Genus 0 Subfields of Symmetric and Alternating Extensions

Tali Monderer

Genus 0 Subfields of Symmetric and Alternating Extensions

Research Thesis

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Mathematics

Tali Monderer

Submitted to the Senate
of the Technion — Israel Institute of Technology
Sivan 5778 Haifa May 2018

This research was carried out under the supervision of Senior Lecturer Danny Neftin, in the Faculty of Mathematics.

The generous financial help of the Technion and through ISF grant 577/15 and BSF grant 2014173 is gratefully acknowledged.

Contents

List of Figures

Abstract

A traditional approach towards the study of polynomials is the investigation of their splitting fields. Given a bivariate polynomial $f(x,t) \in \mathbb{C}[x,t]$ viewed as a polynomial in x over $\mathbb{C}(t)$, the splitting field of f is a Galois extension Ω of the function field $\mathbb{C}(t)$. The Galois group $\mathrm{Gal}(\Omega/\mathbb{C}(t))$ may be viewed as a permutation group and thus investigated using tools from the theory of permutation groups. Since the base field was taken to be a function field, the theory of algebraic function fields introduces more machinery for describing the extension $\Omega/\mathbb{C}(t)$ and its subfields. In particular, the correspondence between compact Riemann surfaces and function fields over $\mathbb{C}$ gives a notion of a genus for function fields over $\mathbb{C}$.

Function fields of genus 0 and 1 are of interest due to some special properties: First, a function field over $\mathbb{C}$ is rational if and only if it is of genus 0. Next, by Faltings' theorem, if a curve has infinitely many rational points, it must be of genus 0 and 1. Some questions on specializations of polynomials may be translated, using Faltings' theorem and basic properties of decomposition fields, into conditions on the genus 0 and 1 subfields of the splitting field of the polynomial.

In this work we consider the case where a Galois extension of $\mathbb{C}(t)$ has a symmetric or alternating Galois group G of large enough degree n and determine the subgroups of G fixing subfields of Ω of genus 0 or 1. We show that a subgroup H that fixes a genus 0 or 1 subfield of a symmetric extension must be $A_{n-1} \leq H \leq S_n$ in general, with an added possibility that $A_{n-2} \lneq H \leq S_{n-2} \times S_2$ in the case of several exceptional types; and that each of these possibilities for such H does in fact occur in some symmetric extension $\Omega/\mathbb{C}(t)$. A key ingredient in the proof of this result is the following condition, developed in the works of Guralnick–Shareshian and Neftin–Zieve: If a subgroup $H \leq S_n$ fixes a subfield of Ω of genus 0 or 1, and n is large enough, then there exists $m \leq 2$ such that

$$O_m(H) = O_{m+1}(H) = \cdots = O_{\frac{n}{2}}(H),$$

where O_k is the number of orbits of H on unordered sets of k elements of $\{1, \ldots, n\}$. The integer m depends on the ramification type of $\Omega/\mathbb{C}(t)$: for a list of exceptional types it must be taken to be $m = 2$, but for the general case $m = 1$ can be taken. We use elementary counting arguments and the Livingstone-Wagner theorem to show that any subgroup that fulfills this condition must be the symmetric or alternating group

on n elements, a point stabilizer of the symmetric or alternating group on n elements, or a subgroup of $S_{n-2} \times S_2$ with a multiply transitive action on $\{1, \ldots, n-2\}$.

Abbreviations and Notations

$\mathbb{Z}$	:	the ring of integers
$\mathbb{C}$	:	the field of complex numbers
$\mathbb{Q}$	:	the field rational numbers
$F[x_1, \ldots, x_n]$	:	the ring of polynomials over F with variables $x_1, \ldots, x_n$
$F(x)$	:	the field obtained by adjoining x to F
S_n	:	the symmetric group on n elements
A_n	:	the alternating group on n elements
$\mathrm{Gal}(\Omega/F)$	:	the Galois group of a Galois extension Ω/F
Ω^H	:	the subfield of Ω fixed by a subgroup $H \leq \mathrm{Gal}(\Omega/F)$
H^σ	:	the conjugate subgroup $\sigma H \sigma^{-1}$
$G_1 \times G_2$	:	the direct product of two groups G_1 and G_2
$G_1 \times_Q G_2$	:	the fiber product of G_1 and G_2 over a shared quotient Q
$A^{\{k\}}$	:	the set of k-sets of A
$A^{\{k\}} \cup B^{\{\ell\}}$	:	the sets with k elements from A and ℓ elements from B,
	:	for A and B are disjoint
$O(A^{\{k\}})$	:	the number of orbits of a fixed group in its action on $A^{\{k\}}$
$O(A^{\{k\}} \cup B^{\{\ell\}})$	:	the number of orbits of a fixed group in its action on $A^{\{k\}} \cup B^{\{\ell\}}$
O_k	:	the number of orbits of a fixed group on the k-sets of a fixed set
$\mathbb{P}_F$	:	the set of places of the function field F
$Q \vert P$	:	a place Q lying above a place P
$E_{F_1/F}(P)$	:	the ramification type of P in F_1/F
$E_{G:H}$	:	the ramification type of P in Ω^H/Ω^G
$R_{F_1/F}(P)$	:	the Riemann-Hurwitz contribution of the place P in F_1/F
$R_{G:H}(P)$	:	the Riemann-Hurwitz contribution of P in Ω^H/Ω^G
$D(\tilde{P}\vert P)$	:	the decomposition group of a place $\tilde{P}$ lying above P
D_P	:	the decomposition group of *some* place $\tilde{P}$ lying above P
$\mathrm{Orbs}_D(G/H)$	:	the orbits of D on the cosets G/H

Chapter 1

Introduction

The genus 0 program seeks to determine the nongeneral minimal genus 0 extensions $\mathbb{C}(x)/\mathbb{C}(t)$. Here a minimal extension is an extension with no nontrivial intermediate fields, and a general extension is a degree n extension of $\mathbb{C}(t)$ whose Galois closure Ω has Galois group $G := \mathrm{Gal}(\Omega/\mathbb{C}(t)) \cong S_n$. The roots of this program lie in the work of Chisini, Ritt, and Zariski [21], focusing mainly on the solvable case. The program was initiated by Guralnick and Thompson, following the classification of finite simple groups. The minimality of the extension $\mathbb{C}(x)/\mathbb{C}(t)$ plays a key role, since it is equivalent to the primitivity of G, in its natural action on the roots of the minimal polynomial for x. The main approach towards the program is based on the Aschbacher–O'Nan–Scott structure theorem for primitive groups. The genus 0 program was carried out by many authors in the greater generality of extensions $\mathbb{C}(x,t)/\mathbb{C}(t)$ with degree sufficiently large in comparison to the genus of $\mathbb{C}(x,t)$. This was completed in recent works by Guralnick–Shareshian [7], and Neftin–Zieve [16]. They show that for every integer $g \geq 0$, there exists a constant N_g such that if $\mathbb{C}(x,t)/\mathbb{C}(t)$ is an extension of degree $n > N_g$ and genus $\leq g$, then either G is A_n or S_n or it is in a list of exceptions and the ramification of $\mathbb{C}(x,t)/\mathbb{C}(t)$ is in an explicit list.

The interest in finding fields of low genus arises in various contexts in arithmetic geometry, complex analysis and dynamics. It arises in the study of Ritt decompositions of polynomials and rational functions, due to the basic property that function fields over $\mathbb{C}$ are rational, that is, of the form $\mathbb{C}(t)$, if and only if their genus is 0. It also often arises due to deep theorems of Siegel and Faltings asserting that an algebraic curve with genus at least 2 (respectively, 1) has finitely many rational (respectively, integral) points. In particular, versions of the above have been used in Müller's finiteness theorem [13] for Hilbert sets, and in the work of Fried [6], and Cassou-Nogues–Couveignes [4] on the reducibility problem of Davenport–Lewis–Schinzel [5].

Müller's theorem asserts that given an irreducible polynomial $f \in \mathbb{Z}[t,x]$ whose Galois group is simple, nonalternating, and is not C_2, there exist only finitely many specializations $f(t_0,x)$ for $t_0 \in \mathbb{Z}$ such that $f(t_0,x)$ is reducible, which is a strong form of Hilbert irreducibility. The problem of Davenport–Lewis–Schinzel concerns the

reducibility of $f(X) - g(Y) \in \mathbb{C}[X, Y]$ for polynomials f and g.

Many of the applications of the genus 0 program are restricted to minimal extensions or alternatively indecomposable polynomials and rational functions, due to the minimality assumption in the genus 0 program. In this work, we remove the minimality assumption and merely assume that the function field $\mathbb{C}(x, t)$ is contained in the Galois closure of a minimal extension $F_1/\mathbb{C}(t)$ of large degree. That is, letting Ω be the Galois closure of such an extension $F_1/\mathbb{C}(t)$ and G the Galois group $\mathrm{Gal}(\Omega/\mathbb{C}(t))$, we ask what subgroups H of G fix a subfield of genus 0 or 1. The full classification of genus 0 and 1 subfields of symmetric and alternating extensions is as follows:

Theorem 1.1. *There exists an integer N such that for every minimal function field extension $F_1/\mathbb{C}(t)$ of degree $n > N$ with Galois closure Ω and Galois group $G = A_n$ or S_n, the fixed field of $H \leq G$ is of genus 0 only if one of the following holds:*

1. *H is S_n, A_n, S_{n-1} or A_{n-1};*
2. *H is the stabilizer of a two element subset of $\{1, \dots, n\}$, and the ramification type of $F_1/\mathbb{C}(t)$ is listed in Table A.1;*
3. *H is the pointwise stabilizer of two elements of $\{1, \dots, n\}$, and the ramification type of $F_1/\mathbb{C}(t)$ is $[n], [a, n-a], [2, 1^{n-2}]$ (Table A.1, I1.1);*
4. *H is the subgroup of A_n that stabilizes a two element subset of $\{1, \dots, n\}$, and the ramification type of $F_1/\mathbb{C}(t)$ is $[1, 2^{\frac{n-1}{2}}], [1, 4^{\frac{n-1}{4}}], [2, 3, 4^{\frac{n-5}{4}}]$ for $n \equiv 5 \mod 8$ (Table A.1, F3.2);*
5. *$H = A_{n-2} \times S_2$, and the ramification type of $F_1/\mathbb{C}(t)$ appears in Table A.2.*

In case 2, the group G can be either A_n or S_n, while in cases 3, 4 and 5 the group G must be S_n.

If $G = S_n$ then the fixed field H is of genus 1 only if one of the following holds:

6. *$H = A_n, S_{n-1}$ or A_{n-1}.*
7. *$H = A_{n-2} \times S_2$ and the ramification type of $F_1/\mathbb{C}(t)$ appears in Table A.3.*

If $G = A_n$ then the field F has no non-trivial subfields of genus 1 other than possibly the one fixed by A_{n-1}.

In cases (2)-(5) the resulting field Ω^H is always of genus 0, and in case (7) the given fields are of genus 1. The case where $A_{n-1} \leq H \leq S_n$ is the "general" case, as this is the only case that can occur of genus 0 or 1 if the ramification type of $F_1/\mathbb{C}(t)$ does not appear in Table A.1 of exceptional types. In these cases (case (1) and case (6)), explicit conditions on the ramification of $F_1/\mathbb{C}(t)$ are given under which Ω^H Is of genus 0 or 1, see Proposition 9.0.1 or Corollary 6.4.

We apply the above theorem to strengthen Hilbert's irreducibility theorem, see Section 10. In contrast to Müller's result, which considers only integer specializations, we consider here the general case of rational specializations. It follows from results on the genus 0 program, e.g. by [9], that if the Galois group G of an irreducible polynomial $f(t,x) \in \mathbb{Q}[t,x]$ over $\mathbb{Q}(t)$ is a nonalternating nonabelian simple group of sufficiently large degree, then its Galois closure contains no minimal extensions of $\mathbb{Q}(t)$ of genus 0 or 1. Thus in combination with Faltings' theorem it follows that there are only finitely many values $t_0 \in \mathbb{Q}$ for which $f(t_0,x)$ is reducible. We consider the general case where G is symmetric or alternating and determine which subgroups appear as the Galois group for infinitely many specializations. Let N be as in Theorem 1.1.

Theorem 1.2. *Let $f(X,t) \in \mathbb{Q}[X,t]$ be an irreducible polynomial with Galois group A_n or S_n for $n > N$. Then there exists a finite set $W \subseteq \mathbb{Q}$ such that for any $t_0 \in \mathbb{Q} \setminus W$, the Galois group H of $f(x,t_0)$ is one of the following:*

1. *$A_n \leq H \leq S_n$.*
2. *$A_{n-1} \leq H \leq S_{n-1}$.*
3. *$A_{n-2} \lneq H \leq S_{n-2} \times S_2$.*

Moreover, if one of the options above occurs for a value in $\mathbb{Q} \setminus W$, it occurs for infinitely many values in $\mathbb{Q} \setminus W$.

Note that case (3) can occur only when the ramification of f is in an explicit list, see Section 10.

Theorem 1.1 is expected to have many further applications. In particular, it played a key role in the work of David–Karasik–Neftin–Zieve concerning the Davenport–Lewis–Schinzel problem. Namely, they determine for which rational functions $f, g \in \mathbb{C}(x)$ such that f is indecomposable of large degree, the curve defined by $f(x) = g(y)$ is reducible. The strategy of the proof is to reduce to the case where $g(X) - t$ has a root in the splitting field of $f(X) - t \in \mathbb{C}(t)[X]$ and then apply our Theorem 1.1 to obtain the possibilities for g.

A special feature of symmetric extensions, due to [7], is that the genus of a subfield fixed by some $H \leq S_n$ can be bounded in terms of the action of H on k-sets (see Theorem 2.1). The condition that a subfield fixed by H is of genus 0 or 1 is thus translated into a necessary condition on the k-orbits of H. This necessary condition is examined in a purely group-theoretic setting to compose a list of candidate groups that may fix a subfield of genus 0 or 1 in a symmetric or alternating extension of large enough degree. After determinine the list of candidations, we return to the function field setting and check for which of the candidate subgroups there exist cases where the field fixed by H is indeed of genus 0 or 1. This involves the calculation of ramification data of various subextensions of a given Galois extension, relying on results by [16] and varients of Abhyankar's lemma.

Acknowledgements. I thank Danny Neftin and Michael Zieve for suggesting this problem to me and supplying various arguments. The generous financial help of the Technion and through ISF grant 577/15 and BSF grant 2014173 is gratefully acknowledged.

Chapter 2

Preliminaries

2.1 Permutation Groups and Their Orbits

This section introduces the theory and notation needed for the statement of Theorem 3.1, and the orbit counting arguments that form most of the steps towards its proof.

2.1.1 Orbits of Permutation Groups

Let A be a finite set of size n. A subset of A of size k is called a k-set of A. Denote by $A^{\{k\}}$ the set of k-sets of A. If A and B are disjoint sets, denote by $A^{\{k\}} \cup B^{\{\ell\}}$ the sets with k elements from A and ℓ elements from B. Fix a group H that acts on A by permutation. Then H also acts on the unordered k-sets of A for $k = 1, \ldots n$. We denote by $O(A^{\{k\}})$ the number of orbits of H in its action on k-sets of A. If A and B are disjoint orbits of H, then H acts on k-sets of $A \cup B$ and sends sets with k and ℓ elements from A and B respectively to sets of the same form, that is, H acts on $A^{\{k\}} \cup B^{\{\ell\}}$. Denote by $O(A^{\{k\}} \cup B^{\{\ell\}})$ the number of orbits of this action. When the identity of A as well as that of H is clear from the context, denote by O_k the number of orbits of the action of H on k-sets of A.

2.1.2 Multiply Transitive Groups

If a permutation group G on n elements has a single orbit on k-tuples of $\{1, \ldots, n\}$ it is called *k-transitive* and if it has a single orbit on unordered k-sets of $\{1, \ldots, n\}$ it is called *k-homogenous*. The Livingstone-Wagner theorem([11]) states that a k-homogenous group is k transitive whenever $k \geq 5$; and also that $O_k \leq O_{k+1}$ for $k \leq \lfloor \frac{n}{2} \rfloor$. A consequence of the classification of finite simple groups is that the only 6-transitive groups are S_n and A_n. Without relying on this classification, the order of transitivity of a permutation group of degree n is known to be bounded by a function of n; one such result is Babai and Seress' elementary proof that a permutation group on n elements is at most $32(\log(n))^2/\log\log n$ ([3]). Take D to be an integer such that $D < \lfloor \frac{n}{2} \rfloor$ and a D-transitive group on n elements must be A_n or S_n. When assuming

the classification of finite simple groups $D = 6$ suffices; else, such an integer D exists but we must take D depending on n.

2.1.3 Stabilizer Subgroups of S_n and A_n

Given a k-set x of $\{1, \ldots, n\}$, the set of all elements of S_n that stabilize x setwise is (up to conjugation) the subgroup $S_k \times S_{n-k} \leq S_n$, where S_k is the set of all permutations on the elements $\{1, \ldots, k\}$ and S_{n-k} is the set of all permutations on the elements $\{k+1, \ldots, n\}$. The set of all elements of S_n that stabilize x pointwise is the subgroup $S_{n-k} \leq S_n$. Let φ be the mapping from S_n to the set of all k-sets of $\{1, \ldots, n\}$ defined by $\varphi(\sigma) = \{\sigma(1), \ldots, \sigma(k)\}$. For two permutations σ_1 and σ_2, it holds that $\varphi(\sigma_1) = \varphi(\sigma_2)$ if and only if $\sigma_1\sigma_2^{-1} \in S_k \times S_{n-k}$ and thus the action of the group S_n on the cosets $S_n/(S_k \times S_{n-k})$ is equivalent to the action of S_n on k-sets of $\{1, \ldots, n\}$.

2.2 Function Fields, Places and Ramification

The following setup follows Chapters 1 and 3 of [20]. The purpose of this section is to provide the definitions of places of a function field and ramification in function field extensions in the algebraic setting, and introduce the properties of function fields relevant to this work.

A *function field* over $\mathbb{K}$ of transcendental degree 1 is a finite extension F of the field $\mathbb{K}(t)$ where t is transcendental over $\mathbb{K}$. A *discrete valuation ring* $\mathcal{O}$ of a function field $F/\mathbb{K}(t)$ is a strict subring $\mathbb{K} \subsetneq \mathcal{O} \subsetneq F$ with the special property that for every element $z \in F$, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$. It can be shown ([20], Proposition 1.1.5 and Theorem 1.1.6) that $\mathcal{O}$ is a local principal ideal domain, that is, contains a unique maximal ideal P such that $P = s\mathcal{O}$ for some $s \in P$, and each nonzero element $z \in F$ can be uniquely represented as $z = s^{n_z}u$ for $n_z \in \mathbb{Z}$ and $u \in \mathcal{O}^x$; Therefore it is possible to define a function $\nu_P : F \to \mathbb{Z} \cup \{\infty\}$ by sending each nonzero z to the integer n_z and sending 0 to ∞. The function ν_P is called a *discrete valuation* of F, the ring $\mathcal{O}_P := \mathcal{O}$ is called a *valuation ring* of F and the ideal P is called a *place* of F. For a function field L, denote by $\mathbb{P}_L$ the set of places of L.

If F_1/F is an algebraic extension of function fields, then ([20], Proposition 3.1.4) for each $Q \in \mathbb{P}_{F_1}$, the set $Q \cap F$ is a place of F. The place Q is then said to *lie over* P or *restrict to* P, and this relation is denoted $Q|P$. For each place $P \in \mathbb{P}_F$, there is at least one and at most $[F_1 : F]$ places $Q \in \mathbb{P}_{F_1}$ such that $Q|P$ ([20], Corollary 3.1.12). If $Q|P$, it holds that $\mathcal{O}_P \subseteq \mathcal{O}_Q$ ([20], Proposition 3.1.4), and there exists an integer $e \geq 1$ such that $\nu_Q|_F = e \cdot \nu_P$. The integer e is called the *ramification index* of Q over P and is denoted by $e(Q|P)$. The *relative degree* of $Q|P$ is defined as the degree of the field extension $(\mathcal{O}_Q/Q)/(\mathcal{O}_P/P)$ and is denoted by $f(Q|P)$. A place P is said to be *ramified* if there is at least one $Q|P$ such that $e(Q|P) > 1$ and otherwise it is *unramified*. Almost all places of F are unramified in F_1/F ([20], Corollary 3.5.5).

For any place $P \in \mathbb{P}_F$ ([20], Theorem 3.1.11) :

$$[F_1 : F] = \sum_{Q \in \mathbb{P}_{F_1}, Q|P} e(Q|P) f(Q|P). \tag{2.1}$$

This identity is called the fundamental equality. If $\mathbb{K}$ is algebraically closed then $f(Q|P) = 1$ ([20], Definition 1.1.4, Remark 1.1.17), and then the fundamental equality reads:

$$[F_1 : F] = \sum_{Q \in \mathbb{P}_{F_1}, Q|P} e(Q|P). \tag{2.2}$$

2.3 Curves and Algebraic Function Fields

Many results related to this work are stated in the language of complex curves and their coverings, as opposed to the language used here, of function fields over $\mathbb{C}$ and their extensions. The two terminologies are interchangeable: There is a one-to-one correspondence between algebraic function fields of one variable over $\mathbb{C}$ (up to $\mathbb{C}$-isomorphism) and smooth projective curves over $\mathbb{C}$ (up to isomorphism), under which all of the terms discussed previously regarding function fields have an analogue in the language of curves. This section is intended to describe this correspondence to a reader who is familiar with the terminology of curves (as it appears in the text by Fulton, [8]). The details given here follow [20], Appendix B, and [8], Chapter 4. For a (smooth projective) curve X defined over $\mathbb{C}$, the function field of X is a function field in the algebraic sense above ([8],Chapter 6.5) In the opposite direction, the key for obtaining a curve from a function field is the primitive element theorem: Let $F/\mathbb{C}(t)$ be a function field. Since $F/\mathbb{C}(t)$ is a finite seperable extension, by the primitive element theorem there exists an element $x \in F$ with $F = \mathbb{C}(t, x)$. Denote by f the minimal polynomial of x over $\mathbb{C}(t)$; then f defines an (affine) curve over $\mathbb{C}$; There exists a smooth projective curve X whose function field is isomorphic to F ([20],B.9). Recall that the projective line over $\mathbb{C}$ is a smooth projective curve whose function field $\mathbb{C}(\mathbb{P}^1)$ is the field of rational functions over $\mathbb{C}$ ([8], excercise 4-8). Denote a parametrization $\mathbb{C}(\mathbb{P}^1) = \mathbb{C}(t)$. A non constant morphism of smooth projective curves is called a *covering* (the term comes from the topological theory of covering spaces). There is a 1-1 correspondence between coverings of $\mathbb{P}^1$ and extensions of $\mathbb{C}(\mathbb{P}^1)$, i.e., extensions of $\mathbb{C}(t)$ ([8], Chapter 7, Corollary 2). Under the above, the places of f correspond to points on X. The local ring of a smooth projective curve at a point is a discrete valuation ring, and the local rings of a curve correspond to the discrete valuation rings of its function field ([8], Chapter 7, Corollary 4); the ramification of a place in an extension field is defined through properties of discrete valuation rings and the same definition applies when working in the language of curves, i.e., when defining the ramification index of a covering at a point.

2.4 The Genus of a Function Field

The *genus* of a function field $F/\mathbb{K}(t)$ is an integer invarient associated with F. Provided here is the algebraic definition of the genus using the theory of divisors, following [20], Section 1.4. Given a function field $F/\mathbb{K}(t)$, define the *divisor group* of F as the free abelian group generated by the places of F. That is, the divisor group may be viewed as the (pointwise) additive group of formal sums of the form

$$\sum_{P\in\mathbb{P}_F} n_P, \text{ with } n_P \in \mathbb{Z} \text{ and all but a finite number of coefficients } n_P \text{ are zero.}$$

This set is denoted $\mathrm{Div}(F)$ and its elements are called *divisors*. Given an element $z \in F$, the *principal divisor* of z is defined by $(z) := \sum_{P\in\mathbb{P}_F} \mu_P(z)P$, where μ_P is the valuation of z at P. For example, for $0 \in F$, the corresponding principal divisor is the formal sum $\sum_{P\in\mathbb{P}_F} 0P$. The notion of a valuation function at a place is extended to divisors by setting

$$\mu_P(A) = \text{the coefficient of } P \text{ in } A.$$

If A is a principal divisor, $A = (z)$ for some $z \in F$, then $\mu_P(A)$ is (by definition of the principal divisor) indeed the valuation of z at the place P. Set a partial order on $\mathrm{Div}(F)$ by

$$A \leq B \text{ if and only if } \nu_P(A) \leq \nu_P(B) \text{ for every } P \in \mathbb{P}_F,$$

and observe the following set:

$$\mathcal{L}(A) = x \in F, (x) \geq -A \cup \{0\}.$$

This set is a finite dimensional vector space over K ([20], Lemma 1.4.6, Proposition 1.4.9) named the *Riemann-Roch space* associated with A. Denote the dimension of $\mathcal{L}(A)$ by $\ell(A)$. It can be shown ([20], Proposition 1.4.14) that there exists an upper bound for the set $\{\deg(A) - \ell(A), A \in \mathrm{Div}(F)\}$; the *genus* of F is defined as

$$\max_{A\in\mathrm{Div}(F)} \{\deg(A) - \ell(A) + 1\}.$$

The resulting maximum is a nonnegative integer ([20], Corollary 1.4.16). We will be interested in the relationship between the genera of subfields in a extension of function fields. The following proposition summarizes some basic properties of the genus that are of interest in this work:

Proposition 2.4.1 (Basic Properties of the Genus)**.** *Let F, F_1 and F_2 be function fields over $\mathbb{K}$ such that $F_1 \subseteq F_2$. Assume that $\mathbb{K}$ is algebraically closed and of characteristic 0. Denote the genera of F, F_1, F_2 by g, g_1, g_2 respectively.*

1. *The field F is of genus 0 if and only if it is rational, i.e., $F = \mathbb{K}(x)$ for some x transcendental over $\mathbb{K}$.*

2. The genera g_1 and g_2 satisfy that $g_1 \geq g_2$.

Proof. For assertion 1, see [20], Remark 1.6.4. Assertion 2 follows from the Riemann-Hurwitz formula (see section 2.5 ahead). ■

The genus of a smooth projective curve over $\mathbb{C}$ is defined in the same way as for a function field over $\mathbb{C}$ (replacing 'places' with 'points' in the definitions above) and the notions of the genus of a curve over $\mathbb{C}$ and the genus of its function field coincide. Every smooth projective curve is a compact Riemann surface; in particular it is a compact, connected surface whose topological genus coincides with the algebraic definition above (for proof of this fact and further information see [12], Chapter VI, Section 3).

2.5 Riemann Hurwitz Formula

In the setup of 2.2, assume for simplicity that $\mathbb{K}$ is algebraically closed of characteristic 0, and let $n = [F_1 : F]$. The Riemann-Hurwitz formula ([20], Definition 3.4.3 and Theorem 3.4.13) relates the genera of F_1 and F with the degree of the extension F_1/F and the ramification of the places of F in F_1:

$$2(g_{F_1} - 1) = n(2g_F - 2) + \sum_{P \in \mathbb{P}_F} \sum_{Q \in \mathbb{P}_{F_1}, Q|P} (e(Q|P) - 1). \tag{2.3}$$

If F' is another field such that $F \subseteq F' \subseteq F_1$, denote by $R_{F_1/F'}(P)$ the Riemann-Hurwitz contribution of the set of all places of F' lying above P, that is,

$$R_{F_1/F'}(P) = \sum_{Q' \in \mathbb{P}_{F'}, Q'|P} (e(Q'|P) - 1).$$

2.6 Tools for Calculation of Ramification

In the previous section, two fundamental constraints on ramification in function field extensions were introduced: the fundumental equality and the Riemann-Hurwitz formula. In this section, some results from the theory of ramification in Galois extensions are discussed, and two tools are provided for the calculation of ramification in function field extensions: Lemmas 7.2.1 and Lemmas 2.6.2.

2.6.1 Ramification in Galois Extensions

In the setup of 2.5, let Ω be the Galois closure of F_1/F and G be the Galois group of Ω/F. Given places $P \in \mathbb{P}_F$ and $\tilde{P} \in \mathbb{P}_\Omega$ such that $\tilde{P}|P$ and an automorphism $\varphi \in G$, the image $\varphi(\tilde{P})$ is another place of Ω lying above P, i.e., G acts on $\mathbb{P}_\Omega$. For $P \in \mathbb{P}_F$, the Galois group G acts transitively on the places of Ω lying above P ([20], Theorem 3.17.1), and as a consequence, for any two places $\tilde{P}_1$ and $\tilde{P}_2$ of Ω lying above P, it holds

that $e(\tilde{P}_1|P) = e(\tilde{P}_2|P) =: e$ and $f(P_1|P) = f(P_2|P) =: f$. The fundamental equality (2.2) now reads:

$$[\Omega : F] = nef, \tag{2.4}$$

where n is the number of places of Ω lying over P. The *decomposition group* of a place $\tilde{P}|P$ in Ω, denoted $D(\tilde{P}|P)$, is the stabilizer of $\tilde{P}$ in the action of G on $\mathbb{P}_\Omega$:

$$D(\tilde{P}|P) := \{\sigma \in G : \sigma(\tilde{P}) = \tilde{P}\}.$$

It follows from the orbit-stabilizer formula and (2.4) that $|D(\tilde{P}|P)| = ef$. Since G acts transitively on the places of Ω lying over P, for any two places $\tilde{P}_1|P$ and $\tilde{P}_2|P$ the decompositions groups $D(\tilde{P}_1|P)$ and $D(\tilde{P}_2|P)$ are conjugate. In a context where it doesn't matter which place is taken over P, we denote by $D_p := D(\tilde{P}|P)$ the decomposition group of some place $\tilde{P}|P$ and say that D_P is the decomposition group of P (while actually it is the decomposition group of some place lying above P). If $\mathbb{K}$ is algebraically closed, the relative degree of any place is 1 and so $|D| = e$. If $\mathbb{K}$ is algebraically closed and of characteristic 0, then D is a cyclic group ([20], Definitions 3.8.1 and 3.8.4, Propositions 3.8.2 and 3.8.5). A generator of D_P is called a *branch cycle* of P in Ω.

2.6.2 Calculating Ramification via Double Cosets

In the same setup as 2.6.1, let H be some subgroup of G, and let P be some place of F. The decomposition group D_p acts on the cosets G/H by left multiplication in G. Denote the set of orbits of D_p on G/H by $\mathrm{Orbs}_{D_P}(G/H)$.

Lemma 2.6.1. *([16], Lemma 2.1) Let Ω/F be a Galois extension of function fields with Galois group G. Let H be some subgroup of G and P some place of F. Let $Q_1, \dots Q_r$ be the places of Ω^H lying above P. Then there is a one-to-one correspondence*

$$\varphi : \{Q_1, \dots Q_r\} \to Orbs_{D_P}(G/H)$$

such that $e(Q_i|P)f(Q_i|P) = |\varphi(Q_i)|$.

Remark. This result holds without any assumptions on $\mathbb{K}$; If $\mathbb{K}$ is algebraically closed, then $f(Q_i|P) = 1$ and so $e(Q_i|P) = |\varphi(Q_i)|$ for $i = 1, \dots r$.

Remark. In the setup above, if $H_1 \leq H$ and $Q'_1, \dots Q'_s$ are the places of Ω^{H_1} lying above Q_1, then the mappings

$$\varphi_1 : \{Q'_1, \dots Q'_s\} \to \mathrm{Orbs}_{D_P}(G/H_1)$$

and

$$\varphi : \{Q_1, \dots Q_r\} \to \mathrm{Orbs}_{D_P}(G/H)$$

given by Lemma 2.6.1 are compatible in the sense that for $\sigma \in G$, the place $\varphi_1^{-1}(D_P \sigma H_1)$ lies above the place $\varphi^{-1}(D_P \sigma H)$.

Denote $\mathrm{Orbs}_{D_P}(G/H) = \{o_1, \dots o_r\}$. Since

$$\sum_{i=1}^{r} |o_i| = |G/H| = [G : H],$$

we reach the following expression for the Riemann-Hurwitz contribution of P in Ω^H/F:

$$R_{\Omega^H/F}(P) = \sum_{i=1}^{r} |o_i| - 1 = [G : H] - |\mathrm{Orbs}_{D_P}(G/H)|. \tag{2.5}$$

Recall that by Galois correspondence $[\Omega^H : F] = [G : H]$. Plug (2.5) into (2.3) to get the following version of the Riemann-Hurwitz formula:

$$2(g_{\Omega^H} - 1) = [G : H](2g_F - 2) + \sum_{P \in \mathbb{P}_F} [G : H] - |\mathrm{Orbs}_{D_P}(G/H)|. \tag{2.6}$$

For reasons of brevity and clarity, when calculating the Riemann-Hurwitz formula for subfields of Ω fixed by subgroups $H_1 \leq H_2 \leq G$ we will write $R_{H_2:H_1}$ instead of $R_{\Omega^{H_1}/\Omega^{H_2}}$, and for $H \leq G$ we will write the genus of the extension Ω^H as g_H instead of g_{Ω^H}.

2.6.3 Abhyankar's Lemma

Abyankhar's lemma is a tool for calculating the ramification of a place in a compositum of function fields:

Lemma 2.6.2 (Abhyankar's Lemma)**.** *([20], Theorem 3.9.1) Let K_1/K and K_2/K be two extensions of function fields; denote their compositum by K_1K_2. Let Q be a place of K_1K_2 that lies over places Q_1,Q_2 and P in K_1, K_2 and K respectively. Then*

$$e(Q|P) = \mathrm{lcm}(e(Q_1|P), e(Q_2|P)).$$

2.7 Ramification Types

Assume that $\mathbb{K}$ is algebraically losed. Let K_1/K be an extension of function field. Let P be a place of K, and let $Q_1, \dots Q_r$ be the places of K_1 lying above P. The set $E_{K_1/K}(P) := [e(Q_1|P), \dots, e(Q_r|P)]$ is called the *ramification type* of P in K_1. Recall that only finitely many places of $\mathbb{P}_K$ are ramified in K', and denote the set containing these places by S. The set $\{E_{K_1/K}(P) : P \in S\}$ is called the *ramification type of* K_1/K. When K_1, K are viewed as subfields of some Galois extension fixed by subgroups $H_1 \leq H_2$ of the Galois group, denote the same set by $E_{H_2:H_1}(P)$.

Let Ω/K be the Galois closure of K_1/K. Denote the subgroup of $\mathrm{Gal}(\Omega/K)$ fixing K_1 by H and let x_P be a branch cycle of P in Ω; then $\mathrm{Gal}(\Omega/K)$ may be viewed as a permutation group on the cosets G/H, and by Lemma 2.6.1, the set $E_{K_1/K}(P)$ is equal to the set of lengths orbits of x_P on the cosets G/H. Therefore $E_{K_1/K}(P)$ may also be viewed as the cycle structure of x_P (as a permutation on $|G/H| = [G : H]$ elements). In particular, if $\mathrm{Gal}(\Omega/K) = S_n$ for some n, then the ramication type of $\Omega^{S_{n-1}}/K$ is the set of cycle structures of the branch cycles of Ω/K (as permutations on $\{1, \ldots, n\}$.

2.8 Symmetric Extensions

2.8.1 Relating the Genus and k-orbits in Symmetric and Alternating Extensions

The following theorem was developed in the works of Guralnick and Shareshian ([16]) and Neftin and Zieve([7]) It provides a necessary condition for a subfield of a symmetric or alternating extension to be of genus 0 or 1.

Theorem 2.1 (Necessary condition on orbits of subgroups fixing fields of genus 0 or 1)**.** *There exists a constant N_0 such that if $\Omega/\mathbb{C}(t)$ is a Galois extension such that $G := \mathrm{Gal}(\Omega/\mathbb{C}(t)) = S_n$ or A_n, for some $n > N_0$, if H is a subgroup of G fixing a subfield of genus 0 or 1, then:*

$$O_2(H) = O_3(H) = \cdots = O_{\lfloor \frac{n}{2} \rfloor}(H). \tag{2.7}$$

Let F be the subfield of Ω fixed by a point stabilizer of G. If the ramification type of $F/\mathbb{C}(t)$ is not an exceptional type listed in Table A.1, then

$$O_1(H) = O_2(H)$$

as well.

Proof of Theorem 2.1. Guralnick and Shareshian ([7], Lemma 2.0.13)[1] relate the genus of H to the number of k-orbits of its action on $\{1, \ldots, n\}$ as follows:

$$g_{\Omega^H} \geq \sum_{t=2}^{\lfloor \frac{n}{2} \rfloor} (O_t - O_{t-1})(g_{F_t} - g_{F_{t-1}}) \tag{2.8}$$

where F_t is a subfield of Ω fixed by a stabilizer of a t-set and g_{F_t} its genus. By the Livingstone-Wagner theorem, $O_t - O_{t-1} \geq 0$ and by [7], Lemma 2.0.12,

$$g_{F_t} - g_{F_{t-1}} \geq 0.$$

[1] The results in [16] and [7] are formulated in the language of curves; for the correspondence between function fields and curves consult 2.3.

Since the summands of 2.8 are non-negative:

$$g_H \geq (O_t - O_{t-1})(g_{F_t} - g_{F_{t-1}}) \tag{2.9}$$

for $1 \leq t \leq \lfloor \frac{n}{2} \rfloor$. By [16],Theorem 3.1, there exists a constant $c > 0$ and polynomial $d = d(t)$ such that

$$g_{F_t} - g_{F_{t-1}} > (cn - dt^{15}) \frac{\binom{n}{t}}{\binom{n}{2}} \tag{2.10}$$

where t is taken from 3 to $\frac{n}{2}$ in general or from $t = 2$ if the ramification data of $F/\mathbb{C}(t)$ is not one of the exceptional types listed in Table A.1. Choose N_0 be large enough such that the right hand side of the inequality (2.10) is strictly greater than 2. For an $n > N_0$, if $g_H = 0$ or $g_H = 1$, then the right hand side of 2.9 must equal 0 or 1. Since $g_{F_t} - g_{F_{t-1}} \geq 2$, the orbits of H on t-sets of $\{1, \ldots, n\}$ satisfy

$$O_{t-1} = O_t \tag{2.11}$$

for $t = 3, \ldots, \frac{n}{2}$ in general, and if the ramification type of $F/\mathbb{C}(t)$ is not listed in Table A.1 the equality can be taken for $t = 2$ as well.

2.9 Subgroups of the Direct Product and Fiber Products

Given three groups H_1, H_2, Q and homomorphisms $\varphi_i : G_i \to Q$, the fiber product $H_1 \times_Q H_2$ is the following subgroup of $H_1 \times H_2$:

$$\{(g_1, g_2) \in H_1 \times H_2 : \varphi_1(g_1) = \varphi_2(g_2)\} \tag{2.12}$$

The following lemma is known as Goursat's lemma. It describes the subgroups of a direct product. A group Q is said to be a *shared quotient* of H_1 and H_2 if there exist normal subgroups $N_1 \lhd H_1$ and $N_2 \lhd H_2$ such that $H_1/N_1 \cong Q \cong H_2/N_2$.

Lemma 2.9.1 (Goursat's lemma)**.** *Let H_1 and H_2 be groups, and $H \leq H_1 \times H_2$. Assume that projections of H onto each of its oordinates are surjective. Then H is a fiber product of the projections of H_1 and H_2 onto some shared quotient of H_1 and H_2.*

Proof. Denote the projections of H onto H_1 and H_2 by π_1 and π_2 respectively. Note that $N_1 := \pi_1(\ker \pi_2)$ is a normal subgroup of $\pi_1(H) = H_1$ and $N_2 := \pi_2(\ker \pi_1)$ is a normal subgroup of $\pi_2(H) = H_2$. For $g \in H_1$, if g_1 and g_2 are two elements of H_2 with $(g, g_1) \in H$ and $(g, g_2) \in H$ then $(1, g_1 g_2^{-1}) \in H$ and thus $g_1 g_2^{-1} \in N_2$. Therefore it is possible to define a homomorphism $\psi : H_1 \to H_2/N_2$ by sending an element $g \in H_1$ to gN_2, for some choice of $g \in H_2$ such that $(g, g_1) \in H$. The kernel of ψ is N_1 and so $H_1/N_1 \cong H_2/N_2$. Denote this shared quotient by Q. Now define a homomorphism $\varphi_i : H_i \to Q$ by sending $g \to g \mod Q$; It holds that $\varphi_1(g_1) = \varphi_2(g_2)$ if and only

if $\psi(g_1) \equiv g_2 \mod N_2$, and the condition $\psi(g_1) \equiv g_2 \mod N_2$ holds if and only if $(g_1, g_2) \in G$. Therefore H equals the fiber product $H_1 \times_Q H_2$.

Chapter 3

Groups Satisfying the Orbits Condition (2.7)

Theorem 3.1 gives a list of subgroups H of S_n or A_n such that the maximal subgroup of S_n containing H is either a one-point or 2-set stabilizer and the orbits of H on k-sets of $\{1, \ldots, n\}$ fulfill condition (2.11). We then prove Theorem 1.1 based on this result.

Theorem 3.1. *Let G be S_n or A_n. Let D be as in Section 2.1.2 and let H be a subgroup of G contained in a one or two point stabilizer such that $O_2(H) = \cdots = O_D(H)$. If $G = S_n$, then H is as follows:*

1. *If H is contained in a one-point stabilizer, H is S_{n-1} or A_{n-1}.*
2. *If H is contained in a two-point stabilizer, H is S_{n-2}, A_{n-2}, $S_2 \times S_{n-2}$, $S_2 \times_{C_2} S_{n-2}$ or $S_2 \times A_{n-2}$.*

If $G = A_n$, then H is as follows:

1. *If H is contained in a one-point stabilizer, H is A_{n-1}.*
2. *If H is contained in a two-point stabilizer, H is A_{n-2} or $S_2 \times_{C_2} S_{n-2}$ (that is, H is either a pointwise stabilizer or a setwise stabilizer of a 2-set).*

Proof of Theorem 1.1 based on Theorems 2.1 and 3.1. Let M be the maximal subgroup of G containing H. By [16], Theorem 1.2, a constant N_1 can be chosen such that if $n > N_1$, either the genus of Ω^M is strictly larger than 2 or M is a point stabilizer or a 2-set stabilizer of G. Thus H is contained in a point stabilizer or a 2-set stabilizer of G. Choose N that is larger than both N_1 and the constant N_0 supplied by Theorem 2.1. Then by Theorem 2.1, H must also satisfy that $O_2(H) = \cdots = O_{\frac{n}{2}}(H)$, and if the ramification type of $F_1/\mathbb{C}(t)$ is not one of the exceptions given in Table A.1 then H satisfies the further condition that $O_1(H) = O_2(H)$. Theorem 3.1 gives the list of possible groups for H under these conditions. Proposition 9.0.1 details which of these options actually occur. ■

Figure 3.1: Candidate genus 0 and 1 subgroups of S_n

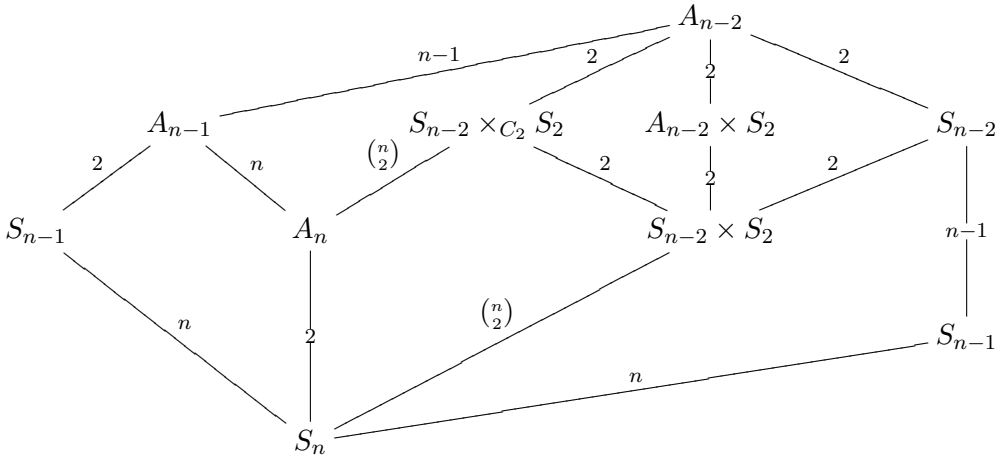
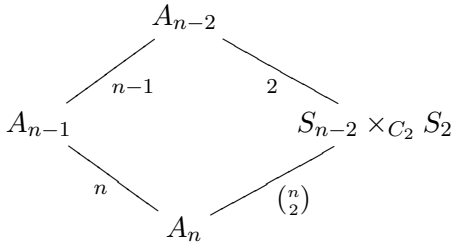


Figure 3.2: Candidate genus 0 and 1 subgroups of A_n



Chapter 4

Orbit Analysis

The initial step towards proving Theorem 3.1 is to show that the group H specified in the theorem has a large enough orbit on which it acts D-homogenously. In this section, Lemma 4.0.1 shows that a subgroup of $S_{n-2} \times S_2$ for which the orbits condition (2.10) holds has an orbit of length at least $n-2$. This is done using basic combinatoric arguments detailed in Lemmas 4.0.2 and 4.0.3.

Lemma 4.0.1. *Let H be a permutation group on n elements, $n \geq 7$. If $H \leq S_{n-2} \times S_2$ and $O_2 = O_3$, then H has a single orbit on $\{1, \dots n-2\}$.*

Remark. Bundy and Hart ([2], Lemma 2.1) show that for a general $H \leq S_n$, if $O_k = O_{k+1}$ for $1 \leq k < \frac{n-1}{2}$ then H has an orbit of length at least $n-k$. The general result relies on representation theory; the weaker version given in Lemma 4.0.1 is proved by elementary counting arguments.

Lemma 4.0.2. *Let H be a permutation group acting on the set $\{1, \dots n\}$, $n \geq 2$, and let X and Y be disjoint unions of orbits of H on $\{1, \dots n\}$; denote $|X| = N_1$ and $|Y| = N_2$ and assume $N_1 \geq N_2$. Let $k \leq N_1 + N_2$. Then*

1. *The orbits of H on k-sets of $X \cup Y$ can be counted as follows:*

$$O((X \cup Y)^{\{k\}}) = \sum_{i=0}^{N_2} O(X^{\{k-i\}} \cup Y^{\{i\}}).$$

2. *If $\ell \leq N_2$ and $X_1, \dots X_r$ are disjoint unions of orbits of H on $X^{\{k\}}$ such that $X^{\{k\}} = \bigcup_{i=1}^{r} X_i$, then*

$$O(X^{\{k\}} \cup Y^{\{\ell\}}) = \sum_{i=1}^{r} O({X_i}^{\{1\}} \cup Y^{\{\ell\}}).$$

3. *For $i \leq N_1$, $j \leq N_2$, the number of orbits of H on $X^{\{i\}} \cup Y^{\{j\}}$ can be bounded as follows:*

$$\max(O(X^{\{i\}}), O(Y^{\{j\}})) \leq O(X^{\{i\}} \cup Y^{\{j\}}) \leq \min(O(X^{\{i\}}) \cdot |Y^{\{j\}}|, |X^{\{i\}}| \cdot O(Y^{\{j\}})).$$

4. For $j = N_2$,

$$O(X^{\{i\}} \cup Y^{\{N_2\}}) = O(X^{\{i\}}).$$

Proof of Lemma 4.0.2. For part (1), note that a k-set of $X \cup Y$ with i elements from Y passes under the action of H to a k-set with i elements from Y, and each k-set of $X \cup Y$ has $0 \leq i \leq N_2$ elements from Y.

For part (2), as $X_1, \ldots X_r$ are disjoint unions of orbits of H on $X^{\{k\}}$ we get $X^{\{1\}} \cup Y^{\{\ell\}} = \bigcup_{i=1}^{r} {X_i}^{\{1\}} \cup Y^{\{\ell\}}$. The result follows from the fact that sets of the form ${X_j}^{\{1\}} \cup Y^{\{\ell\}}$ pass under the action of H to sets of the same form.

For part (3), since X and Y are disjoint, we can view each orbit of H on $X^{\{i\}} \cup Y^{\{j\}}$ as an orbit of H on the ordered tuples $(x^{\{i\}}, y^{\{j\}})$ where $x^{\{i\}}$ is an i-set of X and $y^{\{j\}}$ is a j-set of Y. If x_1 and x_2 are representatives of different orbits of H on $X^{\{i\}}$ and $y \in Y^{\{j\}}$, an element of H that sends (x_1, y) to (x_2, y) must send x_1 to x_2. Therefore $H(x_1, y)$ and $H(x_2, y)$ are different orbits of H on $X^{\{i\}} \cup Y^{\{j\}}$, and so H must have at least $O(X^{\{i\}})$ orbits on $X^{\{i\}} \cup Y^{\{j\}}$. By a symmetric argument, $O(Y^{\{j\}}) \leq O(X^{\{i\}} \cup Y^{\{j\}})$. For a representative x_1 of an orbit of H on $X^{\{i\}}$ and some $y \in Y^{\{j\}}$, $H(x_1, y)$ is an orbit of H on $X^{\{i\}} \cup Y^{\{j\}}$. Since each orbit of H on $X^{\{i\}} \cup Y^{\{j\}}$ can be obtained in this way, we get that $O(X^{\{i\}} \cup Y^{\{j\}}) \leq O(X^{\{i\}}) \cdot |Y^{\{j\}}|$, and by a symmetric argument $O(X^{\{i\}} \cup Y^{\{j\}}) \leq |X^{\{i\}}| \cdot O(Y^{\{j\}})$.

For 4, since $|Y| = N_2$, there is a single N_2-set of Y and the result follows from part 3. ■

Lemma 4.0.3. *Let H be a group acting on n elements where $n \geq 5$. Assume H has two orbits A and B with $|A| > |B| \geq 2$ and assume that H has $|B|$ orbits when acting on the 2-sets of the form $A^{\{1\}} \cup B^{\{1\}}$. Then the action of H on A is not 2-homogenous.*

Proof of Lemma 4.0.3. In order to show that the action of H on A is not 2-homogenous, it suffices to show that this action has a non-trivial block system: If A_1 and A_2 are non-trivial blocks of H such that $|A_2| \geq 2$ we can take elements $a \in A_1$ and $a', a'' \in A_2$. If there exists some $\sigma \in H$ that sends (a', a'') to (a', a), then σ sends some element of the block A_2 to the block A_1 but sends another element of A_2 to to A_2 itself, in contradiction to the assumption that A_1 and A_2 are blocks of H acting on A.

Denote $|B| = N$ and denote the orbits of H on $A^{\{1\}} \cup B^{\{1\}}$ by o_1,...o_N and the elements of B by $\{b_1, b_2, \ldots b_N\}$. Let A_i be the set of elements of A that appear with b_i in the orbit o_1, that is,

$$A_i = \{a \in A : \{a, b_i\} \in o_1\}.$$

We claim that $\{A_i\}_{i=1}^{N}$ is a block system for the action of H on A.

The sets $\{A_i\}_{i=1}^{N}$ are a partition of A: Since A and B are orbits of H, for each $a \in A$ and $b \in B$, the orbit o_1 must have an element containing a and an element

containing b. Therefore $\cup_{i=1}^{N} A_i = A$ and the sets A_i are non-empty. The sets $\{A_i\}_{i=1}^{N}$ are pairwise disjoint: The orbits $o_1, \dots o_N$ form a partition of $A^{\{1\}} \cup B^{\{1\}}$. There are $|A| \cdot |B|$ sets of this type, and since each of the $|B| = N$ orbits is of size at least $|A|$, each orbit must be of size exactly $|A|$. As each element of A must appear in o_1, we get that each element of A appears in o_1 exactly once.

The partition $\{A_i\}_{i=1}^{N}$ is non-trivial: Since $|o_i| = |A| > |B|$ and $|o_1| = |A|$, there is some element $b_i \in B$ that appears twice in the orbit o_1, giving us $|A_i| > 2$.

The partition $\{A_i\}_{i=1}^{N}$ is a block system: For $\sigma \in H$, if σ fixes b_i then it sends each element of A_i to A_i; else, if $\sigma(b_i) = b_j$ for some $j \neq i$ then σ sends A_i to A_j. By a previous argument, these sets are disjoint.

Proof of Lemma 4.0.1. Denote $A := \{1, \dots n-2\}$ and $B = \{n-1, n\}$, and let $A_1, \dots A_s$ be the orbits of H on A. Item 1 of Lemma 4.0.2 for H acting on 2-sets of $\{1, \dots n\}$ reads:

$$O_2 = O(A^{\{2\}}) + O(A^{\{1\}} \cup B^{\{1\}}) + O(B^{\{2\}}). \tag{4.1}$$

For 3-sets of $\{1, \dots n\}$ part 1 reads:

$$O_3 = O(A^{\{3\}}) + O(A^{\{2\}} \cup B^{\{1\}}) + O(A^{\{1\}} \cup B^{\{2\}}). \tag{4.2}$$

By the Livingstone-Wagner theorem for H acting on A, we have

$$O(A^{\{2\}}) \leq O(A^{\{3\}}). \tag{4.3}$$

Since $|B| = 2$, by part 3 of Lemma 4.1 it holds that:

$$O(A^{\{1\}} \cup B^{\{2\}}) = O(A^{\{1\}}) = s,$$

where s denotes the number of orbits of H on A. Since $|B| = 2$, it holds that $O(B^{\{2\}}) = 1$. Therefore if $s \geq 2$, the following inequality is strict (as the left hand side equals one, and the right hand side must be at least s):

$$O(B^{\{2\}}) < O(A^{\{1\}} \cup B^{\{2\}}). \tag{4.4}$$

The goal now is to show that if $s \geq 2$, the following bound on $O(A^{\{1\}} \cup B^{\{1\}})$ holds:

$$O(A^{\{1\}} \cup B^{\{1\}}) \leq O(A^{\{2\}} \cup B^{\{1\}}). \tag{4.5}$$

Assuming (4.5), apply estimates (4.3) and (4.4) to get a strict bound of (4.1) by summands of (4.2). We reach the contradiction $O_2 < O_3$.

Case I: . Assume $s \geq 3$. Let j be a mapping from $\{1, \dots s\}$ to itself that does not fix any points or transpose any two elements (i.e., the sets $\{\{i, j(i)\}\}_{i=1,\dots s}$ are all of

size 2 and pairwise disjoint). Since $s \geq 3$, such a map exists, for example $j(i) = (i+1)$ mod s. For $i = 1, \dots s$ we have by part 3 of Lemma 4.0.2 the inequality:

$$O(A_i{}^{\{1\}} \cup B^{\{1\}}) \leq O(A_i{}^{\{1\}} \cup A_{j(i)}{}^{\{1\}} \cup B^{\{1\}}).$$

Running the sum over all orbits A_i, since $A = \cup_{i=1}^{s} A_i$, part 2 in Lemma 4.0.2 gives:

$$O(A^{\{1\}} \cup B^{\{1\}}) = \sum_{i=1}^{s} O(A_i{}^{\{1\}} \cup B^{\{1\}}) \leq \sum_{i=1}^{s} O(A_i{}^{\{1\}} \cup A_{j(i)}{}^{\{1\}} \cup B^{\{1\}}). \tag{4.6}$$

Since the pairs $\{i, j(i)\}$ are distinct the following estimate holds:

$$\sum_{i=1}^{s} O(A_i{}^{\{1\}} \cup A_{j(i)}{}^{\{1\}} \cup B^{\{1\}}) \leq \sum_{i<j} O(A_i{}^{\{1\}} \cup A_j{}^{\{1\}} \cup B^{\{1\}}). \tag{4.7}$$

Apply part 1 of Lemma 4.0.2 multiple times for $A = \bigcup_{i=1}^{s} A_i$ to get:

$$O(A^{\{2\}}) = \sum_{i=1}^{s} O(A_i{}^{\{2\}}) + \sum_{i<j} O(A_i{}^{\{1\}} \cup A_j{}^{\{1\}}). \tag{4.8}$$

Attain a lower bound on $O(A^{\{2\}})$ by ignoring the left hand summand of (4.8) and estimating the right hand summand using (4.7):

$$O(A^{\{2\}}) \geq \sum_{i<j} O(A_i{}^{\{1\}} \cup A_j{}^{\{1\}} \cup B^{\{1\}}). \tag{4.9}$$

Bound the right hand side of (4.7) using (4.6) to get:

$$O(A^{\{2\}}) \geq O(A^{\{1\}} \cup B^{\{1\}}). \tag{4.10}$$

By part 3 of Lemma 4.1:

$$O(A^{\{2\}}) \leq O(A^{\{2\}} \cup B^{\{1\}}). \tag{4.11}$$

Finally, inequalities (4.6) and (4.11) combined give

$$O(A^{\{1\}} \cup B^{\{1\}}) \leq O(A^{\{2\}} \cup B^{\{1\}}),$$

as required.

Case II: Assume $s = 2$. As $n \geq 5$ and $s = 2$, assume without loss of generality that $|A_1| > 2$. As $A = A_1 \cup A_2$ is a partition of A into disjoint orbits, by part 2 of Lemma 4.0.2:

$$O(A^{\{1\}} \cup B^{\{1\}}) = O(A_1{}^{\{1\}} \cup B^{\{1\}}) + O(A_2{}^{\{1\}} \cup B^{\{1\}}). \tag{4.12}$$

the goal (4.5) now reads:

$$O(A^{\{2\}} \cup B^{\{1\}}) \geq O({A_1}^{\{1\}} \cup B^{\{1\}}) + O({A_2}^{\{1\}} \cup B^{\{1\}}).$$

By the same argument taken with the fact that ${A_1}^{\{2\}}$ and ${A_1}^{\{1\}} \cup {A_2}^{\{1\}}$ are disjoint, and each is a union of some orbits of H on $A^{\{2\}}$:

$$O(A^{\{2\}} \cup B^{\{1\}}) \geq O({A_1}^{\{2\}} \cup B^{\{1\}}) + O({A_1}^{\{1\}} \cup {A_2}^{\{1\}} \cup B^{\{1\}}). \tag{4.13}$$

Use part 3 of Lemma 4.0.2 to estimate $O({A_2}^{\{1\}} \cup B^{\{1\}})$ to get the following lower bound on $O({A_2}^{\{1\}} \cup {A_1}^{\{1\}} \cup B^{\{1\}})$:

$$O({A_2}^{\{1\}} \cup {A_1}^{\{1\}} \cup B^{\{1\}}) \geq O({A_2}^{\{1\}} \cup B^{\{1\}}). \tag{4.14}$$

It remains to show that $O({A_1}^{\{2\}} \cup B^{\{1\}}) \geq O({A_1}^{\{1\}} \cup B^{\{1\}})$. If $O({A_1}^{\{1\}} \cup B^{\{1\}}) = 1$ this holds trivially, so assume that $O({A_1}^{\{1\}} \cup B^{\{1\}}) \geq 2$. Estimate $O({A_1}^{\{1\}} \cup B^{\{1\}})$ and $O({A_1}^{\{2\}} \cup B^{\{1\}})$ using part 3 of Lemma 4.0.2 to get:

$$O({A_1}^{\{1\}} \cup B^{\{1\}}) \leq |B| \cdot O({A_1}^{\{1\}}) = 2.$$

and

$$\max(O({A_1}^{\{2\}}), O(B^{\{1\}})) \leq O({A_1}^{\{2\}} \cup B^{\{1\}}).$$

(So in fact $O({A_1}^{\{1\}} \cup B^{\{1\}}) = 2$). Recall that $2 \geq O(B^{\{1\}})$. Therefore if $O({A_1}^{\{2\}}) \geq 2$, it holds that:

$$\max(O({A_1}^{\{2\}}), O(B^{\{1\}})) = O({A_1}^{\{2\}}) \geq O({A_1}^{\{1\}} \cup B^{\{1\}}), \tag{4.15}$$

and so

$$O({A_1}^{\{2\}} \cup B^{\{1\}}) \geq \max(O({A_1}^{\{2\}}), O(B^{\{1\}})) \geq O({A_1}^{\{1\}} \cup B^{\{1\}})), \tag{4.16}$$

as required.

Else, $O({A_1}^{\{2\}}) = 1$. First, assume that B is not an orbit of H, i.e., B is a union of two fixed points of H. Therefore

$$O({A_1}^{\{1\}} \cup B^{\{1\}}) = 2O({A_1}^{\{1\}}) = 2,$$

and

$$O({A_1}^{\{2\}} \cup B^{\{1\}}) = 2O({A_1}^{\{2\}}) \geq 2 = O({A_1}^{\{1\}} \cup B^{\{1\}}),$$

as required.

It remains to rule out the case where $O({A_1}^{\{2\}}) = 1$ and B is an orbit of H. In this case, A_1 and B are orbits of H such that $|A_1| > |B| \geq 2$, $O({A_1}^{\{2\}}) = 1$ and $O({A_1}^{\{1\}} \cup B^{\{1\}}) = 2$; Lemma 4.0.3 now gives that $O({A_1}^{\{2\}}) \geq 2$, a contradiction.

Chapter 5

Proof of Theorem 3.1

Proof of Theorem 3.1. By assumption, H is contained in a one point stabilizer or in a stabilizer of a two element set.

Case I: H fixes exactly one point of $\{1, \dots n\}$. Without loss of generality, assume that n is the fixed point of H. Denote $A := \{1, \dots n-1\}$ and $B := \{n\}$. These sets are of size $n-1$ and 1 respectively. We will show that H acts D-homogenously on A and therefore $H = A_{n-1}$ or S_{n-1}. Since $|B| = 1$, by part 4 of Lemma 4.0.2, $O(A^{\{j\}} \cup B^{\{1\}}) = 1$ for $j \leq |A|$. Use this fact along with part 1 of Lemma 4.0.2 to count the orbits of H on $\{1, \dots n\}$ and get:

$$O_2 = O(A^{\{2\}}) + O(A^{\{1\}})$$

$$O_3 = O(A^{\{3\}}) + O(A^{\{2\}})$$

$$\dots$$

$$O_D = O(A^{\{D\}}) + O(A^{\{D-1\}}).$$

By assumption, $O_2 = O_3 = \dots = O_D$. By the Livingstone-Wagner theorem for H acting on A, $O(A^{\{i\}}) \leq O(A^{\{i+1\}})$ for $i = 1, \dots, \lfloor \frac{n-1}{2} \rfloor$. Since all left hand sides of the equations above are equal, we get:

$$O(A^{\{1\}}) = O(A^{\{2\}}) = \dots = O(A^{\{D\}}). \tag{5.1}$$

We will show that $O(A^{\{1\}}) = 1$ (that is, A is an orbit of H). Suppose H has $s > 1$ orbits on A, denoted $A_1, \dots A_s$. By assumption H fixes no points in A, so each of the orbits A_i is of size greater than 2. The 2-sets of A are of the form ${A_i}^{\{1\}} \cup {A_j}^{\{1\}}$ for $i \neq j$ or ${A_i}^{\{2\}}$ for $i = 1, \dots, s$. Enumerate $O(A^{\{2\}})$ using part 2 of Lemma 4.0.2 to get:

$$O(A^{\{2\}}) = \sum_{i=1}^{s} O({A_i}^{\{2\}}) + \sum_{i<j} O({A_i}^{\{1\}} \cup {A_j}^{\{1\}}). \tag{5.2}$$

By equality (5.1), $O(A^{\{2\}}) = O(A^{\{1\}}) = s$. There are $\binom{s}{2}$ pairs $\{i, j\}$ with $i, j \in \{1, \dots s\}$

and $i < j$ and the trivial bounds $O(A_i{}^{\{1\}} \cup A_j{}^{\{1\}}) \geq 1$ and $O(A_i{}^{\{2\}}) \geq 1$ hold for each such pair. Use these rough estimates to bound the right hand side of equality (5.2) to get that the integer s must satisfy $s \geq s + \frac{s^2-s}{2}$. Therefore $s = 1$, i.e., $1 = O(A^{\{1\}}) = \cdots = O(A^{\{D\}})$. Therefore H acts D-homogenously on $\{1, \ldots n\}$, as required.

Case II: H stabilizes a two element set pointwise. Without loss of generality assume this set is $B := \{n-1, n\}$ and denote $A := \{1, \ldots n-2\}$. Since $H \leq S_{n-2} \times S_2$ and $O_2 = O_3$, by Lemma 4.0.1, A is an orbit of H. We will show that H acts D-homogenously on A, and so $H = A_{n-2}$ or S_{n-2}. The group H acts pointwise on B and $|B| = 2$, so for $1 \leq i \leq |A|$:

$$O(A^{\{i\}} \cup B^{\{1\}}) = 2O(A^{\{i\}}). \tag{5.3}$$

We claim by induction that $O(A^{\{k\}}) = 1$ for $k = 2, \ldots, D$.

First, use part 1 of Lemma 4.0.2 to count the orbits of H on $\{1, \ldots, n\} = A \cup B$:

$$O_2 = O(A^{\{2\}}) + O(A^{\{1\}} \cup B^{\{1\}}) + O(B^{\{2\}}). \tag{5.4}$$

By (5.3),

$$O(A^{\{1\}} \cup B^{\{1\}}) = 2 \cdot O(A^{\{1\}}) = 2.$$

Since $|B| = 2$, it holds that $|B^{\{2\}}| = 1$ and in particular $O(B^{\{2\}}) = 1$. Plug these values into (5.4) to get:

$$O_2 = O(A^{\{2\}}) + 3. \tag{5.5}$$

Calculate O_3 by part 1 of Lemma 4.0.2:

$$O_3 = O(A^{\{3\}}) + O(A^{\{2\}} \cup B^{\{1\}}) + O(A^{\{1\}} \cup B^{\{2\}}). \tag{5.6}$$

By (5.3) it holds that $O(A^{\{2\}} \cup B^{\{1\}}) = 2O(A^{\{2\}})$. Since $|B| = 2$, part 4 of Lemma 4.0.2 gives that $O(A^{\{1\}} \cup B^{\{2\}}) = O(A^{\{1\}}) = 1$. Overall:

$$O_3 = O(A^{\{3\}}) + 2O(A^{\{2\}}) + 1.$$

By the Livingstone-Wagner theorem, $O(A^{\{i\}}) \leq O(A^{\{i+1\}})$ for $i \leq \lfloor \frac{n-2}{2} \rfloor$. Trivially, $1 \leq O(A^{\{i\}})$ for $i \in \{1, \ldots n-2\}$; so in order to maintain both the equality $O_2 = O_3$ and equalities (5.5) and (5.6), it must hold that $1 = O(A^{\{2\}}) = O(A^{\{3\}})$. Substitute these values into (5.5) to get $O_2 = 4$. By assumption $O_2 = \cdots = O_D$ and so $O_2 = \cdots = O_D = 4$.

Assume that $O(A^{\{k\}}) = 1$ for $2 \leq k < D$. We will show that $O(A^{\{k+1\}}) = 1$ and $O_{k+1} = 4$. For $2 \leq k \leq n-2$, Lemma 4.0.2 gives us

$$O_{k+1} = O(A^{\{k+1\}}) + 2O(A^{\{k\}}) + O(A^{\{k-1\}}). \tag{5.7}$$

By the induction hypothesis $O(A^{\{k\}}) = 1$ and therefore $O(A^{\{k-1\}}) = 1$. As $k+1 \leq D$ we have $O_{k+1} = 4$. Plugging these values in equality (5.7) we get $O_{k+1} = 4$ on the left hand side of the equation, and therefore $O(A^{\{k+1\}}) = 1$, as required.

We have now shown that H is D-homogenous on A. Since H is D-homogenous on A and fixes B pointwise, $H = A_{n-2}$ or $H = S_{n-2}$.

Case III: H has an orbit of length 2. Without loss of generality assume this orbit is $\{n-1, n\}$.

The first step is to show that the action of H on $\{1, \dots n-2\}$ is D-homogenous. Denote $A := \{1, \dots n-2\}$ and $B := \{n-1, n\}$. Since $n \geq 5$, $H \leq S_{n-2} \times S_2$ and $O_2 = O_3$, by Lemma 4.0.1, A is an orbit of H.

Count the orbits of H on k-sets using part 1 of Lemma 4.0.2 to get for $k = 2$:

$$O_2 = O(A^{\{2\}}) + O(A^{\{1\}} \cup B^{\{1\}}) + O(B^{\{2\}}). \tag{5.8}$$

For $k = 3$, the same argument yields:

$$O_3 = O(A^{\{3\}}) + O(A^{\{2\}} \cup B^{\{1\}}) + O(A^{\{1\}} \cup B^{\{2\}}). \tag{5.9}$$

In general, for $k \geq 3$:

$$O_k = O(A^{\{k\}}) + O(A^{\{k-1\}} \cup B^{\{1\}}) + O(A^{\{k-2\}} \cup B^{\{2\}}). \tag{5.10}$$

Bound each summand of (5.8) by a summand of (5.9) as follows:

1. By the Livingstone-Wagner theorem for H acting on A,

$$O(A^{\{2\}}) \leq O(A^{\{3\}}).$$

2. By part 3 of Lemma 4.0.2,

$$O(A^{\{1\}} \cup B^{\{1\}}) \leq O(B^{\{1\}}) \cdot O(A^{\{1\}}) = 2,$$

and so $O(A^{\{1\}} \cup B^{\{1\}}) \in \{1, 2\}$. If $O(A^{\{1\}} \cup B^{\{1\}}) = 1$ then trivially $O(A^{\{1\}} \cup B^{\{1\}}) \leq O(A^{\{2\}} \cup B^{\{1\}})$. If $O(A^{\{1\}} \cup B^{\{1\}}) = 2$, since A and B are both orbits of H with $|A| > |B| \geq 2$, by Lemma 4.0.3 it holds that $O(A^{\{2\}}) \geq 2$. By part 3 of Lemma 4.0.2, it holds that $O(A^{\{2\}}) \leq O(A^{\{2\}} \cup B^{\{1\}})$ and thus $O(A^{\{1\}} \cup B^{\{1\}}) = 2 \leq O(A^{\{2\}} \cup B^{\{1\}})$. In conclusion,

$$O(A^{\{1\}} \cup B^{\{1\}}) \leq O(A^{\{2\}} \cup B^{\{1\}}).$$

3. Since $|B| = 2$, it holds that $O(B^{\{2\}}) = 1$ and so trivially

$$1 = O(B^{\{2\}}) \leq O(A^{\{1\}} \cup B^{\{2\}}).$$

Since $O_2 = O_3$, we attained the following equalities:

1. $O(A^{\{2\}}) = O(A^{\{3\}})$.
2. $O(A^{\{1\}} \cup B^{\{1\}}) = O(A^{\{2\}} \cup B^{\{1\}})$.
3. $1 = O(B^{\{2\}}) = O(A^{\{1\}} \cup B^{\{2\}})$.

Now, bound the summands of (5.9) from above as follows:

1. Since $O(A^{\{1\}} \cup B^{\{1\}}) \leq |B| \cdot O(A^{\{1\}}) = 2$, it holds that
$$O(A^{\{2\}} \cup B^{\{1\}}) \leq 2.$$
2. Since $O(A^{\{2\}}) \leq O(A^{\{2\}} \cup B^{\{1\}})$, it holds that
$$O(A^{\{3\}}) = O(A^{\{2\}}) \leq 2.$$
3. As seen in a previous step, $O(A^{\{1\}} \cup B^{\{2\}}) = 1$. ■

Use these bounds on the right hand side of (5.9) to get that $O_3 \leq 5$.

We now claim that $O(A^{\{2\}}) = 1$. Suppose $O(A^{\{2\}}) \geq 2$. Then by the Livingstone-Wagner theorem for H acting on A, $O(A^{\{4\}}) \geq O(A^{\{3\}}) \geq O(A^{\{2\}}) \geq 2$.

For $k = 4$, equation (5.10) reads:

$$O_4 = O(A^{\{4\}}) + O(A^{\{3\}} \cup B^{\{1\}}) + O(A^{\{2\}} \cup B^{\{2\}}).$$

Since $|B| = 2$, by part 4 of Lemma 4.0.2 it holds that $O(A^{\{2\}} \cup B^{\{2\}}) = O(A^{\{2\}})$. By part 3 of Lemma 4.0.2, it holds that $O(A^{\{3\}} \cup B^{\{1\}}) \geq O(A^{\{3\}})$. Overall we get

$$O_4 \geq O(A^{\{4\}}) + O(A^{\{3\}}) + O(A^{\{2\}}) \geq 6.$$

However, since $O_4 = O_3$ this is a contradiction to the fact that $O_3 \leq 5$. Therefore $O(A^{\{2\}}) = 1$. Since $|A| > |B| = 2$ and $O(A^{\{2\}}) = 1$, Lemma 4.0.3 gives that $O(A^{\{1\}} \cup B^{\{1\}}) \neq 2$. It was previously shown that $O(A^{\{1\}} \cup B^{\{1\}}) \leq 2$, so $O(A^{\{1\}} \cup B^{\{1\}}) = 1$. Plug the values of $O(B^{\{2\}})$, $O(A^{\{2\}})$ and $O(A^{\{1\}} \cup B^{\{1\}})$ into (5.8) to get that $O_2 = 3$.

We now claim by induction that if $O_2 = O_k$ for some $2 \leq k \leq \lfloor \frac{n}{2} \rfloor$, then $O(A^{\{k\}}) = 1$ and $O(A^{\{k-1\}} \cup B^{\{1\}}) = 1$. This was already shown for the base case $k = 2$. Observe equation (5.10) for $k \geq 3$. As each of the three summands of (5.10) is at least 1 and $O_k = O_2 = 3$, each is equal to 1, proving the induction step.

By assumption $O_2 = O_3 = \cdots = O_D$, so we get that H is D-homogenous in its action on A.

Denote by H_1 the projection of H to S_{n-2} and by H_2 the projection of H to S_2. Since $H \leq S_{n-1} \times S_2$ acts D-homogenously on $\{1, \ldots, n-2\}$, the projection H_1 is

D-homogenous on $\{1, \dots n-2\}$. Therefore $H_1 = S_{n-2}$ or $H_1 = A_{n-2}$. Since $\{n-1, n\}$ is an orbit of H, the projection H_2 must contain more elements then the identity permutation on $\{n-1, n\}$, and so $H_2 = S_2$. By Lemma 2.9.1, the group H is a fiber product of projections of H_1 and H_2 onto a shared quotient. The only shared quotients of S_{n-2} and S_2 are $\{e\}$ or S_2, and the only shared quotient of A_{n-2} and S_2 is $\{e\}$. Therefore H is $S_{n-2} \times S_2$, $A_{n-2} \times S_2$ or $S_{n-2} \times_{C_2} S_2$.

Chapter 6

Alternating Extensions Inside Symmetric Extensions

The next few chapters will concern the question: Which of the groups listed in Theorem 3.1 indeed appear as subgroups fixing a genus 0 or 1 subfield of a symmetric or alternating extension? The setup is as follows:

6.1 Setup

Let N_0 be the constant given by Theorem 2.1. Let $\Omega/\mathbb{C}(t)$ be a Galois extension with Galois group G. Assume that $G = S_n$ or A_n, for some $n > N_0$. Denote by F the subfield of Ω fixed by a point stabilizer of G. Theorem 3.1 gives a list of candidate subgroups of G that may fix a subfield of Ω of genus 0 or 1.

In this section, assume that $G = S_n$. We examine the conditions under which A_n and A_{n-1} fix a subfield of Ω of genus 0 or 1.

Theorem 6.1. *The subfield of Ω fixed by $S_2 \times_{C_2} S_{n-2}$ is of genus 0 if and only if the ramification type of $F_2/\mathbb{C}(t)$ is $[1, 2^{\frac{n-1}{2}}], [1, 4^{\frac{n-1}{4}}], [2, 3, 4^{\frac{n-5}{4}}]$ for $n \equiv 5 \mod 8$ (Table A.1, type F3.2), in which case the genus of $\Omega^{S_{n-2}\times S_2}$ is 0.*

Theorem 6.2. *The subfield of Ω fixed by $S_{n-2} \times_{C_2} S_2$ cannot be of genus 1.*

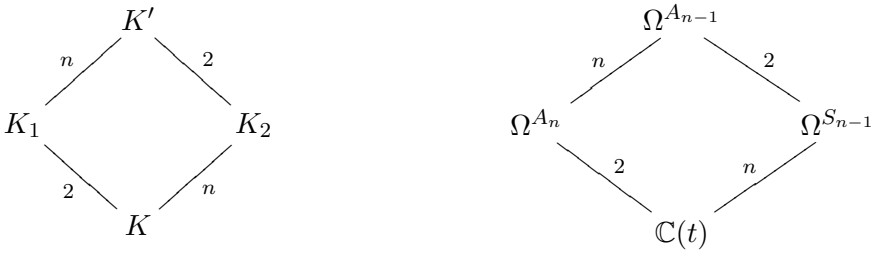
Proof of Theorem 6.2. If Ω^{A_n} is of genus 0, then Ω^{A_n} is a rational function field over $\mathbb{C}$, and thus Ω/Ω^{A_n} is an alternating extension of the field of rational functions over $\mathbb{C}$ of degree $n > N_0$. The constant N_0 was chosen to be such that the subfield of Ω fixed by a 2-set stabilizer of A_n is either very large or of genus 0, so the field Ω^{A_n} cannot be of genus 1; and if Ω^{A_n} is greater than 2 then $\Omega^{S_{n-2}\times_{C_2} S_2}$ must be of genus greater than 2 as well. It remains to determine whether is is possible for the genera of Ω^{A_n} and $\Omega^{S_{n-2}\times_{C_2} S_2}$ both to be 1, i.e., $\Omega^{S_{n-2}\times_{C_2} S_2}/\Omega^{A_n}$ is an unramified extension of elliptic function fields. Such an extension must be Galois ([19], Theorem 4.10), in contradiction to the fact that A_n is a simple group. ■

The following lemma follows from Abhyankar's lemma. It is phrased for general extensions of function fields, and its purpose in our context to calculate the ramification type of $\Omega^{A_{n-1}}/\Omega^{A_n}$ from the ramification type of $\Omega^{S_{n-2}}/\mathbb{C}(t)$.

Lemma 6.1.1. *Let K'/K be a function field extension of degree $2n$ with subfields K_1 and K_2 such that $[K' : K_1] = n$ and $[K' : K_2] = 2$. Let P be a place of K with ramification type $[a_1, \dots a_k, b_1, \dots b_\ell]$ in K_2 where the integers a_i, $i = 1, \dots l$ are even and the integers b_i, $i = 1, \dots \ell$, are odd. Then:*

1. *If P has a single place Q lying above it in K_1, then Q has ramification type $[\frac{a_1}{2}, \frac{a_1}{2}, \dots, \frac{a_k}{2}, \frac{a_k}{2}, b_1, \dots, b_\ell]$ in K'.*
2. *If P is split in K_1, then each of the places of K_1 lying above P has ramification type $[a_1, \dots a_k, b_1, \dots b_\ell]$ in K'.*
3. *Let Ω be the Galois closure of K'/K, and let x_P be a branch cycle of P. Then P is split in K_1 if and only if $x_P \in \mathrm{Aut}(\Omega/K_1)$.*

Figure 6.1: Setup and application of Lemma 6.1.1



Corollary 6.3. *Taking $K' = \Omega^{A_{n-1}}$, $K_1 = \Omega^{A_n}$, $K_2 = \Omega^{S_{n-1}}$ and $K = \mathbb{C}(t)$, the assumptions of Lemma 6.1.1 hold, leading to the following corollaries:*

Assume Ω^{A_n} is of genus 0. Let S be the set of places of Ω^{A_n} ramified in $\Omega^{A_{n-1}}$ and denote $r := |S|$. Then the ramification type of $\Omega^{A_{n-1}}/\Omega^{A_n}$ can be labeled as A_1, A_2, B_1, B_1',..., $B_{\frac{r-2}{2}}$, $B'_{\frac{r-2}{2}}$ such that:

1. *$B_i = B_i'$ for $i = 1, \dots \frac{r-2}{2}$.*
2. *The sets A_i, $i = 1, 2$, can be written as $[c_1^2 \dots c_k^2 b_1 \dots b_k]$ where k, $b_1, \dots b_k$ are odd.*

Corollary 6.4. *Denote the ramification type of $\Omega^{S_{n-1}}/\mathbb{C}(t)$ by $\mathcal{E}$. The genera of $\Omega^{A_n}, \Omega^{A_{n-1}}, \Omega^{S_{n-2}}$ are determined from $\mathcal{E}$ as follows:*

1. *The genus of the field Ω^{A_n} is 0 (respectively, 1) if and only if there are exactly two (respectively, four) odd ramification types in $\mathcal{E}$.*
2. *The genus of the field $\Omega^{S_{n-2}}$ is 0 (respectively, 1) if and only if the total number of entries larger than 1 in $\mathcal{E}$ is $2n-2$ (respectively, $2n$).*

3. The total number of odd entries in odd ramification type of $\mathcal{E}$ is:

$$2g_{A_{n-1}} - 4g_{S_{n-1}} + 2.$$

Proof of Corollary 6.3. Since $[\Omega^{A_n} : \mathbb{C}(t)] = 2$, each place P of $\mathbb{C}(t)$ is either totally split in Ω^{A_n} or has a single place Q of F_1 lying above it with ramification index 2, i.e., P is totally ramified in F_1. Denote the decomposition groups of P and Q in Ω by D_P and D_Q respectively. Note that $D_Q = D_P \cap A_n$, so P is totally ramified if and only if the generator x_P of D_P is an odd permutation.

By assumption $g_{\mathbb{C}(t)} = g_{A_n} = 0$. Take the Riemann-Hurwitz formula for the extension $\Omega^{A_n}/\mathbb{C}(t)$:

$$\sum_{P \in \mathbb{P}_{\mathbb{C}(t)}} R_{\Omega^{A_n}/\mathbb{C}(t)}(P) = 2. \tag{6.1}$$

Therefore there are exactly two places P_1 and P_2 of $\mathbb{C}(t)$ that are not split in Ω^{A_n}. For $i = 1, 2$, denote by Q_i the single place of Ω^{A_n} lying above P_i.

Let $[a_1, \dots a_k, b_1, \dots b_\ell]$ be the ramification type of P_1 in F_2, where $a_1, \dots, a_k$ are even integers and $b_1, \dots, b_\ell$ are odd integers. By assertion 1 of Lemma 6.1.1,

$$E_{A_n:A_{n-1}}(Q_1) = [\frac{a_1}{2}, \frac{a_1}{2}, \dots \frac{a_k}{2}, \frac{a_k}{2}, b_1, \dots b_\ell].$$

Recall the ramification type of P in $\Omega^{S_{n-1}}$ coincides with the cycle structure of x_P. A place P is ramified in Ω^{A_n} if and only if x_P is an odd permutation, so P is ramified in Ω^{A_n} if and only if k is an odd integer (i.e., x_P has an odd number of even length cycles). Since P_1 is ramified in Ω^{A_n}, the integer k must be an odd. Relabel $c_i := \frac{a_i}{2}$ and repeat the argument above for P_2 to get assertion 2.

Let P be one of the $r-2$ remaining places $P \in S - P_1, P_2$ that are split in Ω^{A_n}. By assertion 2 of Lemma 6.1.1, if there are two places, Q_1' and Q_2' of Ω^{A_n} lying above P, each has the same ramification type in $\Omega^{A_{n-1}}$ as P has in $\Omega^{S_{n-1}}$, i.e.: $E_{A_n:A_{n-1}}(Q_1') = E_{A_n:A_{n-1}}(Q_2') = E_{S_n:S_{n-1}}(P)$. Denote $B_1 := E_{A_n:A_{n-1}}(Q_1')$ and $B_1' := E_{A_n:A_{n-1}}(Q_2')$ to get assertion 1.

Proof of Corollary 6.4. For assertion 1, by Lemma 6.1.1, P is ramified in Ω^{A_n} and only if its branch cycle x_P in Ω is odd. Since $[\Omega^{A_n} : \mathbb{C}(t)] = 2$, a place P of $\mathbb{C}(t)$ is ramified in Ω^{A_n} if and only if it is totally ramified, in which case

$$R_{S_n:A_n}(P) = 1.$$

Plug this into the Riemann-Hurwitz formula for $\Omega^{A_n}/\mathbb{C}(t)$ to get that $g_{A_n} = 0$ (respectively, 1) if and only if there are exactly two (respectivley, four) odd ramification types in $\mathcal{E}$. Assertion 2 is given by applying the Riemann-Hurwitz formula to the extension

$\Omega^{S_{n-1}}/\mathbb{C}(t)$, as

$$\sum_P R_{\Omega^{S_{n-1}}/\mathbb{C}(t)}(P) = \sum_{T\in\mathcal{E}}\sum_{e\in T} e - 1$$

. For Assertion 3, apply the Riemann-Hurwitz formula to the extension $\Omega^{A_{n-1}}/\Omega^{S_{n-1}}$. Since $[\Omega^{A_{n-1}} : \Omega^{S_{n-1}}] = 2$, the ramification contribution $\sum_{\mathfrak{p}\in\mathbb{P}_{\Omega^{S_{n-1}}}} E_{S_{n-1}:A_{n-1}}(\mathfrak{p})$ is the total number of places of $\Omega^{S_{n-1}}$ ramified in $\Omega^{A_{n-1}}$. It remains to show that this is also the total number of odd entries in odd ramification types in $\mathcal{E}$. For a place $Q \in \mathbb{P}_{\Omega^{A_{n-1}}}$, let $\mathfrak{q} \in \mathbb{P}_{\Omega^{A_n}}$ be the restriction of Q to Ω^{A_n}, let $\mathfrak{p}$ be the restriction of Q to $\Omega^{S_{n-1}}$, and let P be the place of $\mathbb{C}(t)$ lying below Q, which must therefore must also lie below $\mathfrak{q}$ and $\mathfrak{p}$. By Abhyankar's lemma and the multiplicity of ramification indexes in extensions,

$$e(Q|\mathfrak{p}) = \frac{\mathrm{lcm}((e(\mathfrak{p}|P), e(\mathfrak{q}|P))}{e(\mathfrak{p}|P)}. \tag{6.2}$$

Since $[\Omega : \mathbb{C}(t)] = 2$ it holds that $e(\mathfrak{q}|P) \in \{1, 2\}$, and so $e(Q|\mathfrak{p}) = 2$ if and only if $e(\mathfrak{p}|P)$ is odd and $e(\mathfrak{q}|P) = 2$. Let x_P be a branch cycle of P in Ω. By assertion 3 of Lemma 6.1.1, $e(\mathfrak{q}|P) = 2$ if and only if $x_P \notin A_n$. Recall that under our setup the cycle structure of x_P is $E_{S_n:S_{n-1}}$; Therefore $e(\mathfrak{q}|P) = 2$ if and only if P is an odd place. Each entry e of $E_{S_n:S_{n-1}}$ corresponds to a place $\mathfrak{p}$ of $\Omega^{S_{n-1}}$ with $e(Q|\mathfrak{p}) = e$, and so the number of places of $\Omega^{S_{n-1}}$ ramified in $\Omega^{A_{n-1}}$ is the number of odd entries in odd ramification types of $\mathcal{E}$. ■

Proof of Theorem 6.1 based on Lemma 6.1.1 and Corollary 6.3. Denote by $\mathcal{E}$ the ramification type of $\Omega^{S_{n-1}}/\mathbb{C}(t)$. Since $g_{A_n} = 0$, the field Ω^{A_n} is a rational function field over $\mathbb{C}$, and Ω/Ω^{A_n} is an alternating extension of degree $n > N_0$. By [16], Theorem 1.2, the subfield of Ω/Ω^{A_n} fixed by a 2-set stabilizer is of genus 0 if and only if the ramification type of $\Omega^{A_{n-1}}/\Omega^{A_n}$ appears in Table A.1. We now use Corollary 6.3 to check which entries of Table A.1 that correspond with the alternating group (i.e., all types are even) may appear as the ramification type of $\Omega^{A_{n-1}}/\Omega^{A_n}$. By this corollary, $E_{A_n:A_{n-1}}$ has at most two distinct types that appear without a duplicate. Therefore items $F1.5$, $F1.8$ and $F1.9$ of Table A.1 are the only possible options for $E_{A_n:A_{n-1}}$. In item $F1.9 : [2^{\frac{n-4}{2}}, 4][1^2, 2^{\frac{n-2}{2}}]X3$ the set $[2^{\frac{n-4}{2}}, 4]$ appears only once but contains an even entry without a duplicate, contradicting assertion 2 of Corollary 6.3. Similarly in $F1.8 : \left[1^3, 2^{(n-7)/2}, 4\right], [1, 2^{(n-1)/2}]X3$ the set $\left[1^3, 2^{(n-7)/2}, 4\right]$ appears only once but contains an even entry without a duplicate. Applying Lemma 7.2 in the case where $E_{S_nS_{n-1}}$ is $F3.2 : [1, 2^{\frac{n-1}{2}}], [1, 4^{\frac{n-1}{4}}], [2, 3, 4^{\frac{n-5}{4}}]$ for $n \equiv 5 \mod 8$, we get that $E_{A_n:A_{n-1}}$ is item $F1.5 : [1^2, 2^{\frac{n-5}{2}}, 3], [1, 2^{\frac{n-1}{2}}]X3$. So in this case, the subfield of Ω fixed by $S_2 \times_{C_2} S_{n-2}$ is indeed of genus 0. ■

s

Proof of Lemma 6.1.1. Denote places of K using the letter P, places of K_1 using the letter Q, places of K_2 using the letter $\mathfrak{p}$ and places of K' using the letter $\mathfrak{q}$, with

different places in the same extension distinguished by indexes. Since $[K_1 : K] = 2$, by the fundamental equality any place P of K has at most two places of K_1 lying above it.

Case 1: Assume P has a single place Q lying above it in K_1, and let $\mathfrak{q}$ be a place of K' lying above Q. Let $\mathfrak{p}$ be the restriction of $\mathfrak{q}$ to K_2. Denote $a := e(\mathfrak{q}|P)$. By Abhyankar's lemma, $e(\mathfrak{q}|P) = \text{lcm}(e(Q|P), e(\mathfrak{p}|P) = \text{lcm}(2, x)$, and so $e(\mathfrak{q}|\mathfrak{p}) = \frac{\text{lcm}(x,2)}{x}$ and $e(\mathfrak{q}|Q) = \frac{\text{lcm}(x,2)}{2}$.

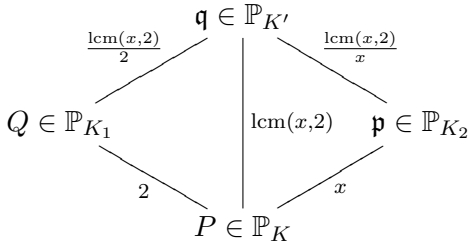


Figure 6.2: Ramification of places lying above P in the setup of Lemma 6.1.1

Since $[K' : K_2] = 2$, the place $\mathfrak{p}$ is either split or totally ramified in K'. If x is even, $e(\mathfrak{q}|\mathfrak{p}) = 1$ and so $\mathfrak{p}$ is split into two places $\mathfrak{q}_1$ and $\mathfrak{q}_2$ in K'. Without loss of generality, assume $\mathfrak{q} = \mathfrak{q}_1$. Repeat the argument above for $\mathfrak{q}_2$ to get that $\mathfrak{q}_2$ lies above Q and $e(\mathfrak{q}_1|Q) = e(\mathfrak{q}_2|Q) = \frac{x}{2}$. If x is odd, $e(\mathfrak{q}|\mathfrak{p}) = 2$ and so $\mathfrak{q}$ is a unique place of K' above $\mathfrak{p}$ and $e(\mathfrak{q} : Q) = a$. Repeat this argument for all places of K_2 lying above K, to get that K_1 has $2k + \ell$ different places lying above it with ramification indexes $\frac{a_1}{2}, \frac{a_1}{2}, \ldots, \frac{a_k}{2}, \frac{a_k}{2}, b_1, \ldots b_\ell$. The sum of these integers is n so by the fundamental equality, these are all the places of K' lying above Q. Therefore $E_{K'/K_1}(Q) = [\frac{a_1}{2}, \frac{a_1}{2}, \ldots, \frac{a_k}{2}, \frac{a_k}{2}, b_1, \ldots b_\ell]$.

Case 2: Assume that P splits into two places Q_1 and Q_2 in K_1. Let $\mathfrak{p}$ be a place of K_2 lying above P and let $\mathfrak{q}$ be some place place of K' lying above $\mathfrak{p}$. Denote $e(\mathfrak{p}|P) = x$. By Abhyankar's lemma (for visual aid see Figure **??** with $Q = Q_i$), $e(\mathfrak{q}|P) = \text{lcm}(e(Q|P), e(\mathfrak{p}|P)) = \text{lcm}(1, x) = x$. Therefore $e(\mathfrak{q}|\mathfrak{p}) = 1$ and $e(\mathfrak{q}|Q) = x$. There are two places $\mathfrak{q}_1$ and $\mathfrak{q}_2$ of K' lying above $\mathfrak{p}$. Each of the places $\mathfrak{q}_1$ and $\mathfrak{q}_2$ lies above exactly one of Q_1 or Q_2. Assume without loss of generality that $\mathfrak{q}_1|Q_1$ and $\mathfrak{q}_2|Q_2$. Take $\mathfrak{q} = \mathfrak{q}_i$ in the previous argument for $i = 1, 2$ to get that $e(\mathfrak{q}_1|Q_1) = x$ and $e(\mathfrak{q}_2|Q_2) = x$. Repeat for all places $\mathfrak{p}$ of K_2 lying above P to get that each of Q_1 and Q_2 has ramification type $[a_1, \ldots a_k, b_1, \ldots b_\ell]$ in K'.

Splitting Critera: Since $[K_1 : K] = 2$, it is a normal extension with Galois group $G' := G/\text{Gal}(K'/K_1)$. The decomposition group of a place $P \in K$ in K_1 is $D'_P := D_P/(\text{Gal}(K'/K_1) \cap D_P)$. A place P is split in K_1 if and only if its decomposition group in K_1 is trivial; this occurs if and only if D'_P is trivial, which occurs if and only if $D_P \subset \text{Gal}(K'/K_1)$, i.e., if and only if $x_P \in \text{Gal}(K'/K_1)$. This proves part 3. ■

Chapter 7

The case $A_{n-2} \times S_2$: Method of Calculation

Throughout this section, assume thesame setup as in Chapter 6 with $G = S_n$. The goal of this section and the one that follows is to determine which of the entries of Table A.1 admit the subgroup $A_{n-2} \times S_2$ of genus 0 or 1.

Proposition 7.0.1. *Let $F/\mathbb{C}(t)$ be a minimal field extension of degree $n > N_0$ with Galois closure by Ω such that $\mathrm{Gal}(\Omega/\mathbb{C}(t)) = S_n$. Then the field fixed by $A_{n-2} \times S_2$ is of genus 0 or 1 if and only if the ramification type of $F/\mathbb{C}(t)$ appears in Tables A.2 (genus 0) or A.3 (genus 1).*

In this section a formula (Proposition 7.0.2) is developed for calculating the Riemann-Hurwitz contribution of places in the extension $\Omega^{A_{n-2}\times S_2}/\Omega^{S_{n-2}\times S_2}$ from the ramification type of $F/\mathbb{C}(t)$. Proposition 7.0.2 is reached by observing that the extension $\Omega^{A_{n-2}}/\Omega^{S_{n-2}\times S_2}$ is Galois with Galois group $C_2 \times C_2$ (Claim 7.1.1). Lemma 7.1.2 is used to calculate ramification in subfields of such an extension.

Proposition 7.0.1 is proved by going over the entries of Table A.1 and using the formula in Proposition 7.0.2 and the Riemann-Hurwitz formula to either directly calculate the genus of $A_{n-2} \times S_2$ or show that it is very large. The actual calculations are handled in Section 8.

Proposition 7.0.2 (Formula for the ramification in $\Omega^{A_{n-2}\times S_2}/\Omega^{S_{n-2}\times S_2}$)**.** *Let P be a place of $\mathbb{C}(t)$, and $F/\mathbb{C}(t)$ a minimal extension of degree n with Galois closure Ω such that $\mathrm{Gal}(\Omega/\mathbb{C}(t)) = S_n$, i.e., $F = \Omega^{S_{n-1}}$.*

Write $E_{F/\mathbb{C}(t)}(P)$ as the disjoint union $A \cup B \cup C$ of the following three sets:

$$A := \{x \in E_{F/\mathbb{C}(t)}(P) : x \text{ odd}\}$$

$$B := \{x \in E_{F/\mathbb{C}(t)}(P) : x \equiv 2 \mod 4\}$$

$$C := \{x \in E_{F/\mathbb{C}(t)}(P) : x \equiv 0 \mod 4\}.$$

Denote $|A| = n_A, |B| = n_B, |C| = n_C$. *If* $n_C + n_B$ *is even (i.e.,* x_P *is an even permutation), then:*

$$R_{(S_2\times S_{n-2}):(S_2\times A_{n-2})}(P) = n_C + n_B \tag{7.1}$$

and otherwise

$$R_{(S_2\times S_{n-2}):(S_2\times A_{n-2})}(P) = \sum_{a\in A}\frac{a-1}{2} + \sum_{\{a_1,a_2\}\in A^{\{2\}}}\gcd(a_1,a_2) + n_C. \tag{7.2}$$

7.1 Ramification in Subfields of a $C_2 \times C_2$ Extension

Claim 7.1.1. *Let* $F/\mathbb{C}(t)$ *be a function field extension of degree* n *with Galois closure* Ω *such that* $\mathrm{Gal}(\Omega/\mathbb{C}(t)) = S_n$. *Then* $\Omega^{A_{n-2}}/\Omega^{S_{n-2}\times S_2}$ *is a Galois extension whose Galois group is the Klein group* $C_2 \times C_2$.

Proof of Claim 7.1.1. The subgroup $A_{n-2} \leq S_{n-2} \times S_2$ is a normal subgroup of $S_2 \times S_{n-2}$, and so the degree 4 extension $\Omega^{A_{n-2}}/\Omega^{S_2\times S_{n-2}}$ is Galois. The fact that the Galois group of $\Omega^{A_{n-2}}/\Omega^{S_2\times S_{n-2}}$ is the Klein group $C_2 \times C_2$ follows either by noting that $(S_{n-2} \times S_2)/A_{n-2} \cong C_2 \times C_2$ or by observing the subgroup lattice of $A_{n-2} \lhd S_{n-2} \times S_2$.

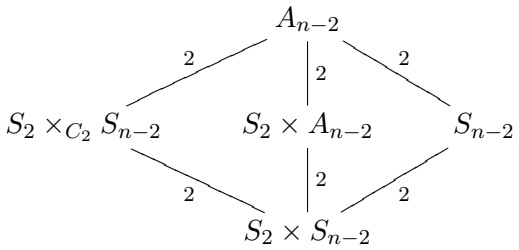


Figure 7.1: Lattice of subgroups of $S_{n-2} \times S_2$ containing A_{n-2}.

Lemma 7.1.2 (Ramification in a $C_2 \times C_2$ Extension)**.** *Let* K'/K *be a Galois extension of function fields over* $\mathbb{C}$ *such that* $\mathrm{Gal}(K'/K) \cong C_2 \times C_2$. *Denote the genera of* K *and* K' *by* g_0 *and* g' *respectively. Denote by* K_1, K_2, K_3 *the three fields fixed by the non-trivial subgroups of* $C_2 \times C_2$ *and let* g_1, g_2, g_3 *be their respective genera. Then every place* P *of* K *is either unramified in all three extensions* K_1, K_2, K_3 *or unramified in exactly one of these three extensions.*

Proof of Lemma 7.1.2. Denote by H_1, H_2, H_3 the subgroups of $C_2\times C_2$ fixing K_1, K_2, K_3 respectively. All subgroups H_i are cyclic of degree 2. Let P be a place of K and $\tilde{P}$ some place of K' lying above P. Since K is a function field over $\mathbb{C}$, the decomposition group $D(\tilde{P}|P)$ must be cyclic, and so $D(\tilde{P}|P) = \{e\}$ or $D(\tilde{P}|P) \cong C_2$. Let H be some subgroup of $C_2 \times C_2$. The ramification index of $\tilde{P}$ over Ω^H is $|H \cap D(\tilde{P}|P)|$. In particular, if $D(\tilde{P}|P) = \{e\}$, then $\tilde{P}$ is unramified over all subfields of K'/K and

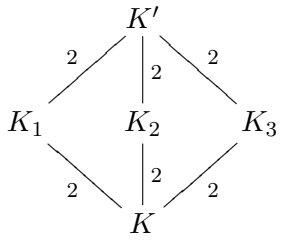


Figure 7.2: Lattice of subfields of a Galois extension K'/K such that $\mathrm{Gal}(K'/K) = C_2 \times C_2$

the place P completely splits in K'. If $D(\tilde{P}|P) \equiv C_2$ then $D(\tilde{P}|P) = H_i$ for some $i \in \{1, 2, 3\}$. Without loss of generality assume $D(\tilde{P}|P) = H_1$. By this assumption, K_1 is the decomposition field of P in Ω, so the place P is unramified in K_1. For the ramification of P in K_2 and K_3, note that $D(\tilde{P}|P) \cap H_2 = D(\tilde{P}|P) \cap H_3 = \{e\}$, and so $\tilde{P}$ is unramified over K_2 and K_3. Since $e(\tilde{P}|P) = 2$, the place P must ramify in K_2 and K_3. ■

Remark. By a theorem of Accola's ([1], Application on page 601) the genera of the subfields of the extension K'/K are related by the equation:

$$g' = g_1 + g_2 + g_3 - 2g_0. \tag{7.3}$$

7.2 Places of $\Omega^{S_{n-2}\times S_2}$, Orbits on Cosets $S_n/(S_{n-2} \times S_2)$, Orbits on 2-sets

The next step towards the proof of Proposition 7.0.2 is to determine when a place $Q \in \Omega^{S_{n-2}\times S_2}$ is ramified in each of the extensions $\Omega^{S_{n-2}\times S_2}$ and $\Omega^{S_{n-2}}$. By Lemma 2.6.1, the ramification type $E_{S_n:S_{n-2}\times S_2}(P)$ can be calculated by examining the orbits of x_P on the cosets $S_n/(S_{n-2} \times S_2)$; in turn, the action of x_P on cosets $S_n/(S_{n-2} \times S_2)$ is equivalent to the action of x_P on 2-sets of $\{1, \ldots, n\}$.

$$\left\{ \begin{array}{c} \text{Places } Q \text{ of} \\ \Omega^{S_{n-2}\times S_2} \text{ lying} \\ \text{above } P \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Orbits of } x_P \text{ on} \\ S_n/(S_{n-2} \times S_2) \end{array} \right\} \tag{7.4}$$

Explicitly, given a place $P \in \mathbb{P}_{\mathbb{C}(t)}$ with places $Q_1, \ldots Q_m$ lying above it in $\Omega^{S_{n-2}\times S_2}$, recall that Lemma 2.6.1 supplies a mapping

$$\varphi : \{Q_1, \ldots Q_m\} \to \mathrm{Orbs}_{D_P}(S_n/(S_{n-2} \times S_2))$$

such that $|\varphi(Q_i)| = e(Q_i|P)$. However, using this lemma for subgroups $H_1 \leq S_{n-2} \times S_2 \leq S_n$ only supplies information on the ramification type $E_{S_n:H_1}(P)$, while here we

are interested in the ramification $E_{(S_{n-2}\times S_2):H_1}(Q)$ for all places Q of $\Omega^{S_{n-2}\times S_2}$ lying above P. The following lemma shows how to derive this information in terms of the orbits of x_P on the cosets $S_n/(S_{S_{n-2}\times S_2})$.

Lemma 7.2.1. *Let $\Omega/\mathbb{C}(t)$ be a Galois extension of function fields with Galois group G. Let $H_1 \lneq H \leq G$ and let Q be a place of Ω^H lying over a place P of $\mathbb{C}(t)$. Write $e(Q|P) = r$ and let φ be as defined in Lemma 2.6.1, also recalled above. The place Q is ramified in Ω^{H_1} if and only if there exists a coset $A \in \varphi(Q)$ and a representative σ of A such that $x_P^r \notin H_1^\sigma$. If $[H : H_1] = 2$ then Q is ramified in Ω^{H_1} if and only if for every representative σ of every coset $A \in \varphi(Q)$, the permutation $x_P^r \notin H_1^\sigma$.*

Proof of Lemma 7.2.1. Let $Q_1', \dots Q_s'$ be the places of Ω^{H_1} lying above P. Apply Lemma 2.6.1 to the extension Ω^H/K to get a mapping

$$\varphi_1 : \{Q_1', \dots, Q_2'\} \to Orbs_{x_P} G/H_1.$$

At least one of the places $Q_1', \dots, Q_s'$ lies above Q, so assume without loss of generality that $Q_1'|Q$, and let σH_1 be some coset in $\varphi_1(Q_1')$. By Lemma 2.6.1, the length of the orbit of x_P on the coset σH_1 is $e(Q_1'|P)$. If for some integer k,

$$x^k \in H_1^\sigma, \tag{7.5}$$

right multiplication by σ gives that $x^k\sigma \in \sigma H_1$, i.e., x^k fixes the coset σH_1. It follows that the integer k divides the length of the orbit of x on σH_1 and so

$$k | e(Q_1'|P).$$

If k is the minimal integer for which (7.5) holds, then $e(Q_1'|P) = k$. Repeating this argument for H gives that r is the minimal integer for which $x^r \in H^\sigma$.

By multiplicativity of the ramification index, $e(Q_1'|Q) = 1$ if and only if $e(Q'|P) = e(Q|P) = r$. By definition, Q is ramified in Ω^{H_1} if and only if $e(Q'|Q) \neq 1$ for some $Q'|Q$. Combining this with previous statements, we get that Q is ramified in Ω^{H_1} if and only if for some $Q'|Q$, the length of the orbit of x_P on some representative of $\varphi_1(Q')$ is not $e(Q|P)$, i.e., $x_P^{e(Q|P)} \notin H_1^\sigma$ for some representative σ of a coset in $\varphi_1(Q')$. By Remark 2, the place $\varphi_1^{-1}(D_P\sigma H)$ lies above Q so $D_P\sigma H$ is some coset in $\varphi(Q)$. This gives the first assertion. If $[H : H_1] = 2$ then the place Q is ramified in Ω^{H_1} if there is a single place Q' of Ω^{H_1} lying above it, so trivially, the place Q is ramified in Ω^{H_1} if and only if for every $Q'|Q$, the ramification index $e(Q'|P) \neq e(Q|P)$, i.e., for every representative σ of every coset A of $\varphi(Q)$,

$$x_P^r \notin H_1^\sigma.$$

. ■

In general, the membership of x_P^r in some subgroup $H \leq G$ might not be easily determined; in our setup, there is extra information that comes from the assumption that $G = S_n$ and H is a subgroup or a conjugate of a subgroup stabilizing some partition of n. This makes it possible to deduce the membership of x_P^r in H from the cycle structure of x.

Recall the following standard definitions: A *partition* of $\{1, \ldots, n\}$ is a set λ of subsets of $\{1, \ldots, n\}$ such that every $i \in \{1, \ldots, n\}$ is contained in exactly one element of λ. If μ and λ are two partitions of $\{1, \ldots n\}$, the partition μ is a *refinement* of λ if every element of μ is a subset of an element of λ, and denote $\mu \leq \lambda$.

Remark. For a permutation $x \in S_n$ presented as a product of disjoint cycles, the sets underlying the cycles form a partition of $\{1, \ldots, n\}$. Denote this partition λ_x. For a partition λ of $\{1, \ldots, n\}$, denote by S_λ the set of elements of S_n fixing the partition λ, that is, S_λ is the set of elements $y \in S_n$ such that for every element $A \in \lambda$, we have $y(A) \subseteq A$. A straighforward check shows that S_λ is a subgroup of S_n and that $x \in S_\lambda$ if and only if $\lambda_x \leq \lambda$.

Remark. If $\sigma \in S_n$ and λ is some partition of $\{1, \ldots, n\}$, then

$$\sigma^{-1}(\lambda) := \{\sigma^{-1}(a) : a \in \lambda\}$$

is a partition of $\{1, \ldots, n\}$ as well, whose stabilizer $S_{\sigma^{-1}(\lambda)}$ is equal to S_λ^σ (The stabilizer subgroup S_λ conjugated by σ).

Proof of Remark 6. For a part $A \subseteq \{1, \ldots, n\}$ and some $x \in S_n$, it holds that $x\sigma^{-1}(A) = \sigma^{-1}(A)$ if and only if $\sigma x \sigma^{-1}(A) = A$. ■

We will say that the *parity* of a partition λ of $\{1, \ldots, n\}$ is *even* if λ has an even number of even parts and *odd* otherwise. (This terminology is not standard and is introduced for the purpose of utility).

Remark. For a permutation $x \in S_n$, the parity of the partition of $\{1, \ldots, n\}$ induced by x is the same as the parity of x. Therefore for a partition λ of $\{1, \ldots, n\}$, it holds that $x \in S_\lambda \cap A_n$ if and only if x is even and $\lambda_x \leq \lambda$.

Combining Lemma 7.2.1 and Remark 7, we determine the ramification of places of $\Omega^{S_{n-2} \times S_2}$ in extensions of $\Omega^{S_{n-2} \times S_2}$ of degree 2:

Claim 7.2.2. *Let Q be a place of $\Omega^{S_{n-2} \times S_2}$ lying over a place P of $\mathbb{C}(t)$. Write $e(Q|P) = r$ and let φ be as defined in Lemma 2.6.1; let $\sigma(S_{n-2} \times S_2)$ be a coset in the orbit $\varphi(Q)$, and let x_P be a branch cycle of P in Ω. Then:*

1. *The place Q is ramified in $\Omega^{S_{n-2}}$ if and only if x_P^r swaps $\sigma(n-1)$ and $\sigma(n)$.*
2. *The place Q is ramified in $\Omega^{S_{n-2} \times_{C_2} S_2}$ if and only if x_P^r is an odd permutation.*

Proof of Claim 7.2.2. By Lemma 2.6.1, $r = e(Q|P)$ is the length of the orbit of x_P on $\sigma S_{n-2} \times S_2$, so:

$$x_P^r \sigma(S_{n-2} \times S_2) = \sigma(S_{n-2} \times S_2),$$

i.e.,

$$x_P^r \in (S_{n-2} \times S_2)^\sigma.$$

By Remark 5, the partition of $\{1, \ldots, n\}$ induced by x_P^r is a refinement of the partition $\{\{\sigma(1), \ldots, \sigma(n-2)\}, \{\sigma(n-1), \sigma(n)\}\}$. In particular x_P^r fixes $\{\sigma(n-1), \sigma^(n)\}$ setwise. By Remark 5, the permutation x_P^r fixes the 2-set $\{\sigma(n-1), \sigma(n)\}$ pointwise if and only if $x_P^r \in S_{n-2}^\sigma$. Take Lemma 7.2.1 with $H = S_{n-2} \times S_2$ and $H_1 = S_{n-2}$. Then Q is ramified in Ω^{H_1} if and only if for some σ of some coset in $\varphi(Q)$, it holds that $x_P^r \notin (S_{n-2})^\sigma$. By the previous argument this occurs if and only if x_P^r transposes $\sigma(n-1)$ and $\sigma(n)$. This gives assertion 1. Now take $H = S_{n-2} \times S_2$ and $H_1 = S_{n-2} \times_{C_2} S_2$. By Lemma 7.2.1, the place Q is ramified in Ω^{H_1} if and only if $x_P^r \notin (\Omega^{S_{n-2} \times_{C_2} S_2})^\sigma$ for some choice of representative σ of some coset in $\varphi(Q)$; By Remark 7, it holds that $x_P^r \in (\Omega^{S_{n-2} \times_{C_2} S_2})^\sigma$ if and only if x^r is even and $\lambda_{x^r} \in (S_{n-2} \times S_2)^\sigma$. As the latter condition holds by assumption, we get that $x^r \notin (S_{n-2} \times_{C_2} S_2)^\sigma$ if and only if x^r is odd. This gives assertion 2. ■

Remark. The second assertion of Claim 7.2.2 remains true if $S_{n-2} \times S_2$ is replaced by any partition stabilizer $S_\lambda \leq S_n$ and $S_{n-2} \times_{C_2} S_2$ is replaced by $S_\lambda \cap A_n$.

7.3 Counting Orbits of x on 2-sets

In the previous section, orbits of x_P on both the cosets $S_n/(S_{n-2} \times S_2)$ and the cosets S_n/H_1 for $H_1 \leq S_{n-2} \times S_2$ were examined directly by taking representatives. However, when only orbits on $S_n/(S_{n-2} \times S_2)$ are of interest, there is a simpler way to calculate the orbits of x_P, by noting that the action of x_P on cosets $S_n/(S_{n-2} \times S_2)$ is equivalent to the action of x_P on $\{1, \ldots, n\}^{\{2\}}$ via the mapping $\psi : \sigma \to \{\sigma(n-1), \sigma(n)\}$. It is easily verified that ψ is well defined on the cosets $S_n/(S_{n-2} \times S_2)$ and that for any $x, \sigma \in S_n$,

$$\psi(x\sigma) = x(\psi\sigma),$$

that is, ψ gives an isomorphisn of S_n-sets. The correspondence 7.4 is now extended as follows:

$$\left\{ \begin{array}{c} \text{Places } Q \text{ of} \\ \Omega^{S_{n-2} \times S_2} \text{ lying} \\ \text{above } P \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Orbits of } x_P \text{ on} \\ S_n/(S_{n-2} \times S_2) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Orbits of } D_P \text{ on} \\ \text{2-sets of} \\ \{1, \ldots, n\} \end{array} \right\} \tag{7.6}$$

The number of orbits of x_P on 2-sets of $\{1, \ldots, n\}$ and the size of these orbits are calculated using Lemma 7.3.4; By Lemma 2.6.1, this calculation gives the number

of places of $\Omega^{S_{n-2}\times S_2}$ lying above P and their ramification over P. For the proof of Proposition 7.0.2, the number of places of $\Omega^{S_{n-2}\times S_2}$ ramified in $\Omega^{A_{n-2}\times S_2}$ is determined by enumerating the orbits of x_P on 2-sets using Lemma 7.3.4, but taking into account only the orbits which correspond to places of $\Omega^{S_{n-2}\times S_2}$ ramified in $\Omega^{A_{n-2}\times S_2}$ by Claims 7.2.2 and 7.1.1 and Lemma 7.1.2.

The following labelling of types orbits on 2-sets reflects the criteria for ramification given in Claim 7.2.2. These labels will be used in the proof of Proposition 7.0.2 when enumerating the orbits of x_P, and the remaining definitions and lemmas in this section supply the technical framework for this enumeration.

Definition 7.3.1. Let x be a permutation on n elements, and let $C_1, \ldots, C_m$ be the orbits of x on $\{1, \ldots, n\}$.

1. An orbit O on $\{1, \ldots, n\}^{\{2\}}$ is of *type A* if it is contained in $C^{\{2\}}$ and C is of odd size.

2. An orbit O on $\{1, \ldots, n\}^{\{2\}}$ is of *type* B_1 if it is contained in $C^{\{2\}}$ and C is of even size ℓ such that $\ell \equiv 2 \mod 4$ and $x^{\ell/2}$ transposes every 2-set of O.

3. An orbit O on $\{1, \ldots, n\}^{\{2\}}$ is of *type* B_2 if it is contained in $C^{\{2\}}$ where C is of even size ℓ such that $\ell \equiv 2 \mod 4$ and $x^{\ell/2}$ does not transpose any 2-set of O.

4. An orbit O on $\{1, \ldots, n\}^{\{2\}}$ is of *type* C_1 if it is contained in $C^{\{2\}}$ where C is of even size ℓ such that $\ell \equiv 0 \mod 4$ and $x^{\ell/2}$ transposes every 2-set of O.

5. An orbit O on $\{1, \ldots, n\}^{\{2\}}$ is of *type* C_2 if it is contained in $C^{\{2\}}$ where C is of even size ℓ such that $\ell \equiv 0 \mod 4$ and $x^{\ell/2}$ does not transpose any 2-set of O.

6. An orbit O on $\{1, \ldots, n\}^{\{2\}}$ is of *type* $D_{\alpha,\beta}$ where $\alpha, \beta \in \{\text{odd}, \text{even}\}$, if it is contained in ${C_1}^{\{1\}} \cup {C_2}^{\{1\}}$ where $C_1 \neq C_2$ are different orbits of x on $\{1, \ldots, n\}$ and the parities of C_1 and C_2 are α and β respectively.

Definition 7.3.2. Let x be a permutation on n elements, and let O be an orbit of x on the cosets $S_n/(S_{n-2} \times S_2)$. The orbit O is of type A, B_1,B_2, C_1, C_2 or $D_{\alpha,\beta}$ if the corresponding orbit of x on $\{1, \ldots, n\}^{\{2\}}$ under (7.6) is of type A, B_1,B_2, C_1, C_2 or $D_{\alpha,\beta}$ respectively.

The following lemma shows that the types C_1,C_2,B_1 and B_2 "cover" all the orbits of x on $C^{\{2\}}$ when C is of even length.

Lemma 7.3.3. *Suppose O is an orbit of x on $\{1, \ldots, n\}^{\{2\}}$ such that x^ℓ transposes some 2-set in O. Then:*

1. *$O \subseteq C^{\{2\}}$, where C is an orbit of x of length 2ℓ.*

2. *x^ℓ transposes every 2-set in O.*

3. $|O| = \ell$.

Furthermore, if y is a permutation that has an orbit of even length 2ℓ, there exists a 2-set of $\{1, \ldots, n\}$ that is transposed by y^ℓ.

Proof of Lemma 7.3.3. Suppose that x^ℓ transposes i and j, where $\{i, j\} \in O$. Then i and j are contained in the same cycle c of x, and $c^\ell(i) = j$. In particular, the cycle $c^{2\ell}$ fixes i, so $c^{2\ell} = Id_C$, where C is the orbit of x on $\{1, \ldots, n\}$ underlying the cycle c. Since $c^\ell \neq Id_C$, it follows that the cycle c is of order exactly 2ℓ. This gives the first assertion.

For the second assertion, note that any 2-set in the orbit of x on $\{i, j\}$ is of the form $\{x^k(i), x^k(j)\}$. The permutation x^ℓ transposes this 2-set since $x^\ell(x^k(i)) = x^k(x^\ell(i)) = x^k(j)$.

For the third assertion, write c in cycle notation:

$$c = (c_1 = i, c_2, \ldots, c_\ell = j, c_{\ell+1}, \ldots, c_{2\ell})$$

it is clear that the sets $\{c_i, c_{\ell+i}\}, i = 1, \ldots \ell$ are distinct 2-sets that form the orbit O. We further see that if y is a permutation that contains c as a cycle (i.e., y has an orbit of even length), there exists a 2-set that is transposed by y^ℓ. ■

The following lemma from [16] gives the number of orbits of x on 2-sets and their size by the type of the orbit. Its use in [16] was to calculate the ramification type of the extension $\Omega^{S_{n-2}}/\mathbb{C}(t)$ from the ramification type of $\Omega^{S_{n-2}}/\mathbb{C}(t)$. In the proof of 7.0.2, this lemma will be used to enumerate the places of $\Omega^{S_{n-2} \times S_2}$ as well, but only places that are ramified in $\Omega^{A_{n-2} \times S_2}$ will be taken into account. The lemma is stated as it is given in [16] with minor changes to adapt the conventions of the notation, and with the labels of the orbit types from Definition 7.3.1 added in parenthesis.

Lemma 7.3.4. *([16], Lemma* 4.1*)*

Let $C_1, C_2 \subseteq \{1, \ldots, n\}$ be orbits of $x \in S_n$ having cardinalities r_1, r_2, respectively. Then the orbits of the action of x on ${C_1}^{\{1\}} \cup {C_2}^{\{2\}}$ consist of:

1. *(r_1, r_2) orbits on ${C_1}^{\{1\}} \cup {C_2}^{\{1\}}$ of cardinality $\mathrm{lcm}(r_1, r_2)$ if $C_1 \neq C_2$ (Orbits of type $D_{\alpha,\beta}$);*
2. *$\frac{r_1 - 1}{2}$ orbits of cardinality r_1 if $C_1 = C_2$ and r_1 is odd (Orbits of type A);*
3. *one orbit of cardinality $\frac{r_1}{2}$ and $\frac{r_1}{2} - 1$ orbits of cardinality r_1 if $C_1 = C_2$ and r_1 is even (Orbits of type B_1, B_2, C_1 and C_2).*

Remark. In Case 3, by Lemma 7.3.3 there exists an orbit of x on ${C_1}^{\{2\}}$ such that x transposes an element in this orbit, and it is of cardinality $\frac{r_1}{2}$. Therefore the single orbit of cardinality $\frac{r_1}{2}$ is of type B_1 or C_1, and the remaining orbits of cardinality r_1 are of type B_2 or C_2, where the distiction between B_i and C_i depends on the value of $r_1 \mod 4$.

Proof of Proposition 7.0.2. Let $Q_1, \dots Q_r$ be the places of $\Omega^{S_{n-2}\times S_2}$ lying over P. Let φ be as in Lemma 2.6.1. Since $[(S_{n-2} \times S_2) : (S_{n-2} \times_{C_2} S_2)] = 2$, the contribution $R_{(S_{n-2}\times S_2):(S_{n-2}\times_{C_2} S_2)}(P)$ is the number of places $Q_i|P$ that are ramified in $\Omega^{S_{n-2}\times_{C_2} S_2}$. By Claim 7.1.1 and Lemma 7.1.2, a place $Q \in \Omega^{S_{n-2}\times S_2}$ is ramified in $\Omega^{A_{n-2}\times S_2}$ if and only if it is ramified in exactly one of $\Omega^{S_{n-2}}$ and $\Omega^{S_{n-2}\times_{C_2} S_2}$. Let σ be some representative of a coset in $\varphi(Q)$, and write $r = e(Q|P)$. Since $[(S_{n-2} \times S_2) : S_{n-2}] = 2$ and $[(S_{n-2} \times S_2) : (S_{n-2} \times_{C_2} S_2)] = 2$, by Claim 7.2.2:

1. The place Q is ramified in $\Omega^{S_{n-2}}$ but not in $\Omega^{S_{n-2}\times_{C_2} S_2}$ if and only if x^r transposes $\sigma(n-1)$ and $\sigma(n)$, and x^r is even.

2. The place Q is ramified in $\Omega^{S_{n-2}\times_{C_2} S_2}$ but not in $\Omega^{S_{n-2}}$ if and only if $\sigma(n-1)$ and $\sigma(n)$ are not transposed by x and x^r is odd.

The following tables classy the orbits of x on $\{1, \dots, n\}^{\{2\}}$ based on the parity of x and the orbits' fulfilment of the following statements:

1. x transposes a 2-set in O.

2. the parity of $x^{|O|}$ is odd.

By Lemma 7.3.3, the permutation $x^{|O|}$ transposes an element of O if and only if O is of type B_1 or C_1. Given the type of O, the parity of the integer $|O|$ is given by Lemma 7.3.4.

First, assume that x is odd. Then the parity of the permutation $x^{|O|}$ is the parity of the integer $|O|$ and so:

	$x^{\|O\|}$ odd	$x^{\|O\|}$ even
$x^{\|O\|}$ transposes an element of O	B_1	C_1
$x^{\|O\|}$ does not transpose an element of $\|O\|$	$D_{odd,odd}$,A	$D_{even,odd}$, $D_{even,even}$, B_2, C_2

It is apparent that a place Q fulfills conditions 1 or 2 if and only if the corresponding orbit $\varphi(Q)$ is of type C_1, $D_{odd,odd}$ or A. By Lemma 7.3.4, the permutation x has:

$$\sum_{i=1}^{n_A} \frac{a_i - 1}{2} + \sum_{i<j}^{n_A} (a_i, a_j) + n_C \tag{7.7}$$

orbits of these types on 2-sets. Therefore, if x is odd, the contribution $R_{S_{n-2}\times S_2:A_{n-2}\times S_2}(P)$ is equal to (7.7), as required.

Next, suppose x is even. Then $x^{|O|}$ is even regardless of the value of $|O|$.

	$x^{\|O\|}$ odd	$x^{\|O\|}$ even
$x^{\|O\|}$ transposes an element of O	-	C_1, B_1
$x^{\|O\|}$ does not transpose an element of $\|O\|$	-	everything but C_1 and B_1

■

It is apparent that a place Q fulfills conditions 1 or 2 hold if and only if the corresponding orbit $\varphi(Q)$ is of type C_1 or B_1. By lemma 7.3.4 there are

$$n_B + n_C \tag{7.8}$$

such orbits of x on 2-sets of $\{1, \ldots, n\}^{\{2\}}$ and therefore the contribution $R_{(S_{n-2}\times S_2):(A_{n-2}\times S_2)}(P)$ is equal to (7.8), as required.

Chapter 8

The case $A_{n-2} \times S_2$: Calculations

Proof of Proposition 7.0.1. Since $A_{n-2} \times S_2 \leq S_{n-2} \times S_2$, it holds that

$$g_{S_{n-2}\times S_2} \leq g_{A_{n-2}\times S_2}.$$

Therefore a necessary condition for $g_{A_{n-2}\times S_2} \leq 1$ is that $g_{S_{n-2}\times S_2} \leq 1$ as well. By [16], Theorem 1.2, the subfield $\Omega^{S_{n-2}\times S_2}$ is of genus ≤ 1 if and only if the ramification type of $F/\mathbb{C}(t)$ appears in Table A.1, in which case $g_{S_{n-2}\times S_2} = 0$.

It remains to determine for which of the entries of Table A.1, the genus $g_{A_{n-2}} \leq 1$ in the resulting Galois extension. For the remainder of the proof, we go over the entries of Table A.1 and for each one, either calculate the genus of $\Omega^{A_{n-2}\times S_2}$ or show that it must be strictly larger than 1.

For each entry $\mathcal{E} = \mathcal{E}(n)$ of Table A.1, denote by G the Galois group of a minimal extension $F/\mathbb{C}(t)$ with ramification type $\mathcal{E}$, viewed as a permutation group on n elements. The resulting group G may be either S_n or A_n, depending on the value of n taken. An entry $\mathcal{E}$ *admits* $A_{n-2} \times S_2$ of genus 0 or 1 if for a function field $F/\mathbb{C}(t)$ with Galois closure Ω such that the ramification type of $F/\mathbb{C}(t)$ is $\mathcal{E}$, we have $\mathrm{Gal}(\Omega/\mathbb{C}(t)) = S_n$ and $g_{A_{n-2}\times S_n}$ is 0 or 1. Otherwise the entry is *eliminated*. A ramification type is *of the form* $[-, a*]$ if the number of entries a is dependent on n and larger than $\frac{n-7}{2}$, and the number of remaining entries of E is not dependent on n. For example, $[1, 2^{\frac{n-4}{2}}, 3]$ is of form $[-, 2*]$ and $[2, 3, 6^{\frac{n-5}{6}}]$ is of form $[-, 6*]$. A ramification type is *odd* if it contains an odd number of even entries, and *even* otherwise.

Remark. In a Galois extension $\Omega/\mathbb{C}(t)$ such that $\mathrm{Gal}(\Omega/\mathbb{C}(t)) = S_n$, by Lemma 2.6.1, the ramification type $E_{\Omega^{S_{n-1}}/\mathbb{C}(t)}(P)$ is the set of orbit lengths of the branch cycle x_P in its action on S_n/S_{n-1}, i.e., the set of cycle lengths of x_P. Therefore $E_{\Omega^{S_{n-1}}/\mathbb{C}(t)}(P)$ is an odd ramification type if and only if the corresponding branch cyle x_P is an odd permutation.

Claim 8.0.1 (Rules of thumb for eliminating entries)**.** *Let $\mathcal{E} = [E_1, \ldots, E_k]$ be an entry of Table A.1. Then:*

1. *Either two types of $\mathcal{E}$ are odd, four types of $\mathcal{E}$ are odd, or $\mathcal{E}$ is eliminated.*

2. *If $\mathcal{E}$ contains $[1^{n-2}, 2]$, $\mathcal{E}$ is eliminated.*

3. *If $\mathcal{E}$ contains a type of the form $[-, 4*]$, then $\mathcal{E}$ is eliminated.*

4. *If $\mathcal{E}$ contains an even type of the form $[-, 2*]$ then $\mathcal{E}$ is eliminated.*

Proof of Claim 8.0.1. For 1, note that by Remark 10 if all types in $\mathcal{E}$ are even then all branch cycles of $\Omega/\mathbb{C}(t)$ are even and therefore the resulting Galois group G must be A_n, in which case $\mathcal{E}$ is eliminated. Else, $G = S_n$. Take the Riemann-Hurwitz formula for the extension $\Omega^{A_n}/\mathbb{C}(t)$:

$$2g_{A_n} = -4 + \sum_{P \in \mathbb{P}_{\mathbb{C}(t)}} R_{S_n:A_n}(P)$$

. Clearly $\sum_{P \in \mathbb{P}_{\mathbb{C}(t)}} R_{S_n:A_n}(P)$ must be even. We claim that $\sum_{P \in \mathbb{P}_{\mathbb{C}(t)}} R_{S_n:A_n}(P)$ is the number of odd types in $\mathcal{E}$: A place P of $\mathbb{C}(t)$ contributes to this sum if and only if it is ramified in Ω^{A_n}, which occurs if and only if the branch cycle x_P is an odd permutation. Since $E_{F/\mathbb{C}(t)}(P)$ is also the cycle structure of x_P, the place P is ramified in Ω^{A_n} if and only if $E_{F/\mathbb{C}(t)}(P)$ is odd. Therefore $\sum_{P \in \mathbb{P}_{\mathbb{C}(t)}} R_{S_n:A_n}(P)$ is equals to the number of odd types $\mathcal{E}$. Each entry of Table A.1 contains at most five ramification types, and so if the number of odd types in $\mathcal{E}$ is even and greater than 0, then $\mathcal{E}$ contains two or four odd types.

For assertions 2, 3 and 4 write the Riemann-Hurwitz formula for the extension $\Omega^{A_{n-2}\times S_2}/\Omega^{S_{n-2}\times S_2}$, taking into account that $g_{S_{n_2}\times S_2} = 0$:

$$2g_{A_{n-2}\times S_2} - 2 = -4 + \sum_{P \in \mathbb{P}_{\mathbb{C}(t)}} R_{S_{n-2}\times S_2:A_{n-2}\times S_2}(P). \tag{8.1}$$

Since each contribution $R_{S_{n-2}\times S_2:A_{n-2}\times S_2}(P)$ is nonnegative, it suffices to show that for some $P \in \mathbb{P}_{\mathbb{C}(t)}$, the contribution $R_{S_{n-2}\times S_2:A_{n-2}\times S_2}(P) \geq 5$, because then bounding the right hand side of (8.1) from below gives:

$$2g_{A_{n-2}\times S_2} \geq -4 + 2 + 5 = 3, \tag{8.2}$$

that is, $g_{A_{n-1}\times S_2} \geq 3/2$. Since $g_{A_{n-2}\times S_2}$ is an integer, necessarily $g_{A_{n-2}\times S_2} \geq 2$.

If $E_{F/\mathbb{C}(t)}(P) = [1^{n-2}, 2]$, then $E_{F/\mathbb{C}(t)}(P)$ is an odd ramification type and so by Proposition 7.0.2, $R_{S_{n-2}\times S_2:A_{n-2}\times S_2}(P) = \binom{n-2}{2}$. Since $n > N_0 > 3$, the expression $n(n-1)/2 \geq 5$, so $g_{A_{n-2}\times S_2} \geq 2$ and $\mathcal{E}$ is eliminated.

If $E_{F/\mathbb{C}(t)}(P)$ is of the form $[-, 4*]$, by Proposition 7.0.2 the contribution $R_{S_{n-2}\times S_2:A_{n-2}\times S_2}(P)$ is greater than the number of entries 4 in $E_{F/\mathbb{C}(t)}(P)$ (regardless of the parity of $E_{F/\mathbb{C}(t)}(P)$). By definition, the number of entries 4 in E_P is larger than $\frac{n-7}{2} > \frac{N_0-7}{2} \geq 5$, and so $\mathcal{E}$ is eliminated in this case as well.

If $E_{F/\mathbb{C}(t)}(P)$ is of the form $[-, 2*]$ and $E_{F/\mathbb{C}(t)}(P)$ is even, then by Proposition 7.0.2, the contribution $R_{S_{n-2}\times S_2:A_{n-2}\times S_2}(P)$ is greater than the number of even entries in $E_{F/\mathbb{C}(t)}(P)$, which again is by definition larger than $\frac{n-7}{2} > \frac{N_0-7}{2} \geq 5$, and $\mathcal{E}$ is eliminated.

We now go over Table A.1, and for each entry, eliminate it or calculate $g_{A_{n-2}\times S_2}$ using Proposition 7.0.2.

I2.1-I2.8: Entries I2.1 and I2.2 are eliminated since they contain $[1^{n-2}, 2]$. Each of the remaining entries contains exactly three ramification types, where one type is $[n]$ and the other types are of the form $[-, 2*]$. If n is an even integer, $[n]$ is odd, and by Claim 8.0.1, assertion 1, the entry must have exactly one odd type apart from $[n]$. The remaining type is an even type of the form $[-, 2*]$, so the entry is eliminated by 8.0.1, assertion 4. This argumet eliminates entries I2.4, I2.7. For the remaining entries, n is an odd integer and so $[n]$ is an even ramification type. The other two types are of the form $[-, 2*]$, and by Claim 8.0.1, assertion 1, these two types are of the same parity. For values of n where these two types are even, the entry is eliminated; else, direct calculation shows that $g_{S_2\times A_{n-2}}$ is of genus 1:

$I2.3$	$[n], [1^3, 2^{\frac{n-3}{2}}], [2^{\frac{n-3}{2}}, 3]$	$g = 1$	$n \equiv 1 \mod 4$
$I2.5$	$[n], \left[1, 2^{(n-1)/2}\right], [1^2, 2^{(n-5)/2}, 3]$	$g = 1$	$n \equiv 3 \mod 4$
$I2.6$	$[n], \left[1^3, 2^{(n-3)/2}\right], [1, 2^{(n-5)/2}, 4]$	$g = 1$	$n \equiv 1 \mod 4$
$I2.8$	$[n], \left[1, 2^{(n-1)/2}\right], [1^3, 2^{(n-7)/2}, 4]$	$g = 1$	$n \equiv n \equiv 3 \mod 4$

I2.9-I2.15 Entries I2.1 and I2.2 are eliminated since they contain $[1^{n-2}, 2]$. Each of the remaining entries contains exactly three ramification types, one of which is $[a, n-a]$ and the other two are of the form $[-, 2*]$.

If n is an odd integer then $[a, n-a]$ is an odd ramification; By Claim 8.0.1, assertion 1, exactly one of the remaining types is even. This type is of the form $[-, 2*]$ and so by Claim 8.0.1, assertion 4, the entry is eliminated. This argument eliminates entries I2.12 and I2.14. If n is an even integer, then the two types apart from $[a, n-a]$ are of the same parity. For values of n where this parity is even, the entry is eliminated by Claim 8.0.1, assertion 1. Else, direct calculation shows that $g_{A_{n-2}\times S_2}$ is of genus 0:

$I2.11$	$[a, n-a], \left[2^{n/2}\right], [1^2, 2^{(n-6)/2}, 4]$	0	$n \equiv 2 \mod 4$
$I2.13$	$[a, n-a], \left[1^2, 2^{(n-2)/2}\right], [2^{(n-4)/2}, 4]$	0	$n \equiv 0 \mod 4$
$I2.15$	$[a, n-a], \left[2^{n/2}\right], [1, 2^{(n-4)/2}, 3]$	0	$n \equiv 2 \mod 4$

F1.1-F1.9 Entries $F1.1$ and $F1.2$ are eliminated since they contain $[1^{n-2}, 2]$. Each remaining entry contains four types of the form $[-, 2^*]$. By Claim 8.0.1, assertion 1, each entry is either eliminated or has 2 or 4 odd types. $G = A_n$. For entries where there are exactly two odd types, the remaining types are even types of the form $[-, 2^*]]$ and so they are eliminated. This argument eliminates entries F1.3, F1.4,F1.6,F1.7. For

the remaining entries, either all types are odd or all types are even, depending on the value of the integer n. In the latter case, the entry is eliminated. In the former case, direct calculation shows that $g_{A_{n-2}\times S_2}$ is of genus 1:

$F1.5$	$\left[1^2, 2^{(n-5)/2}, 3\right], [1, 2^{(n-1)/2}]$ thrice	1	$n \equiv 3 \mod 4$
$F1.8$	$\left[1^3, 2^{(n-7)/2}, 4\right], [1, 2^{(n-1)/2}]$ thrice	1	$n \equiv 3 \mod 4$
$F1.9$	$\left[2^{(n-4)/2}, 4\right], [1^2, 2^{(n-2)/2}]$ thrice	1	$n \equiv 0 \mod 4$

F3.1-F3.3 All entries are eliminated as they contain $[-, 4^*]$.

F4.1-F4.6 All entries are of the form $[-, 2*], [-, 3*], [-, 6*]$. Since 3 is an odd integer, the parity of the type $[-, 3*]$ does not depend on n. If the $[-, 3*]$ type is odd, then exactly one of $[-, 2*]$ and $[-, 6*]$ is even and the entry is eliminated. This argument rules out entries F4.1,F4.2,F4.4,F4.6. If the type $[-, 3*]$ is even and the other two types $[-, 2*]$ and $[-, 6*]$ are even, then the entry is eliminated. If the type $[-, 3*]$ is even and the other two types are odd, direct calculation shows that $g_{A_{n-2}\times S_2} = 0$.

$F4.3$	$\left[1, 2^{(n-1)/2}\right], [1, 3^{(n-1)/3}], [3, 4, 6^{(n-7)/6}]$	0	$n \equiv 7 \mod 12$
$F4.5$	$\left[1^2, 2^{(n-2)/2}\right], [1, 3^{(n-1)/3}], [4, 6^{(n-4)/6}]$	0	$n \equiv 4 \mod 12$

The ramification types for which $g_{A_{n-2}\times S_2}$ is of genus 0 or 1 are summarized in Tables A.2 and A.3. ■

Chapter 9

Ramification Criteria for Fixed Fields of Genus 0 and 1

The following theorem summarizes the results of Chapters 6 and 7, in regard to determining which of the possibilities listed in Theorem 3.1 in fact occurs.

Proposition 9.0.1. *Let $\Omega/\mathbb{C}(t)$ be a Galois extension with Galois group G, where $G = S_n$ or A_n and $n > N_0$. Let F be the subfield of Ω fixed by a point stabilizer of G and assume that the ramification type $\mathcal{E}$ of $F/\mathbb{C}(t)$ is listed in Table A.1.*

If $G = A_n$ then:

1. *The fields fixed by stabilizers of points or 2-sets, i.e., $S_{n-2} \times_{C_2} S_2$ and A_{n-1}, are of genus 0.*

2. *The field fixed by A_{n-2} is of genus strictly greater than 1.*

If $G = S_n$ then:

1. *The fields fixed by stabilizers of points or 2-sets, that is, by $S_{n-2} \times S_2$ and S_{n-1}, are of genus 0.*

2. *The field fixed by A_n is of genus 0 if and only if exactly two cycle types in $\mathcal{E}$ are odd, and of genus 1 if and only if exactly four cycle types in $\mathcal{E}$ are odd.*

3. *The field fixed by A_{n-1} is of genus 0 if and only if the total number of odd entries in $\mathcal{E}$ is 2, and of genus 1 if and only if the total number of odd entries in $\mathcal{E}$ is 4.*

4. *The field fixed by S_{n-2} is either of genus 0 or of genus strictly greater than 1. It is of genus 0 if and only if*

$$\mathcal{E} = [n][a, n-a][2, 1^{n-2}]$$

for an even value of n (Type I1.1 in Table A.1).

5. *Table A.2 contains the types $\mathcal{E}$ for which the field fixed by $A_{n-2} \times S_2$ is of genus 0.*

6. *Table A.3 contains the types $\mathcal{E}$ for which the field fixed by $A_{n-2} \times S_2$ is of genus 1.*

7. *The field fixed by $S_{n-2} \times_{C_2} S_2$ is of genus 0 if and only if*

$$\mathcal{E} = [1, 2^{\frac{n-1}{2}}], [1, 4^{\frac{n-1}{4}}], [2, 3, 4^{\frac{n-5}{4}}]$$

for $n \equiv 5 \mod 8$ (Type F3.2 in Table A.1). If it is not of genus 0, it is of genus strictly greater than 1.

Remark. The criteria for the genus of the subfields fixed by A_n and A_{n-1} (items 2 and 3) inside a symmetric extension hold without the assumption that $\mathcal{E}$ is one of the exceptional types in Table A.1.

Proof of Proposition 9.0.1. **Stabilizers of points and 2-sets:** By [16], Section 4, the fields fixed by one-point and 2-set stabilizers in function field extensions with ramification types appearing in Table A.1 are of genus 0 (Case 1 for $G = A_n$ and $G = S_n$).

Pointwise stabilizers of 2-sets: Denote by F_2 the subfield of Ω fixed by a 2-set stabilizer of G and by F_2' the subfield of Ω fixed by a 2-point stabilizer. Since $[F_2' : F_2] = 2$, in order for F_2' to be of genus 0 (respectively, 1), exactly two (respectively, four) places of F_2 must be ramified in F_2'. By [16], Proposition 5.1, the number of ramified places in this extension is the total number of even entries in $\mathcal{E}$. By directly checking the entries of Table A.1, this condition occurs in the single case $I1.1$ $[n], [a, n-a], [1^{n-2}, 2]$ for n odd, in which there are two even entries in the ramification type and $G = S_n$; In all other cases, there are more than five even entries and so the genus of F_2' is strictly greater than 1. Table A.1 contains no type where $G = A_n$ with a total of two or four even entries, $\Omega^{A_{n-2}}$ never occurs 0 or 1 (Case 4 for $G = A_n$ and $G = S_n$).

Remaining cases: The criteria for case 3 is given in Corollary 6.4, and case 7 is shown in Theorems 6.1 and 6.2. Cases 5 and 6 are shown in Proposition 7.0.1.

Chapter 10

Conclusion and Consequences

The main object of the previous chapters was the proof of Theorem 1.1. This theorem classifies the subgroups of a symmetric or alternating extension $\Omega/\mathbb{C}(t)$ of large enough degree n that fix subfields of genus 0 or 1. It was shown that such a subgroup must be, except for a finite list of cases, the symmetric or alternating group of degree n or a point stabilizer of this group; for the exceptional case, the subgroup fixing a 2-set of $\{1, \ldots, n\}$ and its subgroups of index 2 may also fix a field of genus 0 or 1, and tools were provided to determine the genus of the resulting subfield. In particular it was shown that in any given symmetric or alternating extension of large enough degree, there are at most three maximal non-isomorphic, non-trivial subfields of genus 0 or 1. The following sections will consider some applications of these results.

10.0.1 Consequences: Specializations of Polynomials

This section concerns some applications of the classification given in Theorem 1.1 relating to the study of specializations of a bivariate polynomial $f(x,t) \in \mathbb{Q}[x,t]$. In particular, a proof will be given for Theorem 1.2 stated in the introduction. The key to the applications shown in this chapter is that they involve a setup in which a subfield of a symmetric or alternating extension has infinitely many rational places; Via Faltings' theorem, such subfields are of genus 0 or 1, and thus the characterization of subfields of genus 0 and 1 given in Theorem 1.1 comes into play.

10.1 Hilbert's Irreducibility Theorem

The topic of specializations is closely related to Hilbert's irreducibility theorem, which asserts that given an irreducible bivariate polynomial $f(x,t) \in \mathbb{Q}[x,t]$, there are infinitely many rationals $t_0 \in \mathbb{Q}$ such that $f(x,t_0) \in \mathbb{Q}[x]$ is irreducible. This result is classically used to reduce the problem of realizing a group G over $\mathbb{Q}$ to that of realizing G over $\mathbb{Q}(t)$. However, given a polynomial $f(x,t) \in \mathbb{Q}[x]$ whose Galois group over $\mathbb{Q}(t)$ is G, not all specializations t_0 will yield G as the Galois group of $f(x,t_0)$ over $\mathbb{Q}$, or even yield an irreducible polynomial (For some examples, see [10], Sections 4.2 and

4.3). Given a polynomial p over a field $\mathbb{K}$, denote by $\mathrm{Gal}(p, \mathbb{K})$ the Galois group of p over $\mathbb{K}$. We may ask the following two questions:

Question 10.1.1. If $G = \mathrm{Gal}(f(x,t), \mathbb{Q}(t))$, what subgroups $H \leq G$ appear as $\mathrm{Gal}(f(x,t_0), \mathbb{Q})$ for infinitely many specializations $t_0 \in \mathbb{Q}$?

Question 10.1.2. Given an irreducible polynomial $f(x,t) \in \mathbb{Q}[x,t]$ with infinitely many "bad" specializations (the resulting polynomial is reducible), describe the set of specializations $t_0 \in \mathbb{Q}$ such that $f(x,t_0) \in \mathbb{Q}$ is reducible.

Theorem 1.2 answers Question 10.1.1 for an irreducible polynomial $f(x,t) \in \mathbb{Q}[x,t]$ such that $\mathrm{Gal}(f, \mathbb{Q}(t))$ is the symmetric or alternating group on $n > N$ elements.

Regarding Question 10.1.2, another statement of Hilbert's irreducibility theorem is that there exist finitely many bivariate polynomials $g_i \in \mathbb{Q}[x,t]$, $i = 1, \dots m$ such that Red_f is contained (up to a finite set) in a union of the form:

$$\bigcup_{i=1}^{m} \{t_0 \in \mathbb{Q} : g_i(x,t_0) \text{ has a rational root}\}. \tag{10.1}$$

The sets that appear in the union in the equation (10.1) are called *thin sets* in the sense of Serre (see [18] for more information). The following result restricts the number of polynomials g_i that must be considered:

Theorem 10.1. *Let $f \in \mathbb{Q}[x,t]$ be an irreducible polynomial with geometric monodromy group S_n or A_n such that $n > N$. There exists $m \leq 3$ polynomials $g_i \in \mathbb{Q}[x,t]$, $i \in \{1, \dots, m\}$ such that Red_f differs by a finite set from the set*

$$\bigcup_{i=1}^{m} \{t_0 \in \mathbb{Q} : g_i(x,t_0) \textit{ has a rational root}\}. \tag{10.2}$$

Denote the splitting field of f by Ω and the geometric monodromy group of f by G. If the ramification type of $(\Omega\bar{Q})^{S_{n-1}\cap G}/\mathbb{Q}(t)$ is not in the list of exceptions in Table A.1, then $m \leq 2$.

Definitions and Notation

The places of the rational function field $\mathbb{Q}(t)$ are in a one-to-one correspondence with $\mathbb{Q} \cup \{\infty\}$ ([20], Corollary 1.2.3, this holds for any rational function field). For an element $s \in \mathbb{Q}$, denote by P_s the corresponding place of $\mathbb{Q}(t)$, and given a Galois extension $\Omega/\mathbb{Q}(t)$, let D_s be the decomposition group of P_s in Ω. For a place P_{t_0} that is unramified in Ω, let $\tilde{P} \in \mathbb{P}_\Omega$ lie above P_{t_0}. The decomposition group D_{t_0} is the Galois group of the residue field extension $\Omega_{\tilde{P}}/\mathbb{Q}(t)_{P_{t_0}}$ ([20], Theorem 3.8.2). Since P_{t_0} is a rational place, the bottom field is in fact $\mathbb{Q}$; the Galois extension of $\mathbb{Q}$ obtained in this way is called the *specialization* of $\Omega/\mathbb{Q}(t)$ at t_0. For almost all specializations, the

Galois group of the extension of $\mathbb{Q}$ achieved in this manner is the Galois group over $\mathbb{Q}$ of the specialization of f by t_0.([10], Proposition 2.3) Throughout this section, let N be the constant given by Theorem 1.1.

Relating Extensions of $\mathbb{C}(t)$ to Extensions of $\mathbb{Q}(t)$

Given a polynomial $f \in \mathbb{Q}[X,t]$, the *arithmetic monodromy* group of f is the Galois group of its splitting field over $\mathbb{Q}(t)$ and the *geometric monodromy* of f is the Galois group of its splitting field over $\bar{\mathbb{Q}}(t)$. The arithmetic monodromy group is a normal subgroup of the geometric monodromy group. Denote by Ω the splitting field of f over $\mathbb{Q}(t)$. Then $\Omega\bar{\mathbb{Q}}/\bar{\mathbb{Q}}(t)$ is a Galois extension as well, with Galois group isomorphic to that of the extension $\Omega\mathbb{C}/\mathbb{C}(t)$. This is due to the fact that $\Omega/\bar{\mathbb{Q}}(t)$ and $\mathbb{C}(t)/\bar{\mathbb{Q}}(t)$ are linearly disjoint.

Decomposition Groups Shared by Infinitely Many Places

Given a Galois extension $\Omega/\mathbb{Q}(t)$, denote by $\mathcal{D}$ the set of decomposition groups of $\Omega/\mathbb{Q}(t)$ shared by infinitely many degree-1 (i.e., rational) places of $\mathbb{Q}(t)$.

Lemma 10.1.3 (Properties of the set $\mathcal{D}$)**.** *Let $\Omega/\mathbb{Q}(t)$ be a Galois extension. Then:*

1. *There exists a finite set W_0 such that for any $t_0 \in \mathbb{Q} \setminus W_0$, the decomposition group D_{t_0} is shared by infinitely many rationals (that is, $D \in \mathcal{D}$).*
2. *For $D \in \mathcal{D}$, the field $\Omega^D\bar{Q}$ is of genus 0 or 1.*

Proof. The first assertion follows from the pigeonhole principle and the fact that $\mathbb{Q}(t)$ has infinitely many rational places but $\mathrm{Gal}(\Omega/\mathbb{Q}(t))$ has only finitely many subgroups.

For the second assertion, let t_0 be any rational such that $D = D_{t_0}$. Then there exists a place of degree 1 of the decomposition field Ω^D lying over P_{t_0} ([20], Theorem 3.8.3); since each place of Ω^D restricts to a unique place of $\mathbb{Q}(t)$, the decomposition field Ω^D has a rational place for every t_0 such that $D = D_{t_0}$. In particular, the field Ω^D has infinitely many rational places, and so the algebraic curve associated with this field has infinitely many rational points. By Faltings' theorem this curve is then of genus 0 or 1, i.e., the function field $\Omega^D\bar{Q}$ is of genus 0 or 1. ■

The following proposition follows directly from Lemma 10.1.3 and Theorem 1.1:

Proposition 10.1.4 (Decomposition fields of Symmetric Extensions)**.** *Let $f(X,t) \in \mathbb{Q}[X,t]$ be an polynomial with geometric monodromy group $G = S_n$ or A_n, where $n > N$; let Ω be the splitting field of f over $\mathbb{Q}(t)$. If $D \in \mathcal{D}$, then D is one of the following:*

1. *$A_n \leq D \leq S_n$.*
2. *$A_{n-1} \leq D \leq S_{n-1}$.*

3. $A_{n-2} \lneq D \leq (S_{n-2} \times S_2)$.

Remark. If D_{t_0} is one of the options listed in Proposition 10.1.4 for some $t_0 \in \mathbb{Q} \setminus W_0$, then for infinitely many rationals $s \in \mathbb{Q} - W_0$, the decomposition group $D_s = D_{t_0}$.

Proof of Proposition 10.1.4. Let W_0 be the set given by Lemma 10.1.3. By the first assertion of the lemma, for any $t_0 \in \mathbb{Q} \setminus W_0$, the decomposition group $D_{t_0} \in \mathcal{D}$. By the second assertion of the lemma, for any $D \in \mathcal{D}$, the field $\Omega^D \bar{Q} = \Omega^{D \cap G}$ is of genus 0 or 1. By assumption, $G = \mathrm{Gal}(\Omega\bar{Q}/\bar{\mathbb{Q}}(t))$ is a symmetric or alternating group on $n > N$ and by a basic field-theoretic argument, $\Omega\mathbb{C}/\mathbb{C}(t)$ is a Galois extension with $\mathrm{Gal}(\Omega\mathbb{C}/\mathbb{C}(t)) \cong G$. Therefore $D \cap G$ is a genus 0 or 1 subgroup of a symmetric or alternating extension of degree $n > N$, and the possibilities for $D \cap G$ are given by Theorem 1.1:

1. $A_n \leq D \cap G \leq S_n \cap G$.
2. $A_{n-1} \leq D \cap G \leq S_{n-1} \cap G$.
3. $A_{n-2} \lneq D \cap G \leq (S_{n-2} \times S_2) \cap G$.

Since $G = S_n$ or A_n, nothing is lost by stating that:

1. $A_n \leq D \leq S_n$.
2. $A_{n-1} \leq D \leq S_{n-1}$.
3. $A_{n-2} \lneq D \leq (S_{n-2} \times S_2)$,

as required. ■

Proposition 10.1.4 easily leads to the proof of Theorem 1.2:

Proof of Theorem 1.2. Let W_0 be the finite set of exceptional rationals given by Proposition 10.1.4, and denote by W_1 the set of rationals s such that the place P_s of $\mathbb{Q}(t)$ is ramified in Ω. Note that W_1 is a finite set. Theorem 1.2 now follows from Proposition 10.1.4 by setting $W := W_0 \cup W_1$ and recalling that for an unramified place P_{t_0}, the decomposition group D_{t_0} is the Galois group of the specialization of $\Omega/\mathbb{Q}(t)$ at t_0. ■

Characterization of the Set Red_f

Next, we will use the classification given in Theorem 1.1 to examine the set of reducible specializations of a bivariate polynomial. Given an irreducible bivariate polynomial $f(x,t) \in \mathbb{Q}[x,t]$ and $t_0 \in \mathbb{Q}$, denote by Red_f the set of rationals t_0 such that $f(x,t_0)$ is reducible. By Hilbert's irreducibility theorem, the set $\mathbb{Q} \setminus \mathrm{Red}_f$ is infinite. The set Red_f may be finite or infinite. We will examine the case where Red_f is infinite. Müller ([14],[15], following Fried and others) examined the set $\mathrm{Red}_f \cap \mathbb{Z}$, relying on Siegel's

theorem. When considering integer specializations alone ([15], Proposition 2.1), the set $\mathrm{Red}_f \cap \mathbb{Z}$ corresponds to the set of some rational places on genus 0 subfields of the splitting field of f. Müller's result levereges the restrictions given by Siegel's theorem on the ramification in such subfields. We follow the path suggested by Müller (See [15], Proposition 5.17 and [14], discussion in Chapter 9 regarding the point (c)) for considering rational specializations in general: replace Siegel's theorem by Faltings' theorem, in which case, the set Red_f corresponds to the set of some rational places on genus 0 or 1 subfields of the splitting field of f. However, Faltings theorem does not supply any restrictions on ramification. Under suitable assumptions that allow for the application of Theorem 1.1, the constraints on ramification given by Siegel's theorem are replaced by the classification of genus 0 and 1 subgroups of the splitting field of f. The details follow below.

The membership of a rational t_0 in Red_f is related to its decomposition group by the following standard argument, a combination of Dedekind-Kummer theorem and Lemma 2.6.1:

Proposition 10.1.5. *Let $f(x,t) \in \mathbb{Q}[x,t]$ be an irreducible polynomial. Let $\mathbb{Q}(x,t)$ be the field obtained by adjoining a root of f to $\mathbb{Q}(t)$, and let Ω be its Galois closure. Denote $\mathrm{Gal}(\Omega/\mathbb{Q}(t))$ by G and denote the subgroup of G fixing $\mathbb{Q}(x,t)$ by H. There exists a finite set W, such that for any $t_0 \in \mathbb{Q} \setminus W$, it holds that $t_0 \in \mathrm{Red}_f$ if and only if $D_{t_0} H \neq G$.*

Proof. By Dedekind-Kummer theorem (confer, for example, [20], Theorem 3.3.7, for a function field version), there exists a set W such that for $t_0 \in \mathbb{Q} \setminus W$, the set $E_{\mathbb{Q}(x,t)/\mathbb{Q}(t)}(P_{t_0})$ is equal to the set of degrees of polynomials in the reduction of $f(x,t)$ mod P_{t_0}, i.e., the decomposition of $f(x,t_0)$ in $\mathbb{Q}[x]$. In particular, $f(x,t_0)$ is irreducible if and only if P_{t_0} has a single place above it in $\mathbb{Q}(x,t)$. By Lemma 2.6.1, the set $E_{\mathbb{Q}(x,t)/\mathbb{Q}(t)}(P_{t_0})$ equals the set of lengths of orbits of D_{t_0} on G/H, so $f(x,t_0)$ is irreducible if and only if the action of D_{t_0} on G/H is transitive. Therefore for a rational $t_0 \in \mathbb{Q} \setminus W$, the polynomial $f(x,t_0)$ is reducible if and only if $D_{t_0} H \neq G$. ■

Remark. Proposition 10.1.5 holds without assumptions on the cardinality of Red_f, however, if Red_f is finite then the set $\mathrm{Red}_f \setminus W$ may be empty.

Remark. It is implicit in the statement of Proposition 10.1.5 that the exceptional set W contains the set of rationals corresponding with places of $\mathbb{Q}(t)$ ramified in Ω (i.e., for every $t_0 \in \mathbb{Q} \setminus W$, the inertia group I_{t_0} is trivial.

Given a Galois extension $\Omega/\mathbb{Q}(t)$, denote

$$\mathcal{D}(H) := \{D \in \mathcal{D} : DH \neq G\},$$

and let $\mathcal{D}_{Min}(H)$ be the set of minimal elements of $\mathcal{D}(H)$ under inclusion. For a decomposition group D of $\Omega/\mathbb{Q}(t)$, fix $f_D(x,t) \in \mathbb{Q}[x,t]$ to be the minimal polynomial

over $\mathbb{Q}(t)$ of a primitive element of the decompmosition field Ω^D; If D_1 and D_2 are conjugate subgroups of $\mathrm{Gal}(\Omega/\mathbb{Q}(t))$, then the subfields fixed by them are isomorphic and primitive elements may be chosen such that $f_{D_1} = f_{D_2}$; therefore fix the polynomials f_D such that the mapping $D \to f_D$ is constant on the conjugacy classes of the subgroups of $\mathrm{Gal}(\Omega/\mathbb{Q}(t))$.

If $f(x,t) \in \mathbb{Q}[x,t]$ is such that Red_f is infinite, Proposition 10.1.5 makes it possible to characterize Red_f in the following way:

Corollary 10.2. *Let $\Omega/\mathbb{Q}(t)$ be a Galois extension. Denote its Galois group by G and let $H \leq G$ and let $f(x,t) \in \mathbb{Q}[x,t]$ be a minimal polynomial for a primitive element of Ω^H. Assume that Red_f is infinite. Then the set Red_f differs by a finite set from:*

$$\bigcup_{D \in \mathcal{D}(H)} \{t_0, D_{t_0} = D\}, \tag{10.3}$$

and the set (10.3) is characterized as follows:

$$\bigcup_{D \in \mathcal{D}(H)} \{t_0, D_{t_0} = D\} = \bigcup_{D \in \mathcal{D}_{Min}(H)} \{t_0 \in \mathbb{Q}, f_D(x, t_0) \text{ has a rational root}\}. \tag{10.4}$$

Proof. For $t_0 \in \mathbb{Q} \setminus W$ such that $D_{t_0} \in D(H)$, the decomposition group D_{t_0} has a fixed point in its action on G/D_{t_0}. Therefore there is a rational place of $\Omega^{D_{t_0}}$ lying above P_{t_0} and by Proposition 10.1.5, the polynomial $f_{D_{t_0}}(x, t_0)$ has a root in $\mathbb{Q}$. Given a specialization $t_0 \in \mathbb{Q} \setminus W$ such that $f_D(x, t_0)$ has a root, we need to show that $D_{t_0} \in \mathcal{D}(H)$. By Dedekind-Kummer theorem, there is a rational place P_D of Ω^D lying above P_{t_0}; then ([20], Theorem 3.8.3), $\Omega^D \subseteq \Omega^{D_{t_0}}$, i.e., $D_{t_0} \leq D$; Since $DH \neq G$ then in particular $D_{t_0} H \neq G$ and so $D_{t_0} \in \mathcal{D}(H)$. We have now shown that

$$\bigcup_{D \in \mathcal{D}(H)} \{t_0, D_{t_0} = D\} = \bigcup_{D \in \mathcal{D}(H)} \{t_0 \in \mathbb{Q} : f_D(x, t_0) \text{ has a root}\}. \tag{10.5}$$

It remains to show that the union on the right hand side may be taken over the groups in $\mathcal{D}_{Min}(H)$ alone: If $D_1 \leq D_2$ for $D_1, D_2 \in \mathcal{D}(H)$, and if $f_{D_1}(x, t_0)$ has a root then Ω^{D_1} has a rational place; but since $D_1 \leq D_2$ then Ω^{D_2} has a rational place as well, and therefore $f_{D_2}(x, t_0)$ has a root; so in fact

$$\bigcup_{D \in \mathcal{D}(H)} \{t_0, f_D(x, t_0) \text{ has a root}\} = \bigcup_{D \in \mathcal{D}_{min}(H)} \{t_0, f_D(x, t_0) \text{ has a root}\},$$

as required. ∎

With the technical framework now in place, the classification of genus 0 and 1 subgroups of symmetric and alternating extensions allows us to bound the size of $\mathcal{D}_{Min}(H)$ and thus prove Theorem 10.1:

Proof of Theorem 10.1. Let Ω be the splitting field of f over $\mathbb{Q}(t)$. By Proposition 10.1.4 and Theorem 1.1, the set $\mathcal{D}_{Min}(H)$ is of size at most 2 if the ramification type of $(\Omega\bar{Q})^{S_{n-1}\cap G}/\bar{\mathbb{Q}}(t)$ is not one of the exceptional types in Table A.1) and of size at most 3 otherwise. The conclusion follows from Corollary 10.2. ■

Appendix A

Tables of Exceptional Ramification Types

Table A.1: Reproduction of [16], Table 4.1. In all entries, $a \in \{1, \ldots, n-1\}$ is odd and $(n, a) = 1$.

$I1.1$	$[n], [a, n-a], [1^{n-2}, 2]$		S_n
$I2.1$	$[n], [1^3, 2^{(n-3)/2}], [1, 2^{(n-1)/2}], [1^{n-2}, 2]$	[7, Proposition 3.0.24(e)]	S_n
$I2.2$	$[n], [1^2, 2^{(n-2)/2}]$ twice, $[1^{n-2}, 2]$	[7, Proposition 3.0.24(c)]	S_n
$I2.3$	$[n], \left[1^3, 2^{(n-3)/2}\right], [2^{(n-3)/2}, 3]$	[7, Proposition 3.0.25(b)]	S_n, A_n
$I2.4$	$[n], \left[1^2, 2^{(n-2)/2}\right], [1, 2^{(n-4)/2}, 3]$	[7, Proposition 3.0.25(d)]	S_n
$I2.5$	$[n], \left[1, 2^{(n-1)/2}\right], [1^2, 2^{(n-5)/2}, 3]$	[7, Proposition 3.0.25(f)]	S_n, A_n
$I2.6$	$[n], \left[1^3, 2^{(n-3)/2}\right], [1, 2^{(n-5)/2}, 4]$	[7, Proposition 3.0.25(a)]	S_n, A_n
$I2.7$	$[n], \left[1^2, 2^{(n-2)/2}\right], [1^2, 2^{(n-6)/2}, 4]$	[7, Proposition 3.0.25(c)]	S_n
$I2.8$	$[n], \left[1, 2^{(n-1)/2}\right], [1^3, 2^{(n-7)/2}, 4]$	[7, Proposition 3.0.25(e)]	S_n, A_n
$I2.9$	$[a, n-a], [1^2, 2^{(n-2)/2}], [2^{n/2}], [1^{n-2}, 2]$	[7, Proposition 3.0.24(d)]	S_n
$I2.10$	$[a, n-a], [1, 2^{(n-1)/2}]$ twice, $[1^{n-2}, 2]$	[7, Proposition 3.0.24(f)]	S_n
$I2.11$	$[a, n-a], \left[2^{n/2}\right], [1^2, 2^{(n-6)/2}, 4]$	[7, Proposition 3.0.27(c)]	S_n, A_n
$I2.12$	$[a, n-a], \left[1, 2^{(n-1)/2}\right], [1, 2^{(n-5)/2}, 4]$	[7, Proposition 3.0.27(a)]	S_n
$I2.13$	$[a, n-a], \left[1^2, 2^{(n-2)/2}\right], [2^{(n-4)/2}, 4]$	[7, Proposition 3.0.28(c)]	S_n, A_n
$I2.14$	$[a, n-a], \left[1, 2^{(n-1)/2}\right], [2^{(n-3)/2}, 3]$	[7, Proposition 3.0.27(b)]	S_n
$I2.15$	$[a, n-a], \left[2^{n/2}\right], [1, 2^{(n-4)/2}, 3]$	[7, Proposition 3.0.27(d)]	S_n, A_n
$F1.1$	$\left[1^{n-2}, 2\right], [2^{n/2}], [1^2, 2^{(n-2)/2}]$ thrice	[7, Proposition 3.0.24(a)]	S_n
$F1.2$	$\left[1^{n-2}, 2\right], [1^3, 2^{(n-3)/2}], [1, 2^{(n-1)/2}]$ thrice	[7, Proposition 3.0.24(b)]	S_n
$F1.3$	$\left[1^3, 2^{(n-3)/2}\right], [2^{(n-3)/2}, 3], [1, 2^{(n-1)/2}]$ twice	[7, Proposition 3.0.26(b)]	S_n
$F1.4$	$\left[2^{n/2}\right], [1, 2^{(n-4)/2}, 3], [1^2, 2^{(n-2)/2}]$ twice	[7, Proposition 3.0.26(d)]	S_n
$F1.5$	$\left[1^2, 2^{(n-5)/2}, 3\right], [1, 2^{(n-1)/2}]$ thrice	[7, Proposition 3.0.26(f)]	S_n, A_n
$F1.6$	$\left[1^3, 2^{(n-3)/2}\right], [1, 2^{(n-5)/2}, 4], [1, 2^{(n-1)/2}]$ twice	[7, Proposition 3.0.26(a)]	S_n
$F1.7$	$\left[2^{n/2}\right], [1^2, 2^{(n-6)/2}, 4], [1^2, 2^{(n-2)/2}]$ twice	[7, Proposition 3.0.26(c)]	S_n
$F1.8$	$\left[1^3, 2^{(n-7)/2}, 4\right], [1, 2^{(n-1)/2}]$ thrice	[7, Proposition 3.0.26(e)]	S_n, A_n
$F1.9$	$\left[2^{(n-4)/2}, 4\right], [1^2, 2^{(n-2)/2}]$ thrice;		S_n, A_n
$F3.1$	$\left[1^2, 2^{(n-2)/2}\right], [1, 3, 4^{(n-4)/4}], [4^{n/4}]$	[7, Conjecture 3.0.29(a)]	S_n
$F3.2$	$\left[1, 2^{(n-1)/2}\right], [1, 4^{(n-1)/4}], [2, 3, 4^{(n-5)/4}]$	[7, Conjecture 3.0.29(b)]	S_n, A_n
$F3.3$	$\left[1, 2^{(n-1)/2}\right], [1, 2, 4^{(n-3)/4}], [3, 4^{(n-3)/4}]$	[7, Conjecture 3.0.29(c)]	S_n
$F4.1$	$\left[1^2, 2^{(n-2)/2}\right], [1, 2, 3^{(n-3)/3}], [6^{n/6}]$	[7, Conjecture 3.0.29(d)]	S_n
$F4.2$	$\left[1^2, 2^{(n-2)/2}\right], [2, 3^{(n-2)/3}], [2, 6^{(n-2)/6}]$		S_n
$F4.3$	$\left[1, 2^{(n-1)/2}\right], [1, 3^{(n-1)/3}], [3, 4, 6^{(n-7)/6}]$	[7, Conjecture 3.0.29(e)]	S_n, A_n
$F4.4$	$\left[1, 2^{(n-1)/2}\right], [1, 2, 3^{(n-3)/3}], [3, 6^{(n-3)/6}]$	[7, Conjecture 3.0.29(h)]	S_n
$F4.5$	$\left[1^2, 2^{(n-2)/2}\right], [1, 3^{(n-1)/3}], [4, 6^{(n-4)/6}]$	[7, Conjecture 3.0.29(i)]	S_n, A_n
$F4.6$	$\left[1, 2^{(n-1)/2}\right], [2, 3^{(n-2)/3}], [2, 3, 6^{(n-5)/6}]$	[7, Conjecture 3.0.29(j)]	S_n

Table A.2: Entries of Table A.1 in which the subfield fixed by $A_{n-2} \times S_2$ is of genus 0. Here $1 \leq a \leq n-1$ is an integer coprime to n.

$I2.11$	$[a, n-a], \left[2^{n/2}\right], [1^2, 2^{(n-6)/2}, 4]$	$n \equiv 2 \mod 4$
$I2.13$	$[a, n-a], \left[1^2, 2^{(n-2)/2}\right], [2^{(n-4)/2}, 4]$	$n \equiv 0 \mod 4$
$I2.15$	$[a, n-a], \left[2^{n/2}\right], [1, 2^{(n-4)/2}, 3]$	$n \equiv 2 \mod 4$
$F4.3$	$\left[1, 2^{(n-1)/2}\right], [1, 3^{(n-1)/3}], [3, 4, 6^{(n-7)/6}]$	$n \equiv 7 \mod 12$
$F4.5$	$\left[1^2, 2^{(n-2)/2}\right], [1, 3^{(n-1)/3}], [4, 6^{(n-4)/6}]$	$n \equiv 4 \mod 12$

Table A.3: Entries of Table A.1 in which the subfield fixed by $A_{n-2} \times S_2$ is of genus 1.

$I2.3$	$[n], [1^3, 2^{\frac{n-3}{2}}], [2^{\frac{n-3}{2}}, 3]$	$n \equiv 1 \mod 4$
$I2.5$	$[n], \left[1, 2^{(n-1)/2}\right], [1^2, 2^{(n-5)/2}, 3]$	$n \equiv 3 \mod 4$
$I2.6$	$[n], \left[1^3, 2^{(n-3)/2}\right], [1, 2^{(n-5)/2}, 4]$	$n \equiv 1 \mod 4$
$I2.8$	$[n], \left[1, 2^{(n-1)/2}\right], [1^3, 2^{(n-7)/2}, 4]$	$n \equiv 3 \mod 4$
$F1.5$	$\left[1^2, 2^{(n-5)/2}, 3\right], [1, 2^{(n-1)/2}]$ thrice	$n \equiv 3 \mod 4$
$F1.8$	$\left[1^3, 2^{(n-7)/2}, 4\right], [1, 2^{(n-1)/2}]$ thrice	$n \equiv 3 \mod 4$
$F1.9$	$\left[2^{(n-4)/2}, 4\right], [1^2, 2^{(n-2)/2}]$ thrice;	$n \equiv 0 \mod 4$

Appendix B

MAGMA Check

This section contains MAGMA code that checks that gets a list of ramification types of a symmetric or alternating extension as input and calculates, for the symmetric types only, the genera of the subfields fixed by index-2 subgroups of $S_{n-2} \times S_2$, and the genus of the subfield fixed by A_{n-2} (as a sanity check). The code is partially based on code by Mike Zieve.

B.1 Code

```
S:=[[{*1,2^^5*},{*1,2,4^^2*},{*3,4^^2*}],
[{*1,2^^5*},{*2,3^^3*},{*2,3,6^^1*}]]; //sample input

for m in [1..#S by +1] do
T:=S[m];  //take the ramification type
n:=&+[i:i in T[1]]; //n is the degree of Galois group as perm. group
G:=Sym(n);

branchcycles:=[];
for c in T do //this loop creates a permutation with the given cycle structure.
max:=0;
a:=[];
for i in c do
a cat:=[{@ max+j: j in [1..i] @}];
max+:=i;
end for;
branchcycles cat:=[G!a];
end for;
G:=ncl<G|branchcycles>;
if #G ne Factorial(n) then;
// input for type does not give symmetric extension - skip
```

```
else
mytransposition := G!(n-1, n);
Stab:=Stabilizer(G,{n-1,n});
Candidates := LowIndexSubgroups(Stab,2);
Append(~Candidates,G!!Alt(n-2));
for c in [#Candidates..1 by -1] do
//check genus & print if not what expected
index:=#G/#Candidates[c];
f:=CosetAction(G,Candidates[c]);
//calculate RH contribution of branch cycles
RH:=#branchcycles*index;
for b in [#branchcycles ..1 by -1] do
D:=sub<G | branchcycles[b]>;
RH -:=#Orbits(f(D));
end for;
//substitute in Riemann-Hurwitz formula to calculate genus:
twicegenus:=2-2*index + RH;
if (#Stab/#Candidates[c]) eq 4 then
printf "$%o,A_n-2,%o\n",m,twicegenus/2;
else
if #Candidates[c] ne #Stab then
if mytransposition in Candidates[c] then
printf "$%o,A_n-2xS_2,%o\n",m,twicegenus/2;
else
if  #Fix(Candidates[c]) eq 2 then
printf "$%o,S_n-2,%o\n",m,twicegenus/2;
else
printf "$%o,fiber,%o\n",m,twicegenus/2;
end if;
end if;
else
//do nothing;
end if;
end if;
end for;
end if;
end for;
```

B.2 Results

The check was performed for values (n, a) where $n = 11, \ldots 19$ and a was chosen as some odd integer coprime to n. The values for n and a were substitued into Table A.1 where applicable, and the resulting input was entered into MAGMA.

Table B.1: Genus check results for $n = 11, a = 3$

Type	$S_{n-2} \times_{C_2} S_2$	S_{n-2}	$A_{n-2} \times S_2$	A_{n-2}
$I1.1$	18	**0**	18	36
$I2.1$	20	4	19	43
$I2.5$	5	3	1	9
$I2.8$	4	3	1	8
$I2.10$	23	5	18	46
$I2.12$	2	4	2	8
$I2.14$	2	4	2	8
$F1.2$	25	9	19	53
$F1.3$	4	8	3	15
$F1.5$	10	8	**1**	19
$F1.6$	4	8	3	15
$F1.8$	9	8	**1**	18
$F3.3$	2	4	**1**	7
$F4.6$	8	6	3	17

Table B.2: Genus check results for $n = 12, a = 5$

$Type$	$S_{n-2} \times_{C_2} S_2$	S_{n-2}	$A_{n-2} \times S_2$	A_{n-2}
$I1.1$	22	**0**	22	44
$I2.2$	28	5	23	56
$I2.4$	2	4	2	8
$I2.7$	2	4	2	8
$I2.9$	25	5	25	55
$I2.13$	4	4	**0**	8
$F1.1$	31	10	26	37
$F1.4$	5	9	5	19
$F1.7$	5	9	5	19
$F1.9$	10	9	**1**	20
$F3.1$	2	4	2	8
$F4.1$	10	3	8	21

Table B.3: Genus check results for $n = 13, a = 5$

$Type$	$S_{n-2} \times_{C_2} S_2$	S_{n-2}	$A_{n-2} \times S_2$	A_{n-2}
$I1.1$	28	**0**	28	56
$I2.1$	31	5	31	67
$I2.3$	6	4	**1**	11
$I2.6$	5	4	**1**	10
$I2.10$	28	6	34	68
$I2.12$	2	5	4	11
$I2.14$	3	5	4	12
$F1.2$	31	11	37	79
$F1.3$	6	10	7	23
$F1.6$	5	10	7	22
$F3.2$	**0**	5	5	10

Table B.4: Genus check results for $n = 14, a = 5$

$Type$	$S_{n-2} \times_{C_2} S_2$	S_{n-2}	$A_{n-2} \times S_2$	A_{n-2}
$I1.1$	33	**0**	32	65
$I2.2$	33	6	38	77
$I2.4$	3	5	3	11
$I2.7$	2	5	3	10
$I2.9$	36	6	35	77
$I2.11$	5	5	**0**	10
$I2.15$	6	5	**0**	11
$F1.1$	36	12	41	89
$F1.4$	6	11	6	23
$F1.7$	5	11	6	22
$F4.2$	12	4	13	29

Table B.5: Genus check results for $n = 15, a = 7$

$Type$	$S_{n-2} \times_{C_2} S_2$	S_{n-2}	$A_{n-2} \times S_2$	A_{n-2}
$I1.1$	40	**0**	40	80
$I2.1$	42	6	41	89
$I2.5$	7	5	**1**	13
$I2.8$	6	5	**1**	12
$I2.14$	4	6	4	14
$F1.2,$	49	13	41	103
$F1.3$	6	12	5	23
$F1.5$	14	12	**1**	27
$F1.6$	6	12	5	23
$F1.8$	13	12	**1**	26
$F3.3$	3	6	3	12
$F4.4$	16	4	13	33

Table B.6: Genus check results for $n = 16, a = 7$

$Type$	$S_{n-2} \times_{C_2} S_2$	S_{n-2}	$A_{n-2} \times S_2$	A_{n-2}
$I1.1$	45	**0**	45	90
$I2.2$	53	7	46	106
$I2.4$	3	6	3	12
$I2.7$	3	6	3	12
$I2.9$	49	7	49	105
$I2.13$	6	6	**0**	12
$F1.1$	57	14	50	121
$F1.4$	7	13	7	27
$F1.7$	7	13	7	27
$F1.9$	14	13	**1**	28
$F3.1$	4	6	4	14
$F4.5$	4	4	**0**	8

Table B.7: Genus check results for $n = 17, a = 7$

$Type$	$S_{n-2} \times_{C_2} S_2$	S_{n-2}	$A_{n-2} \times S_2$	A_{n-2}
$I1.1$	154	**0**	53	107
$I2.1$	57	7	57	121
$I2.3$	8	6	**1**	15
$I2.6$	7	6	**1**	14
$I2.10$	54	8	61	123
$I2.12$	4	7	5	16
$I2.14$	5	7	5	17
$F1.2$	57	15	65	137
$F1.3$	8	14	9	31
$F1.6$	7	14	9	30
$F4.6$	19	5	21	45

Table B.8: Genus check results for $n = 18, a = 7$

$Type$	$S_{n-2} \times_{C_2} S_2$	S_{n-2}	$A_{n-2} \times S_2$	A_{n-2}
$I1.1$	60	**0**	59	119
$I2.2$	60	8	67	135
$I2.4$	4	7	4	15
$I2.7$	3	7	4	14
$I2.9$	64	8	63	135
$I2.11$	7	7	**0**	14
$I2.15$	8	7	**0**	15
$F1.1$	64	16	71	151
$F1.4$	8	15	8	31
$F1.7$	7	15	8	30
$F4.1$	21	5	23	49

Table B.9: Genus check results for $n = 19, a = 7$

$Type$	$S_{n-2} \times_{C_2} S_2$	S_{n-2}	$A_{n-2} \times S_2$	A_{n-2}
$I1.1$	69	**0**	69	138
$I2.1$	72	8	71	151
$I2.5$	9	7	**1**	17
$I2.8$	8	7	**1**	16
$I2.10$	78	9	69	56
$I2.12$	5	8	5	18
$I2.14$	5	8	5	18
$F1.2$	81	17	71	169
$F1.3$	8	16		, 31
$F1.5$	18	16	**1**	35
$F1.6$	8	16	7	31
$F1.8$	17	16	**1**	34
$F3.3$	4	8	3	15
$F4.3$	5	5	**0**	10

Appendix C

Bibliography

Bibliography

[1] R. Accola, Two Theorems on Riemann Surfaces with Noncyclic Automorphism Groups, Proceedings of the American Mathematical Society, Volume 25, issue 3 (1970), 598-602.

[2] D. Bundy, S. Hart, The case of equality in the Livingstone-Wagner Theorem, Journal of Algebraic Combinatorics, Volume 29, issue 2 (2009), 2215-227.

[3] L. Babai, Á. Seress, On the degree of transitivity of permutation groups: A short proof, Journal of Combinatorial Theory, Series A, Volume 45, issue 2 (1987), 310-315.

[4] P. Cassou-Noguès, J. Couveignes, Factorizations explicites de $g(y)h(z)$, Acta Arith. 87 (1999), 291–317.

[5] H. Davenport, D. J. Lewis, A. Schinzel, Polynomials of certain special types. Acta Arith. 9 (1964) 107–116.

[6] M. Fried, The field of definition of function fields and a problem in the reducibility of polynomials in two variables. Illinois J. Math. 17 (1973), 128–146.

[7] R. Guralnick, J. Shareshian, Symmetric and Alternating Groups as Monodromy Groups of Riemann Surfaces I: Generic Covers and Covers with Many Branch Points. Appendix by R. Guralnick and R. Stafford. Mem. Amer. Math. Soc. 189 (2007).

[8] W. Fulton, Algebraic Curves: An Introduction to Algebraic Geometry. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[9] D. Frohardt, K. Magaard, Composition factors of monodromy groups. Ann. Math. 154 (2001), 327–345.

[10] D. Krumm, N. Sutherland, Galois groups over rational function fields and explicit Hilbert irreducibility. arXiv:1708.04932.

[11] D. Livingstone, A. Wagner, Transitivity of finite permutation groups on unordered sets. Math. Z., 90 (1965), 393–403.

[12] R. Miranda, Algebraic Curves and Riemann Surfaces. American Mathematical Society, (1995).

[13] P. Müller, Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials Ann. Sc. Norm. Super. Pisa Cl. Sci. (5), Vol. XII (2013), 369–438.

[14] P. Müller, Hilbert's irreducibility theorem for prime degree and general polynomials, Isr. J. Math. (1999) 109: 319. https://doi.org/10.1007/BF02775041

[15] P. Müller, Finiteness results for Hilbert's irreducibility theorem. Annales de l'institut Fourier, 52 (2002), 983–1015.

[16] D. Neftin, M. Zieve, Monodromy groups of indecomposable covers with bounded genus. Preprint, version from December 2016.

[17] D. Neftin, M. Zieve, Monodromy groups of product type. Preprint, version from July 12, 2016.

[18] J-P. Serre, Topics in Galois Theory. 2nd ed. AK Peters (2007).

[19] J. H. Silverman, The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, Second Edition.

[20] H. Stichtenoth, Algebraic function fields and codes. Universitext. Springer-Verlag, Berlin (1993).

[21] O. Zariski, Sulle equazioni algebriche contenenti linearmente un parametro e risolubili per radicali. Atti Accad. Naz. Lincei Rend., Cl. Sci. Fis. Mat. Natur., serie V, 33 (1924), 80–82.

D_P על הקוסטים G/H. אם כן, בהינתן חבורות הפירוק של המקומות של $\mathbb{C}(t)$ המסועפים ב-Ω, ניתן לחשב את ההסתעפות בכל אחד מתתי השדות של ההרחבה, ועקב כך (בעזרת נוסחת רימן-הורביץ) גם את הגנוס של כל אחד מתתי השדות. נניח שהחבורה G היא החבורה הסימטרית על n איברים, ו-P מקום של $\mathbb{C}(t)$ המסועף ב-Ω. ההסתעפות של המקום P בתת השדה של Ω המקובע על ידי המייצב $S_{n-1} \cap G$ שווה לקבוצת אורכי המעגלים של היוצר של D_P (כתמורה על n איברים); אם כן טיפוס ההסתעפות של ההרחבה $\Omega^{S_{n-2}\cap G}/\mathbb{C}(t)$ מתאר את חבורות הפירוק של ההרחבה.

המיון של תתי שדות מגנוס 0 או 1 של הרחבת גלואה עם חבורת גלואה סימטרית או חבורות התמורות הזוגיות יבוצע באופן הבא: בהינתן חבורת תמורות H שפועלת על n איברים, נסמן ב-O_k את מספר המסלולים שלה על קבוצות לא סדורות בגודל k של $\{1,\dots,n\}$. נניח ש-$\Omega/\mathbb{C}(t)$ הרחבת גלואה שחבורת הגלואה שלה G היא החבורה הסימטרית או חבורות התמורות הזוגיות על n איברים. נסמן ב-$\mathcal{E}$ את טיפוס ההסתעפות של השדה $\Omega^{S_{n-1}\cap G}/\mathbb{C}(t)$. מתנאי שפותח בעבודות של Guralnick-Shareshian ו-Neftin-Zieve נובע, שאם תת חבורה H של G מקבעת תת-שדה מגנוס 0 או 1, אז קיים $m \leq 2$ כך ש:

$$O_m = O_{m+1} = \cdots = O_{\frac{n}{2}}$$

כאשר $m = 1$ אם $\mathcal{E}$ לא נמצא ברשימת יוצאי דופן נתונה, ו$m = 2$ אחרת. זהו תנאי הכרחי שעל H לקיים כדי לקבע תת שדה מגנוס 0 או 1, הנתון בלשון של תורת החבורות. באמצעות טיעונים של ספירת מסלולים ומשפט Livingstone-Wagner, נראה שחבורות שמקיימות תנאי זה הן החבורה הסימטרית מסדר n או חבורת התמורות הזוגיות על n איברים, החבורה הסימטרית מסדר $n-1$ או חבורת התמורות הזוגיות מסדר זה, מייצב של נקודה בפעולה של אחת מהחבורות האלה, או תת חבורה של $S_{n-2}\times S_2$ בעלת פעולה 6-טרנזיטיבית על הקבוצה בת ה-n-2 איברים $\{1,\dots,n-2\}$. על פי המיון של חבורות פשוטות סופיות, חבורה 6-טרנזיטיבית על n-2 איברים חייבת להיות החבורה הסימטרית מסדר זה או חבורות התמורות הזוגיות מסדר זה ועל כן ניתן לצמצם את האפשרויות ל-H. ננסח קריטריונים לחישוב של הגנוס של תתי שדות של הרחבה סימטרית או מתחלפת המקובעים על ידי תתי חבורות ברשימה זו ועל כן "חשודים" בכך שהם מגנוס 0 או 1, וכך נקבע אילו מהאפשרויות אכן קורות בפועל. שני הכלים המשמשים לחישוב של הגנוס של הרחבות מדרגה 2 של השדות המקובעים על ידי מייצבים של נקודות וקבוצות בגודל 2, הם הלמה של Abhyankar, שמשמשת לחישוב ההסתעפות בקומפוזיטום של הרחבות שדות, וחישוב ישיר של הפעולה של תמורה על קבוצות בגודל 2.

אם G היא חבורת התמורות הזוגיות על n איברים אז

$$A_{n-1} \leq H \leq A_n$$

או

$$, H = S_{n-2} \times_{C_2} S_2$$

והמקרה השני מתרחש רק כאשר טיפוס ההסתעפות של $\Omega^{A_{n-1}}/\mathbb{C}(t)$ נמצא ברשימה ספציפית של אפשרויות. במקרה ש-G היא חבורת התמורות הזוגיות על n איברים, תת החבורה H מקבעת שדה מגנוס 0.

אם G היא החבורה הסימטרית על n איברים אז $A_{n-1} \leq H \leq S_n$ אלא אם טיפוס ההסתעפות של $\Omega^{S_{n-1}}/\mathbb{C}(t)$ נמצא ברשימה ספציפית של אפשרויות ואז ייתכן בנוסף ש-

$$.A_{n-2} \lneq H \leq S_{n-2} \times S_2$$

במקרה זה ידוע לכל אחת מהאפשרויות האם הגנוס המתקבל הוא 0, 1 או גדול ממש מ-1.

נראה מספר שימושים במשפט אפיון זה לחקר של פולינומים בשני משתנים מעל שדה המספרים הרציונליים. בהינתן פולינום אי-פריק $f(x,t) \in \mathbb{Q}[x,t]$, נסמן ב-Red_f את קבוצת ההצבות הרציונליות t_0 כך שהפולינום $f(x,t_0)$ פריק כאיבר של $\mathbb{Q}[x]$. לפי משפט אי-הפריקות של הילברט, Hilbert Irreducibility Theorem, המשלים $\mathbb{Q} \setminus \mathrm{Red}_f$ הוא קבוצה אינסופית. משפט האפיון לתתי שדות מגנוס אפס שצוטט לעיל מאפשר להוכיח את הטענה הבאה לגבי הקבוצה Red_f:

משפט:

בהינתן פולינום אי פריק בשני משתנים $f(x,t) \in \mathbb{Q}[x,t]$, נניח שחבורת גלואה של f מעל השדה היא החבורה הסימטרית או חבורת התמורות הזוגיות על n איברים עבור $n > N$ כלשהו, ונניח שקבוצת ההצבות הפריקות Red_f היא אינסופית, אז קיימים פולינומים $g_1, \dots g_r \in \mathbb{Q}[x,t]$ כך שהקבוצה Red_f שווה, עד כדי קבוצה סופית, לקבוצה הבאה:

$$\bigcup_{i=1}^{r} \{t_0 \in \mathbb{Q} : g_i(x,t_0) \text{ has a rational root}\}$$

כאשר $r = 2$ אם טיפוס ההסתעפות של תת השדה של Ω המקובע על ידי מייצב של נקודה אחת אינו ברשימת הטיפוסים יוצאי הדופן מהמשפט המרכזי, ו- $r = 3$ אם הטיפוס המדובר היא ברשימת יוצאי הדופן.

מנין החשיבות לטיפוס ההסתעפות בתת ההרחבה המקובעת על ידי מייצב של נקודה בפעולה של חבורת הגלואה הנתונה על $\{1, \dots, n\}$? בהינתן הרחבת גלואה $\Omega/\mathbb{C}(t)$ עם חבורת גלואה G, ניתן להתאים לכל מקום P של שדה הבסיס תת חבורה D_P ציקלית של G, הנקראת חבורת הפירוק של המקום. ההסתעפות של המקום P בתת השדה של Ω המקובע על ידי תת חבורה $H \leq G$ כלשהי שווה לאורכי המסלולים של חבורת הפירוק

תקציר

תורת השדות עוסקת בחקר מאפיינים של פולינום באמצעות חבורת הגלואה המשוייכת לו. חבורה כזאת מהווה חבורת תמורות, וכך ניתן להשתמש בכלים מהעולם של חקר חבורות תמורות - לחקר פולינומים. הרחבת שדות, שחבורת הגלואה שלה היא החבורה הסימטרית על n איברים עבור n כלשהו, נקראת הרחבה סימטרית. הרחבת שדות, שחבורת הגלואה שלה היא חבורת התמורות הזוגיות על n איברים עבור n כלשהו, נקראת הרחבה מתחלפת. כאשר מתבוננים בהרחבות שדות של שדות פונקציות, כלומר, כאשר מתבוננים בחבורות גלואה של פולינומים בשני משתנים $f(x,t) \in \mathbb{C}[x,t]$ מעל שדה בסיס $\mathbb{C}(t)$, נוספים עוד שני כלים הקשורים בחקר של שדות פונקציות: ההסתעפות והגנוס, וזאת במובנם בהקשר של משטחי רימן קומפקטיים. בהינתן הרחבת כלשהי של שדות פונקציות (לאו דווקא הרחבת גלואה), הגנוס של השדות בהרחבה מקושר לדרגת ההרחבה ולהסתעפות בה באמצעות נוסחת רימן-הורביץ.

בעבודה זו נבדוק, בהינתן הרחבה סימטרית או מתחלפת מדרגה גבוהה דיה, אילו תתי שדות שלה הם מגנוס 0 או 1. לתתי שדות כאלה תכונות מיוחדות: ראשית, ממשפט Lüroth נובע ששדה פונקציות מעל המרוכבים הוא מגנוס אפס אם ורק אם הוא רציונלי, כלומר, שדה של פונקציות רציונליות במשתנה כלשהו. בנוסף, משפט Faltings קובע, שלעקום יש אינסוף נקודות רציונליות אם ורק אם הוא מגנוס 0 או 1. אם כן, כל אימת שניתן לנסח תכונה כלשהי במונחים של תתי שדות של הרחבה עם אינסוף מקומות רציונליים, מידע על זהות תתי השדות מגנוס 0 או 1 יעזור לנתח את אותה תכונה. תתי שדות כאלו מופיעים באופן טבעי מעקרון שובך היונים, היות שלכל מקום של שדה הפונקציות הרציונליות מעל המרוכבים יש מקום רציונלי מעליו בתת שדה כלשהו של Ω, ויש מספר סופי של תתי שדות; אבל בנוסף תתי שדות כאלה גם מופיעים כאשר לפולינום אי פריק בשני משתנים יש אינסוף הצבות שנותנות פולינום פריק.

המשפט המרכזי שנוכיח הוא כדלהלן:

משפט:

קיים קבוע N כך שאם $\Omega/\mathbb{C}(t)$ היא הרחבת גלואה שחבורת הגלואה שלה G היא החבורה הסימטרית או חבורת התמורות הזוגיות על n איברים, כאשר $n > N$, ו- H היא תת חבורה של G המקבעת שדה מגנוס 0 או 1, אז H היא אחת מהאפשרויות להלן:

המחקר בוצע בהנחייתו של מרצה בכיר דני נפטין, בפקולטה למתמטיקה.

אני מודה לטכניון ולמענקים ISF 577/15 ו- BSF 2014173 על התמיכה הכספית הנדיבה בהשתלמותי.

תתי שדות מגנוס 0 של הרחבות סימטריות ומתחלפות

חיבור על מחקר

לשם מילוי חלקי של הדרישות לקבלת התואר
מגיסטר למדעים במתמטיקה

טלי מונדרר

הוגש לסנט הטכניון — מכון טכנולוגי לישראל
סיון התשע"ח חיפה מאי 2018

תתי שדות מגנוס 0 של הרחבות סימטריות ומתחלפות

טלי מונדרר