z \in T_1$ (because $s(-z) = -s(z)$ and $q(-s(z)) = q(s(z))$).

Hence it factors through $T_1/z \sim -z$. Choose an isomorphism of $T_1/z \sim -z$ with $\mathbb{CP}^1$. The bijection sends the class of $s$ to the class of the resulting map $\tilde{s} : \mathbb{CP}^1 \cong T_1/z \sim -z \rightarrow \mathbb{CP}^1$ fitting into the diagram

$$
\begin{array}{ccc}
T_1 & \xrightarrow{s} & T \\
\downarrow & & \downarrow q \\
T_1/z \sim -z & \cong & \mathbb{CP}^1 \\
\end{array}
\xrightarrow{\tilde{s}} \mathbb{CP}^1
$$

It is easy to check that this map is well-defined.

The inverse of this map can be defined in the following way. Consider left equivalence class of rational mapping $g : \mathbb{CP}^1 \rightarrow \mathbb{CP}^1$ of degree $p$ invertible in radicals and branched over $w_1, \ldots, w_4$.

It follows from the result of previous section that the squares of local monodromies around points $w_1, \ldots, w_4$ are identity.
Theorem 25 tells us that in the pullback diagram

\[
\begin{array}{cccc}
T_1 & \xrightarrow{\tilde{g}} & T & \\
\downarrow{\tilde{\varphi}} & & \downarrow{\varphi} & \\
\mathbb{C}P^1 & \xrightarrow{g} & \mathbb{C}P^1 & \\
\end{array}
\]

the space \( T_1 \) is a torus, \( \tilde{g} \) is an unramified covering of tori. Hence if we choose the origin in \( T_1 \) to be one of the preimages of \( O \), we get that \( \tilde{g} \) is an isogeny of degree \( p \) over \( T \).

We send the class of \( g \) to the class of \( \tilde{g} \). This map is also well-defined and is the inverse of the map we had defined previously.

Hence all we should do is count the equivalence classes of degree \( p \) isogenies over an elliptic curve \( T \). These are enumerated by the subgroups of \( \pi_1(T, O) \) of index \( p \). Since \( \pi_1(T, O) \) is isomorphic to \( \mathbb{Z}^2 \), the number we are interested in is \( p + 1 \): index \( p \) subgroups of \( \mathbb{Z}^2 \) are in bijection with index \( p \) subgroups of \( \mathbb{Z}_p^2 \), i.e. the points of \( \mathbb{P}^1(\mathbb{F}_p) \).

Next we will construct the space that parametrizes left-right equivalence classes of rational mappings of prime degree with four branching points and inverses expressible in radicals.

First we claim that instead of parameterizing such left-right classes of rational mappings, we can parametrize isogenies of genus one Riemann surfaces with marked quadruples of points which are the fixed points of an involution with fixed points (another way to say it is that the four distinct marked points \( w_1, ..., w_4 \) satisfy \( 2w_i \sim 2w_j \), where \( \sim \) stands for linear equivalence).

Indeed, to any rational function \( g : \mathbb{C}P^1 \rightarrow \mathbb{C}P^1 \) branched at four points with the property that the square of monodromy around each one of them is the identity, we can associate the isogeny \( \tilde{g} : T_1 \rightarrow T \) of elliptic curves that fits into the pullback diagram

\[
\begin{array}{cccc}
T_1 & \xrightarrow{\tilde{g}} & T & \\
\downarrow{\tilde{\varphi}} & & \downarrow{\varphi} & \\
\mathbb{C}P^1 & \xrightarrow{g} & \mathbb{C}P^1 & \\
\end{array}
\]

where \( q \) is the double covering over \( \mathbb{C}P^1 \) with four branching points that coincide with the branching points of \( g \). The mapping \( \tilde{\varphi} \) must be branched over the four regular preimages
under \( g \) of the branching points of \( g \). The curves \( T_1 \) and \( T \) have genus 1 and are equipped with involutions with fixed points - the involutions that interchange the two sheets of the covering \( q \) and of the covering \( \tilde{q} \).

Two rational functions \( g_1 \) and \( g_2 \) are left-right equivalent if and only if they give rise to isomorphic isogenies \( \tilde{g}_1 \) and \( \tilde{g}_2 \) (in the sense that the isogenies are isomorphic and marked points get carried to marked points by the isomorphisms).

Now we can choose origin on the curve \( T \) to be at one of the marked points and the origin of \( T_1 \) to be at its preimage under \( \tilde{g} \). This way we get an isogeny of elliptic curves of prime degree. Different choices of origin give rise to isomorphic isogenies of elliptic curves (composition with translations provide the isomorphisms) and hence we have to parametrize the space of isogenies of degree \( p \) of elliptic curves.

This space is known (see for instance [31]) to be the modular curve that is the quotient of the upper half-plane \( \mathbb{H} \) by the action of the group \( \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) | c \equiv 0 \mod p \} \). This curve admits a degree \( p+1 \) branched covering over the moduli space of elliptic curves (the covering map sends the isogeny to its target elliptic curve). This covering is branched over two points — the classes of elliptic curves \( \mathbb{C}/\langle 1, i \rangle \) and \( \mathbb{C}/\langle 1, \omega \rangle \).

Thus for a generic choice of 4 branching points for the rational map of degree \( p \) with inverse invertible in radicals there are \( p+1 \) left-equivalence classes of such rational functions and all of them are not left-right equivalent to each other. For the choices of these branching points with the property that they are either harmonic or have cross ratio \( e^{\pm i\pi/3} \), among the \( p+1 \) left-equivalence classes there are left-right equivalent ones. Namely for the case that the branching points are harmonic, the \( p+1 \) left-equivalence classes get partitioned by the left-right analytic equivalence relation to \( \frac{p-1}{2} \) pairs and 2 singletons if \( p \equiv 1 \mod 4 \) and just to \( \frac{p+1}{2} \) pairs if \( p \equiv 3 \mod 4 \) (if \( p = 2 \), the partition is to one pair and one singleton). For the case of cross ratio \( e^{\pm i\pi/3} \), the \( p+1 \) left-equivalence classes get partitioned by the left-right analytic equivalence relation to \( \frac{p-1}{3} \) triples and 2
singletons if \( p \equiv 1 \mod 6 \) and just to \( \frac{p+1}{3} \) triples if \( p \equiv 5 \mod 6 \) (if \( p = 3 \), the partition is to one triple and one singleton, if \( p = 2 \), the partition is to one triple).

Finally there is only one class of such mappings up to left-right topological equivalence, since the modular curve is connected.

In other cases the picture is even simpler, since we don’t have any moduli in question.

Namely, for the case \((2,4,4)\), to count left-equivalence classes we should count the number of sublattices of index \( p \) of the lattice of Gaussian integers, which are invariant under multiplication by \( i \). These exist only if \( p = 2 \) or \( p \equiv 1 \mod 4 \), and then, if \( p = 2 \), there is only one such, and if \( p \equiv 1 \mod 4 \), there are two such. These classes of left-equivalence are not left-right-analytically equivalent, and hence also not topologically equivalent with orientation preserving homeomorphisms (they are the connected components of the corresponding Hurwitz scheme).

Similarly in cases \((2,3,6)\) and \((3,3,3)\) we should count the number of sublattices of the lattice of Eisenstein integers, which are invariant under multiplication by the primitive cubic root of unity \( \omega \). These exist only if \( p = 3 \) or \( p \equiv 1 \mod 6 \). If \( p = 3 \) there is one such, and in case \( p \equiv 1 \mod 6 \), there are two such.

### 2.8 Explicit formulae for the rational functions invertible in radicals

In the previous sections we’ve seen that the non-polynomial rational functions of prime degree with the inverse expressible in radicals are in fact the same as the rational functions that express some particular elliptic function on a lattice in terms of an elliptic function on its sublattice. The elliptic functions that appeared were the functions that generated the field of elliptic functions on the lattice, invariant under a certain group of automorphisms of the elliptic curve. For instance in the \((2,2,2,2)\) case, the corresponding rational function should have expressed the Weierstrass function of a lattice in terms of the
Chapter 2. Local branching and rational functions invertible in radicals

Weierstrass function for a sublattice.

Since we would like to derive the expressions for the corresponding rational functions uniformly for cases \((2, 4, 4), (3, 3, 3), (2, 3, 6)\) and \((2, 2, 2, 2)\), we are going to use the following notations:

- \(S_\Lambda(z)\) denotes
  - \(\wp_\Lambda(z)\) in case \((2, 2, 2, 2)\)
  - \(\wp'_\Lambda(z)\) in case \((3, 3, 3)\)
  - \(\wp''_\Lambda(z)\) in case \((2, 4, 4)\)
  - \(\wp^{(4)}_\Lambda(z)\) in case \((2, 3, 6)\)

Also \(W\) will denote the group of roots of unity of degree

- 2 in case \((2, 2, 2, 2)\)
- 3 in case \((3, 3, 3)\)
- 4 in case \((2, 4, 4)\)
- 6 in cases \((2, 3, 6)\)

We will denote by \(g[0]\) the constant term in a Laurent expansion of the meromorphic function \(g\) at 0.

We will need to use the following formula relating the Weierstrass \(\wp\)-function with the Jacobi theta function \(\theta\):

\[
\log(\theta(z))'' = \wp(z) + c
\]

where \(c\) is a constant.

Now we are ready:

Let \(\Lambda\) be a sublattice of index \(p\) in a lattice \(\Lambda'\) and assume that both \(\Lambda\) and \(\Lambda'\) are invariant under multiplication by elements of \(W\). We want to find a rational function \(R\) such that \(S_{\Lambda'}(z) = R(S_\Lambda(z))\).
Since the functions $S_{\Lambda'}$ and $\sum_{u \in \Lambda'/\Lambda} S_{\Lambda}(z - u)$ have the same poles and are both periodic with respect to $\Lambda'$, we can write

$$S_{\Lambda'}(z) - S_{\Lambda'}[0] = \sum_{0 \neq u \in \Lambda'/\Lambda} (S_{\Lambda}(z - u) - S_{\Lambda}(-u)) + S_{\Lambda}(z) - S_{\Lambda}[0]$$

We are now going to group the summands to $W$-orbits and find a formula for $\sum_{\xi \in W} (S_{\Lambda}(z - \xi u) - S_{\Lambda}(z))$ in terms of $S_{\Lambda}(z)$.

To do so, let $f(u) = \prod_{\xi \in W} \frac{\theta(z - \xi u)}{\theta(-\xi u)}$. The function $f$ is periodic with respect to $\Lambda$, has simple zeroes at $u = \xi z$ and a pole of order $|W|$ at 0. Hence $f(u) = C(S_{\Lambda}(u) - S_{\Lambda}(z))$ for some constant $C$.

Now we can take the logarithm of both sides and differentiate the result with respect to $u$ (note that the differentiation is with respect to $u$, not $z$) $|W|$ times. The result is the beautiful formula

$$(-1)^{|W|} \sum_{\xi \in W} (S_{\Lambda}(z - \xi u) - S_{\Lambda}(-\xi u)) = \frac{\partial^{|W|}}{\partial u} \log (S_{\Lambda}(u) - S_{\Lambda}(z))$$

Note that the right hand side is a rational function of $S_{\Lambda}(z)$.

Hence we get

$$S_{\Lambda'}(z) - S_{\Lambda'}[0] = \sum_{0 \neq u \in (\Lambda'/\Lambda)/W} \sum_{\xi \in W} (S_{\Lambda}(z - \xi u) - S_{\Lambda}(-\xi u)) + S_{\Lambda}(z) - S_{\Lambda}[0]$$

$$= (-1)^{|W|} \sum_{0 \neq u \in (\Lambda'/\Lambda)/W} \frac{\partial^{|W|}}{\partial u} \log (S_{\Lambda}(u) - S_{\Lambda}(z)) + S_{\Lambda}(z) - S_{\Lambda}[0]$$

So finally

$$R(w) = (-1)^{|W|} \sum_{0 \neq u \in (\Lambda'/\Lambda)/W} \frac{\partial^{|W|}}{\partial u} \log (S_{\Lambda}(u) - w) + w + S_{\Lambda'}[0] - S_{\Lambda}[0]$$

For instance in the case $(2, 2, 2, 2)$, with lattice $\Lambda'$ generated by 1 and $\tau$ and the lattice $\Lambda$ generated by $p, \tau$, the function $R$ is

$$R(w) = \sum_{u=1}^{p-1} \left( \frac{\varphi''(u)}{\varphi(u) - w} - \left( \frac{\varphi'(u)}{\varphi(u) - w} \right)^2 \right) + w$$
2.9 Auxiliary results used in the chapter

One reason for an algebraic function to be expressible in radicals is that it is a composition of two such functions. Thus one can be interested in theorems that characterize this situation. The following two theorems are of this kind:

Theorem 27. Let \( f : (X, x_0) \rightarrow (Z, z_0) \) be a covering map between two (connected, locally simply connected) pointed spaces and let \( M_f : \pi_1(Z, z_0) \rightarrow S(f^{-1}(z_0)) \) be the monodromy mapping. The covering \( f \) can be decomposed as a composition of two coverings \( g : (X, x_0) \rightarrow (Y, y_0) \) and \( h : (Y, y_0) \rightarrow (Z, z_0) \) if and only if the monodromy group \( M_f(\pi_1(Z, z_0)) \) acts imprimitively on \( f^{-1}(z_0) \).

Theorem 28 (Burnside). Let \( G \leq S(X) \) be a solvable primitive group of permutations of a finite set \( X \). Then the set \( X \) can be identified with the \( F_p^n \)-vector space \( F^n_p \) for some prime number \( p \) and number \( n \geq 1 \) in such a way that the group \( G \) gets identified with a subgroup of affine motions of the vector space \( F^n_p \) that contains all translations.

Corollary 29. Let \( f : (X, x_0) \rightarrow (Z, z_0) \) be a covering map with a solvable group of monodromy. Then it can be decomposed as a composition of covering maps \( (X, x_0) \xrightarrow{f_0} (Y^{(1)}, y_0^{(1)}) \xrightarrow{f_0} (Y^{(2)}, y_0^{(2)}) \rightarrow \ldots \rightarrow (Y^{(k)}, y_0^{(k)}) \xrightarrow{f_k} (Z, z_0) \) so that each covering \( f_i \) has degree \( p_i^{n_i} \) for some prime number \( p_i \) and has primitive monodromy group.

We will start by proving the first theorem in the list.

Proof. For one direction suppose that a covering \( (X, x_0) \xrightarrow{f} (Z, z_0) \) can be decomposed as a composition of coverings \( (X, x_0) \xrightarrow{g} (Y, y_0) \xrightarrow{h} (Z, z_0) \). Then the fiber \( f^{-1}(z_0) \) can be decomposed into blocks which consist of preimages under \( g \) of the points in the fiber \( h^{-1}(z_0) \). These blocks get permuted among themselves by any loop in \( (Z, z_0) \), thus showing that the monodromy group of the covering \( f \) is imprimitive. Conversely, let the monodromy \( M_f \) act imprimitively on the fiber \( f^{-1}(z_0) \). Let \( y_0, \ldots, y_n \) denote a system of blocks that shows that the action is imprimitive (each \( y_i \) is a block). We number them...
so that the block $y_0$ contains the point $x_0$. Then the monodromy action of $\pi_1(Z, z_0)$ on $f^{-1}(z_0)$ gives rise to its action on the set of imprimitivity blocks $y_0, \ldots, y_n$. Denote by $(Y, y_0) \xrightarrow{h} (Z, z_0)$ the covering that corresponds to the subgroup of $\pi_1(Z, z_0)$ that stabilizes the block $y_0$. We call the chosen point $y_0$ by the same name as the block $y_0$, which shouldn’t cause confusion (one can think of $g^{-1}(z_0)$ as the set of blocks $y_0, \ldots, y_n$). It remains to show that the map $f: (X, x_0) \to (Z, z_0)$ factors through $h: (Y, y_0) \to (Z, z_0)$.

By the theorem of lifting of coverings it is enough to show that $f_*(\pi_1(X, x_0))$ is contained in $g_*(\pi_1(Y, y_0))$. The first of these groups is equal to the subgroup of $\pi_1(Z, z_0)$ that stabilizes $x_0$, while the second is equal (by construction) to the subgroup of $\pi_1(Z, z_0)$ that stabilizes the block $y_0$. From the definition of imprimitivity blocks, if a loop stabilizes $x_0$, then it must stabilize the block which contains it, namely $y_0$. This observation finishes the proof that imprimitivity of monodromy action implies that the covering $f$ decomposes.

Now we will give a proof of the second theorem appearing in the works of Galois.

Proof. Let $G \geq G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(k-1)} \geq G^{(k)} = 1$ be the derived series for the group $G$ (i.e. $G^{(i+1)}$ is the commutator subgroup of $G^{(i)}$). Each of the subgroups $G^{(i)}$ is normal in the group $G$. Hence the group $G^{(k-1)}$ is an abelian normal subgroup of $G$. Let $p$ be any prime dividing the order of $G^{(k-1)}$ and let $N \leq G^{(k-1)}$ be the subgroup consisting of elements of order $p$ in it and the identity element: $N = \{ n \in G^{(k-1)} : n^p = 1 \}$. It is a subgroup, because $G^{(k-1)}$ is abelian. It is a characteristic subgroup of $G^{(k-1)}$, hence it is normal in $G$. Since the order of every non-trivial element of $N$ is $p$, the abelian group $N$ can be identified with the $F_p$-vector space $F_p^n$ for some natural number $n$. Since the group $G$ acts primitively on $X$, the action of the normal subgroup $N$ must be transitive (because the orbits under action of any normal subgroup of $G$ form imprimitivity blocks for the action of $G$). Now since $N$ is abelian, the action must be regular as well (because the stabilizers of points in $X$ under the action of a transitive group must all be conjugate
to each other, but in an abelian group this means that the stabilizers of all the points are equal). Thus every element in $N$ that fixes some point in $X$ must fix all points in $X$, hence it is the trivial permutation of the set $X$ and thus must be trivial itself. Since the action of $N$ on $X$ is free and transitive, the points in $X$ can be identified with elements of $N$. Namely, choose $x_0 \in X$ be any point. We will identify any other point $x$ with the unique element $n \in N$ that sends $x_0$ to $x$. Let now $G_{x_0}$ be the stabilizer subgroup of $x_0$ in $G$. We claim that every element $g$ of $G$ can be written uniquely as a product $nh$ with $n \in N$ and $h \in G_{x_0}$. Indeed, let $n$ be the unique element of $N$ that maps $x_0$ to $g \cdot x_0$. Then the element $n^{-1}g$ stabilizes $x_0$, i.e. belongs to $G_{x_0}$. Denote it by $h$. Thus $g = nh$ with $n \in N$ and $h \in G_{x_0}$. If $g = nh = n'h'$ are two representations of $g$ in such form, then $n'^{-1}n = h'h^{-1}$ must be an element of $N$ that fixes $x_0$. But we have proved that it must then be the identity element. Finally, after identifying the points of $X$ with the elements of the $F_p$-vector space $N$, the elements of $G_{x_0}$ act by linear mappings. Indeed, if we denote by star the action of $G_{x_0}$ on $N$ coming from identification of $X$ with $N$, then $g \ast n$ should be the (unique) element of $N$ that sends $x_0$ to $gnx_0$. Since the element $gng^{-1}$ belongs to $N$ and sends $x_0$ to $gnx_0$, we are forced to declare that $g \ast n = gng^{-1}$. Now the fact that $G_{x_0}$ acts linearly on $N$ is evident. Thus we can identify the set $X$ with the vector space $F_p^n$, the abelian group $N$ with the group of translations of this vector-space and the group $G_{x_0}$ with the group of linear transformation of it. 

\[\square\]

### 2.10 Related results

#### 2.10.1 Classification of rational functions of degree 3

We can apply our classification results for instance to the classification of rational functions of degree 3. Indeed, when the degree of the rational function is 3, only the following branching data is possible: 4 double points, 2 double points and one triple point, or 2 triple points. In the first case the function is of the kind we described as case $(2,2,2,2)$
and thus we get the following classification result: for every four-tuple of points in $\mathbb{CP}^1$ there are 4 left equivalence classes of rational functions of degree 3 with four simple branching points. If we look at the moduli space of left-right equivalence classes of such functions, we get that this space admits a degree 4 branched covering over the moduli space of unordered four-tuples of points in $\mathbb{CP}^1$, i.e. over the space $\mathbb{C}$ — the coordinate on this space being the $j$-invariant (which is defined in terms of the cross ratio $\tau$ of these points as $\frac{4}{27} \frac{(\tau^2 - \tau + 1)^3}{\tau^2(\tau - 1)^2}$). It is branched over points 0 and 1 — with a triple branching point over 0 and two double points over 1. It is natural to compactify this branched covering by adding a point $\infty$ in the target, corresponding to the case when two branching points get merged together, and two points in the source — one for the case when the rational function stays a rational function in the limit (with two double branching points and one triple) and one for the case when the rational function degenerates to a mapping from a reducible curve with two irreducible components to the sphere, with the first of these being a triple point for the branched covering. This description of course agrees well with the description of this moduli space as the modular curve $X_0(3)$.

### 2.10.2 Polynomials invertible in radicals

The theorems in section 2.9 tell that a polynomial is invertible in radicals if and only if it is a composition of polynomials of degrees $p^k$ for some prime numbers $p$ invertible in radicals having primitive monodromy groups. For prime degree we have already shown that these polynomials are (up to composition with linear functions) either the power functions $z \to z^p$, or the Chebyshev polynomial. In his work [30] Ritt has shown that if a polynomial of degree $p^k$ with $k > 1$ has primitive solvable monodromy group, then $p = 2, k = 2$, meaning that the polynomial is of degree 4. This allows an absolutely explicit characterization of polynomials invertible in radicals.

**Theorem 30.** A polynomial is invertible in radicals if and only if it is a composition of linear functions, power functions $z \to z^p$, Chebyshev polynomials and polynomials of
To see “if” direction of this theorem, we should show that power functions, Chebyshev polynomials and degree 4 polynomials are all invertible in radicals. For power functions this is trivial. Chebyshev polynomials can be inverted in radicals explicitly: to solve the equation

\[ w = T_n(z) \]

where \( T_n \) is the degree \( n \) Chebyshev polynomial, one can use the following trick. We know that Chebyshev polynomial is defined by the property that \( T_n \left( \frac{u+1/u}{2} \right) = \frac{u^n+u^{-n}}{2} \).

We can write \( w \) as \( \frac{u^n+u^{-n}}{2} \) — for this we should take \( u = \sqrt[n]{w + \sqrt{w^2 - 1}} \). Then

\[ z = \frac{u + 1/u}{2} = \frac{1}{2} \left( \sqrt[n]{w + \sqrt{w^2 - 1}} + \sqrt[n]{w - \sqrt{w^2 - 1}} \right) \]

Finally to find the inverse of a degree 4 polynomial in radicals it is clearly enough to know how to solve a degree 4 polynomial equation \( ax^4 + bx^3 + cx^2 + dx + e = 0 \) in radicals. We will show a beautiful trick [4] that reduces this problem to solving a cubic equation in radicals.

Instead of solving \( ax^4 + bx^3 + cx^2 + dx + e = 0 \) we will introduce a new variable \( y = x^2 \) and try to solve the system of equations \( ay^2 + bxy + cx^2 + dx + e = 0, y = x^2 \). Let us give names to the quadratic forms appearing in these equations

\[ Q_1(x, y) = ay^2 + bxy + cx^2 + dx + e \]

\[ Q_2(x, y) = y - x^2 \]
Consider the pencil of all quadrics defined by equations $Q_1(x, y) + \lambda Q_2(x, y) = 0$. In this pencil there are exactly three singular quadrics:

To find the parameters $\lambda$ that correspond to these singular quadrics, we should solve the cubic equation in $\lambda$ equating the discriminant of the quadric from the pencil to zero. Once this equation is solved, the points of intersection of the quadrics can be found by intersecting any pair of singular quadrics we found — this essentially amounts to simply intersecting pairs of lines.

A cubic equation that we obtained in process is in fact one we can solve already: if the cubic polynomial in question has two finite critical values, it is a Chebyshev polynomial (up to a linear change of variable). If it has only one finite critical value, it is a cube of a linear polynomial.
Chapter 3

Topological methods in Klein’s resolvent problem

The goal of this part of the thesis is to develop a topological approach to Klein’s resolvent problem, i.e. the question whether one can reduce a given algebraic equation depending on several parameters to an equation depending on a smaller number of independent parameters by means of a rational substitution. In other words the question is whether one can express a given algebraic function as a branch of a composition of rational functions and an algebraic function of some given number of parameters $k$ (see section 3.6 below for a precise formulation). The minimal number of parameters $k$ for which it is possible is called the “algebraic essential dimension” of the algebraic function, or, equivalently, of the algebraic equation defining it.

We introduce in 3.4.1 the notion of topological essential dimension of a covering: it is the minimal dimension of a base-space of a covering from which the given covering can be induced by means of a continuous mapping. In sections 3.1–3.5 we prove that the topological essential dimension of a covering over a topological torus is equal to the minimal number of generators of its monodromy group, i.e. its rank. We also prove some refinements of this result needed later in algebraic context.
In section 3.6 we formulate Klein’s resolvent problem and make a couple of preliminary observations that relate it to the notion of topological essential dimension.

In section 3.7 we describe a geometrical construction that makes the topological results on topological essential dimension of coverings over tori relevant. More precisely we describe a family of tori in a given variety in which all the tori are homotopically equivalent inside the variety and for any hypersurface one can find a torus in this family that lives in the complement to this hypersurface. If an algebraic function is defined on this variety, it induces equivalent coverings over the tori in this family. Thus we can apply topological results on coverings over tori in the context of Klein’s resolvent problem.

In section 3.7.1 we completely solve Klein’s resolvent problem for algebraic functions unramified over the algebraic torus: it turns out that the algebraic essential dimension of such function is equal to the rank of its monodromy group. In the same section we use this result to prove that the algebraic essential dimension of the universal algebraic function $z$ defined by the equation $z^n + a_1 z^{n-1} + \ldots + a_n = 0$ is at least $\left\lfloor \frac{n}{2} \right\rfloor$. In section 3.7.3 we give a more general construction which can be applied to get bounds in Klein’s resolvent problem for any given algebraic function (they are of existential character: “if one can find a flag of subvarieties in the base space with complicated enough monodromy group around it, then the algebraic essential dimension is at least equal to the rank of this monodromy group”). We apply them to reprove the bound $\left\lfloor \frac{n}{2} \right\rfloor$ for the universal algebraic function. Finally in 3.7.5 we apply these methods to show that generically one should expect that an algebraic function of degree $\geq 2k$ depending on $k$ parameters doesn’t admit any rational transformation that makes it depend on a smaller number of parameters.
3.1 Notations

3.1.1 Spaces and Their Dimensions

In this paper we are dealing with coverings over topological spaces. When we say a space what we mean is a topological space which admits a universal covering and is homotopically equivalent to a CW-complex. We say that a space is of dimension at most $k$ if it is homotopically equivalent to a CW-complex with cells of dimension at most $k$. A mapping between two spaces means a continuous mapping.

Any constructible algebraic set over the complex numbers is a space in the above sense. Moreover, a smooth affine variety of complex dimension $k$ is a space of dimension at most $k$ [20].

3.1.2 Coverings and Their Monodromy

The notation $\xi_X$ denotes a covering $p_X : (\tilde{X}, \tilde{x}_0) \to (X, x_0)$ between pointed spaces $(\tilde{X}, \tilde{x}_0)$ and $(X, x_0)$. The space $X$ is assumed to be connected, but $\tilde{X}$ is not necessarily connected.

For a given covering $\xi_X$ we can consider the monodromy representation of the fundamental group $\pi_1(X, x_0)$ on the fiber of $p_X$ over the basepoint $x_0$. Namely the monodromy representation is a group homomorphism $M_X : \pi_1(X, x_0) \to S(p_X^{-1}(x_0))$ which maps the class of a loop $\gamma$ in the fundamental group to the permutation that sends the point $\tilde{x} \in p_X^{-1}(x_0)$ to the other endpoint of the unique lift $\tilde{\gamma}$ of the loop $\gamma$ to a path in $\tilde{X}$ starting at $\tilde{x}$. The image of the monodromy representation is called the monodromy group.

In fact specifying a covering over $(X, x_0)$ is equivalent to specifying the fiber over the basepoint $x_0$, a point in this fiber, and the monodromy action of $\pi_1(X, x_0)$ on the fiber. Indeed, given a set $L$, an action $M : \pi_1(X, x_0) \to S(L)$ of the fundamental group $\pi_1(X, x_0)$ on $L$ and a point $l_0 \in L$, we can construct a covering over $(X, x_0)$, whose fiber
over $x_0$ can be identified with $L$ and with this identification the basepoint of the total space of the covering gets identified with $l_0$ and the monodromy representation of the fundamental group gets identified with $M$.

To do so let $p^u_X : (U, u_0) \rightarrow (X, x_0)$ denote the universal covering over $(X, x_0)$. The fundamental group $\pi_1(X, x_0)$ acts on the total space $U$ via deck transformations of the universal covering. We define $\tilde{X}$ as the quotient of the product space of $U \times L$ by the equivalence relation $(\alpha \cdot u, l) \sim (u, M(\alpha) \cdot l)$, where $u \in U$, $l \in L$ and $\alpha \in \pi_1(X, x_0)$. Let $[u, l]$ denote the class of point $(u, l) \in U \times L$ under this equivalence. We choose the point $\tilde{x}_0 = [u_0, l_0]$ as the basepoint of $\tilde{X}$. The covering map $p_X : (\tilde{X}, \tilde{x}_0) \rightarrow (X, x_0)$ is defined by the formula $p_X([u, l]) = p^u_X(u)$ (it is easy to see that this map is well-defined and is a covering map). Since the action of $\pi_1(X, x_0)$ on the fiber of the universal covering over $x_0$ is free and transitive, each point $[u, l] \in p_X^{-1}(x_0)$ is represented by a unique pair of the form $(u_0, l')$. We identify this point with the element $l' \in L$. With this identification the monodromy action of the constructed covering on the fiber $p_X^{-1}(x_0)$ is identified with $M$ and the basepoint $[u_0, l_0]$ gets identified with $l_0$.

### 3.2 $G$-labelled coverings

Let $G$ be a group. A $G$-labelled covering $\xi_X$ is a covering map $p_X : (\tilde{X}, \tilde{x}_0) \rightarrow (X, x_0)$ between pointed topological spaces together with an identification of the monodromy group with a subgroup of $G$. Explicitly, the labelling is an injective group homomorphism $L_X : M_X(\pi_1(X, x_0)) \rightarrow G$ from the monodromy group to $G$. We refer to the composition of the monodromy representation $M_X$ and the labelling map $L_X$ simply as “the monodromy map” $\mathcal{M}_X = L_X \circ M_X : \pi_1(X, x_0) \rightarrow G$. The image of $\mathcal{M}_X$ in $G$ is called “the monodromy group of the $G$-labelled covering”, or, if no confusion could arise, “the monodromy group”.

For every map $f : X \rightarrow Y$ and any $G$-labelled covering $\xi_Y$ we can define the induced
$G$-labelled covering $f^*\xi_Y$ over $X$ in the obvious way. For a map $f : X \to Y$ which induces a surjective homomorphism on the fundamental groups, the monodromy group of $f^*\xi_Y$ is equal to that of $\xi_Y$.

In this paper we want to deal with coverings, however the additional structure of labelling has to be introduced for the definition of characteristic classes below: the value of a characteristic class on a covering with monodromy group isomorphic to $G$ may depend on the labelling.

Note also that any covering with finite fibers can be considered as an $S(n)$-labelled covering, once the fiber over the base-point is identified with the set of labels $1, \ldots, n$.

### 3.3 Characteristic Classes for Coverings

In the definition below we use the category of coverings whose objects are coverings over connected topological spaces and morphisms between two coverings $\xi_X$ and $\xi_Y$ are pairs of maps $(f, g)$ making the diagram

$$
\begin{array}{ccc}
(\tilde{X}, \tilde{x}_0) & \xrightarrow{g} & (\tilde{Y}, \tilde{y}_0) \\
\downarrow^{p_X} & & \downarrow^{p_Y} \\
(X, x_0) & \xrightarrow{f} & (Y, y_0)
\end{array}
$$

commutative and such that $g : p_X^{-1}(x) \to p_Y^{-1}(f(x))$ is a bijection for every $x \in X$.

The category of $G$-labelled coverings has $G$-labelled coverings as objects and a morphism of $G$-labelled coverings $\xi_X$ and $\xi_Y$ is a morphism of the underlying coverings with the additional requirement about the labellings: $\mathcal{M}_X = \mathcal{M}_Y \circ f_*$.

**Definition 6.** Let $\mathcal{C}$ be any subcategory of the category of coverings or of the category of $G$-labelled coverings for some group $G$. A **characteristic class** for category $\mathcal{C}$ of degree $k$ with coefficients in an abelian group $A$ is a mapping $w$ which assigns to any covering $\xi_X$ from $\mathcal{C}$ a cohomology class $w(\xi_X) \in H^k(X, A)$ such that if $(f, g)$ is a morphism from $\xi_X$ to $\xi_Y$ then $w(\xi_Y) = f^*w(\xi_X)$. 
Here are some examples of characteristic classes.

**Example 3.** Let $G$ be a discrete group and $A$ — an abelian group. Let $(BG, b_0)$ be the classifying space for the group $G$. For $k > 0$ let $w \in H^k(BG, A)$ be any class in the cohomology of group $G$. Let $\xi_X$ be a $G$-labelled covering. The map $M_X : \pi_1(X, x_0) \to G$ gives rise to a unique homotopy class of maps $\text{cl}_X : (X, x_0) \to (BG, b_0)$ so that $M_X = \text{cl}_X* : \pi_1(X, x_0) \to \pi_1(BG, b_0) = G$. Let $w(\xi_X) \in H^k(X, A)$ be the pullback of the class $w$ through $\text{cl}_X$. It is easy to check that the class $w$ thus constructed is characteristic.

**Example 4.** Let $G$ be a finitely generated abelian group. Let $n$ be any natural number and suppose that $G/nG$ is isomorphic to $(\mathbb{Z}_n)^k$ for some $k$ (this is automatically true if $n$ is prime for example). Fix such an isomorphism of $G/nG$ with $(\mathbb{Z}_n)^k$. For a $G$-labelled covering $\xi_X$ let $c \in H^1(X, G)$ be the cohomology class obtained from $M_X$ by identification $\text{Hom}(\pi_1(X, x_0), G) \cong \text{Hom}(H_1(X), G) \cong H^1(X, G)$ (the first equality follows because $G$ is abelian). One can also think of this class as the Čech cohomology class that defines the principal $G$-bundle associated with the covering $\xi_X$.

Let now $p_j : G \to \mathbb{Z}_n$ be the composite of the quotient map $G \to G/nG$ and the projection from $(\mathbb{Z}_n)^k$ to the $j$-th factor in the product. Let $w(\xi_X)$ be the cup product of the images of $c$ under the maps $p_j* : H^1(X, G) \to H^1(X, \mathbb{Z}_n)$, i.e. $w(\xi_X) = p_1*(c) \cup \ldots \cup p_k*(c) \in H^k(X, \mathbb{Z}_n)$. Once again it is easy to see that the class $w$ is characteristic.

**Example 5.** Every $n$-sheeted covering $\xi_X$ gives rise to an $n$-dimensional real vector bundle by the change of fiber over a point $x \in X$ from $p_X^{-1}(x)$ to the real vector space spanned by the points of $p_X^{-1}(x)$. Stiefel-Whitney classes of this bundle give rise to characteristic classes for the category of $n$-sheeted coverings.

Example 3 is a very general way of constructing characteristic classes for $G$-labelled coverings (indeed, all characteristic classes can be produced this way). It involves however computing the cohomology of a group. Example 4 is an extremely simple construction, but it will prove powerful enough for our purposes: finding a topological obstruction to
inducing a given covering with abelian monodromy group from a covering over a space of a small dimension. Example 5 has been used in [2]. A variation on example 3 with group $S(n)$ and with coefficients taken in an $S(n)$-module $\mathbb{Z}$ with action given by the sign representation $S(n) \to \text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$ has been used in [33] (note however that our definition of characteristic classes is too restrictive to include this as an example).

Remark. Characteristic classes defined for all $n$-sheeted coverings are rather weak in distinguishing coverings, whose monodromy group consists only of even permutations. For example consider the degree 3 covering $\xi_X$ over the circle $X = S^1$ given by $p : S^1 \to S^1$, $p(z) = z^3$ (we think of the circle as the circle of unit-length complex numbers). Then every characteristic class $w$ (with any coefficients) vanishes on $\xi_X$. Indeed, consider figure eight $Y = S^1 \vee S^1$ with the base point $y_0$ being the common point of the two circles. Let $a, b$ denote the two loops corresponding to the two circles in figure eight. Now consider the covering $\xi_Y$ with monodromy representation sending $[a] \in \pi_1(Y,y_0)$ to the permutation $(12) \in S(3)$ and $[b] \in \pi_1(Y,y_0)$ to $(23)$. Then our covering $\xi_X$ is induced from $\xi_Y$ by mapping $g : X \to Y$ sending the loop that goes around the circle $X$ to the path $aba^{-1}b^{-1}$ in $Y$ (indeed, $(123) = (12)(23)(12)^{-1}(23)^{-1}$), and hence $w(\xi_X) = g^*(w(\xi_Y))$. However $g^* : H^1(Y) \to H^1(X)$ is clearly the zero map, so no characteristic class for 3-sheeted coverings can distinguish $\xi_X$ from the trivial covering.

By taking Cartesian product of $k$ copies of this example, we get a covering over a $k$-dimensional torus, which can be induced from a covering over some space (a product of $k$ figure-eights) through a map that induces the zero map on the reduced cohomology ring. Thus all characteristic classes defined for 3$^k$-sheeted coverings must vanish on it. In section 3.4.6 we will show that this covering can’t be induced from any covering over a space of dimension smaller than $k$, thus showing it is very far from being trivial.
3.4 Inducing Coverings from Spaces of Low Dimension

3.4.1 Topological Essential Dimension

**Definition 7.** Let $\xi_X$ be a covering. We say that the topological essential dimension of this covering is $k$ if it can be induced from a covering over a space of dimension $k$ and it cannot be induced from any covering over a space of dimension strictly smaller than $k$.

3.4.2 From Coverings to Coverings with the Same Monodromy Group

Below we show that a covering which can be induced from some other covering over a space of dimension $k$ can also be induced from a covering over a space of dimension $k$ with the same monodromy group as the original one. This makes it easier to prove lower bounds on topological essential dimension of coverings.

**Lemma 31.** Let $h : (X, x_0) \to (Y, y_0)$ be a mapping between pointed spaces. Then there exists a pointed space $(\tilde{Y}, \tilde{y}_0)$ and maps $g : (\tilde{Y}, \tilde{y}_0) \to (Y, y_0)$, $f : (X, x_0) \to (\tilde{Y}, \tilde{y}_0)$ so that $h = g \circ f$, the mapping $g$ is a covering map and the homomorphism $f_* : \pi_1(X, x_0) \to \pi_1(\tilde{Y}, \tilde{y}_0)$ induced by $f$ on the fundamental groups is surjective.

The proof of the lemma is an explicit construction: we define the covering $g : (\tilde{Y}, \tilde{y}_0) \to (Y, y_0)$ as the covering over $(Y, y_0)$ that corresponds under the Galois correspondence for coverings to the subgroup $h_*(\pi_1(X, x_0))$ in $\pi_1(Y, y_0)$ (that is we “unwind” all the loops in $Y$ that are not the images of loops from $X$). Then we define $f : (X, x_0) \to (\tilde{Y}, \tilde{y}_0)$ as the unique lifting of the mapping $h : (X, x_0) \to (Y, y_0)$ through the map $g$ (which exists because $h_*(\pi_1(X, x_0)) = g_*(\pi_1(\tilde{Y}, \tilde{y}_0))$). It remains to check that the mapping $f$ thus defined induces a surjective homomorphism on the fundamental
groups, i.e. that $f_*(\pi_1(X,x_0)) = \pi_1(\tilde{Y},\tilde{y}_0)$. Because $g_*$ is injective, this is equivalent to verifying that $g_*(f_*(\pi_1(X,x_0))) = g_*(\pi_1(\tilde{Y},\tilde{y}_0))$. This is true, since both sides are equal to $h_*(\pi_1(X,x_0))$: the left side, because $g_* \circ f_* = h_*$ and the right side — by construction.

**Lemma 32.** Let $f : (X,x_0) \to (Y,y_0)$ be a map inducing a surjective homomorphism of fundamental groups. Let covering $\xi_X$ over $X$ be induced from a covering $\xi_Y$ over $Y$ by means of the map $f$. Suppose that the covering $\xi_X$ can be $G$-labelled. Then the covering $\xi_Y$ can also be $G$-labelled in a way that the $G$-labelled covering $\xi_X$ is induced from the $G$-labelled covering $\xi_Y$ (as a $G$-labelled covering).

**Proof.** Let $M_X$ and $M_Y$ be the monodromy representations of the coverings $\xi_X$ and $\xi_Y$ and let $L_X$ be the labelling $L_X : M_X(\pi_1(X,x_0)) \to G$. We define the labelling $L_Y : M_Y(\pi_1(Y,y_0)) \to G$ as follows: a permutation in $M_Y(\pi_1(Y,y_0))$ is realized as the monodromy along some element $\alpha \in \pi_1(Y,y_0)$. Since $f_* : \pi_1(X,x_0) \to \pi_1(Y,y_0)$ is surjective by assumption, $\alpha = f_*(\beta)$ for some $\beta \in \pi_1(X,x_0)$. We define the image of the permutation we started with under $L_Y$ to be $L_X(M_X(\beta))$. This definition doesn’t depend on the choice of $\alpha$ or its preimage $\beta$ since the covering $\xi_X$ is induced from the covering $\xi_Y$ by means of $f$ (in fact the monodromy along $\beta$ doesn’t depend on the choice of $\beta$: it is the same as the permutation we started with after identifying the fiber of $p_Y$ over $y_0$ with the fiber of $p_X$ over $x_0$).

We will be mainly interested in the following corollary of these lemmas:

**Corollary 33.** Let $\xi_X$ be a $G$-labelled covering. Suppose it can be induced (as a covering, not necessarily as a $G$-labelled covering) from a covering over a space $Y$ of dimension $\leq k$. Then it can also be induced from a $G$-labelled covering over a space $\tilde{Y}$ of dimension $\leq k$ by means of a map $f : (X,x_0) \to (\tilde{Y},\tilde{y}_0)$ with the property that $f_* : \pi_1(X,x_0) \to \pi_1(\tilde{Y},\tilde{y}_0)$ is surjective.

**Proof.** Let the covering $\xi_X$ be induced from the covering $\xi_Y$ by means of the map $h : (X,x_0) \to (Y,y_0)$. From Lemma 31 above one can construct pointed space $(\tilde{Y},\tilde{y}_0)$ and
maps \( g : (\tilde{Y}, \tilde{y}_0) \to (Y, y_0) \) and \( f : (X, x_0) \to (\tilde{Y}, \tilde{y}_0) \) so that \( g \) is a covering map, \( f \) induces surjective homomorphism on the fundamental groups and \( h = g \circ f \). The space \( \tilde{Y} \) is of dimension \( \leq m \), because it covers the space \( Y \). The covering \( \xi_X \) is induced from the covering \( g^* \xi_Y \) on \( \tilde{Y} \) by means of \( f \). According to Lemma 32, the covering \( g^* \xi_Y \) can be \( G \)-labelled so that the \( G \)-labelled covering \( \xi_X \) is induced from it by means of \( f \) as a \( G \)-labelled covering.

### 3.4.3 Equivalent Coverings

It turns out that some essential properties of a covering depend only on the abstract isomorphism class of its monodromy representation, rather than on the isomorphism class of the covering itself. The purpose of this section is to show that equivalent coverings in this sense have the same topological essential dimension.

**Definition 8.** Let \( \xi_{X,1} \) and \( \xi_{X,2} \) be two coverings over the same space \( X \) with monodromy representations \( M_{X,1} : \pi_1(X, x_0) \to S(p_{X,1}^{-1}(x_0)) \) and \( M_{X,2} : \pi_1(X, x_0) \to S(p_{X,2}^{-1}(x_0)) \) respectively. The coverings \( \xi_{X,1} \) and \( \xi_{X,2} \) are called **equivalent** if there exists an isomorphism

\[
g : M_{X,1}(\pi_1(X, x_0)) \to M_{X,2}(\pi_1(X, x_0))
\]

making the following diagram commutative:

\[
\begin{array}{ccc}
\pi_1(X, x_0) & \xrightarrow{M_{X,1}} & M_{X,1}(\pi_1(X, x_0)) \\
& \searrow g \quad \swarrow M_{X,2} & \\
& M_{X,2}(\pi_1(X, x_0)) & \\
\end{array}
\]

One can think of equivalent coverings as coverings that can be obtained from each other by means of change of the fiber.

This definition is important for us because of the following lemma.

**Lemma 34.** Suppose that the covering \( \xi_{X,1} \) is induced from the covering \( \xi_{Y,1} \) by means of map \( f : (X, x_0) \to (Y, y_0) \) that induces surjective homomorphism on fundamental groups.
Let $\xi_{X,2}$ be a covering on $X$ which is equivalent to the covering $\xi_{X,1}$. Then there exists a covering $\xi_{Y,2}$ over $Y$ so that $\xi_{X,2} = f^*(\xi_{Y,2})$, that is the covering $\xi_{X,2}$ is also induced from a covering over the same space $Y$.

**Proof.** Since the covering $\xi_{X,1}$ is induced from the covering $\xi_{Y,1}$, we can identify the corresponding fibers $p_{X,1}^{-1}(x_0)$ and $p_{Y,1}^{-1}(y_0)$. Let $I : S(p_{X,1}^{-1}(x_0)) \to S(p_{Y,1}^{-1}(y_0))$ be the corresponding identification of the permutation groups. Then $I \circ M_{X,1} = M_{Y,1} \circ f_*$, where $\pi_1(X,x_0) \to S(p_{Y,1}^{-1}(y_0))$ (because $\xi_{X,1} = f^*(\xi_{Y,1})$). Let $g : M_{X,1}(\pi_1(X,x_0)) \to M_{X,2}(\pi_1(X,x_0))$ denote the isomorphism showing that the coverings $\xi_{X,1}$ and $\xi_{X,2}$ are equivalent. We define action $M_{Y,2} : \pi_1(Y,y_0) \to S(p_{X,2}^{-1}(x_0))$ as follows: let $\alpha \in \pi_1(Y,y_0)$ be any element. Since $f_* : \pi_1(X,x_0) \to \pi_1(Y,y_0)$ is surjective, we can choose $\beta \in \pi_1(X,x_0)$ so that $f_*\beta = \alpha$. Define $M_{Y,2}(\alpha)$ as $M_{X,2}(\beta)$. This definition is independent of the choice of the preimage $\beta$ of $\alpha$, because $M_{X,2}(\beta) = g(M_{X,1}(\beta)) = g(I^{-1}(M_{Y,1}(f_*\beta))) = g(I^{-1}(M_{Y,1}(\alpha)))$, and the right hand side is independent of the choice.

By construction of section 3.1.2, the action $M_{Y,2}$ defines a covering $\xi_{Y,2}$ for which $M_{Y,2}$ is the monodromy action, and since $M_{Y,2} \circ f_* = M_{X,2}$ by definition, the covering $\xi_{X,2}$ is induced from it by means of the map $f$. □

**Remark.** This lemma shows in particular that if $\xi_X$ is a covering with connected total space $\tilde{X}$ then it is equivalent to its associated Galois covering (i.e. the minimal Galois covering that dominates $\xi_X$).

### 3.4.4 Dominance

Later we need the notion of one covering being more “complicated” than another covering:

**Definition 9.** We say that a covering $\xi_{X}^1$ ($p_1 : \tilde{X}^1 \to X$) **dominates** the covering $\xi_{X}^2$ ($p_2 : \tilde{X}^2 \to X$) if there exists a covering map $p : \tilde{X}^1 \to \tilde{X}^2$ making the following diagram commutative.
Lemma 35. Suppose that the covering $\xi_X$ on $X$ can be induced from a covering $\xi_Y$ on $Y$ by means of a map $f : X \to Y$ inducing a surjective homomorphism on fundamental groups. Suppose also that the covering $\xi_X$ dominates a covering $W \to X$:

\[
\begin{array}{ccc}
\tilde{X} & \longrightarrow & W \\
p_X & & \downarrow \\
X & \downarrow & \\
\end{array}
\]

(the maps $\tilde{X} \to W$ and $W \to X$ in the diagram above are covering maps).

Then the covering $W \to X$ can be induced by means of the map $f$ from a covering on $Y$.

Proof. The proof consists of an explicit construction of the covering on $Y$ from which the covering $W \to X$ is induced by means of $f$ and is similar to the proof of Lemma 34.

Let $x_0$ be the base point in $X$ and let $y_0 = f(x_0)$ be the base point in $Y$. Denote by $F$ the fiber $p_Y^{-1}(y_0)$ of $\xi_Y$ over $y_0$. Since $\xi_X$ is induced from $\xi_Y$, the fiber of $\xi_X$ over $x_0$ can be naturally identified with $F$ as well. Let $M^X_F$ denote the monodromy action of $\pi_1(X, x_0)$ on $F$ corresponding to the covering $\xi_X$ and let $M^Y_F$ denote the monodromy action of $\pi_1(Y, y_0)$ on $F$ corresponding to the covering $\xi_Y$. Since $\xi_X = f^*(\xi_Y)$, we have $M^X_F = M^Y_F \circ f_*$. 

Denote by $Q$ the fiber of $W \to X$ over $x_0$. Let $M^X_Q$ denote the monodromy action of $\pi_1(X, x_0)$ on $Q$. Let $q : F \to Q$ denote the restriction of the covering map $\tilde{X} \to W$ to the fiber $F$. For every $\beta \in \pi_1(X, x_0)$ the diagram
commutes (this is equivalent to the fact that $\xi_X$ dominates $W \to X$).

We will now introduce an action $M_Y^X$ of $\pi_1(Y, y_0)$ on $Q$ satisfying $M_Q^X = M_Q^X \circ f_*$. This action will give rise to the required covering on $Y$ from which $W \to X$ is induced.

Let $\alpha \in \pi_1(Y, y_0)$ be any element. Let $\beta$ be any of its preimages under $f_*$. We define $M_Y^X(\alpha)$ to be $M_Q^X(\beta)$. This element in fact does not depend on the choice of $\beta$. Indeed, let $\beta'$ be another preimage of $\alpha$. Then $M_Y^X(\beta)$ and $M_Y^X(\beta')$ are equal, since both are equal to $M_Y^X(\alpha)$. But then $M_Q^X(\beta)$ and $M_Q^X(\beta')$ must be the same, since both make the diagram

$$
\begin{array}{ccc}
F & \xrightarrow{M_Y^X(\beta)} & F \\
\downarrow^q & & \downarrow^q \\
Q & \xrightarrow{M_Q^X(\beta)} & Q
\end{array}
$$

commutative and $q : F \to Q$ is surjective.

The facts that $M_Y^X$ thus defined is an action and that $M_Q^X = M_Q^X \circ f_*$ are easy to verify.

The following corollary is important to us:

**Corollary 36.** The topological essential dimension of a covering is at least as large as the topological essential dimension of any covering it dominates.

**Proof.** Lemma 31 implies that if a covering can be induced from a covering over a space of dimension $\leq k$, then is can be induced from a space of dimension $\leq k$ by means of a map that induces surjective homomorphism on fundamental groups. Lemma 35 above implies then that any covering that it dominates can also be induced from a space of dimension $\leq k$. 

□
3.4.5 Lower Bound on Topological Essential Dimension

The considerations above allow us to prove the following result:

**Theorem 37.** Suppose the topological essential dimension of a covering $\xi_X$ is $< k$ and suppose it can be $G$-labelled. Then any degree $k$ characteristic class for the category of $G$-labelled coverings vanishes on the $G$-labelled covering $\xi_X$.

**Proof.** According to Corollary 33 if the covering $\xi_X$ can be induced from a covering on a space of dimension $< k$, the corresponding $G$-labelled covering can also be induced from a $G$-labelled covering on a space of dimension $< k$. But then naturality of characteristic classes implies that any degree $k$ characteristic class for the category of $G$-labelled coverings must vanish on it.

3.4.6 Example

Before stating general results, we go back to example in remark 3.3 in section 3.3: the covering $\xi_X$ over the space $X = S^1$ given by the map $p_X : S^1 \to S^1$ sending $z \in S^1$ to $p_X(z) = z^3$ (we think of $S^1$ as of unit length complex numbers). This covering can be $\mathbb{Z}_3$-labelled in an obvious way (in fact in two ways — we have to choose one of them). Consider the covering $\xi_X \times \ldots \times \xi_X$ over $X^k$, the $k$-dimensional torus. The $\mathbb{Z}_3$-labelling of $\xi_X$ induces a $\mathbb{Z}_3 \times \ldots \times \mathbb{Z}_3$-labelling of $\xi_X \times \ldots \times \xi_X$. The characteristic class from example 4 with coefficients in $\mathbb{Z}_3$ having degree $k$ doesn’t vanish for this covering.

Theorem 37 then implies that it has topological essential dimension $k$.

3.5 Coverings over Tori

**Definition 10.** The minimal number of generators of a finitely generated abelian group $G$ is called the **rank** of $G$. 
We now proceed to proving that the topological essential dimension of a covering over the topological torus $T = (S^1)^n$ is equal to the rank of its monodromy group.

**Theorem 38.** A covering $\xi_T$ over a torus $T$ can be induced from a covering over a $k$-dimensional space if and only if the monodromy group of the covering $\xi_T$ has rank $\leq k$. In the case $\xi_T$ can be induced from a covering over some space of dimension $k$, it can also be induced from a covering over a $k$-dimensional torus $(S^1)^k$.

Before we prove this result, we describe a normal form for the equivalence class of a covering over a torus.

Let $\xi_m$ denote the covering over the circle $S^1$ given by the map $p_m : S^1 \to S^1$ sending $z \in S^1$ to $z^m \in S^1$ (we think of $S^1$ as of the circle of unit length complex numbers). Let also $\xi_\infty$ denote the covering given by the map $p_\infty : \mathbb{R} \to S^1$ sending $x \in \mathbb{R}$ to $e^{ix} \in S^1$.

Then the following lemma holds:

**Lemma 39.** Every covering over a torus $T = (S^1)^n$ is equivalent to the covering $\xi_1^s \times \xi_{m_1} \times \xi_{m_2} \times \ldots \times \xi_{m_t} \times \xi_\infty^r$ for some integer numbers $s, t, r \geq 0$ with $s + t + r = n$ and natural numbers $m_1, \ldots, m_t \geq 2$ satisfying the divisibility condition $m_1 | m_2 | \ldots | m_t$.

**Remark.** Note that the covering $\xi_1^s$ in the representation above is just the trivial degree 1 covering over the $s$-dimensional torus.

**Proof.** Let $t_0 \in T$ be an arbitrary point of the torus and let $M_T : \pi_1(T, t_0) \to S(p_T^{-1}(t_0))$ be the monodromy representation of the covering $\xi_T$. Choose a basis $e_1, \ldots, e_n$ for the free abelian group $\pi_1(T, t_0)$ so that $\pi_1(T, t_0)$ gets identified with the group $\mathbb{Z}^n$ spanned on the generators $e_1, \ldots, e_n$. The kernel of the homomorphism $M_T$ is a subgroup of $\mathbb{Z}^n$, hence it is also a free abelian group. Choose a basis $E_1, \ldots, E_q$ for the kernel. We can express each vector $E_i$ as an integer linear combination of the basis vectors $e_j$: $E_i = \sum_j a_{i,j} e_j$. By a suitable change of bases $e$ and $E$ for the lattice and its sublattice we can bring the matrix $(a_{i,j})$ to its Smith normal form, that is after a change of bases we
get $E_1 = e_1, \ldots, E_s = e_s, E_{s+1} = m_1 \cdot e_{s+1}, E_{s+2} = m_2 \cdot e_{s+2}, \ldots, E_q = m_t \cdot e_q$, where $s$ is the number of ones in the Smith normal form of the matrix, $q = s + t$ and $m_1, \ldots, m_t \geq 2$ are integers with the divisibility property $m_1 | m_2 | \ldots | m_t$.

This means that the monodromy representation $M_T$, considered as a mapping onto its image, is isomorphic to the product of trivial maps $\mathbb{Z} \to 0$ in the first $s$ coordinates, quotient maps $\mathbb{Z} \to \mathbb{Z}_{m_i}$ in the next $t$ coordinates and identity maps $\mathbb{Z} \to \mathbb{Z}$ in the remaining $r = n - s - t$ coordinates. Thus the covering $\xi_T$ is equivalent to the covering $\xi_1^s \times \xi_{m_1} \times \xi_{m_2} \times \ldots \times \xi_{m_t} \times \xi_r^r$.

We now proceed to the proof of Theorem 38.

**Proof.** Let $G$ denote the monodromy group of the covering $\xi_T$. From Lemma 39 above the covering $\xi_T$ is equivalent to the covering $\xi_1^s \times \xi_{m_1} \times \xi_{m_2} \times \ldots \times \xi_{m_t} \times \xi_r^r$ for some integers $s, t, r \geq 0$ with $s + t + r = n$ and natural numbers $m_1, \ldots, m_t$ satisfying $m_1 | m_2 | \ldots | m_t$.

The monodromy group $G$ of this covering is isomorphic to the sum of $k = t + r$ cyclic groups: $G = \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_t} \oplus \mathbb{Z}^r$. This group cannot be represented as a sum of less than $k = t + r$ cyclic groups ($k$ being the dimension of the $\mathbb{Z}_p$-vector space $G/pG$ for $p$ being some prime divisor of $m_1$).

The covering $\xi_1^s \times \xi_{m_1} \times \xi_{m_2} \times \ldots \times \xi_{m_t} \times \xi_r^r$ clearly can be induced from the covering $\xi_{m_1} \times \xi_{m_2} \times \ldots \times \xi_{m_t} \times \xi_r^r$ over $k = t + r$-dimensional torus via the projection on the last $k$ coordinates. This projection map induces a surjective homomorphism on the fundamental groups, hence the covering $\xi_T$, being equivalent to the covering $\xi_1^s \times \xi_{m_1} \times \xi_{m_2} \times \ldots \times \xi_{m_t} \times \xi_r^r$, also can be induced from a covering over $k$-dimensional torus according to Lemma 34.

It remains to show that the covering $\xi_T$ can’t be induced from a covering over a space of dimension $< k$. Suppose to the contrary that it can. Lemma 34 then tells us that the equivalent covering $\xi_1^s \times \xi_{m_1} \times \xi_{m_2} \times \ldots \times \xi_{m_t} \times \xi_r^r$ also can be induced from a space of dimension $< k$. 

Covering $\xi_s^i \times \xi_{m_1} \times \xi_{m_2} \times \ldots \times \xi_{m_t} \times \xi_{r_\infty}$ can be $G$-labelled in a natural way ($G$ being its monodromy group $\mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_t} \oplus \mathbb{Z}^r$). By Theorem 37, every degree $k$ characteristic class for the category of $G$-labelled coverings must vanish on it.

However if we consider the characteristic class of degree $k$ from example 4 with coefficients in $\mathbb{Z}_{m_1}$, we find that it doesn’t vanish!

Corollary 36 implies that a slightly stronger result holds as well:

**Theorem 40.** Suppose the covering $\xi_T$ over a torus $T$ has monodromy group of rank $k$. Then it is not dominated by any covering of topological essential dimension strictly smaller than $k$.

Later, in algebraic context, we will need a version of this result dealing with a tower of coverings dominating a given one. We state the result now:

**Theorem 41.** Suppose $\xi_T$ is a covering over the torus $T$ with monodromy group of rank $k$. Let $f : T_s \to T$ be a covering map over $T$ that factors as the composition of covering maps $T_s \xrightarrow{f_s} T_{s-1} \to \ldots \to T_1 \xrightarrow{f_1} T_0 = T$ and assume that each covering $f_i : T_i \to T_{i-1}$ is of topological essential dimension $\leq k_i$. Then the rank of monodromy group of the covering $f^*\xi_T$ is at least $k - \sum k_i$. In particular if $\sum k_i < k$, the covering $f^*\xi_T$ is not trivial.

Three lemmas will be needed to prove this theorem:

**Lemma 42.** Let $A, B, C$ be three finitely generated abelian groups that fit into the exact sequence

$$0 \to A \to B \to C \to 0.$$  

Then rank $B \leq$ rank $A +$ rank $C$.  

Chapter 3. Topological methods in Klein’s resolvent problem

Proof. Let $p$ be a prime number such that $\text{rank } B = \dim B \otimes \mathbb{Z}_p$. The exact sequence of $\mathbb{Z}_p$ vector spaces

$$A \otimes \mathbb{Z}_p \to B \otimes \mathbb{Z}_p \to C \otimes \mathbb{Z}_p \to 0$$

shows that $\dim B \otimes \mathbb{Z}_p \leq \dim A \otimes \mathbb{Z}_p + \dim C \otimes \mathbb{Z}_p$. Since $\text{rank } A \geq \dim A \otimes \mathbb{Z}_p$ and similarly for $C$, we have $\text{rank } B = \dim B \otimes \mathbb{Z}_p \leq \text{rank } A + \text{rank } C$. \hfill $\square$

This algebraic lemma is applicable in topological context due to the following:

Lemma 43. Let $(X_3,x_3) \xrightarrow{f} (X_2,x_2) \xrightarrow{g} (X_1,x_1)$ be two covering maps and assume that $X_2$ is connected and the monodromy group of $g \circ f$ is abelian. Let $G(f), G(g), G(g \circ f)$ be the monodromy groups of the coverings $f, g, g \circ f$ respectively. These monodromy groups fit into an exact sequence

$$0 \to G(f) \to G(g \circ f) \to G(g) \to 0.$$

Proof. Let $M_g$ and $M_{g \circ f}$ denote the monodromy representations of $\pi_1(X_1,x_1)$ on the permutation groups $S(g^{-1}(x_1))$ and $S((g \circ f)^{-1}(x_1))$ and let $M_f$ denote the monodromy representation of $\pi_1(X_2,x_2)$ on $S(f^{-1}(x_2))$.

The map $f$ maps the fiber $(g \circ f)^{-1}(x_1)$ to $g^{-1}(x_1)$ and hence induces a map $f_* : S((g \circ f)^{-1}(x_1)) \to S(g^{-1}(x_1))$. The restriction of this map to $G(g \circ f)$ maps $G(g \circ f)$ onto $G(g)$ because the following diagram commutes:

$$\begin{array}{ccc}
\pi_1(X_1,x_1) & \xrightarrow{M_{g \circ f}} & G(g \circ f) \subset S((g \circ f)^{-1}(x_1)) \\
& \searrow_{M_g} & \downarrow_{f_*} \\
& & G(g) \subset S(g^{-1}(x_1))
\end{array}$$

The kernel of the restriction of $f_*$ to $G(g \circ f)$ is equal to $M_{g \circ f}(\ker M_g)$. Now we claim that $M_{g \circ f}(\ker M_g)$ is isomorphic to $G(f)$.

Let $r : M_{g \circ f}(\ker M_g) \to G(f)$ be the following map: it sends a permutation of the fiber $(g \circ f)^{-1}(x_1)$ that belongs to $M_{g \circ f}(\ker M_g)$ to its restriction to the fiber $f^{-1}(x_2)$. This restriction is a permutation of $f^{-1}(x_2)$ that lies in $G(f)$ because if the initial permutation
is realized as the monodromy along a loop $\gamma$ whose class in $\pi_1(X_1, x_1)$ is in the kernel of $M_g$, then this loop lifts to a loop based at $x_2$ and the monodromy of $f$ realized along this loop is the required permutation in $G(f)$.

The map $r$ is clearly a group homomorphism. It is onto because a permutation in $G(f)$ can be realized as the monodromy of $f$ along a loop in $X_2$ based at $x_2$. The monodromy of $g \circ f$ along the image of this loop under $g$ is a preimage of the permutation we started with under $r$.

Finally we want to show that the map $r$ is one-to-one. Suppose that a permutation in $M_{g \circ f}(\ker M_g)$ restricts to a trivial permutation on the fiber $f^{-1}(x_2)$. Since this permutation is in $M_{g \circ f}(\ker M_g)$, it can be realized as the monodromy of $g \circ f$ along a loop $\gamma$ in $X_1$ based at $x_1$ that lifts to a closed loop in $X_2$ with any choice of the lift of $x_1$ to a point in $g^{-1}(x_1)$. Let $\alpha$ be one such lift with $\alpha(0) = \tilde{x}_2 \in g^{-1}(x_1)$. It is enough to show that the monodromy of $f$ along this loop is trivial. Choose a path $\beta$ in $X_2$ connecting $x_2$ to $\tilde{x}_2$. The monodromy of $g \circ f$ along the loop $g_*(\beta \alpha \beta^{-1})$ is $M_{g \circ f}(g_* \beta g_* \alpha g_* \beta^{-1}) = M_{g \circ f}(g_* \beta)M_{g \circ f}(g_* \alpha)M_{g \circ f}(g_* \beta)^{-1} = M_{g \circ f}(\gamma)$ since the monodromy group of $g \circ f$ is abelian. In particular the monodromy of $g \circ f$ along $g_*(\beta \alpha \beta^{-1})$ restricts to the trivial permutation on $f^{-1}(x_1)$, which means that the monodromy of $f$ along $\alpha$ restricts to the trivial permutation of $f^{-1}(\tilde{x}_2)$. Since this conclusion holds for any lift of $\gamma$ to a loop $\alpha$ based at any point $\tilde{x}_2 \in g^{-1}(x_1)$, the monodromy of $g \circ f$ along $\gamma$ is trivial. \qed

This lemma can be applied to prove the following claim about coverings over a torus:

**Lemma 44.** Let $T_k \xrightarrow{f_k} T_{k-1} \rightarrow \ldots \rightarrow T_1 \xrightarrow{f_1} T_0$ be a sequence of covering maps, where $T_0$ is a torus, $T_1, \ldots, T_{k-1}$ are connected, while $T_k$ is not necessarily connected. Then rank of the monodromy group of the composite covering $f_k \circ \ldots \circ f_1$ is smaller than or equal to the sum of the ranks of the monodromy groups of the coverings $f_i$.

**Proof.** The proof is a simple induction on $k$ based on the fact that the fundamental group
of a torus is a finitely generated abelian group and the previous two lemmas.

Finally this allows us to prove Theorem 41:

Proof. Theorem 38 implies that the rank of monodromy group of the covering \( f_i : T_i \to T_{i-1} \) is at most \( k_i \). If we denote by \( \tilde{k} \) the rank of the monodromy of the covering \( f^* \xi_T \), then the lemma above implies that the rank of the composition of the covering \( f^* \xi_T \) with \( f \) is at most \( \tilde{k} + \sum k_i \). On the other hand this rank is at least \( k \), since this covering dominates the covering \( \xi_T \). Hence \( \tilde{k} \geq k - \sum k_i \).

3.6 Klein’s Resolvent Problem

3.6.1 Algebraic Functions — Definition

We are going to use below the phrases “algebraic function”, “composition of rational and algebraic functions”, “branched covering associated to an algebraic function” and so on. In this small section we define these notions.

Definition 11. An algebraic function \( z \) on an irreducible variety \( X \) is a choice of a branched covering \( \tilde{X} \to X \) and a regular function \( z : \tilde{X} \to \mathbb{C} \). We say that \( z \) is an algebraic function defined over \( X \). The variety \( \tilde{X} \) is called the Riemann surface of \( z \) (even though it is not necessarily a surface).

An algebraic function \( z' \) with Riemann surface \( \tilde{X}' \) is called a restriction of algebraic function \( z \) with Riemann surface \( \tilde{X} \) if there exist a branched covering \( \tilde{X}' \to \tilde{X} \) making the following diagram commutative
Two algebraic functions are called equivalent if they are both restrictions of the same algebraic function.

**Example 6.** The universal algebraic function of degree \( n \) is the function \( z \) on \( \mathbb{C}^n \) defined by the equation \( z^n + a_1 z^{n-1} + \ldots + a_n = 0 \), i.e. the function

\[
\begin{array}{ccc}
\tilde{\mathbb{C}}^n & \xrightarrow{z} & \mathbb{C} \\
\downarrow^{(a_1, \ldots, a_n)} & & \\
\mathbb{C}^n & & \\
\end{array}
\]

where \( \tilde{\mathbb{C}}^n = \{(z, a_1, \ldots, a_n) | z^n + a_1 z^{n-1} + \ldots + a_n = 0 \} \).

This function is called universal, because any algebraic function \( w \) of degree \( n \) can be induced from it. More precisely if \( w \) is the function

\[
\begin{array}{ccc}
\tilde{W} & \xrightarrow{w} & \mathbb{C} \\
\downarrow^{p} & & \\
W & & \\
\end{array}
\]

then it fits into a diagram

\[
\begin{array}{ccc}
\tilde{W} & \xrightarrow{w} & \tilde{\mathbb{C}}^n \\
\downarrow & & \downarrow \\
W & \xrightarrow{p} & \mathbb{C} \\
\end{array}
\]

where the arrow in the lower row sends a point in \( W \) to the elementary symmetric functions of the values of \( w \) at that point.

An algebraic function has in fact a natural Riemann surface. Namely to a function

\[
\begin{array}{ccc}
\tilde{X} & \xrightarrow{z} & \mathbb{C} \\
\downarrow^{p} & & \\
\tilde{X} & & \\
\end{array}
\]

we associate an equivalent algebraic function with Riemann surface \( \tilde{X}_z = \{(x, t) \in X \times \mathbb{C} | \exists \tilde{x} \in \tilde{X} \text{ with } p(\tilde{x}) = x, z(\tilde{x}) = t \} \). We then define \( z(x, t) = t \) and \( p(x, t) = x \) for \( (x, t) \in \tilde{X}_z \). We also define a map from \( \tilde{X} \) to \( \tilde{X}_Z \) by sending \( \tilde{x} \in \tilde{X} \) to \((p(\tilde{x}), z(\tilde{x}))\). With these definitions the following diagram becomes commutative
showing that the function we started with is equivalent to the one we defined.

Given two algebraic functions $z_1, z_2$ with Riemann surfaces $\tilde{X}_1$ and $\tilde{X}_2$ respectively, one can find a common Riemann surface for them (i.e. find $\tilde{X}$, a map $\tilde{X} \to X$ and functions $z_1', z_2'$ on $\tilde{X}$ such that $z_i'$ is a restriction of $z_i$). Namely one can take $\tilde{X} = \tilde{X}_1 \times_X \tilde{X}_2$ and $z_i'$ to be the pullback of $z_i$ to $\tilde{X}$ through the obvious maps from $\tilde{X}$ to $\tilde{X}_1$ and $\tilde{X}_2$.

With this construction one can define sums, products and quotients of algebraic functions (the quotient being defined only where the denominator doesn’t vanish).

**Example 7.** In question 9 below we will need to give an interpretation of an expression $R(x, z(x))$ for a regular function $R : X \times \mathbb{C} \to \mathbb{C}$ and an algebraic function

$$
\begin{array}{c}
\tilde{X} \\
p \\
\downarrow \\
X
\end{array}
\xrightarrow{z} \mathbb{C}
$$

This expression is defined as the algebraic function

$$
\begin{array}{c}
\tilde{X} \\
p \\
\downarrow \\
X
\end{array}
\xrightarrow{R \circ (p, z)} \mathbb{C}
$$

Here $R \circ (p, z)$ is the composition $\tilde{X} \xrightarrow{(p, z)} X \times \mathbb{C} \xrightarrow{R} \mathbb{C}$.

**Remark.** Since the domain of an algebraic function is not assumed to be irreducible, the algebraic function might have several independent branches.

**Remark.** According to our definition the sum $\sqrt{x} + \sqrt{x}$ is defined as $z + w$ on the variety $\{(x, z, w) \in \mathbb{C}^3 | z^2 = x, w^2 = x\}$, i.e. it has two independent branches: $2\sqrt{x}$ and 0.
3.6.2 Statement of the Problem

Klein’s resolvent problem is the problem of deciding whether a given algebraic equation depending on several independent parameters admits a rational transformation transforming it into an equation depending on a smaller number of algebraically independent parameters (see [8]).

More precisely we introduce the following definition:

**Definition 12.** An algebraic function \( z \) defined over a Zariski open subset of a variety \( X \) is said to be **rationally induced** from an algebraic function \( w \) defined over a Zariski open subset of a variety \( Y \) if there exists a Zariski open subset \( U \) of \( X \), a rational morphism \( r \) from \( X \) to \( Y \) and a rational function \( R \) on \( X \times \mathbb{C} \) such that:

- the function \( z(x) \) is defined for all \( x \in U \),
- the function \( R(x, w(r(x))) \) is defined for all \( x \in U \),
- the function \( z(x) \) is a branch of \( R(x, w(r(x))) \) for \( x \in U \).

It is assumed that the functions \( r(x) \), \( w(r(x)) \) and \( R(x, w(r(x))) \) are all defined for \( x \in U \).

This definition can be used to formulate Klein’s resolvent problem precisely:

**Example 8.** The function \( z \) on \( \mathbb{C}^n \) defined by \( z^n + a_1 z^{n-1} + \ldots + a_n = 0 \) can be rationally induced from the function \( w \) on \( \mathbb{C}^{n-1} \) defined by \( w^n + b_2 w^{n-2} + \ldots + b_n = 0 \). To see this let \( R(a_1, \ldots, a_n, w) = w - \frac{a_1}{n} \) and let \( r : \mathbb{C}^n \to \mathbb{C}^{n-1} \) be the mapping that sends \( (a_1, \ldots, a_n) \) to the coefficients \( b_2, \ldots, b_n \) in the expansion \( (w - \frac{a_1}{n})^n + a_1 (w - \frac{a_1}{n})^{n-1} + \ldots + a_n = w^n + b_2 w^{n-1} + \ldots + b_n \). Here \( U \) can be taken as \( \mathbb{C}^n \).

**Example 9.** The function \( w \) on \( \mathbb{C}^{n-1} \) defined by \( w^n + b_2 w^{n-2} + \ldots + b_n = 0 \) can be rationally induced from a function \( y \) on \( \mathbb{C}^{n-2} \) defined by \( y^n + c_2 y^{n-2} + \ldots + c_{n-2} y^2 + c_{n-1} y + c_{n-1} = 0 \). To see this let \( R(b_2, \ldots, b_n, y) = \frac{b_n}{b_{n-1}} y \) and let \( r : \mathbb{C}^{n-1} \to \mathbb{C}^{n-2} \) be
defined by

\[ r(b_2, \ldots, b_n) = (\left( \frac{b_{n-1}}{b_n} \right)^2 b_2, \left( \frac{b_{n-1}}{b_n} \right)^3 b_3, \ldots, \left( \frac{b_{n-1}}{b_n} \right)^{n-1} b_{n-1}). \]

Here \( U \) can be taken as the set defined by \( b_{n-1} \neq 0, b_n \neq 0 \) in \( \mathbb{C}^{n-1} \).

**Question 9** (Klein’s resolvent problem for algebraic functions). Given an algebraic function \( z \) on an irreducible variety \( X \) what is the smallest number \( k \) such that the function \( z \) can be rationally induced from an algebraic function \( w \) on some variety \( Y \) of dimension \( \leq k \)?

The examples preceding this section show that for the universal algebraic function of degree \( n \) the answer to this question is at most \( n - 2 \).

As most of the arguments for treating this question will be geometrical in nature, we would like to restate this question in geometric terms. Instead of an algebraic function we will talk of a branched covering defined by it (see section \[3.6.1\] above). Question \[9\] can then be reformulated:

**Definition 13.** A branched covering \( \xi_X \) over an irreducible variety \( X \) is **rationally induced** from a branched covering \( \xi_Y \) over a variety \( Y \) if there exists a dominant rational morphism \( f : X \to Y \) and a Zariski open subset \( U \) of \( X \) such that the restriction of the branched covering \( \xi_X \) to \( U \) is a covering and this covering is dominated by the restriction of the branched covering \( f^*(\xi_Y) \) to \( U \) (the mapping \( f \) is assumed to be defined everywhere on \( U \)).

**Question 10** (Klein’s resolvent problem for branched coverings). Let \( \xi_X \) be a branched covering over an irreducible variety \( X \). For what numbers \( k \) there exists a branched covering \( \xi_Y \) over an irreducible variety \( Y \) of dimension \( k \), such that the branched covering \( \xi_X \) can be rationally induced from it?

The questions above have very close analogues that can be formulated algebraically in terms of field extensions (see \[7,6\]):
Question 11 (Essential dimension of field extension). Let $E/K$ be a finite degree extension of fields and suppose $K$ is of finite transcendence degree over $\mathbb{C}$. For what numbers $k$ there exists a field $e \subset E$ of transcendence degree $k$ over $\mathbb{C}$ so that $E = K(e)$?

In other words we are trying to get the extension $E/K$ by adjoining to the field of rationality $K$ “irrationalities” (elements of $e$) depending on as few parameters as possible (the number of parameters being the transcendence degree of $e$ over $\mathbb{C}$).

The minimal number of such parameters is called the essential dimension of the extension $E/K$.

Questions 10 and 11 become equivalent if in question 10 one allows only branched coverings with irreducible total spaces. Alternatively they become equivalent if in question 11 one replaces field extension $E/K$ by an étale algebra $E$ over $K$.

We will discuss only questions 9, 10.

Hilbert has formulated a version of Klein’s resolvent problem as problem 13 in his famous list. While his question has been formulated with continuous functions (and has been answered by Kolmogorov and Arnold), one closely related and completely open question about algebraic function is the following:

Question 12 (Algebraic version of Hilbert’s 13th problem). Let $E/K$ be a finite field extension. What is the smallest number $k$ such that there exist a tower of field extensions $K = K_0 \subset K_1 \subset \ldots \subset K_n$ with the property that $E$ is contained in $K_n$ and each extension $K_i/K_{i-1}$ is of essential dimension at most $k$?

In the language of branched coverings its analogue is as follows:

Question 13 (A version of Hilbert’s 13th problem for branched coverings). Let $\xi_X$ be a branched covering over an irreducible variety $X$. What is the smallest number $k$ for which one can find a Zariski open set $U \subset X$ and a tower of branched coverings $X_n \rightarrow X_{n-1} \rightarrow \ldots \rightarrow X_0 = X$ such that the restriction of $\xi_X$ to $U$ is a covering which is dominated by the restriction of the composite branched covering $X_n \rightarrow X_0$ to $U$ and such that each
branched covering $X_i \rightarrow X_{i-1}$ can be rationally induced from a branched covering over a space of dimension $\leq k$?

While we can’t say anything intelligent about this question, we can prove some lower bound on the length of the tower for any fixed $k$. To state a precise result we need the following definition:

**Definition 14.** A branched covering $\xi_X$ on a variety $X$ is said to be dominated by a tower of extensions of dimensions $k_1, \ldots, k_n$ if there exists a tower of branched coverings $X_n \rightarrow X_{n-1} \rightarrow \ldots \rightarrow X_0 = X$ such that $\xi_X$ is a subcovering of a covering dominated by the covering $X_n \rightarrow X$ over some Zariski open set $U \subset X$ and each covering $X_i \rightarrow X_{i-1}$ can be rationally induced from a space of dimension at most $k_i$.

### 3.6.3 Especially Interesting Cases

Due to its universal nature the case when $X = \mathbb{C}^n$ and $z = z(x_1, \ldots, x_n)$ is the universal algebraic function satisfying $z^n + x_1 z^{n-1} + \ldots + x_n = 0$ was especially interesting to classics. This case was considered by Kronecker and Klein in [21] for $n = 5$.

Classics were also interested in the special case when the algebraic function is as before, but the domain on which it is defined supports the square root of the discriminant as a rational function on it. Namely

$$X = \{(x_1, \ldots, x_n, D)|D^2 = \text{discriminant of } z^n + x_1 z^{n-1} + \ldots + x_n = 0\}.$$ 

In particular Kronecker showed that for $n = 5$ this function can’t be rationally induced from a space of dimension one.

### 3.6.4 From Algebra to Topology

The following lemma allows us to use topological considerations to approach question 9.
Lemma 45. Suppose that an algebraic function $z$ over a variety $X$ is rationally induced from an algebraic function $w$ on a variety $Y$ of dimension $k$. Then there exists a Zariski open subset $U$ such that the covering associated to the restriction of the algebraic function $z$ to $U$ has topological essential dimension $\leq k$.

This lemma tells that if an algebraic function has algebraic essential dimension $k$, then its restriction to some Zariski open subset has topological essential dimension at most $k$.

Proof. According to definition 12 there exist a rational morphism $r$ from $X$ to $Y$, a rational function $R$ on $X \times \mathbb{C}$ and a Zariski open set $U$ of $X$ such that $z(x)$ is a branch of the function $R(x, w(r(x)))$ for $x \in U$.

By replacing $Y$ by the image of $r$, we can assume that $r$ is dominant. By further replacing $Y$ by its Zariski open subset and shrinking $U$ if necessary, we can assume that $Y$ is affine. By shrinking $U$ further we can also assume that the covering associated to the algebraic function $x \to R(x, w(r(x)))$ is unramified over $U$.

Since $Y$ is affine variety, it is Stein and hence is homotopically equivalent to a topological space of dimension $\leq k$. In particular the covering associated to the algebraic function $x \to w(r(x))$ over $U$ can be induced from a space of dimension $\leq k$. Since the covering associated to $x \to R(x, w(r(x)))$ is dominated by it, Corollary 36 implies that is also can be induced from a space of dimension $\leq k$. Finally, because the function $z(x)$ is a branch of $x \to R(x, w(r(x)))$, the covering associated to it can also be induced from a space of dimension $\leq k$. \hfill \Box

In a similar fashion we can prove the following:

Lemma 46. Suppose that an algebraic function $z$ over a variety $X$ is dominated by a tower of extensions of dimensions $k_1, \ldots, k_n$. Then there exists a Zariski open subset $U$ such that the covering associated to the restriction of the algebraic function $z$ to $U$ is
dominated by a covering that is a composition of coverings \( U_n \to U_{n-1} \to \ldots \to U_0 = U \) such that each \( U_i \to U_{i-1} \) has topological essential dimension \( \leq k_i \).

3.7 Results in Klein’s resolvent Problem

3.7.1 Algebraic functions on the algebraic torus

In this section we completely answer question [9] for algebraic functions unramified on \((\mathbb{C} \smallsetminus \{0\})^n\). Before we do so, we show by example that the problem is not completely trivial.

Example 10. Let \( z(x, y) = \sqrt{x} + \sqrt[3]{y} \). We claim that it is induced from an algebraic function of one variable. Namely, one can verify that

\[
\sqrt{x} + \sqrt[3]{y} = \frac{y}{x} \left( \left( \sqrt[3]{\frac{x^3}{y^2}} \right)^2 + \left( \sqrt[3]{\frac{x^3}{y^2}} \right)^3 \right),
\]

so if we let \( R(x, y, w) = \frac{y}{x}(w^2+w^3), w(r) = \sqrt{r}, r(x, y) = \frac{x^3}{y^2} \), then \( z(x, y) = R(x, y, w(r(x, y))) \) for \( x, y \neq 0 \).

On the other hand a similarly looking function \( \sqrt{x} + \sqrt[3]{y} \) can’t be rationally induced from an algebraic function of one variable, as Theorem 47 below shows.

Now we state the main result of this section. In what follows \( \mathbb{C}^* \) stands for \( \mathbb{C} \smallsetminus \{0\} \).

Theorem 47. Let \( z \) be an algebraic function on the torus \((\mathbb{C}^*)^n\) unramified over \((\mathbb{C}^*)^n\). Let \( k \) denote the rank of its monodromy group. Then \( z \) can be rationally induced from an algebraic function on \((\mathbb{C}^*)^k\) and it cannot be rationally induced from an algebraic function on a variety of dimension \(< k\).

Moreover, it is dominated by a tower of extensions of dimensions \( k_1, \ldots, k_s \) if and only if \( k_1 + \ldots + k_s \geq k \).

Proof. We first show that \( z \) can be rationally induced from an algebraic function on \((\mathbb{C}^*)^k\).
A choice of coordinates $x_1, \ldots, x_n$ on $(\mathbb{C}^*)^n$ gives rise to a choice of generators $\gamma_1, \ldots, \gamma_n$ of $\pi_1((\mathbb{C}^*)^n)$, because $(\mathbb{C}^*)^n$ retracts to the torus $|x_1| = 1, \ldots, |x_n| = 1$ and the corresponding $\gamma_i$ is the loop in this torus for which all $x_j$ are constant for $j \neq i$ (with $dx_i/x_i$ defining the positive orientation on it). A toric change of coordinates in $(\mathbb{C}^*)^n$ gives rise to a linear change of generators in $\pi_1((\mathbb{C}^*)^n)$.

Let $A$ denote the subgroup of loops in $\pi_1((\mathbb{C}^*)^n)$ that leave all the branches of $z$ invariant under the monodromy action.

Choose coordinates $x_1, \ldots, x_n$ in $(\mathbb{C}^*)^n$ so that $A = \langle \gamma_1^{m_1}, \ldots, \gamma_n^{m_n} \rangle$ with $m_n|m_{n-1}| \cdots |m_1$ (this is possible because of Smith normal form theorem mentioned in the proof of Lemma 39). Since $k$ is the rank of the monodromy group $\pi_1((\mathbb{C}^*)^n)/A$, we have $m_{k+1} = 1, \ldots, m_n = 1$.

The function $\psi(x_1, \ldots, x_n) = z(x_1^{m_1}, \ldots, x_n^{m_n})$ is invariant under monodromy action, hence is rational. Hence

$$z(x_1, \ldots, x_n) = \psi(x_1^{1/m_1}, \ldots, x_k^{1/m_k}, x_{k+1}, \ldots, x_n),$$

where $\psi$ is rational.

The primitive element theorem implies that the field extension

$$\mathbb{C}(x_1^{1/m_1}, \ldots, x_k^{1/m_k})/\mathbb{C}(x_1, \ldots, x_k)$$

is generated by one element, say the algebraic function $w(x_1, \ldots, x_k)$. But then each $x_i^{1/m_i}$ is a rational function of $w$: $x_i^{1/m_i} = r_i(x, w(x))$, where $x$ stands for $(x_1, \ldots, x_k)$.

Hence the function

$$z(x_1, \ldots, x_n) = \psi(r_1(w(x), x), \ldots, r_k(w(x), x), x_{k+1}, \ldots, x_n)$$

where $x = (x_1, \ldots, x_k)$ is rationally induced from the function $w$ on $(\mathbb{C}^*)^k$.

Moreover, if $k_1 + \ldots + k_s \geq k$ then the function $z$ lies in the extension of the field of rational functions on $(\mathbb{C}^*)^n$ by first adding to it the first $k_1$ functions $x_i^{m_i}$, then the next $k_2$ and so on. By what we have already showed $j$-th step can be accomplished by adding
one algebraic function that can be rationally induced from a space of dimension $k_j$. This shows that $z$ is dominated by a tower of extensions of dimensions $k_1, \ldots, k_s$.

Now suppose that the function $z$ is rationally induced from an algebraic function over a variety $Y$ of dimension smaller than $k$.

Lemma 45 then implies that there exists a Zariski open subset $U$ of $(\mathbb{C}^*)^n$ over which the covering associated to the algebraic function $z$ can be induced from a topological space of dimension $< k$.

It follows from the results in [24] that for sufficiently small $\epsilon_1, \ldots, \epsilon_n$ the torus $|x_1| = \epsilon_1, \ldots, |x_n| = \epsilon_n$ lies entirely inside $U$: see remark 3.7.1 below for an informal explanation of this result.

The space $(\mathbb{C}^*)^n$ can be retracted onto this torus. Hence the monodromy group of the restriction of the covering associated to $z$ to this torus coincides with the full monodromy group of $z$ over $(\mathbb{C}^*)^n$ and thus its rank is $k$ as well. But then Theorem 38 tells that this covering can’t be induced from a covering over a space of dimension $< k$. This however contradicts Lemma 45.

Similar proof shows that if the function $z$ is dominated by a tower of extensions of dimensions $k_1, \ldots, k_s$ then $k \leq k_1 + \ldots + k_s$, except instead of Lemma 45 we use Lemma 46 and instead of the topological result 38 we use the Theorem 41. \hfill \Box

Remark. The proof of the result above relies crucially on the following observation

**Theorem 48.** If $\Sigma \subset \mathbb{C}^n$ is an algebraic hypersurface, then for some numbers $\epsilon_1, \ldots, \epsilon_n$ the torus $|x_1| = \epsilon_1, \ldots, |x_n| = \epsilon_n$ lies entirely in $\mathbb{C}^n \setminus \Sigma$.

**Proof.** Let $C_i$ denote the $i$-dimensional plane $x_{i+1} = \ldots = x_n = 0$. Define $\Sigma_i$ inductively as follows: $\Sigma_n = \Sigma$. For each $0 \leq i \leq n - 1$ define $\Sigma_i$ as the intersection of $C_i$ with the closure of the union of irreducible components of $\Sigma_{i+1}$ that are not equal to $C_i$. Each $\Sigma_i$ is thus a hypersurface in $C_i$.

Choose $\epsilon_1 > 0$ to be smaller than the distance from the origin to the closest non-zero point among the points in $\Sigma_1$. Let $T_1$ be the circle $|x_1| = \epsilon_1$ in $C_1$. 
Each irreducible component of $\Sigma_2$ is either disjoint from $T_1$, or is equal to $C_1$ (indeed, if it contains a point of $T_1$, this point must be not in $\Sigma_1$ and hence by definition of $\Sigma_1$ the irreducible component must be equal to $C_1$). Let $\varepsilon_2 > 0$ be smaller than the distance from $T_1$ to the closest irreducible component of $\Sigma_2$ that is not equal to $C_1$. The torus $T_2$ defined by $|x_1| = \varepsilon_1, |x_2| = \varepsilon_2$ in $C_2$ is by definition disjoint from $\Sigma_2$.

We continue to define $\varepsilon_i$ and $T_i$ inductively in exactly the same manner until we get to $T_n$ which is disjoint from $\Sigma_n = \Sigma$.

The construction of such torus is justified in more details in [24]. In the same paper a more general construction (with the ambient space $C^n$ replaced by an arbitrary algebraic variety and the flag $C_0 \subset C_1 \subset \ldots \subset C_{n-1}$ replaced by an arbitrary flag of subvarieties) is given. We use it in 3.7.3 below.

These tori have been originally used in [2] to prove multidimensional reciprocity laws (see also [22], [23]).

3.7.2 Application to Universal Algebraic Function

We can use this theorem to prove some bounds for the questions in section 3.6.3 for the universal algebraic function of degree $n$.

**Theorem 49.** Let $z(x_1, x_2, \ldots, x_n)$ denote the universal algebraic function of degree $n$ (i.e. the function satisfying $z^n + x_1z^{n-1} + \ldots + x_n = 0$). The function $z$ has algebraic essential dimension at least $\lfloor \frac{n}{2} \rfloor$, i.e. it can’t be rationally induced from an algebraic function over a space of dimension $< \lfloor n/2 \rfloor$.

**Proof.** Suppose that $n = 2k$ is even.

Consider the mapping $S$ that sends $(a_1, \ldots, a_k, s_1, \ldots, s_k) \in C^{2k}$ to the coefficients $(x_1, \ldots, x_n)$ satisfying

$$\prod_{i=1}^{k}(w - (a_i + s_i))(w - (a_i - s_i)) = w^n + x_1w^{n-1} + \ldots + x_n.$$
It is easy to check that the mapping $S$ is onto, hence if the function $z$ can be rationally induced from an algebraic function over a space of dimension at most $k$, then the pullback of $z$ through $S$ also can.

Notice however that the pullback of $z$ through $S$ is the function $w = w(a_1, \ldots, a_k, s_1, \ldots, s_k)$ satisfying
\[
\prod_{i=1}^{k} (w - (a_i + \sqrt{s_i})) (w - (a_i - \sqrt{s_i})) = 0.
\]
This function is an algebraic function unramified over the algebraic torus with coordinates $a_1, \ldots, a_k, s_1, \ldots, s_k$ and its monodromy group is isomorphic to $\mathbb{Z}_2^k$, i.e. has rank $k$. By Theorem [17] this function can’t be induced from an algebraic function over a space of dimension $< k$ and hence $z$ also can’t.

If $n = 2k + 1$ is odd, we can apply the same argument to the function $w$ satisfying
\[
\left(\prod_{i=1}^{k} (w - (a_i + \sqrt{s_i})) (w - (a_i - \sqrt{s_i}))\right) (w - a_{k+1}) = 0.
\]

Similar technique can be applied to analyse what happens if the square root of discriminant is adjoined to the domain of rationality. Namely we can prove the following theorem:

**Theorem 50.** Let $z(x_1, x_2, \ldots, x_n)$ denote the algebraic function satisfying the equation
\[
z^n + x_1 z^{n-1} + \ldots + x_n = 0
\]
on the variety
\[
\{(x_1, \ldots, x_n, d) \in \mathbb{C}^n \times \mathbb{C}| d^2 = \text{discriminant of } z^n + x_1 z^{n-1} + \ldots + x_n = 0\}.
\]
The function $z$ has algebraic essential dimension at least $2\lfloor n/4 \rfloor$, i.e. it can’t be rationally induced from an algebraic function over a space of dimension $< 2\lfloor n/4 \rfloor$. 
Proof. Suppose that \( n = 4k \) is divisible by four.

Let \( w_i \) denote the expressions

\[
\begin{align*}
w_{4i} &= a_i + \sqrt{s_i} + \sqrt{t_i} + b_i \sqrt{s_i t_i} \\
w_{4i+1} &= a_i - \sqrt{s_i} + \sqrt{t_i} - b_i \sqrt{s_i t_i} \\
w_{4i+2} &= a_i + \sqrt{s_i} - \sqrt{t_i} - b_i \sqrt{s_i t_i} \\
w_{4i+3} &= a_i - \sqrt{s_i} - \sqrt{t_i} + b_i \sqrt{s_i t_i}
\end{align*}
\]

and let the function \( w = w(a_1, \ldots, a_k, b_1, \ldots, b_k, s_1, \ldots, s_k, t_1, \ldots, t_k) \) satisfy \( \prod_{i=1}^{4k} (w - w_i) = 0 \). The monodromy of this algebraic function is realized by even permutations only, hence its discriminant is a square of some rational function in the variables \( a, b, s, t \). Hence this algebraic function can be induced from the function \( z \) in the statement of the theorem by means of a map \( S \) that sends the point \( (a_1, \ldots, a_k, b_1, \ldots, b_k, s_1, \ldots, s_k, t_1, \ldots, t_k) \) to the point \( (x_1, \ldots, x_n, d) \) where \( x_1, \ldots, x_n \) are the coefficients of the expanded version of the equation \( \prod_{i=1}^{4k} (z - w_i) = z^n + x_1 z^{n-1} + \ldots + x_n \) that \( w \) satisfies and \( d \) is the rational function whose square is equal to the discriminant of \( w \). The image of the mapping \( S \) is in fact dense in \( X \). Indeed, if \( (x_1, \ldots, x_{4k}, d) \) is a point in \( X \), denote by \( z_1, \ldots, z_{4k} \) the roots of the equation \( z^n + x_1 z^{n-1} + \ldots + x_n = 0 \). Then the equations

\[
\begin{align*}
a_i &= \frac{z_{4i} + z_{4i+1} + z_{4i+2} + z_{4i+3}}{4} \\
\sqrt{s_i} &= \frac{z_{4i} - z_{4i+1} + z_{4i+2} - z_{4i+3}}{4} \\
\sqrt{t_i} &= \frac{z_{4i} + z_{4i+1} - z_{4i+2} - z_{4i+3}}{4} \\
b_i \sqrt{s_i t_i} &= \frac{z_{4i} - z_{4i+1} - z_{4i+2} + z_{4i+3}}{4}
\end{align*}
\]

are clearly solvable for the variables \( a_i, b_i, s_i, t_i \) for \( (z_1, \ldots, z_{4k}) \) in a Zariski open subset of \( \mathbb{C}^{4k} \) and the solution is a point that gets mapped by means of \( S \) either to \( (x_1, \ldots, x_{4k}, d) \) or to \( (x_1, \ldots, x_{4k}, -d) \). Since \( X \) is irreducible, the image of \( S \) is a dense Zariski open set in \( X \).
Hence if the function \( z \) can be rationally induced from an algebraic function on a space of dimension \(< 2k\), the function \( w \) also can. However \( w \) is an algebraic function that is unramified on the algebraic torus with coordinates \( a, b, s, t \) and its monodromy group is isomorphic to \((\mathbb{Z}_2^2)^k\), i.e. has rank \( 2k \). By Theorem 47 this function can’t be rationally induced from an algebraic function on a space of dimension \(< 2k\).

In case \( n = 4k+1 \) we can consider instead of \( w \) from the argument above the function \( w(a_1, \ldots, a_{k+1}, b_1, \ldots, b_k, s_1, \ldots, s_k, t_1, \ldots, t_k) \) satisfying \((\prod_{i=1}^{4k} (w - w_i))(w - a_{k+1}) = 0\) with the same \( w_i \) as above.

Cases \( n = 4k + 2 \) and \( n = 4k + 3 \) can be handled in the same way.

### 3.7.3 Lower Bound from Local Monodromy Around a Flag

Theorem 47 about algebraic functions unramified on the algebraic torus \((\mathbb{C}^*)^n\) has a local analogue.

**Definition 15.** An algebraic function \( z \) defined over a classically open subset \( V \) of a complex algebraic variety \( X \) is said to be **meromorphically induced** from an algebraic function \( w \) defined on a classically open subset of a complex algebraic variety \( Y \) if there exists a Zariski open subset \( U \) of \( X \), an analytic mapping \( r \) from \( U \cap V \) to \( Y \) and an \( \epsilon \)-meromorphic function \( R \) on \( V \times \mathbb{C} \) such that:

- the function \( R(x, w(r(x))) \) is defined for all \( x \in U \cap V \),
- the function \( z(x) \) is a branch of \( R(x, w(r(x))) \) for \( x \in U \cap V \).

**Theorem 51.** Let \( z \) be a germ at the origin \((0, \ldots, 0)\) of an algebraic function defined on \((\mathbb{C} \setminus \{0\})^n\) such that for every algebraic function representing the germ there exists an \( \epsilon > 0 \) such that this algebraic function is unramified on the punctured polydisc \( \{ (x_1, \ldots, x_n) \in (\mathbb{C}^*)^n \text{ with } 0 < |x_i| < \epsilon \text{ for all } i \} \). Let \( k \) denote the rank of its monodromy group on this punctured polydisc (it is obviously the same for all representatives of the germ). Then the restriction of \( z \) to this polydisc can be meromorphically induced from an algebraic...
function on \( \mathbb{C}^k \) and it cannot be meromorphically induced from an algebraic function on a variety of dimension \(< k\) by means of a germ at the origin of a meromorphic mapping.

Moreover \( z \) is dominated by a germ at origin of a tower of extensions of dimensions \( k_1, \ldots, k_s \) if and only if \( k_1 + \ldots + k_s \geq k \).

The proof of this version of Theorem 47 practically coincides with the proof of Theorem 47 itself.

We will now present a construction that allows one to use this result to obtain some information about any algebraic function. To do so we recall the concept of a Parshin point and a neighbourhood of a Parshin point:

**Definition 16.** Let \( X \) be a variety. A Parshin point is a flag \( V \cdot \) of germs at a point \( p \in X \) of varieties \( V_n \supset V_{n-1} \supset \ldots \supset V_0 = \{p\} \) with \( \dim V_i = i \) such that each \( V_i \) irreducible along \( V_{i-1} \).

Theorem 2.2.1 in [23] Mazin shows that for any Parshin point and any Zariski open set \( U \subset X \) one can find a regular mapping \( \phi: D \to X \) from a polydisc \( D = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \text{ with } |x_i| < \epsilon \text{ for all } i \} \) to \( X \) sending the standard flag in \( \mathbb{C}^n \) (i.e. \( \mathbb{C}^n \supset Z(x_1) \supset \ldots \supset Z(x_1, \ldots, x_n) \), where \( Z(x_1, \ldots, x_k) \) denotes the germ at origin of the set where \( x_1 = \ldots = x_k = 0 \)) to the flag \( V \) and sending the complement to the coordinate cross isomorphically onto a (classically) open subset of \( U \) contained in the complement to \( V_{n-1} \).

Let now \( z \) be an algebraic function defined on a Zariski open subset \( U \) of a variety \( X \). By shrinking \( U \) we can assume that this function is unramified over \( U \). Then any Parshin point in \( X \) gives rise to a neighbourhood in the above sense and hence, via pullback, to an algebraic function \( \phi^*z \) on the polydisc \( D \) unramified over the punctured polydisc \( \{(x_1, \ldots, x_n) \in (\mathbb{C}^*)^n \text{ with } 0 < |x_i| < \epsilon \text{ for all } i \} \). To this function we can apply Theorem 51 if the monodromy group of \( \phi^*z \) on the punctured polydisc has rank \( k \), then the original function \( z \) can’t be rationally induced from an algebraic function on a variety of dimension \(< k\).
Thus we arrive at the following theorem:

**Theorem 52.** Let $z$ be an algebraic function defined on a variety $X$. Suppose that there exists a Parshin point on $X$ and its punctured neighbourhood as described above such that the monodromy group of $z$ on this punctured neighbourhood has rank $k$. Then $z$ can’t be rationally induced from an algebraic function on a variety of dimension $< k$.

Moreover $z$ is not dominated by a tower of extensions of dimensions $k_1, \ldots, k_s$ if $k_1 + \ldots + k_s < k$.

We can apply Theorem 52 above to reprove theorems 49 and 50.

All we have to do is exhibit flags around which the monodromy of the universal algebraic function of degree $n$ has rank $\lfloor n/2 \rfloor$ (for Theorem 49) or has rank $2 \lfloor n/4 \rfloor$ and is realized by even permutations only (for Theorem 50).

We will show how to choose such flags for the case $n = 4$.

Let $z$ be the function satisfying $z^4 + x_1 z^3 + x_2 z^2 + x_3 z + x_4 = 0$. Let $\sigma : \mathbb{C}^4 \to \mathbb{C}^4$ be the function sending roots $z_1, \ldots, z_4$ of this equation to its coefficients $x_1, \ldots, x_4$.

The branched covering $\sigma$ is the Galois covering associated to $z$, so it’s enough to consider it instead of the function $z$.

We will exhibit the flags we are interested in as images under $\sigma$ of flags in $\mathbb{C}^4$ with coordinates $z_1, \ldots, z_4$.

The first flag is the image of the flag $Z(z_1 = z_2) \supset Z(z_1 = z_2, z_3 = z_4) \supset Z(z_1 = z_2 = z_3 = z_4) \supset Z(z_1 = z_2 = z_3 = z_4 = 0)$ where $Z$ (equation) stands for the set of points $(z_1, \ldots, z_4)$ for which the equation holds. This is a flag of irreducible varieties and its image under $\sigma$ is a Parshin point.

The branched covering $\sigma$ realizes the quotient of $\mathbb{C}^4$ by the action of the permutation group $S_4$ acting by permuting coordinates. Hence the monodromy of $\sigma$ in a neighbourhood of flag can be identified with the group of all permutations that stabilize any of the flags in its preimage. In our case the permutations that stabilize the flag $Z(z_1 = z_2) \supset Z(z_1 = z_2, z_3 = z_4) \supset Z(z_1 = z_2 = z_3 = z_4) \supset Z(z_1 = z_2 = z_3 = z_4 = 0)$ are
the trivial permutation, \((z_1, z_2), (z_3, z_4)\) and \((z_1, z_2)(z_3, z_4)\). Hence the monodromy of \(z\) around the flag has rank 2.

![Diagram](image)

**Figure 3.1:** In the case \(n = 4\) the torus on which the obstruction lives is the set of \(x_1,\ldots,x_4\) corresponding to the roots \(z_1,\ldots,z_n\) satisfying \(|z_1 - z_2| = 2\epsilon_4, |z_3 - z_4| = 2\epsilon_3, |\frac{z_1 + z_2}{2} - \frac{z_3 + z_4}{2}| = 2\epsilon_2, |\frac{z_1 + z_2 + z_3 + z_4}{4}| = \epsilon_1\)

For the situation where we are only allowing even permutations, the flag \(Z(z_1 + z_2 = z_3 + z_4) \supset Z(z_1 = z_3, z_2 = z_4) \supset Z(z_1 = z_2 = z_3 = z_4) \supset Z(z_1 = z_2 = z_3 = z_4 = 0)\) has the desired properties. The permutations of \(S_4\) that stabilize this flag are the trivial permutation, \((z_1, z_2)(z_3, z_4), (z_1, z_3)(z_2, z_4)\) and their product \((z_1, z_4)(z_2, z_3)\). These permutations are even. Hence the monodromy of \(z\) around the image of this flag under \(p\) is of rank 2 and consists of even permutations only.

For larger values of \(n\) the corresponding flags should be:

- In the case of universal algebraic function, the image of the flag

\[
Z(z_1 = z_2) \supset Z(z_1 = z_2, z_3 = z_4) \supset Z(z_1 = z_2, z_3 = z_4, z_5 = z_6) \supset \ldots
\]
continued until there are no more unused pairs of coordinates to make equal and then continued all the way to a point in an arbitrary manner.

- In the case of universal algebraic function with the square root of the discriminant adjoined to the field of rationality, the image of the flag

\[
Z(z_1 + z_2 = z_3 + z_4) \supset Z(z_1 = z_3, z_2 = z_4) \supset \\
Z(z_1 = z_3, z_2 = z_4, z_5 + z_6 = z_7 + z_8) \supset \\
Z(z_1 = z_3, z_2 = z_4, z_5 = z_7, z_6 = z_8) \supset \ldots
\]

continued until there are no more unused quadruples of coordinates to use and then continued all the way to a point in an arbitrary manner.

### 3.7.4 Essential dimension at a prime \( p \)

In [29] it is proposed to study the following aspect of algebraic essential dimension of algebraic functions: fix a prime \( p \). Consider the pullback of the given algebraic function to all possible branched coverings over its base space that have degree not divisible by \( p \) and find the minimal algebraic essential dimension of all such functions. This minimal essential dimension is called “the essential dimension at \( p \)”.

In this section we note that all the results of this paper are actually results about the essential dimension at some prime \( p \) (which means that our methods are of type I in the terminology of [29]).

More precisely:

**Theorem 53.** Let \( z \) be an algebraic function defined on a variety \( X \). Consider a Parshin point on \( X \) and its punctured neighbourhood. Let \( G \) denote the monodromy group of \( z \) on this punctured neighbourhood. Suppose that \( p \) is a prime and \( G/pG \) has rank \( k \). Then the algebraic essential dimension of \( z \) at \( p \) is at least \( k \).

**Proof.** The main observation is as follows:
Suppose that $\xi_T$ is a covering over a torus with monodromy group $G$ and suppose that the rank of $G/pG$ is $k$. Let $f : T_1 \to T$ be a covering map of degree relatively prime to $p$ ($T_1$ could be disconnected). Let $\bar{f} : \bar{T}_1 \to T$ be a restriction of $f$ to a connected component of $T_1$ such that the degree of $\bar{f}$ is prime to $p$. Then $\bar{f}^*(\xi_T)$ has monodromy group $G_1$ with $G_1/pG_1$ of rank $k$.

This topological statement on coverings over tori translates to the statement of the theorem once applied to the covering given by the function $z$ over the punctured neighbourhood of the Parshin point.

In particular the lower bounds $\lfloor \frac{n}{2} \rfloor$ and $2\lfloor \frac{n}{4} \rfloor$ for the universal algebraic function and for the universal algebraic function with square root of the discriminant adjoined to the field of rationality are actually bounds on the algebraic essential dimension at the prime 2. Using flags where $p$-tuples of roots coincide one can prove the lower bound of $\lfloor \frac{n}{p} \rfloor$ on the algebraic essential dimension at $p$ of the universal algebraic function and (for $p \neq 2$) for the universal algebraic function with the square root of the discriminant adjoined to the field of rationality. In [25] it is shown that these bounds on the essential dimension at $p$ are in fact exact.

### 3.7.5 Generic algebraic function of $k$ parameters and degree $\geq 2k$ can’t be simplified

The same flag that we used to show that the universal function of $n$ parameters can’t be reduced to less than $\lfloor n/2 \rfloor$ parameters gives some useful information about any other algebraic function as well. Indeed, any algebraic function of degree $n$ can be induced from the universal algebraic function. Thus we can think of it as the restriction of the universal algebraic function to some subvariety $X$ in $\mathbb{C}^n$. To this function we can apply our arguments with the flag obtained by intersecting a flag in $\mathbb{C}^n$ with $X$.

*Notation 1.* Let $\sigma : \mathbb{C}^n \to \mathbb{C}^n$ be the mapping that sends the point $(z_1, \ldots, z_n)$ to the co-
coefficients \((x_1, \ldots, x_n)\) of the equation \(z^n + x_1 z^{n-1} + \ldots + x_n = 0\). We will denote by \(D_k\) the image under \(\sigma\) of the set \(\{(z_1, \ldots, z_n) \mid z_1 = z_2, \ldots, z_{2k-1} = z_{2k}, \text{no other equalities hold between the } z_i \text{'s}\}\).

Let \(x^o\) be the image under \(\sigma\) of a point \((z_1^o, \ldots, z_n^o)\) with \(z_1^o = z_2^o, \ldots, z_{2k-1}^o = z_{2k}^o\) and no other equalities between the \(z_i\)’s. The branches of the algebraic functions

\[
(\tilde{z}_1 - \tilde{z}_2)^2, \ldots, (\tilde{z}_{2k-1} - \tilde{z}_{2k})^2,
\]

\[
\frac{z_1 + z_2}{2} - \tilde{z}_1, \ldots, \frac{z_{2k-1} + z_{2k}}{2} - \tilde{z}_{2k-1},
\]

\[
\tilde{z}_{2k+1} - \tilde{z}_{2k-1}, \ldots, \tilde{z}_n - \tilde{z}_n
\]

that assume the value 0 at the point \((x_1^o, \ldots, x_n^o)\) form a coordinate system in a neighbourhood of \(x^o\). If we denote these coordinate functions by \(\tilde{x}_1, \ldots, \tilde{x}_n\), then the discriminant is defined in a small neighbourhood of the point \(z^o\) by the equation \(\tilde{x}_1 \cdot \ldots \cdot \tilde{x}_k = 0\). This shows that \(D_k\) is contained in the locus of the points where the discriminant variety has a normal crossing singularity. If we choose the coordinates on the source \(\mathbb{C}^n\) to be \((\tilde{z}_1, \ldots, \tilde{z}_n) = (z_1 - z_2, \ldots, z_{2k-1} - z_{2k}, \frac{z_1 + z_2}{2} - \tilde{z}_1, \ldots, \frac{z_{2k-1} + z_{2k}}{2} - \tilde{z}_{2k-1}, z_{2k+1} - z_{2k-1}, \ldots, z_n - z_n)\) then in these coordinates \(p\) is given by the formula \((\tilde{x}_1, \ldots, \tilde{x}_n) = \sigma(\tilde{z}_1, \ldots, \tilde{z}_n) = (\tilde{z}_1^2, \ldots, \tilde{z}_{k+1}^2, \ldots, \tilde{z}_n).

**Theorem 54.** Let \(z_X\) be the algebraic function obtained by restricting the universal algebraic function on \(\mathbb{C}^n\) to a subvariety \(X \subset \mathbb{C}^n\). Let \(D_k\) be the subset of \(\mathbb{C}^n\) defined above. Suppose that \(X\) and \(D_k\) intersect transversally at least at one point. Then the function \(z_X\) can’t be rationally induced from a function of less than \(k\) parameters.

**Proof.** Let \(\sigma\) denote as before the function that sends the roots \(z_1, \ldots, z_n\) of the equation \(z^n + x_1 z^{n-1} + \ldots + x_n = 0\) to its coefficients \(x_1, \ldots, x_n\).

Let \(x^o = \sigma(z^o)\) be a point in the intersection of \(X\) with \(D_k\) and \(z^o = (z_1^o, \ldots, z_n^o)\) is such that \(z_1 = z_2, \ldots, z_{2k-1} = z_{2k}\) and no other equalities hold between the \(z_i\)’s. As we noted before, one can find coordinates \(\tilde{x}_1, \ldots, \tilde{x}_n\) and \(\tilde{z}_1, \ldots, \tilde{z}_n\) in small neighbourhoods of the points \(x^o\) and \(z^o\) respectively so that the mapping \(\sigma\) in these coordinates is given by the formula \(\sigma(\tilde{z}_1, \ldots, \tilde{z}_n) = (\tilde{z}_1^2, \ldots, \tilde{z}_{k+1}^2, \ldots, \tilde{z}_n)\).
Since $D_k$ is given in these coordinates by the equations $\tilde{x}_1 = \ldots = \tilde{x}_k = 0$ and $X$ is transversal to it, one sees that $X$ is transversal to the map $\sigma$ and hence its preimage $Z = p^{-1}(X)$ is a manifold in a neighbourhood of the point $z^o$. The formula for $\sigma$ shows that the tangent space to $Z$ at the point $z^o$ contains the vectors $\partial/\partial\tilde{z}_1, \ldots, \partial/\partial\tilde{z}_k$. In particular the differentials $d\tilde{z}_1, \ldots, d\tilde{z}_k$ are linearly independent on this tangent space and hence the functions $\tilde{z}_1, \ldots, \tilde{z}_k$ can be extended to local coordinates on $Z$ by adding if necessary some of the other $\tilde{z}_i$'s. Let's assume without loss of generality that $\tilde{z}_1, \ldots, \tilde{z}_k, \ldots, \tilde{z}_m$ are local coordinates on $Z$. By the transversality condition $X \pitchfork D_k$ and the definition of $Z$ as the preimage of $X$ it follows that $\tilde{x}_1, \ldots, \tilde{x}_m$ are local coordinates on $X$ at $x^o$. In these coordinates the restriction of $\sigma$ on $Z$ is given by $\sigma(\tilde{z}_1, \ldots, \tilde{z}_m) = (\tilde{z}_1^2, \ldots, \tilde{z}_k^2, \tilde{z}_{k+1}, \ldots, \tilde{z}_m)$. Hence the local monodromy of $z_X$ around the flag on $X$ given by $\{\tilde{x}_1 = 0\} \supset \ldots \supset \{\tilde{x}_1 = \ldots = \tilde{x}_m = 0\}$ is of rank $k$ and hence $z_X$ is not rationally induced from any algebraic function with less than $k$ parameters.

We will use this theorem now to show that a generic algebraic function depending on $k$ parameters and having degree $n$ can’t be rationally induced from an algebraic function of less than $k$ parameters provided that $n \geq 2k$. The word “generic” can be made precise in many ways. What follows is one of them:

**Theorem 55.** Let $L$ be a linear space of polynomials on $\mathbb{C}^n$ that contains constants and linear functions. Then for generic $p_1, \ldots, p_{n-k} \in L$ the algebraic function obtained from the universal algebraic function on $\mathbb{C}^n$ by restriction to the set $p_1(x) = 0, \ldots, p_{n-k}(x) = 0$ can’t be rationally induced from an algebraic function of less than $k$ parameters provided that $n \geq 2k$.

**Proof.** According to Theorem 54 it is enough to show that for generic $p_1, \ldots, p_{n-k} \in L$ the intersection of $D_k$ with $p_1(x) = 0, \ldots, p_{n-k}(x) = 0$ is non-empty and transversal. Since the set of polynomials for which the intersection is non-empty and transversal is
an algebraic set, it is enough to show it has non-zero measure.

The fact that the set of equations in $L^k$ whose zero set intersects $D^k$ transversally is of full measure follows from Sard’s lemma.

Indeed, consider the subset $I = \{(f, x) | f(x) = 0, f \in L^k, x \in \mathbb{C}^n\}$. This subset is a submanifold of $L^{n-k} \times \mathbb{C}^n$. Indeed, the differential of the evaluation function $(f, x) \rightarrow \mathbb{C}^k$ evaluated on a tangent vector $(\phi, \xi) \in T_{(f, x)}L^{n-k} \times \mathbb{C}^n$ is equal to $\phi(x) + d_x f(\xi)$. Since $L$ contains all constants, this differential is of full rank at all points.

For every point $f \in L^{n-k}$ which is regular for the projection from $I$ to $L^{n-k}$, the zero set of $f$ is a submanifold of $\mathbb{C}^n$, hence by Sard’s lemma the zero set of $f$ is a submanifold of $\mathbb{C}^n$ for almost all $f \in L^{n-k}$.

In a similar way we can show it is transversal to $D_k$ for almost all $f \in L^{n-k}$.

Indeed, the projection from $I$ onto $\mathbb{C}^n$ is a submersion (if we fix $\xi \in T_x \mathbb{C}^n$, we can choose $\phi \in T_f L^{n-k}$ so that $\phi(x) + d_x f(\xi) = 0$, because $L$ contains all constants).

Hence the preimage $I_D$ of $D_k$ under this projection is a submanifold of $I$.

Now we claim that for any point $f \in L^{n-k}$ which is regular for the projection from $I_D$ to $L^{n-k}$ the set $\{x \in \mathbb{C}^k | f(x) = 0\}$ is transversal to $D_k$. Indeed, let $x \in D_k$ be a point such that $f(x) = 0$ and let $\xi$ be any vector in $T_x \mathbb{C}^n$. As we noted before the projection from $I$ to $\mathbb{C}^n$ is a submersion and hence we can find $\phi \in T_f L^{n-k}$ such that $(\phi, \xi) \in T_{(f, x)} I$, i.e. $d_x f(\xi) = -\phi(x)$. Since $f$ is a regular point of the projection from $I_D$ to $L^{n-k}$, one can find a vector $\xi' \in T_x D_k$ such that $(\phi, \xi') \in T_{(f, x)} I_D$. Thus $d_x f(\xi) = -\phi(x) = d_x f(\xi')$, i.e. $\xi - \xi' \in \ker d_x f$. Hence $\xi$ is a sum of a vector tangent to $D_k$ and a vector tangent to the level set of $f$, i.e. the level set of $f$ is indeed transversal to $D_k$.

Sard’s lemma then guarantees that for almost any $f$ the level set of $f$ is transversal to $D_k$.

Finally we have to show that the set of equations having at least one solution on $D_k$ is of full measure.

Suppose that the dimension of the space $L$ is equal to $l$. 
All fibers of the projection from $I_D$ to $\mathbb{C}^n$ are $(n - k)(l - 1)$-dimensional. Indeed, the condition that an equation in $L$ vanishes at a given point $x$ is a linear condition and it is never satisfied by all equations in $L$ as $L$ contains constants. Thus the space $I_D$ is $(n - k)l$-dimensional. Since the set $I_D$ is an affine manifold its image under projection to $L^{n-k}$ is either of full measure or is contained in a proper affine subvariety of $L^{n-k}$. Suppose that the latter is the case. Then the dimension of each component of the preimage of any point $f \in L^{n-k}$ is at least 1 by ([28], theorem 3.13). One can however find equations $f \in L^{n-k}$ whose zero set on $D_k$ contains an isolated point $x \in D_k$: for instance one can take affine functions that vanish at $x$ and whose differentials are linearly independent when restricted to the tangent space $T_xD_k$.

We’ll now give another result of a similar nature.

**Theorem 56.** Let $L$ be a linear space of polynomials on $\mathbb{C}^k$ that contains constants and linear functions. Then for generic $p_1, \ldots, p_n \in L$ the algebraic function satisfying $z^n + p_1(x)z^{n-1} + \ldots + p_n(x) = 0, x \in \mathbb{C}^k$ can’t be rationally induced from an algebraic function of less than $k$ parameters provided that $n \geq 2k$.

**Proof.** The proof is similar to the proof of the previous theorem. We will show that for generic choice of $(p_1, \ldots, p_n) \in L^n$ the image of $\mathbb{C}^k$ under the map $(p_1, \ldots, p_n)$ is transversal to $D_k$ and intersects $D_k$ non-trivially.

Transversality follows from transversality theorem [14]: the evaluation map from $L^n \times \mathbb{C}^k$ is transversal to $D_k$ because $L$ contains all linear functions. Hence for $p$ in a set of full measure in $L^n$ the map $p : \mathbb{C}^k \to \mathbb{C}^n$ is transversal to $D_k$.

To show that for generic $p$ the image of this map intersects $D_k$ non-trivially, we notice that the evaluation map described above is onto (since $L$ contains all constants) and hence the preimage of $D_k$ is at least $ln$-dimensional. Hence if it’s projection onto $L^n$ is not of full measure, it is contained in a proper subvariety of $L^n$. This implies then...
that for generic $p \in L^n$ all components of the intersection of $p(C^k)$ with $D_k$ are at least one-dimensional. This however contradicts the fact that all constants are in $L$: using them we can send $C^k$ to only one point in $D_k$.

\[ \square \]

**Remark.** The condition that $L$ contains constants and linear functions can be somewhat weakened. It is in fact enough to require that $L$ contains at least some polynomials $p_1, \ldots, p_{n-k}$ such that the set $p_1(x) = 0, \ldots, p_{n-m}(x) = 0$ intersects $D_k$ and at least some polynomial in $L$ doesn’t vanish at one of the points of intersection.

**Remark.** Versions of the previous two theorems where being rationally induced from an algebraic function on a variety of dimension $< k$ is replaced with being dominated by a tower of extensions of dimensions $k_1, \ldots, k_s$ with $k_1 + \ldots + k_s < k$ are also correct for the same reasons.
Bibliography


