An L_3-U_3-quotient algorithm for finitely presented groups

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften
der RWTH Aachen University zur Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Mathematiker

Sebastian Georg Reinhold Jambor

aus Engelskirchen

Berichter: Universitätsprofessor Dr. Wilhelm Plesken
Universitätsprofessorin Dr. Gabriele Nebe

Tag der mündlichen Prüfung: 17.07.2012

Contents

1 Introduction 5

2 The L_2-quotient algorithm 11
- 2.1 Representations of free groups . . . 12
- 2.2 Representations and ideals . . . 15
- 2.3 Actions on representations, trace tuples and ideals . . . 16
- 2.4 Detecting epimorphisms onto proper subgroups . . . 16
- 2.5 From ring quotients to group quotients . . . 18
- 2.6 The algorithms . . . 19

3 Characters of group representations 23
- 3.1 Absolute irreducible representations . . . 24
- 3.2 Actions on representations and characters . . . 25
- 3.3 Detecting certain subgroups of $\mathrm{GL}(n, K)$ . . . 26
- 3.4 Detecting certain subgroups of $\mathrm{PSL}(n, K)$ . . . 27

4 The L_3-U_3-quotient algorithm 31
- 4.1 Representations of free groups . . . 32
  - 4.1.1 Trace polynomials . . . 32
  - 4.1.2 The quadratic relation . . . 34
  - 4.1.3 A generating set for $K^{3\times 3}$ . . . 38
  - 4.1.4 Deciding absolute irreducibility . . . 41
- 4.2 Representations and ideals . . . 41
- 4.3 Actions on representations, trace tuples and ideals . . . 42
- 4.4 Detecting epimorphisms onto proper subgroups . . . 44
- 4.5 From ring quotients to group quotients . . . 49
- 4.6 The algorithms . . . 49
  - 4.6.1 Handling non-maximal prime ideals . . . 51

5 Theoretical consequences 53
- 5.1 A generalization of Lubotzky's One For Almost All Theorem . . . 53
- 5.2 L_3-ideals of positive Krull dimension . . . 54

6 Examples 57
- 6.1 Groups with finitely many quotients of L_3-type . . . 57
  - 6.1.1 A detailed example . . . 57
  - 6.1.2 The Coxeter presentations $(2, m, n; k)$ . . . 59

6.1.3 Modifying presentations of simple groups . . . 59
6.2 Finitely many quotients in almost every characteristic . . . 60
6.2.1 One-relator quotients of the modular group . . . 60
6.2.2 Coxeter presentations . . . 63
6.3 Infinitely many quotients in one characteristic . . . 66
6.3.1 Counting quotients . . . 66
6.3.2 Adding relators . . . 71

7 Counting generators 73
7.1 Generator pairs of order 2 and order 4 . . . 73
7.1.1 The formula for $\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n)$ . . . 76
7.1.2 The formula for $\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n)$ . . . 79
7.2 Generator pairs of order 2 and order 3 . . . 80
7.2.1 The formula for $\mathrm{pgu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$ . . . 83
7.2.2 The formula for $\mathrm{pgl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$ . . . 84
7.2.3 The formula for $\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$ . . . 85
7.2.4 The formula for $\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$ . . . 87

8 Implementation of the quotient algorithms 91
8.1 Orbits of sign systems . . . 91
8.1.1 Degree 2 . . . 91
8.1.2 Degree 3 . . . 92
8.2 Split up words . . . 93
8.3 Words with powers . . . 93
8.4 Presentations with short and long relations . . . 94

9 Computation of minimal associated primes 97
9.1 Theoretical background . . . 97
9.2 The algorithms . . . 99
9.3 An alternative method to compute the necessary primes . . . 100
9.4 Minimal associated prime ideals in the quotient algorithms . . . 102

Index 103

Bibliography 105

Chapter 1

Introduction

This thesis presents an L$_3$-U$_3$-quotient algorithm for finitely presented groups on two generators. Given a finitely presented group $G = \langle g_1, g_2 \,|\, r_1(g_1, g_2), \ldots, r_k(g_1, g_2)\rangle$, it finds all quotients of G which are isomorphic to one of the groups $\mathrm{PSL}(3, q)$, $\mathrm{PSU}(3, q)$, $\mathrm{PGL}(3, q)$, or $\mathrm{PGU}(3, q)$. This is done simultaneously for any prime power q, so q is not part of the input of the algorithm, but the algorithm finds all possible choices of q by itself.
The motivation for this algorithm is the desire to understand finitely presented groups. Although these groups are easy to define, they raise a series of hard problems which are unsolvable in general. One of the most famous problems is the word problem, first formulated by Dehn ([Deh11]): given a finitely presented group G on generators $g_1, \ldots, g_n$ and a word w in the g_i, decide whether w represents the identity element in G. It was proved by Novikov [Nov55] and Boone [Boo58] that the word problem is unsolvable in general. In fact, Boone proves that there exists a finitely presented group on two generators and 32 relations which has an unsolvable word problem. The unsolvability of the word problem implies in particular that it is in general not possible to prove whether a finitely presented group G contains any non-trivial elements at all.

Some historical background

Although one of the fundamental problems, namely deciding equality of two elements, is undecidable for finitely presented groups in general, there are various methods to investigate those groups.

Methods for constructing normal forms

One of the oldest methods is the Todd-Coxeter coset enumeration ([TC36]): given a finitely presented group G which is finite, it will, given enough time and memory, enumerate all elements of G. It is not an algorithm in the usual sense, since it will not terminate if it is given an infinite group. Furthermore, there are no complexity bounds on the memory or time requirements. Another method in this direction is the Knuth-Bendix rewriting ([KB70]). Like the coset enumeration, it is not guaranteed to terminate, and even if it terminates, it may run arbitrarily long. Unlike the coset enumeration, it does not enumerate all elements and can therefore in some cases also handle infinite groups. A third method comprises automatic group techniques ([EHR91]). These combine Knuth-Bendix rewriting and methods from finite state automata theory to construct normal forms for elements. As the Knuth-Bendix rewriting, this approach also can in some cases handle infinite groups.

Quotient algorithms for soluble groups

The methods described so far all try to describe the full group. If this is possible, the word problem and some of the other problems can be solved. In fact, if the finitely presented group is in fact finite, it is often possible to determine a composition series for it, cf. e.g. [CHN12]. The quotient algorithms take another approach. Instead of trying to gather information about the full group, they only check whether the group in question has certain quotients, i.e., normal subgroups such that the quotient has a certain structure. While this only gives partial information about the group, it has the advantage that those methods are algorithms in the usual sense, so they are guaranteed to terminate. In some cases, information about a quotient already suffices to decide some of the hard problems. For example, if a word does not represent the identity element in the quotient, it cannot represent the identity element in the original group.

The simplest of these algorithms is the abelian quotient algorithm. It works by computing the Smith normal form of a certain integer matrix, and is often taught in undergraduate algebra courses. More sophisticated methods are several nilpotent quotient algorithms ([Wam74], [Mac86], [HN80]), finite soluble quotient algorithms ([Ple87], [Nie94]), and polycyclic quotient algorithms ([BCM81], [Lo96]), which compute the biggest finite nilpotent, finite soluble, or polycyclic quotient, respectively, in case it exists. But if the group G is perfect, all of those quotients are trivial.

Quotient algorithms for non-soluble quotients. The L_2-quotient algorithm

There is a very easy method to handle non-soluble quotients. Given any finite group H, it is easy to check whether it is a quotient of G. This works by running over all generator tuples of H and checking whether the relations of G are satisfied. This naive approach is in principle independent of H, and works very well for groups of small order. However, if the order of H becomes reasonably large, it becomes infeasible. Another disadvantage is that it only works for one group H at a time.

The first approach which tests for an infinite family of non-soluble groups whether they occur as quotients of a given finitely presented group is the L_2-quotient algorithm of Plesken and Fabiańska ([PF09]). This tests whether $\mathrm{L}_2(q)$ is a quotient of a given finitely presented group on two or three generators, and it does this simultaneously for any prime power q. In particular, it can check whether G has infinitely many quotients which are isomorphic to some $\mathrm{L}_2(q)$, and enumerates them all.

The L_3-U_3-quotient algorithm

Almost all of the groups $\mathrm{L}_2(q)$ are in fact simple groups, and more generally, the groups $\mathrm{L}_n(q)$ are simple for all $n \geq 2$ and all prime powers q, except for $(n, q) \in \{(2, 2), (2, 3)\}$. So naturally the next step in the development of quotient algorithms is to design an L_3-quotient algorithm. Note that the groups $\mathrm{L}_3(q^2)$ contain another finite simple group, namely the group $\mathrm{U}_3(q)$. The algorithm works by constructing homomorphisms into $\mathrm{L}_3(q^k)$ and removing those homomorphisms which map onto proper subgroups. Since one of those subgroups is $\mathrm{U}_3(q)$, the design of an L_3-quotient algorithm inherently involves the design of an U_3-quotient algorithm, leading to an L_3-U_3-quotient algorithm.

Short description of the L_3-U_3-quotient algorithm

There are two main ideas of the L_2-quotient algorithm and the L_3-U_3-quotient algorithm. The first idea is an old idea from representation theory: a lot of information about a representation can already be read off of the traces of the images, i.e., of the character of the representation. While in the classical theory this is used primarily for representations of finite groups over fields of characteristic zero, it still remains an invaluable tool for representations of infinite groups over arbitrary fields if one restricts to absolutely irreducible representations. Looking at the character only has the further advantage that the minimal field over which a representation is realizable can always be read off, since for finite fields it coincides with the field generated by the character values. The second idea is that of trace polynomials. If $\Delta\colon F_2 \to \mathrm{SL}(3,K)$ is a representation of the free group of rank 2, then for any word $w \in F_2$ the trace of $\Delta(w)$ can be expressed as a polynomial in finitely many traces. Furthermore, this polynomial is independent of Δ and of K. This allows to translate the relations of the finitely presented group into relations of a polynomial ring, thereby translating concepts from non-commutative group theory to concepts of commutative algebra. Solutions of the system of polynomial equations then lead to representations of the finitely presented group.

The role of commutative algebra

The main tool in commutative algebra are Gröbner bases. The concept of a Gröbner basis is very similar to the Knuth-Bendix rewriting: both methods construct normal forms using certain rewriting rules. But while the Knuth-Bendix rewriting process is never guaranteed to terminate, there are algorithms to compute Gröbner bases which always terminate. This already indicates that it is much more pleasant to work in the commutative setting than in the non-commutative setting.

For the L_2-quotient algorithm and the L_3-U_3-quotient algorithm, the central mechanism from commutative algebra is an algorithm to compute the minimal associated primes over an polynomial ring with coefficients in the integers. An algorithm to accomplish this was developed by Fabiańska in [Fab09] for the L_2-quotient algorithm. This approach however is too slow for the L_3-U_3-quotient algorithm. Therefore, parts of the algorithm are replaced by new methods in this thesis, which are also of interest outside of group theory.

Generalizing the L_n-quotient algorithms

It is natural to ask whether the algorithms can be generalized in two directions. First, to allow finitely presented groups on more than two generators, and second, to L_n-quotient algorithms for $n \geq 4$. Unfortunately, both directions seem infeasible. The formulation of the algorithm needs a presentation for certain invariant rings, cf. Section 4.1. Although these rings are always finitely generated by a theorem of Donkin ([Don92]), the number of generators becomes too large for practical purposes. For an L_3-quotient algorithm on three generators, a presentation of the invariant ring $K[\mathrm{SL}(3,K)^3]^{\mathrm{SL}(3,K)}$ is needed, where K is an arbitrary algebraically closed field and $\mathrm{SL}(3,K)$ acts by simultaneous conjugation on $\mathrm{SL}(3,K)^3$. Such a presentation has not been constructed yet, but Lopatin shows in [Lop04] that the invariant ring $K[(K^{3\times 3})^3]^{\mathrm{GL}(3,K)}$ has a minimal generating set of 48 generators if $\mathrm{char}(K) \neq 3$. The ring has Krull dimension 19, so there are a lot of relations among the generators, which are explicitly computed in [Hog12] for $K = \mathbb{C}$. Although these results concern a bigger ring, the corresponding results for the ring $K[\mathrm{SL}(3,K)^3]^{\mathrm{SL}(3,K)}$ can be expected to be of a similar nature.

For an L_4-quotient algorithm on two generators, a presentation of $K[\mathrm{SL}(4,K)^2]^{\mathrm{SL}(4,K)}$ is needed. Here, even less is known. In [DS06], a minimal generating set of $K[(K^{4\times 4})^2]^{\mathrm{GL}(4,K)}$ consisting of 32 elements is given for $K = \mathbb{C}$, and in [DLS09] some relations are computed.

Considering that the runtime of the L_3-U_3-quotient algorithm compared to the L_2-quotient algorithm is already fairly high, where the L_2-quotient algorithm is based on a presentation of the invariant ring on three generators without any relations, and the L_3-U_3-quotient algorithm is based on a presentation with nine generators and one relation, it is hard to believe that an L_4-quotient algorithm on two generators or an L_3-quotient algorithm on three generators would terminate in reasonable time for any non-trivial examples.

Outline

Here is an outline of this thesis. In Chapter 2, the L_2-quotient algorithm by Plesken and Fabiańska is presented. This serves two purposes. First, it presents the main ideas of the algorithm, which are the same as for the L_3-U_3-quotient algorithm, but they are much easier to present in degree 2. Second, it shows several techniques the proofs of which are specific to degree 2. This gives the proper motivation to generalize and prove these techniques in Chapter 3. Although they are used here only for the L_3-U_3-quotient algorithm, they seem to be of general interest. For example, an absolutely irreducible representation of an arbitrary group over an arbitrary field is uniquely determined by its character, and many properties of the representation can easily be read off of the character.

Chapter 4 presents the L_3-U_3-quotient algorithm. This chapter parallels the structure of Chapter 2, which emphasizes the general similarities of both algorithms.

The methods developed for the L_3-U_3-quotient algorithm can be applied to prove a generalization of a theorem of Lubotzky. This is done in Chapter 5. Furthermore, some general results can be proved about finitely presented groups with infinitely many quotients isomorphic to some $\mathrm{L}_3(q)$ or $\mathrm{U}_3(q)$.

In Chapter 6 the algorithm is applied to several examples of finitely presented groups. The main focus here are groups with infinitely many quotients of L_3-type. Using some general techniques, a precise enumeration of all quotients can be given.

The next chapter deals with an interesting combinatorial problem first raised by P. Hall in [Hal36] to count the number of generators of a given group or a family of groups, where the generators have a prescribed order. Explicit formulæ for four families of groups can be given, which seem to be unknown up to now.

The last two chapters deal with the implementation of the L_2-quotient algorithm and the L_3-U_3-quotient algorithm on the computer. Chapter 8 focuses on the group theoretic side, while Chapter 9 is concerned with the commutative algebra, namely the computation of minimal associated prime ideals of an ideal in a polynomial ring over an Euclidean domain. These results are also of general interest outside of quotient algorithms.

Acknowledgments

I would like to express my gratitude to my supervisor Professor Plesken. His constant support and interest are invaluable, and his excitement for mathematics is truly contagious.

I am also grateful to Daniel Robertz, who would always answer all questions concerning commutative algebra. Particularly helpful were several discussions about the computation of minimal associated prime ideals.

I would like to thank Steve Donkin, who gave me the proof of Proposition 4.5, which is essential for the L$_3$-U$_3$-quotient algorithm. While he visited Aachen he also taught me some invariant theory of matrices, in particular the trace calculus involved. This simplified some of the proofs of Section 4.1.

During a stay at the University of Sydney I also had some very helpful and interesting discussions with Allan Steel, for which I am very thankful. While the results of these discussions do not show in this thesis directly, they show in the implementation of the algorithms in Magma. Furthermore, some of Allan's optimizations in Magma lead to a huge speed-up of the L$_3$-U$_3$-quotient algorithms, making the computation of examples possible which were infeasible before.

I would also like to thank Eamonn O'Brien for reading Chapter 3 and making several helpful comments and suggestions, and Wolfgang Krass for proof-reading the thesis for typographical errors.

Finally, I would like to thank my colleagues at Lehrstuhl B for a very pleasant working atmosphere.

Chapter 2

The L_2-quotient algorithm

In this chapter, the L_2-quotient algorithm of Plesken and Fabiańska, cf. [PF09], is presented. Given a finitely presented group G on two generators, it computes all quotients of G which are isomorphic to one of the groups $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$ simultaneously for all prime powers q. Although the results in this chapter are basically all contained in [PF09], I decided to repeat them in this place for various reasons.

First, the algorithm will be generalized in Chapter 4 to an L_3-U_3-quotient algorithm. While many of the ideas of the L_2-quotient algorithm can be adapted to the L_3-U_3-quotient algorithm, there are all kinds of complications and pitfalls to overcome. It is easier to see and to understand these complications with a thorough understanding of the L_2-quotient algorithm. Moreover, the presentation here details the bare essentials of the algorithm, while in [PF09] there are already various optimizations which are not adaptable to degree 3. By focusing on the essential parts, it is easier to see the parallels of the two algorithms. To make the analogies even more apparent, the structures of Chapter 2 and Chapter 4 are the same, so for each part of the algorithm one can see directly how the theory translates from degree 2 to degree 3.

Another reason of the presentation here is that several results of [PF09] can be generalized to representations of arbitrary groups of arbitrary degree, cf. Chapter 3. For example, the fact that an absolutely irreducible representation $F_2 \to \mathrm{SL}(2, K)$ is uniquely determined by its character, up to conjugacy, has a direct generalization.

The outline of this chapter is as follows. Every homomorphism $G \to \mathrm{PSL}(2, q)$ of a finitely generated group G lifts to a representation $F_m \to \mathrm{SL}(2, q)$, where F_m is the free group on m generators. Section 2.1 is a detailed study of these representations, with the primary focus on the case $m = 2$. The main result is that the character of these representations can be calculated by knowing only three prescribed values. Conversely, for any tuple of three prescribed values there exists a representation whose character affords exactly these values; if the representation is absolutely irreducible, then it is unique, up to equivalence.

Roughly speaking, the algorithm works by translating the relations of a finitely presented group to relations of a polynomial ring in such a way that not too much information is lost. The mechanism to do this is described in Section 2.2. In Section 2.3 various actions on representations, characters and ideals are defined, which are needed for the rest of the chapter. Section 2.1 links representations to triples of traces; in Section 2.4 these triples are used to get information about the image of the representation.

Section 2.5 proves a correspondence between quotients of the finitely presented group and quotients of the polynomial ring, which finally leads to the formulation of the algorithm in

Section 2.6.

2.1 Representations of free groups

In this section representations of free groups with values in $\mathrm{SL}(2,K)$ are studied, where the main focus is on the case of free groups of rank 2. All of the results can also be generalized to free groups of rank 3, cf. [Fab09], but since the point of this chapter is to lay the foundations of the L$_3$-U$_3$-quotient algorithm, which only works for two generator groups, the case of rank 3 is not presented here.

One of the most important ideas of the algorithm is to reduce every statement about a representation $\Delta\colon F_2 \to \mathrm{SL}(2,q)$ to a statement about the three character values

$$t := (\mathrm{Tr}(\Delta(g_1)), \mathrm{Tr}(\Delta(g_2)), \mathrm{Tr}(\Delta(g_1 g_2))),$$

where g_1 and g_2 are generators of F_2. The results in this section give the theoretical background to why this is possible.

The character $\chi_\Delta\colon F_2 \to \mathbb{F}_q\colon g \mapsto \mathrm{Tr}(\Delta(g))$ can be described by the three values in t. More precisely, every character value can be expressed as a polynomial of these three values, and this polynomial is independent of Δ and q. Actually, this result can be proved in a more general setting, cf. Theorem 2.1.

Moreover, for any three values $t = (t_1, t_2, t_{12}) \in \mathbb{F}_q^3$, there exists a representation $\Delta\colon F_2 \to \mathrm{SL}(2,\overline{\mathbb{F}_q})$ with the prescribed character values, and it is unique in case Δ is absolutely irreducible.

Some of these results have already been studied before. In case of the characters of representations of F_2 with values in $\mathrm{SL}(2,\mathbb{C})$, the results go as far back as 1897, when they were asserted by Fricke and Klein, cf. [FK65]. Considerable work on the triples of traces was also done by Macbeath, cf. [Mac69]. Where possible, I tried to list references to existing results and how they relate to the results given here.

As mentioned above, the following theorem was already asserted by Fricke and Klein in [FK65] for the case $\mathrm{SL}(2,\mathbb{C})$, but the first rigorous proof was given by Horowitz in [Hor72], which is constructive and valid for $\mathrm{SL}(2,R)$, where R is any commutative ring. A considerably shorter proof was given in [PF09], using the rule

$$\mathrm{Tr}(A^2B) = \mathrm{Tr}(A)\,\mathrm{Tr}(AB) - \mathrm{Tr}(B), \tag{2.1}$$

which holds for all $A, B \in \mathrm{SL}(2,R)$. We will also make use of the equation

$$\mathrm{Tr}(ABC) = \mathrm{Tr}(A)\,\mathrm{Tr}(BC) + \mathrm{Tr}(B)\,\mathrm{Tr}(AC) + \mathrm{Tr}(C)\,\mathrm{Tr}(AB) - \mathrm{Tr}(A)\,\mathrm{Tr}(B)\,\mathrm{Tr}(C) - \mathrm{Tr}(ACB), \tag{2.2}$$

which holds for all $A, B, C \in \mathrm{SL}(2,R)$, cf. [Hor72].

Theorem 2.1 ([Hor72, Theorem 3.1], [PF09, Lemma 2.1]). *Let F_n be the free group on the generators $g_1, \dots, g_n$. Let*

$$\Phi := \{\varphi\colon \{1,\dots,k\} \to \{1,\dots,n\} \mid k \in \mathbb{N}, \varphi \textit{ strictly increasing}\}.$$

For every $\varphi \in \Phi$ let x_φ be an indeterminate over $\mathbb{Z}$.

For every word $w \in F_n$ there exists a polynomial $p_w \in S := \mathbb{Z}[x_\varphi \,|\, \varphi \in \Phi]$, such that for any commutative ring R and any representation $\Delta\colon F_n \to \mathrm{SL}(2,R)$ we have

$$\mathrm{Tr}(\Delta(w)) = \varepsilon_\Delta(p_w),$$

where $\varepsilon_\Delta\colon S \to R$ is the evaluation map which sends x_φ to $\mathrm{Tr}(\Delta(g_{\varphi(1)} \cdots g_{\varphi(k)}))$.

Proof (cf. [PF09, Lemma 2.1]). We can assume that w is cyclically reduced. Furthermore, note that the trace does not change if the letters of w are permuted cyclically. We will proceed by induction on the length of w. There is nothing to prove if w is of the form $g_{i_1} \cdots g_{i_k}$ with $i_1 < \cdots < i_k$. Furthermore, if $w = g_i^{-1}$ for some i, we can set $p_w := x_i$, since $\mathrm{Tr}(A^{-1}) = \mathrm{Tr}(A)$ for all $A \in \mathrm{SL}(2,R)$. Assume first that some letter $x \in \{g_1, \ldots, g_n\}$ occurs with a negative exponent in w; we can assume that $w = x^{-1}v = x^{-2}xv$ for some $v \in F_n$. Because of equation (2.1) we can set $p_w := p_x p_v - p_{xv}$, so we are reduced to the case where all exponents are positive. Next, assume that w is of the form $w = xyxv$ with $x \in F_n - \{1\}$ and $y, v \in F_n$. Then $w = (xy)^2 y^{-1} v$, and again using equation (2.1) we can set $p_w := p_{xy} p_{xv} - p_{y^{-1}v}$. We are left to deal with the case where w is of the form $w = g_{i_1} \cdots g_{i_k}$ where the i_j are pairwise distinct. We can assume $i_1 < i_j$ for all $j \in \{2, \ldots, k\}$. If $i_1 < \cdots < i_k$, we are done. Otherwise, let j be the smallest index with $i_j > i_{j+1}$. Set $w_1 := g_{i_1} \cdots g_{i_{j-1}}$, $w_2 := g_{i_j}$, and $w_3 := g_{i_{j+1}} \cdots g_{i_k}$, so $w = w_1 w_2 w_3$. Then by equation (2.2) we can set $p_w := p_{w_1} p_{w_2 w_3} + p_{w_2} p_{w_1 w_3} + p_{w_3} p_{w_1 w_2} - p_{w_1} p_{w_2} p_{w_3} - p_{w_1 w_3 w_2}$. Either $w_1 w_3 w_2$ is of the desired form, or we repeat this process. This terminates after finitely many steps. □

Definition 2.2. The polynomials p_w in the last theorem are called **generalized Chebyshev polynomials** or **trace polynomials**.

In general, there are various choices for p_w. For example, if $n = 3$, then p_1 can be chosen both as 2 and as

$$\begin{aligned} x_{123}^2 + (x_1x_2x_3 - x_1x_{12} - x_2x_{13} - x_3x_{12})x_{123} + x_1^2 + x_2^2 + x_3^2 + x_{12}^2 + x_{23}^2 + x_{13}^2 \\ - x_1x_2x_{12} - x_1x_3x_{13} - x_2x_3x_{23} + x_{12}x_{23}x13 - 2, \end{aligned}$$

cf. [PF09, Theorem 2.3]. The reason is that the trace of a product of three matrices satisfies a quadratic relation in terms of traces of products of fewer matrices. However, in the case $n = 2$ the result is optimal in the following sense.

Theorem 2.3 ([PF09, Theorem 2.2])**.** *For $n = 2$ and any $w \in \mathbb{F}_2$, the polynomial p_w satisfying the property of Theorem 2.1 is unique.*

Proof ([PF09, Theorem 2.2]). Define a representation $\Delta\colon F_2 \to \mathrm{SL}(2, \mathbb{Q}(\alpha,\beta,\gamma))$ by

$$g_1 \mapsto \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix}, \; g_2 \mapsto \begin{pmatrix} 0 & -1 \\ 1 & \gamma \end{pmatrix},$$

where $\mathbb{Q}(\alpha,\beta,\gamma)$ is the function field over $\mathbb{Q}$. Since $\alpha + \alpha^{-1}, \gamma, \beta + \alpha^{-1}\gamma$ are algebraically independent, this proves the uniqueness. □

This uniqueness is the reason that any triple $t \in \mathbb{F}_q^3$ occurs as traces of some representation. While the proof of the next theorem does not show this reason, it has the advantage that it gives an explicit representation. The connection between the uniqueness of the trace polynomials and the existence of representations will be apparent in Chapter 4.

Definition 2.4. Let K be a field. Then a triple $t = (t_1, t_2, t_{12}) \in K^3$ is called a **trace tuple** of K. If $\Delta\colon F_2 \to \mathrm{SL}(2, \overline{K})$ is a representation with $\mathrm{Tr}(\Delta(g_1)) = t_1$, $\mathrm{Tr}(\Delta(g_2)) = t_2$, and $\mathrm{Tr}(\Delta(g_1g_2)) = t_{12}$, then Δ is said to **afford** the trace tuple t.

Theorem 2.5 ([Mac69, Theorem 1], [PF09, Proposition 3.1])**.** *Let K be any field, and let $t = (t_1, t_2, t_{12}) \in K^3$ be a trace tuple. There exists a representation $\Delta\colon F_2 \to \mathrm{SL}(2, \overline{K})$ affording t. Moreover, if Δ is absolutely irreducible, there exists a representation with values in $\mathrm{SL}(2, K)$ affording t.*

Proof ([PF09, Proposition 3.1]). Let α be a root of $X^2 - t_1X + 1$. The representation

$$\Delta\colon F_2 \to \mathrm{SL}(2, \overline{K})\colon g_1 \mapsto \begin{pmatrix} \alpha & t_2(\alpha - t_1) + t_{12} \\ 0 & t_1 - \alpha \end{pmatrix},\ g_2 \mapsto \begin{pmatrix} 0 & -1 \\ 1 & t_2 \end{pmatrix}$$

satisfies the hypothesis. The last statement is an immediate consequence of Wedderburn's Theorem. □

Remark 2.6. Macbeath actually proves that there always is a representation over K (not only over the algebraic closure), if K is a finite field. However, his prove uses ternary quadratic forms and some geometric arguments, whereas the proof above is very elementary.

By Wedderburn's Theorem, the images of an absolutely irreducible representation $\Delta\colon F_2 \to \mathrm{SL}(2, K)$ form a generating set of $K^{2\times 2}$. In degree 2 we can even give a precise description of the images which will form a basis, which can be used to give a criterion for Δ to be absolutely irreducible, based only on the trace tuple.

Lemma 2.7 ([PF09, Proposition 3.1])**.** *Let K be any field and $\Delta\colon F_2 \to \mathrm{SL}(2, K)$ a representation. Then Δ is absolutely irreducible if and only if $(I_2, \Delta(g_1), \Delta(g_2), \Delta(g_1g_2))$ is a basis of $K^{2\times 2}$.*

Proof. Assume that Δ is absolutely irreducible. Let $X_i := \Delta(g_i)$. Then $K^{2\times 2}$ has a basis consisting of words in X_1 and X_2. Since X_1 and X_2 do not commute, the triple (I_2, X_1, X_2) is linearly independent. Suppose (I_2, X_1, X_2, X_1X_2) is linearly dependent. By the Cayley-Hamilton Theorem,

$$0 = (X_1{+}X_2)^2 - (\mathrm{Tr}(X_1){+}\mathrm{Tr}(X_2))(X_1{+}X_2) + I_2 = X_1X_2 + X_2X_1 - \mathrm{Tr}(X_1)X_2 - \mathrm{Tr}(X_2)X_1 - 2I_2,$$

so (I_2, X_1, X_2, X_2X_1) is linearly dependent. But then every word in X_1 and X_2 can be reduced to a linear combination of I_2, X_1, X_2, which is a contradiction. □

Theorem 2.8 ([Mac69, Theorem 2], [BH95, Proposition 4.1], [PF09, Proposition 3.1])**.** *Let $\Delta\colon F_2 \to \mathrm{SL}(2, K)$ be a representation with traces $t := (t_1, t_2, t_{12}) := (\Delta(g_1), \Delta(g_2), \Delta(g_1g_2))$. Then Δ is absolutely irreducible if and only if t is not a zero of $\rho := x_1^2 + x_2^2 + x_{12}^2 - x_1x_2x_{12} - 4$.*

Proof ([PF09, Proposition 3.1]). Write the 2×2-matrices $\Delta(w)$ as 4×1-vectors; then ρ is the determinant of $(I_2, \Delta(g_1), \Delta(g_2), \Delta(g_1g_2))$. □

Remark 2.9. Macbeath again proves this for finite fields K, and his condition involves the non-singularity of a ternary quadratic form, which is however equivalent to the condition given in the theorem. Brumfiel and Hilden consider the more general case where K is a commutative ring, where the condition is that ρ specializes to a unit in K.

Following the motto that properties of representations should be expressed as properties of the trace tuples, it makes sense to call a trace tuple absolutely irreducible.

Definition 2.10. Let $t = (t_1, t_2, t_{12}) \in K^9$ be a trace tuple. Then t is called **absolutely irreducible** if t is not a zero of ρ.

An important result of ordinary representation theory is that the representation of a finite group is uniquely determined, up to equivalence, by its character. This result holds only in characteristic zero and is false in general. However, if one assumes that the representation in question is absolutely irreducible, then the result can be generalized, as in the next theorem. A further generalization is given in the next chapter.

Theorem 2.11 ([Mac69, Theorem 3], [BH95, Proposition 4.5], [PF09, Proposition 3.1])**.** *Let $\Delta, \Delta' \colon F_2 \to \mathrm{SL}(2, K)$ be absolutely irreducible representations with*

$$(t_1, t_2, t_{12}) := (\Delta(g_1), \Delta(g_2), \Delta(g_1g_2)) = (\Delta'(g_1), \Delta'(g_2), \Delta'(g_1g_2)).$$

Then Δ and Δ' are $\overline{K}$-equivalent.

Proof ([PF09, Proposition 3.1]). Let $v \in \overline{K}^{2\times 1}$ be an eigenvector of $\Delta(g_1)$. Since Δ is absolutely irreducible, $(v, \Delta(g_2)v)$ is linearly independent. With respect to this basis, Δ is equivalent to the representation given in the proof of Theorem 2.5. Similarly, Δ' is equivalent to the same representation. □

2.2 Representations and ideals

In this section fix a finitely presented group $G = \langle g_1, g_2 \,|\, r_1, \ldots, r_k \rangle$ on two generators with the relations $r_1, \ldots, r_k$. The aim is to find all epimorphisms of G onto groups of the form $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$, where q is a prime power. This is done by translating the group relations into relations for the polynomial ring $\mathbb{Z}[x_1, x_2, x_{12}]$, yielding the so-called trace presentation ideals. Proposition 2.13 shows that the trace triples of absolutely irreducible representations are zeroes of these ideals.

Note that every homomorphism $\delta \colon G \to \mathrm{PSL}(2, q)$ is induced by a representation $\Delta \colon F_2 \to \mathrm{SL}(2, q)$ such that $\Delta(r_i) = s_i I_2$ with $s_i \in \{\pm 1\}$ for all $i = 1, \ldots, k$.

Definition 2.12. Let $G = \langle g_1, g_2 \,|\, r_1, \ldots, r_k \rangle$ and $s \in \{\pm 1\}^k$. Then the **trace presentation ideal** of G with respect to s is defined as

$$I_s(G) := \langle p_{r_i h} - s_i p_h \,|\, h \in \{1, g_1, g_2, g_1 g_2\}, i \in \{1, \ldots, k\} \rangle \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}].$$

An element $s \in \{\pm 1\}^k$ is called a **sign system** for G.

Proposition 2.13 ([PF09, Proposition 3.3])**.** *Let $\Delta \colon F_2 \to \mathrm{SL}(2, q)$ be an absolutely irreducible representation with trace tuple $t = (t_1, t_2, t_{12})$. Then Δ induces a homomorphism $G \to \mathrm{PSL}(2, q)$ if and only if t is a zero of a trace presentation ideal $I_s(G)$ for some $s \in \{\pm 1\}^k$.*

Proof. Δ induces a homomorphism $G \to \mathrm{PSL}(2, q)$ if and only if all relations are satisfied, i.e., if and only if $\Delta(r_i(g_1, g_2)) = s_i I_2$ for some $s_i \in \{\pm 1\}$ for $1 \leq i \leq k$. But $\Delta(r_i(g_1, g_2)) = s_i I_2$ is equivalent to $S(\Delta(r_i(g_1, g_2)), \Delta(h)) = S(s_i I_2, \Delta(h))$ for all $h \in \{1, g_1, g_2, g_1 g_2\}$, where $S \colon K^{2\times 2} \times K^{2\times 2} \to K$ is the trace bilinear form, since $(I_2, \Delta(g_1), \Delta(g_2), \Delta(g_1 g_2))$ is a basis of $K^{2\times 2}$, by Lemma 2.7. This proves the proposition. □

2.3 Actions on representations, trace tuples and ideals

Different epimorphisms $F_2 \to \mathrm{SL}(2,q)$ can lead to the same epimorphism $F_2 \to \mathrm{PSL}(2,q)$, up to automorphisms of $\mathrm{PSL}(2,q)$. To describe which trace tuples lead to equivalent epimorphisms $F_2 \to \mathrm{PSL}(2,q)$, it is most convenient to introduce the action of two groups. Roughly speaking, the action of the sign changes accounts for the fact that we deal with $\mathrm{PSL}(2,q)$ instead of $\mathrm{SL}(2,q)$, while the action of the Galois group accounts for the part of the outer automorphism group of $\mathrm{PSL}(2,q)$ which does not come from matrix conjugation.

Definition 2.14. Set $\Sigma := \{\pm 1\}^2$, the group of **sign changes**. If $\Delta\colon F_2 \to \mathrm{SL}(2,q)$ is a representation, define a representation ${}^{\sigma}\Delta$ for $\sigma = (\sigma_1, \sigma_2) \in \Sigma$ by

$$ {}^{\sigma}\Delta\colon F_2 \to \mathrm{SL}(2,q)\colon g_1 \mapsto \sigma_1\Delta(g_1),\ g_2 \mapsto \sigma_2\Delta(g_2). $$

This defines an action of Σ on the set of representations $F_2 \to \mathrm{SL}(2,q)$ and induces actions on the set of characters and the set of trace tuples. To be more precise, if $t := (t_1, t_2, t_{12}) \in \mathbb{F}_q^3$ is a trace tuple,

$$ {}^{\sigma}t = (\sigma_1 t_1, \sigma_2 t_2, \sigma_1\sigma_2 t_{12}). $$

Furthermore, Σ acts on $\mathbb{Z}[x_1, x_2, x_{12}]$ via ring automorphisms by setting

$$ {}^{\sigma}x_1 := \sigma_1 x_1,\ {}^{\sigma}x_2 := \sigma_2 x_2,\ {}^{\sigma}x_{12} := \sigma_1\sigma_2 x_{12}, $$

and this action induces an action on the set of ideals of $\mathbb{Z}[x_1, x_2, x_{12}]$.

Definition 2.15. Let $\Gamma := \mathrm{Gal}(\mathbb{F}_q)$. If $\Delta\colon F_2 \to \mathrm{SL}(2,q)$ is a representation, define a representation ${}^{\gamma}\Delta$ for $\gamma \in \Gamma$ by

$$ {}^{\gamma}\Delta\colon F_2 \to \mathrm{SL}(2,q)\colon g \mapsto \gamma(\Delta(g)). $$

This defines an action of Γ on the set of representations $F_2 \to \mathrm{SL}(2,q)$ and induces actions on the set of characters and the set of trace tuples.

Remark 2.16. There is a bijection between the maximal ideals of $\mathbb{Z}[x_1, x_2, x_{12}]$ and the $\mathrm{Gal}(\mathbb{F}_q)$-orbits of trace tuples $t = (t_1, t_2, t_{12}) \in \mathbb{F}_q^3$, where q ranges over all prime powers as follows: Given a trace tuple $t = (t_1, t_2, t_{12}) \in \mathbb{F}_q^3$ such that t generates $\mathbb{F}_q/\mathbb{F}_p$, let $\mathfrak{t}$ be kernel of the ring epimorphism defined by $\mathbb{Z}[x_1, x_2, x_{12}] \to \mathbb{F}_q\colon x_i \mapsto t_i$. Conversely, if $\mathfrak{t} \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}]$ is a maximal ideal, then $\mathbb{Z}[x_1, x_2, x_{12}]/\,\mathfrak{t} \cong \mathbb{F}_q$ for some prime power q. Let $\varphi\colon \mathbb{Z}[x_1, x_2, x_{12}] \to \mathbb{F}_q$ be the corresponding epimorphism, and set $t = (\varphi(x_1), \varphi(x_2), \varphi(x_{12}))$, which is well-defined up to $\mathrm{Gal}(\mathbb{F}_q)$-conjugacy. Note for example that t is a zero of an ideal $I \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}]$ if and only if I is contained in $\mathfrak{t}$.
This bijection respects the action of Σ on the trace tuples and on the ideals of $\mathbb{Z}[x_1, x_2, x_{12}]$. We will use this correspondence in the following to switch between trace tuples and maximal ideals, without explicitly mentioning it.

2.4 Detecting epimorphisms onto proper subgroups

Let $t = (t_1, t_2, t_{12}) \in \mathbb{F}_q$ be a trace tuple with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(2,q)$. The aim of this section is to decide whether Δ induces an epimorphism onto $\mathrm{PSL}(2,q)$ or $\mathrm{PGL}(2,q)$, based solely on t. This can be done using Dickson's classification of subgroups of $\mathrm{PSL}(2,q)$.

Proposition 2.17 (Dickson, cf. e.g. [Hup67, Hauptsatz II.8.27]). *Let $U \leq \mathrm{SL}(2,q)$ be an absolutely irreducible subgroup such that the character values generate $\mathbb{F}_q$. Denote by $\overline{U}$ the image in $\mathrm{PSL}(2,q)$. Then one of the following cases occurs.*

1. *$\overline{U}$ is isomorphic to A_4, S_4, or A_5. Following [Hor72], these groups are called **exceptional**.*
2. *$\overline{U}$ is a dihedral group.*
3. *$\overline{U}$ is isomorphic to $\mathrm{PGL}(2,r)$ if $q = r^2$ is a square.*
4. *$\overline{U} = \mathrm{PSL}(2,q)$.*

Absolute irreducibility of Δ can be decided using Theorem 2.8, so assume in the following that Δ is absolutely irreducible. By Dickson's result, this leaves only finitely many possibilities for the image of the induced projective representation.
For the exceptional groups A_4, S_4, and A_5 one can use the fact that they can be presented by $\langle g_1, g_2 \mid g_1^2, g_2^3, (g_1g_2)^k\rangle$ with $k \in \{3,4,5\}$ and the fact that the order of an element $x \in \mathrm{SL}(2,q)$ is already determined by the trace, if $(|x|, q) = 1$.

Proposition 2.18 ([PF09, Lemmas 3.7 – 3.9]). *Let $t = (t_1, t_2, t_{12})$ be an absolutely irreducible trace tuple with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(2,q)$. Then the induced projective representation maps onto a group isomorphic to A_4 if and only if one of the t_i is zero and the other are ± 1, or all t_i are ± 1 with an even number of -1. Equivalently, t is the zero of one of the 12 ideals $\langle x_1 - \zeta_1, x_2 - \zeta_2, x_{12} - \zeta_{12}\rangle \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}]$, where $\zeta_1, \zeta_2, \zeta_{12} \in \{-1, 0, 1\}$ such that either $\zeta_1\zeta_2\zeta_{12} = -1$, or exactly one of them is zero.*
Similarly, there are 18 ideals for S_4 and 76 ideals for A_5.

The connection between element orders and traces also gives a test for the dihedral groups, since group elements x and y generate a dihedral group if and only if two of the three elements x, y, xy have order 2.

Proposition 2.19 ([PF09, Lemma 3.6]). *Let $t = (t_1, t_2, t_{12})$ be an absolutely irreducible trace tuple with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(2,q)$. Then the induced projective representation maps onto a dihedral group if and only if two entries of t are zero. Equivalently, t is a zero of one of the ideals $\langle x_1, x_2\rangle$, $\langle x_1, x_{12}\rangle$, $\langle x_2, x_{12}\rangle \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}]$.*

Given a representation $\Delta\colon F_2 \to \mathrm{SL}(2,q)$ with trace tuple $t = (t_1, t_2, t_{12}) \in \mathbb{F}_q$ such that t generates $\mathbb{F}_q/\mathbb{F}_p$, the results above can be used to decide whether Δ is absolutely irreducible, and in case it is, whether the induced projective representation maps onto A_4, S_4, A_5, or a dihedral group. If q is even or not a square, this implies that the induced projective representation maps onto $\mathrm{PSL}(2,q)$. Otherwise, it is possible that the image of the induced projective representation is is the full PGL over the subfield of index 2. There are various criteria to decide which case occurs.

Proposition 2.20 ([PF09, Algorithm 4.2, Remark 4.3]). *Let $t = (t_1, t_2, t_{12})$ be an absolutely irreducible trace tuple such that t_1, t_2, t_{12} generate $\mathbb{F}_q/\mathbb{F}_p$, and assume that $q = r^2$ is an odd square. Furthermore, assume that the trace tuple is not dihedral (cf. Proposition 2.19). The following are equivalent:*

1. *The induced projective representation maps onto a subgroup of $\mathrm{PGL}(2,r)$.*

2. *There exists a subgroup $U = \langle u_1, u_2, u_3 \rangle \leq F_2$ of index 2 such that $p_{u_i}(t) \in \mathbb{F}_r$ for $i = 1, \ldots, 3$, where p_{u_i} is the trace polynomial of Theorem 2.1.*

3. *There exists $1 \neq \sigma \in \Sigma$ such that ${}^\sigma t = {}^\gamma t$, where $\gamma \in \operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_r)$ is the Frobenius.*

4. *The maximal ideal of $\mathbb{Z}[x_1, x_2, x_{12}]$ corresponding to t (cf. Remark 2.16) has a non-trivial stabilizer in Σ.*

Remark 2.21. The first three statements of the proposition are equivalent without the assumption that the trace tuple is not dihedral. However, we will use the fourth statement for the L$_2$-algorithm and the corresponding generalization for the L$_3$-U$_3$-algorithm.

2.5 From ring quotients to group quotients

Let G be a finitely presented group on two generators. The aim of the L$_2$-quotient algorithm is to enumerate all quotients G/N which are isomorphic to $\mathrm{PSL}(2,q)$ or $\mathrm{PGL}(2,q)$, for some prime power q. Now $G/N \cong H$ if and only if there exists an epimorphism $\varphi\colon G \to H$ with $N = \ker\varphi$, and if $\psi\colon G \to H$ is another epimorphism, $\ker\varphi = \ker\psi$ if and only if ψ and φ differ only by an automorphism of H. The results of this section show that the decision whether two representations lead to the same quotient can again be done based on the trace tuple alone.

First note that the automorphism groups of the classical groups are well-known.

Remark 2.22. Every automorphism α of $\mathrm{PSL}(2,q)$ can be written as $\alpha = f \circ d \circ i$, where i is an inner, d a diagonal, and f a field automorphism, cf. [Ste60]. Since $\mathrm{PSL}(2,q) \leq \mathrm{PGL}(2,q) \trianglelefteq \operatorname{Aut}(\mathrm{PSL}(2,q))$, this also implies the same result if α is an automorphism of $\mathrm{PGL}(2,q)$.

Proposition 2.23. *Let $\Delta_i\colon F_2 \to \mathrm{SL}(2,q)$ be absolutely irreducible representations inducing homomorphisms $\delta_i\colon F_2 \to \mathrm{PSL}(2,q)$, for $i = 1,2$. Assume that either both δ_i are surjective, or $q = r^2$ is a square and the images of δ_i are both isomorphic to $\mathrm{PGL}(2,r)$. Then $\ker\delta_1 = \ker\delta_2$ if and only if ${}^\gamma\Delta_1 \sim {}^\sigma\Delta_2$ for some $\gamma \in \Gamma = \operatorname{Gal}(\mathbb{F}_q)$ and $\sigma \in \Sigma$. If t_i is the trace tuple corresponding to Δ_i, this is equivalent to ${}^\gamma t_1 = {}^\sigma t_2$.*

Proof. Assume ${}^\gamma\Delta_1 \sim {}^\sigma\Delta_2$, i.e., there exists $X \in \mathrm{GL}(2,q)$ with $X \cdot {}^\gamma\Delta_1(g) \cdot X^{-1} = {}^\sigma\Delta_2(g)$ for all $g \in G$ Since X can be written as $X = D \cdot I$ with $I \in \mathrm{SL}(2,q)$ and $D \in \mathrm{GL}(2,q)$ a diagonal matrix, this proves that ${}^\gamma\Delta_1 \sim {}^\sigma\Delta_2$ if and only if $\delta_1 = \alpha \circ \delta_2$ for some $\alpha \in \operatorname{Aut}(\mathrm{PSL}(2,q))$, by the last remark. In particular, ${}^\gamma\Delta_1 \sim {}^\sigma\Delta_2$ implies $\ker\delta_1 = \ker\delta_2$.

Now assume conversely $\ker\delta_1 = \ker\delta_2$. If both δ_i are surjective, they differ only by an automorphism of $\mathrm{PSL}(2,q)$, so ${}^\gamma\Delta_1 \sim {}^\sigma\Delta_2$ for some $\gamma \in \operatorname{Gal}(\mathbb{F}_q)$ and some $\sigma \in \Sigma$ by the argument above. If the images of both δ_i are isomorphic to $\mathrm{PSL}(2,r)$, they differ by an automorphism of $\mathrm{PGL}(2,r)$ (there is only one conjugacy class of subgroups of $\mathrm{PSL}(2,q)$ isomorphic to $\mathrm{PGL}(2,r)$, so after applying an inner automorphism, we can in fact assume that the images are equal). We have to show that this automorphism extends to an automorphism of $\mathrm{PSL}(2,q)$. Let $\alpha \in \operatorname{Aut}(\mathrm{PGL}(2,r))$ with $\delta_1 = \alpha \circ \delta_2$. Then $\alpha = f \circ d \circ i$, where i is inner, d is diagonal, and f is a field automorphism of $\mathbb{F}_r$. For i and d the extension to $\mathrm{PSL}(2,q)$ is immediate. Furthermore, f extends to an automorphism $\widetilde{f}$ of $\mathbb{F}_q$ such that $\sqrt{f(a)} = \pm\widetilde{f}(\sqrt{a})$ for all $a \in \mathbb{F}_r$, where $\sqrt{f(a)}$ and $\sqrt{a}$ denote arbitrary roots of $X^2 - f(a)$ and $X^2 - a$, respectively. But $\mathrm{PGL}(2, r)$ embeds into $\mathrm{PSL}(2, q)$ via

$$\mathrm{PGL}(2, r) \to \mathrm{PSL}(2, q) \colon \overline{M} \mapsto \overline{\frac{1}{\sqrt{\det(M)}} M},$$

so $\widetilde{f} \circ d \circ i$ is an extension of $\alpha = f \circ d \circ i$. □

Corollary 2.24. *For every quotient $G/N \cong \mathrm{PSL}(2, q)$ or $G/N \cong \mathrm{PGL}(2, q)$ there exists exactly one Σ-orbit of maximal ideals of $\mathbb{Z}[x_1, x_2, x_{12}]$, where each ideal contains some trace presentation ideal $I_s(G)$.*

Proof. This follows by Remark 2.16 and Propositions 2.13 and 2.23. □

Remark 2.25. Let $I_s(G) \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}]$ be a trace presentation ideal and $\mathfrak{t} \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}]$ a maximal ideal containing it. Then $\mathfrak{t}$ also contains the radical of $I_s(G)$. But the radical is the intersection of the minimal associated prime ideals, i.e., the set of minimal elements of all prime ideals containing $I_s(G)$. This set is finite and can be computed effectively, cf. Chapter 9. Since $\mathfrak{t}$ is prime and contains an intersection of the minimal associated prime ideals, it must already contain one of those ideals. Thus, no information is lost by considering only the minimal associated prime ideals of $I_s(G)$.

The minimal associated prime ideals give more precise information about the zeroes of $I_s(G)$. For example, it can be read off of the prime ideal whether all zeroes are not absolutely irreducible, in which case the prime ideal can be disregarded. Similar considerations hold for the zeroes yielding dihedral or exceptional groups. If all remaining prime ideals are maximal, this already proves that G has only finitely many quotients which are isomorphic to some $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$.

2.6 The algorithms

By Remark 2.16, every maximal ideal of $\mathbb{Z}[x_1, x_2, x_{12}]$ gives rise to a representation $\Delta \colon F_2 \to \mathrm{SL}(2, q)$, but this representation does not necessarily induce an epimorphism onto $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, \sqrt{q})$. It is convenient to have a notation for those ideals which give rise to epimorphisms.

Definition 2.26. A prime ideal $P \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}]$ is called an L_2**-ideal**, if it does not contain the irreducibility indicator ρ of Theorem 2.8 and none of the ideals of Propositions 2.18 and 2.19.

A set Λ of L_2-ideals is called **minimal**, if no ideal of Λ contains a Σ-conjugate of another element of Λ. In other words, $P \not\supseteq {}^{\sigma}Q$ for all $\sigma \in \Sigma$ and all $P, Q \in \Lambda$ with $P \neq Q$.

Algorithm 2.27 (L_2-quotients, [PF09, Algorithm 4.1])**.** *Input:* A finitely presented group

$$G = \langle g_1, g_2 \mid r_1, \ldots, r_k \rangle$$

on two generators.

Output: A minimal set Λ of L_2-ideals satisfying the following property. If $\Delta \colon F_2 \to \mathrm{SL}(2, q)$ with $q > 5$ is a representation with trace tuple t inducing an epimorphism of G onto $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, \sqrt{q})$, then ${}^{\sigma}t$ is a zero of an ideal in Λ for some $\sigma \in \Sigma$.

Algorithm:

1. Compute the set $\mathcal{P}'$ of all minimal associated prime ideals of $I_s(G)$, where $s \in \{\pm 1\}^k$ ranges over all sign systems. Let $\mathcal{P}$ be the set of all minimal elements of $\mathcal{P}'$ with respect to inclusion.

2. Choose a set of representatives $\mathcal{R}$ of $\mathcal{P}$ under the action of Σ.

3. Return all elements of $\mathcal{R}$ which do not lead to reducible representations or to epimorphisms onto A_4, S_4, A_5, or a dihedral group.

Remark 2.28.

1. The condition $q > 5$ in the algorithm comes from the fact that $\mathrm{L}_2(2) \cong \mathrm{D}_6$ is a dihedral group, $\mathrm{L}_2(3) \cong \mathrm{A}_4$, and $\mathrm{L}_2(4) \cong \mathrm{L}_2(5) \cong \mathrm{A}_5$. The algorithm could be adapted to include also these groups, but for the ease of the presentation and the implementation I decided against this. Furthermore, these small groups can be easily found by other methods anyway.

2. Although in step 1 the minimal associated primes are calculated, it is again necessary to take the minimal elements $\mathcal{P}$ of $\mathcal{P}'$. The reason lies in characteristic 2: a prime ideal which contains 2 can contain two different trace presentation ideals $I_s(G)$ and $I_{s'}(G)$.

3. For an efficient implementation, it is not advisable to compute the minimal associated prime ideals of all trace presentation ideals $I_s(G)$, since many of them are removed in step 2 of the algorithm. Instead, one should try to anticipate the action of Σ in step 2 already in step 1, i.e., compute a set of elements of Σ which are really necessary. See [PF09] or Chapter 8 for details.

4. An efficient method to compute the minimal associated primes of an ideal in $\mathbb{Z}[x_1, x_2, x_{12}]$ is presented in Chapter 9 below.

5. Every maximal ideal returned by the algorithm corresponds to a unique L_2-quotient. On the other hand, every prime ideal P which is not maximal corresponds to infinitely many L_2-quotients, but not every maximal ideal $\mathfrak{t}$ containing P will necessarily give an L_2-quotient. There are still possibilities for $\mathfrak{t}$ to yield reducible representations, or quotients isomorphic to A_4, S_4, A_5, or dihedral groups. However, there are infinitely many maximal ideals giving L_2-images, and if P has dimension 1, usually a precise enumeration of the corresponding L_2-quotients can be given. Cf. [PF09, Section 8] for details or Chapter 5, where the analogous results for the L_3-U_3-quotient algorithm are proved.

Every maximal ideal returned by Algorithms 2.27 gives rise to a quotient isomorphic to $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$. The following algorithm, based on Proposition 2.20, decides which case occurs.

Algorithm 2.29 (L_2-type, [PF09, Algorithm 4.2])**.** *Input:* A maximal ideal $\mathfrak{t} \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}]$, such that the image of the corresponding projective representation is isomorphic to either $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$ for some prime power q.
Output: The exact isomorphism type of the image.
Algorithm:

1. Let p be the prime contained in $\mathfrak{t}$. Compute the dimension n of the $\mathbb{F}_p$-vector space $\mathbb{F}_p[x_1, x_2, x_{12}]/(\mathbb{F}_p \otimes \mathfrak{t})$.

2. If $p = 2$, if n is odd or if $\mathfrak{t}$ has a trivial stabilizer in Σ, return $\mathrm{PSL}(2, p^n)$. Otherwise, return $\mathrm{PGL}(2, p^{n/2})$.

Given a maximal ideal $\mathfrak{t} \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}]$ it is often desirable to construct a corresponding representation $\Delta \colon F_2 \to \mathrm{SL}(2, q)$, where $\mathbb{F}_q = \mathbb{Z}[x_1, x_2, x_{12}]/\,\mathfrak{t}$. In [Fab09, Algorithm 9], an algorithm is presented to accomplish this. It works by taking the representation of Theorem 2.5; if $X^2 - t_1 X + 1$ is irreducible over $\mathbb{F}_q$, a Galois descent is performed to get a representation over $\mathbb{F}_q$ instead of $\mathbb{F}_{q^2}$.

In Chapter 3, a general algorithm is presented which works for any character of an absolutely irreducible representation.

Chapter 3

Characters of group representations in arbitrary characteristic

The aim of this chapter is to generalize the character theory of Chapter 2 as far as possible. The question is: given a representation $\Delta\colon G \to \mathrm{GL}(n, K)$ with character $\chi_\Delta\colon G \to K\colon g \mapsto \mathrm{Tr}(\Delta(g))$, where G is an arbitrary group, $n \in \mathbb{N}$, and K is an arbitrary field, what can be said about Δ by knowing χ_Δ alone?

For the L_2-quotient algorithm, the character of a representation is the fundamental tool. Theorem 2.11 shows that an absolutely irreducible representation $\Delta\colon F_2 \to \mathrm{SL}(2, K)$ is uniquely determined, up to equivalence, by its character; this result is generalized in Proposition 3.1. Later on in Chapter 2, the character is used to determine whether the corresponding projective representation $F_2 \to \mathrm{PSL}(2, K)$ is surjective, or in case it is not to determine the image.

There are roughly two types of absolutely irreducible subgroups of $\mathrm{PSL}(2, q)$. First, there are the so-called exceptional groups, i.e., groups isomorphic to A_4, S_4, or A_5. For each one of these groups there is a specific test which checks whether it is isomorphic to the image of the projective representation, cf. Proposition 2.18. The other subgroups fall into infinite families of groups. They are the dihedral groups or groups isomorphic to some $\mathrm{PGL}(2, q')$. But although there are infinitely many dihedral groups, there is a uniform way to detect images which are dihedral, cf. Proposition 2.19. The generalizations of the dihedral groups are the imprimitive groups; the result corresponding to Proposition 2.19 is given in Proposition 3.7. Similarly, there is a uniform test for groups isomorphic to some PGL, cf. Proposition 2.20, which can be generalized as in Theorem 3.17.

In the study of representations of higher degree, new families of subgroups arise. For example, the image of a projective representation $F_2 \to \mathrm{PSL}(n, q^2)$ for $n > 2$ can be a subgroup of $\mathrm{PSO}(n, q^2)$ or $\mathrm{PSU}(n, q)$, i.e., the projective orthogonal group or the projective unitary group, respectively. These images did not play a role in the L_2-quotient algorithm, since $\mathrm{PSO}(2, q)$ is a dihedral group and $\mathrm{PSU}(2, q) \cong \mathrm{PSL}(2, q)$. However, for the L_3-U_3-quotient algorithm, or if one studies representations of higher degree, these families of subgroups are important.

Note that by Theorem 2.1, the character of a representation $\Delta\colon F_2 \to \mathrm{SL}(2, K)$ is determined by finitely many character values. In this chapter we will not use this result but instead assume that the character is given as an abstract map. A generalization of Theorem 2.1 for representations of degree 3 will be given in Chapter 4.

3.1 Absolute irreducible representations

The first result is a generalization of Theorem 2.11: it is true in general that an absolutely irreducible representation is uniquely determined by its character, up to equivalence. As usual, if $\Delta\colon G \to \mathrm{GL}(n,K)$ is a representation, write χ_Δ for the corresponding character.

Proposition 3.1. *Let G be a group, K a field, and let $\Delta_i\colon G \to \mathrm{GL}(n,K)$ be absolutely irreducible representations for $i = 1, 2$ such that $\chi_{\Delta_1} = \chi_{\Delta_2}$. Then Δ_1 and Δ_2 are equivalent.*

Proof. Let $\chi = \chi_{\Delta_1} = \chi_{\Delta_2}$, and denote by $\mathrm{rad}(\chi)$ the radical of the bilinear form $KG \times KG \to K\colon (x,y) \mapsto \chi(xy)$. Denote the extension of Δ_i to $KG \to K^{n\times n}$ again by Δ_i. Then $\ker(\Delta_i) \subseteq \mathrm{rad}(\chi)$, and since $KG/\ker(\Delta_i)$ is simple, we see that in fact equality holds. Thus there are isomorphisms $KG/\mathrm{rad}(\chi) \to \Delta_i(KG) = K^{n\times n}$ which are induced by $x \mapsto \Delta_i(x)$. Hence $\Delta_1(x) \mapsto \Delta_2(x)$ is an automorphism of $K^{n\times n}$, which has to be inner by the Skolem-Noether theorem. □

This raises the following question: Let $\Delta\colon F_m \to \mathrm{GL}(n,K)$ be a representation with character $\chi_\Delta =: \chi$. Can the absolute irreducibility of Δ be read off of χ? According to Theorem 2.8, this is possible for representations $\Delta\colon F_2 \to \mathrm{SL}(2,K)$. More precisely, Δ is absolutely irreducible if and only if $(\chi(a), \chi(b), \chi(ab))$ is not a zero of the polynomial $\rho := x_1^2 + x_2^2 + x_{12}^2 - x_1x_2x_{12} - 4$. This can be generalized as follows. Denote by $W_{m,\ell}$ the reduced words of F_m of length at most ℓ, and let $\{x_w \mid w \in W_{m,\ell}\}$ be indeterminates.

Proposition 3.2. *For any $m, n \in \mathbb{N}$ there exists an ideal $\rho_{m,n} \trianglelefteq \mathbb{Z}[x_w \mid w \in W_{m,(n^2-1)^2}]$ such that for any representation $\Delta\colon F_m \to \mathrm{GL}(n,K)$ with character $\chi = \chi_\Delta$ the following are equivalent:*

1. *Δ is absolutely irreducible.*
2. *The tuple $(\chi(w) \mid w \in W_{m,(n^2-1)^2})$ is not a zero of $\rho_{m,n}$.*

Proof. By Wedderburn's Theorem, Δ is absolutely irreducible if and only if the set $\{\Delta(w) \mid w \in F_m\}$ is a generating set for $K^{n\times n}$ as a K-vector space. Note that $\langle\Delta(W_{m,i+1})\rangle = \langle\Delta(W_{m,i})\rangle$ for some i implies $\langle\Delta(W_{m,j})\rangle = \langle\Delta(W_{m,i})\rangle$ for all $j \geq i$. In particular, the chain

$$\langle\Delta(W_{m,0})\rangle \subseteq \langle\Delta(W_{m,1})\rangle \subseteq \cdots$$

stabilizes after at most n^2 steps. Thus Δ is absolutely irreducible if and only if $\Delta(W_{m,n^2-1})$ is a generating system of $K^{n\times n}$. This last condition can be tested with the trace bilinear form $S\colon K^{n\times n} \times K^{n\times n} \to K\colon (a,b) \mapsto \chi(ab)$ as follows. Define the matrix $\Sigma := (S(\Delta(v), \Delta(w)))_{v,w} = (\chi(vw))_{v,w}$, where v and w run through W_{m,n^2-1}. Then Δ is absolutely irreducible if and only if Σ has rank n^2, since the trace bilinear form is non-degenerate. Setting $\rho_{m,n}$ to be the ideal generated by the $n^2 \times n^2$-minors of the matrix $(x_{vw})_{v,w}$, where v and w run through W_{m,n^2-1}, yields the desired result. □

Remark 3.3. The last result is only of theoretical value and not very efficient in applications, since the size of $W_{m,(n^2-1)^2}$ (and therefore the rank of the polynomial ring) grows exponentially with m and n. However, in special applications, the rank of the polynomial ring can be reduced to a practical value. Theorem 2.8 already shows that if $m = n = 2$ and Δ takes values in the special linear group, the number of indeterminates can be assumed to be 3. In the next chapter we will see that if $m = 2$, $n = 3$ and Δ takes values in the special linear group, 9 variables suffice, cf. Proposition 4.2.

By Proposition 3.1, an absolutely irreducible representation is uniquely determined by its character, up to equivalence. Hence it would be good to have a method which constructs the representation, given its character only. Here is a first step into that direction.

Proposition 3.4. *Let G be a finitely generated group, K a field, and $\chi\colon G \to K$ the character of an absolutely irreducible representation $\Delta\colon G \to \mathrm{GL}(n,K)$. Denote by $M = K^{n\times 1}$ the corresponding simple module. It is possible to construct $M^n = M \oplus \cdots \oplus M$ using just χ.*

Proof. We may assume that G is the free group on m generators $g_1, \ldots, g_m$. Let $(B_1, \ldots, B_{n^2})$ be any basis of $K^{n\times n}$. To determine the action of G on $M^n \equiv K^{n\times n}$ it is enough to determine values $\lambda_{ijk} \in K$ such that $\Delta(g_i)B_j = \sum_k \lambda_{ijk}B_k$, where $1 \le i \le m$ and $1 \le j,k \le n^2$. Since the trace bilinear form S is non-degenerate, each λ_{ijk} is uniquely determined by the n^2 equations $S(\Delta(g_i)B_j, B_\ell) = S(\sum_k \lambda_{ijk}B_k, B_\ell)$, where $1 \le \ell \le n^2$.
As in Proposition 3.2, we can choose a tuple of words $w = (w_1, \ldots, w_{n^2}) \in G$ such that $B := (\Delta(w_1), \ldots, \Delta(w_{n^2}))$ is a basis of $K^{n\times n}$, giving the linear equations

$$\chi(g_i \cdot w_j \cdot w_\ell) = \sum_k \lambda_{ijk}\chi(w_k \cdot w_\ell),$$

which only involve values of χ. □

Further techniques have to be applied to decompose the module M^n. For example, if K is a finite field, the Meat Axe (cf. [Par84], [HR94]) is a powerful and efficient tool.

3.2 Actions on representations and characters

As in Chapter 2, most of the results are best expressed using group actions. There is a direct generalization of the actions in Section 2.3, but there is also a new action by a cyclic group of order 2, which acts by inverse transposition.

Definition 3.5. Let $\Delta\colon G \to \mathrm{GL}(n,K)$ be an absolutely irreducible representation with character χ.

1. Define an action of $\mathrm{Gal}(K)$ on the representations of G into $\mathrm{GL}(n,K)$ by

   $${}^{\alpha}\Delta\colon G \to \mathrm{GL}(n,K)\colon g \mapsto \alpha(\Delta(g))$$

   for $\alpha \in \mathrm{Gal}(K)$, where $\alpha(\Delta(g))$ means to apply α entry-wise, and let ${}^{\alpha}\chi$ be the character of ${}^{\alpha}\Delta$.

2. Let $\mathrm{C}_2 = \langle\tau\rangle$ be a cyclic group of order 2 generated by τ. Then τ acts on the representations of G into $\mathrm{GL}(n,K)$ by

   $${}^{\tau}\Delta = \Delta^{-\mathrm{tr}}\colon G \to \mathrm{GL}(n,K)\colon g \mapsto \Delta(g)^{-\mathrm{tr}};$$

   denote by ${}^{\tau}\chi$ the character of ${}^{\tau}\Delta$.

This gives an action of $\mathrm{Gal}(K) \times \mathrm{C}_2$ on the set of absolutely irreducible representations of G. If G is a free group, we have an action by roots of unity. Let $F_m := \mathrm{Fr}(g_1, \ldots, g_m)$ be the free group on the generators $g_1, \ldots, g_m$, and denote by $\mu_n(K)$ the group of n-th roots of unity contained in K. If K is the finite field $\mathbb{F}_q$, we also write $\mu_n(q)$ instead of $\mu_n(K)$.

Definition 3.6. Let $\Delta\colon F_m \to \mathrm{GL}(n,q)$ be a representation with character χ. For $\sigma \in \mu_n(q)^m$ define

$$^{\sigma}\Delta\colon F_m \to \mathrm{GL}(n,q)\colon g_i \mapsto \sigma_i\Delta(g_i),$$

where $\sigma = (\sigma_1, \dots, \sigma_m)$, and define $^{\sigma}\chi$ to be the character of $^{\sigma}\Delta$.

3.3 Detecting certain subgroups of $\mathrm{GL}(n,K)$

Now we are able to describe several families of subgroups of $\mathrm{GL}(n,K)$, based only on the character. The first result is a generalization of Proposition 2.19. In general, it is possible to detect imprimitive groups with cyclic factor groups, i.e., the induced action on some vector space decomposition is cyclic. The dihedral groups correspond to the case where the cyclic group has order 2.

The next two results concern orthogonal, symplectic and unitary subgroups. They did not come up in the context of the L_2-quotient algorithm, since their image in $\mathrm{PSL}(2,q)$ is isomorphic to either a dihedral group, or to some $\mathrm{PSL}(2,q')$.

We begin with the imprimitive groups. Let $\Delta\colon G \to \mathrm{GL}(n,K)$ be an absolutely irreducible representation over an algebraically closed field K, and let $V = K^{n\times 1}$ be the natural KG-module. Assume that Δ is imprimitive, i.e., $V = \bigoplus_{i=1}^{k} V_i$ as vector space such that the action of G on V permutes the V_i. If the induced permutation group on the V_i is cyclic, this can be read off of the character.

Proposition 3.7. *Let K be an algebraically closed field, and let $\Delta\colon G \to \mathrm{GL}(n,K)$ be an absolutely irreducible representation with character χ. Then Δ is imprimitive with cyclic permutation group if and only if there exists a non-trivial homomorphism $\psi\colon G \to \mathrm{C}_n$ such that $\chi(w) = 0$ for all $w \in G$ with $\psi(w) \neq 1$.*

Proof. Let $V = K^{n\times 1}$ be the natural KG-module.

Assume that Δ is imprimitive with cyclic permutation group, i.e., $V \cong \bigoplus_{i=1}^{k} V_i$, and the action of G on the V_i induces an epimorphism $\psi\colon G \to \mathrm{C}_k$. Let $N := \ker\psi$. Then N is the stabilizer of V_1, so V_1 is a KN-module and $V \cong V_1 \otimes_{KN} KG$. After a suitable conjugation, the matrices $\Delta(w)$ are Kronecker products; in particular, $\mathrm{Tr}(\Delta(w)) = 0$ for all $w \in G - N$.

Conversely, assume that $\chi(w) = 0$ for all $w \in G$ with $\psi(w) \neq 1$, where $\psi\colon G \to \mathrm{C}_n$ is a non-trivial homomorphism; let $N := \ker(\psi)$. Suppose V_N is (absolutely) irreducible, so $\Delta(N)$ contains a basis of $K^{n\times n}$. Let $w \in G - N$, and $S\colon K^{n\times n} \times K^{n\times n} \to K$ the trace bilinear form. Then $S(\Delta(w), \Delta(x)) = \chi(wx) = 0$ for all $x \in N$, and since S is non-degenerate, this implies $\Delta(w) = 0$, which is a contradiction. Hence V_N is reducible, so $V_N = V_1 \oplus \cdots \oplus V_k$ for KN-submodules $V_1, \dots, V_k \leq V_N$. Since G/N is cyclic, the V_i are pairwise non-isomorphic and therefore permuted under the action of G by Clifford's Theorem. □

If the field contains enough roots of unity, a representation is imprimitive with cyclic permutation group if and only if the character has a non-trivial stabilizer under the action by the roots of unity.

Corollary 3.8. *Let K be an algebraically closed field of characteristic coprime to n, and let $\Delta\colon F_m \to \mathrm{GL}(n,K)$ be an absolutely irreducible representation of the free group F_m with character χ. Then Δ is imprimitive with cyclic permutation group if and only if $^{\sigma}\chi = \chi$ for some non-trivial $\sigma \in \mu_n(K)^m$.*

Proof. For $\sigma = (\sigma_1, \ldots, \sigma_m) \in \mu_n(K)^m$ define a homomorphism $\psi\colon F_m \to \mathrm{C}_n$ by $g_i \mapsto \sigma_i$. This gives a bijection between the non-trivial elements of $\mu_n(K)^m$ and the non-trivial homomorphisms $F_m \to \mathrm{C}_n$. Furthermore, ${}^{\sigma}\chi(w) = \psi(w)\chi(w)$, so χ is invariant under σ if and only if $\chi(w) = 0$ whenever $\psi(w) \neq 1$. The result follows by the last proposition. □

Specifically for the L_3-U_3-quotient algorithm, we need the following result. The proof is similar to the proof of Proposition 3.7.

Proposition 3.9. *Let K be an algebraically closed field, and let $\Delta\colon G \to \mathrm{GL}(3, K)$ be an absolutely irreducible representation with character χ. Then Δ is imprimitive with permutation group S_3 if and only if there exists a non-trivial homomorphism $\psi\colon G \to \mathrm{S}_3$ such that $\chi(w) = 0$ for all $w \in G$ with $|\psi(w)| = 3$.*

Next are the orthogonal, symplectic and unitary groups.

Proposition 3.10. *Let G be a group, K a field of characteristic $\neq 2$, and $\Delta\colon G \to \mathrm{GL}(n, K)$ an absolutely irreducible representation with character χ such that ${}^{\tau}\chi = \chi$, i.e., $\chi(g) = \chi(g^{-1})$ for all $g \in G$.*
Then there is a symmetric or alternating form on $K^{n\times 1}$ which is invariant under $\Delta(G)$, i.e., Δ is conjugate to an orthogonal or symplectic representation.

Proof. The representations Δ and $\Delta^{-\mathrm{tr}} = (g \mapsto \Delta(g)^{-\mathrm{tr}})$ are absolutely irreducible with the same traces, so by Proposition 3.1 they are equivalent. Let $y \in \mathrm{GL}(n, K)$ such that $y\Delta(g)y^{-1} = \Delta(g)^{-\mathrm{tr}}$ for all $g \in G$. Then

$$\Delta(g) = (\Delta(g)^{-\mathrm{tr}})^{-\mathrm{tr}} = y^{-\mathrm{tr}}y\Delta(g)y^{-1}y^{\mathrm{tr}}$$

for all $g \in G$, so $y^{-\mathrm{tr}}y$ lies in the centralizer of Δ by Schur's Lemma. Hence $y^{-\mathrm{tr}}y = \lambda I_n$ for some $\lambda \in K$. But $y^{\mathrm{tr}} = \lambda y = \lambda^2 y^{\mathrm{tr}}$, so either $\lambda = 1$, in which case y is symmetric, or $\lambda = -1$, in which case y is skew-symmetric. □

Proposition 3.11. *Let G be a group and K a field with an automorphism α of order 2. Let $\Delta\colon G \to \mathrm{GL}(n, K)$ be an absolutely irreducible representation with character χ such that ${}^{\tau}\chi = {}^{\alpha}\chi$, i.e., $\chi(g) = \alpha(\chi(g^{-1}))$ for all $g \in G$. Then Δ is conjugate to a unitary representation.*

Proof. As in the last proposition, there exists $y \in \mathrm{GL}(n, K)$ with $y\Delta(g)y^{-1} = \alpha(\Delta(g)^{-\mathrm{tr}})$ for all $g \in G$, and we have $y = \lambda\alpha(y)^{\mathrm{tr}}$ for some $\lambda \in K$. Applying α to this last equation and transposing gives $\alpha(\lambda)^{-1} = \lambda$, so λ has norm 1 over the fixed field. By Hilbert's Theorem 90, cf. [Lan02], there exists $\mu \in K$ with $\lambda = \alpha(\mu)/\mu$, and by replacing y with μy we can assume that y is Hermitian. □

3.4 Detecting certain subgroups of PSL(n, K)

This section presents a generalization of Proposition 2.20 to arbitrary degree.
Note that the determinant map gives the following subgroups of $\mathrm{GL}(n, q)$ which contain $\mathrm{SL}(n, q)$.

Definition 3.12. For $k|(q-1)$ define

$$\mathrm{GL}^k(n, q) := \{A \in \mathrm{GL}(n, q) \mid \det(A) \in \mathbb{F}_q^{*k}\},$$

i.e., those invertible matrices whose determinant is a k-th power in $\mathbb{F}_q$.

In particular, $\mathrm{GL}^1(n,q) = \mathrm{GL}(n,q)$ and $\mathrm{GL}^{q-1}(n,q) = \mathrm{SL}(n,q)$. These groups give rise to the subgroups $\mathrm{PGL}^k(n,q) := \mathrm{GL}^k(n,q)/\operatorname{Z}(\mathrm{GL}^k(n,q))$ of $\mathrm{PGL}(n,q)$. But whereas the groups $\mathrm{GL}^k(n,q)$ are all pairwise non-isomorphic, the same holds for the groups $\mathrm{PGL}^k(n,q)$ if and only if $\mathbb{F}_q$ contains a primitive n-th root of unity. More precisely, the following holds, as can be seen using the lattice of normal subgroups of $\mathrm{GL}(n,q)$.

Remark 3.13. Let k_1 and k_2 be divisors of $q-1$. Then $\mathrm{PGL}^{k_1}(n,q) \cong \mathrm{PGL}^{k_2}(n,q)$ if and only if $\mathbb{F}_q^{*k_1}\mathbb{F}_q^{*d} = \mathbb{F}_q^{*k_2}\mathbb{F}_q^{*d}$, where $d := (q-1)/(n,q-1)$. In particular, there is a bijection between the divisors k of $(n,q-1)$ and the isomorphism classes of $\mathrm{PGL}^k(n,q)$.

Thus we only have to consider the groups $\mathrm{PGL}^k(n,q)$ with $k|(n,q-1)$. These groups can be embedded into a PSL as follows.

Remark 3.14. Let $k|(n,q-1)$, and let $\ell \in \mathbb{N}$ such that every element in $\mathbb{F}_q^{*k}$ has an n-th root in $\mathbb{F}_{q^\ell}^*$. Then $\mathrm{PGL}^k(n,q)$ embeds into $\mathrm{PSL}(n,q^\ell)$ via

$$\mathrm{PGL}^k(n,q) \hookrightarrow \mathrm{PSL}(n,q^\ell)\colon \overline{M} \mapsto \overline{\sqrt[n]{\mathrm{Det}(M)}^{-1} M}.$$

We will use this embedding to regard $\mathrm{PGL}^k(n,q)$ as a subgroup of $\mathrm{PSL}(n,q^\ell)$.
The action in Definition 3.6 allows us to identify the projective representations into $\mathrm{PSL}(n,q)$ which take values in one of the smaller groups $\mathrm{PGL}^k(n,q')$ defined above. To do this, we use Theorem 3.17 below.
We will need the following elementary lemma.

Lemma 3.15. *If $f = t^\ell - a \in \mathbb{F}_q[t]$, then f has a root in $\mathbb{F}_{q^\ell}$.*

Proof. Proceed by induction on the number of prime factors of ℓ, where the case $\ell = 1$ is trivial. Let r be a prime dividing ℓ, so $\ell = rm$ for some $m \in \mathbb{N}$. Note first that $t^r - a$ has a root α in $\mathbb{F}_{q^r}$: If $(r,q-1) = 1$ then taking r-th powers is an automorphism, so $t^r - a$ already has a root in $\mathbb{F}_q$; otherwise, $\mathbb{F}_q$ has a primitive r-th root of unity, in which case this is a corollary of Hilbert's Theorem 90. Now $t^m - \alpha \in \mathbb{F}_{q^r}[t]$ is a divisor of $t^\ell - a$, and it has a root in $\mathbb{F}_{(q^r)^m} = \mathbb{F}_{q^\ell}$ by the induction hypothesis. □

Recall that $F_m := \mathrm{Fr}(g_1,\ldots,g_m)$ is the free group on the generators $g_1,\ldots,g_m$, and for a representation $\Delta\colon G \to \mathrm{SL}(n,q)$, we denote by $\overline{\Delta}\colon G \to \mathrm{PSL}(n,q)$ the induced projective representation. Furthermore, $\mu_n(q^\ell)$ is the largest subgroup of $\mathbb{F}_{q^\ell}^*$ whose order divides n.
We will also need the norm function defined on $\mu_n(q^\ell)^m$:

Definition 3.16. Let $\ell \in \mathbb{N}$. Define

$$\mathrm{N}\colon \mu_n(q^\ell)^m \to \mu_n(q)^m\colon \sigma = (\sigma_1,\ldots,\sigma_m) \mapsto (\mathrm{N}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}(\sigma_1),\ldots,\mathrm{N}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}(\sigma_m)),$$

where $\mathrm{N}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}\colon \mathbb{F}_{q^\ell}^* \to \mathbb{F}_q^*$ is the norm of $\mathbb{F}_{q^\ell}/\mathbb{F}_q$.

Theorem 3.17. *Let $k|(n,q-1)$, and let $\Delta\colon F_m \to \mathrm{SL}(n,q^\ell)$ be an absolutely irreducible representation with character χ. Then $\overline{\Delta}(F_m)$ is conjugate to a subgroup of $\mathrm{PGL}^k(n,q)$ if and only if ${}^\alpha\chi = {}^\sigma\chi$ for some $\sigma \in \mu_n(q^\ell)^m$ with $\mathrm{N}(\sigma) = 1 = (1,\ldots,1)$ and $k|(n/|\sigma|)$, where α is the Frobenius automorphism of $\mathbb{F}_{q^\ell}/\mathbb{F}_q$.*

Proof. Assume first that $\overline{\Delta}(F_m)$ is conjugate to a subgroup of $\mathrm{PGL}^k(n,q)$. We can assume that it is in fact a subgroup of $\mathrm{PGL}^k(n,q)$, since we are only interested in the traces. Set $X_i := \Delta(g_i)$ for $i = 1,\dots,m$; then there exist $\lambda_i \in \mathbb{F}_{q^\ell}$ and $\widetilde{X}_i \in \mathrm{GL}^k(n,q)$ with $X_i = \lambda_i \widetilde{X}_i$. Furthermore, $\lambda_i^n = \det(\widetilde{X}_i)^{-1} \in \mathbb{F}_q^{*k}$ for all i, so λ_i is an n-th root of an element in $\mathbb{F}_q$. Thus $\alpha(\lambda_i) = \sigma_i\lambda_i$ for some $\sigma_i \in \mu_n(q^\ell)$. The element $\sigma := (\sigma_1,\dots,\sigma_m) \in \mu_n(q^\ell)^m$ satisfies ${}^\alpha\chi = {}^\sigma\chi$, and since $\lambda_i = \alpha^\ell(\lambda_i) = \mathrm{N}(\sigma_i)\lambda_i$ we get $\mathrm{N}(\sigma) = 1$. Finally, $\lambda_i^{|\sigma|} \in \mathbb{F}_q^*$, hence $\lambda_i^n \in \mathbb{F}_q^{*n/|\sigma|}$. It is clear that $\mathbb{F}_q^{*n/|\sigma|}$ is the smallest subgroup of $\mathbb{F}_q^*$ containing $\mathbb{F}_q^{*n}$ and all determinants, so $k|(n/|\sigma|)$.

Now assume conversely ${}^\alpha\chi = {}^\sigma\chi$ for some $\sigma \in \mu_n(q^\ell)^m$ with $\mathrm{N}(\sigma) = 1$ and $k|(n/|\sigma|)$. By Proposition 3.1, ${}^\alpha\Delta$ and ${}^\sigma\Delta$ are equivalent, so $y({}^\sigma\Delta)y^{-1} = {}^\alpha\Delta$ for some $y \in \mathrm{GL}(n,q^\ell)$. For every $w \in F_m$ there exists $\rho \in \mu_n(q^\ell)$ with ${}^\sigma\Delta(w) = \rho\Delta(w)$, and we get

$$\begin{aligned}\Delta(w) &= \alpha^{\ell-1}(y\rho\Delta(w)y^{-1})\\ &= \alpha^{\ell-1}(\rho)\alpha^{\ell-1}(y)\alpha^{\ell-2}(y\rho\Delta(w)y^{-1})\alpha^{\ell-1}(y)^{-1}\\ &= \underbrace{\alpha^{\ell-1}(\rho)\cdots\rho}_{=1}\,\alpha^{\ell-1}(y)\cdots\alpha(y)y\Delta(w)y^{-1}\alpha(y)^{-1}\cdots\alpha^{\ell-1}(y)^{-1}.\end{aligned}$$

Since w is arbitrary and Δ is absolutely irreducible, Schur's Lemma yields $\alpha^{\ell-1}(y)\cdots\alpha(y)y = \lambda I_n$ for some $\lambda \in \mathbb{F}_{q^\ell}$. Applying α to this equation and conjugating with y^{-1}, we see that λ is fixed by α, hence $\lambda \in \mathbb{F}_q$; by replacing y with $\sqrt[\ell]{\lambda}^{-1}y \in \mathrm{GL}(n,q^\ell)$ (which exists according to the lemma) we can assume $\alpha^{\ell-1}(y)\cdots\alpha(y)y = I_n$. But then Hilbert's Theorem 90 for matrices applies (see [GH97, Proposition 1.3]), so there exists $z \in \mathrm{GL}(n,q^\ell)$ with $y = \alpha(z)^{-1}z$. An easy verification shows ${}^\alpha({}^z\Delta) = {}^\sigma({}^z\Delta)$, so for the rest of the proof we can assume ${}^\alpha\Delta = {}^\sigma\Delta$ and we will show $\overline{\Delta}(F_m) \subseteq \mathrm{PGL}^k(n,q)$.

Since $\alpha(\Delta(g_i)) = \sigma_i\Delta(g_i)$ for all i and σ_i has norm 1, there exists $\lambda_i \in \mathbb{F}_{q^\ell}$ with $\alpha(\Delta(g_i)) = \alpha(\lambda_i)\lambda_i^{-1}\Delta(g_i)$ by Hilbert's Theorem 90. Set $X_i := \Delta(g_i)$ and $\widetilde{X}_i := \lambda_i^{-1}X_i$. Then $\alpha(\widetilde{X}_i) = \widetilde{X}_i$, hence $\widetilde{X}_i \in \mathrm{GL}(n,q)$. Furthermore, $\alpha(\lambda_i) = \sigma_i\lambda_i$, so $\lambda_i^{|\sigma|} \in \mathbb{F}_q^*$ and $\lambda_i^n \in \mathbb{F}_q^{*n/|\sigma|} \leq \mathbb{F}_q^{*k}$, hence $\widetilde{X}_i \in \mathrm{GL}^k(n,q)$. In other words, for each word $w \in F_m$, the image $\Delta(w)$ has the form $\sqrt[n]{\det(W)}^{-1}W$ for some $W \in \mathrm{GL}^k(n,q)$. Thus $\overline{\Delta}(F_m) \subseteq \mathrm{PGL}^k(n,q)$. □

In Chapter 4, the last theorem is applied in the following simpler form.

Corollary 3.18. *Let n be prime with $n \nmid q$, and let $\Delta\colon F_m \to \mathrm{SL}(n,q^n)$ be an absolutely irreducible representation with character χ. Then $\overline{\Delta}(F_m)$ is conjugate to a subgroup of $\mathrm{PGL}(n,q)$ if and only if ${}^\alpha\chi = {}^\sigma\chi$ for some $\sigma \in \langle\zeta\rangle^m$, where α is a generator of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ and $\zeta \in \mathbb{F}_{q^n}$ is a primitive n-th root of unity.*

Chapter 4

The L_3-U_3-quotient algorithm

This chapter presents an L_3-U_3-quotient algorithm. Given a finitely presented group on two generators, the algorithm finds all quotients isomorphic to $\mathrm{PSL}(3,q)$, $\mathrm{PSU}(3,q)$, $\mathrm{PGL}(3,q)$, or $\mathrm{PGU}(3,q)$, for any prime power q.

The basic ideas of the L_3-U_3-quotient algorithm are the same as for the L_2-quotient algorithm. First convert the relations of the group into relations of some polynomial ring. Then compute the minimal associated primes and remove all prime ideals which do not give absolutely irreducible representations, or which will lead to epimorphisms onto proper subgroups. To make the analogy of the two algorithms even more apparent, the organization of the sections of this chapter is the same as in Chapter 2.

Here is a more detailed outline. Section 4.1 studies the representations of a free group into $\mathrm{SL}(3,K)$ for an arbitrary field K, and is the longest section of this chapter. First the trace polynomials for degree 3 are introduced, which allow the determination of any character value of a representation $\Delta\colon F_m \to \mathrm{SL}(3,K)$ by knowing only finitely many values. For $m = 2$, the trace polynomials are polynomials in nine variables, but they are not unique. The non-uniqueness stems from a quadratic relation, which is determined later in the section. If this relation is satisfied for a tuple t of nine values in $\mathbb{F}_q$, there exists a representation affording t. The four matrices $(I_2, \Delta(g_1), \Delta(g_2), \Delta(g_1g_2))$ always form a basis of $K^{2\times 2}$ if the representation $\Delta\colon F_2 \to \mathrm{SL}(2,K)$ is absolutely irreducible. The analogue for degree 3 is proved in this first section. Finally, an effective test is developed to decide absolute irreducibility of representations $F_2 \to \mathrm{SL}(3,K)$.

Section 4.2 defines the trace presentation ideals for degree 3, and Section 4.3 defines various actions on representations, trace tuples, and ideals, which play an even more important role than in degree 2.

To decide surjectivity of a projective representation $F_2 \to \mathrm{PSL}(3,q)$, more subgroups have to be considered than in degree 2; this is done in Section 4.4.

Finally, Section 4.5 draws the connection between ring quotients and group quotients, which allows the presentation of the algorithms in the last section.

While the basic ideas are the same for the L_2-quotient and the L_3-U_3-quotient algorithm, there are several complications and new obstacles to overcome on the way to an L_3-U_3-quotient algorithm. Some of them are already mentioned above, and others are mentioned later. One complication however deserves special attention to avoid too much confusion later on. The center of the groups $\mathrm{SL}(3,q)$ plays a central role in the algorithms. It is trivial or generated by ζI_3, where ζ is a primitive third root of unity, in case it exists. To deal with the sign systems uniformly for any characteristic, we need to work with a polynomial ring over $\mathbb{Z}[\zeta]$ instead of $\mathbb{Z}$. However, we also use a bijection between $\mathrm{Gal}(\mathbb{F}_q)$-orbits of trace tuples and maximal ideals of a polynomial ring, cf. Remarks 2.16 and 4.22, which is best dealt with using a polynomial ring over $\mathbb{Z}$. This forces us to switch between two polynomial rings, depending on the context.

4.1 Representations of free groups

The aim of this section is to give a precise description of representations of the free group on two generators into $\mathrm{SL}(3, q)$ for prime powers q.

As seen in Section 2.1, every absolutely irreducible representation $\Delta\colon F_2 \to \mathrm{SL}(2, q)$ is uniquely determined by the traces of the matrices $\Delta(g_1)$, $\Delta(g_2)$, and $\Delta(g_1g_2)$, and for any given triple of field elements there exists a corresponding representation. The results of this section are the corresponding analogues in degree 3.

By Proposition 3.1, every absolutely irreducible representation is uniquely determined by its character, so the first step is to describe the character by finitely many values, using trace polynomials. This can be done for free groups of arbitrary degree. To get unique trace polynomials, further work has to be done, resulting in a quadratic relation for the traces.

While in Section 2.1, given a trace tuple (t_1, t_2, t_{12}) it is easy to write down a representation affording this tuple, this seems not to be possible in degree 3. Instead, we will use invariant theory to prove the existence of such a representation, without actually constructing one.

Another important result of Section 2.1 is that $(I_2, \Delta(g_1), \Delta(g_2), \Delta(g_1g_2))$ is always a basis if Δ is absolutely irreducible; this immediately gives a test whether a representation is absolutely irreducible, based only on the trace tuple. The third part of this section gives a generalization of this important result. While this also gives a test for absolute irreducibility just as in degree 2, this is not efficient in practice. So in the last part, an alternative test is developed.

The theory of the trace polynomials has a tight relationship to the invariant theory of tuples of matrices, acted upon by the general linear group. This topic has a long history, and many results concerning the case of two matrices of degree 3 have been given. The introduction of [Law07a] gives a good overview. Despite of this long history and the long list of results on this topic, I decided to include this section for various reasons. First, the results on this topic so far mostly consider the case of matrices over an algebraically closed field of characteristic zero, while for the L$_3$-U$_3$-quotient algorithm a characteristic free approach is needed. Second, while it should be possible, it is not easy to get a construction for the trace polynomials from the invariant theoretic results, since they only try to give minimal generating sets and are not concerned with the question how any invariant can be written as a polynomial in these generators. And third, the approach presented here seems to be shorter than the results published so far.

4.1.1 Trace polynomials

The first result is the analogue of Theorem 2.1, which introduces the trace polynomials for degree 2 and allows the computation of all character values by the knowledge of only finitely many.

The proof of Theorem 2.1 relies on the two relations (2.1) and (2.2), so what are the appropriate analogues in degree 3? As pointed out to me by Steve Donkin, both (2.1) and (2.2) are consequences of the Cayley-Hamilton Theorem. This result always holds in characteristic zero, i.e., every relation of traces of generic matrices is a consequence of the Cayley-Hamilton Theorem, cf. [Pro76, Theorem 4.6].

Lemma 4.1. *Let R be a commutative ring and $X_1, X_2, X_3 \in \mathrm{SL}(3, R)$. Set $X_{-i} := X_i^{-1}$ for $i \in \{1, 2, 3\}$, and let $t_{i_1,\ldots,i_k} := \mathrm{Tr}(X_{i_1} \cdots X_{i_k})$ for $i_1, \ldots, i_k \in \{\pm1, \pm2, \pm3\}$. The following relations for the traces hold:*

$$t_{1,2,1,3} = t_{-1,2}t_3 + t_{-1,3}t_2 + t_{-1}t_{2,3} + t_{1,2}t_{1,3} - t_{-1}t_2t_3 - t_{-1,2,3} - t_{-1,3,2}$$

and

$$\begin{aligned} t_{1,2,-1,3} + t_{-1,2,1,3} = t_1(t_{-1,2,3} + t_{-1,3,2} - t_2t_{-1,3} - t_3t_{-1,2}) + t_{-1}(t_{1,2,3} + t_{1,3,2} - t_2t_{1,3} - t_3t_{1,2}) \\ + t_{1,2}t_{-1,3} + t_{1,3}t_{-1,2} + (t_1t_{-1} + 1)(t_2t_3 - t_{2,3}) \end{aligned}$$

Proof. Assume first that R is an algebraically closed field of characteristic 0. Let $Y_1, \ldots, Y_4 \in R^{3\times3}$. For $\sigma \in \mathrm{S}_4$ with cycle decomposition $\sigma = (i_1, \ldots, i_k)(i_{k+1}, \ldots, i_\ell)\cdots$ define

$$\mathrm{Tr}_\sigma(Y_1, \ldots, Y_4) := \mathrm{Tr}(Y_{i_1} \cdots Y_{i_k})\,\mathrm{Tr}(Y_{i_{k+1}} \cdots Y_{i_\ell}) \cdots .$$

Then the *fundamental trace relation*

$$\sum_{\sigma\in\mathrm{S}_4} \mathrm{sgn}(\sigma)\,\mathrm{Tr}_\sigma(Y_1, \ldots, Y_4) = 0$$

holds, cf. [Pro76, Theorem 4.3]. Setting $Y_i := X_i$ for $i = 1, 2, 3$ and $Y_4 := X_1^{-1}$ yields the second relation. Setting $Y_i := X_i$ for $i = 1, 2, 3$ and $Y_4 := X_1$, and using the relation $A^2 = A^{-1} + \mathrm{Tr}(A)A - \mathrm{Tr}(A^{-1})I_3$ for all $A \in \mathrm{SL}(3, R)$ yields the first relation. Thus the relations hold if R is an algebraically closed field of characteristic 0.
Next assume that $X_i = (x^i_{jk})_{jk}$ with indeterminates x^i_{jk}, and

$$\widehat{R} = \mathbb{Z}[x^i_{jk} \,|\, 1 \le i, j, k \le 3]/\langle \det(X_i) - 1 \,|\, 1 \le i \le 3\rangle.$$

Regard the X_i as elements of $\mathrm{SL}(3, \widehat{R})$. Since $\widehat{R}$ is an integral domain (each $\det(X_i) - 1$ is irreducible, and the variables of the three polynomials are disjoint), it is embeddable into an algebraically closed field, so the relations hold in this case.
Finally let R and the X_i be arbitrary. We can assume that R is generated as a ring by the entries of the X_i. But then R is an epimorphic image of $\widehat{R}$, hence the relations hold in general. □

Proposition 4.2. *Let F_m be the free group on the generators $g_1, \ldots, g_m$ and $g_{-i} := g_i^{-1}$ for $1 \le i \le m$. Let*

$$\begin{aligned} \Phi := \{\varphi\colon \{1, \ldots, k\} \to \{\pm1, \ldots, \pm m\} \,|\, k \in \mathbb{N}, \varphi \text{ injective}, \varphi(1) < \varphi(i) \text{ for all } i > 1, \\ \varphi(i) + \varphi(i + 1) \ne 0, \varphi(i) < \varphi(j) \text{ for all } i < j \text{ with } \varphi(i) + \varphi(j) = 0\}. \end{aligned}$$

For every $\varphi \in \Phi$ let x_φ be an indeterminate over $\mathbb{Z}$.
For every word $w \in F_m$ there exists a polynomial $p_w \in S := \mathbb{Z}[x_\varphi \,|\, \varphi \in \Phi]$, such that for every commutative ring R and any representation $\Delta\colon F_m \to \mathrm{SL}(3, R)$,

$$\mathrm{Tr}(\Delta(w)) = \varepsilon_\Delta(p_w),$$

where $\varepsilon_\Delta\colon S \to R$ is the evaluation map which sends x_φ to $\mathrm{Tr}(\Delta(g_{\varphi(1)} \cdots g_{\varphi(k)}))$.

Proof. The proof is constructive and works by induction on the length $|w|$ of w.
Let $w = g_{i_1} \cdots g_{i_k}$. Since $\operatorname{Tr}(XY) = \operatorname{Tr}(YX)$ for all $X, Y \in R^{3\times 3}$, we can assume that $i_1 < i_j$ for all $j > 1$. Define $\varphi\colon \{1, \ldots, k\} \to \{\pm 1, \ldots, \pm m\}$ by $\varphi(j) := i_j$. By our assumption $\varphi(1) < \varphi(j)$ for all $j > 1$, and we assume that w is reduced, so $\varphi(i) + \varphi(i+1) \neq 0$ for all i. If $\varphi \in \Phi$, set $p_w := x_\varphi$. If φ is not injective, then the first relation in the preceding lemma can be used to define p_w as a polynomial in the p_v with $|v| < |w|$.
It remains to deal with the case where $\varphi(i) + \varphi(j) = 0$ for some $i < j$ with $\varphi(i) > \varphi(j)$. Let i be minimal with this property. By the second relation of the preceding lemma,

$$\begin{aligned}
\operatorname{Tr}(\Delta(g_{\varphi(1)} \cdots g_{\varphi(k)})) &= \operatorname{Tr}(g_{\varphi(i)} g_{\varphi(i+1)} \cdots g_{\varphi(j-1)} g_{-\varphi(i)} g_{\varphi(j+1)} \cdots g_{\varphi(k)} g_{\varphi(1)} \cdots g_{\varphi(i-1)}) \\
&= -\operatorname{Tr}(g_{-\varphi(i)} g_{\varphi(i+1)} \cdots g_{\varphi(j-1)} g_{\varphi(i)} g_{\varphi(j+1)} \cdots g_{\varphi(k)} g_{\varphi(1)} \cdots g_{\varphi(i-1)}) + q \\
&= -\operatorname{Tr}(g_{\varphi(1)} \cdots g_{\varphi(i-1)} g_{-\varphi(i)} g_{\varphi(i+1)} \cdots g_{\varphi(j-1)} g_{\varphi(i)} g_{\varphi(j+1)} \cdots g_{\varphi(k)}) + q,
\end{aligned}$$

where q is a polynomial in the p_v, with v running over words of length smaller than $|w|$. This process terminates after finitely many steps. □

The p_w of Proposition 4.2 are again called **trace polynomials**.

4.1.2 The quadratic relation

As in Chapter 2, the polynomial p_w in Proposition 4.2 is not unique. While in degree 2 there is at least uniqueness if one restricts to the two generator case, in degree 3 not even this holds. The reason for this is that the traces are not algebraically independent. Note that p_w is a polynomial in the nine variables

$$x_1, x_{-1}, x_2, x_{-2}, x_{1,2}, x_{-1,2}, x_{-2,1}, x_{-2,-1}, x_{-2,1,2,-1} =: x_{[1,2]},$$

corresponding to the traces of the two matrices, their inverses, the products of two matrices, and their commutator. Thus, by Proposition 3.1 an absolutely irreducible representation $\Delta\colon F_2 \to \mathrm{SL}(3, K)$ is uniquely determined, up to equivalence, by the traces of the nine matrices

$$\Delta(g_1), \Delta(g_1^{-1}), \Delta(g_2), \Delta(g_2^{-1}), \Delta(g_1 g_2), \Delta(g_1^{-1} g_2), \Delta(g_2^{-1} g_1), \Delta(g_2^{-1} g_1^{-1}), \Delta([g_1, g_2]),$$

which we will always denote by $t_1, t_{-1}, \ldots, t_{-2,-1}, t_{[1,2]} := t_{-2,1,2,-1}$. However, given nine elements $t_1, \ldots, t_{[1,2]} \in K$, it is not possible in general to find a representation which affords these traces. In fact, $t_{[1,2]}$ satisfies a quadratic relation in the other eight traces. The aim of this subsection is to find this quadratic relation, which will give analogues of Theorems 2.3 and 2.5.
As noted in the introduction, the invariant theory of two 3×3-matrices has a long history, and the following relation for the trace of the commutator already occurs in [Nak02] (in a more general form), and in [Law07b] (for two matrices in $\mathrm{SL}(3, \mathbb{C})$).

Lemma 4.3. *Let R be a commutative ring and $X_1, X_2 \in \mathrm{SL}(3, R)$. Set $X_{-i} := X_i^{-1}$ for $i \in \{1, 2\}$, and let $t_{i_1,\ldots,i_k} := \operatorname{Tr}(X_{i_1} \cdots X_{i_k})$ for $i_1, \ldots, i_k \in \{1, 2\}$ and $t_{[1,2]} := t_{-2,1,2,-1}$. The following relation for the traces holds:*

$$\begin{aligned}
r_{[1,2]} :=& t_{[1,2]}^2 - (t_1 t_{-1} t_2 t_{-2} - t_{-1} t_{-2} t_{1,2} - t_1 t_{-2} t_{-1,2} - t_{-1} t_2 t_{-2,1} - t_1 t_2 t_{-2,-1} \\
&\qquad + t_1 t_{-1} + t_{1,2} t_{-2,-1} + t_2 t_{-2} + t_{-1,2} t_{-2,1} - 3) t_{[1,2]}
\end{aligned}$$

$$
\begin{aligned}
&+ t_1t_{-1}t_2^2t_{-2}^2 + t_1^2t_{-1}^2t_2t_{-2} - t_{-1}^3t_2t_{-2} - t_1t_{-1}t_{-2}^3 - t_1^3t_2t_{-2} - t_1t_{-1}t_2^3\\
&+ t_1^2(t_2^2t_{1,2} + t_{-2}^2t_{-2,1}) + t_{-1}^2(t_{-2}^2t_{-2,-1} + t_2^2t_{-1,2})\\
&- t_1^2(t_{-1}t_2t_{-2,-1} + t_{-1}t_{-2}t_{-1,2}) - t_{-1}^2(t_1t_2t_{-2,1} + t_1t_{-2}t_{1,2})\\
&- t_2^2(t_{-1}t_{-2}t_{-2,1} + t_1t_{-2}t_{-2,-1}) - t_{-2}^2(t_{-1}t_2t_{1,2} + t_1t_2t_{-1,2})\\
&- t_1t_2t_{-2}t_{1,2}t_{-2,1} - t_1t_{-1}t_{-2}t_{-2,1}t_{-2,-1} - t_{-1}t_2t_{-2}t_{-1,2}t_{-2,-1} - t_1t_{-1}t_2t_{1,2}t_{-1,2}\\
&+ t_1^2(t_{-2}t_{1,2} + t_{-1,2}t_{-2,-1} + t_2t_{-2,1}) + t_{-1}^2(t_{-2}t_{-1,2} + t_{1,2}t_{-2,1} + t_2t_{-2,-1})\\
&+ t_2^2(t_1t_{-1,2} + t_{-1}t_{1,2} + t_{-2,1}t_{-2,-1}) + t_{-2}^2(t_{1,2}t_{-1,2} + t_{-1}t_{-2,1} + t_1t_{-2,-1})\\
&+ t_{1,2}^2(t_{-1}t_{-1,2} + t_{-2}t_{-2,1} - 2t_1t_2) + t_{-2,-1}^2(t_1t_{-2,1} + t_2t_{-1,2} - 2t_{-1}t_{-2})\\
&+ t_{-1,2}^2(t_{-2}t_{-2,-1} + t_1t_{1,2} - 2t_{-1}t_2) + t_{-2,1}^2(t_{-1}t_{-2,-1} + t_2t_{1,2} - 2t_1t_{-2})\\
&+ t_1t_{-1}(t_{-1,2}t_{-2,1} + t_{1,2}t_{-2,-1}) + t_2t_{-2}(t_{-1,2}t_{-2,1} + t_{1,2}t_{-2,-1})\\
&+ t_1t_{-1}t_2t_{-2} + t_{1,2}t_{-1,2}t_{-2,1}t_{-2,-1}\\
&+ 3t_1(t_2t_{-2,-1} - t_{1,2}t_{-2,1}) + 3t_2(t_{-1}t_{-2,1} - t_{1,2}t_{-1,2})\\
&+ 3t_{-1}(t_{-2}t_{1,2} - t_{-1,2}t_{-2,-1}) + 3t_{-2}(t_1t_{-1,2} - t_{-2,1}t_{-2,-1})\\
&+ t_1^3 + t_2^3 + t_{-1}^3 + t_{-2}^3 + t_{1,2}^3 + t_{-1,2}^3 + t_{-2,1}^3 + t_{-2,-1}^3\\
&+ 9 = 0,
\end{aligned}
$$

Proof. This can be verified with a simple Gröbner basis calculation over $\mathbb{Z}$. □

Remark 4.4. Exchanging X_1 and X_2 gives a new quadratic relation for $t_{[2,1]} := t_{-2,-1,2,1}$. But the trace is invariant under cyclic permutation of the products (e.g. $t_{2,1} = t_{1,2}$), so in fact all that changes is that $t_{[1,2]}$ is replaced by $t_{[2,1]}$. If $r_{[1,2]}$ is regarded as a quadratic polynomial in the indeterminate $t_{[1,2]}$, this shows that the trace of the commutators and the trace of its inverse are the two zeroes of a quadratic polynomial in traces of lower degree.

In fact, the last remark gives a way to find the relation $r_{[1,2]}$ in the first place, which is a considerably harder task than checking its validity. I will outline two approaches how to do this. Both approaches rely on the following observation. If the trace of the commutator and the trace of its inverse satisfy a quadratic relation, then it is enough to write the sum and the product of the two traces as polynomials in traces of lower degree. Furthermore, to find a candidate of the relation, it is enough to assume that $R = \mathbb{C}$. Note that a relation for the sum of the traces is already given in Lemma 4.1 if X_3 is replaced by X_2^{-1}, so we now focus on the product.

The first approach is due to Nakamoto, who constructs a relation for the traces of two matrices $X_1, X_2 \in R^{3\times 3}$, where R is an arbitrary commutative ring in [Nak02]. First assume that $X_1 = (a_{ij})_{i,j}$ and $X_2 = (b_{ij})_{i,j}$ are matrices of indeterminates over $\mathbb{C}$. Introduce variables $t_{i_1,\dots,i_k}$ for $i_1, \dots, i_k \in \{1,2\}$, where $t_{i_1,\dots,i_k}$ and $t_{j_1,\dots,j_\ell}$ are considered equal if $k = \ell$ and the j's are a cyclic permutation of the i's. Give a bidegree to t_i by counting the i's equal to 1 and 2, respectively; this defines a bigrading on the polynomial ring $\mathbb{C}[t_i \mid i \in \{1,2\}^k,\ k \in \mathbb{N}]$. View $\mathbb{C}^{3\times 3} \times \mathbb{C}^{3\times 3}$ as an affine variety, and identify the coordinate ring $\mathbb{C}[\mathbb{C}^{3\times 3} \times \mathbb{C}^{3\times 3}]$ with the polynomial ring $\mathbb{C}[a_{ij}, b_{ij} \mid 1 \le i,j \le 3]$, which is bigraded in an obvious way (i.e., every a_{ij} has bidegree $(1,0)$, and every b_{ij} has bidegree $(0,1)$). Let $\mathrm{GL}(n,\mathbb{C})$ act by conjugation on $\mathbb{C}^{3\times 3} \times \mathbb{C}^{3\times 3}$, then the invariant ring $\mathbb{C}[\mathbb{C}^{3\times 3} \times \mathbb{C}^{3\times 3}]^{\mathrm{GL}(3,\mathbb{C})}$ is also bigraded and

$$\mathbb{C}[t_i \mid i \in \{1,2\}^k,\ k \in \mathbb{N}] \to \mathbb{C}[\mathbb{C}^{3\times 3} \times \mathbb{C}^{3\times 3}]^{\mathrm{GL}(3,\mathbb{C})} \colon t_i \mapsto \mathrm{Tr}(X_{i_1} \cdots X_{i_k})$$

defines a graded homomorphism. Now a relation for the traces is just an element of the kernel of this map.

The product $\operatorname{Tr}(X_1X_2X_1^2X_2^2)\operatorname{Tr}(X_2X_1X_2^2X_1^2)$ has bidegree $(6,6)$, so any relation involving this product can be assumed to be homogeneous of bidegree $(6,6)$. There are 305 monomials in the t_i of bidegree $(6,6)$, so a relation has to be a linear combination of these monomials. To find the coefficients of this linear combination, simply specify the a_{ij} and b_{ij} to values in $\mathbb{C}$. Every specification gives a linear equation for the t_i, and choosing enough specifications gives a system of linear equations which has a one-dimensional kernel. Solving this equation yields the relation for the product of the traces (see [Nak02] for more details).

The second approach uses Gröbner bases. As noted above, to find the relation, it is enough to assume that $X_1, X_2 \in \mathrm{SL}(3,\mathbb{C})$. Since the trace is invariant under conjugation, we can alter the X_i by simultaneous conjugation. Let v be an eigenvector of X_1. Assume that $\Delta\colon F_2 \to \mathrm{SL}(3,\mathbb{C})\colon g_i \mapsto X_i$ defines an irreducible representation, then (v, X_2v) is linearly independent. We further assume that (v, X_2v, X_1X_2v) is linearly independent, so X_1 and X_2 can be assumed of the form

$$X_1 = \begin{pmatrix} a_{1,1} & 0 & a_{1,3} \\ 0 & 0 & a_{2,3} \\ 0 & 1 & a_{3,3} \end{pmatrix},\ X_2 = \begin{pmatrix} 0 & b_{1,2} & b_{1,3} \\ 1 & b_{2,2} & b_{2,3} \\ 0 & b_{3,2} & b_{3,3} \end{pmatrix}$$

with $a_{ij}, b_{ij} \in \mathbb{C}$. Let t_1 be the trace of X_1, then $a_{3,3} = t_1 - a_{1,1}$. Also, if t_{-1} is the trace of the adjoint of X_1, then $a_{2,3} = (t_1 - a_{3,3})a_{3,3} - t_{-1}$. Similarly, one can replace $a_{1,3}, b_{1,2}, b_{1,3}, b_{2,2}$ by polynomials in $a_{3,3}, b_{2,3}, b_{3,3}, t_1, t_{-1}, t_2, t_{-2}, t_{1,2}, t_{-1,2}, t_{-2,1}$.

Now assume that the a_{ij}, b_{ij}, and t_{ij} are indeterminates. Let

$$R = \mathbb{Q}[a_{3,3}, b_{2,3}, b_{3,3}, t_1, t_{-1}, t_2, t_{-2}, t_{1,2}, t_{-1,2}, t_{-2,1}, t_{-2,-1}],$$

and $I := \langle \det(X_1) - 1, \det(X_2) - 1, \operatorname{Tr}(X_2^{\mathrm{ad}}X_1^{\mathrm{ad}}) - t_{-2,-1}\rangle$. Compute a Gröbner basis of I with respect to a degree inverse lexicographic ordering. The normal form of

$$\operatorname{Tr}(X_1X_2X_1^{\mathrm{ad}}X_2^{\mathrm{ad}})\operatorname{Tr}(X_2X_1X_2^{\mathrm{ad}}X_1^{\mathrm{ad}})$$

is a polynomial in the t_i, so the relation is found.

There is a possible third approach, using the representation theory of the symmetric group. By the Procesi-Razmyslov theory, every relation between the traces in characteristic zero is a consequence of the Cayley-Hamilton Theorem, and there is a tight relationship between the relation of the traces and the symmetric group as follows. Let $X_1, \dots, X_m \in K^{n\times n}$ and $\sigma \in \mathrm{S}_m$. Write $\sigma = (i_1, \dots, i_k)(j_1, \dots, j_\ell)\cdots$ in cycle decomposition, including the cycles of length 1, and define $\operatorname{Tr}_\sigma(X_1, \dots, X_m) := \operatorname{Tr}(X_{i_1}\cdots X_{i_k})\operatorname{Tr}(X_{j_1}\cdots X_{j_\ell})\cdots$. Furthermore, let $I(n+1,m) \trianglelefteq K\,\mathrm{S}_m$ be the ideal generated by all simple factors corresponding to Young diagrams of at least $n+1$ rows. Then $\sum_{\sigma\in\mathrm{S}_m} a_\sigma \operatorname{Tr}_\sigma(X_1,\dots,X_m)$ is a trace identity (i.e., $\sum_{\sigma\in\mathrm{S}_m} a_\sigma \operatorname{Tr}_\sigma(X_1,\dots,X_m) = 0$ for all possible choices of the X_i) if and only if $\sum_{\sigma\in\mathrm{S}_m} a_\sigma\sigma \in I(n+1,m)$, cf. [Pro76, Theorem 4.3]. As in the proof of Lemma 4.1, it is likely that the relation for the product of the traces comes from an element $\sigma \in I(4,8)$ such that σ contains a cycle with cycle structure $(4,4)$.

This last approach is more general than the other two above, since it would give a relation for eight arbitrary matrices. However, finding the element in $I(4,8)$ seems to be harder as well, and since we are only interested in the two generator case, this will not be pursued here.

We are now able to prove the uniqueness of the trace polynomials in degree 3. The proof uses a result in the invariant theory of $\mathrm{SL}(n, K)$ for algebraically closed fields of arbitrary characteristic, given by Steve Donkin, cf. [Don92].
The proof of the following proposition is due to Steve Donkin.

Proposition 4.5 (Donkin, [Don10], [Don92]). *Let K be an algebraically closed field. The invariant ring*

$$K[\underbrace{\mathrm{SL}(n,K) \times \cdots \times \mathrm{SL}(n,K)}_{m \text{ times}}]^{\mathrm{GL}(n,K)},$$

where $\mathrm{GL}(n,K)$ acts by simultaneous conjugation, is finitely generated. More specifically, it is generated by the coefficients of the characteristic polynomials of products of matrices $x_{i_1} \cdots x_{i_r}$, where the $i_j \in \{1, \ldots, m\}$, and x_k is in the kth component of $\mathrm{SL}(n,K) \times \cdots \times \mathrm{SL}(n,K)$.

Proof. We use the notations and results of [Don92]. Let G be a reductive group acting on an affine variety V and let A be a closed G-stable subset. Call (V, A) a *good pair* if $K[V]$ has a good filtration and so does the defining ideal I_A of A. If (V, A) is a good pair, then the map $K[V]^G \to K[A]^G$ is surjective.
In the case of $G = \mathrm{GL}(n,K)$, $V = \mathrm{GL}(n,K)$ and $A = \mathrm{SL}(n,K)$ it is easy to see that (V, A) is a good pair, since the defining ideal is $(\det -1)K[G]$, which is isomorphic to $K[G]$. On general ground, if (V_i, A_i) are good pairs, then $(V_1 \times V_2, A_1 \times A_2)$ is a good pair. So the map on invariants $K[\mathrm{GL}(n,K) \times \cdots \times \mathrm{GL}(n,K)]^G \to K[\mathrm{SL}(n,K) \times \cdots \times \mathrm{SL}(n,K)]^G$ is surjective. □

In the case of $n = 3$, the coefficients of the characteristic polynomial are just the trace and the trace of the inverse. This gives a proof of the uniqueness of the trace polynomials, which is an adaptation of the argument in [Law07b]. Note that we will write $x_{[1,2]}$ for $x_{-2,1,2,-1}$.

Proposition 4.6. *For any word $w = w(a,b) \in \mathrm{Fr}(a,b)$, there exists a unique polynomial*

$$p_w \in \mathbb{Z}[x_1, x_{-1}, x_2, x_{-2}, x_{1,2}, x_{-1,2}, x_{-2,1}, x_{-2,-1}, x_{[1,2]}]$$

with $\deg_{x_{[1,2]}}(p_w) < 2$ satisfying the following property. For any representation $\Delta\colon F_2 \to \mathrm{SL}(3,R)$ over an integral domain R we have

$$\mathrm{Tr}(\Delta(w)) = p_w(\mathrm{Tr}(X_1), \mathrm{Tr}(X_1^{-1}), \mathrm{Tr}(X_2), \ldots, \mathrm{Tr}(X_2^{-1}X_1^{-1}), \mathrm{Tr}([X_1, X_2])),$$

where $X_1 := \Delta(g_1)$ and $X_2 := \Delta(g_2)$. Furthermore, for any algebraically closed field K, the invariant ring $K[\mathrm{SL}(3,K) \times \mathrm{SL}(3,K)]^{\mathrm{GL}(3,K)}$ is isomorphic to $K[x_1, \ldots, x_{[1,2]}]/\langle r_{[1,2]} \rangle$.

Proof. The existence of p_w follows by Proposition 4.2.
Now let K be an algebraically closed field. Then, by Donkin's Theorem, the map

$$\varphi\colon K[x_1, \ldots, x_{[1,2]}] \to K[\mathrm{SL}(3,K) \times \mathrm{SL}(3,K)]^{\mathrm{GL}(3,K)}$$

is surjective. The invariant ring is an integral domain of Krull dimension 8, while the polynomial ring $K[x_1, \ldots, x_{[1,2]}]$ has Krull dimension 9; thus the kernel is a principal ideal. By Lemma 4.3 it contains $\langle r_{[1,2]} \rangle$ (where the t_i are replaced by x_i), hence $\ker \varphi = \langle r_{[1,2]} \rangle$. This also proves the uniqueness of the trace polynomials. □

Definition 4.7. Let $t = (t_1, t_{-1}, t_2, t_{-2}, t_{1,2}, t_{-1,2}, t_{-2,1}, t_{-2,-1}, t_{[1,2]}) \in \mathbb{F}_q^9$. Then t is called a **trace tuple**, if $t_{[1,2]}$ satisfies the quadratic relation $r_{[1,2]}$ of Lemma 4.3.
If $\Delta\colon F_2 \to \mathrm{SL}(3, \overline{K})$ is a representation with $\mathrm{Tr}(\Delta(g_1)) = t_1$, $\mathrm{Tr}(\Delta(g_1^{-1})) = t_{-1}$, $\mathrm{Tr}(\Delta(g_2)) = t_2$, etc., then Δ is a representation **affording** the trace tuple t.

In degree 2, it is possible to write down for every trace tuple $t = (t_1, t_2, t_{12}) \in K$ a representation affording t, cf. Theorem 2.5. There does not seem to be an easy way to do this in degree 3. However, using invariant theory it is easy to prove that such a representation always exists.

Theorem 4.8. *Let $t \in K^9$ be a trace tuple. There exists a representation $\Delta\colon F_2 \to \mathrm{SL}(3, \overline{K})$ affording t.*

Proof. Assume without loss of generality that K is algebraically closed. Set $G := \mathrm{GL}(3, K)$ and $X := \mathrm{SL}(3, K) \times \mathrm{SL}(3, K)$. By Proposition 4.6 we have

$$K[X/\!\!/G] = K[X]^G = K[x_1, \ldots, x_{[1,2]}]/\langle r_{[1,2]}\rangle,$$

where $X/\!\!/G$ denotes the categorical quotient, cf. e.g. [DK02, Section 2.3]. Now t is a zero of $r_{[1,2]}$ and hence a point of $X/\!\!/G$. Since $X \to X/\!\!/G$ is surjective, there is a representation $\Delta\colon F_2 \to \mathrm{SL}(3, K)$ affording t. □

4.1.3 A generating set for $K^{3\times3}$

In degree 2, if $\Delta\colon F_2 \to \mathrm{SL}(2, K)$ is absolutely irreducible, then $(I_2, \Delta(g_1), \Delta(g_2), \Delta(g_1g_2))$ is a basis of $K^{2\times2}$, cf. Lemma 2.7. This has two important applications. First, it yields the criterion in Theorem 2.8 for absolute irreducibility in term of the traces. And second, it allows the definition of the trace presentation ideal. So it is obviously desirable to get an analogous result in degree 3. Sadly, such a nice tuple does not exist here. The best thing possible is to give a set of fourteen matrices which form a generating set if the representation is absolutely irreducible. The corresponding irreducibility criterion is not as useful as in degree 2 and will be replaced by a better criterion in the next subsection, but the tuple allows the definition of the trace presentation ideal in Section 4.2.
Unfortunately, the proof of the result is rather technical.

Lemma 4.9. *Let K be a field and $X_1, X_2, X_3 \in \mathrm{SL}(3, K)$. Set $X_{-i} := X_i^{-1}$ for $i \in \{1, 2, 3\}$, and let $t_{i_1,\ldots,i_k} := \mathrm{Tr}(X_{i_1} \cdots X_{i_k})$ for $i_1, \ldots, i_k \in \{1, 2, 3\}$. The following relations for the matrices hold.*

$$X_1X_2X_1 = -X_1^{-1}X_2 - X_2X_1^{-1} + t_{-1}X_2 + t_2X_1^{-1} + t_{1,2}X_1 + (t_{-1,2} - t_{-1}t_2)I_3. \tag{4.1}$$

$$\begin{aligned} X_1X_2X_1^{-1} = -X_1^{-1}X_2X_1 &+ t_1(X_2X_1^{-1} + X_1^{-1}X_2) + t_{-1}(X_1X_2 + X_2X_1) \\ &- (t_1t_2 - t_{1,2})X_1^{-1} - (t_1t_{-1} + 1)X_2 - (t_{-1}t_2 - t_{-1,2})X_1 \\ &+ (t_1t_{-1}t_2 - t_{-1}t_{1,2} - t_1t_{-1,2} + t_2)I_3. \end{aligned} \tag{4.2}$$

$$\begin{aligned} X_1^{-1}X_2^{-1}X_1X_2 = X_2^{-1}X_1X_2X_1^{-1} &+ t_2(X_2^{-1} + X_1^{-1}X_2X_1) - t_{-2}(X_2 + X_1X_2X_1^{-1}) \\ &+ t_{-2,-1}(X_1X_2 + X_2X_1) - t_{-1,2}(X_1X_2^{-1} + X_2^{-1}X_1) \end{aligned}$$

$$\begin{aligned}&- (t_1t_2 - t_{1,2})X_1^{-1}X_2^{-1} + (t_1t_{-2} - t_{-2,1})X_2X_1^{-1}\\&- (t_1t_{-2,-1} - t_{-2})X_2 + (t_1t_{-1,2} - t_2)X_2^{-1} - (t_2t_{-2,-1} - t_{-2}t_{-1,2})X_1\\&+ (t_1t_2t_{-2,-1} - t_1t_{-2}t_{-1,2} - t_{1,2}t_{-2,1} + t_{-2,1}t_{-1,2})I_3. \quad (4.3)\end{aligned}$$

Proof. By [Pro76, Corollary 4.4], the relation

$$\begin{aligned}0 = &-X_1X_2X_3 - X_1X_3X_2 - X_2X_1X_3 - X_2X_3X_1 - X_3X_1X_2 - X_3X_2X_1\\&+ t_1(X_2X_3 + X_3X_2) + t_2(X_1X_3 + X_3X_1) + t_3(X_1X_2 + X_2X_1)\\&- (t_1t_2 - t_{1,2})X_3 - (t_1t_3 - t_{1,3})X_2 - (t_2t_3 - t_{2,3})X_1\\&+ (t_1t_2t_3 - t_{1,2}t_3 - t_{1,3}t_2 - t_{2,3}t_1 + t_{1,2,3} + t_{1,3,2})I_3.\end{aligned}$$

holds for all matrices in characteristic zero, and since the coefficients are all integers, the relation holds in general (cf. the proof of Lemma 4.1).
Replacing X_3 by X_1 and X_1^{-1} and using the trace polynomials as well as the relation $X_1^2 = X_1^{-1} + t_1X_1 - t_{-1}I_3$ yields (4.1) and (4.2), respectively. For the last relation, replace first X_3 by $X_1^{-1}X_2^{-1}$ and subtract from this equation the equation which arises from replacing X_1 by X_2^{-1}, X_2 by X_1, and X_3 by $X_2X_1^{-1}$. □

Proposition 4.10. *Let $\Delta\colon F_2 \to \mathrm{SL}(3, K)$ be an absolutely irreducible representation; set $X_1 := \Delta(g_1)$ and $X_2 := \Delta(g_2)$. Then*

$$\begin{aligned}(I_3, X_1, X_1^{-1}, X_2, X_2^{-1}, X_1X_2, X_2X_1, X_1^{-1}X_2, X_2X_1^{-1},&\\X_1X_2^{-1}, X_2^{-1}X_1, X_1^{-1}X_2^{-1}, X_2^{-1}X_1^{-1}, [X_1, X_2])&\end{aligned}$$

is a generating set of $K^{3\times3}$.

Proof. If Δ is absolutely irreducible, there exists a basis of $K^{3\times3}$ consisting of words in $X_1, X_2, X_1^{-1}, X_2^{-1}$. By (4.1), every word of length at least 5 can be reduced to a linear combination of words of smaller length, hence there exists a basis of words of length at most 4, where every letter occurs at most once. There are eight words of length 4 such that every letter occurs exactly once, and every one of them can be reduced to linear combination of $X_1^{-1}X_2^{-1}X_1X_2$ and words of length at most 3, or to a linear combination of $X_2^{-1}X_1X_2X_1^{-1}$ and words of length at most 3, using (4.2). By (4.3),

$$\begin{aligned}(I_3, X_1, X_1^{-1}, X_2, X_2^{-1}, X_1X_2, X_2X_1, X_1^{-1}X_2, X_2X_1^{-1}, X_1X_2^{-1}, X_2^{-1}X_1, X_1^{-1}X_2^{-1}, X_2^{-1}X_1^{-1},&\\X_1X_2X_1^{-1}, X_1X_2^{-1}X_1^{-1}, X_2X_1X_2^{-1}, X_2X_1^{-1}X_2^{-1}, [X_1, X_2])&\end{aligned}$$

is a generating set of $K^{3\times3}$.
Assume first that $(I_3, X_1, X_1^{-1}, X_2, X_2^{-1})$ is linearly dependent. Then X_1^{-1} or X_2^{-1} is a linear combination of the other matrices. We handle the case $X_2^{-1} \in \langle I_3, X_1, X_1^{-1}, X_2\rangle$; the other case is analogous. Using the fact that X_2^{-1} is a linear combination in the other four matrices and relations (4.1) and (4.2), it is easy to see that

$$(I_3, X_1, X_1^{-1}, X_2, X_1X_2, X_2X_1, X_1^{-1}X_2, X_2X_1^{-1}, X_1^{-1}X_2^{-1}X_1)$$

is a basis set of $K^{3\times3}$. Multiplying on the right by X_2 yields the basis

$$(X_2, X_1X_2, X_1^{-1}X_2, X_2^2, X_1X_2^2, X_2X_1X_2, X_1^{-1}X_2^2, X_2X_1^{-1}X_2, [X_1, X_2]),$$

and the first eight elements can be reduced to linear combinations of words of length at most 2, hence

$$(I_3, X_1, X_1^{-1}, X_2, X_1X_2, X_2X_1, X_1^{-1}X_2, X_2X_1^{-1}, [X_1, X_2])$$

is a basis. This finishes the proof if $X_2^{-1} \in \langle I_3, X_1, X_1^{-1}, X_2\rangle$, and similarly if $X_1^{-1} \in \langle I_3, X_1, X_2, X_2^{-1}\rangle$.
Now assume that $(I_3, X_1, X_1^{-1}, X_2, X_2^{-1})$ is linearly independent. We prove that there exists a basis consisting of words of length at most two. Suppose that this is not the case. Then there is a word w_3 of length 3 which cannot be written as a linear combination of words of smaller length; by relation 4.1 and without loss of generality we can assume that $w_3 = X_1X_2X_1^{-1}$. Then $(I_3, X_1, X_1^{-1}, X_2, X_2^{-1}, X_1X_2, X_2X_1^{-1})$ has to be linearly independent. Suppose

$$(I_3, X_1, X_1^{-1}, X_2, X_2^{-1}, X_1X_2, X_2X_1^{-1}, w_2)$$

is linearly dependent for every word w_2 of length 2. Then the words $X_1X_2^{-1}X_1^{-1}$, $X_2X_1X_2^{-1}$, $X_2X_1^{-1}X_2^{-1}$, and $[X_1, X_2]$ can be reduced to linear combinations of words of length at most 2, thus

$$(I_3, X_1, X_1^{-1}, X_2, X_2^{-1}, X_1X_2, X_2X_1^{-1}, X_1X_2X_1^{-1})$$

is a generating system, which is a contradiction. Hence there exists a word w_2 of length 2 such that $(I_3, X_1, X_1^{-1}, X_2, X_2^{-1}, X_1X_2, X_2X_1^{-1}, w_2)$ is linearly independent, and since w_3 cannot be written as a linear combination of words of smaller length,

$$(I_3, X_1, X_1^{-1}, X_2, X_2^{-1}, X_1X_2, X_2X_1^{-1}, w_2, X_1X_2X_1^{-1})$$

is a basis.
Multiplying this basis with X_1^{-1} from the left and X_1 from the right yields again bases, which we call $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively. Every element in $\mathcal{B}_1$ except possibly $X_1^{-1}w_2$ can be written as a linear combination of words of length at most 2, hence $X_1^{-1}w_2$ must be a word which cannot be written as such a linear combination. The same argument for $\mathcal{B}_2$ shows that w_2X_1 cannot be shortened. Then $X_1^{-1}w_2 = X_1^{-1}ZX_1$ for some $Z \in \{X_2, X_2^{-1}\}$, and $w_2X_1 = X_1^{-1}Z'X_1$ for some $Z' \in \{X_2, X_2^{-1}\}$, which is a contradiction. Hence the initial assumption that there is no basis of words of length at most 2 is wrong, which proves the proposition. □

For the formulation of the L3-quotient algorithm, it is enough to have a generating set for the matrix algebra. However, to construct a representation from a trace tuple as outlined in Proposition 3.4, a basis of the matrix algebra is needed. The proposition shows that one of the $\binom{14}{9} = 2002$ possible subsets of the 14 matrices form a basis for $K^{3\times 3}$, but it would be expensive to try them all. A careful analysis of the proof shows that this number can actually be reduced.

Corollary 4.11. *Let $\Delta\colon F_2 \to \mathrm{SL}(3, K)$ be an absolutely irreducible representation; set $X_i := \Delta(g_i)$. One of the following 72 tuples is a basis of $K^{3\times 3}$.*

- $(I_3, X_1, X_1^{-1}, X_2, X_1X_2, X_2X_1, X_1^{-1}X_2, X_2X_1^{-1}, [X_1, X_2])$.
- $(I_3, X_1, X_2, X_2^{-1}, X_1X_2, X_2X_1, X_1X_2^{-1}, X_2^{-1}X_1, [X_1, X_2])$.
- $(I_3, X_1, X_1^{-1}, X_2, X_2^{-1}, w_1, w_2, w_3, w_4)$, *where*

  $\{w_1, w_2, w_3, w_4\} \subseteq \{X_1X_2, X_2X_1, X_1^{-1}X_2, X_2X_1^{-1}, X_1X_2^{-1}, X_2^{-1}X_1, X_1^{-1}X_2^{-1}, X_2^{-1}X_1^{-1}\}$

  is one of the 70 possible subsets of cardinality 4.

4.1.4 Deciding absolute irreducibility

In Theorem 2.8, the knowledge of a basis of $K^{2\times 2}$ is used to compute the irreducibility indicator ρ, which has the property that a representation with trace tuple t is absolutely irreducible if and only if t is a zero of ρ. Since Proposition 4.10 gives a generating set of $K^{3\times 3}$, a similar idea can be applied in degree 3 as follows. Let M be the 14×14-matrix with entries $\mathrm{Tr}(X \cdot Y)$, where X and Y run through the elements of the generating set in Proposition 4.10. Since the trace bilinear form is non-degenerate, the matrix M has rank 9 if and only if the 14 matrices form a generating set for K. This can be translated into conditions for determinants of 9×9-submatrices which generate an ideal ρ of $\mathbb{Z}[x_1, \dots, x_{[1,2]}]$. Using Corollary 4.11, the number of generators can be reduced to 72. A representation $\Delta\colon F_2 \to \mathrm{SL}(3, K)$ is absolutely irreducible if and only if the corresponding trace tuple is a zero of ρ. Unfortunately, the generators are very big, which makes it rather unpleasant to work with this ideal. For example, it seems that it is not even possible to compute a Gröbner basis.

Here is another approach to compute small ideal generators which can actually be handled. Let $\Delta\colon F_2 \to \mathrm{SL}(3, K)$ be a representation. We can assume that K is algebraically closed. Set $X_1 := \Delta(g_1)$ and $X_2 := \Delta(g_2)$. Then Δ is not absolutely irreducible if and only if either X_1 and X_2 are conjugate to matrices of the form $\left(\begin{smallmatrix} a & a' \\ 0 & Y_1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} b & b' \\ 0 & Y_2 \end{smallmatrix}\right)$, respectively, or X_1 and X_2 are conjugate to matrices of the form $\left(\begin{smallmatrix} a & 0 \\ a'' & Y_1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} b & 0 \\ b'' & Y_2 \end{smallmatrix}\right)$, with $a, b \in K^*$, $a', b' \in K^{1\times 2}$, $a'', b'' \in K^{2\times 1}$, and $Y_1, Y_2 \in \mathrm{GL}(2, K)$. For $i \in \{1, 2, -1, -2\}^k$ let $t_i := \mathrm{Tr}(X_{i_1} \cdots X_{i_k})$ and $s_i := \mathrm{Tr}(Y_{i_1} \cdots Y_{i_k})$. Note that $\det(Y_1) = a^{-1}$, so $\sqrt{a}Y_1$ is a matrix of determinant 1, and similarly for Y_2. Using the trace polynomials of Theorem 2.1 and Proposition 4.2, we see that the following relations hold:

$$t_1 = a + s_1,\ t_2 = b + s_2,\ t_{-1} = a^{-1} + s_1 a,\ t_{-2} = b^{-1} + s_2 b,$$
$$t_{1,2} = s_{1,2} + ab,\ t_{-1,2} = a(s_1 s_2 - s_{1,2}) + a^{-1} b,$$
$$t_{-2,1} = b(s_1 s_2 - s_{1,2}) + b^{-1} a,\ t_{-2,-1} = a^{-1} b^{-1} s_{1,2} + ab,$$
$$t_{[1,2]} = a s_1^2 + b s_2^2 + ab s_{1,2}^2 - ab s_1 s_2 s_{1,2} - 1.$$

The first four equations can be used to write a, b, a^{-1}, b^{-1} in terms of the t_i and s_i, leaving five conditions on the s_i and t_i. Now regard the s_i and t_i as indeterminates, and use an elimination ordering to remove the s_i. The corresponding ideal is the analogue of ρ in degree 3.

Proposition 4.12. *There exists an ideal $\rho \trianglelefteq \mathbb{Z}[x_1, \dots, x_{[1,2]}]$ satisfying the following condition: a representation $\Delta\colon F_2 \to \mathrm{SL}(3, K)$ with trace tuple t is absolutely irreducible if and only if t is not a zero of ρ.*

Remark 4.13. The ideal ρ can be effectively computed. It can be generated by 10 elements, and has Krull dimension 6.

Definition 4.14. A trace tuple $t \in \mathbb{F}_q^9$ is called **absolutely irreducible** if it is not a zero of the ideal ρ of Proposition 4.12.

4.2 Representations and ideals

Now we are for the first time confronted with the problem that $\mathbb{Z}$ does not contain a third root of unity. Here is a description of the problem. Let $G = \langle g_1, g_2 \,|\, r_1, \dots, r_k \rangle$ be a finitely presented group, and let $\delta\colon G \to \mathrm{PSL}(3,q)$ be a homomorphism. Then there exists a representation $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ inducing δ, i.e., $\Delta(r_i) \in \mathrm{Z}(\mathrm{SL}(3,q))$ for all $i = 1,\dots,k$. If $\mathbb{F}_q$ contains a primitive third root of unity ζ then $\mathrm{Z}(\mathrm{SL}(3,q)) = \langle \zeta I_3 \rangle$, so $\Delta(r_i) \in \mathrm{Z}(\mathrm{SL}(3,q))$ is equivalent to $\Delta(r_i) = s_i I_3$ for some $s_i \in \langle\zeta\rangle$. Our goal is, as in the L$_2$-quotient algorithm, to construct all possible representations with this property, for all possible prime powers q. Thus we have to work with a universal ring which contains a primitive third root of unity ζ. To do this, we adjoin ζ to $\mathbb{Z}$ and work with the ring $\mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$.

Definition 4.15. Let $G = \langle g_1, g_2 \,|\, r_1,\dots,r_k\rangle$ and $s \in \langle\zeta\rangle^k$. The **trace presentation ideal** of G with respect to s is defined as

$$I_s(G) := \langle p_{r_i h} - s_i p_h \,|\, h \in \{1, g_1, g_1^{-1}, g_2, g_2^{-1}, g_1g_2, g_2g_1, g_1^{-1}g_2, g_2g_1^{-1}, g_1g_2^{-1}, g_2^{-1}g_1, g_1^{-1}g_2^{-1}, g_2^{-1}g_1^{-1}, [g_1,g_2]\}, i \in \{1,\dots,k\}\rangle \trianglelefteq \mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}].$$

An element $s \in \langle\zeta\rangle^k$ is called a **sign system** for G.

As in Section 2.2 we get the following result, using Proposition 4.10.

Proposition 4.16. *Let $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ be an absolutely irreducible representation with trace tuple $t = (t_1,\dots,t_{[1,2]}) \in \mathbb{F}_q^9$. Then Δ induces a homomorphism $G \to \mathrm{PSL}(3,q)$ if and only if t is a zero of a trace presentation ideal $I_s(G)$ for some $s \in \langle\zeta\rangle^k$.*

4.3 Actions on representations, trace tuples and ideals

Two important groups acting on various objects in degree 2 are the group of sign changes acting on representations, trace tuples and ideals, and the Galois group acting on representations and trace tuples. These two groups together with their actions have direct analogues in degree 3. However, there are two more groups in degree 3, which do not play a role in degree 2.

The first one is a cyclic group of order 2, which induces the graph automorphism on $\mathrm{SL}(3,q)$, and acts correspondingly on the ring $\mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$. This group is not visible in degree 2, since the graph automorphism of $\mathrm{SL}(2,q)$ is an inner automorphism.

The other group is again cyclic of order 2 and acts on $\mathbb{Z}[\zeta]$ by sending ζ to its inverse.

Note that some of the actions in this section are already defined in the last chapter in a more general form. They are repeated here for convenience and to fix some notation.

Definition 4.17. Let $\Sigma := \langle\zeta\rangle^2$, the group of **sign changes**, where ζ is a primitive third root of unity. Assume that q is a prime power with $q \equiv 1 \mod 3$.

If $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ is a representation, define a representation ${}^\sigma\Delta$ for $\sigma = (\sigma_1,\sigma_2) \in \Sigma$ by

$${}^\sigma\Delta\colon F_2 \to \mathrm{SL}(3,q)\colon g_1 \mapsto \sigma_1\Delta(g_1),\ g_2 \mapsto \sigma_2\Delta(g_2).$$

This defines an action of Σ on the set of representations $F_2 \to \mathrm{SL}(3,q)$, and induces actions on the set of characters and the set of trace tuples. To be more precise, if $t := (t_1,\dots,t_{[1,2]}) \in \mathbb{F}_q^9$ is a trace tuple,

$${}^\sigma t = (\sigma_1 t_1, \sigma_1^{-1}t_{-1}, \sigma_2 t_2, \sigma_2^{-1}t_{-2}, \sigma_1\sigma_2 t_{1,2}, \sigma_1^{-1}\sigma_2 t_{-1,2}, \sigma_2^{-1}\sigma_1 t_{-2,1}, \sigma_2^{-1}\sigma_1^{-1}t_{-2,-1}, t_{[1,2]}).$$

Furthermore, Σ acts on $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$ via ring automorphisms by setting

$$\begin{gathered} {}^{\sigma}x_1 := \sigma_1 x_1,\ {}^{\sigma}x_{-1} := \sigma_1^{-1} x_{-1},\ {}^{\sigma}x_2 := \sigma_2 x_2,\ {}^{\sigma}x_{-2} := \sigma_2^{-1} x_{-2}, \\ {}^{\sigma}x_{1,2} := \sigma_1\sigma_2 x_{1,2},\ {}^{\sigma}x_{-1,2} := \sigma_1^{-1}\sigma_2 x_{-1,2},\ {}^{\sigma}x_{-2,1} := \sigma_1\sigma_2^{-1} x_{-2,1},\ {}^{\sigma}x_{-2,-1} := \sigma_1^{-1}\sigma_2^{-1} x_{-2,-1}, \\ {}^{\sigma}x_{[1,2]} := x_{[1,2]}, \end{gathered}$$

and this action induces an action on the set of ideals of $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$.

Definition 4.18. Let $T := \langle \tau \rangle$ be a cyclic group of order 2. If $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ is a representation, define a representation ${}^{\tau}\Delta$ by

$${}^{\tau}\Delta = \Delta^{-\,\mathrm{tr}}\colon F_2 \to \mathrm{SL}(3,q)\colon g \mapsto \Delta(g)^{-\,\mathrm{tr}}.$$

This defines an action of T on the set of representations $F_2 \to \mathrm{SL}(3,q)$, and induces actions on the set of characters and the set of trace tuples. To be more precise, if $t := (t_1, \dots, t_{[1,2]}) \in \mathbb{F}_q^9$ is a trace tuple, then

$${}^{\tau}t = (t_{-1}, t_1, t_{-2}, t_2, t_{-2,-1}, t_{-2,1}, t_{-1,2}, t_{1,2}, t_{[2,1]}),$$

where

$$\begin{aligned} t_{[2,1]} := t_1t_{-1} + t_2t_{-2} + t_{1,2}t_{-2,-1} + t_{-1,2}t_{-2,1} - t_1t_2t_{-2,-1} - t_{-1}t_{-2}t_{1,2} \\ - t_{-1}t_2t_{-2,1} - t_1t_{-2}t_{-1,2} + t_1t_{-1}t_2t_{-2} - t_{[1,2]} - 3 \end{aligned}$$

(cf. Lemma 4.1).
Furthermore, T acts on $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$ via ring automorphisms by setting

$$\begin{gathered} {}^{\tau}x_1 := x_{-1},\ {}^{\tau}x_{-1} := x_1,\ {}^{\tau}x_2 := x_{-2},\ {}^{\tau}x_{-2} := x_2, \\ {}^{\tau}x_{1,2} := x_{-2,-1},\ {}^{\tau}x_{-1,2} := x_{-2,1},\ {}^{\tau}x_{-2,1} := x_{-1,2},\ {}^{\tau}x_{-2,-1} := x_{1,2}, \\ {}^{\tau}x_{[1,2]} := x_{[2,1]}, \end{gathered}$$

where

$$\begin{aligned} x_{[2,1]} := x_1x_{-1} + x_2x_{-2} + x_{1,2}x_{-2,-1} + x_{-1,2}x_{-2,1} - x_1x_2x_{-2,-1} - x_{-1}x_{-2}x_{1,2} \\ - x_{-1}x_2x_{-2,1} - x_1x_{-2}x_{-1,2} + x_1x_{-1}x_2x_{-2} - x_{[1,2]} - 3, \end{aligned}$$

and this action induces an action on the set of ideals of $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$. Similarly, T acts on $\mathbb{Z}[x_1, \dots, x_{[1,2]}]$ and its ideals.

Definition 4.19. Let $Z := \langle z \rangle$ be a cyclic group of order 2. Z acts on $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$ via ring automorphisms by sending ζ to ζ^{-1} and fixing all indeterminates. This induces an action on the set of ideals of $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$.

Remark 4.20. Combining the last three actions yields an action of $\Sigma \rtimes (T \times Z)$ via ring automorphisms on $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$ and hence on the set of its ideals, where T and Z both act by inversion on Σ.

Definition 4.21. Let $\Gamma := \mathrm{Gal}(\mathbb{F}_q)$. If $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ is a representation, define a representation ${}^{\gamma}\Delta$ for $\gamma \in \Gamma$ by

$${}^{\gamma}\Delta\colon F_2 \to \mathrm{SL}(3,q)\colon g \mapsto \gamma(\Delta(g)).$$

This defines an action of Γ on the set of representations $F_2 \to \mathrm{SL}(3,q)$, and induces actions on the set of characters and the set of trace tuples.

As in degree 2, we identify trace tuples with maximal ideals.

Remark 4.22. There is a bijection between the maximal ideals $\mathfrak{t}$ of $\mathbb{Z}[x_1,\dots,x_{[1,2]}]$ and the $\mathrm{Gal}(\mathbb{F}_q)$-orbits of trace tuples $t = (t_1,\dots,t_{[1,2]}) \in \mathbb{F}_q^9$, where q ranges over all prime powers. Unfortunately, most of the time we work with ideals in the ring $\mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$, and a maximal ideal $\mathfrak{t}$ of $\mathbb{Z}[x_1,\dots,x_{[1,2]}]$ can split into two maximal ideals of $\mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$. However, there is a bijection between the $\mathrm{Gal}(\mathbb{F}_q)$-orbits of trace tuples $t = (t_1,\dots,t_{[1,2]})$ and Z-orbits of maximal ideals of $\mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$. By abuse of notation, such a maximal ideal is again denoted by $\mathfrak{t}$.

Here is an example to illustrate the complications arising from ζ.

Example 4.23. Note that $\mathrm{SL}(3,2)$ is generated by $A_1 := \left(\begin{smallmatrix}1&1&0\\0&1&0\\0&0&1\end{smallmatrix}\right)$ and $A_2 := \left(\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right)$. Let $\Delta\colon F_2 \to \mathrm{SL}(3,2)\colon g_i \mapsto A_i$ be the corresponding representation with trace tuple $t = (1,1,0,0,1,1,0,0,1) \in \mathbb{F}_2^9$. Then t is a zero of

$$\mathfrak{t} = \langle x_1+1, x_{-1}+1, x_2, x_{-2}, x_{1,2}+1, x_{-1,2}+1, x_{-2,1}, x_{-2,-1}, x_{[1,2]}+1\rangle.$$

But $\mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]/\,\mathfrak{t} = \mathbb{F}_4$. Thus, unlike in degree 2, the quotient of $\mathfrak{t}$ is not necessarily the character field.
Furthermore, set $\sigma := (\zeta,1)$. Then ${}^{\sigma}\Delta$ is a representation over $\mathbb{F}_4$ with trace tuple ${}^{\sigma}t = (\zeta,\zeta^2,0,0,\zeta,\zeta^2,0,0,1)$. So the character field of ${}^{\sigma}\Delta$ is $\mathbb{F}_4$; in particular, it is not possible to conjugate ${}^{\sigma}\Delta$ to a representation over $\mathbb{F}_2$, although the image of the corresponding projective representation is isomorphic to $\mathrm{PSL}(3,2) = \mathrm{SL}(3,2)$.

To circumvent these complications, one always has to take the Σ-conjugate of t which generates the smallest field. The corresponding ideal of $\mathbb{Z}[x_1,\dots,x_{[1,2]}]$ yields the character field.

4.4 Detecting epimorphisms onto proper subgroups

The classification of subgroups of $\mathrm{PSL}(3,q)$ was done by Mitchell for odd q and by Hartley for even q. A more modern treatment will appear in the book [BHRD12] by Bray, Holt, and Roney-Dougal.

Proposition 4.24 (Mitchell [Mit11], Hartley [Har25])**.** *Let $U \le \mathrm{SL}(3,q)$ be an absolutely irreducible subgroup such that the character values generate $\mathbb{F}_q$, and such that no Σ-conjugate of the character generates a proper subfield of $\mathbb{F}_q$. Denote by $\overline{U}$ the image in* $\mathrm{PSL}(3,q)$*. Then one of the following cases occurs.*

1. *$\overline{U}$ is isomorphic to one of the groups* A$_6$, L$_2$(7), PGU(3, 2), PSU(3, 2), *H_{36} (a subgroup of index two in* PSU(3, 2)*),* A$_7$ *or* M$_{10}$*. Following Macbeath [Mac69], these groups are called* ***exceptional****.*

2. *U is an imprimitive group.*

3. *$\overline{U}$ is isomorphic to* $\mathrm{PSO}(3, q)$ *if q is odd.*

4. *$\overline{U}$ is isomorphic to* $\mathrm{PSU}(3, r)$ *if $q = r^2$ is a square.*

5. *$\overline{U}$ is isomorphic to* $\mathrm{PGL}(3, r)$ *if $q = r^3$ is a cube.*

6. *$\overline{U}$ is isomorphic to* $\mathrm{PGU}(3, r)$ *if $q = r^6$ is a sixth power.*

7. *$\overline{U}$ is* $\mathrm{PSL}(3, q)$.

M_{10} denotes the Mathieu group on 10 points, i.e., a point stabilizer in the sporadic simple group M_{11}. The groups $\mathrm{PGU}(3, 2)$, $\mathrm{PSU}(3, 2)$ and H_{36} are also called Hessian groups.

Let $t = (t_1, \ldots, t_{[1,2]}) \in \mathbb{F}_q^9$ be a trace tuple with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(3, q)$. We want to decide, as in the case of degree 2, whether Δ induces an epimorphism onto some PSL, PGL, PSU, or PGU.

Absolutely irreducibility can be decided using Proposition 4.12, so we assume in the following that Δ is absolutely irreducible.

The first thing to decide is whether Δ induces an epimorphism onto an exceptional group. As in Proposition 2.18, there is a set of finitely many ideals which accomplishes this.

Proposition 4.25. *Let $t = (t_1, \ldots, t_{[1,2]}) \in \mathbb{F}_q^9$ be an absolutely irreducible trace tuple with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(3, q)$. There exist 57 ideals of $\mathbb{Z}[x_1, \ldots, x_{[1,2]}]$ such that the projective representation induced by Δ maps onto $\mathrm{L}_2(7)$ if and only if t is a zero of one of the 57 ideals. Similarly, there are 53 ideals for A_6, 64 ideals for $\mathrm{PGU}(3, 2)$, 4 ideals for $\mathrm{PSU}(3, 2)$, 6 ideals for H_{36}, 916 ideals for A_7, and 234 ideals for M_{10}.*

Proof. Every finite group has only finitely many presentations on two generators; e.g., $\mathrm{L}_2(7)$ has 57 presentations, A_6 has 53 presentations, etc. For every presentation, construct the trace presentation ideals with respect to all sign systems and compute the minimal associated prime ideals. Remove all prime ideals which contain the ideal ρ in Proposition 4.12 and take the intersection of all remaining ideals. The result is now clear by Proposition 4.16, since none of the groups has nontrivial absolutely irreducible quotients. □

All the work for the other subgroups was essentially done in the last chapter. We only translate the results to the language of ideals.

Next are the imprimitive groups. The following proposition is the analogue of Proposition 2.19. First, we need two lemmas, which show that it is not necessary to know all values of the character, but only finitely many.

Lemma 4.26. *Let $n \in \{2, 3\}$ and $\Delta\colon F_m \to \mathrm{GL}(n, K)$ a representation with character χ. Furthermore, let $\psi\colon F_m \to \mathrm{C}_n$ be a homomorphism. Then $\chi(w) = 0$ for all $w \in F_m - \ker\psi$ if and only if $\chi(g_\varphi) = 0$ for all $\varphi \in \Phi$ with $g_\varphi \notin \ker\psi$, where $g_\varphi := g_{\varphi(1)} \cdots g_{\varphi(k)}$.*

Proof. The proofs are similar for degree 2 and 3, so we give only the proof for $n = 3$.

Let $w = g_{i_1} \cdots g_{i_k}$ with $\psi(w) \neq 1$. We show $\chi(w) = 0$ by induction on $|w|$. Assume without loss of generality that $i_1 < i_j$ for all $j \in \{2, \ldots, k\}$, and define $\varphi\colon \{1, \ldots, k\} \to \{\pm 1, \ldots, \pm m\}$ by $\varphi(j) := i_j$. If $\varphi \in \Phi$, there is nothing to show. Otherwise, φ is not injective, or $\varphi(j) + \varphi(\ell) = 0$ for some $j < \ell$ with $\varphi(j) > \varphi(\ell)$. Consider the first case, so $\varphi(j) = \varphi(\ell)$ for some $j < \ell$. Set

$$w_1 := g_{\varphi(j)},\ w_2 := g_{\varphi(j+1)} \cdots g_{\varphi(\ell-1)},\ \text{and } w_3 := g_{\varphi(\ell+1)} \cdots g_{\varphi(k)} g_{\varphi(1)} \cdots g_{\varphi(j-1)}.$$

Furthermore, set $X_i := \Delta(w_i)$, so $\chi(w) = \mathrm{Tr}(X_1X_2X_1X_3)$. There are only finitely many possibilities for $\psi(w_i)$ such that $\psi(w) = \psi(w_1)^2\psi(w_2)\psi(w_3) \neq 1$. Assume for example that $\psi(w_1) \neq 1$ and $\psi(w_2) = \psi(w_3) = 1$. Using the notation of Lemma 4.1 this implies

$$t_{-1,2} = t_{-1,3} = t_{-1} = t_{1,2} = t_{-1,2,3} = t_{-1,3,2} = 0,$$

since $\psi(w_1^{-1}w_2)$, $\psi(w_1^{-1}w_3)$, $\psi(w_1^{-1})$, …are non-trivial. Hence $\chi(w) = t_{1,2,1,3} = 0$ by Lemma 4.1. Similar arguments show $\chi(w) = 0$ for the other possible choices of $\psi(w_i)$, thus proving the result if φ is not injective. The other case is analogous. □

Lemma 4.27. *Let $\Delta\colon F_m \to \mathrm{GL}(3, K)$ be an absolutely irreducible representation with character χ and $\psi\colon F_m \to \mathrm{S}_3$ an epimorphism. Then $\chi(w) = 0$ for all $w \in F_m$ with $|\psi(w)| = 3$ if and only if $\chi(g_\varphi) = 0$ for all $\varphi \in \Phi$ with $|\psi(g_\varphi)| = 3$ and $\chi(g_\varphi)\chi(g_\varphi^{-1}) = 1$ for all $\varphi \in \Phi$ with $|\psi(g_\varphi)| = 2$, where $g_\varphi := g_{\varphi(1)} \cdots g_{\varphi(k)}$.*

Proof. Assume first that $\chi(w) = 0$ for all $w \in F_m$ with $|\psi(w)| = 3$. Then clearly $\chi(g_\varphi) = 0$ for all $\varphi \in \Phi$ with $|\psi(g_\varphi)| = 3$. It remains to show that $\chi(g_\varphi)\chi(g_\varphi^{-1}) = 1$ for all $\varphi \in \Phi$ with $|\psi(g_\varphi)| = 2$. Set $w_1 := g_\varphi$, and choose $w_2 \in F_m$ such that $|\psi(w_2)| = 2$ and $|\psi(w_1w_2)| = 3$. Set $X_i := \Delta(w_i)$ and use the notation of Lemma 4.1. Then

$$t_{i,i,i,j} = t_{i,j}(t_i^2 - t_{-i}) + t_j(1 - t_it_{-i}) + t_{-i,j}t_i$$

for all $i, j \in \{\pm1, \pm2\}$. Since $|\psi(w_i^3w_j)| = |\psi(w_iw_j)| = |\psi(w_i^{-1}w_j)| = 3$ whenever $|i| \neq |j|$, this implies $t_j(1 - t_it_{-i}) = 0$. In particular, either $t_it_{-1} - 1 = 0$ for all i or $t_i = 0$ for all i. Suppose the latter case occurs. Let $N := \ker\psi$, and let H be the subgroup of index 2 in G containing N. Note that every $w \in F_m$ with $|\psi(w)| = 2$ differs from either w_1 or w_2 only by a kernel element, so replacing w_1 or w_2 by w in the argument above shows $\chi(w) = 0$. Denote by $V := K^{3\times1}$ the natural KG-module. Since V has dimension 3, the KH-module V_H must be absolutely irreducible as well, so $\Delta(H)$ contains a basis of $K^{3\times3}$. But $\psi(hw_1)$ has order 2 for every $h \in H$, so $\chi(hw_1) = 0$ for all $h \in H$, and as in the proof of Proposition 3.7 this yields a contradiction. Hence $t_1t_{-1} = \chi(g_\varphi)\chi(g_\varphi^{-1}) = 1$.
Conversely, assume that $\chi(g_\varphi) = 0$ for all $\varphi \in \Phi$ with $|\psi(g_\varphi)| = 3$ and $\chi(g_\varphi)\chi(g_\varphi^{-1}) = 1$ for all $\varphi \in \Phi$ with $|\psi(g_\varphi)| = 2$. As in the last corollary, one proves that this implies $\chi(w) = 0$ for all $w \in F_m$. □

Proposition 4.28. *Let $t = (t_1, \ldots, t_{[1,2]}) \in \mathbb{F}_q^9$ be an absolutely irreducible trace tuple with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(3, q)$. Then Δ is imprimitive if and only if t is a zero of one of the seven ideals*

$$\begin{gathered}
\langle x_1, x_{-1}, x_{1,2}, x_{-1,2}, x_{-2,1}, x_{-2,-1}\rangle, \langle x_2, x_{-2}, x_{1,2}, x_{-1,2}, x_{-2,1}, x_{-2,-1}\rangle,\\
\langle x_1, x_{-1}, x_2, x_{-2}, x_{1,2}, x_{-2,-1}\rangle, \langle x_1, x_{-1}, x_2, x_{-2}, x_{-1,2}, x_{-2,1}\rangle,\\
\langle x_1x_{-1} - 1, x_2x_{-2} - 1, x_{1,2}, x_{-1,2}, x_{-2,1}, x_{-2,-1}, x_{[1,2]}\rangle,\\
\langle x_1x_{-1} - 1, x_2, x_{-2}, x_{1,2}x_{-2,-1} - 1, x_1x_{1,2} + x_{-1,2}, x_{-1}x_{-2,-1} + x_{-2,1}, x_{[1,2]}\rangle,\\
\langle x_1, x_{-1}, x_2x_{-2} - 1, x_{1,2}x_{-2,-1} - 1, x_{-2}x_{-2,-1} + x_{-1,2}, x_2x_{1,2} + x_{-2,1}, x_{[1,2]}\rangle.
\end{gathered}$$

Proof. This follows from Propositions 3.7 and 3.9 and the last two lemmas. The first four ideals correspond to the four epimorphisms of F_2 onto C_3, the last three to the three epimorphisms of F_2 onto S_3. □

The results of the last chapter show that many properties of a representation can already be read off of its character. The last result shows that for imprimitivity it suffices to look at the trace tuple, not at the whole character. The aim of the next lemma goes into the same direction. It shows that the stabilizers of the characters under various actions is the stabilizer of the corresponding trace tuple, so it can be easily computed. This will be used to detect epimorphisms onto other subgroups.

Lemma 4.29. *Let $\Delta\colon F_2 \to \mathrm{SL}(3, K)$ be a representation with character χ and trace tuple $t = (t_1, \ldots, t_{[1,2]}) \in K^9$.*

1. *If ${}^{\tau}t = t$, then ${}^{\tau}\chi = \chi$.*
2. *Assume that $q = r^2$ is a square. Let γ be the generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_r)$. If ${}^{\gamma}t = {}^{\tau}t$, then ${}^{\gamma}\chi = {}^{\tau}\chi$.*
3. *Assume that $q = r^3$ is a cube and $\mathbb{F}_q$ contains a primitive third root of unity ζ. Let γ be the generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_r)$ and $\sigma \in \Sigma$. If ${}^{\gamma}t = {}^{\sigma}t$, then ${}^{\gamma}\chi = {}^{\sigma}\chi$.*

Proof. We prove the first point, the other two points are proved analogously. Note that ${}^{\tau}\chi = \chi$ clearly implies ${}^{\tau}t = t$; so assume now ${}^{\tau}t = t$. By Proposition 4.2, we have to show that $p_w = p_{w^{-1}}$ for all $w \in F_2$, where p_w is the trace polynomial of w. The proof is by induction on $|w|$, where the cases

$$w \in \{1, g_1^{\pm 1}, g_2^{\pm 1}, g_1 g_2, g_1^{-1} g_2, g_2^{-1} g_1, g_2^{-1} g_1^{-1}, [g_1, g_2], [g_2, g_1]\}$$

are covered by the hypothesis. Now assume that w is not in this set. Then the construction of p_w is based on the two relations in Lemma 4.1. The first relation is

$$t_{1,2,1,3} = t_{-1,2} t_3 + t_{-1,3} t_2 + t_{-1} t_{2,3} + t_{1,2} t_{1,3} - t_{-1} t_2 t_3 - t_{-1,2,3} - t_{-1,3,2},$$

and it is easy to check that $t_{-3,-1,-2,-1} = t_{1,2,1,3}$, provided $t_{-1,2} = t_{-2,1}$, $t_3 = t_{-3}$, etc. Similar considerations apply for the second relation of Lemma 4.1, which proves the first point. □

Note that the projective representation induced by Δ maps into $\mathrm{PSO}(3, q)$ if and only if a Σ-conjugate of Δ maps into $\mathrm{SO}(3, q)$. Together with Proposition 3.10 and the last lemma this proves the following result.

Proposition 4.30. *Let $t = (t_1, \ldots, t_{[1,2]}) \in \mathbb{F}_q^9$ be an absolutely irreducible trace tuple with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(3, q)$. Then the induced projective representation maps into $\mathrm{PSO}(3, q)$ if and only if some Σ-conjugate of t is a zero of the ideal*

$$\langle x_1 - x_{-1}, x_2 - x_{-2}, x_{1,2} - x_{-2,-1}, x_{-1,2} - x_{-2,1}, x_{[1,2]} - x_{[2,1]} \rangle,$$

where $x_{[2,1]}$ is defined in Definition 4.18.

This only leaves the possibilities $\mathrm{PSL}(3, q)$, $\mathrm{PGL}(3, r)$, $\mathrm{PSU}(3, r)$, and $\mathrm{PGU}(3, r)$, for appropriate r. To check whether the induced projective representation maps into $\mathrm{PGL}(3, r)$, we use the following result, which is the analogue of Proposition 2.20.

Proposition 4.31. *Assume $q = r^3$ with $3 \nmid r$. Let $t = (t_1, \ldots, t_{[1,2]}) \in \mathbb{F}_q^9$ be an absolutely irreducible trace tuple with corresponding ideal $\mathfrak{t} \trianglelefteq \mathbb{Z}[\zeta][x_1, \ldots, x_{[1,2]}]$ and representation $\Delta\colon F_2 \to \mathrm{SL}(3, q)$, such that Δ is not imprimitive. The image of the induced projective representation is isomorphic to a subgroup of $\mathrm{PGL}(3, r)$ if and only if $\mathfrak{t}$ has a non-trivial stabilizer in Σ.*

Proof. Let χ be the character of Δ and γ a generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_r)$. By Theorem 3.17, the projective representation induced by Δ maps into $\mathrm{PGL}(3, r)$ if and only if ${}^{\gamma}\chi = {}^{\sigma}\chi$ for some $\sigma \in \Sigma$. By Lemma 4.29 this is the case if and only if ${}^{\gamma}t = {}^{\sigma}t$. But t and ${}^{\gamma}t$ are both zeroes of $\mathfrak{t}$, so ${}^{\gamma}t = {}^{\sigma}t$ implies ${}^{\sigma}\,\mathfrak{t} = \mathfrak{t}$. Conversely, if ${}^{\sigma}\,\mathfrak{t} = \mathfrak{t}$, then both t and ${}^{\sigma}t$ are zeroes of $\mathfrak{t}$. But all zeroes of $\mathfrak{t}$ are Galois conjugate, hence ${}^{\sigma}t = {}^{\gamma'}t$ for some Galois automorphism γ' of order 3. □

Maps into $\mathrm{PSU}(3, r)$ are detected as follows.

Proposition 4.32. *Assume $q = r^2$. Let $t = (t_1, \ldots, t_{[1,2]}) \in \mathbb{F}_q^9$ be an absolutely irreducible trace tuple with corresponding ideal $\mathfrak{t} \trianglelefteq \mathbb{Z}[\zeta][x_1, \ldots, x_{[1,2]}]$ and representation $\Delta\colon F_2 \to \mathrm{SL}(3, q)$. The induced projective representation maps into $\mathrm{PSU}(3, q)$ if and only if T fixes a Z-orbit of a Σ-conjugate of $\mathfrak{t}$.*

Proof. Let $\Delta\colon F_2 \to \mathrm{SL}(3, q)$ be a representation affording t. Then the induced projective representation maps into $\mathrm{PSU}(3, r)$ if and only if a Σ-conjugate of Δ maps into $\mathrm{SU}(3, r)$. By Proposition 3.11 this is the case if and only if T induces an action by the Galois group on a Σ-conjugate of t. Using the bijection of Remark 4.22 between $\mathrm{Gal}(\mathbb{F}_q)$-orbits of trace tuples and Z-orbits of maximal ideals of $\mathbb{Z}[\zeta][x_1, \ldots, x_{[1,2]}]$, this is equivalent to the fact that T fixes a Z-orbit of a Σ-conjugate of $\mathfrak{t}$. □

The results in this section show that properties of a projective representation correspond to properties of an associated trace tuple. For example, an absolutely irreducible representation is imprimitive if and only if the trace tuple is a zero of one of seven ideals. It is convenient to give the trace tuples the corresponding names.

Definition 4.33. Let $t \in \mathbb{F}_q^9$ be a trace tuple.

1. If t is a zero of one of the seven ideals in Proposition 4.28, then t is called **imprimitive**.
2. If ${}^{\sigma}t$ is a zero of the ideal in Proposition 4.30 for some $\sigma \in \Sigma$, then t is called **orthogonal**.
3. Assume that $q = r^2$ is a square and γ is a generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_r)$. If ${}^{\gamma}({}^{\sigma}t) = {}^{\sigma}t$ for some $\sigma \in \Sigma$, then t is called **unitary**.
4. Assume that $q = r^3$ is a cube and γ is a generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_r)$. If ${}^{\gamma}t = {}^{\sigma}t$ for some $\sigma \in \Sigma$, then t is called **pgl**.
5. If t is both unitary and pgl, it is called **pgu**.

4.5 From ring quotients to group quotients

Remark 4.34. Every automorphism α of $\mathrm{PSL}(3,q)$ or $\mathrm{PSU}(3,q)$ can be written as $\alpha = g \circ f \circ d \circ i$, where i is an inner, d a diagonal, f a field and g a graph automorphism, cf. [Ste60]. Since $\mathrm{PSL}(3,q) \leq \mathrm{PGL}(3,q) \trianglelefteq \mathrm{Aut}(\mathrm{PSL}(3,q))$ and $\mathrm{PSU}(3,q) \leq \mathrm{PGU}(3,q) \trianglelefteq \mathrm{Aut}(\mathrm{PSU}(3,q))$, this also implies the same result if α is an automorphism of $\mathrm{PGL}(3,q)$ or $\mathrm{PGU}(3,q)$.

The proof of the following result is almost the same as the proof of Proposition 2.23.

Proposition 4.35. *Let $\Delta_i\colon F_2 \to \mathrm{SL}(3,q)$ be absolutely irreducible representations inducing homomorphisms $\delta_i\colon F_2 \to \mathrm{PSL}(3,q)$, for $i = 1,2$. Assume that either both δ_i are surjective, or $q = r^2$ and both δ_i map onto $\mathrm{PSU}(3,r)$, or $q = r^3$ and both δ_i map onto $\mathrm{PGL}(3,r)$, or $q = r^6$ and both δ_i map onto $\mathrm{PGU}(3,r)$. Then $\ker\delta_1 = \ker\delta_2$ if and only if ${}^{\gamma}\Delta_1 \sim {}^{\alpha}\Delta_2$ for some $\gamma \in \Gamma = \mathrm{Gal}(\mathbb{F}_q)$ and $\alpha \in \Sigma \rtimes T$. If t_i is the trace tuple corresponding to Δ_i, then this is equivalent to ${}^{\gamma}t_1 = {}^{\alpha}t_2$.*

Corollary 4.36. *For every quotient G/N isomorphic to $\mathrm{PSL}(3,q)$, $\mathrm{PGL}(3,q)$, $\mathrm{PSU}(3,q)$, or $\mathrm{PGU}(3,q)$ there exists exactly one $\Sigma \rtimes (T \times Z)$-orbit of maximal ideals of $\mathbb{Z}[\zeta][x_1,\ldots,x_{[1,2]}]$, where each ideal contains some trace presentation ideal $I_s(G)$.*

Proof. This follows by Remark 4.22 and Propositions 4.16 and 4.35. □

4.6 The algorithms

Definition 4.37. A prime ideal $P \trianglelefteq \mathbb{Z}[\zeta][x_1,\ldots,x_{[1,2]}]$ is called an L_3**-ideal**, if it does not contain the irreducibility indicator ρ of Proposition 4.12 and none of the ideals of Propositions 4.28 and 4.25, and no Σ-conjugate contains the ideal of Proposition 4.30.
A set Λ of L_3-ideals is called **minimal**, if no ideal of Λ contains a Σ-conjugate of another element of Λ. In other words, $P \not\supseteq {}^{\sigma}Q$ for all $\sigma \in \Sigma$ and all $P, Q \in \Lambda$ with $P \neq Q$.
A finite group H is called a group of L_3**-type**, if it is isomorphic to a group $\mathrm{PSL}(3,q)$, $\mathrm{PGL}(3,q)$, $\mathrm{PSU}(3,q)$, or $\mathrm{PGU}(3,q)$, for some prime power $q > 2$.

Algorithm 4.38 (L_3-Quotients)**.** *Input:* A finitely presented group $G = \langle g_1, g_2 \mid r_1, \ldots, r_k\rangle$ on two generators.
Output: A minimal set Λ of L_3-ideals satisfying the following property. If $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ is a representation with trace tuple t inducing an epimorphism of G onto a group of L_3-type, then ${}^{\sigma}t$ is a zero of an ideal in Λ for some $\sigma \in \Sigma$.
Algorithm:

1. Compute the set $\mathcal{P}'$ of all minimal associated prime ideals of $I_s(G)$, where $s \in \langle\zeta\rangle^k$ ranges over all sign systems. Let $\mathcal{P}$ be the set of all minimal elements of $\mathcal{P}'$ with respect to inclusion.

2. Choose a set of representatives $\mathcal{R}$ of $\mathcal{P}$ under the action of $\Sigma \rtimes (Z \times T)$.

3. Return all elements of $\mathcal{R}$ which do not lead to reducible representations or to epimorphisms onto A_6, $\mathrm{L}_2(7)$, $\mathrm{PGU}(3,2)$, $\mathrm{PSU}(3,2)$, H_{36}, A_7, or M_{10}, or onto orthogonal or imprimitive groups.

Remark 4.39. 1. As in the L_2-quotient algorithm, the groups $\mathrm{L}_3(2) \cong \mathrm{L}_2(7)$, $\mathrm{U}_3(2)$ and $\mathrm{PGU}(3,2)$ are excluded, for ease of presentation and implementation.

2. As in the L$_2$-quotient algorithm, one should avoid to iterate over all possible trace presentation ideals, cf. Chapter 8.

As in degree 2, we need a decision routine to get the isomorphism type of the maximal ideals constructed by Algorithm 4.38.

Algorithm 4.40 (L$_3$-Type)**.** *Input:* A maximal ideal $\mathfrak{t} \trianglelefteq \mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$, such that the image of the corresponding projective representation is isomorphic to a group of L$_3$-type.
Output: The exact isomorphism type of the image.
Algorithm:

1. Let p be the prime contained in $\mathfrak{t}$ and compute

$$n := \min\{\dim_{\mathbb{F}_p} \left(\mathbb{Z}[x_1, \dots, x_{[1,2]}]/(\mathbb{F}_p \otimes ({}^{\sigma}\,\mathfrak{t} \cap \mathbb{Z}[x_1, \dots, x_{[1,2]}]))\right) \mid \sigma \in \Sigma\}.$$

2. If $p = 3$, return $\mathrm{PSU}(3, p^{n/2})$ if $\mathfrak{t}$ is fixed by T and $\mathrm{PSL}(3, p^n)$ otherwise.

   If $3 \nmid (p^n - 1)$ return $\mathrm{PSL}(3, p^n)$.

   Otherwise let S be the stabilizer of $\mathfrak{t}$ in Σ.

   (a) If S is trivial, return $\mathrm{PSU}(3, p^{n/2})$ if the Z-orbit of some Σ-conjugate of $\mathfrak{t}$ is fixed by T and $\mathrm{PSL}(3, p^n)$ otherwise.

   (b) If S is non-trivial, return $\mathrm{PGU}(3, p^{n/6})$ if the Z-orbit of some Σ-conjugate of $\mathfrak{t}$ is fixed by T and $\mathrm{PGL}(3, p^{n/3})$ otherwise.

Proof. If $3 \nmid p^n - 1$, the groups $\mathrm{PGL}(3, p^n)$ and $\mathrm{PSL}(3, p^n)$ as well as the groups $\mathrm{PGU}(3, p^n)$ and $\mathrm{PSU}(3, p^n)$ are isomorphic. Furthermore, if $p \neq 3$ and $3 \nmid p^n - 1$, then n is odd, so $\mathrm{PSL}(3, p^n)$ has no unitary subgroup. This explains the first two rows of step 2. In the other cases, $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]/\,\mathfrak{t} \cong \mathbb{F}_{p^n}$, so the rest is an immediate application of Propositions 4.31 and 4.32. □

Given an absolutely irreducible trace tuple $t \in \mathbb{F}_q$, it is possible to construct a corresponding representation. The algorithm is based on Proposition 3.4.

Algorithm 4.41 (L$_3$-Generators)**.** *Input:* A maximal ideal $\mathfrak{t} \trianglelefteq \mathbb{Z}[x_1, \dots, x_{[1,2]}]$, such that the corresponding trace tuple t is absolutely irreducible.
Output: A representation $\Delta\colon F_2 \to \mathrm{SL}(3, q)$ affording t, where $\mathbb{F}_q = \mathbb{Z}[x_1, \dots, x_{[1,2]}]/\,\mathfrak{t}$.
Algorithm:

1. Let $\chi\colon F_2 \to \mathbb{F}_q$ be the character encoded by t. Choose a tuple $w = (w_1, \dots, w_9) \in F_2$ such that the matrix $(\chi(w_i w_j))_{i,j=1,\dots,9}$ is non-singular.

2. For $i = 1, 2$ and $j = 1, \dots, 9$ solve the system of nine linear equations

$$\chi(g_i w_j w_\ell) = \sum_{k=1}^{9} \lambda_{ijk} \chi(w_k w_\ell), \quad 1 \leq \ell \leq 9$$

   in the variables λ_{ijk}.

3. Use the Meat Axe (cf. [Par84]) to decompose the representation

$$\widetilde{\Delta}\colon F_2 \to \mathrm{SL}(9,q)\colon g_i \mapsto (\lambda_{ijk})_{j,k=1,\dots,9}$$

into $\widetilde{\Delta} = \mathrm{Diag}(\Delta,\Delta,\Delta)$, where $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ is an absolutely irreducible representation. Return Δ.

Note that by Corollary 4.11 there are at most 72 tuples to consider in step 1 of the algorithm (in reality, it usually suffices to test only a few).

4.6.1 Handling non-maximal prime ideals

It often happens that Algorithm 4.38 returns a prime ideal P which is not maximal. In this case, the finitely presented group has infinitely many L_3-images; in particular, it is infinite. However, it is not immediately clear which $\mathrm{L}_3(q)$ or $\mathrm{U}_3(q)$ occur as images. For example, it might happen that for some maximal ideal $\mathfrak{t} \supseteq P$, the corresponding representation is not absolutely irreducible. Since there are infinitely many maximal ideals containing P, it would be nice to know beforehand which of those lead to absolutely irreducible representations and which do not. Similar considerations apply for the other types of subgroups of $\mathrm{L}_3(q)$. The algorithms in this section accomplish exactly this.

Algorithm 4.42 (L_3-IrreducibilityCondition)**.** *Input:* An L_3-ideal P which is not maximal. *Output:* A set of prime ideals $\mathcal{P}$ satisfying the following property. If $\mathfrak{t} \trianglelefteq \mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$ is a maximal ideal containing P with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(3,q)$, then Δ is not absolutely irreducible if and only if $\mathfrak{t}$ contains some ideal in $\mathcal{P}$.
Algorithm: Return the set of minimal associated prime ideals of $P+\rho$, where ρ is the ideal of Proposition 4.12.

Algorithm 4.43 (L_3-ImprimitiveCondition)**.** *Input:* An L_3-ideal P which is not maximal. *Output:* A set of prime ideals $\mathcal{P}$ satisfying the following property. If $\mathfrak{t} \trianglelefteq \mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$ is a maximal ideal containing P with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ such that Δ is absolutely irreducible, then Δ is imprimitive if and only if $\mathfrak{t}$ contains some ideal in $\mathcal{P}$.
Algorithm: Let $I_1,\dots,I_7$ be the ideals of Proposition 4.28. Compute the set of minimal associated primes $\mathcal{P}_i$ of $P+I_i$ for $i=1,\dots,7$. Return the set of minimal elements of $\bigcup_{i=1}^{7}\mathcal{P}_i$.

Algorithm 4.44 (L_3-OrthogonalCondition)**.** *Input:* An L_3-ideal P which is not maximal. *Output:* A set of prime ideals $\mathcal{P}$ satisfying the following property. If $\mathfrak{t} \trianglelefteq \mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$ is a maximal ideal containing P with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ such that Δ is absolutely irreducible, then the induced projective representation maps into an orthogonal group if and only if $\mathfrak{t}$ contains some ideal in $\mathcal{P}$.
Algorithm: Let $I_1,\dots,I_9$ be the set of all Σ-conjugates of the ideal in Proposition 4.30. Compute the set of minimal associated primes $\mathcal{P}_i$ of $P+I_i$ for $i=1,\dots,9$. Return the set of minimal elements of $\bigcup_{i=1}^{9}\mathcal{P}_i$.

Algorithm 4.45 (L_3-ExceptionalCondition)**.** *Input:* An L_3-ideal P which is not maximal. *Output:* A set of prime ideals $\mathcal{P}$ satisfying the following property. If $\mathfrak{t} \trianglelefteq \mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$ is a maximal ideal containing P with corresponding representation $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ such that Δ is absolutely irreducible, then the induced projective representation maps onto one of the exceptional groups A_6, $\mathrm{L}_2(7)$, $\mathrm{PGU}(3,2)$, $\mathrm{PSU}(3,2)$, H_{36}, A_7, or M_{10}, if and only if $\mathfrak{t}$ contains some ideal in $\mathcal{P}$.

Algorithm: Let I_i run through all the ideals of Proposition 4.25. Compute the set of minimal associated primes $\mathcal{P}_i$ of $P + I_i$ for all i. Return the set of minimal elements of $\bigcup_i \mathcal{P}_i$.

If $P \trianglelefteq \mathbb{Z}[\zeta][x_1, \ldots, x_{[1,2]}]$ is an L_3-ideal which is not maximal, it gives rise to infinitely many L_3-quotients. As is shown in Chapter 6, one can study those quotients by imposing further conditions, e.g. by adding relations to the ideal. This new ideal is not prime any more in general, so it is handy to have the following algorithm which computes all zeroes of the new ideal.

Algorithm 4.46 (L_3-ideals)**.** *Input:* An ideal $I \trianglelefteq \mathbb{Z}[\zeta][x_1, \ldots, x_{[1,2]}]$.
Output: A minimal set Λ of L_3-ideals satisfying the following property. If $\Delta\colon F_2 \to \mathrm{SL}(3, q)$ with $q > 2$ is a representation with trace tuple t inducing an epimorphism of G onto $\mathrm{PSL}(3, q)$, $\mathrm{PSU}(3, \sqrt[2]{q})$, $\mathrm{PGL}(3, \sqrt[3]{q})$, or $\mathrm{PGU}(3, \sqrt[6]{q})$, where t is a zero of I, then ${}^{\sigma}t$ is a zero of an ideal in Λ for some $\sigma \in \Sigma$.
Algorithm:

1. Compute the set $\mathcal{P}$ of minimal associated prime ideals of I.

2. Choose a set of representatives $\mathcal{R}$ of $\mathcal{P}$ under the action of Σ.

3. Return all elements of $\mathcal{R}$ which do not lead to reducible representations or to epimorphisms onto A_6, $\mathrm{L}_2(7)$, $\mathrm{PGU}(3, 2)$, $\mathrm{PSU}(3, 2)$, H_{36}, A_7, or M_{10}, or onto orthogonal or imprimitive groups.

Chapter 5

Theoretical consequences

The theory developed for the L_3-U_3-quotient algorithm has some interesting consequences which are not of an algorithmic nature. First of all, it leads to a generalization of a theorem on matrix groups by Lubotzky for degree 3. Furthermore, if a finitely presented group G on two generators has infinitely many quotients of L_3-type, this infiniteness still has a certain structure. For example, if G has quotients of L_3-type in infinitely many characteristics, then it has quotients of L_3-type in almost every characteristic, cf. Theorem 5.8. In certain cases there is even a bound on the degree of the finite fields, cf. Proposition 5.6.

5.1 A generalization of Lubotzky's One For Almost All Theorem

Fix some $n \in \mathbb{N}$. For a prime p denote by $\pi_p\colon \mathrm{SL}(n, \mathbb{Z}) \to \mathrm{SL}(n, p)$ the reduction mod p. In [Lub99], Lubotzky proves the following theorem.

Theorem 5.1 ([Lub99, Proposition 1])**.** *Let $A \subseteq \mathrm{SL}(n, \mathbb{Z})$. Assume that $\langle \pi_p(A) \rangle = \mathrm{SL}(n, p)$ for some prime p with $(n, p) \notin \{(2, 2), (2, 3), (3, 2), (4, 2)\}$. Then $\langle \pi_q(A) \rangle = \mathrm{SL}(n, q)$ for almost all primes q, i.e., for all but finitely many primes.*

Using the results of the preceeding chapter, we can give a generalization of Lubotzky's Theorem for the case $n = 3$. If R is a ring and $P \trianglelefteq R$ a prime ideal, denote by $\pi_P\colon \mathrm{SL}(3, R) \to \mathrm{SL}(3, R/P)$ the reduction mod P. Furthermore, for a subgroup $U \leq \mathrm{SL}(3, q)$ denote by $\overline{U} \leq \mathrm{PSL}(3, q)$ the corresponding projective subgroup.

Theorem 5.2. *Let R be an order of a number field or a univariate polynomial ring over a finite field, and $A \subseteq \mathrm{SL}(3, R)$. Assume that there exists a prime ideal $\{0\} \neq P \trianglelefteq R$ such that $\overline{\langle \pi_P(A) \rangle}$ is a group of L_3-type not isomorphic to $\mathrm{L}_3(2)$, $\mathrm{U}_3(2)$, or $\mathrm{PGU}(3, 2)$. Then $\overline{\langle \pi_Q(A) \rangle}$ is a group of L_3-type for almost all prime ideals $\{0\} \neq Q \trianglelefteq \mathcal{O}$.*

We will need the following elementary lemma.

Lemma 5.3. *Let R be a Noetherian domain of Krull dimension 1 and $\mathcal{P}$ an infinite set of prime ideals of R. Then $\bigcap \mathcal{P} = \{0\}$.*

Proof. Let $I = \bigcap \mathcal{P}$. Then I is a radical ideal, and since R is Noetherian, we can write $I = Q_1 \cap \cdots \cap Q_k$ for finitely many prime ideals $Q_1, \ldots, Q_k \trianglelefteq R$. Choose pairwise distinct

$P_1, \dots, P_{k+1} \trianglelefteq R$; for every $1 \leq i \leq r+1$ we have $Q_1 \cap \cdots Q_k \subseteq P_i$, and since P_i is prime there exists some j with $Q_j \subseteq P_i$. In particular, there exists some j with $Q_j \subseteq P_i \cap P_k$ for some $1 \leq i \neq k \leq r+1$. But then Q_j must have Krull dimension 1, i.e. $Q_j = \{0\}$, which shows $I = \{0\}$. □

Proof of Theorem 5.2. By adjoining a primitive third root of unity ζ to R if necessary, we can assume that R is a residue class ring of $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$. In particular, we can regard trace tuples in R as zeroes of ideals in $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$.

Assume $\overline{\langle \pi_P(A) \rangle} \cong G(q)$, where $G(q)$ is one of the groups $\mathrm{L}_3(q)$, $\mathrm{U}_3(q)$, $\mathrm{PGL}(3,q)$, or $\mathrm{PGU}(3,q)$, for some prime power $q > 2$. Since $G(q)$ is finite, we can assume that A is finite, so $A = \{a_1, \dots, a_k\}$. Furthermore, $G(q)$ can be generated by two elements (cf. [Ste62]), so in particular there exist words $w_1, w_2 \in F_k$, the free group of rank k, such that

$$\langle \pi_P(w_1(a_1, \dots, a_k)), \pi_P(w_2(a_1, \dots, a_k)) \rangle \cong G(q).$$

Since $\langle w_1(a_1, \dots, a_k), w_2(a_1, \dots, a_k) \rangle \leq \langle A \rangle$ we can assume in fact $|A| = 2$. Let t be the trace tuple corresponding to the representation $F_2 \to \mathrm{SL}(3,R)\colon g_i \mapsto a_i$. For every prime ideal $Q \trianglelefteq R$ let $t_Q \in R/Q$ be the image of the trace tuple in R/Q. Then t_Q is the trace tuple of the representation $F_2 \to \mathrm{SL}(3, R/Q)\colon g_i \mapsto \pi_Q(a_i)$, whose image is $\langle \pi_Q(A) \rangle$. It is enough to show that for all but finitely many prime ideals $\{0\} \neq Q \trianglelefteq R$, t_Q is an absolutely irreducible trace tuple which is not imprimitive or orthogonal, and which does not lead to an exceptional group.

Let $\{0\} \neq I = \langle f_1, \dots, f_k \rangle \trianglelefteq \mathbb{Z}[\zeta][x_1, \dots, x_n]$, and let $\mathcal{Q}$ be the set of prime ideals $\{0\} \neq Q \trianglelefteq R$ such that t_Q is a zero of I, i.e., $f_i(t) \in Q$ for all $1 \leq i \leq k$. If $\mathcal{Q}$ is infinite, this implies $f_i(t) \in \bigcap \mathcal{Q} = \{0\}$ by Lemma 5.3, i.e., $f_i(t) = 0$, so t is a zero of I.

Now let I run through the ideals of Propositions 4.12, 4.25, 4.28, and 4.30 to see that there are only finitely many prime ideals $\{0\} \neq Q \trianglelefteq R$ such that t_Q is absolutely irreducible, imprimitive, orthogonal or exceptional. This proves the theorem. □

5.2 L_3-ideals of positive Krull dimension

A finitely presented group on two generators has infinitely many quotients of L_3-type if and only if it has an L_3-ideal of positive Krull dimension. There are roughly three types which behave quite differently. The first kind leads to L_3-quotients in a single characteristic, but of arbitrary high degree of the field. The second kind leads to L_3-quotients in almost every characteristic, but of bound degree of the fields. And the third kind exhibits both phenomena, i.e., it leads to L_3-quotients in almost every characteristic, and of arbitrary high degree of the field.

Definition 5.4. Let $P \trianglelefteq \mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$ be an L_3-ideal which is not maximal. Let d be the Krull dimension of P and $P \cap \mathbb{Z} = \langle p \rangle$ for some $p \in \mathbb{Z}_{\geq 0}$.

1. If $p \neq 0$, then P is called an ideal of type $\mathrm{L}_3(p^{\infty^d})$. If $d = 1$, we also write $\mathrm{L}_3(p^\infty)$.

2. If $p = 0$ and $d = 1$, set $k := \mathrm{Dim}_{\mathbb{Q}}(\mathbb{Q}[\zeta][x_1, \dots, x_{[1,2]}]/P \otimes_{\mathbb{Z}} \mathbb{Q})$. Then P is called an ideal of type $\mathrm{L}_3(\infty^k)$.

3. If $p = 0$ and $d > 1$, P is called an ideal of type $\mathrm{L}_3(\infty^{\infty^{d-1}})$. If $d = 2$, we also write $\mathrm{L}_3(\infty^\infty)$.

The ∞ in $\mathrm{L}_3(p^\infty)$ indicates that there are infinitely many choices for the exponent, cf. Proposition 5.5. Similarly, $\mathrm{L}_3(\infty^k)$ indicates that there are infinitely many choices for the prime, cf. Proposition 5.6. Finally, $\mathrm{L}_3(\infty^\infty)$ indicates that there are infinitely many choices for the prime as well as for the exponent. A higher Krull dimension allows an even higher degree of freedom.

Proposition 5.5. *Let G be a finitely presented group on two generators, and let P be an L_3-ideal of G of type $\mathrm{L}_3(p^{\infty^d})$. There exist infinitely many $k \in \mathbb{N}$ such that G has quotients isomorphic to $\mathrm{L}_3(p^k)$, $\mathrm{U}_3(p^k)$, $\mathrm{PGL}(3,p^k)$, or $\mathrm{PGU}(3,p^k)$. Furthermore, for every $k \in \mathbb{N}$ there exist at most finitely many quotient of G of L_3-type over $\mathbb{F}_{p^k}$ which come from zeroes of P.*

Proof. Set $R := \mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]/P$; then R has characteristic p and Krull dimension d. Thus there exist infinitely many $k \in \mathbb{N}$ such that there exist epimorphisms $\varphi\colon R \to \mathbb{F}_{p^k}$. Every such epimorphism yields a trace tuple $t \in \mathbb{F}_{p^k}^9$, by setting $t_i := \varphi(x_i)$. We show that the set of those trace tuples such that the corresponding quotient is not of L_3-type are zeroes of an ideal of dimension at most $d-1$.

The argument is analogous to the one given in the proof of Theorem 5.2. Note that t yields a group of L_3-type if and only if it is not a zero of some ideal of Propositions 4.12, 4.25, 4.28, or 4.30. Let I be the intersection of all of those ideals, so t yields a group of L_3-type if and only if t is not a zero of I. We show $I \not\subseteq P$. For suppose $I \subseteq P$. Since I is an intersection of ideals $I_1 \cap \dots \cap I_r$ and P is prime, this implies $I_j \subseteq P$ for some j. But then P contains one of the ideals of the propositions, hence it is not an L_3-ideal, which is a contradiction.

Now t is a zero of I if and only if φ factors over $I+P$. But $I+P \supsetneqq P$ shows that $I+P$ has dimension at most $d-1$. Thus there are infinitely many zeroes of P which are not zeroes of $I+P$, i.e., giving quotients of L_3-type.

For the last statement notice that every finitely generated ring R has only finitely many epimorphisms onto $\mathbb{F}_{p^k}$ for any given k. □

This result indicates that there is no *qualitative* difference between the L_3-ideals of type $\mathrm{L}_3(p^\infty)$ and $\mathrm{L}_3(p^{\infty^2})$, in the sense that they exhibit the same type of quotients of L_3-type. There is however a *quantitative* difference, in the sense that for a given $k \in \mathbb{N}$, there are more quotients coming from ideals of the latter type than from ideals of the former type. This observation can be made more precise by defining so called growth parameters, cf. [PF09, Proposition 3.14].

Proposition 5.6. *Let G be a finitely presented group on two generators, and let P be an L_3-ideal of G of type $\mathrm{L}_3(\infty^k)$. For almost all primes p there exists $\ell | k$ such that G has quotients of L_3-type over $\mathbb{F}_{p^\ell}$. Furthermore, for every prime p there exist at most finitely many quotients of L_3-type in characteristic p which come from zeroes of P.*

Proof. Set $R := \mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]/P$; then R has characteristic 0 and Krull dimension 1. As in the proof of Proposition 5.5 one shows that almost all primes occur, and that for every prime p there are at most finitely many quotients of L_3-type in characteristic p.

It remains to show the statement about ℓ. To see this, let K be the quotient field of R and $\mathcal{O} \subseteq K$ the maximal order. Then for almost all primes p we have $\mathcal{O}_{\langle p \rangle} = R_{\langle p \rangle}$; in particular, the residue class fields of $\mathcal{O}$ and R in characteristic p are the same. But for all primes p the degree of the residue class field of $\mathcal{O}$ is a divisor of k. □

Corollary 5.7. *Let G be a finitely presented group on two generators, and let P be an* L_3*-ideal of G of type* $\mathrm{L}_3(\infty^{\infty^d})$*. For almost all primes p there exists infinitely many $k \in \mathbb{N}$ such that G has quotients of* L_3*-type over* $\mathbb{F}_{p^k}$*.*

Proof. Set $R := \mathbb{Z}[\zeta][x_1, \ldots, x_{[1,2]}]/P$; then R has characteristic 0 and Krull dimension $d+1$. Let $Q \trianglelefteq \mathbb{Z}[\zeta][x_1, \ldots, x_{[1,2]}]$ be a prime ideal containing P of Krull dimension 1 such that R/Q has characteristic 0. The $\mathbb{Q}$-dimension of $\mathbb{Q} \otimes_{\mathbb{Z}} (R/Q)$ can be arbitrarily high. By the argument in the proof of Proposition 5.5, some choice of Q will yield an L_3-ideal of type $\mathrm{L}_3(\infty^k)$ for some k. □

The next theorem is similar to Lubotzky's Theorem.

Theorem 5.8. *Let G be a finitely presented group on two generators which has quotients of* L_3*-type in infinitely many characteristics. Then G has quotients of* L_3*-type in almost every characteristic.*

Proof. Let $\mathcal{P}$ be the set of characteristics where quotients of L_3-type occur. For any $p \in \mathcal{P}$ choose a trace tuple $t_p \in \overline{\mathbb{F}_p}^9$ leading to a quotient of L_3-type. Then every t_p is a zero of some trace presentation ideal of G. Since there are only finitely many trace presentation ideals, and every trace presentation ideal has only finitely many minimal associated prime ideals, there exists a prime ideal P such that t_p is a zero of P for infinitely many $p \in \mathcal{P}$. In particular, P must be an L_3-ideal of type $\mathrm{L}_3(\infty^k)$ for some $k \in \mathbb{N}$ or $\mathrm{L}_3(\infty^{\infty^d})$ for some $d \in \mathbb{N}$, so the result follows by Proposition 5.6 or Corollary 5.7. □

The results of this section can be made more precise for any given P. This is done in Chapters 6 and 7, where the infinite set of L_3-quotients is explicitly enumerated.

Chapter 6

Examples

Now the algorithm will be applied to several finitely presented groups. For this, an implementation in the computer algebra system Magma ([BCP97]) is used. There are roughly two types of examples: finitely presented groups which have only finitely many quotients of L_3-type, and the others which have infinitely many such quotients.

In the first case, the algorithm gives no information on whether the group in question is finite or infinite. It does however give an infinite list of simple groups which do *not* occur as quotients. While this might seem trivial at first, there appears to be no other method to get a similar result without determining the isomorphism type of the group, or proving it finite. Furthermore, often a group is proved finite by finding a small simple quotient, and then using coset enumeration; the algorithm shows which groups can *not* be used.

In the second case, the algorithm proves that the group is infinite. But the output of the algorithm can be used for much more than a mere proof of infinity; it gives a lot of structural information about the group. The groups with infinitely many quotients of L_3-type can be further divided. Those groups which have quotients in infinitely many characteristics, and those which have only quotients in a single characteristic, or in finitely many characteristics. The former type seems to occur much more often than the latter.

In a lot of cases, a detailed enumeration of all quotients of L_3-type can be given. The easiest cases where this is possible are the ones where all prime ideals returned by the algorithm have Krull dimension 0 or 1. However, even if the Krull dimension is bigger, definite results can be given. This is done in the next chapter, where all quotients of L_3-type of the group $\mathrm{C}_2 * \mathrm{C}_3$ are counted.

6.1 Groups with finitely many quotients of L_3-type

There are various examples of finitely presented groups which only have finitely many quotients of L_3-type. The examples given in this section come from two different sources. The first is by altering known presentations of finite simple groups; the second is the family of group presentations defined by Coxeter.

6.1.1 A detailed example

The first example is used to illustrate the algorithm step by step.

Example 6.1. Let $G = \langle a, b | a^2, b^4, (ab)^{11}, (ab^2)^5 \rangle$. In theory, there are $3^4 = 81$ sign systems to consider, but as explained in Section 8.1 it suffices to handle the five sign systems

$$s_1 := (1,1,1,1),\ s_2 := (1,1,\zeta,1),\ s_3 := (1,1,1,\zeta),\ s_4 := (1,1,\zeta,\zeta),\ s_5 := (1,1,\zeta,\zeta^2).$$

In step 1 of Algorithm 4.38, the various minimal associated prime ideals are calculated. For $I_{s_1}(G)$ they are

$$P_1 := \langle x_1 - 3, x_{-1} - 3, x_2 - 3, x_{-2} - 3x_{1,2} - 3, x_{-1,2} - 3, x_{-2,1} - 3, x_{-2,-1} - 3, x_{[1,2]} - 3, \rangle$$

and

$$P_2 := \langle 881, x_1 + 1, x_{-1} + 1, x_2 + 880, x_{-2} + 880,\\ x_{1,2} + 604, x_{-1,2} + 604, x_{-2,1} + 604, x_{-2,-1} + 604, x_{[1,2]} + 245 \rangle,$$

for $I_{s_2}(G)$ they are

$$P_3 := \langle 3, \zeta + 2, x_1, x_{-1}, x_2, x_{-2}, x_{1,2}, x_{-1,2}, x_{-2,1}, x_{-2,-1}, x_{[1,2]} \rangle$$

and

$$P_4 := \langle 5081, x_1 + 1, x_{-1} + 1, x_2 + 5080, x_{-2} + 5080, x_{1,2} + 338\zeta + 3225, x_{-1,2} + 338\zeta + 3225,\\ x_{-2,1} + 4743\zeta + 2887, x_{-2,-1} + 4743\zeta + 2887, x_{[1,2]} + 1467 \rangle$$

and $I_{s_i}(G)$ for $i = 3, 4, 5$ only have the one associated prime ideal P_3. So $\mathcal{P}' = \{P_1, P_2, P_3, P_4\}$, but $P_3 \supseteq P_1$, hence $\mathcal{P} = \{P_1, P_2, P_4\}$ is the list of minimal prime ideals computed in step 1. Since the three ideals all contain different integers, or no integer at all, it is obvious that they can not lie in the same orbit under $\Sigma \rtimes (Z \times T)$, so $\mathcal{R} = \mathcal{P}$ in step 2.

In step 3, the various subgroups are tested. The ideal P_1 contains the ideal ρ of Proposition 4.12, so it does not lead to an absolutely irreducible representation and is therefore removed. The other two ideals pass the irreducibility test; however the ideal P_2 gives a representation into $\mathrm{PSO}(3, 881)$, and hence is also removed. This leaves the ideal P_4, which is neither orthogonal nor imprimitive. Furthermore, G has no epimorphisms onto one of the exceptional groups, so P_4 is an L_3-ideal.

The algorithm returns the set $\{P_4\}$.

Now Algorithm 4.40 can be called to compute the L_3-type of P_4. In step 1, n is computed to be 2. The stabilizer of P_4 in Σ is trivial, and ${}^{z}P_4 = {}^{\tau}P_4$, so P_4 corresponds to an epimorphism onto $\mathrm{PSU}(3, 5081)$. This also can be readily seen by looking at the corresponding trace tuple

$$t = (-1, -1, 1, 1, 1856 + 4743\zeta, 1856 + 4743\zeta, 2194 + 338\zeta, 2194 + 338\zeta, -1467) \in \mathbb{F}_{5081^2}^9.$$

It is obvious that no Σ-conjugate of t lies in the proper subfield $\mathbb{F}_{5081}$ by looking at the entries t_1 and t_2. These entries also already show that the stabilizer in Σ is trivial. Finally ${}^{\tau}t = {}^{\alpha}t$, where $\alpha\colon \mathbb{F}_{5081^2} \to \mathbb{F}_{5081^2} \colon x \mapsto x^{5081}$ is the Galois automorphism of order 2, which proves that the corresponding representation is unitary.

6.1.2 The Coxeter presentations $(2, m, n; k)$

For a quadruple (ℓ, m, n, k) of positive integers, Coxeter defined the presentation

$$(\ell, m, n; k) := \langle a, b \mid a^\ell, b^m, (ab)^n, [a, b]^k \rangle,$$

cf. [Cox39]. These groups were extensively studied, see e.g. [EJ08] for an overview and references.

If $\ell = 2$, for almost every choice of m, n, k there are at most finitely many L_3-images. To see this, note that the trace presentation ideal of the free group F_2 has dimension 9. Assume that $\Delta\colon F_2 \to \mathrm{SL}(3, k)$ is an absolutely irreducible representation such that the corresponding projective representation factors over $(2, m, n; k)$, and let $t = (t_1, \ldots, t_{[1,2]}) \in \mathbb{F}_q^9$ be the trace tuple of Δ. Acting by sign changes we can assume that $\Delta(a)$ has order 2, so the characteristic polynomial is $(X - 1)(X + 1)^2 = X^3 + X^2 - X - 1$, i.e., $t_1 = t_{-1} = 1$. Furthermore, $\Delta(ab) = \Delta(a^{-1}b)$ and $\Delta(ab^{-1}) = \Delta(a^{-1}b^{-1})$, hence $t_{1,2} = t_{-1,2}$ and $t_{-2,1} = t_{-2,-1}$. Therefore, any trace presentation ideal of $\langle a, b \mid a^2 \rangle$ has dimension 5. Specifying the order of b and of ab imposes conditions on t_2, t_{-2}, $t_{1,2}$ and $t_{-2,-1}$, since $X^3 - t_2X^2 + t_{-2}X = 1$ is the characteristic polynomial of $\Delta(b)$, and similarly for $\Delta(ab)$; so a trace presentation ideal of $\langle a, b \mid a^2, b^m, (ab)^n \rangle$ has dimension at most 1.

The trace of the commutator (and of its inverse) satisfies a quadratic relation in the other traces. Hence it can happen that the specification of the order of $[a, b]$ does not reduce the dimension of the trace presentation ideal; however, this phenomenon is rather exceptional, and usually a further specification of the order of $[a, b]$ yields an ideal which is either trivial or of dimension 0.

Example 6.2. We study the groups $(2, 4, 7; k)$ for various $k \in \mathbb{N}$.

For $k \leq 4$ there are no L_3 quotients at all, and $(2, 4, 7; 5)$ has the quotient $\mathrm{L}_3(2^2)$. For $k = 14$, there are infinitely many quotients, which is further studied in Section 6.2.

For $k = 40$ the group has the L_3 quotients $\mathrm{L}_3(2^2)$, $\mathrm{L}_3(11^2)$, $\mathrm{U}_3(17)$, $\mathrm{U}_3(41)$, and $\mathrm{L}_3(79)$. For $k = 41$ the group has the single quotient $\mathrm{L}_3(39067496161)$.

The algorithm also works for fairly high values of k and big primes. For example, for $k = 1009$, there are two quotients, namely $\mathrm{U}_3(889937)$ and

$$\begin{aligned}\mathrm{U}_3(&712629196439971659726943917611425260543107994854691601726702394289853 4\\&342612440686912662395520441822133366882525875284985976442123790562851 3\\&797015907757647355258299704135245743615338637345560735042850519361388 4\\&32729481102530544469023852885383845223228045690286655883153).\end{aligned}$$

6.1.3 Modifying presentations of simple groups

Interesting examples of finitely presented groups with only finitely many L_3 quotients can be constructed by taking presentations of simple groups and modifying the relations. In fact, the example in Section 6.1.1 is of this kind. Here are some other examples.

Example 6.3. The Mathieu group M_{22} can be presented as

$$\langle a, b \mid r_1, \ldots, r_7 \rangle := \langle a, b \mid a^2, b^4, (ab)^{11}, (ab^2)^5, [a, b]^6, [a, bab]^3, (ababab^{-1})^5 \rangle,$$

where the relation $r_5 = [a, b]^6$ is redundant, cf. [WWT$^+$]. The group $\langle a, b \mid r_1, r_2, r_3, r_4 \rangle$ has a single quotient isomorphic to $\mathrm{U}_3(5081)$ (cf. Section 6.1.1), and $\langle a, b \mid r_1, r_2, r_3, r_5 \rangle$ has a single quotient isomorphic to $\mathrm{U}_3(27191)$. While $\langle a, b \,|\, r_1, r_2, r_3, r_7\rangle$ has no L_3 or U_3 quotients, $\langle a, b \,|\, r_1, r_2, r_4, r_7\rangle$ has quotients isomorphic to $\mathrm{L}_3(4)$ and $\mathrm{L}_3(151)$. Moreover, $\mathrm{L}_3(31)$, $\mathrm{U}_3(5)$ and $\mathrm{U}_3(41)$ are quotients of $\langle a, b \,|\, r_1, r_2, r_5, r_7\rangle$, and $\mathrm{L}_3(3319)$ is a quotient of $\langle a, b \,|\, r_1, r_2, r_6, r_7\rangle$. A modification of the relations can give fairly big quotients. For instance, by altering the relation r_6 and computing the quotients of $\langle a, b \,|\, r_1, r_2, r_3, [a, bab]^i\rangle$ for various $i \in \mathbb{N}$ yields quotients $\mathrm{U}_3(23)$ and $\mathrm{L}_3(199)$ for $i = 4$, quotients $\mathrm{U}_3(419)$ and $\mathrm{U}_3(746957111)$ for $i = 5$, and quotients $\mathrm{U}_3(769)$, $\mathrm{U}_3(9437)$ and $\mathrm{U}_3(133078695023)$ for $i = 7$.

Example 6.4. The Mathieu group M_{23} can be presented as

$$\begin{aligned}\langle a, b \,|\, r_1, \ldots, r_9\rangle := \langle a, b \,|\, & a^2, b^4, (ab)^{23}, (ab^2)^6, [a, b]^6, (abab^{-1}ab^2)^4, \\ & (ab)^3ab^{-1}ab^2(abab^{-1})^2(ab)^3(ab^{-1})^3, (abab^2ab^2)^6, (abab^2)^3(ab^2ab^{-1})^2abab^2abab^{-1}ab^2\rangle,\end{aligned}$$

where r_8 is redundant, cf. [WWT$^+$]. The group $\langle a, b \,|\, r_1, r_2, r_4, r_6, r_8\rangle$ has a quotient isomorphic to $\mathrm{U}_3(11)$, and $\langle a, b \,|\, r_1, r_2, r_4, r_5, r_8\rangle$ has a quotient isomorphic to $\mathrm{U}_3(23)$, while the groups $\langle a, b \,|\, r_1, r_2, r_7\rangle$ and $\langle a, b \,|\, r_1, r_2, r_9\rangle$ have no L_3 or U_3 quotients.

6.2 Groups with finitely many quotients of L_3-type in almost every characteristic

If the algorithm returns prime ideals which are not maximal, this proves that the finitely presented group has infinitely many quotients of L_3-type. If furthermore the prime ideal has Krull dimension 1, a very precise description of all quotients can be given. There are two types of such prime ideals which demand different techniques to describe the quotients, cf. Section 5.2. The first type contains a prime number, and the second type does not. The former case is treated in the next section, this section is concerned with the latter. In this case, the description is based on some results from algebraic number theory. Assume that P is a prime ideal of $\mathbb{Z}[\zeta][x_1, \ldots, x_{[1,2]}]$ of dimension 1, and $P \cap \mathbb{Z} = \{0\}$. Then almost all zeroes of P are images of a trace tuple with values in the order of a number field (or a localization thereof). Hence the action of the Galois group in characteristic p is determined by the action of the Galois group of the number field. More precisely, the Galois group in characteristic p is determined by an element of the Galois group in characteristic zero, called the Frobenius automorphism, which is unique up to conjugation (cf. e.g. [Neu99, Section I.§8]). Thus the study of infinitely many primes is reduced to the study of finitely many conjugacy classes. This section gives two examples.

6.2.1 One-relator quotients of the modular group

The authors of [CHN12] study one-relator quotients of the modular group. More precisely, they study the groups $\langle a, b \,|\, a^2, b^3, r\rangle$, for all words r of length up to 36. The number of relators to consider can be reduced by utilizing the automorphism group of $\langle a, b \,|\, a^2, b^3\rangle$. Using coset enumeration, Knuth-Bendix completion and automatic groups, they can decide for most groups if they are infinite or finite, and compute the order in the finite case, cf. [CHN12, Section 3]. Only 48 groups are left, which are dealt with later in the paper.

We will now focus on these 48 groups and study them using the L_3-U_3-quotient algorithm. All of the 48 relators are given in [CHN12, Section 5]; the corresponding quotient groups are labeled $Q_1, \ldots, Q_{48}$. All but four of them have no L_3 or U_3 quotients at all. Set $u := ab$ and

$v := ab^{-1}$. The groups $Q_7 = \langle a, b \mid a^2, b^3, u^3vu^3vu^2v^3u^2\rangle$ and $Q_{12} = \langle a, b \mid a^2, b^3, u^{10}v^2uvuv^2\rangle$ have the single quotient $\mathrm{L}_3(3)$, which is already noted in [CHN12]; in fact, they show that both groups are finite.

The group Q_{28} is proved infinite. We can prove the stronger result:

Proposition 6.5. *Let $G = Q_{28} = \langle a, b \mid a^2, b^3, u^4vuvuvuv^4u^2v^2\rangle$, where $u = ab$ and $v = ab^{-1}$. For every prime $p \neq 2, 13$ there exists exactly one quotient of G of L_3-type in characteristic p. More precisely, let $K/\mathbb{Q}$ be the splitting field of $X^6 - 11X^3 + 27$ with Galois group $\Gamma := \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{D}_{12} = \langle (3,4)(5,6), (1,5)(2,3)(4,6)\rangle$. For any prime $p \neq 2, 3, 11$ denote by $\varphi_p \in \Gamma$ the Frobenius automorphism mod p. The quotient in characteristic p is isomorphic to $\mathrm{L}_3(p)$, $\mathrm{U}_3(p)$, $\mathrm{PGL}(3,p)$, or $\mathrm{PGU}(3,p)$, depending on whether φ_p has a fixed point, is a fixed point free element of order 2, has order 3, or has order 6, respectively.*

Furthermore, the quotient in characteristic 3 is isomorphic to $\mathrm{L}_3(3)$; there are no quotients of L_3-type in characteristic 2 and characteristic 13. There is a single L_2 quotient $\mathrm{PGL}(2,13)$.

Each of the quotients $\mathrm{L}_3(p)$, $\mathrm{U}_3(p)$, $\mathrm{PGL}(3,p)$, and $\mathrm{PGU}(3,p)$ occurs for infinitely many primes p. More precisely, we have

Corollary 6.6. *The set of all primes p such that $\mathrm{L}_3(p)$ is a quotient of Q_{28} is infinite and has a density, namely $1/3$. Similarly, there are infinitely many primes such that $\mathrm{U}_3(p)$, $\mathrm{PGL}(3,p)$, and $\mathrm{PGU}(3,p)$ are quotients of Q_{28}, with densities $1/3$, $1/6$, and $1/6$, respectively.*

All of these cases can be distinguished using the knowledge of the decomposition of $X^6 - 11X^3 + 27$ mod p alone, without knowing the Frobenius automorphism. Using Gauß reciprocity, some of these cases can still be distinguished by weaker equivalence conditions.

Corollary 6.7. *Let $p \neq 2, 13$ be a prime. The isomorphism type of the L_3 quotient of Q_{28} in characteristic p is given in the following table.*

	$p^3 \equiv \pm 1 \mod 13$	$p^3 \not\equiv \pm 1 \mod 13$
$p \equiv 1 \mod 3$	$\mathrm{L}_3(p)$ *or* $\mathrm{PGL}(3,p)$	$\mathrm{U}_3(p)$
$p \not\equiv 1 \mod 3$	$\mathrm{L}_3(p)$	$\mathrm{U}_3(p)$ *or* $\mathrm{PGU}(3,p)$

Proof of Proposition 6.5. The L_2-quotient algorithm verifies the statement about the single quotient $\mathrm{PGL}(2,13)$.

The L_3-U_3 quotient algorithm returns the single prime ideal

$$\begin{aligned} P = \langle x_1 + 1, x_{-1} + 1, x_2, x_{-2}, x_{1,2} + 8x_{-1,2} + x^5_{-2,-1} - 11x^2_{-2,-1}, x^3_{-1,2} + x^3_{-2,-1} - 11,\\ 3x^2_{-1,2} + x^4_{-2,-1} - 11x_{-2,-1}, x_{-1,2}x_{-2,-1} - 3, 9x_{-1,2} + x^5_{-2,-1} - 11x^2_{-2,-1},\\ x_{-2,1} - x_{-2,-1}, x_{[1,2]} - 2, x^6_{-2,-1} - 11x^3_{-2,-1} + 27\rangle, \end{aligned}$$

which has Krull dimension 1, so it is of type $\mathrm{L}_3(\infty^{12})$. Let p be a prime, and let $t = (t_1, \ldots, t_{[1,2]}) \in \overline{\mathbb{F}_p}$ be a zero of P. Using Algorithms 4.42, 4.43 and 4.44 one checks that t is always absolutely irreducible, it is imprimitive if and only if $p = 2$, and orthogonal if and only if $p = 13$ (the degeneration in characteristic 13 to an orthogonal trace tuple explains the single L_2 quotient $\mathrm{PGL}(2,13)$, since $\mathrm{PSO}(3,q) \cong \mathrm{PGL}(2,q)$ for every prime power q). The exceptional groups do not occur in any characteristic.

We deal with the case $p = 3$ separately. Computing the minimal associated primes of $P + \langle 3\rangle$ and taking orbits under T using Algorithm 4.46 shows that there is a single quotient isomorphic to $\mathrm{L}_3(3)$.

Now assume $p \notin \{2, 3, 13\}$. Then $\alpha := t_{-2,-1}$ is a zero of $\mu := X^6 - 11X^3 + 27$, and since $p \neq 3$ we see $\alpha \neq 0$, so

$$t = (-1, -1, 0, 0, 3/\alpha, 3/\alpha, \alpha, \alpha, 2).$$

The discriminant of μ is $3^{12}13^3$. Since we assume $p \neq 3, 13$, there are six different choices for α, giving six different choices for the trace tuple. But if α is a root of μ, then $3/\alpha$ and $\zeta\alpha$ is also a root of μ. Hence all six trace tuples lie in a single orbit under $\Sigma \rtimes T$, and in every characteristic there is at most one L_3 or U_3 quotient.
Assume first that φ_p has a fixed point. Then μ has a root in $\mathbb{F}_p$, so we can assume that $t \in \mathbb{F}_p^9$ which shows that the quotient is isomorphic to $\mathrm{L}_3(p)$.
For the other cases the action of the Galois group is important. Note that the zeroes of μ are α, $3\zeta/\alpha$, $\zeta\alpha$, $3/\alpha$, $\zeta^2\alpha$, and $3\zeta^2/\alpha$. Labeling these roots by $1, \ldots, 6$, respectively, the Galois group is given by $\Gamma \cong \langle (1, 2, 3, 4, 5, 6), (1, 4)(2, 3)(5, 6)\rangle$; representatives of the conjugacy classes are $()$, $(2, 6)(3, 5)$, $(1, 2)(3, 6)(4, 5)$, $(1, 4)(2, 5)(3, 6)$, $(1, 3, 5)(2, 4, 6)$ and $(1, 2, 3, 4, 5, 6)$. The first two elements are already taken care of. Now assume $\varphi_p = (1, 2)(3, 6)(4, 5)$. Then

$$^{\varphi_p}({}^{(1,\zeta^2)}t) = (-1, -1, 0, 0, \zeta\alpha, \zeta\alpha, 3\zeta^2/\alpha, 3\zeta^2/\alpha, 2) = {}^{\tau}({}^{(1,\zeta^2)}t),$$

so the quotient in characteristic p is isomorphic to $\mathrm{U}_3(p)$, cf. Proposition 4.32. If $\varphi_p = (1, 4)(2, 5)(3, 6)$ then ${}^{\varphi_p}t = {}^{\tau}t$, which also yields $\mathrm{U}_3(p)$.
If $\varphi_p = (1, 3, 5)(2, 4, 6)$,

$$^{\varphi_p}t = (-1, -1, 0, 0, 3\zeta^2/\alpha, 3\zeta^2/\alpha, \zeta\alpha, \zeta\alpha, 2) = {}^{(1,\zeta^2)}t,$$

hence the quotient in characteristic p is isomorphic to $\mathrm{PGL}(3, p)$, cf. Proposition 4.31.
Finally, if $\varphi_p = (1, 2, 3, 4, 5, 6)$ then $\varphi_p^3 = (1, 4)(2, 5)(3, 6)$ shows that the trace tuple is unitary, and φ_p^2 shows that the tuple is pgl, hence the quotient is isomorphic to $\mathrm{PGU}(3, p)$. □

Proof of Corollary 6.6. This is an application of Chebotarev's Density Theorem, cf. [Neu99, Theorem VII.13.4]. The conjugacy classes of the dihedral group

$$\Gamma := \mathrm{D}_{12} = \langle (3, 4)(5, 6), (1, 5)(2, 3)(4, 6)\rangle$$

are $()^\Gamma$ of size 1 and $(3, 4)(5, 6)^\Gamma$ of size 3, both resulting in the L_3-type quotient $\mathrm{L}_3(p)$, $(1, 2)(3, 5)(4, 6)^\Gamma$ of size 1 and $(1, 2)(3, 6)(4, 5)^\Gamma$ of size 3 yielding $\mathrm{U}_3(p)$, and $(1, 3, 4)(2, 5, 6)^\Gamma$ and $(1, 5, 4, 2, 3, 6)^\Gamma$ both of size 2 yielding $\mathrm{PGL}(3, p)$ and $\mathrm{PGU}(3, p)$, respectively. □

Proof of Corollary 6.7. First note that if $\zeta \in \mathbb{F}_p$, then μ must be reducible. To see this, suppose that μ is irreducible; let γ be a generator of the Galois group. Then $\gamma(\alpha) = 3\zeta/\alpha$, and, since ζ is in the ground field, $\gamma(3\zeta/\alpha) = \alpha$. Thus, γ has order 2, which is a contradiction. Hence μ splits into linear factors, into three quadratic factors, or into two cubic factors, if $3|p - 1$.
Next note that μ can be written as $(X^3 - \beta_1)(X^3 - \beta_2)$ for some $\beta_1, \beta_2 \in \mathbb{F}_p$ if and only if $X^2 = 13$ has a solution in $\mathbb{F}_p$.
Finally note that if $\zeta \notin \mathbb{F}_p$, then $X^3 - \beta$ has always a solution in $\mathbb{F}_p$.
By the Gauss reciprocity law, $X^2 = 13$ has a solution in $\mathbb{F}_p$ if and only if $p \equiv \pm 1, \pm 3, \pm 4 \mod 13$. Summing up these results shows that the quotients occur as given in the table. □

The fourth group in the list of [CHN12] which has L_3-type quotients is Q_{30}; this group also has finitely many quotients in any characteristic, but here the decomposition of a polynomial mod p is not enough to distinguish all cases. The proof is omitted, it is similar to the proof of Proposition 6.5.

Proposition 6.8. *Let $G = Q_{30} = \langle a, b \mid a^2, b^3, u^4vuv^2u^2vuv^4uv\rangle$, where $u = ab$ and $v = ab^{-1}$. The only L_2-type quotient of G is $\mathrm{PGL}(2, 11)$. The L_3-type quotients in characteristic 3, 5, 11, and 37 are $\mathrm{L}_3(3^2)$, $\mathrm{PGU}(3, 5)$, $\mathrm{PGU}(3, 11)$, and $\mathrm{PGL}(3, 37^2)$.*
Let $K/\mathbb{Q}$ be the splitting field of $X^{12} - 9X^9 + 27X^6 - 21X^3 + 1$ with Galois group

$$\begin{aligned}\Gamma &:= \mathrm{Gal}(K/\mathbb{Q})\\ &\cong \langle(7,12)(8,11)(9,10),(1,9)(2,10)(3,7)(4,8)(5,11)(6,12),(3,5)(4,6)(7,9)(8,10)\rangle.\end{aligned}$$

For any prime $p \neq 3, 5, 11, 37$ denote by $\varphi_p \in \Gamma$ the Frobenius automorphism mod p. Table 6.1 lists the L_3-type quotients of G in characteristic p, and the density of primes and the smallest prime for every Frobenius automorphism.

representative of φ_p^Γ	L_3-type quotients	density of primes	smallest p
$()$	$\mathrm{L}_3(p)$, $\mathrm{L}_3(p)$	1/144	2269
$(1,2)(3,6)(4,5)$	$\mathrm{U}_3(p)$, $\mathrm{L}_3(p)$	6/144	79
$(1,3,5)(2,4,6)$	$\mathrm{PGL}(3,p)$, $\mathrm{L}_3(p)$	4/144	379
$(1,3)(2,4)(7,9)(8,10)$	$\mathrm{L}_3(p)$, $\mathrm{L}_3(p)$	9/144	59
$(1,2)(3,4)(5,6)(7,9)(8,10)$	$\mathrm{U}_3(p)$, $\mathrm{L}_3(p)$	6/144	131
$(1,3)(2,4)(7,10,11,8,9,12)$	$\mathrm{L}_3(p)$, $\mathrm{PGU}(3,p)$	12/144	29
$(1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$	$\mathrm{U}_3(p)$, $\mathrm{U}_3(p)$	1/144	401
$(1,2)(3,6)(4,5)(7,8)(9,12)(10,11)$	$\mathrm{U}_3(p)$, $\mathrm{U}_3(p)$	9/144	31
$(1,7)(2,8)(3,9)(4,10)(5,11)(6,12)$	$\mathrm{L}_3(p^2)$	6/144	67
$(1,7)(2,8)(3,11)(4,12)(5,9)(6,10)$	$\mathrm{L}_3(p^2)$	6/144	23
$(1,2)(3,6)(4,5)(7,9,11)(8,10,12)$	$\mathrm{U}_3(p), \mathrm{PGL}(3,p)$	12/144	19
$(1,2)(3,4)(5,6)(7,12,9,8,11,10)$	$\mathrm{U}_3(p), \mathrm{PGU}(3,p)$	4/144	191
$(1,3,5)(2,4,6)(7,9,11)(8,10,12)$	$\mathrm{PGL}(3,p), \mathrm{PGL}(3,p)$	4/144	199
$(1,7,2,8)(3,9,6,12)(4,10,5,11)$	$\mathrm{U}_3(p^2)$	18/144	7
$(1,7,2,8)(3,11,6,10)(4,12,5,9)$	$\mathrm{U}_3(p^2)$	18/144	2
$(1,7,3,9,5,11)(2,8,4,10,6,12)$	$\mathrm{PGL}(3,p^2)$	12/144	97
$(1,7,3,11,5,9)(2,8,4,12,6,10)$	$\mathrm{PGL}(3,p^2)$	12/144	47
$(1,4,5,2,3,6)(7,10,11,8,9,12)$	$\mathrm{PGU}(3,p)$, $\mathrm{PGU}(3,p)$	4/144	89

Table 6.1: The L_3-type quotients of Q_{30} in characteristic $p \neq 3, 5, 11, 37$

6.2.2 Coxeter presentations

This section is a continuation of Example 6.2, where the groups

$$(2, 4, 7; k) = \langle a, b \mid a^2, b^4, (ab)^7, [a, b]^k\rangle$$

for various $k \in \mathbb{N}$ are studied. The algorithm can compute the quotients of L_3-type for any fixed value k. By looking at the group $\langle a, b \mid a^2, b^4, (ab)^7\rangle$ instead, a uniform answer for any value of k can be given. Furthermore, the infinite number of quotients for $k = 14$ can be explained.

Proposition 6.9. *Let $k \in \mathbb{N}$. The group $G = (2,4,7;k) = \langle a, b \mid a^2, b^4, (ab)^7, [a,b]^k \rangle$ has infinitely many quotients of L_3-type if and only if $14|k$.*
More precisely, let $\mathcal{P}$ be the set of primes > 7 such that $(X^2 - (\alpha - 1)X + 1)|(X^k - 1)$ for some root $\alpha \in \mathbb{F}_{p^2}$ of $X^2 - 5X + 1$. Then $\mathcal{P}$ is finite, and for any $p \in \mathcal{P}$, the group $(2,4,7;k)$ has L_3-quotients in characteristic p as specified in the following table.

	$p^3 \equiv 1 \mod 7$	$p^3 \not\equiv 1 \mod 7$
$p \equiv 1 \mod 3$	$\mathrm{L}_3(p)^2$	$\mathrm{L}_3(p^2)$
$p \not\equiv 1 \mod 3$	$\mathrm{L}_3(p^2)$	$\mathrm{U}_3(p)^2$

If $7|k$, the group has the additional quotients $\mathrm{L}_3(2^2)$ and $\mathrm{U}_3(2^3)$.
If $14 \nmid k$, this is a complete list of quotients of L_3-type of $(2,4,7;k)$. If $14|k$, there is the additional quotient $\mathrm{L}_3(7)$, and for any prime $p \neq 2,3,7$ there is an additional finite number of quotients of L_3-type, given in the following table.

	$p \equiv \pm 1 \mod 7$	$p \not\equiv \pm 1 \mod 7$
$p \equiv 1 \mod 3$	$\mathrm{L}_3(p)^3$	$\mathrm{L}_3(p^3)$
$p \not\equiv 1 \mod 3$	$\mathrm{U}_3(p)^3$	$\mathrm{U}_3(p^3)$

For the proof we need the following technical lemma.

Lemma 6.10. *Let $\mathcal{O}$ be a Noetherian integral domain of Krull dimension 1 and $f, g \in \mathcal{O}[X]$ with f monic. For a prime ideal $P \trianglelefteq \mathcal{O}$ denote by f_P and g_P the reduction of f and g to $(\mathcal{O}/P)[X]$. If $f_P | g_P$ in $(\mathcal{O}/P)[X]$ for infinitely many prime ideals $P \trianglelefteq \mathcal{O}$, then $f|g$ in $\mathcal{O}[X]$.*

Proof. Let $\mathcal{P}$ be an infinite set of prime ideals $P \trianglelefteq \mathcal{O}$ such that $f_P | g_P$; define $R := \prod_{P \in \mathcal{P}} \mathcal{O}/P$. By Lemma 5.3, the canonical homomorphism $\alpha \colon \mathcal{O} \to R$ is injective, and $\alpha(f)|\alpha(g)$ in $R[X]$. Now $f|g$ in $\mathcal{O}[X]$ follows by applying division with remainder, where care has to be taken since R is not an integeral domain. The hypotheses of the proposition are still satisfied if g is replaced by the polynomial $g - \mathrm{lc}(g)X^{\deg(g)-\deg(f)}f$, which has a smaller degree. Eventually, we arrive at a polynomial g' of degree less than $\deg(f)$ which is divisible by f. Since f is monic, this is only possible if $g' = 0$. This shows that the cofactor of $\alpha(f)$ in $\alpha(g)$ has a preimage in $\mathcal{O}[X]$, so $f|g$. □

Proof of Proposition 6.9. The L_3-U_3-quotient algorithm for the group $\langle a, b \mid a^2, b^4, (ab)^7 \rangle$ returns the two prime ideals

$$P_1 := \langle x_1 + 1, x_{-1} + 1, x_2 - 1, x_{-2} - 1, x_{1,2} + x_{-2,-1}\zeta + x_{-2,-1}, x_{-1,2} + x_{-2,-1}\zeta + x_{-2,-1},$$
$$x_{-2,1} - x_{-2,-1}, x_{-2,-1}^3 + 2x_{-2,-1}^2\zeta + 2x_{-2,-1}^2 - x_{-2,-1}\zeta + 1, x_{[1,2]} + x_{-2,-1}^2\zeta + x_{-2,-1}^2 + x_{-2,-1}\zeta\rangle$$

and

$$P_2 := \langle x_1 + 1, x_{-1} + 1, x_2 - 1, x_{-2} - 1, x_{1,2} - x_{-2,-1}\zeta - x_{-2,-1} + \zeta, x_{-1,2} - x_{-2,-1}\zeta - x_{-2,-1} + \zeta,$$
$$x_{-2,1} - x_{-2,-1}, x_{-2,-1}^2 - x_{-2,-1}\zeta - x_{-2,-1} + 2\zeta, x_{[1,2]} - x_{-2,-1}\zeta - 2x_{-2,-1} + \zeta - 2\rangle,$$

which both have Krull dimension 1. We start with the first ideal. Let $t \in \mathbb{F}_q^9$ be a zero of P_1, and let $\Delta \colon F_2 \to \mathrm{SL}(3,q)$ be a representation affording t. Then $t_{[2,1]} = t_{[1,2]} =: \alpha$ is a zero of

X^3-4X^2+3X+1, so the characteristic polynomial of $\Delta([a,b])$ is $\chi = X^3-\alpha X^2+\alpha X-1$. The discriminant of χ is $-\alpha^2+11\alpha-23$, and $\langle -A^2+11A-23, A^3-4A^2+3A+1\rangle = \langle 7, A+1\rangle \trianglelefteq \mathbb{Z}[A]$ shows that χ has no multiple roots if $7 \nmid q$. In particular, it is also the minimal polynomial of $\Delta([a,b])$, so $\Delta([a,b])$ is conjugate to the companion matrix of χ. Thus the order of $\Delta([a,b])$ is the order of $X + \langle\chi\rangle$ in $(\mathbb{F}_q[X]/\langle\chi\rangle)^*$.

Since $\chi | X^{14}-1$, the order of $\Delta([a,b])$ divides 14. Obviously, the order cannot be 1 or 2; the remainder of X^7-1 by χ is -2, so $\Delta([a,b])$ has order 7 if $2|q$ and order 14 otherwise.

Note that $t_{1,2}$ is a root of $X^6+2X^5+5X^4+3X^2+X+1$ which has discriminant $-3^3\cdot 7^4\cdot 13^2$. If q is not a power of 3, 7, or 13, the trace tuple t has the form

$$t = (-1,-1,1,1,\zeta\beta,\zeta\beta,\zeta^2\beta,\zeta^2\beta,\beta^2-\beta),$$

where β is one of the three roots of $g = X^3-4X^2+3X+1$. The polynomial g has discriminant 7^2 and Galois group C_3, so modulo $p \neq 7$ it is either irreducible or splits completely. Moreover, it is irreducible mod p if and only if $p \neq \pm 1 \mod 7$. To see this, note that $\mathbb{Q}(\beta) = \mathbb{Q}(\zeta_7+\zeta_7^{-1})$, where ζ_7 is a primitive seventh root of unity, so the claim follows by the decomposition of primes in cyclotomic fields, cf. e.g. [Neu99, Theorem I.10.3].

As in the proof of Proposition 6.5 one checks that for $p \neq 2,3,7,13$ the quotients occur as listed in the table. Running Algorithm 4.46 for $P_1+\langle p\rangle$, where $p \in \{2,7,13\}$, shows that the prime $p=13$ fits into this scheme, and that $p=7$ yields $\mathrm{L}_3(7)$ and $p=2$ yields $\mathrm{U}_3(2^3)$. For $p=3$, the trace tuple is orthogonal. This completes the analysis of the ideal P_1.

Now let $t \in \mathbb{F}_q^9$ be a zero of P_2, and let $\Delta\colon F_2 \to \mathrm{SL}(3,q)$ be a representation affording t. We first determine the quotients of L_3-type of $\langle a,b \,|\, a^2, b^4, (ab)^7\rangle$ in any characteristic. Algorithm 4.45 shows that for $p=3$ the quotient is isomorphic to $\mathrm{L}_2(7)$, and for $p=5$ the quotient is isomorphic to A_7. Furthermore, for $p=7$ the trace tuple t is also a zero of P_1, so it is already taken care of. In fact, $p=7$ is the only characteristic where P_1 and P_2 have common zeroes, since

$$\begin{aligned} P_1+P_2 = \langle 7, x_1+1, x_{-1}+1, x_2+6, x_{-2}+6, x_{1,2}+4\zeta, x_{-1,2}+4\zeta,\\ x_{-2,1}+3\zeta+3, x_{-2,-1}+3\zeta+3, x_{[1,2]}+1\rangle. \end{aligned}$$

Now let $p \neq 3,5,7$; let $\beta := t_{1,2}$. Then β is a zero of $X^4-X^3-X^2-2X+4$, which has discriminant $2^2\cdot 3^2\cdot 7^2$. For any prime $p \neq 2,3,5,7$, the trace tuple is of the form

$$t = (-1,-1,1,1,\beta,\beta,-\zeta-\beta\zeta^2,-\zeta-\beta\zeta^2,(\beta-1)(\zeta+2)),$$

and it is easy to show that the quotients occur as listed in the first table. Algorithm 4.46 shows that the quotient in characteristic 2 is $\mathrm{L}_3(2^2)$, and the image of $[a,b]$ in $\mathrm{L}_3(2^2)$ is 7.

We now check what happens if the order of the commutator is specified. The characteristic polynomial of $\Delta([a,b])$ is $\chi = X^3-\alpha X^2+\alpha X-1$, where α is a root of X^2-5X+1. As above, one checks that χ has no multiple roots if q is not a power of 5 or 7, so in this case χ is also the minimal polynomial.

Furthermore, there is no exponent e such that $\Delta([a,b])^e = \zeta^i I_3$ for some $i \in \{1,2\}$, since the characteristic polynomial of $\Delta([a,b])^e$ is $X^3-\beta X^2+\beta X-1$, where β is a polynomial in α, and the characteristic polynomial of $\zeta^i I_3$ is $X^3-3\zeta^i X^2+3\zeta^{2i}X-1$. Hence the order of $\Delta([a,b]) \in \mathrm{SL}(3,q)$ and of $\overline{\Delta}([a,b]) \in \mathrm{PSL}(3,q)$ coincide.

For any value of $k \in \mathbb{N}$, there are only finitely many characteristics such that $\chi | X^k-1$ by Lemma 6.10. Since $\chi = (X-1)(X^2-(\alpha-1)X+1)$, and χ is square-free, this is equivalent to $(X^2-(\alpha-1)X+1)|(X^k-1)$, which proves the proposition (the primes $2,3,7$ have to be treated separately, since they are ramified in $\mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]/P_2$). □

The set $\mathcal{P}$ in the last proposition can easily be computed. Here is an example.

Example 6.11. Let $k=36$. Let p be a prime and $\alpha\in\mathbb{F}_{p^2}$ a root of X^2-5X+1. Then

$$\begin{aligned}X^{36}-1\equiv{}&(2782610343194293206\alpha-580764594358284687)X\\&-7936555419886547\,16\alpha+165645556529530167\quad\bmod\widetilde{\chi},\end{aligned}$$

so $\widetilde{\chi}|X^{36}-1$ if and only if

$$c_1:=2782610343194293206\alpha-580764594358284687=0$$

and

$$c_0:=-793655541988654716\alpha+165645556529530167=0.$$

The list of primes for which this is satisfied can now be computed by elementary methods, for example by computing the minimal associated primes of the ideal $\langle c_1,c_0,\alpha^2-5\alpha+1\rangle\trianglelefteq\mathbb{Z}[\alpha]$, where α is regarded as an indeterminate. In this case, the minimal associated primes are

$$\langle 3,\alpha+2\rangle,\ \langle 5,\alpha+3\rangle,\ \langle 37,\alpha+4\rangle,\ \langle 109,\alpha+66\rangle,\ \langle 127,\alpha+113\rangle,$$

so $\mathcal{P}=\{37,109,127\}$, and the complete list of L_3-type quotients of $(2,4,7;36)$ is given by $\mathrm{L}_3(37)$, $\mathrm{L}_3(109)$, and $\mathrm{L}_3(127)$.

6.3 Groups with infinitely many quotients of L_3-type in a single characteristic

In the previous section, groups with infinitely many quotients of L_3-type are studied, where in every characteristic there are only finitely many quotients. These quotients arise from prime ideals of Krull dimension 1 in $\mathbb{Z}[\zeta][x_1,\dots,x_{[1,2]}]$ such that the residue class ring has characteristic zero. In this section, an example of a prime ideal of Krull dimension 1 is studied, where the residue class ring has positive characteristic.
Let

$$G:=\langle a,b\,|\,a^2,b^3,[a,b]^5,[a,babab]^3\rangle.$$

Running the algorithm on the group G yields the ideal

$$P:=\langle 2,x_1+1,x_{-1}+1,x_2,x_{-2},x_{[1,2]}+\zeta+1,x_{1,2}+x_{-1,2},x_{-2,1}+x_{-2,-1},x_{-1,2}x_{-2,-1}+x_{[1,2]}+1\rangle,$$

which has Krull dimension 1. So G has infinitely many L_3 and U_3 quotients, but all of them are defined in characteristic 2. We will analyze this example from two different perspectives.

6.3.1 Counting quotients

There are infinitely many L_3 and U_3 quotients of G, but only finitely many of any given order. For any given $n\in\mathbb{N}$, the number of quotients of G which are isomorphic to one of the groups $\mathrm{PSL}(3,2^n)$, $\mathrm{PGL}(3,2^n)$, $\mathrm{PSU}(3,2^n)$, and $\mathrm{PGU}(3,2^n)$ can be given explicitly.
We first fix some notation.

Definition 6.12. Let G be a finitely presented group on two generators, p a prime and $n \in \mathbb{N}$. Denote by $\mathrm{psl}_G(3, p^n)$ the number of normal subgroups $N \trianglelefteq G$ with $G/N \cong \mathrm{PSL}(3, p^n)$, and define $\mathrm{psu}_G(3, p^n)$ similarly. Furthermore, if $p^n \equiv 1 \mod 3$, define $\mathrm{pgl}_G(3, p^n)$ to be the number of normal subgroups $N \trianglelefteq G$ with $G/N \cong \mathrm{PGL}(3, p^n)$, and if $p^n \equiv -1 \mod 3$ define $\mathrm{pgu}_G(3, p^n)$ similarly.

We restrict to the case $p^n \equiv 1$ for $\mathrm{pgl}_G(3, p^n)$, since $\mathrm{PGL}(3, p^n) \cong \mathrm{PSL}(3, p^n)$ if $p^n \not\equiv 1 \mod 3$, and similarly, $\mathrm{PGU}(3, p^n) \cong \mathrm{PSU}(3, p^n)$ if $p^n \not\equiv -1 \mod 3$.
To simplify notation later on, define $\mathrm{psl}_G(3, p^x) = \mathrm{psu}_G(3, p^x) = \mathrm{pgl}_G(3, p^x) = \mathrm{pgu}_G(3, p^x) = 0$ if $x \in \mathbb{Q}$ is not a positive integer. Furthermore, define $\mathrm{pgl}(3, p^n) = 0$ if $p^n \not\equiv 1 \mod 3$ and $\mathrm{pgu}(3, p^n) = 0$ if $p^n \not\equiv -1 \mod 3$.
The aim is to derive formulæ for $\mathrm{psl}_G(3, p^n)$, etc. We will make extensive use of the Möbius μ-Function and of

$$\chi \colon \mathbb{Q} \to \{0, 1\} \colon x \mapsto \begin{cases} 1, & \text{if } x \in \mathbb{Z}, \\ 0, & \text{otherwise,} \end{cases}$$

the characteristic function of $\mathbb{Z}$ in $\mathbb{Q}$. Here is the main result.

Proposition 6.13. *Let $G = \langle a, b \mid a^2, b^3, [a, b]^5, [a, babab]^3 \rangle$ and $n \in \mathbb{N}$.*

1. $\mathrm{pgu}_G(3, 2^n) = 0$.

2. *If n is odd,* $\mathrm{pgl}_G(3, 2^n) = 0$. *If n is even. Then*

$$\mathrm{pgl}_G(3, 2^n) = \frac{2}{3n} \sum_{r \mid n} \mu\left(\frac{n}{r}\right) (1 - \chi\left(\frac{n}{3r}\right)) \chi\left(\frac{r}{2}\right) (2^r - 1).$$

3. *If n is odd,* $\mathrm{psu}_G(3, 2^n) = 0$. *If n is even, then*

$$\mathrm{psu}_G(3, 2^n) = \frac{1}{n} \sum_{r \mid n} \mu\left(\frac{n}{r}\right) \left(1 - \chi\left(\frac{n}{2r}\right)\right) 2^r.$$

4. *If n is odd or $n = 2$,* $\mathrm{psl}_G(3, 2^n) = 0$. *If $n = 2m$ is even, two cases occur. If m is even, then*

$$\mathrm{psl}_G(3, 2^n) = \frac{1}{3n} \sum_{r \mid n} \mu\left(\frac{n}{r}\right) 2^r - \frac{1}{2} \mathrm{psu}_G(3, 2^m) - \frac{1}{3} \mathrm{pgl}_G(3, 2^{n/3}),$$

and if m is odd,

$$\mathrm{psl}_G(3, 2^n) = \frac{1}{3n} \sum_{r \mid n} \mu\left(\frac{n}{r}\right) 2^r + \frac{1}{3n} \sum_{r \mid m} \mu\left(\frac{m}{r}\right) 2^r - \frac{1}{3} \mathrm{pgl}_G(3, 2^{n/3}).$$

Furthermore, $\mathrm{psl}_G(3, p^n) = \mathrm{psu}_G(3, p^n) = \mathrm{pgl}_G(3, p^n) = \mathrm{pgu}_G(3, p^n) = 0$ *for all odd primes p.*

A special case of these formulæ merits particular attention. The complexity of the formulæ stems one the one hand from the fact that certain case distinctions have to be made based on the divisors of n, and on the other hand from the subfield structure of $\mathbb{F}_{2^n}$. All of these complications vanish if $m > 3$ is prime; in this case the formulæ have nice forms.

	$\mathrm{psl}_G(3,2^{2m})$	$\mathrm{psu}_G(3,2^{2m})$	$\mathrm{pgl}_G(3,2^{2m})$
$m=1$	0	2	1
2	0	4	2
3	3	10	7
4	8	32	20

Table 6.2: Number of quotients of L_3-type of G isomorphic to $\mathrm{L}_3(2^{2m})$, $\mathrm{U}_3(2^{2m})$ and $\mathrm{PGL}(3,2^{2m})$ for small values of m

Corollary 6.14. *Let $m>3$ be prime. Then*

$$\mathrm{psl}_G(3,2^{2m}) = \frac{2^{2m}-2^2}{6m},\ \mathrm{psu}_G(3,2^{2m}) = \frac{2^{2m}-2^2}{2m},\ \textit{and}\ \mathrm{pgl}_G(3,2^{2m}) = \frac{2^{2m}-2^2}{3m}.$$

Example 6.15. The first few values of the formulæ are given in Table 6.2.

The remainder of this section is concerned with the proof of Proposition 6.13, which is done in several steps.
Assume $q=2^n$, and let $t\in\mathbb{F}_q^9$ be a zero of P. By abuse of notation, we denote a fixed primitive third root of unity of $\overline{\mathbb{F}_q}$ again by ζ. This introduces a little subtlety, since there are two epimorphisms of $\mathbb{Z}[\zeta]$ onto $\mathbb{F}_2[\zeta]$, so t has one of the following forms: either

$$t=(1,1,0,0,\alpha,\alpha,\zeta/\alpha,\zeta/\alpha,\zeta^2),$$

or

$$t=(1,1,0,0,\alpha,\alpha,\zeta^2/\alpha,\zeta^2/\alpha,\zeta)$$

for some $0\neq\alpha\in\mathbb{F}_q$. We will always argue with the first form, the arguments for the second form are analogous.
The following well-known lemma is often used implicitly.

Lemma 6.16. *Let p be a prime and $k,m\in\mathbb{N}$. There exist $\sum_{r|m}\mu\left(\frac{m}{r}\right)p^{kr}$ tuples $\alpha\in\mathbb{F}_{p^m}^k$ such that $\mathbb{F}_{p^m}=\mathbb{F}_p[\alpha_1,\ldots,\alpha_k]$.*

Proof. This is a standard inclusion-exclusion argument. □

Lemma 6.17. *Let $t\in\mathbb{F}_{2^n}^9$ be a zero of P such that $\mathbb{F}_2[t]=\mathbb{F}_{2^n}$. Then n is even. Furthermore, t is absolutely irreducible if and only if $n\geq 4$.*

Proof. Let $t=(1,1,0,0,\alpha,\alpha,\zeta/\alpha,\zeta/\alpha,\zeta^2)$. Clearly n must be even, since $\zeta\in\mathbb{F}_2[t]$. Furthermore, Algorithm 4.42 shows that t is absolutely irreducible if and only if $\alpha\notin\{1,\zeta,\zeta^2\}$. The same argument applies for the other form for t. □

Lemma 6.18. *Let $t\in\mathbb{F}_{2^{2m}}^9$ be a zero of P such that t is unitary. Then m is even.*

Proof. Let $t=(1,1,0,0,\alpha,\alpha,\zeta/\alpha,\zeta/\alpha,\zeta^2)$, and let γ_2 be a generator of $\mathrm{Gal}(\mathbb{F}_{2^{2m}}/\mathbb{F}_{2^m})$. Then t is unitary if and only if $\gamma_2(\alpha)=\zeta/\alpha$. But then

$$\alpha=\gamma_2^2(\alpha)=(\gamma_2(\zeta)/\zeta)\alpha,$$

hence ζ lies in the fixed field of γ_2, which is $\mathbb{F}_{2^m}$. Thus m must be even. □

Proof of Proposition 6.13, 1. Suppose that there is a tuple $t \in \mathbb{F}_2^{6n}$ leading to a quotient isomorphic to $\mathrm{PGU}(3, 2^n)$. Then t is in particular unitary. By Lemma 6.18, all unitary zeroes of P generate a field whose degree is divisible by four. But then $2|n$, so $2^n \equiv 1 \mod 3$. In this case, $\mathrm{PGU}(3, p^n) \cong \mathrm{PSU}(3, p^n)$, so we set $\mathrm{pgu}_G(3, p^n) = 0$. □

Lemma 6.19. *Let $t \in \mathbb{F}_{2^n}$ be a zero of P. Then t is never imprimitive, and it does not lead to an exceptional group.*

Proof. Apply Algorithms 4.43 and 4.45 to P. □

Lemma 6.20. *Let $\beta \in \mathbb{F}_{2^m}$ such that $X^3 - \beta \in \mathbb{F}_{2^m}[X]$ is irreducible. Then $\mathbb{F}_2[\zeta, \beta] = \mathbb{F}_2[\beta]$.*

Proof. Suppose $\zeta \notin \mathbb{F}_2[\beta] =: \mathbb{F}_{2^\ell}$. Then $3 \nmid (2^\ell - 1)$; in particular, $x \mapsto x^3$ is a bijection on $\mathbb{F}_{2^\ell}^*$, so β is a cube. This is a contradiction to the fact that $X^3 - \beta$ is irreducible. □

We will need the next lemma later on for arbitrary primes, so we formulate and prove it in this generality.

Lemma 6.21. *Let p be a prime and $n \in \mathbb{N}$ such that $p^n \equiv 1 \mod 3$. There exist*

$$\frac{2}{3} \sum_{r|n} \mu\left(\frac{n}{r}\right)(1 - \chi\left(\frac{n}{3r}\right))\chi\left(\frac{p^r - 1}{3}\right)(p^r - 1)$$

elements $\beta \in \mathbb{F}_{p^n}^*$ such that $\mathbb{F}_p[\beta] = \mathbb{F}_{p^n}$ and $X^3 - \beta \in \mathbb{F}_{p^n}[X]$ is irreducible.

Proof. There are $2/3(p^n - 1)$ elements in $\mathbb{F}_{p^n}^*$ which are non-cubes. However, not all of these elements generate the field, some lie in proper subfields. So assume that β lies in a subfield $\mathbb{F}_{p^r}$ for some $r|n$. If $3 \nmid p^r - 1$, then every element in $\mathbb{F}_{p^r}^*$ is a cube. If $3|p^r - 1$ and the index of $\mathbb{F}_{p^r}$ in $\mathbb{F}_{p^n}$ is divisible by three, then every element of $\mathbb{F}_{p^r}^*$ is a cube in $\mathbb{F}_{p^n}$, by Hilbert's Theorem 90. Finally, if $3|p^r - 1$ and the index of $\mathbb{F}_{p^r}$ in $\mathbb{F}_{p^n}$ is not divisible by three, then $\beta \in \mathbb{F}_{p^r}^*$ is a cube in $\mathbb{F}_{p^r}$ if and only if it is a cube in $\mathbb{F}_{p^n}$. A standard inclusion-exclusion argument yields the result. □

Note that $\chi\left(\frac{p^r-1}{3}\right) = \chi\left(\frac{r}{2}\right)$ if $p \equiv -1 \mod 3$ and $\chi\left(\frac{p^r-1}{3}\right) = 1$ if $p \equiv 1 \mod 3$.

Lemma 6.22. *Let n be even. The number of pgl zeroes $t \in \mathbb{F}_{2^{3n}}$ of P such that $\mathbb{F}_2[t] = \mathbb{F}_{2^{3n}}$ is*

$$4 \sum_{r|n} \mu\left(\frac{n}{r}\right)(1 - \chi\left(\frac{n}{3r}\right))\chi\left(\frac{r}{2}\right)(2^r - 1)$$

Proof. Let $t = (1, 1, 0, 0, \alpha, \alpha, \zeta/\alpha, \zeta/\alpha, \zeta^2)$; then t is pgl if and only if the minimal polynomial of α over $\mathbb{F}_{2^n}$ is $X^3 - \beta$, cf. Proposition 4.31, and every choice for β gives three choices for α. Furthermore, $\mathbb{F}_2[\alpha, \zeta] = \mathbb{F}_{2^{3n}}$ if and only if $\mathbb{F}_2[\beta, \zeta] = \mathbb{F}_{2^n}$. Similar arguments hold for the other form for t. The result now follows by Lemmas 6.21 and 6.20 and a standard inclusion-exclusion argument. □

Proof of Proposition 6.13, 2. Lemma 6.22 lists the number of pgl tuples in $\mathbb{F}_{p^{3n}}$ which generate the field. No subgroups have to be considered. However, we have to consider the action of $\Sigma \rtimes (\mathrm{Gal}(\mathbb{F}_{2^{3n}}) \times T)$ to account for the fact that different choices for the trace tuple can give the same quotient, cf. Proposition 4.35. Note that the stabilizer of P in Σ is $\langle(1, \zeta)\rangle$, so it suffices to consider this subgroup. Since the action of $\langle(1, \zeta)\rangle$ induces a Galois action, it is in fact enough to consider $\mathrm{Gal}(\mathbb{F}_{2^{3n}}) \times T$. This group however acts regularly. Hence, the number of different trace tuples has to be divided by $|\mathrm{Gal}(\mathbb{F}_{2^{3n}}) \times T| = 6n$, which yields the result. □

Lemma 6.23. *Let $n \in \mathbb{N}$ be even. There exist*

$$\sum_{r|n} \mu\left(\frac{n}{r}\right)\left(1 - \chi\left(\frac{n}{2r}\right)\right) 2^{r-1}$$

elements $\beta \in \mathbb{F}_{2^n}$ such that $\mathbb{F}_2[\zeta, \beta] = \mathbb{F}_{2^n}$ and $X^2 + \beta X + \zeta \in \mathbb{F}_{2^n}[X]$ is irreducible.

Proof. Assume $\mathbb{F}_2[\beta, \zeta] = \mathbb{F}_{2^r}$. Then $X^2 + \beta X + \zeta$ is reducible over $\mathbb{F}_{2^r}$ if and only if there exists $\alpha \in \mathbb{F}_{2^r}^*$ with $X^2 + \beta X + \zeta = (X + \alpha)(X + \zeta/\alpha)$. Note that $\alpha = \zeta/\alpha$ if and only if $\alpha = \zeta^2$, in every other case the polynomial has two different roots. Hence there are $(2^r - 1 - 1)/2 + 1 = 2^{r-1}$ reducible polynomials of the form $X^2 + \beta X + \zeta$, and also 2^{r-1} irreducible polynomials. Such a polynomial is irreducible over $\mathbb{F}_{2^n}$ if and only if the index of $\mathbb{F}_{2^r}$ in $\mathbb{F}_{2^n}$ is odd. A standard inclusion-exclusion principle counting the number of irreducible polynomials in $\mathbb{F}_{2^n}$ which are not defined over a smaller field yields the result. □

Lemma 6.24. *Let n be even. The number of unitary zeroes $t \in \mathbb{F}_{2^{2n}}^9$ such that $\mathbb{F}_2[t] = \mathbb{F}_{2^{2n}}$ is*

$$6 \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(1 - \chi\left(\frac{n}{2r}\right)\right) 2^{r}$$

Proof. Let $t = (1, 1, 0, 0, \alpha, \alpha, \zeta/\alpha, \zeta/\alpha, \zeta^2)$ and γ_2 a generator of $\mathrm{Gal}(\mathbb{F}_{2^{2n}}/\mathbb{F}_{2^n})$. Then t is unitary if and only if a Σ-conjugate t' of t satisfies $\gamma_2(t'_{1,2}) = \gamma_2(t'_{-2,-1})$. Since γ_2 fixes ζ, only one element in the Σ-orbit has this property, and we can assume without loss of generality that this element is t, so $\gamma_2(\alpha) = \zeta/\alpha$. The minimal polynomial over $\mathbb{F}_{p^n}$ is $(X - \alpha)(X - \zeta/\alpha) =: X^2 + \beta X + \zeta$, and $\mathbb{F}_2[\alpha, \zeta] = \mathbb{F}_{2^{2n}}$ if and only if $\mathbb{F}_2[\beta, \zeta] = \mathbb{F}_{2^n}$. Lemma 6.23 lists the number of such β, and every choice gives two choices for α. Similar arguments apply for the other choice for t. □

Proof of Proposition 6.13, 3. Lemma 6.24 lists the number of unitary trace tuples. Since n is even, $\mathrm{PGU}(3, 2^n) = \mathrm{PSU}(3, 2^n)$, so no subgroups have to be considered.
However, only one element in every $\Sigma \rtimes (\mathrm{Gal}(\mathbb{F}_{2^{2n}}) \times T)$-orbit has to be counted. Since T induces a Galois action, and the stabilizer of P in Σ is $\langle(1, \zeta)\rangle$, the number of tuples counted above has to be divided by $6n$. □

Lemma 6.25. *Let $n = 2m \geq 4$ be even. The number of zeroes $t \in \mathbb{F}_{2^n}$ of P such that $\mathbb{F}_2[t] = \mathbb{F}_{2^n}$ is*

$$\begin{cases} 2\sum_{r|n} \mu\left(\frac{n}{r}\right) 2^r & \textit{if } m \textit{ is even,} \\ 2\sum_{r|n} \mu\left(\frac{n}{r}\right) 2^r + 2\sum_{r|m} \mu\left(\frac{m}{r}\right) 2^r & \textit{if } m \textit{ is odd.} \end{cases}$$

Proof. Let $t = (1, 1, 0, 0, \alpha, \alpha, \zeta/\alpha, \zeta/\alpha, \zeta^2)$. Then $\mathbb{F}_2[t] = \mathbb{F}_2[\zeta, \alpha]$. If m is even, then $\mathbb{F}_2[\zeta, \alpha] = \mathbb{F}_{2^n}$ if and only if $\mathbb{F}_2[\alpha] = \mathbb{F}_{2^n}$, so the formula counts the number of generators of $\mathbb{F}_{2^n}$. This formula is multiplied by two to account for the other form for t.
If m is odd, then $\mathbb{F}_2[\zeta, \alpha] = \mathbb{F}_{2^n}$ if and only if $\mathbb{F}_2[\alpha] = \mathbb{F}_{2^n}$ of $\mathbb{F}_2[\alpha] = \mathbb{F}_{2^m}$. The same argument applies as above. □

Proof of Proposition 6.13, 4. Lemma 6.17 shows that n must be even and at least four. Now Lemma 6.25 counts the number of trace tuples which generate the field. Some of these tuples can be unitary or pgl, so they have to be subtracted. Furthermore, the group $\Sigma \rtimes (\mathrm{Gal}(\mathbb{F}_{p^n}) \times T)$ acts regularly on the remaining tuples, so the result has to be divided by $6n$. This yields the result. □

6.3.2 Adding relators

From a theoretical point of view, the counting in the last section is done by taking quotients of the ring $\mathbb{Z}[\zeta][x_1, \ldots, x_{[1,2]}]$. Another way to continue the example is by taking quotients of the group G instead, by adding another relator. Adding the relation $(ab)^{13}$ to G yields the quotient $\mathrm{U}_3(2^2)$; in fact, the resulting group is isomorphic to $\mathrm{U}_3(2^2)$, cf. [WWT$^+$]. We will now try to add the relator $(ab)^i$ for some $i \in \mathbb{N}$ to get some of the other groups as quotients. First note that adding a relator $(ab)^i$ will always give only finitely many quotients.

Proposition 6.26. *Let $i \in \mathbb{N}$. The group $\langle a, b \mid a^2, b^3, [a,b]^5, [a, babab]^3, (ab)^i\rangle$ has only finitely many quotients of L_3-type.*

Proof. Let $t = (1, 1, 0, 0, \alpha, \alpha, \zeta/\alpha, \zeta/\alpha, \zeta^2) \in \mathbb{F}_{2^{2k}}$ be a trace tuple, and $\Delta\colon F_2 \to \mathrm{SL}(3, 2^{2k})$ a representation realizing it. Then $\Delta(ab)$ has the characteristic polynomial

$$\chi = X^3 - t_{1,2}X^2 + t_{-2,-1}X - 1 = X^3 - \alpha X^2 - \zeta/\alpha X - 1.$$

The resultant of χ and χ' is ζ, so χ has no multiple roots for any value of α; in particular, χ is the minimal polynomial of $\Delta(ab)$. Now if t is a trace tuple for the group $\langle a, b | a^2, b^3, [a, b]^5, [a, babab]^3, (ab)^i\rangle$, then $|\Delta(ab)|\,\big|\,3i$, hence $\chi | X^{3i} - 1$. But there are only finitely many choices for α such that this is true. □

Proposition 6.27. *Let $m \in \mathbb{N}$ with $m \geq 2$, let $\alpha \in \mathbb{F}_{2^{4m}}$ be a primitive element of norm ζ over $\mathbb{F}_{2^{2m}}$, and let i be the order of $X + \langle\chi\rangle \in (\mathbb{F}_{2^{4m}}[X]/\langle\chi\rangle)^*$, where $\chi = X^3 - \alpha X^2 + \zeta/\alpha X - 1$. Then $\mathrm{U}_3(2^{2m})$ is a quotient of $\langle a, b \mid a^2, b^3, [a, b]^5, [a, babab]^3, (ab)^{ki}\rangle$ for any $k \in \mathbb{N}$. Furthermore, if $\langle a, b \mid a^2, b^3, [a, b]^5, [a, babab]^3, (ab)^j\rangle$ has a quotient isomorphic to $\mathrm{U}_3(2^{2m})$, then $j = ki$ for some $k \in \mathbb{N}$ and some i as above.*

Proof. Let $t = (1, 1, 0, 0, \alpha, \alpha, \zeta/\alpha, \zeta/\alpha, \zeta^2) \in \mathbb{F}_{2^{4m}}$ and $\Delta\colon F_2 \to \mathrm{SL}(3, 2^{2k})$ a representation realizing t. Then t is a zero of P, so $\overline{\Delta}$ factors over $\langle a, b \mid a^2, b^3, [a, b]^5, [a, babab]^3\rangle$, where $\overline{\Delta}$ is the corresponding projective representation. The minimal polynomial of α over $\mathbb{F}_{2^{2m}}$ is $X^2 + \beta X + \zeta$, so t is unitary (see proof of Lemma 6.24. Since χ is squarefree, $\Delta(ab)$ is conjugate to the companion matrix of χ. Hence $|\Delta(ab)| = |X + \langle\chi\rangle| = i$. Furthermore, $\mathrm{PSU}(3, 2^{2m}) = \mathrm{SU}(3, 2^{2m})$, so $|\Delta(ab)| = |\overline{\Delta}(ab)|$; hence $\overline{\Delta}$ factors over $\langle a, b \mid a^2, b^3, [a, b]^5, [a, babab]^3, (ab)^{ki}\rangle$. Now assume that $\mathrm{U}_3(2^{2m})$ is a quotient of $\langle a, b \mid a^2, b^3, [a, b]^5, [a, babab]^3, (ab)^j\rangle$ for some $j \in \mathbb{N}$. Any unitary trace tuple corresponding to a quotient of $\langle a, b \mid a^2, b^3, [a, b]^5, [a, babab]^3\rangle$ has the form $t = (1, 1, 0, 0, \alpha, \alpha, \zeta/\alpha, \zeta/\alpha, \zeta^2) \in \mathbb{F}_{2^{4m}}$ for some α of norm ζ, and the order of the image of ab is $|X + \langle\chi\rangle|$. □

Example 6.28. Let $m = 2$. We first compute the possible minimal polynomials $X^2 + \beta X + \zeta$ of α, where β is given implicitly by its minimal polynomial. The possible minimal polynomials for β such that $[\mathbb{F}_2[\zeta, \beta] : \mathbb{F}_2] = 4$ are

$$\mu_1 = X^2 + X + \zeta,\ \mu_2 = X^2 + \zeta X + \zeta,\ \mu_3 = X^2 + \zeta^2 X + 1,$$
$$\mu_4 = X^2 + \zeta^2 X + \zeta^2,\ \mu_5 = X^2 + X + \zeta^2,\ \mu_6 = X^2 + \zeta X + 1,$$

but for μ_5 and μ_6 the polynomial $X^2 + \beta X + \zeta$ is reducible, so they are of no interest. For each of the other choices, the order of $X + \langle\chi\rangle$ can be computed. For μ_2 it is 17, for μ_1 and μ_3 it is 241, and for μ_4 it is 255. This shows that $\mathrm{U}_3(2^4)$ is a quotient of $\langle a, b | a^2, b^3, [a, b]^5, [a, babab]^3, (ab)^i\rangle$

if and only if i is a multiple of 17, 241, or 255. Note also that, by the formulæ in Proposition 6.13, $\langle a, b | a^2, b^3, [a, b]^5, [a, babab]^3 \rangle$ has four quotients isomorphic to $\mathrm{U}_3(2^4)$, so they correspond to the four choices of the μ_j.
The same calculations can be done for the quotients $\mathrm{U}_3(2^{2m})$ for different m. For example, the smallest orders i of ab such that $\mathrm{U}_3(2^{2m})$ appears as a quotient are 65, 257, 205, 4097, 3277 and 65537 for $m = 3, \dots, 8$, respectively.

Similar considerations can be applied to the quotients $\mathrm{PGL}(3, 2^{2k})$ and $\mathrm{PSL}(3, 2^{2k})$. For example, the quotients $\mathrm{PGL}(3, 2^2)$, $\mathrm{PGL}(3, 2^4)$ and $\mathrm{PGL}(3, 2^6)$ occur for $i = 21$, 153 and 189, respectively.

Chapter 7

Counting generators

In this chapter we apply the algorithm to a combinatorial problem, namely to count the number of different ways to generate a group of L_3-type by two elements of prescribed order. The most interesting case is the generation by an element of order 2 and an element of order 3; these are the smallest possible values, since two elements of order 2 generate a dihedral group. The first results on this problem are given by P. Hall in [Hal36], where he counts the number of ways to generate the groups $\mathrm{PSL}(2,p)$ for a prime p by an element of order 2 and an element of order 3. This was subsequently generalized by Plesken and Fabiańska in [PF09] to the groups $\mathrm{PSL}(2,q)$ and $\mathrm{PGL}(2,q)$ for an arbitrary prime power q.
Here, the groups $\mathrm{PSL}(3,q)$, $\mathrm{PSU}(3,q)$, $\mathrm{PGL}(3,q)$, and $\mathrm{PGU}(3,q)$ are considered for an arbitrary prime power q. Note that this amounts to counting the quotients of L_3-type of the group $C_2 * C_3$.
Remember the notation from Section 6.3.1:

Definition 7.1. Let G be a finitely presented group on two generators, p a prime and $n \in \mathbb{N}$. Denote by $\mathrm{psl}_G(3,p^n)$ the number of normal subgroups $N \trianglelefteq G$ with $G/N \cong \mathrm{PSL}(3,p^n)$, and define $\mathrm{psu}_G(3,p^n)$ similarly. Furthermore, if $p^n \equiv 1 \mod 3$, define $\mathrm{pgl}_G(3,p^n)$ to be the number of normal subgroups $N \trianglelefteq G$ with $G/N \cong \mathrm{PGL}(3,p^n)$, and if $p^n \equiv -1 \mod 3$ define $\mathrm{pgu}_G(3,p^n)$ similarly.

Define $\mathrm{psl}_G(3,p^x) = \mathrm{psu}_G(3,p^x) = \mathrm{pgl}_G(3,p^x) = \mathrm{pgu}_G(3,p^x) = 0$ if $x \in \mathbb{Q}$ is not a positive integer. Furthermore, define $\mathrm{pgl}(3,p^n) = 0$ if $p^n \not\equiv 1 \mod 3$ and $\mathrm{pgu}(3,p^n) = 0$ if $p^n \not\equiv -1 \mod 3$.
Furthermore, μ is the Möbius μ-function and

$$\chi\colon \mathbb{Q} \to \{0,1\}\colon x \mapsto \begin{cases} 1, & \text{if } x \in \mathbb{Z}, \\ 0, & \text{otherwise,} \end{cases}$$

the characteristic function of $\mathbb{Z}$ in $\mathbb{Q}$.

7.1 Generator pairs of order 2 and order 4

The results for the case $C_2 * C_4$ are both easier to state and to prove, so we do this first. This will already show the general strategy for the case $C_2 * C_3$, so we can focus on the complications arising in that case in the next section. Here are the main results.

Proposition 7.2. *Let p be a prime and $n \in \mathbb{N}$ an integer. Assume $n \geq 2$. Then*

$$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n) = \frac{1}{2n}\Big(\sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r - \mathrm{red}(p^n)\Big),$$

where

$$\mathrm{red}(p^n) = \begin{cases} 0, & \text{if } p = 2, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(1 - \chi\left(\frac{n}{2r}\right)\right)(p^r - 1), & \text{if } p^n \equiv 1 \mod 4, \\ 3\sum_{r|n} \mu\left(\frac{n}{r}\right)(p^r - 1), & \text{if } p^n \equiv -1 \mod 4. \end{cases}$$

If $n = 1$, then

$$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p) = \begin{cases} 0, & \text{if } p \in \{2, 3\}, \\ 1, & \text{if } p = 5, \\ 13, & \text{if } p = 7, \\ \frac{1}{2}(p^2 - 2p + 1 - (1 - (\frac{-7}{p})) - (1 - (\frac{-3}{p}))(2 + (\frac{5}{p}))), & \text{if } p \equiv 1 \mod 4, \\ \frac{1}{2}(p^2 - 4p + 5 - (1 - (\frac{-7}{p})) - (1 - (\frac{-3}{p}))(2 + (\frac{5}{p}))), & \text{if } p \equiv -1 \mod 4, \end{cases}$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol.

Proposition 7.3. *Let p be a prime and $n \in \mathbb{N}$ an integer. Assume $n \geq 3$. Then*

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n) = \frac{1}{2n}\Big(\mathrm{irr}(p^n) - n\,\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^{n/2}) - \sum_{r|n} \mu\left(\frac{n}{r}\right) p^r\Big),$$

where

$$\mathrm{irr}(p^n) = \begin{cases} \sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - p^r), & \text{if } p = 2, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - 3(p^r - 1)), & \text{if } p \equiv 1 \mod 4, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - (1 - \chi\left(\frac{r}{2}\right))(p^r + 1) - \chi\left(\frac{r}{2}\right) 3(p^r - 1)), & \text{if } p \equiv -1 \mod 4. \end{cases}$$

If $n = 1$, then

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p) = \begin{cases} 1, & \text{if } p = 2, \\ 2, & \text{if } p = 3, \\ 17, & \text{if } p = 7, \\ \frac{1}{2}(p^2 - 4p + 5 - (1 + (\frac{-7}{p})) - (1 + (\frac{-3}{p}))(2 + (\frac{5}{p}))), & \text{if } p \equiv 1 \mod 4, \\ \frac{1}{2}(p^2 - 2p + 1 - (1 + (\frac{-7}{p})) - (1 + (\frac{-3}{p}))(2 + (\frac{5}{p}))), & \text{if } p \equiv -1 \mod 4, \end{cases}$$

and if $n = 2$, then

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^2) = \begin{cases} 1, & \text{if } p = 2, \\ 11, & \text{if } p = 3, \\ 126, & \text{if } p = 5, \\ \frac{1}{4}(p^4 - 6p^2 + 6p - 5 + 2(1 + (\frac{5}{p}))), & \text{otherwise}, \end{cases}$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol.

As in Section 6.3.1, the formulæ greatly simplify if the allowed exponents are not arbitrary.

Corollary 7.4. *Let n be an odd prime. Then*

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n) = \begin{cases} (p^{2n} - p^n - p^2 + p)/2n, & \text{if } p = 2, \\ (p^{2n} - 2p^n - p^2 + 2p)/2n, & \text{if } p \equiv 1 \mod 4, \\ (p^{2n} - 4p^n - p^2 + 4p)/2n, & \text{if } p \equiv -1 \mod 4, \end{cases}$$

and

$$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n) = \begin{cases} (p^{2n} - p^n - p^2 + p)/2n, & \text{if } p = 2, \\ (p^{2n} - 4p^n - p^2 + 4p)/2n, & \text{if } p \equiv 1 \mod 4, \\ (p^{2n} - 2p^n - p^2 + 2p)/2n, & \text{if } p \equiv -1 \mod 4. \end{cases}$$

Example 7.5. The first few values of the formulæ are given in Table 7.1.

$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n)$	$n = 1$	2	3	4
$p = 2$	1	1	9	27
3	2	11	112	766
5	5	126	2520	48378
7	17	536	19488	718836
11	49	3495	294800	26783970

$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n)$	$n = 1$	2	3	4
$p = 2$	0	3	9	30
3	0	16	104	800
5	1	144	2560	48672
7	13	576	19376	720000
11	38	3600	294360	26791200

Table 7.1: Values of $\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n)$ and $\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n)$ for small n and p

The remainder of this section is concerned with the proof of the two propositions.
The L_3-U_3-quotient algorithm for the group $\mathrm{C}_2 * \mathrm{C}_4$ returns the ideal

$$P := \langle x_1+1, x_{-1}+1, x_2-1, x_{-2}-1, x_{1,2}-x_{-1,2}, x_{-2,-1}-x_{-2,1}, x_{[1,2]}-x_{-1,2}x_{-2,1}-x_{-2,1}-x_{-1,2}\rangle$$

which is of Krull dimension 3. Every zero of P has the form

$$t = (-1, -1, 1, 1, \alpha, \alpha, \beta, \beta, \alpha\beta + \alpha + \beta) \in \mathbb{F}_{p^n}^9,$$

where $\alpha, \beta \in \mathbb{F}_{p^n}$ are arbitrary. Furthermore, Algorithm 4.42 shows that t is not absolutely irreducible if and only if it is a zero of

$$\rho := (x_{-2,1} + 2 + x_{-1,2})({x_{-2,1}}^2 - 2\,x_{-2,1} - 2\,x_{-1,2} + 2 + {x_{-1,2}}^2).$$

The strategy for both proofs is the same; count the number of absolutely irreducible trace tuples which are zeroes of P, and remove those which yield epimorphisms onto proper subgroups.

7.1.1 The formula for $\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^n)$

The next two lemmas are used to count unitary trace tuples.

Lemma 7.6. *Let p be prime and $n = 2m \in \mathbb{N}$; denote by Tr the trace function of $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$. For any $\vartheta \in \mathbb{F}_p$ there exist*

$$\sum_{r|m} \mu\left(\frac{m}{r}\right)\left(1 - \chi\left(\frac{m}{2r}\right)\right)(p^r - 1)$$

elements $\alpha \in \mathbb{F}_{p^n}$ such that $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$ and $\mathrm{Tr}(\alpha) = \vartheta$.

Proof. The function $\mathrm{Tr}\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is linear, so ϑ has $p^n/p^m = p^m$ pre-images in $\mathbb{F}^{p^n}$. One of those pre-images already lies in $\mathbb{F}_{p^m}$, so there are $p^m - 1$ elements of trace ϑ in $\mathbb{F}_{p^n}$ which do not lie in a subfield of even index. This leaves the odd-index subfields, for which the same reasoning applies, so a standard inclusion-exclusion argument yields the formula in the statement. □

Lemma 7.7. *Let p be an odd prime and $m \in \mathbb{N}$. If $p^m \equiv -1 \mod 4$, there are*

$$\sum_{r|m} \mu\left(\frac{m}{r}\right)(p^r - 1)$$

elements $\vartheta \in \mathbb{F}_{p^m}$ such that $\mathbb{F}_{p^m} = \mathbb{F}_p[\vartheta]$ and $X^2 - \vartheta X + ((\vartheta - 1)^2 + 1)/2$ is irreducible. If $p^m \equiv 1 \mod 4$, no such elements exist.

Proof. The discriminant of $X^2 - \vartheta X + ((\vartheta - 1)^2 + 1)/2$ is $-(\vartheta - 2)^2$, so the polynomial is irreducible if and only if $\vartheta \neq 2$ and $-1 \notin \mathbb{F}_{p^m}^{*2}$. So if $p^m \equiv -1 \mod 4$, the formula just describes the number of generators $\neq 2$ of $\mathbb{F}_{p^m}$, cf. Lemma 6.16. □

Lemma 7.8. *Let p be a prime and $n \in \mathbb{N}$. If $n > 1$, the number of absolutely irreducible unitary zeroes $t \in \mathbb{F}_{p^{2n}}$ of P such that $\mathbb{F}_p[t] = \mathbb{F}_{p^{2n}}$ is*

$$\sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r - \mathrm{red}(p^n),$$

with $\mathrm{red}(p^n)$ defined as in Proposition 7.2. If $n = 1$, the number is

$$\begin{cases} 2, & \text{if } p = 2, \\ p^2 - 2p + 1, & \text{if } p \equiv 1 \mod 4, \\ p^2 - 4p + 5, & \text{if } p \equiv -1 \mod 4. \end{cases}$$

Proof. Let $t = (-1, -1, 1, 1, \alpha, \alpha, \beta, \beta, \alpha\beta + \alpha + \beta) \in \mathbb{F}_{p^{2n}}^9$ be a zero of P and γ_2 the generator of $\mathrm{Gal}(\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n})$. Then t is unitary if and only if $\beta = \gamma_2(\alpha)$. Thus, there is a bijection between generators of $\mathbb{F}_{p^{2n}}$ and unitary trace tuples which are zeroes of P.
Let $\rho_1 := (x_{-2,1} + 2 + x_{-1,2})$ and $\rho_2 := ({x_{-2,1}}^2 - 2\,x_{-2,1} - 2\,x_{-1,2} + 2 + {x_{-1,2}}^2)$. Then t is absolutely irreducible if and only if it is not a zero of $\rho = \rho_1\rho_2$. Assume first $p = 2$. Then $\rho_2 = \rho_1^2$, and t is a zero of ρ if and only if $\alpha + \beta = 0$, i.e., $\alpha = \beta$. But this implies $\alpha = \gamma_2(\alpha)$, which is not possible since α is a primitive element. Hence in characteristic 2, all unitary trace tuples are absolutely irreducible.

Now assume that p is odd. If t is a zero of ρ_1, then $\mathrm{Tr}(\alpha) = -2$, where Tr is the trace of $\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n}$. The number of trace tuples satisfying this is given in Lemma 7.6. If t is a zero of ρ_2, then $(\mathrm{Tr}(\alpha) - 1)^2 - 2\,\mathrm{N}(\alpha) + 1 = 0$, where N is the norm on $\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n}$. Since $\gamma_2(\alpha) \neq \alpha$, the minimal polynomial of α over $\mathbb{F}_{p^n}$ is

$$X^2 - \mathrm{Tr}(\alpha)X + \mathrm{N}(\alpha) = X^2 - \mathrm{Tr}(\alpha)X + \frac{(\mathrm{Tr}(\alpha) - 1)^2 + 1}{2}.$$

Note that α generates $\mathbb{F}_{p^{2n}}$ if and only if $\mathrm{Tr}(\alpha)$ generates $\mathbb{F}_{p^n}$; Lemma 7.7 lists the number of possible values of generators $\mathrm{Tr}(\alpha)$ such that the polynomial is irreducible; each of those choices yields two choices for α.
Note that the resultant of ρ_1 and ρ_2 with respect to $x_{-1,2}$ is $2(x_{-2,1}^2 + 2x_{-2,1} + 5)$, which has discriminant -2^6. Thus ρ_1 and ρ_2 have two common zero if $n = 1$ and $\sqrt{-1} \notin \mathbb{F}_p$. □

There is no need to consider imprimitive representations, by the following lemma.

Lemma 7.9. *Let $t \in \mathbb{F}_{p^n}^9$ be an imprimitive zero of P. Then t is orthogonal.*

Proof. Apply Algorithm 4.28 to P. □

The next few lemmas deal with the exceptional groups.

Lemma 7.10. *The number of zeroes $t \in \mathbb{F}_{p^n}$ of P such that the corresponding projective representation maps onto $\mathrm{L}_2(7)$ and $\mathbb{F}_{p^n} = \mathbb{F}_p[t]$ is*

$$\begin{cases} 1, & \text{if } n = 1 \text{ and } p = 7, \\ 2, & \text{if } n = 1 \text{ and } \sqrt{-7} \in \mathbb{F}_p^* \text{ or } n = 2 \text{ and } \sqrt{-7} \notin \mathbb{F}_p^*, \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, such a tuple is unitary if and only if $n = 2$ and $\sqrt{-7} \notin \mathbb{F}_p$, and orthogonal if and only if $p = 7$.

Proof. Algorithm 4.45 returns the ideal

$$\langle x_{-1,2}^2 + x_{-1,2} + 2, x_{-1,2} + x_{-2,1} + 1 \rangle$$

for $\mathrm{L}_2(7)$, and $x_{-1,2}^2 + x_{-1,2} + 2$ has discriminant -7. □

Lemma 7.11. *The number of zeroes $t \in \mathbb{F}_{p^n}$ of P such that the corresponding projective representation maps onto A_6 and $\mathbb{F}_{p^n} = \mathbb{F}_p[t]$ is*

$$\begin{cases} 2, & \text{if } n = 2 \text{ and } p = 5, \\ 4, & \text{if } n = 1 \text{ and } \zeta \in \mathbb{F}_p \text{ and } \sqrt{5} \in \mathbb{F}_p \\ & \text{or } n = 2 \text{ and } \zeta \notin \mathbb{F}_p \text{ or } \sqrt{5} \notin \mathbb{F}_p \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, such a tuple is unitary if and only if $n = 2$, $p \neq 2$ and $\sqrt{5} \in \mathbb{F}_p$.

Proof. Algorithm 4.45 returns the two ideals

$$\langle x_{-1,2}^2 - \zeta x_{-1,2} - \zeta^2, x_{-2,1} - \zeta x_{-1,2}\rangle \text{ and}$$
$$\langle x_{-1,2}^2 - \zeta^2 x_{-1,2} - \zeta, x_{-2,1} - \zeta^2 x_{-1,2}\rangle,$$

for A_6, and the discriminants of the quadratic polynomials are $5\zeta^2$ and $5\zeta^4$, respectively. □

Lemma 7.12. *The number of zeroes $t \in \mathbb{F}_{p^n}$ of P such that the corresponding projective representation maps onto the Hessian group H_{36} of order 36 and $\mathbb{F}_{p^n} = \mathbb{F}_p[t]$ is*

$$\begin{cases} 2, & \text{if } n = 1 \text{ and } p \equiv 1 \mod 3 \\ & \text{or } n = 2 \text{ and } p \equiv -1 \mod 3, \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, such a tuple is unitary if and only if $n = 2$ and $\zeta \notin \mathbb{F}_p$.
The other Hessian groups $\mathrm{PGL}(3,2)$ and $\mathrm{PSU}(3,2)$ do not occur.

Proof. Algorithm 4.45 returns the two ideals

$$\langle x_{-1,2} - \zeta, x_{-2,1} - \zeta^2\rangle \text{ and}$$
$$\langle x_{-1,2} - \zeta^2, x_{-2,1} - \zeta\rangle,$$

for H_{36}; furthermore, Algorithm 4.42 shows that a zero of those ideals is not absolutely irreducible if and only if $p = 3$. □

Lemma 7.13. *The number of zeroes $t \in \mathbb{F}_{p^n}$ of P such that the corresponding projective representation maps onto A_7 or M_{10} and $\mathbb{F}_{p^n} = \mathbb{F}_p[t]$ is*

$$\begin{cases} 4, & \text{if } n = 2 \text{ and } p = 5, \\ 0, & \text{otherwise.} \end{cases}$$

Every such tuple is unitary.

Proof. Algorithm 4.45 returns the ideals

$$\langle x_{-1,2} + \zeta + 3, x_{-2,1} + \zeta^2 + 3\rangle, \quad \langle x_{-1,2} + \zeta^2 + 3, x_{-2,1} + \zeta + 3\rangle,$$
$$\langle x_{-1,2} + 2\zeta + 3, x_{-2,1} + 2\zeta^2 + 3\rangle, \quad \langle x_{-1,2} + 2\zeta^2 + 3, x_{-2,1} + 2\zeta + 3\rangle,$$

for A_7 and

$$\langle x_{-1,2} + \zeta + 2, x_{-2,1} + \zeta^2 + 2\rangle, \quad \langle x_{-1,2} + \zeta^2 + 2, x_{-2,1} + \zeta + 2\rangle,$$
$$\langle x_{-1,2} + 2\zeta + 1, x_{-2,1} + 2\zeta^2 + 1\rangle, \quad \langle x_{-1,2} + 2\zeta^2 + 1, x_{-2,1} + 2\zeta + 1\rangle,$$

for M_{10}. □

We are now able to proof the first proposition.

Proof of Proposition 7.2. Note that the group $\mathrm{PSU}(3,p^n)$ occurs as subgroup of $\mathrm{PSL}(3,p^{2n})$, so we have to count the unitary tuples in $\mathbb{F}_{p^{2n}}$ which are absolutely irreducible and do not lead to epimorphisms onto proper subgroups.

From the list of all trace tuples we remove those which are not absolutely irreducible, orthogonal, imprimitive, or lead to exceptional groups.

The formula for the absolutely irreducible unitary trace tuples is given in Lemma 7.8.

An orthogonal trace tuple is never unitary, and by Lemma 7.9 neither are imprimitive tuples. Lemmas 7.10 – 7.13 list the number of trace tuples yielding exceptional groups, which is easily rewritten to be as in the statement.

Finally, the action of the group $\Sigma \rtimes (\mathrm{Gal}(\mathbb{F}_{p^{2n}}) \times T)$ has to be accounted for. But the stabilizer of t in Σ is trivial, and T acts by a Galois automorphism, so it is enough to consider the action of $\mathrm{Gal}(\mathbb{F}_{p^{2n}})$, which acts regularly. This explains the division by $2n$. □

7.1.2 The formula for $\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3,p^n)$

For the second proposition, two more results are needed.

Lemma 7.14. *Let p be a prime and $n \in \mathbb{N}$. The number of absolutely irreducible zeroes $t \in \mathbb{F}_{p^{2n}}$ of P such that $\mathbb{F}_p[t] = \mathbb{F}_{p^{2n}}$ is $\sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r}-p^r)$ if $p=2$, $\sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r}-3(p^r-1))$ if $p \equiv 1 \mod 4$, and*

$$\sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - (1-\chi\left(\frac{r}{2}\right))(p^r+1) - \chi\left(\frac{r}{2}\right)3(p^r-1))$$

if $p \equiv -1 \mod 4$.

Proof. Let $t = (-1,-1,1,1,\alpha,\alpha,\beta,\beta,\alpha\beta+\alpha+\beta) \in \mathbb{F}_{p^n}^9$ be a zero of P. By Lemma 6.16 the number of tuples $(\alpha,\beta) \in \mathbb{F}_{p^n}$ such that $\mathbb{F}_p[\alpha,\beta] = \mathbb{F}_{p^n}$ is $\sum_{r|n} \mu\left(\frac{n}{r}\right) p^{2r}$. We now count the number of such tuples which are zeroes of ρ. Set $\rho_1 := (x_{-2,1} + 2 + x_{-1,2})$ and $\rho_2 := ({x_{-2,1}}^2 - 2\,x_{-2,1} - 2\,x_{-1,2} + 2 + {x_{-1,2}}^2)$. Clearly there are p^n zeroes of ρ_1, hence $\sum_{r|n} \mu\left(\frac{n}{r}\right) p^r$ zeroes of ρ_1 which generate the field. If $p=2$, then $\rho_2 = \rho_1^2$, which yields the result. So assume in the following that p is odd.

The discriminant of ρ_2 regarded as a polynomial in $x_{-2,1}$ is $-4(x_{-1,2}-1)^2$, so ρ_2 has one zero in $\mathbb{F}_{p^n}$ if $p^n \equiv -1 \mod 4$, and $2(p^n-1)+1$ zeroes in $\mathbb{F}_{p^n}$ if $p^n \equiv 1 \mod 4$. Note that it is possible that ρ_1 and ρ_2 have common zeroes. This is the case if and only if $x_{-2,1}^2 + 2x_{-2,1} + 5 = 0$. This polynomial has discriminant -16, so there are two common zeroes if $p^n \equiv 1 \mod 4$, and none otherwise. In total there are $3(p^n-1)$ zeroes in $\mathbb{F}_{p^n}$ if $p^n \equiv 1 \mod 4$, and p^n+1 zeroes if $p^n \equiv -1 \mod 4$. Note that $p^n \equiv -1 \mod 4$ if and only if $p \equiv -1 \mod 4$ and n is odd. This explains the distinction of those two cases and the occurrence of $\chi\left(\frac{r}{2}\right)$ in the formula. □

Lemma 7.15. *The number of irreducible orthogonal zeroes $t \in \mathbb{F}_{p^n}$ of P such that $\mathbb{F}_{p^n} = \mathbb{F}_p[t]$ is*

$$\begin{cases} 0, & \text{if } p = 2, \\ p-2, & \text{if } n = 1 \text{ and } p \neq 2, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right) p^r, & \text{if } n > 1 \text{ and } p \neq 2. \end{cases}$$

Proof. Let $t = (-1,-1,1,1,\alpha,\alpha,\beta,\beta,\alpha\beta+\alpha+\beta) \in \mathbb{F}_{p^n}^9$ be a zero of P. The trace tuple is orthogonal if and only if $\alpha = \beta$. In this case, t is not absolutely irreducible if and only if $\rho(\alpha,\alpha) = 4(\alpha+1)(\alpha-1)^2 = 0$, which proves the lemma. □

Proof of Proposition 7.3. The proof is analogous to the proof of Proposition 7.2. Count all trace tuples (cf. Lemma 6.16); then remove the ones which are not absolutely irreducible (cf. Lemma 7.14), unitary (if n is even, giving the term $n\,\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_4}(3, n/2)$), orthogonal (cf. Lemma 7.15) or exceptional (cf. Lemmas 7.10 – 7.13). Finally, divide by $2n$ to account for the action of $\mathrm{Gal}(\mathbb{F}_{p^n}) \times T$.

The cases $p = 2, 3, 5, 7$ are treated separately for $n = 1, 2$ to account for the different behavior of the orthogonal groups ($p = 2$), the groups $\mathrm{L}_2(7)$ ($p = 7$), A_6 ($p = 3$ and $p = 5$), and H_{36} ($p = 3$). Note however that for $p = 5$ and $n = 1$ the value of $\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p)$ is expressible by the abstract formula, and similarly for $p = 7$ and $n = 2$ for $\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_4}(3, p^2)$. □

7.2 Generator pairs of order 2 and order 3

Proposition 7.16. *Let p be a prime and $n \in \mathbb{N}$ such that $p^n \equiv -1 \mod 3$. Then*

$$\mathrm{pgu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \frac{1}{3n} \sum_{r|n} \mu\left(\frac{n}{r}\right) (1 - \chi\left(\frac{n}{3r}\right))(p^{2r} - p^r - 2).$$

Proposition 7.17. *Let p be a prime and $n \in \mathbb{N}$ such that $p^n \equiv 1 \mod 3$. Then*

$$\mathrm{pgl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \frac{p^n}{3n} \sum_{r|n} \mu\left(\frac{n}{r}\right) (1 - \chi\left(\frac{n}{3r}\right))\chi\left(\frac{p^r - 1}{3}\right) (p^r - 1) - \frac{1}{2}\mathrm{pgu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^{n/2}).$$

Proposition 7.18. *Let $p > 2$ be a prime and $n \in \mathbb{N}$ an integer. Assume $n \geq 2$. If $p^n \not\equiv -1 \mod 3$, then*

$$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \frac{1}{2n}\Big(\sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r - \sum_{r|n} \mu\left(\frac{n}{r}\right) \left(1 - \chi\left(\frac{n}{2r}\right)\right) 2(p^r - 1)\Big).$$

If $p^n \equiv -1 \mod 3$, then

$$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \frac{1}{6n}\Big(\sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r - \sum_{r|n} \mu\left(\frac{n}{r}\right) 6(p^r - 1)\Big) - \frac{1}{3}\mathrm{pgu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^{n/3}).$$

If $p = 2$ and $n > 1$ then

$$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \frac{1}{6n}\Big(\sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r - \sum_{r|n} \mu\left(\frac{n}{r}\right) (3p^r - 2)\Big) - \frac{1}{3}\mathrm{pgu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^{n/3}),$$

if n is odd, and

$$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \frac{1}{2n}\Big(\sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r - \sum_{r|n} \mu\left(\frac{n}{r}\right) (1 - \chi\left(\frac{n}{2r}\right))p^r\Big),$$

if n is even. If $n = 1$, then

$$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p) = \begin{cases} 0, & \text{if } p = 2, \\ 15, & \text{if } p = 7, \\ \frac{1}{6}(p^2 - 7p + 16 - 3(1 - \left(\frac{-7}{p}\right))), & \text{if } p \equiv -1 \mod 3, \\ \frac{1}{2}(p^2 - 3p + 2 - (1 - \left(\frac{-7}{p}\right))), & \text{otherwise.} \end{cases}$$

Proposition 7.19. *Let p be a prime and $n \in \mathbb{N}$ an integer. Assume $n \geq 3$. If $p = 3$, then*

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \frac{1}{2n}\Big(\sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - 3p^r) - n\,\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^{n/2})\Big);$$

if $p^n \equiv 1 \mod 3$, then

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \frac{1}{6n}\Big(\mathrm{irr}(p^n) - 3n\,\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^{n/2}) \\ - 2n\,\mathrm{pgl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^{n/3}) - n\,\mathrm{pgu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^{n/6})\Big)$$

where

$$\mathrm{irr}(p^n) := \begin{cases} \sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - 7p^r), & \text{if } p \equiv 1 \mod 3, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - 2p^r - \chi\left(\frac{r}{2}\right)2(p^r - 1)) & \\ \quad - \sum_{r|\frac{n}{2}} \mu\left(\frac{n}{2r}\right)2(p^{2r} - 2p^r), & \text{if } p = 2 \text{ and } (n, 4) = 2, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - 2p^r - \chi\left(\frac{r}{2}\right)2(p^r - 2)), & \text{if } p = 2 \text{ and } (n, 4) = 4, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - 5p^r - \chi\left(\frac{r}{2}\right)2(p^r - 2)) & \\ \quad - \sum_{r|\frac{n}{2}} \mu\left(\frac{n}{2r}\right)2(p^{2r} - 2p^r), & \text{if } p \equiv -1 \mod 3 \text{ and } (n, 4) = 2, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - 5p^r - \chi\left(\frac{r}{2}\right)2(p^r - 2)), & \text{if } p \equiv -1 \mod 3 \text{ and } (n, 4) = 4; \end{cases}$$

and if $p^n \equiv -1 \mod 3$, then

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \begin{cases} \frac{1}{2n}\sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - 2p^r), & \text{if } p = 2, \\ \frac{1}{2n}\sum_{r|n} \mu\left(\frac{n}{r}\right)(p^{2r} - 3p^r), & \text{otherwise.} \end{cases}$$

If $n = 1$, then

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p) = \begin{cases} 1, & \text{if } p = 2, \\ 3, & \text{if } p = 7, \\ \frac{1}{6}(p^2 - 7p + 18 - 3(1 + \left(\frac{-7}{p}\right))), & \text{if } p \equiv 1 \mod 3, \\ \frac{1}{2}(p^2 - 3p + 4 - (1 + \left(\frac{-7}{p}\right))), & \text{otherwise,} \end{cases}$$

and if $n = 2$, then

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^2) = \begin{cases} 0, & \text{if } p = 2, \\ 13, & \text{if } p = 3, \\ \frac{1}{12}(p^4 - 11p^2 + 16p - 10), & \text{if } p \equiv -1 \mod 3, \\ \frac{1}{12}(p^4 - 11p^2 + 16p - 6), & \text{otherwise,} \end{cases}$$

Again, the following special cases are noteworthy for their simplicity.

Corollary 7.20. *Let $n > 3$ be prime. Then*

$$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \begin{cases} (p^{2n} - 2p^n - p^2 + 2p)/2n, & \text{if } p = 2, \\ (p^{2n} - 7p^n - p^2 + 7p)/6n, & \text{if } p \equiv 1 \mod 3, \\ (p^{2n} - 3p^n - p^2 + 3p)/2n, & \text{otherwise} \end{cases}$$

and

$$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = \begin{cases} (p^{2n} - 4p^n - p^2 + 4p)/6n, & \textit{if } p = 2, \\ (p^{2n} - 7p^n - p^2 + 7p)/6n, & \textit{if } p \equiv 2 \mod 3, \\ (p^{2n} - 3p^n - p^2 + 3p)/2n, & \textit{otherwise} \end{cases}$$

If $p \equiv 1 \mod 3$*, then*

$$\mathrm{pgl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = (p^{2n} - p^{n+1})/3n,$$

and if $p \equiv -1 \mod 3$*,*

$$\mathrm{pgu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n) = (p^{2n} - p^n - p^2 + p)/3n.$$

Example 7.21. The first few values of the formulæ are given in Table 7.2.

$\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$	$n = 1$	2	3	4
$p = 2$	1	0	8	7
3	2	13	108	762
5	7	35	2540	16006
7	3	164	6398	239132
11	45	1123	294580	8924990

$\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$	$n = 1$	2	3	4
$p = 2$	0	2	2	28
3	0	14	108	790
5	0	138	818	48594
7	15	564	19432	719700
11	10	3570	97888	26789370

Table 7.2: Values of $\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$ and $\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$ for small n and p

The case $G := \mathrm{C}_2 * \mathrm{C}_3$ is more involved than the case $\mathrm{C}_2 * \mathrm{C}_4$. The additional complications are:

1. Since not every finite field contains a third root of unity ζ, it can happen that the trace tuple $t \in \mathbb{F}_{p^n}$ generates $\mathbb{F}_{p^n}/\mathbb{F}_p$, while another element ${}^{\sigma}t$ in the orbit under Σ does not. These orbits have to be excluded.

2. We will get imprimitive groups, PGL, and PGU as images, so three more families of groups have to be considered.

On the other hand, a lot of the arguments are similar in both cases, so the arguments can be kept brief there.
Again, there is only one ideal which is not rejected by the irreducibility test, namely

$$P := \langle x_1 + 1, x_{-1} + 1, x_2, x_{-2}, x_{1,2} - x_{-1,2}, x_{-2,-1} - x_{-2,1}, x_{[1,2]} - x_{-1,2}x_{-2,1} + 1 \rangle,$$

which again is of Krull dimension 3. Every zero of P is of the form

$$t = (-1, -1, 0, 0, \alpha, \alpha, \beta, \beta, \alpha\beta - 1) \in \mathbb{F}_{p^n};$$

the reducible trace tuples are the zeroes of

$$\rho := (x_{-2,1} + 2 + x_{-1,2})(x_{-2,1}^2 - 2x_{-2,1} - x_{-1,2}x_{-2,1} - 2x_{-1,2} + 4 + x_{-1,2}^2).$$

Furthermore, t is imprimitive but not orthogonal if and only if $\alpha\beta = 1$.
Note that P is fixed under the action of $\Sigma' := \langle(1,\zeta)\rangle \leq \Sigma$.

7.2.1 The formula for $\mathrm{pgu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$

A pgu tuple is always absolutely irreducible; we prove this more generally for pgl tuples, which is needed later.

Lemma 7.22. *Let $t \in \mathbb{F}_{p^{3n}}^9$ be a zero of P which is pgl. Then t is absolutely irreducible.*

Proof. Let $t = (-1, -1, 0, 0, \alpha, \alpha, \beta, \beta, \alpha\beta - 1) \in \mathbb{F}_{p^{3n}}$ be a zero of P. By Proposition 4.31, t is pgl if and only if ${}^{(1,\zeta)}t = {}^{\gamma}t$, where $\gamma \in \mathrm{Gal}(\mathbb{F}_{p^{3n}}/\mathbb{F}_{p^n})$ is a Galois automorphism of order 3. This is the case if and only if (α, β) has one of the following three forms:

$$(\alpha, \beta) = (\sqrt[3]{\delta}, 0), \ (\alpha, \beta) = (0, \sqrt[3]{\delta}), \ \text{or } (\alpha, \beta) = (\sqrt[3]{\delta}, \lambda\sqrt[3]{\delta}^2),$$

where $\delta \in \mathbb{F}_{p^n}$ is a generator of $\mathbb{F}_{p^n}$ which is not a cube, and $\lambda \in \mathbb{F}_{p^n}$. One easily checks that the first two forms cannot be zeroes of ρ. For the third form, note that $(1, \sqrt[3]{\delta}, \sqrt[3]{\delta}^2)$ is a basis of $\mathbb{F}_{p^{3n}}/\mathbb{F}_{p^n}$; using this, it is again easily checked that (α, β) cannot be a zero of ρ. □

Lemma 7.23. *Let p be a prime such that $p \equiv -1 \mod 3$ and n an odd integer. The number of absolutely irreducible pgu zeroes $t \in \mathbb{F}_{p^{6n}}^9$ of P such that $\mathbb{F}_{p^{6n}} = \mathbb{F}_p[t]$ is*

$$2\sum_{r|n} \mu\left(\frac{n}{r}\right)(1 - \chi\left(\frac{2n}{3r}\right))(p^{2r} - 1).$$

Proof. Let $t = (-1, -1, 0, 0, \alpha, \alpha, \beta, \beta, \alpha\beta - 1) \in \mathbb{F}_{p^{6n}}$ be a zero of P and $\gamma_2 \in \mathrm{Gal}(\mathbb{F}_{p^{6n}}/\mathbb{F}_{p^n})$ be the Galois automorphism of order 2. For t to be pgu and $\mathbb{F}_{p^{6n}} = \mathbb{F}_p[t]$ it is necessary and sufficient that $\alpha = \sqrt[3]{\delta}$ and $\beta = \gamma_2(\alpha)$ for some $\delta \in \mathbb{F}_{p^{2n}}$ such that $\mathbb{F}_{p^{2n}} = \mathbb{F}_p[\delta]$ and δ is not a third power in $\mathbb{F}_{p^{2n}}$. Here, $\sqrt[3]{\delta}$ is one of the three roots of $X^3 - \delta$. The result follows from Lemma 6.21, using that $\chi\left(\frac{p^r-1}{3}\right) = \chi\left(\frac{r}{2}\right)$. □

Lemma 7.24. *Let p be a prime such that $p \equiv -1 \mod 3$ and n an odd integer. There exist*

$$\frac{2}{3}\sum_{r|n} \mu\left(\frac{n}{r}\right)(1 - \chi\left(\frac{2n}{3r}\right))(p^r + 1)$$

elements $\delta \in \mathbb{F}_{p^{2n}}$ with $\mathbb{F}_p[\delta] = \mathbb{F}_{p^{2n}}$ such that δ has norm 1 over $\mathbb{F}_{p^n}$ and $X^3 - \delta \in \mathbb{F}_{p^{2n}}[X]$ is irreducible.

Proof. Let $\mathrm{N}\colon \mathbb{F}_{p^{2n}}^* \to \mathbb{F}_{p^n}^*$ denote the norm. Since N is surjective, there exist $(p^{2n} - 1)/(p^n - 1) = p^n + 1$ elements of norm 1. However, some of those are cubes. So assume $x^3 \in \ker(N)$. Then $\mathrm{N}(x)^3 = 1$, so $\mathrm{N}(x) = \zeta^i$ for some $0 \leq i \leq 2$. Since $\mathrm{N}(x) \in \mathbb{F}_{p^n}$ and $p^n \not\equiv 1 \mod 3$, we must have $i = 0$, so $x \in \ker(N)$. In other words, $\mathbb{F}_{p^{2n}}^{*3} \cap \ker(N) = \ker(N)^3$, so 1/3 of all elements in $\ker(N)$ are cubes. Let $x \in \ker(N)$ be a non-cube. Then x can lie in a proper subfield. But it cannot lie in a subfield of odd degree or in a subfield whose index is divisible by three (cf. proof of Lemma 6.21). Hence there are

$$\sum_{r|2n} \mu\left(\frac{2n}{r}\right)\chi\left(\frac{r}{2}\right)(1-\chi\left(\frac{2n}{3r}\right))(p^{r/2}+1) = \sum_{r|n} \mu\left(\frac{n}{r}\right)(1-\chi\left(\frac{n}{3r}\right))(p^r+1)$$

generators of $\mathbb{F}_{p^{2n}}$ of norm 1 which are not cubes. □

Lemma 7.25. *Let p be a prime such that $p \equiv -1 \mod 3$ and n an odd integer. The number of zeroes $t \in \mathbb{F}_{p^{6n}}^9$ of P such that $\mathbb{F}_{p^{6n}} = \mathbb{F}_p[t]$ and t is both pgu and imprimitive is*

$$2\sum_{r|n} \mu\left(\frac{n}{r}\right)(1-\chi\left(\frac{2n}{3r}\right))(p^r+1).$$

Proof. Let $t = (-1,-1,0,0,\alpha,\alpha,\beta,\beta,\alpha\beta-1) \in \mathbb{F}_{p^{6n}}$ be a zero of P. As stated above, t is imprimitive if and only if $\alpha\beta = 1$. Since t is unitary, this is equivalent to the fact that α has norm 1. This obviously implies that δ has norm 1, but in fact it is equivalent, so if $\delta\gamma(\delta) = 1$, then $\sqrt[3]{\delta}\gamma_2(\sqrt[3]{\delta}) = 1$. For suppose $\sqrt[3]{\delta}\gamma_2(\sqrt[3]{\delta}) = \zeta$. Then ζ lies in the field $\mathbb{F}_{p^{3n}}$; but $3 \nmid p^{3n}-1$ by our assumption, which is a contradiction. The result follows by Lemma 7.24. □

Proof of Proposition 7.16. Lemma 7.23 lists the number of absolutely irreducible pgu tuples. The only subgroups to consider are the imprimitive ones, which are handled by Lemma 7.25. Finally, the action of $\Sigma' \rtimes (\mathrm{Gal}(\mathbb{F}_{p^{6n}}) \times T)$ has to be accounted for. But since the tuples are unitary and pgl, the action has a kernel of order 6. The factor group however acts regularly, so the number of trace tuples has to be divided by $6n$. □

7.2.2 The formula for $\mathrm{pgl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$

Lemma 7.26. *Let p be a prime and $n \in \mathbb{N}$ such that $p^n \equiv 1 \mod 3$. The number of absolutely irreducible pgl zeroes $t \in \mathbb{F}_{p^{3n}}^9$ of P such that $\mathbb{F}_{p^{3n}} = \mathbb{F}_p[t]$ is*

$$2(p^n+1)\sum_{r|n} \mu\left(\frac{n}{r}\right)(1-\chi\left(\frac{n}{3r}\right))\chi\left(\frac{p^r-1}{3}\right)(p^r-1).$$

Proof. Let $t = (-1,-1,0,0,\alpha,\alpha,\beta,\beta,\alpha\beta-1) \in \mathbb{F}_{p^{3n}}$ be a zero of P. Then t is pgl with $\mathbb{F}_p[t] = \mathbb{F}_{p^{3n}}$ if and only if (α,β) is of one of the forms

$$(\alpha,\beta) = (\sqrt[3]{\delta}, 0),\ (\alpha,\beta) = (0, \sqrt[3]{\delta}),\ \text{or } (\alpha,\beta) = (\sqrt[3]{\delta}, \lambda\sqrt[3]{\delta}^2),$$

where $\lambda \in \mathbb{F}_{p^n}^*$, $X^3 - \delta \in \mathbb{F}_{p^n}[X]$ is irreducible and $\sqrt[3]{\delta}$ is one of the three roots in $\mathbb{F}_{p^{3n}}$. The formula now follows by Lemma 6.21. □

Lemma 7.27. *Let p be a prime and $n \in \mathbb{N}$ such that $p^n \equiv 1 \mod 3$. The number of zeroes $t \in \mathbb{F}_{p^{3n}}^9$ of P such that $\mathbb{F}_{p^{3n}} = \mathbb{F}_p[t]$ and t is both pgl and imprimitive is*

$$2\sum_{r|n} \mu\left(\frac{n}{r}\right)(1-\chi\left(\frac{n}{3r}\right))\chi\left(\frac{p^r-1}{3}\right)(p^r-1).$$

Proof. Let $t = (-1, -1, 0, 0, \alpha, \alpha, \beta, \beta, \alpha\beta - 1) \in \mathbb{F}_{p^{3n}}$ be a zero of P. As stated above, t is imprimitive if and only if $\alpha\beta = 1$. This implies that $(\alpha, \beta) = (\sqrt[3]{\delta}, \lambda\sqrt[3]{\delta}^2)$ in the notation of the proof of Lemma 7.26, and $1 = \alpha\beta = \lambda\delta$. Hence $\lambda = \delta$, i.e., every choice of δ gives three possibilities for tuples which are both pgl and imprimitive. □

Proof of Proposition 7.17. Lemma 7.26 lists the number of absolutely irreducible pgu tuples. The only subgroups to consider are the imprimitive ones, which are handled by Lemma 7.27. The action of $\Sigma' \rtimes (\mathrm{Gal}(\mathbb{F}_{p^{3n}}) \times T)$ has a kernel of order 3, but the factor group acts regularly. so the number of trace tuples has to be divided by $6n$. □

7.2.3 The formula for $\mathrm{psu}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$

Lemma 7.28. *Let $p \neq 3$ be a prime and $m \in \mathbb{N}$. If $p^m \equiv -1 \mod 3$, there are*

$$\sum_{r|m} \mu\left(\frac{m}{r}\right)(p^r - 1)$$

elements $\beta \in \mathbb{F}_{p^m}$ such that $\mathbb{F}_{p^m} = \mathbb{F}_p[\beta]$ and $X^2 - \beta X + ((\beta - 1)^2 + 3)/3$ is irreducible. If $p^m \equiv 1 \mod 3$, no such elements exist.

Proof. We use a different method than in Lemma 7.7 to incorporate the case $p = 2$. Assume $\zeta \in \mathbb{F}_{p^n}$; then the polynomial factors as

$$(X + \frac{1}{3}(\beta - 1)(\zeta - 1) + \zeta^2)(X + \frac{1}{3}(\beta - 1)(\zeta^2 - 1) + \zeta).$$

This shows that the polynomial is irreducible if and only if $\beta \neq 4$ and $\zeta \notin \mathbb{F}_{p^n}$. A standard argument yields the formula. □

Lemma 7.29. *Let p be an odd prime and $n \in \mathbb{N}$. If $n > 1$, the number of absolutely irreducible unitary zeroes $t \in \mathbb{F}_{p^{2n}}$ of P such that $\mathbb{F}_p[t] = \mathbb{F}_{p^{2n}}$ is*

$$\begin{cases} \sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r - \sum_{r|n} \mu\left(\frac{n}{r}\right)(1 - \chi\left(\frac{n}{2r}\right))(p^r - 1), & \text{if } p^n \not\equiv -1 \mod 3, \\ \sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r - \sum_{r|n} \mu\left(\frac{n}{r}\right) 3(p^r - 1), & \text{otherwise.} \end{cases}$$

If $n = 1$, the number is

$$\begin{cases} p^2 - 2p + 1, & \text{if } p \not\equiv -1 \mod 3, \\ p^2 - 4p + 5, & \text{otherwise.} \end{cases}$$

Furthermore, if $p = 2$, the number is

$$\begin{cases} \sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r - \sum_{r|n} \mu\left(\frac{n}{r}\right) 2(p^r - 1), & \text{if } n \text{ is odd,} \\ \sum_{r|2n} \mu\left(\frac{2n}{r}\right) p^r, & \text{if } n \text{ is even.} \end{cases}$$

Proof. This is analogous to the proof of Lemma 7.8, using Lemmas 7.6 and 7.28. □

Lemma 7.30. *Let p be an odd prime and $n \in \mathbb{N}$ such that $p^n \equiv -1 \mod 3$. If $n > 1$, the number of absolutely irreducible unitary zeroes $t \in \mathbb{F}_{p^{2n}}$ of P such that $\mathbb{F}_p[t] = \mathbb{F}_{p^{2n}}$ and $\mathbb{F}_p[{}^\sigma t] = \mathbb{F}_{p^n}$ for some $\sigma \in \Sigma$ is*

$$2\sum_{r|n} \mu\left(\frac{n}{r}\right)(p^r - 1);$$

if $n = 1$, this number is $2p - 6$. If $p = 2$, no such tuples exist.

Proof. Let $t = (-1,-1,0,0,\alpha,\alpha,\beta,\beta,\alpha\beta-1) \in \mathbb{F}_{p^{3n}}$ be a unitary zero of P. Note that $\mathbb{F}_p[{}^{(1,\zeta)}t] = \mathbb{F}_{p^n}$ if and only if $\alpha = \zeta^2\alpha'$ for some non-zero generator α' of $\mathbb{F}_{p^n}$, and similarly for $(1,\zeta^2)$ instead of $(1,\zeta)$. Hence, every non-zero generator α' of $\mathbb{F}_{p^n}$ gives two choices for α. Let γ_2 be the generator of $\mathrm{Gal}(\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n})$; then $(\alpha,\gamma_2(\alpha))$ is a zero of ρ if and only if $\alpha \in \{-\zeta,-\zeta^2,2\zeta,2\zeta^2\}$. These cases can only occur if $n = 1$. □

Lemma 7.31. *Let p be prime and $n \in \mathbb{N}$. There are*

$$\begin{cases} \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(1-\chi\left(\frac{n}{2r}\right)\right)p^r, & \textit{if } p = 2, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(1-\chi\left(\frac{n}{2r}\right)\right)(p^r-1), & \textit{otherwise} \end{cases}$$

elements $\alpha \in \mathbb{F}_{p^{2n}}$ such that $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^{2n}}$ and $\mathrm{N}(\alpha) = 1$, where N is the norm function of $\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n}$.

Proof. There are $(p^{2n}-1)/(p^n-1) = p^n+1$ elements of norm 1 in $\mathbb{F}_{p^{2n}}$, but two of them are ± 1 (one, if $p = 2$), and some lie in odd-index subfields. The formula follows by an inclusion-exclusion argument. □

Lemma 7.32. *Let p be a prime and $n \in \mathbb{N}$. If $n > 1$, the number of absolutely irreducible unitary zeroes $t \in \mathbb{F}_{p^{2n}}^9$ such that t is imprimitive, $\mathbb{F}_p[t] = \mathbb{F}_{p^n}$ and $\mathbb{F}_p[{}^\sigma t]$ is not a proper subfield for any $\sigma \in \Sigma'$*

$$\begin{cases} \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(1-\chi\left(\frac{n}{2r}\right)\right)p^r, & \textit{if } p = 2, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(1-\chi\left(\frac{n}{2r}\right)\right)(p^r-1), & \textit{otherwise} \end{cases}$$

If $n = 1$, the number is

$$\begin{cases} 0, & \textit{if } p = 2, \\ p-5 & \textit{if } p \equiv -1 \mod 3, \\ p-1 & \textit{otherwise.} \end{cases}$$

Proof. Let $t = (-1,-1,0,0,\alpha,\alpha,\beta,\beta,\alpha\beta-1) \in \mathbb{F}_{p^n}$ be a zero of P. Then t is imprimitive if and only if $\alpha\beta = 1$. Since t is also unitary, this is equivalent to the fact that α has norm 1. Lemma 7.31 lists the number of such tuples. If $\{\alpha,\beta\} = \{-\zeta,-\zeta^2\}$, then the tuple is not absolutely irreducible, and if $\{\alpha,\beta\} = \{\zeta,\zeta^2\}$, the tuple can be conjugated into a proper subfield. These cases occur only if $p \equiv -1 \mod 3$ and $n = 1$. □

Lemma 7.33. *The number of zeroes $t \in \mathbb{F}_{p^n}$ of P such that the corresponding projective representation maps onto $\mathrm{L}_2(7)$ and $\mathbb{F}_{p^n} = \mathbb{F}_p[t]$ is*

$$\begin{cases} 3, & \textit{if } n = 1 \textit{ and } p = 7, \\ 2, & \textit{if } n = 2 \textit{ and } p = 3 \textit{ or } n = 1 \textit{ and } \sqrt{-7} \in \mathbb{F}_p^* \textit{ and } p \equiv -1 \mod 3, \\ 6, & \textit{if } n = 2 \textit{ and } \sqrt{-7} \notin \mathbb{F}_p^* \textit{ or } n = 1 \textit{ and } \sqrt{-7} \in \mathbb{F}_p^* \textit{ and } p \equiv 1 \mod 3, \\ 0, & \textit{otherwise.} \end{cases}$$

If $n = 2$, $\sqrt{-7} \notin \mathbb{F}_p^*$ and $p \equiv 1 \mod 3$, two of those tuples satisfy $\gamma(t_{-1,2}) = t_{-2,1}$, where γ_2 is a generator of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$; if $n = 2$, $\sqrt{-7} \notin \mathbb{F}_p^*$ and $p \equiv -1 \mod 3$, all six tuples satisfy $\gamma(t_{-1,2}) = t_{-2,1}$. If $p = 7$, the tuples are orthogonal.
The other exceptional groups do not occur as quotients of $\mathrm{C}_2 * \mathrm{C}_3$.

Proof. This is analogous to the proof of Lemma 7.10. □

Proof of Proposition 7.18. Lemma 7.29 lists the number of absolutely irreducible unitary zeroes. If $p^n \equiv -1 \mod 3$, some of them can be conjugated into a proper subfield (Lemma 7.30). Furthermore, the tuples can be imprimitive (Lemma 7.32) or pgu (the latter case can only occur if $p^n \equiv -1 \mod 3$). If $n = 1$ and $\left(\frac{-7}{p}\right) = -1$, there are also two tuples yielding $\mathrm{L}_2(7)$, cf. Lemma 7.33.
Finally, the acting group has to be taken into account. Since we only count the unitary tuples with $\beta = \gamma_2(\alpha)$, where γ_2 is a generator of $\mathrm{Gal}(\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n})$, the group is $\mathrm{Gal}(\mathbb{F}_{p^{2n}}) \times T$ if $p^n \equiv -1 \mod 3$ and $\Sigma' \rtimes (\mathrm{Gal}(\mathbb{F}_{p^{2n}}) \times T)$ otherwise. Both actions have a kernel of order 2, thus in the first case we have to divide by $2n$, in the second by $6n$. □

7.2.4 The formula for $\mathrm{psl}_{\mathrm{C}_2 * \mathrm{C}_3}(3, p^n)$

Lemma 7.34. *Let p be a prime and $n \in \mathbb{N}$. The number of absolutely irreducible zeroes $t \in \mathbb{F}_{p^{3n}}^9$ of P such that $\mathbb{F}_{p^n} = \mathbb{F}_p[t]$ is*

$$\begin{cases} \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(p^{2r} - (1-\chi\left(\frac{r}{2}\right))p^r - \chi\left(\frac{r}{2}\right)(3p^r - 2)\right), & \text{if } p = 2, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(p^{2r} - p^r\right), & \text{if } p = 3, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(p^{2r} - 3(p^r - 1)\right), & \text{if } p \equiv 1 \mod 3, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)\left(p^{2r} - (1-\chi\left(\frac{r}{2}\right))(p^r + 1) - \chi\left(\frac{r}{2}\right)3(p^r - 1)\right), & \text{if } p \equiv -1 \mod 3. \end{cases}$$

Proof. Let $t = (-1, -1, 0, 0, \alpha, \alpha, \beta, \beta, \alpha\beta - 1) \in \mathbb{F}_{p^n}$ be a zero of P. Set $\rho_1 := x_{-2,1} + 2 + x_{-1,2}$ and $\rho_2 := x_{-2,1}^2 - 2x_{-2,1} - x_{-1,2}x_{-2,1} - 2x_{-1,2} + 4 + x_{-1,2}^2$. Then t is absolutely irreducible if and only if $\rho(\alpha\beta) \neq 0$. For odd p the argument is the same as in Lemma 7.14, using that the discriminant of ρ_2 with respect to $x_{-2,1}$ is $-3(x_{-1,2} - 2)^2$.
For $p = 2$ a new argument is needed. Note that ρ_2 factors over $\mathbb{F}_4 = \mathbb{F}_2[\zeta]$ as $(x_{-1,2} + \zeta x_{-2,1})(x_{-1,2} + \zeta^2 x_{-2,1})$. Thus ρ_2 has $2(p^n - 1) + 1$ zeroes in $\mathbb{F}_{p^n}$ if n is even and one zero if n is odd. Furthermore, ρ_1 and ρ_2 have the zero $\alpha = \beta = 0$ in common. Now the result follows again by a standard argument. □

Lemma 7.35. *Let p be a prime with $p \equiv -1 \mod 3$ and let $n \in \mathbb{N}$ be odd. If $n > 1$, there are*

$$\sum_{r|n} \mu\left(\frac{n}{r}\right) 2(p^{2r} - p^r - 1)$$

absolutely irreducible zeroes $t \in \mathbb{F}_{p^{2n}}^9$ of P with $\mathbb{F}_p[t] = \mathbb{F}_{p^{2n}}$ but $\mathbb{F}_p[{}^\sigma t] = \mathbb{F}_{p^n}$ for some $\sigma \in \Sigma'$. If $n = 1$ and $p \neq 2$ there are $2p^2 - 2p - 4$ such zeroes, and if $n = 1$ and $p = 2$ there are $2p^2 - 2p$ such zeroes.

Proof. Let $t = (-1, -1, 0, 0, \alpha, \alpha, \beta, \beta, \alpha\beta - 1) \in \mathbb{F}_{p^{2n}}$ be a zero of P. Then $\mathbb{F}_p[t] = \mathbb{F}_{p^{2n}}$ but $\mathbb{F}_p[{}^\sigma t] = \mathbb{F}_{p^n}$ if and only if $\alpha = \zeta\alpha'$ and $\beta = \zeta^2\beta'$ or $\alpha = \zeta^2\alpha'$ and $\beta = \zeta\beta'$, where $\mathbb{F}_p[\alpha', \beta'] = \mathbb{F}_{p^n}$. Thus every choice of generators $(\alpha', \beta') \neq (0, 0)$ of $\mathbb{F}_{p^n}$ gives two choices for (α, β), yielding $\sum_{r|n} \mu\left(\frac{n}{r}\right) 2(p^{2r} - 1)$ choices in total. However, some of these choices are not absolutely irreducible.
So assume that $(\alpha, \beta) = (\zeta\alpha', \zeta^2\beta')$ is a zero of ρ. Assume it is a zero of $\rho_1 = x_{-1,2} + x_{-2,1} + 2$. Then $\alpha' = \zeta(2 - \beta') + 2$, which is only possible if $\beta' = \alpha' = 2$; in particular, this only happens

if $n = 1$. Now assume that it is a zero of $\rho_2 := x_{-2,1}^2 - 2x_{-2,1} - x_{-1,2}x_{-2,1} - 2x_{-1,2} + 4 + x_{-1,2}^2$. Then

$$0 = \zeta\beta'^2 - 2\zeta^2\beta' - \alpha'\beta' - 2\zeta\alpha' + 4 + \zeta^2\alpha'^2 = -(\alpha' + \beta' + 2)(\zeta\alpha' + \alpha' - 2 - \zeta\beta').$$

There are $\sum_{r|n} \mu\left(\frac{n}{r}\right) p^r$ possibilities for $\alpha' + \beta' + 2 = 0$. If $\zeta\alpha' + \alpha' - 2 - \zeta\beta' = 0$, then $\beta' = \alpha' + \zeta^2(\alpha' - 2)$, which is only possible if $\alpha' = \beta' = 2$; but this case is already handled above. The case $(p, n) = (2, 1)$ has to be handled separately, to account for the fact that $2 = 0$. □

Lemma 7.36. *Let p be an odd prime and $n \in \mathbb{N}$. The number of absolutely irreducible orthogonal zeroes $t \in \mathbb{F}_{p^n}^9$ such that $\mathbb{F}_p[t] = \mathbb{F}_{p^n}$ and $\mathbb{F}_p[{}^\sigma t]$ is not a proper subfield for any $\sigma \in \Sigma'$ is*

$$\begin{cases} p-1 & \text{if } p = 3 \text{ and } n = 1, \\ p-2 & \text{if } p \equiv -1 \mod 3 \text{ and } n = 1, \\ 3p-8 & \text{if } p \equiv 1 \mod 3 \text{ and } n = 1, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right) p^r & \text{if } p = 3 \text{ and } n > 1 \\ & \text{or } p \equiv -1 \mod 3 \text{ and } n > 1 \text{ odd}, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right)(3p^r - 2) & \text{otherwise.} \end{cases}$$

Proof. Let $t = (-1, -1, 0, 0, \alpha, \alpha, \beta, \beta, \alpha\beta - 1) \in \mathbb{F}_{p^n}$ be a zero of P. Then t is orthogonal if and only if $\alpha = \beta$, $\alpha = \zeta\beta$, or $\alpha = \zeta^2\beta$, so if $\zeta \in \mathbb{F}_{p^n}$ there are $3(p^n - 1) + 1$ such tuples, and if $\zeta \notin \mathbb{F}_{p^n}$ there are only p^n such tuples. However, not all of those tuples are absolutely irreducible. The six exceptions are

$$(\alpha, \beta) \in \{(-1, -1), (2, 2), (2\zeta, 2\zeta^2), (-\zeta, -\zeta^2), (2\zeta^2, 2\zeta), (-\zeta^2, -\zeta)\},$$

which can be easily seen using ρ. Furthermore, if $p \equiv -1 \mod 3$ and $(n, 4) = 2$, some of those tuples have Σ'-conjugates which lie in a proper subfield. These are exactly the tuples $(\alpha, \beta) = (\zeta\alpha', \zeta^2\alpha')$ and $(\alpha, \beta) = (\zeta^2\alpha', \zeta\alpha')$ for some generator α' of $\mathbb{F}_{p^{n/2}}$, so they are already taken care of above. A standard inclusion-exclusion principle now yields the result. □

Lemma 7.37. *Let p be a prime and $n \in \mathbb{N}$. The number of absolutely irreducible imprimitive zeroes $t \in \mathbb{F}_{p^n}^9$ such that $\mathbb{F}_p[t] = \mathbb{F}_{p^n}$ and $\mathbb{F}_p[{}^\sigma t]$ is not a proper subfield for any $\sigma \in \Sigma'$ and t is not orthogonal is*

$$\begin{cases} 0 & \text{if } p = 2 \text{ and } n = 1, \\ p-3 & \text{if } p \not\equiv 1 \mod 3 \text{ and } n = 1, \\ p-7 & \text{if } p \equiv 1 \mod 3 \text{ and } n = 1, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right) p^r & \text{if } p \not\equiv -1 \mod 3 \text{ and } n > 1 \\ & \text{or } p \equiv -1 \mod 3 \text{ and } (n, 4) \neq 2, \\ \sum_{r|n} \mu\left(\frac{n}{r}\right) p^r - 2\sum_{r|\frac{n}{2}} \mu\left(\frac{n}{2r}\right)(p^r - 1) & \text{if } p \equiv -1 \mod 3 \text{ and } (n, 4) = 2. \end{cases}$$

Proof. Let $t = (-1, -1, 0, 0, \alpha, \alpha, \beta, \beta, \alpha\beta - 1) \in \mathbb{F}_{p^n}$ be a zero of P. Using Algorithms 4.43 and 4.44 one sees that t is imprimitive and absolutely irreducible but not orthogonal if and only if $\beta\alpha = 1$ with $\alpha \notin \{\pm 1, \pm\zeta, \pm\zeta^2\}$. The argument is now the same as in the last lemma. □

Proof of Proposition 7.19. Lemma 7.34 lists the number of absolutely irreducible trace tuples which generate the field. However, if $p \equiv -1 \mod 3$ and $(n,4) = 2$, a Σ'-conjugate could generate a proper subfield, cf. Lemma 7.35. Now the subgroups have to be handled. The tuple can be orthogonal (Lemma 7.36) or imprimitive (Lemma 7.37), and if $n \in \{1,2\}$, it can lead to an exceptional group (Lemma 7.33). Furthermore, it can be unitary, pgl or pgu.
Finally, if $\zeta \in \mathbb{F}_{p^n}$, the acting group is $\Sigma' \rtimes (\mathrm{Gal}(\mathbb{F}_{p^n}) \times T)$, otherwise it is $\mathrm{Gal}(\mathbb{F}_{p^n}) \times T$. In the first case, the number of trace tuples has to be divided by $6n$, in the latter case by $2n$. $\square$

Chapter 8

Implementation of the quotient algorithms

The purpose of this short chapter is to highlight parts of the algorithms which can be optimized for run-time efficiency. These results are not needed to understand the algorithms presented in Chapters 2 and 4. However, they are crucial for an efficient implementation on the computer. The optimizations presented here are independent of each other, so they should be combined to get the optimal performance.

In addition to the four methods described here, a further optimization concerns the computation of the minimal associated prime ideals. Since this is also of independent interest, it is presented in a separate chapter.

8.1 Orbits of sign systems

The aim of this section is to reduce the number of sign systems to consider in the L$_2$-quotient and the L$_3$-U$_3$-quotient algorithms.

Let $G = \langle g_1, g_2 \,|\, r_1, \ldots, r_k \rangle$ be a finitely presented group, and assume that $\delta\colon G \to \mathrm{PSL}(2,q)$ is a projective representation. Then there exists a representation $\Delta\colon F_2 \to \mathrm{SL}(2,q)$ inducing δ, i.e., $\Delta(r_i) = s_i I_2$ with $s_i \in \{\pm 1\}$ for all $i \in \{1, \ldots, k\}$. For the L$_2$-algorithm this means in theory that the trace presentation ideals $I_s(G)$ for all $s \in \{\pm 1\}$ have to be considered. However, for every $\sigma \in \Sigma$, the representation ${}^{\sigma}\Delta$ also induces δ, and ${}^{\sigma}\Delta(r_i) = r_i(\sigma_1, \sigma_2) s_i I_2$. So usually ${}^{\sigma}\Delta$ belongs to a different trace presentation ideal than Δ, which means that only one of them has to be considered.

The present section will make these ideas precise. For the L$_2$-algorithm, the results are taken from [PF09, Remark 3.4]. For the L$_3$-algorithm, similar considerations hold. Additionally, there is the action of the group Z, which further reduces the set of sign systems.

8.1.1 Degree 2

Definition 8.1. Let $G = \langle g_1, g_2 \,|\, r_1, \ldots, r_k \rangle$ be a finitely presented group. For $\sigma \in \Sigma$ and $s \in \{\pm 1\}^k$ set

$$ {}^{\sigma}s := (r_1(\sigma_1, \sigma_2)^{-1} s_1, \ldots, r_k(\sigma_1, \sigma_2)^{-1} s_k); $$

this defines an action of Σ on the set of sign systems $\{\pm 1\}^k$.

The action of Σ on the sign systems induces an action on the trace presentation ideals. This is exactly the action of Σ on ideals given in Definition 2.14.

Proposition 8.2. *Let $G = \langle g_1, g_2 \,|\, r_1, \ldots, r_k \rangle$ be a finitely presented group and $s \in \{\pm 1\}^k$. Then*

$$^{\sigma}(I_s(G)) = I_{^{\sigma}s}(G)$$

for all $\sigma \in \Sigma$. In particular, any minimal associated prime of $I_{^{\sigma}s}(G)$ is a Σ-conjugate of a minimal associated prime of $I_s(G)$.

Proof. Let $\sigma \in \Sigma$ and $w \in F_2$. An easy induction on $|w|$ using the construction of the trace polynomials in Theorem 2.1 shows $^{\sigma}p_w = w(\sigma_1, \sigma_2)p_w$. Remember that

$$I_s(G) := \langle p_{r_i h} - s_i p_h \,|\, h \in \{1, a, b, ab\}, i \in \{1, \ldots, k\} \rangle \trianglelefteq \mathbb{Z}[x_1, x_2, x_{12}].$$

Now $^{\sigma}I_s(G)$ is generated by the elements

$$^{\sigma}(p_{r_i h} - s_i p_h) = r_i(\sigma_1, \sigma_2)h(\sigma_1, \sigma_2)p_{r_i h} - s_i h(\sigma_1, \sigma_2)p_h.$$

Multiplying by scalars one gets the elements $p_{r_i h} - s_i r_i(\sigma_1, \sigma_2)^{-1} p_h$, which are the generators of $I_{\sigma s}(G)$. □

This can be used to speed up the L$_2$-quotient algorithm. If two trace presentation ideals $I_s(G)$ and $I_{s'}(G)$ lie in the same Σ-orbit, then every minimal associated prime of $I_s(G)$ is Σ-conjugate to a minimal associated prime of $I_{s'}(G)$ and will be eliminated in step 2 of Algorithm 2.27. Hence step 1 and step 2 of Algorithm 2.27 can be replaced by:

0. Compute the kernel K and a set of orbit representatives S of the action of Σ on the sign systems $\{\pm 1\}^k$.

1. Compute the set $\mathcal{P}'$ of all minimal associated prime ideals of $I_s(G)$, where s ranges over all elements in S. Let $\mathcal{P}$ be the set of all minimal elements of $\mathcal{P}'$ with respect to inclusion.

2. Choose a set of representatives $\mathcal{R}$ of $\mathcal{P}$ under the action of K.

8.1.2 Degree 3

As in the degree 2 case, the action by sign changes can be used to reduce the number of sign systems to consider. Since the automorphism group of $\langle \zeta \rangle$ is non-trivial, there is the additional action of the group Z, which further reduces the number of sign systems.
As everything is completely analogous to degree 2, here are only the results.

Definition 8.3. Let $G = \langle g_1, g_2 \,|\, r_1, \ldots, r_k \rangle$ be a finitely presented group. The group $\Sigma \rtimes Z$ acts on the set $\langle \zeta \rangle^k$ by

$$^{\sigma}s := (r_1(\sigma_1, \sigma_2)^{-1}s_1, \ldots, r_k(\sigma_1, \sigma_2)^{-1}s_k)$$

and

$$^{z}s := (s_1^{-1}, \ldots, s_k^{-1}),$$

where $s \in \langle \zeta \rangle^k$, $\sigma \in \Sigma$, and $Z = \langle z \rangle$.

Proposition 8.4. *Let $G = \langle g_1, g_2 \,|\, r_1, \ldots, r_k\rangle$ be a finitely presented group and $s \in \langle\zeta\rangle^k$. Then*

$${}^{\alpha}(I_s(G)) = I_{{}^{\alpha}s}(G)$$

for all $\alpha \in \Sigma \rtimes Z$. In particular, any minimal associated prime of $I_{{}^{\alpha}s}(G)$ is a $\Sigma \rtimes Z$-conjugate of a minimal associated prime of $I_s(G)$.

Now the first steps of the quotient algorithm can be adapted as in the degree 2 case. However, since $\Sigma \rtimes Z$ is no longer abelian, the stabilizers of the different sign systems may differ, so this has to be taken care of.

0. Compute a set of orbit representatives S of the action of $\Sigma \rtimes Z$ on the sign systems $\langle\zeta\rangle^k$.
1. For every $s \in S$ compute the set of minimal associated prime ideals of $I_s(G)$ and choose a set of orbit representatives under the action of the stabilizer of s in $\Sigma \rtimes Z$. Let $\mathcal{R}'$ be the set of all representatives for all $s \in S$.
2. Let $\mathcal{R}$ be the set of minimal elements of $\mathcal{R}'$.

8.2 Split up words

It is obvious from the proof of Theorem 2.1 that the effort to construct the trace polynomial p_w grows exponentially with $|w|$. Furthermore, the degree of p_w is proportional to the length of w, which has effects on the Gröbner basis algorithms. It is therefore desirable to keep the word lengths small. As already mentioned in [PF09], if a relation r_i can be written as $r_i = v_i w_i$, then $\Delta(r_i(g_1, g_2)) = s_i I_2$ is equivalent to $\Delta(v_i(g_1, g_2)) = s_i \Delta(w_i^{-1}(g_1, g_2))$. So instead of working with the generators $p_{r_i h} - s_i p_h$ of the trace presentation ideal $I_s(G)$, it is more efficient to work with $p_{v_i h} - s_i p_{w_i^{-1} h}$, where the words v_i and w_i are about half as long as r_i.

8.3 Words with powers

As mentioned in the previous section, the time complexity to compute the trace polynomial p_w with the algorithm in Theorem 2.1 is exponential in the length of the word w. However, if w is of the form $w = w_1(w_2)^n w_3$ for sub-words $w_1, w_2, w_3 \in F_2$ and $n > 1$, the following lemma can give a huge performance boost.

Lemma 8.5. *Let $X, Y \in \mathrm{SL}(2, R)$ and $j \geq 1$. Then*

$$\begin{aligned}\mathrm{Tr}(X^{2j-1}Y) = \mathrm{Tr}(XY) \sum_{i=0}^{j-1} (-1)^{i+j-1} \binom{j+i-1}{j-i-1} \mathrm{Tr}(X)^{2i} \\ + \mathrm{Tr}(Y) \sum_{i=0}^{j-2} (-1)^{i+j-1} \binom{j+i-1}{j-i-2} \mathrm{Tr}(X)^{2i+1}\end{aligned}$$

and

$$\mathrm{Tr}(X^{2j}Y) = \mathrm{Tr}(XY) \sum_{i=0}^{j-1} (-1)^{i+j-1} \binom{j+i}{j-i-1} \mathrm{Tr}(X)^{2i+1}$$

$$+\operatorname{Tr}(Y)\sum_{i=0}^{j-1}(-1)^{i+j}\binom{j+i-1}{j-i-1}\operatorname{Tr}(X)^{2i}.$$

Proof. This is an elementary induction on j using the relation (2.1). □

An analogous reduction holds in degree 3.

Lemma 8.6. *Let $X, Y \in \mathrm{SL}(3,R)$ and $n \geq 1$. Then*

$$\operatorname{Tr}(X^nY) = c_n\operatorname{Tr}(XY) + c_{n-1}\operatorname{Tr}(X^{-1}Y) + d_n\operatorname{Tr}(Y),$$

where

$$c_n := \sum_{j=0}^{\lfloor\frac{n-1}{2}\rfloor}\sum_{i=0}^{\lfloor\frac{n-j-1}{2}\rfloor}(-1)^{i+j}\binom{i}{j}\binom{n-i-j-1}{i}\operatorname{Tr}(X^{-1})^{i-j}\operatorname{Tr}(X)^{n-2i-j-1}$$

and

$$d_n := \sum_{j=0}^{\lfloor\frac{n-2}{2}\rfloor}\sum_{i=0}^{\lfloor\frac{n-j-2}{2}\rfloor}(-1)^{i+j+1}\binom{i+1}{j}\binom{n-i-j-2}{i}\operatorname{Tr}(X^{-1})^{i+1-j}\operatorname{Tr}(X)^{n-2i-j-2}.$$

Proof. By the first relation of Lemma 4.1, for all 3×3-matrices of determinant 1 the relation

$$\operatorname{Tr}(X^2Y) = \operatorname{Tr}(X)\operatorname{Tr}(XY) - \operatorname{Tr}(Y)\operatorname{Tr}(X^{-1}) + \operatorname{Tr}(X^{-1}Y)$$

holds. Therefore it suffices to show

$$c_{n+1} = \operatorname{Tr}(X)c_n - \operatorname{Tr}(X^{-1})c_{n-1} + c_{n-2}$$

and

$$d_{n+1} = \operatorname{Tr}(X)d_n - \operatorname{Tr}(X^{-1})d_{n-1} + d_{n-2},$$

which is a technical but elementary induction. □

8.4 Presentations with short and long relations

The optimization in this section is based on two observations. The first is that Gröbner basis algorithms usually cope better with polynomials of small degree. For the second observation assume $G = \langle g_1, g_2 \mid R_1 \cup R_2\rangle$ with sets of relations R_1 and R_2; set $G_i := \langle g_1, g_2 \mid R_i\rangle$ for $i = 1.2$. Then $t \in \mathbb{F}_q^3$ is a zero of $I_s(G)$ for some sign system s of G if and only if t is a zero of $I_{s_1}(G_1) + I_{s_2}(G_2)$, where s_i is a sign system of G_i for $i = 1, 2$ such that the concatenation of s_1 and s_2 is s.

These observations can be applied if the finitely presented group has both short and long relations. Let $G = \langle g_1, g_2 \mid r_1, \ldots, r_\ell, r_{\ell+1}, \ldots, r_k\rangle$, where $r_1, \ldots, r_\ell$ are "short" relations, and $r_{\ell+1}, \ldots, r_k$ are "long" relations. Let $R_1 := \{r_1, \ldots, r_\ell\}$ and $R_2 := \{r_{\ell+1}, \ldots, r_k\}$. First call Algorithm 2.27 with input G_1; let $\mathcal{R}$ be the output.

Now for every sign system s_2 of G_2, instead of using the trace presentation ideal $I_{s_2}(G_2)$ in step 1 of the algorithm, use the ideals $I_{s_2}(G) + P$, where P runs over $\mathcal{R}$. To be more precise, when computing the generators of $I_{s_2}(G_2)$ using Theorem 2.1 and Lemma 8.5, compute the normal form with respect to P after each step. This will keep the degree of the generators low, which has a positive impact on the Gröbner basis algorithms and hence on the computation of the minimal associated primes.

Of course, the distinction between short and long relations depends on the particular example. In the Magma implementation of the L_2-quotient algorithm, by default a relation is considered short if it is of length ≤ 50 and long otherwise, and for the L_3-U_3-quotient algorithm, words of length ≤ 20 are considered short, but these bounds can be set arbitrarily by the user.

Chapter 9

Computation of minimal associated primes

In this chapter, an algorithm to compute the minimal associated primes of an ideal in $\mathbb{Z}[x_1, \ldots, x_n]$ is presented. This is the main tool from commutative algebra for the L_2-quotient and L_3-U_3-quotient algorithms, and therefore a very efficient algorithm is needed. The one described here is a variation of the algorithm by Gianni, Trager and Zacharias, cf. [GTZ88], which is commonly called the GTZ algorithm. The latter is implemented in many computer algebra systems for ideals in $K[x_1, \ldots, x_n]$, where K is a field of characteristic zero, although the original algorithm allows arbitrary ground fields. The main difference between the GTZ algorithm and the algorithm presented here is that a saturation is replaced by a Gröbner basis computation with coefficients in a Euclidean ring, cf. Remark 9.5. Furthermore, the algorithms here only achieve a reduction to the zero-dimensional case. For the primary decomposition of zero-dimensional ideals one of the known algorithms is used, e.g. [GTZ88] for ideals in characteristic zero, and [Ste05] for ideals in positive characteristic.

Note that Sections 9.1 and 9.2 are basically contained in [Fab09], where they are used for the L_2-quotient algorithm. However, the algorithms in Section 9.2 are often too slow for the L_3-U_3-quotient algorithm. The bottleneck is a Gröbner basis computation over the integers. The novel approach presented in this chapter is a replacement of the Gröbner basis calculation over the integers by several Gröbner basis computations over the rationals in Section 9.3, or more generally where the integers are replaced by a Euclidean domain and the rationals by the quotient field.

In Section 9.4 some remarks are made which concern the special application of the quotient algorithms.

9.1 Theoretical background

Let R be a Euclidean domain. For an ideal $I \trianglelefteq R[x_1, \ldots, x_n]$ let $\mathrm{MinAss}(I)$ denote the set of minimal associated prime ideals of I. Furthermore, for any $q \in R$ set

$$\mathrm{MinAss}_q(I) := \{P \in \mathrm{MinAss}(I) \mid P \cap R = \langle q \rangle\}.$$

Note that $\mathrm{MinAss}_q(I) \neq \emptyset$ implies $q = 0$ or q prime. A prime q with $\mathrm{MinAss}_q(I) \neq \emptyset$ is called **necessary**. Since $\mathrm{MinAss}(I)$ is a finite set, there are only finitely many necessary primes, up to multiplication with units in R. The first result gives a computational method to obtain a finite set which contains all necessary primes; such a set is called a **sufficient** set of primes. Similar results already appear in [GTZ88, Proposition 3.7], [Fab09, Lemma 1.3.7] and [PSS11, Lemma 2.2]. In Section 9.3, an alternative method is presented to compute such a finite set, which in some instances is much faster.

Proposition 9.1. *Let $I \trianglelefteq R[x_1, \dots, x_n]$ be an ideal with Gröbner basis G. Let $\mathcal{P}$ be the set of all prime divisors of leading coefficients of elements of G. Then*

$$\operatorname{MinAss}(I) = \operatorname{MinAss}_0(I) \cup \bigcup_{p \in \mathcal{P}} \operatorname{MinAss}_p(I).$$

Proof. Let $\widetilde{\mathcal{P}} := \{p \in R \mid p \text{ prime}, \operatorname{MinAss}_p(I) \neq \emptyset\}$. It suffices to show $\widetilde{\mathcal{P}} \subseteq \mathcal{P}$. Let $I = \bigcap_{i=1}^r Q_i$ be a primary decomposition of I and $P_i := \sqrt{Q_i}$. Assume that the Q_i are numbered such that $P_{m+1}, \dots, P_r$ meet $\widetilde{\mathcal{P}}$ but $P_1, \dots, P_m$ do not. Let $\widetilde{S}$ be the multiplicatively closed set generated by $\widetilde{\mathcal{P}}$ and S the multiplicatively closed set generated by $\mathcal{P}$. By [AM69, Proposition 4.9], $\widetilde{S}$ is minimal with the property

$$\widetilde{S}^{-1} I \cap R[x_1, \dots, x_n] = \bigcap_{i=1}^m Q_i = (K \otimes_R I) \cap R[x_1, \dots, x_n],$$

where K denotes the quotient field of R. But by [AL94, Proposition 4.4.4],

$$S^{-1} I \cap R[x_1, \dots, x_n] = (K \otimes_R I) \cap R[x_1, \dots x_n],$$

hence $\widetilde{S} \subseteq S$ and therefore $\widetilde{\mathcal{P}} \subseteq \mathcal{P}$. □

The computation of $\operatorname{MinAss}_q(I)$ can be reduced to a computation to a computation of minimal associated prime ideals in a polynomial ring over a field. Note that this reduces the dimension of the polynomial ring.

Proposition 9.2. *Let $I \trianglelefteq R[x_1, \dots, x_n]$.*

1. *Let K denote the quotient field of R. Then*

$$\operatorname{MinAss}_0(I) = \{P' \cap R[x_1, \dots, x_n] \mid P' \in \operatorname{MinAss}(K \otimes_R I)\}.$$

2. *Let $p \in R$ be a prime element. Then*

$$\operatorname{MinAss}_p(I) = \{\nu_p^{-1}(\widetilde{P}) \mid \widetilde{P} \in \operatorname{MinAss}(\nu_p(I)) \textit{ with } \widetilde{P} \not\supseteq \nu_p(P') \textit{ for all } P' \in \operatorname{MinAss}_0(I)\},$$

where $\nu_p \colon R[x_1, \dots, x_n] \to R/\langle p \rangle [x_1, \dots, x_n]$ denotes the natural epimorphism.

Proof. The first point is well-known, cf. e.g. [AM69, Proposition 4.9]. The second point is proved in [Fab09, Lemma 1.3.11]; since it is reasonably short, the proof is repeated here. Let $P_1, \dots, P_r$ be the minimal associated primes of I, and $\widetilde{P}_1, \dots, \widetilde{P}_s$ the minimal associated primes of $\nu_p(I)$. Then for any $i \in \{1, \dots, s\}$ we have

$$P_1 \cap \cdots \cap P_r = \sqrt{I} \subseteq \nu_p^{-1}\left(\sqrt{\nu_p(I)}\right) \subseteq \nu_p^{-1}\big(\widetilde{P}_i\big),$$

so $\nu_p^{-1}\big(\widetilde{P}_i\big)$ contains some minimal associated prime of I.
Now let $j \in \{1, \dots, r\}$ such that $p \in P_j$. Then $\widetilde{P}_1 \cap \cdots \cap \widetilde{P}_s \subseteq \nu_p(P_j)$, so $\widetilde{P}_i \subseteq \nu_p(P_j)$ for some i, and hence $\nu_p^{-1}\big(\widetilde{P}_i\big) \subseteq P_j$. But we proved above that $P_k \subseteq \nu_p^{-1}\big(\widetilde{P}_i\big)$ for some k, and hence $P_k = \nu_p^{-1}\big(\widetilde{P}_i\big) = P_j$, by the minimality of P_j. □

9.2 The algorithms

Although the next two algorithms are based on the same theoretical background and therefore could be regarded as one algorithm, they are split here. This is done one the one hand so that it matches the implementation, and on the other hand for the convenience of the reader, since the description as a single algorithm would require a more technical approach.
The first algorithm reduces the computation of minimal associated primes of an ideal in $\mathbb{Z}[x_1, \dots, x_n]$ to the computation of minimal associated primes of ideals defined over fields. Again, this could be easily done in a more general context where $\mathbb{Z}$ is replaced by an arbitrary Euclidean domain, but since $\mathbb{Z}$ is the most important ring for the L_2-quotient and L_3-U_3-quotient algorithms, we restrict to this case.

Algorithm 9.3. *Input:* An ideal $I \trianglelefteq \mathbb{Z}[x_1, \dots, x_n]$.
Output: The set of minimal associated prime ideals of I.
Algorithm:

1. Compute a Gröbner basis G of I, and let $\mathcal{P}$ be the set of all prime divisors of leading coefficients of G.

2. Call Algorithm 9.4 with input $\mathbb{Q} \otimes_{\mathbb{Z}} I$ to get $\mathrm{MinAss}(\mathbb{Q} \otimes_{\mathbb{Z}} I)$. Compute
$$\mathrm{MinAss}_0(I) = \{P' \cap \mathbb{Z}[x_1, \dots, x_n] \mid P' \in \mathrm{MinAss}(\mathbb{Q} \otimes_{\mathbb{Z}} I)\}.$$

3. For every prime $p \in \mathcal{P}$ let $\nu_p \colon \mathbb{Z}[x_1, \dots, x_n] \to \mathbb{F}_p[x_1, \dots, x_n]$ be the natural epimorphism. Call Algorithm 9.4 with input $\nu_p(I)$ to get $\mathrm{MinAss}(\nu_p(I))$. Compute
$$\mathrm{MinAss}_p(I) = \{\nu_p^{-1}(\widetilde{P}) \mid \widetilde{P} \in \mathrm{MinAss}(\nu_p(I)) \text{ with } \widetilde{P} \not\supseteq \nu_p(P') \text{ for all } P' \in \mathrm{MinAss}_0(I)\}.$$

4. Return $\mathrm{MinAss}_0(I) \cup \bigcup_{p \in \mathcal{P}} \mathrm{MinAss}_p(I)$.

The second algorithm reduces the computation of minimal associated primes of ideals of arbitrary dimension to the computation of minimal associated primes of ideals of dimension zero.

Algorithm 9.4. *Input:* An ideal $I \trianglelefteq K[x_1, \dots, x_n]$, where K is a field.
Output: The set of minimal associated prime ideals of I.
Algorithm:

1. If I is zero-dimensional, call one of the well-known algorithms to compute $\mathrm{MinAss}(I)$ and return. Otherwise, let x_i be a variable such that $I \cap K[x_i] = \{0\}$.

2. Compute a Gröbner basis G of I regarded as an ideal in $K[x_i][x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$, i.e., an ideal in a polynomial ring of rank $n-1$ over the coefficient ring $K[x_i]$. Let $\mathcal{P}$ be the set of all prime divisors of leading coefficients of G.

3. Call the algorithm recursively with input $K(x_i) \otimes_{K[x_i]} I$ to get $\mathrm{MinAss}(K(x_i) \otimes_{K[x_i]} I)$. Compute
$$\mathrm{MinAss}_0(I) = \{P' \cap K[x_1, \dots, x_n] \mid P' \in \mathrm{MinAss}(K(x_i) \otimes_{K[x_i]} I)\}.$$

4. (If K is a number field or a finite field) For every prime p let $L := K[x_i]/\langle p\rangle$ and $\nu_p\colon K[x_1,\dots,x_n] \to L[x_1,\dots,x_{i-1},x_{i+1},\dots,x_n]$ the natural epimorphism. Call the algorithm recursively with input $\nu_p(I)$ to get $\mathrm{MinAss}(\nu_p(I))$. Compute

   $$\mathrm{MinAss}_p(I) = \{\nu_p^{-1}(\widetilde{P}) \mid \widetilde{P} \in \mathrm{MinAss}(\nu_p(I)) \text{ with } \widetilde{P} \not\supseteq \nu_p(P') \text{ for all } P' \in \mathrm{MinAss}_0(I)\}.$$

   (If K is not a number field or a finite field) For every prime p call the algorithm recursively with input $I + \langle p\rangle$ to get $\mathrm{MinAss}(I + \langle p\rangle)$. Compute

   $$\mathrm{MinAss}_p(I) = \{P \in \mathrm{MinAss}(I + \langle p\rangle) \mid P \not\supseteq P' \text{ for all } P' \in \mathrm{MinAss}_0(I)\}.$$

5. Return $\mathrm{MinAss}_0(I) \cup \bigcup_{p\in\mathcal{P}} \mathrm{MinAss}_p(I)$.

Remark 9.5. 1. There is a distinction in step 4 of Algorithm 9.4, based on the ground field K. This is done since there is a fast arithmetic in Magma for number fields and for finite fields, but e.g. no arithmetic for fields of the form $K(x,y)[z]/\langle p\rangle$, where $p \in K(x,y)[z]$ is an irreducible polynomial.

2. The algorithms terminate since in every step the dimension of the polynomial ring or of the ideal is reduced. This is the case since

   $$\dim(k[x_1,\dots,x_n]) = \dim(R[x_1,\dots,x_n]) - \dim(R),$$

   where k is either the quotient field of R or a residue class field $R/\langle p\rangle$ for a non-zero prime $p \in R$, and

   $$\dim(I + \langle p\rangle) = \dim(I) - 1$$

   if $p \in K[x_i]$ is a prime where $K[x_i] \cap I = \{0\}$.

3. The correctness of the algorithms follows by Proposition 9.2.

4. The main difference to the algorithm by Gianni, Trager and Zacharias in [GTZ88] is step 2 of Algorithm 9.4. They compute a polynomial $f \in K[x_i]$ such that $((K(x_i) \otimes_{K[x_i]} I) \cap K[x_1,\dots,x_n]) \cap (I + \langle f\rangle) = I$; this is done using a saturation process. Then in step 4 the algorithm is called recursively with input $I + \langle f\rangle$. Furthermore, they do not use field extensions, so they only use the second branch in step 4.

9.3 An alternative method to compute the necessary primes

The method presented in Proposition 9.1 to compute the necessary primes is based on a Gröbner basis computation with coefficients in a Euclidean domain. This computation can be very expensive compared to a Gröbner basis with coefficients in the quotient field. Some recent changes in Magma implemented by Allan Steel address these problems, but for some examples the Gröbner basis computation is still very slow, to the extent that it becomes the bottle neck of the algorithm. This seems to be especially the case if the coefficients of the Gröbner basis are very large.

The methods in this section replace the Gröbner basis computation with coefficients in the Euclidean domain R by several Gröbner basis computations with coefficients in the quotient field, thereby eliminating one possible bottle neck of the algorithm. The results have been published in [Jam11].

The next result is based on the fact that $\mathrm{MinAss}_p(I) \neq 0$ for a prime $p \in R$ if and only if $(I : p) \neq I$.

Proposition 9.6. *Let $I \trianglelefteq R[x_1, \dots, x_n]$ and K the quotient field of R; let G be a reduced Gröbner basis of $K \otimes_R I =: KI$. Let $S \subseteq R$ be the multiplicatively closed subset generated by all prime divisors of denominators which occurred during Buchberger's algorithm applied to any generating set of I, and $T \subseteq S$ the multiplicatively closed subset generated by all prime divisors of denominators of G. Then:*

1. *For any prime $p \in R - S$ we have $(I : p) = I$. In particular, the prime numbers which occur in associated primes of I are contained in S.*

2. *Assume that T is generated by $p_1, \dots, p_\ell$, and that S is generated by $p_1, \dots, p_m$. Then*

$$T^{-1}(I : (p_{\ell+1} \cdots p_m)^\infty) = \langle G \rangle_{T^{-1}R[x_1,\dots,x_n]}.$$

Proof. Let $I = \langle f_1, \dots, f_r \rangle$. Then any $g \in G$ can be written as $g = \sum_{i=1}^r \frac{z_i}{s_i} f_i$ with $z_i \in R[x_1, \dots, x_n]$ and $s_i \in S$, for all i.

1. Let $f \in (I : p) \subseteq KI$. Then $f \in KI \cap R[x_1, \dots, x_n]$, so $f = \sum_{g \in G} \lambda_g g$ with $\lambda_g \in T^{-1}R[x_1, \dots, x_n]$ since all $g \in G$ are monic; thus $sf \in I$ for a suitable $s \in S$. But $pf \in I$, and p and s are coprime, hence $f \in I$.

2. By the first statement, we have $KI \cap R[x_1, \dots, x_n] = S^{-1}I \cap R[x_1, \dots, x_n] = (I : (p_1 \cdots p_m)^\infty)$, so localizing gives

$$T^{-1}(I : (p_{\ell+1} \cdots p_m)^\infty) = T^{-1}(KI \cap R[x_1, \dots, x_n]) = \mathbb{Q}I \cap T^{-1}R[x_1, \dots, x_n].$$

   But G is a Gröbner basis of $KI \cap T^{-1}R[x_1, \dots, x_n] \trianglelefteq T^{-1}R[x_1, \dots, x_n]$, which yields the result. □

A key fact of the last result is that it is independent of the monomial order. In particular, the necessary primes occur as denominators in *every* Gröbner basis computation. This has two important consequences which address the following problems. The denominators during the Gröbner basis computation can become very big, so factorization becomes a problem. And even if they can be factored, the set of all prime divisors might be big, although the set of necessary primes is small.

Corollary 9.7. *Let D_1, D_2 be the set of denominators occurring during two Gröbner basis computations of KI with respect to different monomial orders. Set*

$$D := \{\gcd(d_1, d_2) \mid d_1 \in D_1, d_2 \in D_2\}.$$

Then any necessary prime divides some element of D.

Thus computing Gröbner bases with respect to different monomial orders can give a prefactorization of the denominators and at the same time reduce the number of primes to consider.
The set of primes computed in this way is usually still redundant, i.e., there are primes p which occur as divisors of denominators for every Gröbner basis computation, but they do not occur as elements of associated prime ideals. The next result gives an easy test for almost all primes to check whether they are necessary.

Lemma 9.8. *Let $I \trianglelefteq R[x_1, \dots, x_n]$ and let $p \in R$ be prime. Then $(I : p^\infty) \supsetneqq I$ if and only if $\nu_p((I : p^\infty)) \supsetneqq \nu_p(I)$, where $\nu_p \colon R[x_1, \dots, x_n] \to R/\langle p\rangle[x_1, \dots, x_n]$ denotes the canonical epimorphism.*

Proof. Assume $(I : p^\infty) \supsetneqq I$ and let $\ell \in \mathbb{N}$ be minimal with $(I : p^\ell) = (I : p^\infty)$. Choose $f \in (I : p^\ell) - (I : p^{\ell-1})$ and suppose $\nu_p(f) \in I$. Then $\nu_p(f) = \nu_p(g)$ for some $g \in I$, so $p|(f - g)$; in particular, $\frac{f-g}{p} \in (I : p^\infty)$. But $p^\ell \frac{f-g}{p} = p^{\ell-1} f - p^{\ell-1} g \notin I$, by the choice of f, which is a contradiction. □

Proposition 9.9. *Let G, S and T be as in Proposition 9.6, and let p be a prime not contained in T. Then p is contained in an associated prime of I if and only if $\langle\, \nu_p(G)\, \rangle_{R/\langle p\rangle[x_1,\dots,x_n]} \supsetneqq \nu_p(I)$.*

Proof. We may assume $p \in S$. Then

$$\langle \nu_p(G) \rangle_{R/\langle p\rangle[x_1,\dots,x_n]} = \nu_p(\langle G\rangle_{T^{-1}R[x_1,\dots,x_n]}) = \nu_p((I : p^\infty))$$

by the second statement of Proposition 9.6. The claim now follows by the lemma. □

We can now formulate a new method to compute a sufficient set of primes.

Algorithm 9.10. *Input:* An ideal $I \trianglelefteq \mathbb{Z}[x_1, \dots, x_n]$.
Output: A finite set $\mathcal{P} \subseteq R$ of primes such that any prime $p \in R$ with $\mathrm{MinAss}_p(I) \neq \emptyset$ is associated to an element in $\mathcal{P}$.
Algorithm:

1. Compute a Gröbner basis G of KI, where K is the quotient field of R, and let D be the set of denominators occurring during the Gröbner basis computation. Try to compute the set S of prime divisors.

2. If the factorization of the elements in D is not possible, or if the set S is too big, compute a Gröbner basis with respect to some other monomial order; let D' be the set of denominators occurring during this computation. Replace D by $\{\gcd(d, d') \,|\, d \in D, d' \in D'\}$ and try again to compute S. Repeat this step until S can be computed and is small enough.

3. Return the set of primes $p \in S$ which either divide a denominator of G or which satisfy $\langle \nu_p(G)\rangle \supsetneqq \nu_p(I)$.

This algorithm replaces step 1 of Algorithm 9.3 and step 2 of Algorithm 9.4.

9.4 Minimal associated prime ideals in the quotient algorithms

For the L_2-quotient algorithm, the trace presentation ideals are ideals of $\mathbb{Z}[x_1, x_2, x_{1,2}]$, i.e., the polynomial ring over $\mathbb{Z}$ in three variables. For the L_3-U_3-quotient algorithm, the ring $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$ has to be considered, i.e., the polynomial ring over $\mathbb{Z}[\zeta]$ in nine variables. In practice, for the latter ring we do not work with Gröbner bases with coefficients in $\mathbb{Z}[\zeta]$, but instead we regard ζ as an indeterminate and work with the polynomial ring $\mathbb{Z}[\zeta, x_1, \dots, x_{[1,2]}]$ in ten variables and add the relation $\zeta^2 + \zeta + 1$ to every ideal. This way, no prime factorization over $\mathbb{Z}[\zeta]$ is needed, and we can work with Gröbner basis algorithms over $\mathbb{Z}$.

Both rings have a natural grading. In the ring $\mathbb{Z}[x_1, x_2, x_{1,2}]$, the variables x_1 and x_2 correspond to traces of single matrices, while $x_{1,2}$ corresponds to the trace of a product. Therefore it seems natural to regard x_1 and x_2 as variables of degree 1, and $x_{1,2}$ as a variable of degree 2. Furthermore, for Gröbner basis computations, we use the graded degrevlex order on $\mathbb{Z}[x_1, x_2, x_{1,2}]$. Example computations show that a graded degrevlex order can be much faster than an ungraded degrevlex order, although for the L_2-quotient algorithm both methods are reasonably fast.

For the L_3-U_3-quotient algorithm the commutative algebra is often the bottle neck. Here we regard x_1, x_{-1}, x_2, x_{-2} as variables of degree 1, $x_{1,2}, x_{-1,2}, x_{-2,1}, x_{-2,-1}$ as variables of degree 2, and $x_{[1,2]}$ as a variable of degree 4, and give the ring $\mathbb{Z}[\zeta][x_1, \dots, x_{[1,2]}]$ the graded degrevlex order. In this case, the order has an even bigger impact, and there are several examples which are not computable using an ungraded degrevlex order.

On the other hand, the choice of whether $x_1 < x_2$ or $x_2 < x_1$ does not seem to have an effect on the runtime, and similarly for the other variables. Thus in this application there are some good choices to alter the monomial order in Algorithm 9.10. In the Magma implementation, the algorithm tries up to five different monomial orders until the largest element in D is smaller than 10^{50}, at which a factorization is started, and until the set S has at most 30 elements. This seems to work well in practice.

Index

absolutely irreducible trace tuple, 41
affording a trace tuple, 14, 38

exceptional group, 17, 44

generalized Chebyshev polynomial, 13

Hessian group, 45

L_2-ideal, 19
L_3-ideal, 49
imprimitive group, 26
imprimitive trace tuple, 48

minimal associated prime ideal, 19
minimal set of L_2-ideals, 19
minimal set of L_3-ideals, 49

necessary prime, 97

orthogonal trace tuple, 48

$\mathrm{pgl}_G(3, p^n)$, 67
pgl trace tuple, 48
$\mathrm{pgu}_G(3, p^n)$, 67
pgu trace tuple, 48
$\mathrm{psl}_G(3, p^n)$, 67
$\mathrm{psu}_G(3, p^n)$, 67

sign changes, 16, 42
sign system, 15, 42
sufficient set of primes, 98

trace polynomial, 13, 34
trace presentation ideal, 15, 42
trace tuple, 14, 38
    absolutely irreducible, 15, 41
    imprimitive, 48
    orthogonal, 48
    pgl, 48
    pgu, 48
    unitary, 48

L_3-type, 49

unitary trace tuple, 48

$x_{[1,2]}$, 34

Bibliography

[AL94] William W. Adams and Philippe Loustaunau. An introduction to Gröbner bases, volume 3 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 1994.

[AM69] Michael F. Atiyah and Ian G. Macdonald. Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BCM81] Gilbert Baumslag, Frank B. Cannonito, and Charles F. Miller, III. Some recognizable properties of solvable groups. Math. Z., 178(3):289–295, 1981.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BH95] G. W. Brumfiel and H. M. Hilden. SL(2) representations of finitely presented groups, volume 187 of Contemporary Mathematics. American Mathematical Society, Providence, RI, 1995.

[BHRD12] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal. The maximal subgroups of the low-dimensional finite classical groups. LMS Lecture Notes. Cambridge University Press, 2012. In preparation.

[Boo58] William W. Boone. The word problem. Proc. Nat. Acad. Sci. U.S.A., 44:1061–1065, 1958.

[CHN12] Marston Conder, George Havas, and M.F. Newman. On one-relator quotients of the modular group. Preprint, 2012.

[Cox39] H. S. M. Coxeter. The abstract groups $G^{m,n,p}$. Trans. Amer. Math. Soc., 45(1):73–150, 1939.

[Deh11] M. Dehn. Über unendliche diskontinuierliche Gruppen. Math. Ann., 71(1):116–144, 1911.

[DK02] Harm Derksen and Gregor Kemper. Computational invariant theory. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[DLS09] Vesselin Drensky and Roberto La Scala. Defining relations of low degree of invariants of two 4×4 matrices. Internat. J. Algebra Comput., 19(1):107–127, 2009.

[Don92] Stephen Donkin. Invariants of several matrices. Invent. Math., 110(2):389–401, 1992.

[Don10] Stephen Donkin. Private communication, 2010.

[DS06] V. Drensky and L. Sadikova. Generators of invariants of two 4×4 matrices. C. R. Acad. Bulgare Sci., 59(5):477–484, 2006.

[EHR91] D. B. A. Epstein, D. F. Holt, and S. E. Rees. The use of Knuth-Bendix methods to solve the word problem in automatic groups. J. Symbolic Comput., 12(4-5):397–414, 1991. Computational group theory, Part 2.

[EJ08] M. Edjvet and A. Juhász. The groups $G^{m,n,p}$. J. Algebra, 319(1):248–266, 2008.

[Fab09] Anna Fabiańska. Algorithmic analysis of presentations of groups and modules. PhD thesis, RWTH Aachen University, 2009.

[FK65] Robert Fricke and Felix Klein. Vorlesungen über die Theorie der automorphen Funktionen. Band 1: Die gruppentheoretischen Grundlagen. Band II: Die funktionentheoretischen Ausführungen und die Andwendungen, volume 4 of Bibliotheca Mathematica Teubneriana, Bände 3. Johnson Reprint Corp., New York, 1965.

[GH97] Stephen P. Glasby and Robert B. Howlett. Writing representations over minimal fields. Comm. Algebra, 25(6):1703–1711, 1997.

[GTZ88] Patrizia Gianni, Barry Trager, and Gail Zacharias. Gröbner bases and primary decomposition of polynomial ideals. J. Symbolic Comput., 6(2-3):149–167, 1988. Computational aspects of commutative algebra.

[Hal36] Philip Hall. The Eulerian functions of a group. Quart. J. Math., os-7(1):134–151, 1936.

[Har25] Robert W. Hartley. Determination of the ternary collineation groups whose coefficients lie in the GF(2^n). Ann. of Math. (2), 27(2):140–158, 1925.

[HN80] George Havas and M. F. Newman. Application of computers to questions like those of Burnside. In Burnside groups (Proc. Workshop, Univ. Bielefeld, Bielefeld, 1977), volume 806 of Lecture Notes in Math., pages 211–230. Springer, Berlin, 1980.

[Hog12] Torsten Hoge. A presentation of the trace algebra of three 3x3 matrices. J. Algebra, 358:257–268, 2012.

[Hor72] Robert D. Horowitz. Characters of free groups represented in the two-dimensional special linear group. Comm. Pure Appl. Math., 25:635–649, 1972.

[HR94] Derek F. Holt and Sarah Rees. Testing modules for irreducibility. J. Austral. Math. Soc. Ser. A, 57(1):1–16, 1994.

[Hup67] B. Huppert. Endliche Gruppen. I. Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[Jam11] Sebastian Jambor. Computing minimal associated primes in polynomial rings over the integers. Journal of Symbolic Computation, 46(10):1098–1104, 2011.

[KB70] Donald E. Knuth and Peter B. Bendix. Simple word problems in universal algebras. In Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967), pages 263–297. Pergamon, Oxford, 1970.

[Lan02] Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

[Law07a] Sean Lawton. Generators, relations and symmetries in pairs of 3 × 3 unimodular matrices. J. Algebra, 313(2):782–801, 2007.

[Law07b] Sean Lawton. Generators, relations and symmetries in pairs of 3 × 3 unimodular matrices. J. Algebra, 313(2):782–801, 2007.

[Lo96] Eddie Horkuen Lo. A polycyclic quotient algorithm. ProQuest LLC, Ann Arbor, MI, 1996. Thesis (Ph.D.)–Rutgers The State University of New Jersey - New Brunswick.

[Lop04] A. A. Lopatin. The ring of invariants of three third-order matrices over a field of prime characteristic. Sibirsk. Mat. Zh., 45(3):624–633, 2004.

[Lub99] Alexander Lubotzky. One for almost all: generation of $\mathrm{SL}(n, p)$ by subsets of $\mathrm{SL}(n, \mathbf{Z})$. In Algebra, K-theory, groups, and education (New York, 1997), volume 243 of Contemp. Math., pages 125–128. Amer. Math. Soc., Providence, RI, 1999.

[Mac69] A. M. Macbeath. Generators of the linear fractional groups. In Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), pages 14–32. Amer. Math. Soc., Providence, R.I., 1969.

[Mac86] I. D. Macdonald. Nilpotent quotient algorithms. In Proceedings of groups—St. Andrews 1985, volume 121 of London Math. Soc. Lecture Note Ser., pages 268–272, Cambridge, 1986. Cambridge Univ. Press.

[Mit11] Howard H. Mitchell. Determination of the ordinary and modular ternary linear groups. Trans. Amer. Math. Soc., 12(2):207–242, 1911.

[Nak02] Kazunori Nakamoto. The structure of the invariant ring of two matrices of degree 3. J. Pure Appl. Algebra, 166(1-2):125–148, 2002.

[Neu99] Jürgen Neukirch. Algebraic number theory, volume 322 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Nie94] Alice C. Niemeyer. A finite soluble quotient algorithm. J. Symbolic Comput., 18(6):541–561, 1994.

[Nov55] P. S. Novikov. Ob algoritmičeskoĭ nerazrešimosti problemy toždestva slov v teorii grupp (On the algorithmic unsolvability of the word problem in group theory). Trudy Mat. Inst. im. Steklov. no. 44. Izdat. Akad. Nauk SSSR, Moscow, 1955.

[Par84] R. A. Parker. The computer calculation of modular characters (the meat-axe). In Computational group theory (Durham, 1982), pages 267–274. Academic Press, London, 1984.

[PF09] Wilhelm Plesken and Anna Fabiańska. An L_2-quotient algorithm for finitely presented groups. J. Algebra, 322(3):914–935, 2009.

[Ple87] W. Plesken. Towards a soluble quotient algorithm. J. Symbolic Comput., 4(1):111–122, 1987.

[Pro76] C. Procesi. The invariant theory of $n \times n$ matrices. Advances in Math., 19(3):306–381, 1976.

[PSS11] Gerhard Pfister, Afshan Sadiq, and Stefan Steidel. An algorithm for primary decomposition in polynomial rings over the integers. Cent. Eur. J. Math., 9(4):897–904, 2011.

[Ste60] Robert Steinberg. Automorphisms of finite linear groups. Canad. J. Math., 12:606–615, 1960.

[Ste62] Robert Steinberg. Generators for simple groups. Canad. J. Math., 14:277–283, 1962.

[Ste05] Allan Steel. Conquering inseparability: primary decomposition and multivariate factorization over algebraic function fields of positive characteristic. J. Symbolic Comput., 40(3):1053–1075, 2005.

[TC36] J.A. Todd and H.S.M. Coxeter. A practical method for enumerating cosets of a finite abstract group. Proc. Edinb. Math. Soc., II. Ser., 5:26–34, 1936.

[Wam74] J. W. Wamsley. Computation in nilpotent groups (theory). In Proceedings of the Second International Conference on the Theory of Groups (Australian Nat. Univ., Canberra, 1973), pages 691–700. Lecture Notes in Math., Vol. 372, Berlin, 1974. Springer.

[WWT$^+$] Robert Wilson, Peter Walsh, Jonathan Tripp, Ibrahim Suleiman, Richard Parker, Simon Norton, Simon Nickerson, Steve Linton, John Bray, and Rachel Abbott. Atlas of Finite Group Presentations - Version 3. (`http://brauer.maths.qmul.ac.uk/Atlas/v3/`).