Presentations On Standard Generators For Some Classical Groups

Bachelor Thesis

Emma Katharina Ahrens

September 30, 2019

Supervised by Prof. Dr. Alice C. Niemeyer
and Dominik Bernhardt, M.Sc.

Submitted to Lehrstuhl B für Mathematik,
RWTH Aachen University

Contents

Notation

$\mathbb{N}$	set of natural numbers without 0
$\mathbb{Z}$	set of integers
$i, j, k, \ell, n, d, e \in \mathbb{N}$	natural numbers
f, g	polynomial functions
p and q	prime resp. prime power
M	matrix of a given dimension over a given field
$m_{i,j}$	defines the entry in the i-th row and j-th column of the matrix M
1 or id	neutral element of multiplication
I_n	identity matrix
μ_a	minimal polynomial of a
G	a group
$\lvert G\rvert$	order of the group G
$N \leq G$	N is subgroup of G
$N \trianglelefteq G$	N is normal subgroup of G
$G \cong H$	the groups, resp. fields, G and H are isomorphic
$\langle X \rangle$	the smallest group, resp. field, containing the elements in X
$\langle X \rangle_H$	the smallest normal subgroup of H containing the elements in X
$\varphi, \phi, \psi, \chi$	homomorphisms between groups or fields
$a^\pi, \varphi(x)$	application of π, resp. φ, to a, resp. x
$\mathrm{Ker}(\phi)$	the kernel of the homomorphism ϕ
$\mathrm{Im}(\phi)$	the image of the homomorphism ϕ
G/N	the quotient group of G and the normal subgroup N
$\det(M)$	determinant of the matrix M
$\mathrm{tr}(\alpha)$	field trace of α
ω	primitive element of a group
$\overline{x}$	Frobenius homomorphism
$\tilde{x}$	natural representation of $x \in \mathrm{GF}(p)$ in $\mathbb{N}$
$\{X \mid R\}$	presentation on the generators X with relators R
$\langle X \mid R \rangle$	group presented by the presentation $\{X \mid R\}$
$\mathrm{GF}(q)$	Galois field of order q
$\mathrm{GL}(n, q)$	general linear group: group of invertible $n \times n$ matrices over the field $\mathrm{GF}(q)$

S_n	symmetric group on the set $\{1, \ldots, n\}$
H_n	hyperoctahedral group: group of signed permutations
SH_n	signed permutation group: group of signed permutation matrices of determinant 1
$\mathrm{SL}(n, q)$	special linear group of degree n over the field $\mathrm{GF}(q)$
$\mathrm{PSL}(n, q)$	projective special linear group
$\mathrm{GU}(n, q)$	general unitary group of degree n over the field $\mathrm{GF}(q^2)$
$\mathrm{SU}(n, q)$	special unitary group
$\mathrm{PSU}(n, q)$	projective special unitary group

1. Introduction

This thesis lists *short* presentations for some finite classical and related groups on *standard generators*. These presentations can be used to verify isomorphisms of a given group algorithmically and every presentation given in this work is implemented in GAP. I follow the approach used by C.R. Leedham-Green and E.A. O'Brien in [LGOB19].

The obtained results are applied in the *matrix group recognition project* (see [Lee01]), which is a project in computational group theory. It aims to analyse a given matrix group G over a finite field and to algorithmically determine information about it. Some points of interest are the size of the group G, the membership of elements, and solving the word problem. One goal of this project is to check isomorphisms between subgroups of G and finite classical and related groups which can be done using presentations.

[LGOB19] defines *standard generators* for all finite classical groups and related simple groups. For a given group G there exist efficient *constructive recognition algorithms* which can be used to compute the standard generators of G. For that reason, our presentations are also defined on those standard generators which are listed in [LGOB09].

Since we want to verify the isomorphisms automatically (e.g. using GAP), we need to make sure that the performance of our algorithms is acceptable. It is crucial to make sure that even matrix groups, whose matrices are high dimensional, can be verified in reasonable time on today's computer centres. To achieve that goal, the number of matrix multiplications needs to be minimised. Additionally, to avoid memory problems, the number of stored large matrices shall be as small as possible.

A first approach tries to optimise the presentations from a mathematical point of view. Its goal is to minimise the number of generators and relations of the presentations. To measure the length of presentations numerically, we define the *bit-length* of a presentation (see Definition 20) which counts the number of generators and the number of multiplications in the relations. Leedham-Green and O'Brien have obtained the following result.

Theorem 1. *Every classical group of rank r defined over* $\mathrm{GF}(q)$ *has a presentation on its standard generators with $O(r)$ relations and total bit-length $O(r + \log q)$.*

All the presentations listed in this work have a bit-length smaller or equal $O(r + \log q)$ and hence we call them *short*.

The second approach is to optimise the implementation of those presentations. We can store products of matrices that are needed in several relations to avoid recalculation. On the other hand, it is important not to store too many products, because this might cause memory problems. This problem is addressed in Chapter 7.

In Chapter 2, I define everything that is needed to understand the results listed in the following chapters. This includes frequently used notation, the finite classical and related groups and presentations. Then I observe the symmetric group (Chapter 3), the group of signed permutation matrices (Chapter 4), the special linear group of degree 2 (Chapter 5) and the special unitary group of degree 3 (Chapter 6). For each, I list the standard generators of the group and presentations on those standard generators. Additionally, presentations for the projective groups are specified. My implementation is presented in Chapter 7. Note that the code is written in GAP and publicly available (see [GAP] and [Ahr]).

1.1. Matrix Group Recognition Project

To further motivate the results of this paper, I want to give some more prospects of the *matrix group recognition project* which is extracted from [OBr19].

Let n and q be natural numbers such that $\mathrm{GL}(n,q)$ is the general linear group of matrices of dimension n over the Galois field $\mathrm{GF}(q)$. Further $G \leq \mathrm{GL}(n,q)$ is the matrix group generated by $M_1, \ldots, M_k$.

In this context, we say that we can solve the *word problem* for a group $G := \langle M_1, \ldots, M_k \rangle$ if we can write any given element $M \in G$ as a product of the matrices $M_1, \ldots, M_k$. Furthermore, an epimorphism $\varphi : G \to H$ is called a *reduction* if φ is *explicitely computable* (which means that a computer can compute function values and preimages) and if H is *smaller* than G. Here, we call H smaller if we can either solve the word problem directly in H or it can be solved in fewer steps than in G.

The *Composition Tree algorithm* constructs a composition tree for the group G. This is done by randomised *constructive recognition algorithms* that search for reductions $\varphi : G \to H$. Simultaneously, homomorphisms $\iota : G \to N$ are constructed where N is the kernel of φ. The algorithm continues recursively on H and N and builds a Composition Tree until the word problem is solved in all leafs of this tree (see Figure 1.1). Note that $G/N \cong H$. If we can solve the word problem in N and H, then we can also solve it in G. Having solved the word problem in G, we can obtain all the desired information about the group.

Since the algorithms are randomised, we have to verify the results of the constructive recognition algorithms. Since we know the properties of the leafs (e.g. the isomorphism types), we construct a presentation for the whole group G using presentations for the leaf groups. The presentations obtained in the next chapters can be used for this purpose.

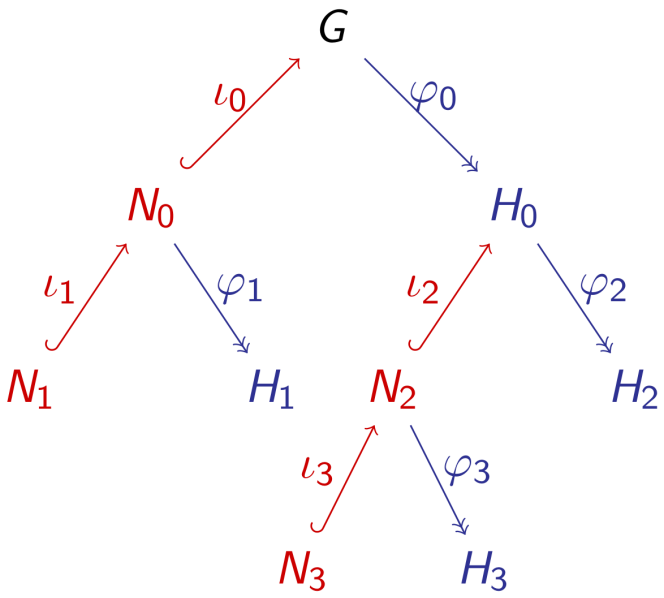


Figure 1.1.: Examplary *Composition Tree* of the group G.

2. Mathematical Background

In this chapter we establish notation, give basic definitions and prove a few theorems that should be observed independently from the work in the following chapters. Section 2.1 lists definitions and theorems. To understand the general ideas underpinning this work it is essential to be familiar with the mathematical background outlined in Section 2.2.

2.1. Definitions and General Theorems

Here we define some notation which is frequently used in the following chapters.

Definition 2 (Normal Closure, [HEO05], page 14)**.** *Let G be a group and $R \subseteq G$ a subset of G. Then the* ***normal closure*** *of R in G, which will be written as $\langle R \rangle_G$, is defined as the intersection of all normal subgroups N of G containing R. We set*

$$\langle R \rangle_G := \bigcap_{N \trianglelefteq G,\, R \subseteq N} N.$$

Theorem 3 (Inner Semidirect Product, [Hup67], page 89)**.** *Let G be a group with two subgroups $N, U \leq G$ such that $G = NU$, $N \trianglelefteq G$ and $U \cap N = \{1\}$. Then the following holds:*

(1) For every element $g \in G$ there exist a unique $n \in N$ and an element $u \in U$ such that $g = nu$.

(2) For $n_1, n_2 \in N$ and $u_1, u_2 \in U$ we have $(n_1u_1)(n_2u_2) = (n_1 n_2^{u_1^{-1}})(u_1u_2)$ with $n_1 n_2^{u_1^{-1}} \in N$ and $u_1u_2 \in U$.

Then we write $G := NU = N \rtimes U$ and call G a ***semidirect product*** *of N with U.*

Related to the inner semidirect product is the outer semidirect product, which is given for completeness.

Definition 4 (Outer Semidirect Product, [Hup67], page 89)**.** *Let H and K be groups and $\phi : K \times H \to K : (k, h) \mapsto k^h$ an action of H on K, such that for every $h \in H$ the function $(\cdot, h)^\phi$ is an automorphism of K. We define*

$$G := \{(k, h) \mid k \in K, h \in H\}$$

with

$$(k_1, h_1)(k_2, h_2) = (k_1(k_2, h_1)^\phi, h_1h_2)$$

for all $k_1, k_2 \in K$ and $h_1, h_2 \in H$. Then G is a group with the above defined multiplication and we write $G := K \rtimes H$ and call it the ***outer semidirect product*** *of K with H.*

Note that $\{\mathrm{id}\} \times H \leq K \rtimes H$ is a subgroup and $K \times \{\mathrm{id}\} \trianglelefteq K \rtimes H$ is a normal subgroup of the outer direct product $K \rtimes H$ with the notation in Definition 4. Thus those groups form an inner direct product of $K \rtimes H$.

Definition 5 (Permutation Group, [Ker71], page 5)**.** *A* ***permutation group*** *G on Ω is a subgroup of the symmetric group $\mathrm{S}(\Omega)$.*

A similar concept is the wreath product.

Definition 6 (Wreath Product, [Hup67], page 95)**.** *Let G be a group and H a permutation group on Ω. Then the* ***wreath product*** *$G \wr H$ of G with H is the set*

$$\{(f, \pi) \mid \pi \in H, f : \Omega \to G\}$$

with the multiplication

$$(f_1, \pi_1)(f_2, \pi_2) = (g, \pi_1\pi_2)$$

where $g(i) = f_1(i)f_2(i^{\pi_1})$ for $i \in \Omega$.

Now we list and prove a few theorems, which will be needed later. Note that they are very general and could be helpful in many different proofs.

Theorem 7. *Let G and H be finite groups, $\varphi : G \twoheadrightarrow H$ an epimorphism and $N \trianglelefteq G$ and $M \trianglelefteq H$ normal subgroups such that*

- *$G/N \cong H/M$ and*
- *$N \cong M$.*

Then G and H are isomorphic.

The prerequisites of Theorem 7 state that this commutative diagram holds:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \downarrow{\scriptstyle \trianglelefteq} & & \downarrow{\scriptstyle \trianglelefteq} \\ N & \xrightarrow{\sim} & M \end{array}$$

Proof. From the isomorphism between G/N and H/M it follows that $|G/N| = |H/M|$ and $N \cong M$ implies that $|N| = |M|$. Then

$$|G| = |G/N||N| = |H/M||M| = |H|.$$

Together with the epimorphism φ, it follows that $G \cong H$. □

Lemma 8. *Let $q := p^e$, p a prime, $e \in \mathbb{N}$ and $\omega \in \mathrm{GF}(q)$ a primitive element. Then we have*

$$\sum_{i=0}^{\frac{q-1}{2}-1} \omega^{2i} = 0.$$

Proof. We know that $(\omega^{\frac{q-1}{2}})^2 = \omega^{q-1} = 1$ and thus $\omega^{\frac{q-1}{2}} = -1$.

Suppose first that $q \equiv 1 \bmod 4$. Then $\frac{q-1}{2}$ is even and the terms of the sum can be paired such that

$$\begin{aligned}
\sum_{i=0}^{\frac{q-1}{2}-1} \omega^{2i} &= \omega^0 + \omega^2 + \omega^4 + \ldots + \omega^{q-3} \\
&= \omega^0 + \omega^2 + \ldots + \omega^{\frac{q-1}{2}-2} + \omega^{\frac{q-1}{2}} + \ldots + \omega^{q-3} \\
&= (\omega^0 + \omega^{\frac{q-1}{2}}) + (\omega^2 + \omega^{\frac{q-1}{2}+2}) + \ldots + (\omega^{\frac{q-1}{2}-2} + \omega^{q-3}) \\
&= \underbrace{(\omega^0 - \omega^0)}_{=0} + \underbrace{(\omega^2 - \omega^2)}_{=0} + \ldots + \underbrace{(\omega^{\frac{q-1}{2}-2} - \omega^{\frac{q-1}{2}-2})}_{=0} = 0.
\end{aligned}$$

Note that $2(\frac{q-1}{2} - 1) = q - 3 = (\frac{q-1}{2} - 2) + \frac{q-1}{2}$.

Now suppose $q \equiv 3 \bmod 4$. Then $\frac{q-1}{2}$ is odd and we can reorder the sum to obtain

$$\begin{aligned}
\sum_{i=0}^{\frac{q-1}{2}-1} \omega^{2i} &= \omega^0 + \omega^2 + \omega^4 + \ldots + \omega^{q-3} \\
&= \omega^0 + \omega^2 + \ldots + \omega^{\frac{q-1}{2}-1} + \omega^{\frac{q-1}{2}+1} + \ldots + \omega^{\frac{q-1}{2}-1} \\
&= \omega^0 + \omega^{\frac{q-1}{2}+1} + \omega^2 + \omega^{\frac{q-1}{2}+3} + \ldots + \omega^{\frac{q-1}{2}-1} + \omega^{\frac{q-1}{2}-1} \\
&= \omega^0 - \omega^1 + \omega^2 - \omega^3 \pm \ldots + \omega^{\frac{q-1}{2}-1}.
\end{aligned}$$

Then it follows that

$$\begin{aligned}
(1+\omega)(\omega^0 - \omega^1 + \omega^2 - \omega^3 \pm \ldots + \omega^{\frac{q-1}{2}-1}) = \omega^0 + \omega^{\frac{q-1}{2}} = 1 - 1 = 0 \\
\Leftrightarrow (1+\omega) \sum_{i=0}^{\frac{q-1}{2}-1} \omega^{2i} = 0.
\end{aligned}$$

We know that $1 + \omega \neq 0$, thus $\sum_{i=0}^{\frac{q-1}{2}-1} \omega^{2i} = 0$. □

Lemma 9. *Let $q := p^e \in \mathbb{N}$, where p is a prime. Then we call*

$$\bar{\cdot} : \mathrm{GF}(q^2) \to \mathrm{GF}(q^2), x \mapsto x^q$$

*the **Frobenius homomorphism**. This map is an automorphism of $\mathrm{GF}(q^2)$, the fixed field of $\bar{\cdot}$ is $\mathrm{GF}(q)$ and we have $\overline{x+y} = \overline{x} + \overline{y}$.*

See [Nie18] for proofs of those claims.

Definition 10 (Trace)**.** *Let $k, e \in \mathbb{N}$. Then we define the homomorphism*

$$\mathrm{tr} : \mathrm{GF}(k^e) \to \mathrm{GF}(k^e), x \mapsto \sum_{i=0}^{e-1} x^{k^i}$$

and call it the ***trace*** *of an element.*

Lemma 11. *Let $q \in \mathbb{N}$ be a prime power. Then the kernel of the field homomorphism $\mathrm{tr} : \mathrm{GF}(q^2) \to \mathrm{GF}(q^2), x \mapsto x + x^q$ has order q and the image is $\mathrm{GF}(q)$.*

Proof. Let $\omega \in \mathrm{GF}(q^2)$ be a primitive element and suppose $k \in \mathbb{N}$ such that $\omega^k \in \mathrm{Ker(tr)}$, i.e.

$$\omega^k + \omega^{kq} = 0.$$

Then we obtain

$$\begin{aligned} &\omega^k + \omega^{kq} = 0 \Leftrightarrow \omega^k = -\omega^{kq} \\ \Leftrightarrow\ &\omega^k = \omega^{\frac{q^2-1}{2}} \omega^{kq} \Leftrightarrow 1 = \omega^{\frac{q^2-1}{2} + k(q-1)} \\ \Leftrightarrow\ &\frac{q^2-1}{2} + k(q-1) \equiv 0 \bmod q^2 - 1. \end{aligned}$$

This holds for all $k = \frac{q+1}{2}m$, where $m \in \mathbb{N}$ is odd. The elements ω^{k_1} and ω^{k_2}, for $k_1 = \frac{q+1}{2}m_1$ and $k_2 := \frac{q+1}{2}m_2$, are unequal for odd natural numbers $m_1 \neq m_2$ and $k_1, k_2 \leq q^2 - 1$. Thus we may choose any odd $m \leq 2(q-1)$ and the kernel has $q-1$ elements and zero, thus order q.

It follows with the homomorphism theorem, that the image of tr has also order q and for every $x \in \mathrm{GF}(q^2)$ we have

$$\mathrm{tr}(x)^q = \mathrm{tr}(x),$$

thus the image $\mathrm{Im(tr)} \subseteq \mathrm{GF}(q)$ and it follows directly that $\mathrm{Im(tr)} = \mathrm{GF}(q)$. □

Lemma 12. *Let $f : \mathrm{GF}(q^2) \to \mathrm{GF}(q), \alpha \mapsto \alpha^{q+1}$, then the kernel of f has cardinality $|\mathrm{Ker}(f)| = q + 1$.*

Proof. Let $\omega \in \mathrm{GF}(q^2)$ be a primitive element, $\alpha \in \mathrm{GF}(q^2)$ and $k \in \mathbb{N}$ such that $\alpha = \omega^k$. Then $f(\alpha) = 1 \Leftrightarrow \alpha^{q+1} = 1 \Leftrightarrow \omega^{k(q+1)} = \omega^0$. This holds if $k = m(q-1)$ for some $m \in \mathbb{N}$. We have $\omega^k \neq \omega^{k'}$ for all $1 < k, k' < q^2$ and $k \neq k'$. Thus $\mathrm{Ker}(f) = \{\omega^{m(q-1)} \mid 1 \leq m \leq q+1\}$ and the claim holds. □

2.2. Presentations

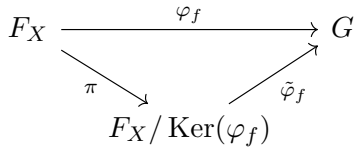
In this section we introduce presentations of groups. The idea is to construct an isomorphism between a group G and a quotient of a free group F_X. First we define free groups.

Definition 13 (Free group, [Joh90], page 1)**.** *Let F be a group and $X \subseteq F$ a subset. Then the group F is called the **free group** on X if, for any group G and any map $f : X \to G$, there is a unique homomorphism $\varphi_f : F \to G$ extending f such that $x^{\varphi_f} = x^f$ for all $x \in X$.*
*From now on we will write F_X for the free group on a set X, where X is called the **basis** and $|X|$ the **rank** of the group F_X.*

The following proposition highlights the importance of presentations. It states that for every group G there exists a quotient group of a free group which is isomorphic to G. As an implication we obtain that there exists a presentation for every group.

Proposition 14 ([Joh90], page 19)**.** *Every group is isomorphic to a factor group of some free group.*

Proof. Let G be a group and X a set of generators of G. Then we define the map $f : X \to G, x \mapsto x$. Then Definition 13 states that there exists a unique homomorphism $\varphi_f : F_X \to G$ extending f. We obtain



where π is the canonical surjective map and $\tilde{\varphi}_f$ is bijective because $\operatorname{Im}(\varphi_f) = G$. The isomorphism $G \cong F_X / \operatorname{Ker}(\varphi_f)$ follows by the homomorphism theorem for groups (see [Hup67], page 15). □

Now we define a presentation. For every presentation we specify a presented group, which is a quotient group of a free group.

Definition 15 (Presentation of a group, [HEO05], page 36)**.** *Let X be a set, F_X the free group on X and $R \subseteq F_X$. Then we call $\{X \mid R\}$ a **presentation** for the group $G := F_X/N$, where $N = \langle R \rangle_{F_X}$ is the normal closure of R in F_X. We write $G = \langle X \mid R \rangle$.*
*The elements of R are called **relators** and G is **finitely presented** if X and R are finite sets.*

Since we have seen that there exists an isomorphic quotient group of a free group for every group G (see Proposition 14), it follows with the previous lemma that there exists a presentation for every group G.

Proposition 16 ([Joh90], page 54)**.** *Every group has a presentation.*

Proof. We use Proposition 14. Let G be a group, X a set of generators of G and F_X the free group on X. Then there exists an unique homomorphism $\varphi_f : F_X \to G$ (see the proof of Proposition 14) and the proposition yields $G \cong F_X/Ker(\varphi_f)$. Now we can write $G = \langle X \mid Ker(\varphi_f)\rangle$ and obtain the presentation. □

We know now that every group has a presentation. For our purposes we are interested in finite presentations, which means that the number of generators and relators is finite. Since we use this kind of presentation a lot in subsequent chapters, we define a shorter notation for simplicity.

Definition 17 ([Joh90], page 41)**.** *Let G be finitely presented by $\{X \mid R\}$ with $X := \{x_1, \ldots, x_n\}$ a set, F_X the free group on X and $\{r_1, \ldots, r_m\} =: R \subseteq F_X$. Then we write $r_i = r_i(x_1, \ldots, x_n) \in F_X$ and call r_i a relator of G. From now on we also use*

$$\{x_1, \ldots, x_n \mid r_1, \ldots, r_m\}$$

as a notation for a finite presentation.

The main task in this thesis is to determine presentations for the finite classical and related groups. We do this by seeking homomorpisms between a group G and a presented group. If we can prove that those two groups are isomorphic, then the presentation is a presentation for G. The next proposition offers a way to show that a map from generators of a free group to elements in G can be extended to a homomorphism from the quotient group of the free group to G.

Proposition 18 (Substitution Test, [Joh90], page 56)**.** *Let $\langle X \mid R\rangle$ be a presentation of the group G, H another group and $\varphi : X \to H$ a map. Then φ extends to a homomorphism $\varphi'' : G \to H$ if and only if, for all $x \in X$ and $r \in R$, the result of substituting x^φ for x in r yields the identity in H, thus $r(x_1^\varphi, \ldots, x_n^\varphi) = e_H$ for all $r \in R$ if $X = \{x_1, \ldots, x_n\}$ is a finite set.*

Proof. Let $\varphi : X \to H$ be a map. Then this map extends to a unique homomorphism $\varphi' : F_X \to H$, because F_X is the free group on X.
Now the homomorphic extension $\varphi'' : G = F_X/R \to H,\ gR \mapsto \varphi'(g)$ is well-defined if the images are independent of the representatives, thus for all $g \in F_X$ and $r \in R$

$$\begin{aligned} &\varphi'(gr) = \varphi'(g) \\ \Leftrightarrow\ &\varphi'(r) = \varphi'(r(x_1, \ldots, x_n)) = \mathrm{id}_H \\ \Leftrightarrow\ &r(x_1^{\varphi'}, \ldots, x_n^{\varphi'}) = r(x_1^\varphi, \ldots, x_n^\varphi) = \mathrm{id}_H\,. \end{aligned}$$

It follows that $R \subseteq \mathrm{Ker}(\varphi')$.
Conversely, let $R \subseteq \mathrm{Ker}(\varphi')$. Then $\varphi'' : G \to H$ is independent of the representatives of G and thus φ'' is well-defined. □

This last proposition is used frequently to prove the correctness of presentations.

Proposition 19 ([Bou13], Proposition 4.7)**.** *Let $G := \langle X \rangle$, $H \leq G$ and $S = \cup_{i=1}^{r} H g_i$ for some $g_i \in G$ and $g_1 = 1$. If $g_i a \in S$ for all $a \in X \cup X^{-1}$, then $G = S$. If we know that the order $|x|$ is finite for all $x \in X$, then it is enough to show that $g_i a \in S$ for all $x \in X$.*

Refer to [Bou13] for a proof of this proposition.

Now we define the length of a presentation. The shorter the length of a presentation, the faster is the evaluation of the relations on the generators of some group G. Since a main aspiration of this work is to verify isomorphisms between a group G and a classical or related group in a fast and efficient way, we aim to give presentations that are as short as possible. For this purpose we define the bit-length of a presentation, which essentially counts the number of generators and the number of multiplications used in the relations.

Definition 20 (Bit-Length, [LGOB19], page 4)**.** *The **bit-length** of a presentation $\{X \mid R\}$ is defined as $|X|$ plus the total number of bits required to encode the words in R as strings over the alphabet $X \cup X^{-1}$, where all exponents are encoded as binary strings.*

Leedham-Green and O'Brien show in [LGOB19] that for every classical group there exists a presentation whose bit-length is limited by some linear function depending on the rank of the group and the field over which it is defined.

Theorem 21 ([LGOB19], page 5)**.** *Every classical group of rank r defined over $\mathrm{GF}(q)$ has a presentation on its standard generators with $O(r)$ relations and total bit-length $O(r + \log q)$.*

All the presentations given in the next chapters (except for the Coxeter presentation of the symmetric group in Lemma 25) are of length limited by the function given in Theorem 21. We call those presentations **small**.

3. Symmetric Group S_n

We state two presentations of the symmetric group in this chapter. The symmetric group is closely related to the alternating group, which yields one family of finite simple groups. Before we look at the presentations, we analyse the elements in the group. This helps us to prove the correctness of the presentations.

Definition 22 (Symmetric Group, [Hup67], page 24)**.** *The* ***symmetric group*** $\mathrm{S}_n := \{f : \{1,\dots,n\} \to \{1,\dots,n\} \mid f \text{ bijective}\}$ *is the group of all bijections on a set of size* n*. We write the elements of* S_n *as permutations, hence as products of disjoint cycles, and the action of a permutation* $g \in \mathrm{S}_n$ *on an element* $m \in \{1,\dots,n\}$ *as* m^g*.*

For a presentation of the symmetric group, we need to know a bit more about the group. We want to find sets of generators of the symmetric group and the next lemma is useful for that purpose.

Lemma 23. *Every transposition* $\tau_i = (i, i+1) \in \mathrm{S}_n$ *can be written as a product of* $\tau_1 = (1,2) \in \mathrm{S}_n$ *and the* n*-cycle* $g := (1,2,\dots,n) \in \mathrm{S}_n$*.*

Proof. We verify this by induction.

- Base Case: Let $i := 2$. Then we have $g^{-1}\tau_1 g = (n,\dots,1)(1,2)(1,\dots,n) =: h$ and
$$x^h = x \text{ for all } x \in \{1,4,5,\dots,n\}.$$
Also $2^h = 3$ and $3^h = 2$, thus $h = (2,3) = \tau_2$.
- The induction hypothesis is that $\tau_i = g^{-i+1}\tau_1 g^{i-1}$ holds for an $i \in \{1,\dots,n-1\}$.
- Induction Step: Now $i \mapsto i+1$. Then it follows that $g^{-i}\tau_1 g^i = g^{-1}g^{-(i-1)}\tau_1 g^{i-1}g$ and with the induction hypothesis $g^{-1}g^{-(i-1)}\tau_1 g^{i-1}g = g^{-1}\tau_{i-1}g = (n,\dots,1)(i-1,i)(1,\dots,n) =: h$. Again
$$x^h = x \text{ for all } x \in \{1,2,\dots,i-1,i,i+3,i+4,\dots,n-1,n\}$$
and $i^h = i+1$ and $(i+1)^h = i$. Hence $h = (i,i+1)$ and the assumption follows.

□

We have shown that two permutations suffice to construct any transposition $(i, i+1) \in \mathrm{S}_n$. We are able to determine two different sets of generators of the symmetric group from this result.

Lemma 24. *The symmetric group* S_n *is generated by* $(1,2)$ *and* $(1,\ldots,n)$ *or the set of adjacent transpositions* $(i,i+1)$ *for* $i \in \{1,\ldots,n-1\}$.

Proof. It is proven in [Beu94], page 211, that $\mathrm{S}_n = \langle (1,2),\ldots,(n-1,n)\rangle$. From Lemma 23 we know that every transposition $(i,i+1)$ with $i \in \{1,\ldots,n-1\}$ can be written as a product of $(1,2)$ and $(1,\ldots,n)$. Also $(1,2),(1,\ldots,n) \in \mathrm{S}_n$, thus

$$\langle (1,2),(1,\ldots,n)\rangle = \mathrm{S}_n\,.$$

□

We obtained two different generating sets of the symmetric group and the next section defines a presentation on each set.

3.1. Presentation

In this section we want to prove that the group presented by the short presentation

$$\{X \mid R\} := \{\, U,V \mid U^2 = V^n = (UV)^{n-1} = (UU^V)^3 = (UU^{V^j})^2 = 1 \text{ for } 2 \le j \le n/2 \,\},$$

which was given [Moo96], p.357-367, is isomorphic to the symmetric group S_n for $n > 2$. A few steps are needed for the verification of this claim. We show that there exists another presentation

$$\{\tilde{X} \mid \tilde{R}\} := \{\, \tau_1,\ldots,\tau_{n-1} \mid \tau_i^2 = (\tau_i\tau_{i+1})^3 = (\tau_i\tau_j)^2 = 1 \;\forall j > i+1 \,\}$$

for the symmetric group S_n. Then we use this presentation to prove the existence of the epimorphisms $\varphi'' : \langle X \mid R\rangle \to \mathrm{S}_n$ and $\theta'' : \langle \tilde{X} \mid \tilde{R}\rangle \to \langle X \mid R\rangle$. If all these requirements hold, then it follows that φ'' is isomorphic and the presentation $\langle X \mid R\rangle$ is correct.

First we prove that the presentation $\{\tilde{X} \mid \tilde{R}\}$ is a presentation of S_n. Thus we show the existence of a well-defined isomorphism $\chi'' : \langle \tilde{X} \mid \tilde{R}\rangle \to \mathrm{S}_n$.

Lemma 25 ([Moo96] and [Bou13], p.13)**.** *The symmetric group* S_n *has the presentation*

$$\{\tilde{X} \mid \tilde{R}\} := \{\, \tau_1,\ldots,\tau_{n-1} \mid \tau_i^2 = (\tau_i\tau_{i+1})^3 = (\tau_i\tau_j)^2 = 1 \;\forall j > i+1 \,\}$$

for $n > 2$.

Proof. Let $\chi : \tilde{X} \to \mathrm{S}_n$ be a map with $\tau_i \mapsto (i,i+1)$. The group S_n is generated by $\{(1,2),(2,3),\ldots,(n-1,n)\}$ by Lemma 24 and we have

- $\tilde{r}_i^1(\tau_1,\ldots,\tau_{n-1}) := \tau_i^2$ for $i \in \{1,\ldots,n-1\}$. Thus

$$\tilde{r}_i^1(\tau_1^\chi,\ldots,\tau_{n-1}^\chi) = (i,i+1)^2 = \mathrm{id}_{\mathrm{S}_n}\,.$$

- $\tilde{r}_i^2(\tau_1, \ldots, \tau_{n-1}) := (\tau_i\tau_{i+1})^3$ for $i \in \{1, \ldots, n-2\}$ and

$$\begin{aligned}\tilde{r}_i^2(\tau_1^\chi, \ldots, \tau_{n-1}^\chi) &= ((i, i+1)(i+1, i+2))^3 \\ &= (i, i+2, i+1)^3 = \mathrm{id}_{\mathrm{S}_n}.\end{aligned}$$

- $\tilde{r}_i^3(\tau_1, \ldots, \tau_{n-1}) := (\tau_i\tau_{i+l})^2$ for $i \in \{1, \ldots, n-3\}$ and $j > i+1$. Thus

$$\tilde{r}_i^3(\tau_1^\chi, \ldots, \tau_{n-1}^\chi) = ((i, i+1)(j, j+1))^2 = \mathrm{id}_{\mathrm{S}_n}$$

  because $i, i+1, j$ and $j+1$ are pairwise distinct.

Let $\tilde{N} := \langle \tilde{R} \rangle_{F_{\tilde{X}}}$. It follows with Lemma 18 that there exists a homomorphic extension $\chi'' : F_{\tilde{X}}/\tilde{N} \to \mathrm{S}_n$ of χ, which is also surjective since $\tilde{N} \leq \mathrm{Ker}(\chi'')$. Thus $|F_{\tilde{X}}/\tilde{N}| \geq |\mathrm{S}_n| = n!$.

Now we call G_n the group presented by $\{\tilde{X} \mid \tilde{R}\}$ for some $n \in \mathbb{N}$. We use induction to show that $|G_n| \leq n!$ for all $2 \leq n \in \mathbb{N}$.

- Base Case: Assume that $n := 2$. Then $G_n := \langle \tau_1 \mid \tau_1^2 \rangle$ and $|G_n| = 2 = 2!$.
- Induction Hypothesis: $|G_n \leq n!$ for an arbitrary but fixed $n \in \mathbb{N}$ with $2 \leq n$.
- Induction Step: Let $2 \leq n \in \mathbb{N}$ such that $|G_n| \leq n!$. We define $H := \langle \tau_2, \ldots, \tau_n \rangle \leq G_{n+1}$. We can renumber the generators of H to $\tau_1, \ldots, \tau_{n-1}$ and obtain that the relations of G_n are satisfied. We apply the induction hypothesis and it follows that $|H| \leq n!$.

  We want to prove that $|G_{n+1} : H| \leq n+1$. Since $\chi''(H) \cong \mathrm{S}_n$ is a stabilizer of 1 in S_{n+1}, we obtain that $\{g_0, \ldots, g_n\}$ is a coset representation where $\chi''(g_i)$ maps 1 to $i+1$ for any $0 \leq i \leq n$. Thus we choose $g_0 = 1$ and $g_i = \tau_1 \cdots \tau_i \in G_{n+1}$. We define $S := \cup_{i=0}^n H g_i$ and we need to prove that $S = G_n$. Using Proposition 19 we obtain that it is sufficient to prove that $g_i\tau_j \in S$ for all $0 \leq i, j \leq n$.

  Case 1 Let $j > i+1$. Then it follows that $g_i\tau_j = \tau_j g_i \in S$ since $\tau_j \in H$.

  Case 2 Let $j = i+1$. Then we have $g_i\tau_j = g_{i+1} \in S$.

  Case 3 Let $j = 1$. Then we have $g_i\tau_j = g_{i-1} \in S$.

  Case 4 Let $j < i$. Again we use induction and show that $g_i\tau_j = \tau_{j+1}g_i \in S$ for all $1 \leq i - j \leq n-1$ and $\tau_{j+1} \in H$.

  - Base Case: Assume that $i - j = 1$ with $i \geq 2$ and $j = i - 1$. Then $g_i\tau_j = g_{i-2}\tau_{i-1}\tau_i\tau_{i-1} = g_{i-2}\tau_i\tau_{i-1}\tau_i = \tau_i g_{i-2}\tau_{i-1}\tau_i = \tau_i g_i = \tau_{j+1}g_i \in S$.
  - Induction Hypothesis: The claim holds for an arbitrary but fixed $n \in \mathbb{N}$.
  - Induction Step: We assume the induction hypothesis and show that the claim holds for $n+1 = i - j$. Then we obtain $g_i\tau_j = g_{i-1}\tau_i\tau_j = g_{i-1}\tau_j\tau_i = \tau_{j+1}g_{i-1}\tau_i = \tau_{j+1}g_i \in S$.

  Hence $|G_{n+1} : H| \leq n+1$ and $|G_{n+1}| \leq (n+1)!$.

Now χ'' is an isomorphism and Lemma 25 follows. □

In the next lemma we show that there exists a subgroup $M \leq \langle X \mid R\rangle$ such that $\langle X \mid R\rangle/M \cong \mathrm{S}_n$.

Lemma 26. *Let $\varphi : X \to \mathrm{S}_n$ be a map with $U \mapsto (1,2)$ and $V \mapsto (1,\dots,n)$. Then there exists a surjective homomorphic extension $\varphi'' : \langle X \mid R\rangle \to \mathrm{S}_n$ of φ.*

Proof. Lemma 24 states that $\langle (1,2),(1,\dots,n)\rangle = \mathrm{S}_n$. Hence φ is surjective. Using Proposition 18 it remains to show that for every $r \in R$ the substitution of $x \in X$ by $x^{\varphi''}$ is equal to the identity in S_n.

- $r_1(U,V) := U^2$. Then
$$r_1(U^{\varphi''}, V^{\varphi''}) = (1,2)^2 = \mathrm{id}_{\mathrm{S}_n}.$$
- $r_2(U,V) := V^n$. Then
$$r_2(U^{\varphi''}, V^{\varphi''}) = (1,\dots,n)^n = \mathrm{id}_{\mathrm{S}_n}.$$
- $r_3(U,V) := (UV)^{n-1}$. Then
$$r_3(U^{\varphi''}, V^{\varphi''}) = ((1,2)(1,\dots,n))^{n-1} = (1,3,4,\dots,n)^{n-1} = \mathrm{id}_{\mathrm{S}_n}.$$
- $r_4(U,V) := (UU^V)^3$. Then
$$r_4(U^{\varphi''}, V^{\varphi''}) = ((1,2)(1,2)^{(1,\dots,n)})^3 = ((1,2)(2,3))^3 = (1,3,2)^3 = \mathrm{id}_{\mathrm{S}_n}.$$
- $r_5(U,V) := (UU^{V^j})^2$ for $2 \leq j \leq n/2$. With Lemma 23 it follows that
$$r_5(U^{\varphi''}, V^{\varphi''}) = ((1,2)(1,2)^{(1,\dots,n)^j})^2 = ((1,2)(j+1,j+2))^2 \overset{1)}{=} \mathrm{id}_{\mathrm{S}_n}$$
where 1) follows because $1, 2, j+1, j+2$ are pairwise distinct.

Thus there exists a surjective homomorpic extension $\varphi'' : \langle X \mid R\rangle = F_X/N \to \mathrm{S}_n$ of φ where $N = \langle R\rangle_{F_X}$. □

We have shown that there exists an isomorphism $\chi'' : \langle \tilde{X} \mid \tilde{R}\rangle \to \mathrm{S}_n$ and an epimorphism $\varphi'' : \langle X \mid R\rangle \to \mathrm{S}_n$. The next step is to show that there exists an epimorphism $\theta'' : \langle \tilde{X} \mid \tilde{R}\rangle \to \langle X \mid R\rangle$. The proof is similar to the proof of Lemma 26.

Lemma 27. *The map $\theta : \tilde{X} \to \langle X \mid R\rangle = F_X/N$ with $\tau_i \mapsto U^{V^{i-1}}N$, where $N = \langle R\rangle_{F_X}$, extends to an epimorphism $\theta'' : \langle \tilde{X} \mid \tilde{R}\rangle \to \langle X \mid R\rangle$.*

Proof. Again Proposition 18 is used to verify that there exists such an extension. When substituting $\tilde{x} \in \tilde{X}$ by $\tilde{x}^\theta$ in the relations in $\tilde{R}$ then the result should be N.

- $\tilde{r}_i^1(\tau_1, \ldots, \tau_{n-1}) := \tau_i^2$ for an $i \in \{1, \ldots, n-1\}$. Then

$$\begin{aligned}\tilde{r}_i^1(\tau_1^\theta, \ldots, \tau_{n-1}^\theta) &= (U^{V^{i-1}}N)^2 \\ &\overset{1)}{=} V^{-(i-1)}UV^{i-1}V^{-(i-1)}UV^{i-1}N \\ &= V^{-(i-1)}U^2V^{i-1}N \\ &\overset{2)}{=} V^{-(i-1)}V^{i-1}N = N\end{aligned}$$

  where 1) follows because N is a normal subgroup and 2) from the relation $U^2 \in R$.

- $\tilde{r}_i^2(\tau_1, \ldots, \tau_{n-1}) := (\tau_i\tau_{i+1})^3$ for an $i \in \{1, \ldots, n-2\}$. Then

$$\begin{aligned}\tilde{r}_i^2(\tau_1^\theta, \ldots, \tau_{n-1}^\theta) &= (U^{V^{i-1}}NU^{V^i}N)^3 \\ &\overset{1)}{=} (V^{-(i-1)}UV^{i-1}V^{-i}UV^i)^3N \\ &= V^{-(i-1)}(UV^{-1}UV)^3V^{i-1}N \\ &= V^{-(i-1)}(UU^V)^3V^{i-1}N \\ &\overset{2)}{=} V^{-(i-1)}V^{i-1}N = N\end{aligned}$$

  where 1) follows again because N is a normal subgroup and 2) because $(UU^V)^3$ is a relation in R.

- $\tilde{r}_i^3(\tau_1, \ldots, \tau_{n-1}) := (\tau_i\tau_{i+l})^2$ for an $i \in \{1, \ldots, n-1\}$ and $l > 1$. Then

$$\begin{aligned}\tilde{r}_i^3(\tau_1^\theta, \ldots, \tau_{n-1}^\theta) &= (U^{V^{i-1}}NU^{V^{i+l-1}}N)^2 \\ &\overset{1)}{=} (U^{V^{i-1}}U^{V^{i+l-1}})^2N \\ &= (V^{-(i-1)}UV^{i-1}V^{-(i+l-1)}UV^{i+l-1})^2N \\ &\overset{2)}{=} V^{-(i-1)}(UV^{-l}UV^l)^2V^{i-1}N \\ &= V^{-(i-1)}V^{i-1}N = N\end{aligned}$$

  where 1) follows once again because N is a normal subgroup and 2) because $(UU^{V^l})^2$ is a relation in R for $l > 1$.

Now such an extension θ'' exists and $\langle\tilde{R}\rangle_{F_{\tilde{X}}} = \tilde{N} \leq \mathrm{Ker}(\theta'')$, thus we obtain that this extension is also surjective. □

Everything is ready to prove that the short presentation given in Theorem 28 is a presentation of the symmetric group S_n.

Theorem 28. *For $n > 2$ the symmetric group S_n has the presentation*

$$\{X \mid R\} := \{\, U, V \mid U^2 = V^n = (UV)^{n-1} = (UU^V)^3 = (UU^{V^j})^2 = 1 \text{ for } 2 \leq j \leq n/2 \,\}.$$

Proof. By Lemma 26 there exists an epimorphism $\varphi'' : \langle X \mid R \rangle \to \mathrm{S}_n$, thus

$$\langle X \mid R \rangle / M \cong \mathrm{S}_n$$

for a subgroup $M \leq \langle X \mid R \rangle$.
On the other hand it is known by Lemma 25 that there exists an isomorphism $\chi : \mathrm{S}_n \to F_{\tilde{X}}/\tilde{N}$ and Lemma 27 implies that there is an epimorphism $\theta'' : \langle \tilde{X} \mid \tilde{R} \rangle \to \langle X \mid R \rangle$. Thus

$$\mathrm{S}_n / \hat{M} \cong \langle \tilde{X} \mid \tilde{R} \rangle / \tilde{M} \cong \langle X \mid R \rangle$$

for a subgroup $\hat{M} \leq \mathrm{S}_n$ and an isomorphic subgroup $\tilde{M} \leq \langle \tilde{X} \mid \tilde{R} \rangle$.
It follows that $\langle X \mid R \rangle \cong \mathrm{S}_n$ and $\{X \mid R\}$ is a presentation of S_n. □

We have shown that there exists a short presentation of the symmetric group. Note that the presentation given in Lemma 25 is not a short presentation. Only the presentation given in Theorem 28 is short.

4. Group of Signed Permutation Matrices of Determinant 1 SH_n

The group of signed permutation matrices of determinant 1, in short SH_n, is isomorphic to a subgroup of the hyperoctahedral group H_n, which is the group of all signed permutations on the set $\{\pm 1, \ldots, \pm n\}$. This chapter starts with the definition of signed permutations and the hyperoctahedral group in Section 4.1. In the next section we define the group of signed permutation matrices of determinant 1 and Section 4.3 gives a presentation for this group.

4.1. Hyperoctahedral Group H_n

This section defines the hyperoctahedral group H_n. We start by defining signed permutation cycles. Using those cycles we can easily define general signed permutations.

Definition 29 (Signed Permutation Cycle, [LGOB19], page 7)**.** *A* ***signed permutation cycle*** $(a_1, \ldots, a_l)^\epsilon$*, with* $\epsilon = \pm 1$ *and* $a_i \in \{\pm 1, \ldots, \pm n\}$*, is a permutation where* $|a_1|, \ldots, |a_l|$ *are pairwise distinct and for* $\epsilon = +1$ *we define*

$$(a_1, \ldots, a_l)^+ := (a_1, \ldots, a_l)(-a_1, \ldots, -a_l).$$

For $\epsilon = -1$ *we define*

$$(a_1, \ldots, a_l)^- := (a_1, \ldots, a_l, -a_1, \ldots, -a_l).$$

We can already observe that $a_i \mapsto a_j$ implies that $-a_i \mapsto -a_j$. Remembering the signification of cycles for permutations in the symmetric group (every permutation can be written as a product of permutation cycles), we define signed permutations in a similar way.

Definition 30 (Signed Permutation)**.** *A* ***signed permutation*** *on* $\{\pm 1, \ldots, \pm n\}$ *is a product of signed permutation cycles on* $\{\pm 1, \ldots, \pm n\}$*, as defined in Definition 29.*

Now we prove the observation that we already made looking at the permutation cycles. We state that the negation of a number a is mapped to the negation of a^π for any number $a \in \{\pm 1, \ldots, \pm n\}$ and signed permutation π.

Lemma 31. *Let* $\pi = (a_1, \ldots, a_l)^\epsilon$ *be a signed permutation cycle with* $\epsilon = \pm 1$ *and* $a_i \in \{\pm 1, \ldots, \pm n\}$*, we have* $a^\pi = -(-a)^\pi$ *for every* $a \in \{\pm 1, \ldots, \pm n\}$*.*

Proof. Let $a \in \{\pm 1, \dots, \pm n\}$. If $a \neq a_i$ and $a \neq -a_i$ for all $i \in \{1, \dots, l\}$, then $a^\pi = a = -(-a)^\pi$.
Now let $a = a_i$ for some $i \in \{1, \dots, l\}$ and $\epsilon = +1$. Then with Definition 29 it follows that

$$a^\pi = a_i^\pi = a_i^{(a_1,\dots,a_l)(-a_1,\dots,-a_l)} = a_{i+1}$$
$$= -(-a_{i+1}) = -(-a_i)^{(a_1,\dots,a_l)(-a_1,\dots,-a_l)} = -(-a_i)^\pi = -(-a)^\pi,$$

where $a_{i+1} = -a_1$ if $i = l$. Now let $\epsilon = -1$. Then it follows again with Definition 29 that

$$a^\pi = a_i^\pi = a_i^{(a_1,\dots,a_l,-a_1,\dots,-a_l)} = a_{i+1}$$
$$= -(-a_{i+1}) = -(-a_i)^{(a_1,\dots,a_l,-a_1,\dots,-a_l)} = -(-a_i)^\pi = -(-a)^\pi,$$

where $a_{i+1} = -a_1$ if $i = l$. If $a = -a_i$ for an $i \in \{1, \dots, l\}$, then we can rename $\tilde{a_i} := -a_i$ and $a = \tilde{a_i}$ for an $i \in \{1, \dots, l\}$. The permutation $\tilde{\pi} = (\tilde{a_1}, \dots, \tilde{a_l})^\epsilon$ is equal to π, thus the claim follows. □

Now we define the hyperoctahedral group as the group of all permutations that fulfil the requirement that $a^\pi = -(-a)^\pi$ for $a \in \{\pm 1, \dots, \pm n\}$ and π is a permutation on the set. Note that we have shown in the previous lemma that the signed permutation cycles satisfy this requirement.

Definition 32 (Hyperoctahedral Group)**.** *The* ***hyperoctahedral group*** H_n *is the group of permutations* π *of the set* $\{\pm 1, \dots, \pm n\}$ *with* $a^\pi = -(-a)^\pi$.

Since the signed permutation cycles lie in the hyperoctahedral group, we can deduce that the signed permutations (that are products of signed permutation cycles) also lie in the group. We prove that the hyperoctahedral group is exactly the group of all signed permutations.

Theorem 33. *The hyperoctahedral group* H_n *is the group of all signed permutations on* $\{\pm 1, \dots, \pm n\}$.

Proof. We fix $n \in \mathbb{N}$ and define G as the group of all signed permutations on $\{\pm 1, \dots, \pm n\}$. For any $\pi \in G$ that consists of only one distinct non-trivial cycle it follows with Lemma 31 that $\pi \in \mathrm{H}_n$. For a product $\pi_1\pi_2 \in G$ of signed permutation cycles and $a \in \{\pm 1, \dots, \pm n\}$ we have

$$a^{\pi_1\pi_2} = (a^{\pi_1})^{\pi_2} = (-(-a)^{\pi_1})^{\pi_2} = -((-a)^{\pi_1})^{\pi_2} = -(-a)^{\pi_1\pi_2}$$

for any $a \in \{\pm 1, \dots, \pm n\}$ and thus every element of G lies in H_n.
Now let $\pi \in \mathrm{H}_n$. Then we have $\pi(a) = -\pi(-a)$ for every $a \in \{\pm 1, \dots, \pm n\}$ by Definition 32.

- If $a^\pi = a$ for all $a \in \{\pm 1, \dots, \pm n\}$, then $\pi = \mathrm{id}$ and thus $\pi \in G$.

- If it is $a^\pi = b$ for an $a \in \{\pm 1, \dots, \pm n\}$ and $a \neq b \in \{\pm 1, \dots, \pm n\}$, then it is also $(-a)^\pi = -a^\pi = -b$.
  We define $M := (a, a^\pi, \dots, a^{\pi^{l-1}})$, where l is the smallest natural number with $a^{\pi^l} = a$. We know that there exists a $\pi_1 \in \mathrm{H}_n$ such that M and π_1 are disjoint cycles and $\pi = M\pi_1$.

  Assuming that $-b \in M$, it follows directly that $-a \in M$ and that there exists a $k \in \mathbb{N}$ with $k < l$ and $a^{\pi^k} = -a$. Thus M is a signed permutation and can be written as
  $$M = (a, a^\pi, \dots, a^{\pi^{k-1}}, -a, (-a)^\pi, \dots, (-a)^{\pi^{k-1}}).$$

  Now we assume that $-b \notin M$. Since $-a \notin M$, it holds that $(-a)^{\pi^l} = -a^{\pi^l} = -a$ and we define
  $$\tilde{M} := (-a, (-a)^\pi, \dots, (-a)^{\pi^{l-1}}).$$

  The permutations M and $\tilde{M}$ are distinct and there exists a $\pi_2 \in \mathrm{H}_n$, which is also distinct to M and $\tilde{M}$, with $\pi = M\pi_1 = M\tilde{M}\pi_2$. Note that $M\tilde{M}$ is a signed permutation.

For π_1 resp. π_2 it follows recursively that they are a product of signed permutations, thus π is a also a signed permutation and $\pi \in G$. It follows that $\mathrm{H}_n = G$. □

Now that we have specified the hyperoctahedral group, we look at a subgroup and an isomorphic group.

4.2. Group SH_n

Before we define the group of signed permutation matrices of determinant 1, we look at a group which is isomorphic to the hyperoctahedral group. This is the group of all signed permutation matrices. A signed permutation matrix is related to a permutation matrix, but there might exist entries unequal to 0 and 1.

Definition 34 (Signed Permutation Matrix)**.** *A* ***signed permutation matrix*** $M \in \mathbb{R}^{n\times n}$ *of degree* n *is a monomial matrix where the non-zero entries are* ± 1*. We denote the set of signed permutation matrices of degree* n H_n^M*.*

We define a map from signed permutations to signed permutation matrices. Later we show that this map is an isomorphism.

Definition 35. *Let* $\pi \in \mathrm{H}_n$ *be a signed permutation on* $\{\pm 1, \dots, \pm n\}$*. Then we define* $\varphi(\pi) = M_\pi \in \mathbb{R}^{n\times n}$ *as the correlating signed permutation matrix, explicitely*

$$\varphi : \mathrm{H}_n \to \mathrm{H}_n^M, \pi \mapsto M_\pi \text{ with } (M_\pi)_{i,j} := \begin{cases} +1, & \text{if } i^\pi = j \\ -1, & \text{if } i^\pi = -j \\ 0, & \text{otherwise.} \end{cases}$$

Example. Let $(1,2)^-(4)^- =: \pi \in H_4$. Then we obtain with Definition 35 that

$$\varphi(\pi) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Note that this matrix has determinant $\det(M_\pi) = -1$.

We show that the map φ is an isomorphism and deduce that the group of signed permutations and the group of signed permutation matrices are isomorphic.

Lemma 36. *The group of signed permutation matrices H_n^M is isomorphic to the hyperoctahedral group H_n.*

Proof. See [Fra66]. We use the function $\varphi : \mathrm{H}_n \to \mathrm{H}_n^M$ defined in Definition 35. The map φ is injective, because if we have $\pi, \tilde{\pi} \in \mathrm{H}_n$ with $\varphi(\pi) = \varphi(\tilde{\pi})$, then $\pi = \tilde{\pi}$ follows directly from Definition 35.

Let $\{e_1, \ldots, e_n\}$ be the set of standard basis vectors of $\mathbb{R}^n$, $M \in M_n$ a signed permutation matrix of degree n and $\mathrm{sgn} : \mathbb{Z} \to \{\pm 1\}, \pm|n| \mapsto \pm 1$ the signum function. Then we define $\pi_M : \{\pm 1, \ldots, \pm n\} \to \{\pm 1, \ldots, \pm n\}, i \mapsto j$ such that $\mathrm{sgn}(i)Me_{|i|} = \mathrm{sgn}(j)e_{|j|}$. The function π_M is a well-defined permutation because of the properties of the signed permutation matrix M in Definition 34 (namely that there is exactly one non-zero entry in every column and line). Since $-(\mathrm{sgn}(i)Me_{|i|}) = \mathrm{sgn}(-i)Me_{|-i|}$, we have $(-i)^{\pi_M} = -j = -i^{\pi_M}$ and π_M is also well-defined as a signed permutation.

Thus φ is an isomorphism and the lemma follows. □

The next theorem inspires our proof of the correctness of the presentation given in Section 4.3.

Theorem 37. *The hyperoctahedral group H_n is isomorphic to the wreath product $C_2 \wr S_n \cong (C_2)^n \rtimes S_n$.*

Proof. See Definition 4 and Definition 6 for the definition of wreath products and semidirect products and [Ker71], page 39, and [Fra66] for the proof. □

We finally give a definition of the group of signed permutation matrices of determinant 1. In the next section we look at a presentation of this group.

Definition 38 (Group of Signed Permutation Matrices of Determinant 1)**.** *Let $n \in \mathbb{N}$ and H_n^M be the group of all signed permutation matrices. Then we define*

$$\mathrm{SH}_n := \{M \in H_n^M \mid \det(M) = 1\} \leq H_n^M$$

and call it the group of signed permutation matrices of determinant 1.

Lemma 39. *The group SH_n is isomorphic to a subgroup of the hyperoctahedral group H_n.*

Proof. Since the groups H_n and H_n^M are isomorphic, this follows directly. □

Before stating a presentation of the group SH_n and proving its correctness, we need to find a generating set to build a presentation on. A generating set is presented in the next theorem - note the similarity to one of the generating sets of the symmetric group (see Theorem 24).

Theorem 40. *The group SH_n is generated by $\varphi(u)$ and $\varphi(v)$, where $u := (1,2)^-$, $v := (1,\dots,n)^\epsilon$, $\epsilon := (-1)^{n+1}$ and φ as in Definition 35.*

Proof. We have

$$\varphi(u) = \begin{pmatrix} 0 & -1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

with $\det(\varphi(u)) = 1$ and thus $\varphi(u) \in \mathrm{SH}_n$. Also

$$\varphi(v) = \begin{pmatrix} 0 & 0 & 0 & \dots & \epsilon 1 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

with $\det(\varphi(v)) = 1$ for $\epsilon = (-1)^{n+1}$. Thus $\varphi(v) \in \mathrm{SH}_n$ and $\langle \varphi(u), \varphi(v) \rangle \subseteq \mathrm{SH}_n$.

Now let $M \in \mathrm{SH}_n$, then we know that M is a signed permutation matrix. There exists a matrix $N \in \langle \varphi(u), \varphi(v) \rangle$ such that the non-zero entries of M and N are similar. Thus there exists a diagonal matrix D with entries ± 1 such that $M = DN$. We have $\det(M) = \det(D)\det(N) \Leftrightarrow \det(D) = 1$.

Consequently the matrix D has an even number of negative entries, say I is the maximal set such that $D_{i,i} = -1$ for $i \in I$. Then $|I|$ is even. We obtain

$$\varphi(u)^2 = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } (\varphi(u)^2)^{\varphi(v)} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Via a proof of induction it follows that

$$((\varphi(u)^2)^{\varphi(v)^j})_{i,i} = \begin{cases} -1, & j = i+1 \text{ or } j = i+2 \\ 1, & \text{otherwise} \end{cases}$$

for $j < n-1$ and $i \in \{1,\dots,n\}$. Multiplying those matrices we can obtain any diagonal matrix with diagonal entries ± 1 and an even number of negative entries and thus we obtain the matrix D as a product of the matrices $\{(\varphi(u)^2)^{\varphi(v)^j} \mid 0 \le j < n-1\}$. As a result it follows that $DN = M \in \langle \varphi(u), \varphi(v) \rangle$ and $\mathrm{SH}_n \subseteq \langle \varphi(u), \varphi(v) \rangle$. □

4.3. Presentation of SH_n

In this section we provide a presentation of the group of signed permutation matrices of determinant 1 on the generators defined in Theorem 40.

To make this section more readable, we set some notation in the next remark that is used until the end of this chapter.

Remark 41. *Let $n \in \mathbb{N}$ and the dimension of the matrices is $n \times n$. Further $\epsilon := (-1)^{n+1}$, $u := (1,2)^-$ and $v := (1,\dots,n)^\epsilon$. Then we define*

$$M_u := \varphi(u) \quad \text{and} \quad M_v := \varphi(v),$$

where $M_u, M_v \in \mathrm{SH}_n$. We know from Theorem 40 that $\langle M_u, M_v\rangle = \mathrm{SH}_n$.

We show the correctness of the following presentations of the group of signed permutation matrices of determinant 1.

Remark 42. *The group SH_n has the presentation*

$$\begin{aligned}\{X' \mid R'_{odd}\} := \{\, U', V' \mid {} & U'^4 = U'^{2V'U'}U'^2U'^{2V'} = V'^n = (U'V')^{n-1} = (U'U'^{V'})^3 \\ & = [U', U'^{V'^j}] = 1 \ \text{ for } 2 < j < (n+1)/2\}\end{aligned}$$

for an odd $n \in \mathbb{N}$ and

$$\begin{aligned}\{X' \mid R'_{even}\} := \{\, U', V' \mid {} & U'^4 = U'^{2V'U'}U'^2U'^{2V'} = (U'U'^{V'})^3 = [V'^n, U'] = V'^{2n} = 1, \\ & V'^n = (U'V')^{n-1}, [U', U'^{V'^j}] = 1 \ \text{ for } 2 < j < (n+1)/2\}\end{aligned}$$

if n is even. We write $\{X' \mid R'\}$ if we want R to change according as n is odd or even.

The proof of the correctness of those presentations resembles the proof in Chapter 3 since we use Proposition 18 to show the existence of an epimorphism from the presented group $\langle X' \mid R'\rangle$ in the group SH_n.

Lemma 43. *There exists an epimorphism $\psi : G' = \langle X' \mid R'\rangle \to \mathrm{SH}_n$ with $\psi(U') = M_u$ and $\psi(V') = M_v$.*

Proof. We have

$$\begin{aligned}u^4 &= (1,2,-1,-2)^4 = \mathrm{id}, \\ u^{2vu}u^2u^{2v} &= ((1)^-(2)^-)^{(1,\dots,n)^\epsilon(1,2)^-}(1)^-(2)^-((1)^-(2)^-)^{(1,\dots,n)^\epsilon} \\ &= ((2)^-(3)^-)^{(1,2)^-}(1)^-(2)^-(2)^-(3)^- = (1)^-(3)^-(1)^-(3)^- = \mathrm{id}, \\ (uu^v)^3 &= ((1,2)^-((1,2)^-)^{(1,\dots,n)^\epsilon})^3 = ((1,2)^-(2,3)^-)^3 \\ &= ((1,3,-2)(-1,-3,2))^3 = \mathrm{id} \ \text{ and} \\ [u, u^{v^j}] &= [(1,2)^-, (j+1, j+2)^-] \\ &= ((1,2)^-)^{-1}((j+1,j+2)^-)^{-1}(1,2)^-(j+1,j+2)^- \\ &= \mathrm{id} \ \text{ for } 2 < j < (n+1/2).\end{aligned}$$

For an odd $n \in \mathbb{N}$ we have

$$\begin{aligned} v^n &= ((1,\dots,n)^+)^n = \mathrm{id}, \\ (uv)^{n-1} &= ((1,3,4,\dots,n)^+)^{n-1} = \mathrm{id} \end{aligned}$$

and for an even $n \in \mathbb{N}$ we have

$$\begin{aligned} [v^n, u] &= [((1,\dots,n)^-)^n, (1,2)^-] = [(1)^- \cdots (n)^-, (1,2)^-] \\ &= (1)^- \cdots (n)^- (2,1)^- (1)^- \cdots (n)^- (1,2)^- = \mathrm{id}, \\ v^{2n} &= ((1)^- \cdots (n)^-)^2 = \mathrm{id} \text{ and} \\ (uv)^{n-1} &= ((1,3,\dots,n)^- (2)^-)^{n-1} = (1)^- \cdots (n)^- = v^n. \end{aligned}$$

Thus the relations also hold for the matrices M_u and M_v, the requirements for Proposition 18 are fulfilled and ψ is an epimorphism. □

We use Theorem 7 to prove the isomorphism between the generated group $\langle X' \mid R' \rangle$ and the group SH_n. Thus we need to prove all the prerequisites first. We start by providing a normal subgroup of SH_n.

Lemma 44. *The set* $A := \langle \{a_i := \varphi((u^2)^{v^{i-1}}) \mid 1 \le i \le n\} \rangle$ *is a normal subgroup of* SH_n.

Proof. We have $a_i = \varphi((i)^-(i+1)^-)$,

$$\varphi^{-1}(a_i)^v = ((i)^-(i+1)^-)^{(1,\dots,n)^\epsilon} = (i+1)^-(i+2)^- = \varphi^{-1}(a_{i+1})$$

for $i < n$ and

$$\varphi^{-1}(a_n)^v = (\epsilon 1)^-(\epsilon 2)^- = (1)^-(2)^- = \varphi^{-1}(a_1).$$

Thus $a_i^{M_v} \in A$ for every $i \in \{1,\dots,n-1\}$.
For $i > 2$ it is $a_i^{M_u} = a_i$. If $i = 2$, then we have

$$\varphi^{-1}(a_i)^u = ((2)^-(3)^-)^{(1,2)^-} = (1)^-(3)^- = \varphi^{-1}(a_1 a_2).$$

And for $i = 1$ we obtain $\varphi^{-1}(a_i)^u = ((1)^-(2)^-)^{(1,2)^-} = (1)^-(2)^- = \varphi^{-1}(a_1)$. So $a_i^{M_u} \in A$ for every $i \in \{1,\dots,n-1\}$. Since M_u and M_v generate SH_n, it follows that $a^M \in A$ for every $a \in A$ and $M \in \mathrm{SH}_n$ and A is a normal subgroup of SH_n. □

We have shown that there exists a normal subgroup $A \trianglelefteq \mathrm{SH}_n$. The next lemma states that $\mathrm{SH}_n / A \cong \mathrm{S}_n$. In the succeeding lemmata we show that there exists a normal subgroup $A' \trianglelefteq \langle X' \mid R' \rangle$ such that $\langle X' \mid R' \rangle / A' \cong \mathrm{S}_n$.

Lemma 45. *Let* A *be as in Lemma 44 and* SH_n *the group of signed permutation matrices of determinant* 1 *and degree* n. *Then* SH_n / A *is isomorphic to the symmetric group* S_n.

Proof. We use the same notation as in Theorem 28. Let $\phi : X \to \mathrm{SH}_n/A$ be a map with $U^\phi = M_u A$ and $V^\phi = M_v A$. Then according to Proposition 18 there exists an epimorphism $\phi'' : S_n \cong F_X/\langle R\rangle_{F_X} \to \mathrm{SH}_n/A$ if $r_i(U^\phi, V^\phi) \in A$ holds for every relation $r_i(U,V) \in R$.

- $r_1(U,V) := U^2$. Then
$$r_1(U^\phi, V^\phi) = (\varphi(u)A)^2 = \varphi(u)^2 A = \varphi((1)^-(2)^-)A = A.$$
- $r_2(U,V) := V^n$. If n is even, it follows that
$$r_2(U^\phi, V^\phi) = (\varphi(v)A)^n = \varphi(v)^n A = \varphi((1)^- \cdots (n)^-)A = A.$$
And if n is odd, we obtain
$$r_2(U^\phi, V^\phi) = (\varphi(v)A)^n = \varphi(v)^n A = \mathrm{id}_{\mathrm{SH}_n} A.$$
- $r_3(U,V) := (UV)^{n-1}$. Then
$$r_3(U^{\varphi''}, V^{\varphi''}) = (\varphi(u)A\varphi(v)A)^{n-1} = (\varphi(uv))^{n-1}A = \varphi(((1,3,\ldots,n)^\epsilon)^{n-1})A,$$
which is equal to $\varphi((1)^- \cdots (n)^-)A = A$ for even n and $\mathrm{id}_{\mathrm{SH}_n} A$ for odd n.
- $r_4(U,V) := (UU^V)^3$. Then we obtain
$$\begin{aligned} r_4(U^{\varphi''}, V^{\varphi''}) &= (\varphi(u)A(\varphi(u)A)^{\varphi(v)A})^3 = \varphi((uu^v)^3)A \\ &= \varphi(((1,2)^-(2,3)^-)^3)A = \varphi(((1,3,-2)^+)^3)A = A. \end{aligned}$$
- $r_5(U,V) := (UU^{V^j})^2$ for $2 \le j \le n/2$. Then we have
$$\begin{aligned} r_5(U^{\varphi''}, V^{\varphi''}) &= (\varphi(u)A(\varphi(u)A)^{(\varphi(v)A)^j})^2 = \varphi((uu^{v^j})^2)A \\ &= \varphi(((1,2)^-(j,j+1)^-)^2)A = \varphi((1)^-(2)^-(j)^-(j+1)^-)A = A, \end{aligned}$$
and either $j = 2$ and thus $\varphi((1)^-(j+1)^-) \in A$ or $j \neq 2$ and $\varphi(((1)^-(2)^-)((j)^-(j+1)^-)) \in A$.

Thus there exists an epimorphism $\phi'' : S_n \to \mathrm{SH}_n/A$.
Now let $\varphi(\pi)A \in \mathrm{SH}_n/A$ be an equivalence class. Then we know that $\varphi(\pi)A = \{\varphi(\pi)a \mid a \in A\}$. Let $\varphi(\tilde{\pi}) \in \mathrm{H}_n$ be a matrix where all entries are 1 or 0 with $|i^\pi| = |i^{\tilde{\pi}}|$. If $\det(\varphi(\pi)) = 1$, then $\varphi(\pi)A = \{\varphi(\tilde{\pi})a \mid a \in A\}$. And if $\det(\varphi(\pi)) = -1$, then $\varphi(\pi)A = \{\varphi((1)^-\tilde{\pi})a \mid a \in A\}$. Using Lemma 24 we know that there exists an element $\sigma \in \varphi(\pi)A$ that is generated by $\varphi(u)$ and $\varphi(v)$ for every $\varphi(\pi)A \in \mathrm{SH}_n/A$ and if follows that ϕ'' is also injective and thus an isomorphism. □

Similarly to $A \trianglelefteq \mathrm{SH}_n$ we need a subgroup $A' \trianglelefteq \langle X' \mid R'\rangle$ to fulfil the prerequisites of Theorem 7.

Lemma 46. *The set* $A' := \langle \{a'_i := (U'^2)^{V'^{i-1}} \mid 1 \leq i < n\} \rangle$ *is a normal subgroup of the group* $G' := F_{X'}/N'$*, where* X' *and* R' *are defined as in the presentation*

$$\{X' \mid R'\} := \{\, U', V' \mid U'^4 = U'^{2V'U'}U'^2U'^{2V'} = V'^n = (U'V')^{n-1} = (U'U'^{V'})^3 \\ = [U', U'^{V'^j}] = 1 \ \text{ for } 2 < j < (n+1)/2\}.$$

and $N' = \langle R' \rangle_{F_{X'}}$ *is the normal closure of* R' *in* $F_{X'}$*.*

Proof. For $i \in \{1, \ldots, n-1\}$ we have $a_i'^{V'} = a'_{i+1}$. For $i = n$ we obtain $a_n'^{V'} = ((U'^2)^{V'^{n-1}})^{V'} = (U'^2)^{V'^n} = U'^2 = a'_1$, because $V'^n = \mathrm{id}$ is a relation in R'. Thus $a_i'^{V'} \in A'$ for every $i \in \{1, \ldots, n-1\}$.
Furthermore we have $a_1'^{U'} = a'_1 \in A'$. Since there exists the relator $U'^{2V'U'}U'^2U'^{2V'} \in R'$, we obtain

$$a_2'^{U'}a'_1a'_2 = \mathrm{id} \Leftrightarrow a_2'^{U'} = a_2'^{-1}a_1'^{-1} = a'_2a'_1 \in A'.$$

For $2 < i < n$ we have

$$\begin{aligned} a_i'^{U'} &= U'^{-1}(U'^2)^{V'^{i-1}}U' = U'^{-1}(U'^{V'^{i-1}})^2U' \\ &= U'^{-1}U'^{V'^{i-1}}U'U'^{V'^{i-1}} = U'^{-1}U'(U'^{V'^{i-1}})^2 = a'_i, \end{aligned}$$

because of the relator $[U', U'^{V'^j}] \in R'$. Thus A' is a normal subgroup. □

Now that we have a normal subgroup $A' \trianglelefteq \langle X' \mid R \rangle$, we show that the quotient group $\langle X' \mid R' \rangle / A'$ is isomorphic to the symmetric group S_n. We can thus derive that $\langle X' \mid R' \rangle / A' \cong \mathrm{SH}_n / A$.

Lemma 47. *Let* A' *be as in Lemma 46 and* $G = \langle X' | R' \rangle$ *the group that is defined by the presentation in Remark 41. Then* G/A' *is isomorphic to the symmetric group* S_n*.*

Proof. We define $\varphi : X \to G/A'$ with $\varphi(U) = A'U'$ and $\varphi(V) = A'V'$, where X is the set in Theorem 28. Since we have

$$\begin{aligned} (A'U')^2 &= A', \\ (A'V')^n &= A'V'^n = A', \\ (A'U'A'V')^{n-1} &= A'(U'V')^{n-1} = A', \\ (A'U'(A'U')^{A'V'})^3 &= A'(U'U'^{V'})^3 = A' \text{ and} \\ (A'U'(A'U')^{(A'V')^j})^2 &= A'(U'U'^{V'^j})^2 = A'U'^{-1}(U'^{V'^j})^{-1}U'U'^{V'^j} \\ &= A'[U', U'^{V'^j}] = A' \text{ for } 2 < j < (d+1)/2, \end{aligned}$$

we obtain that there exists an subjective homomorphic extension $\varphi'' : S_n \to G/A'$ by Proposition 18. Furthermore we obtain $U^2 = \mathrm{id}$ and thus

$$(A'U'^4)^{\varphi^{-1}} = (A'U'^{2V'U'}U'^2U'^{2V'})^{\varphi} = \mathrm{id}\,.$$

Also
$$(A'V'^n)^{\varphi^{-1}} = (A'(U'V')^{n-1})^{\varphi^{-1}} = (A'(U'U'^{V'})^3)^{\varphi^{-1}} = \mathrm{id}$$
and
$$(A'[U', U'^{V'^j}])^{\varphi^{-1}} = U^{-1}(U^{V^j})^{-1}UU^{V^j} = (UU^{V^j})^2 = \mathrm{id}\,.$$
For even $n \in \mathbb{N}$ it follows that $(A'[V'^n, U'])^{\varphi^{-1}} = V^{-n}U^{-1}V^nU = U^{-1}U = \mathrm{id}$ and $(A'V'^{2n})^{\varphi^{-1}} = \mathrm{id}$.
Using Proposition 18 we obtain φ^{-1} is a well-defined homomorphism and φ is an isomorphism. □

Proposition 48. *Define A as in Lemma 44 and A' as in Lemma 46. Then $A \cong A'$.*

Proof. We remember that $A := \langle \{a_i := \varphi((u^2)^{v^{i-1}}) \mid 1 \le i \le n\}\rangle$ and $A' := \langle \{a'_i := (U'^2)^{V'^{i-1}} \mid 1 \le i \le n\}\rangle$ and define
$$\psi : A \to A', a_i \mapsto a'_i.$$
We know that $a_i^2 = \varphi((u^2)^{v^{i-1}})^2 = \varphi((u^4)^{v^{i-1}}) = \varphi(\mathrm{id}^{v^{i-1}}) = \mathrm{id}$ and $(a'_i)^2 = ((U'^2)^{V'^{i-1}})^2 = (U'^4)^{V'^{i-1}} = \mathrm{id}$ using the relations of the presentation in Remark 41. Also a_i and a_j commute for $1 \le i, j \le n$, because both are diagonal matrices (see proof of Theorem 40). Using the relation $U'^{2V'U'}U'^2U'^{2V'} = 1$ in G', we follow that $a_2'^{U'}a'_1a'_2 = 1 \Leftrightarrow a_2'^{U'} = a'_2a'_1$. Now $(a_2'^{U'})^2 = 1$ implies that $(a'_2a'_1)^2 = 1 \Leftrightarrow a'_2a'_1a'_2a'_1 = 1 \Leftrightarrow a_2'^{-1}a_1'^{-1}a'_2a'_1 = 1$ and thus a'_1 and a'_2 commute. From the relation $[U', U'^{V'^j}] = 1$ for $3 \le j \le n-1$ we can conclude that a'_1 and a'_j commute and thus a'_i and a'_j commute for all $1 \le i, j \le n$.

Consequently the map ψ is a well-defined isomorphism and the result follows. □

We have shown all the prerequisites of Theorem 7 and we combine this to prove the correctness of the presentation $\{X' \mid R'\}$ for the group of signed permutation matrices of determinant 1.

Theorem 49. *There exists an isomorphism $G' \cong \mathrm{SH}_n$ between the group G' of the presentation in Remark 42 and the group SH_n.*

Proof. We show the isomorphism by using Theorem 7. According to Lemma 43 there exists an epimorphism $\psi : G' = \langle X' \mid R'\rangle \to \mathrm{SH}_n$. As shown in Lemma 44 and Lemma 46, there exist normal subgroups $A \trianglelefteq \mathrm{SH}_n$ and $A' \trianglelefteq G'$ such that $A \cong A'$ (which is proven in Proposition 48). Furthermore we have $G'/A' \cong S_n \cong \mathrm{SH}_n/A$ with Lemma 45 and Lemma 47. Thus all the requirements for Theorem 7 are fulfilled and the correctness of the presentation in Remark 42 is proven. □

5. Special Linear Group $\mathrm{SL}(2, q)$

This chapter gives presentations of the special linear group $\mathrm{SL}(2, q)$ of degree 2 depending on q. It is divided into two sections. In the first one I define the special linear group and present generators of $\mathrm{SL}(2, q)$. In the second section I list various presentations for $\mathrm{SL}(2, q)$ and $\mathrm{PSL}(2, q)$.

Throughout this chapter we use the presentations of $\mathrm{SL}(2, q)$ and $\mathrm{PSL}(2, q)$ as given in [CR80] and [CRW90] and modify them to obtain presentations on the standard generators defined in [LGOB09], page 841. The generating set and presentations by Campbell, Robertson and Williams can be found in Appendix A.

5.1. Definition and Generators

We start with definitions of the groups and give a generating set for the special linear group of degree 2.

Definition 50 (Special Linear Group, [Hup67], page 177)**.** *The* ***special linear group over the field*** K ***of degree*** **n** *is defined as*

$$\mathrm{SL}(n, \mathrm{K}) := \{M \in \mathrm{GL}(n, \mathrm{K}) \mid \det(M) = 1\} \leq \mathrm{GL}(n, \mathrm{K}).$$

We study the special linear group of degree 2 over some finite field. Hence we have $\mathrm{K} = \mathrm{GF}(q)$ for some $q = p^e$, p a prime and $1 < e \in \mathbb{N}$, or $\mathrm{K} = \mathrm{GF}(p)$, if K is a field of prime order. We can thus change the notation and write $\mathrm{SL}(2, q)$ instead of $\mathrm{SL}(2, \mathrm{GF}(q))$, since this is shorter.

Definition 51 (Projective Special Linear Group, [Hup67], page 177)**.** *The* ***projective special linear group*** *is defined as*

$$\mathrm{PSL}(2, q) := \mathrm{SL}(2, q)/\mathrm{Z}(\mathrm{SL}(2, q)),$$

where

$$\mathrm{Z}(\mathrm{SL}(2, q)) = \{aI_2 \mid \det(aI_2) = a^2 = 1\}.$$

Now that the groups are defined, we take a look at single elements of the special linear group $\mathrm{SL}(2, q)$. We want to find a generating set of this group.

Lemma 52. *Let $q = p^e$ for a prime p, $\omega \in \mathrm{GF}(q)$ is a primitive element and*

$$\tau := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \delta := \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}$$

are two matrices in $\mathrm{GF}(q)^{2\times 2}$*. Then the matrix*

$$\tau_1 := \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$$

is a product of τ *and* δ*.*

Proof. We first show that there exist $a_0, \ldots, a_{e-1} \in \mathrm{GF}(p)$ such that $\omega = \sum_{i=0}^{e-1} a_i \omega^{2i}$. We define the abelian group $V := \langle w^{2i} \mid 1 \leq i \leq (q-1)/2 \rangle$ and thus V is a $\mathrm{GF}(p)$-vector space. The $\mathrm{GF}(p)$-vector space V is an abelian group regarding addition, which follows from the definition of a vector space (see [Beu94], page 59). Also the multiplication is associative, commutative and a neutral element (the neutral element of V) exists. Thus the $\mathrm{GF}(p)$-vector space V is a ring and we have $V \subseteq \mathrm{GF}(q)$. Now we define K as the field closure of V, which is a subfield of $\mathrm{GF}(q)$.

The order of ω is q, thus it holds for the group V that $|V| \geq (q-1)/2 + 1$. It follows that $|\mathrm{K}| > q/2$. We also know that $|\mathrm{K}| \mid q$ and it follows that $|\mathrm{K}| = q$ and $\mathrm{K} = \mathrm{GF}(p)(\omega^2) = \mathrm{GF}(q)$.

The elements $1, \omega^2, \ldots, \omega^{2e}$ are not linearly independent. Thus a linear combination

$$\omega = \sum_{i=0}^{e-1} a_i \omega^{2i} \tag{5.1}$$

exists, where $a_i \in \mathrm{GF}(p)$ for all i.

Since p is a prime, we have $\mathbb{Z}/p\mathbb{Z} \cong \mathrm{GF}(p)$ and define $\tilde{j} \in \mathbb{N}$ as the smallest positive integer in the natural representation of $\mathrm{GF}(p)$ in $\mathbb{N}$.

It is $\delta^{-1}\tau\delta = \begin{pmatrix} 1 & \omega^2 \\ 0 & 1 \end{pmatrix}$ and $(\delta^{-i}\tau\delta^{i})^{\tilde{j}} = \begin{pmatrix} 1 & j\omega^{2i} \\ 0 & 1 \end{pmatrix}$ for elements $i \in \mathbb{N}$, $j \in \mathrm{GF}(p)$ and $\tilde{j}$ the corresponding element in $\mathbb{N}$ to j.

We set $\tau_1 := \prod_{i=0}^{e-1} \begin{pmatrix} 1 & a_i\omega^{2i} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$ using the linear combination defined in Equation 5.1. □

As you can see later, this last lemma helps us to shorten the generating set given in Theorem 99 since we can drop the matrix y. The next theorem lists three matrices that form a generating set of $\mathrm{SL}(2,q)$.

Theorem 53 ([LGOB09], page 841)**.** *Let* $q = p^e$ *for a prime* p*,* $1 < e \in \mathbb{N}$ *and* $\omega \in \mathrm{GF}(q)$ *a primitive element. Then*

$$\tau := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ \delta := \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix} \text{ and } U := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generate the special linear group $\mathrm{SL}(2,q)$*.*

Proof. We have $\det(\tau) = \det(\delta) = \det(U) = 1$, thus the defined matrices are in $\mathrm{SL}(2,q)$ and $\langle \tau, \delta, U \rangle \subseteq \mathrm{SL}(2,q)$.

Now let $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,q)$. Then $\det(M) = ad - bc = 1$. We use the Gaussian elimination (see [Beu94], page 116) to write

$$M = \underbrace{\begin{pmatrix} 1 & -\frac{b}{d-\frac{bc}{a}} \\ 0 & 1 \end{pmatrix}}_{=:L_1} \underbrace{\begin{pmatrix} 1 & 0 \\ -\frac{c}{a} & 1 \end{pmatrix}}_{=:L_2} \underbrace{\begin{pmatrix} a & 0 \\ 0 & d-\frac{bc}{a} \end{pmatrix}}_{=:D}.$$

We can construct the matrix D as a power of δ, because we have $1 = ad - bc = a(d - \frac{bc}{a})$ and thus $a^{-1} = d - \frac{bc}{a}$. Furthermore $a \in \mathrm{GF}(q)$ and thus there exists a natural number k such that $\omega^k = a^{-1}$. It follows that $D = \delta^k$.

As proven in Lemma 52 we can construct the matrix

$$\tau_1 = \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$$

as a product of τ and δ. Let $\gamma := -\frac{b}{d-\frac{bc}{a}}$. Then there exists an element $l \in \mathbb{N}$ such that $\omega^l = \gamma$. If $l = 2m$ is even, then we have $\tau^{\delta^m} = L_1$, and if $l = 2m+1$ then $\tau_1^{\delta^m} = L_1$, where $m \in \mathbb{N}$.

Similarly for $\beta := \frac{c}{a}$ there exists a natural number $r \in \mathbb{N}$ such that $\omega^r = \beta$. Then we define $\tilde{L_2} := \tau^{\delta^n}$, if $r = 2n$, and $\tilde{L_2} := \tau_1^{\delta^n}$, if $r = 2n+1$, where $n \in \mathbb{N}$. It is $\tilde{L_2} := \begin{pmatrix} 1 & \frac{c}{a} \\ 0 & 1 \end{pmatrix}$. By conjugating with the matrix U we obtain

$$\tilde{L_2}^U = \begin{pmatrix} 1 & 0 \\ -\frac{c}{a} & 1 \end{pmatrix} = L_2.$$

Thus every matrix $M \in \mathrm{SL}(2,q)$ is a product of the matrices τ, δ and U and the claim follows. □

Those matrices are based on the standard generators of $\mathrm{SL}(n,q)$ as in [LGOB09], page 841, but instead of U^{-1} we use U. This is needed since the relations of the presentations in the next section are not fulfilled if we use U^{-1}.

5.2. Presentations

Now we look at the different presentations for different groups $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$, depending on q. Again we define some notation in order to make this section more readable. The notation in Remark 54 is implicitly assumed throughout the rest of this chapter.

Remark 54. *Let $q := p^e$, where p is an odd prime, $1 < e \in \mathbb{N}$ and $\omega \in \mathrm{GF}(q)$ a primitive element.*

- *Then we define the natural number $k \in \mathbb{N}$ as the smallest number such that $1+\omega = \omega^k$. We define $m := \lfloor k/2 \rfloor \in \mathbb{N}$ and the map $f : \mathrm{GF}(q) \to \mathrm{GF}(q), t \mapsto 1+t-t^k$.*
- *Also $g : \mathrm{GF}(q) \to \mathrm{GF}(q)$ is a map such that $g(\omega^2) = \omega$. The existence of this map is proven in Lemma 52 (more specifically $g(t) := \sum_{i=0}^{e-1} a_i t^i$ as defined in Equation 5.1). Furthermore we define $\mu_\omega : \mathrm{GF}(q) \to \mathrm{GF}(q)$ as the minimal polynomial of ω. The coefficients of all the defined polynomials are over $\mathrm{GF}(p)$.*
- *For a polynomial $h(t) = a_k t^k + \ldots + a_0$ over $\mathrm{GF}(p)$ and a matrix $\tau \in \mathrm{GF}(q)^{2\times 2}$, there are different ways to evaluate the equation $\tau^{h(t)}$.*

  If we have defined a matrix τ_1, then $\tau^{h(t)} := \prod_{i=0}^{k} \tau_i^{\tilde{a_i}}$, where $\tau_{2i} := \tau^{\delta^i}$, if i is even, and $\tau_{2i+1} = \tau_1^{\delta^i}$, if i is odd.

  If there exists no predefined matrix τ_1, then $\tau^{h(t)} := \prod_{i=0}^{k} (\tau^{\delta^i})^{\tilde{a_i}}$.

  Sometimes all matrices τ_i, $0 \le i \le k$ are already explicitely specified. Then $\tau^{h(t)} := \prod_{i=0}^{k} (\tau_i)^{\tilde{a_i}}$.
- *Note that $\tilde{a_i}$ is the smallest positive integer in the natural representation of $\mathrm{GF}(p)$ in $\mathbb{N}$.*

We assume that the presentation in Theorem 100 of [CRW90] for the group $\mathrm{PSL}(2,q)$ is correct. Note that the elements in Theorem 99 satisfy the relations of this presentation. Now we derive a presentation on the standard generators defined in Theorem 53 from this presentation.

Theorem 55 (Presentation of $\mathrm{PSL}(2,q)$, [LGOB19], Theorem 3.1)**.** *We assume the requirements listed in Remark 54. Then $\mathrm{PSL}(2,q)$ has the presentation*

$$\begin{aligned}\{\tau, \delta, U \mid \tau_1 := \tau^{g(t)} = \prod_{i=0}^{e-1} (\tau^{\delta^i})^{\tilde{a_k}};\ (\tau U)^3 = (U\delta)^2 = U^2 = (\tau_1 U\delta)^3 = \delta^{(q-1)/2} \\ = \tau^p = [\tau, \tau_1] = [\tau_1, \tau^\delta] = \tau^{\mu(t)} = 1, \\ \begin{cases} \tau^{\delta^m} = \tau\tau_1 \text{ and } \tau_1^{\delta^m} = \tau_1\tau^\delta, & \text{if } 1+\omega \in \mathrm{GF}(q)^2, \\ \tau_1^{\delta^m} = \tau\tau_1 \text{ and } \tau^{\delta^{m+1}} = \tau_1\tau^\delta, & \text{otherwise} \end{cases} \}.\end{aligned}$$

Proof. We prove that this presentation is just a rewritten version of the presentation in Theorem 100.

By simply replacing the generators in the theorem above with the generators $w = U\tau^{-1}$, $x = \tau$, $z = \tau\delta^{-1}$ and $y = \tau^{g(t)}$ for the polynomial $g(t)$ over $\mathrm{GF}(p)$ such that $g(\omega^2) = \omega$ holds, one obtains the relations

$$\begin{aligned} R := \{\ & (U\tau^{-1})^3 = U^2 = (U\delta^{-1})^2 = (U\tau^{-1}\tau_1\tau\delta^{-1})^3 = \tau^p = \tau_1^p = (\tau\delta^{-1})^{(q-1)/2} \\ & = [\tau, \tau_1] = [\tau_1, (\tau^\delta)^{\tau^{-1}}] = \tau^{\mu(t)} = \tau_1^{\mu(t)} = 1, \\ & \begin{cases} \tau\tau_1(\tau^{\delta^m})^{-1} = \tau_1\tau^\delta(\tau_1^{\delta^m})^{-1} = 1, & \text{if } 1+\omega \in \mathrm{GF}(q)^2 \\ \tau\tau_1(\tau_1^{\delta^m})^{-1} = \tau_1\tau^\delta(\tau^{\delta^{m+1}})^{-1} = 1, & \text{otherwise} \end{cases} \}. \end{aligned}$$

Using the relation $U^2 = 1$ we obtain that $(U\tau^{-1})^3 = 1 \Leftrightarrow (\tau U)^3 = 1$. Also $(U\delta^{-1})^2 = 1 \Leftrightarrow (U\delta)^2 = 1$ for the same reason and we have $U\delta = \delta^{-1}U$. Then it follows with $[\tau, \tau_1] = 1$ that

$$(U\tau^{-1}\tau_1\tau\delta^{-1})^3 = (U\tau_1\delta^{-1})^3 = 1 \Leftrightarrow (U\tau_1\delta^{-1})^3 U = U \Leftrightarrow U(\tau_1 U\delta)^3 = U \Leftrightarrow (\tau_1 U\delta)^3 = 1.$$

We have $\tau_1^p = (\tau^{g(t)})^p = (\prod_{i=0}^{e-1}(\tau^{\delta^i})^{\tilde{a}_i})^p = \prod_{i=0}^{e-1}((\tau^p)^{\delta^i})^{\tilde{a}_i} = 1$, if the relation $\tau^p = 1$ holds. Hence this relation is redundant. Now it follows with Lemma 8 that

$$(\tau\delta^{-1})^{(q-1)/2} = \left(\prod_{i=0}^{\frac{q-1}{2}-1} \tau^{\delta^i}\right)\delta^{-\frac{q-1}{2}} = \begin{pmatrix} 1 & \sum_{i=0}^{\frac{q-1}{2}-1}\omega^{2i} \\ 0 & 1 \end{pmatrix}\delta^{-\frac{q-1}{2}} = \delta^{-\frac{q-1}{2}}.$$

Thus we can replace the relation $(\tau\delta^{-1})^{\frac{q-1}{2}} = 1$ with $\delta^{\frac{q-1}{2}} = 1$.

The relation $[\tau_1, (\tau^\delta)^{\tau^{-1}}] = 1$ is equivalent to $[\tau_1, \tau^\delta] = 1$, because τ and τ_1 commute. We can omit the relation $\tau_1^{\mu(t)}$, because $\tau^{\mu(t)} = 1$, and it already follows that $\tau_1^{\mu(t)} = \tau^{g(t)\mu(t)} = (\tau^{\mu(t)})^{g(t)} = 1$. Thus this presentation is another presentation of the group $\mathrm{PSL}(2, q)$. □

We modify the presentation for $\mathrm{PSL}(2, q)$ to obtain a presentation for the group $\mathrm{SL}(2, q)$.

Theorem 56 (Presentation of $\mathrm{SL}(2, q)$, [LGOB19], Theorem 3.2)**.** *We assume the requirements that are established in Remark 54. Then a presentation for* $\mathrm{SL}(2, q)$ *is given by replacing the relations*

$$(\tau U)^3 = 1, \quad (U\delta)^2 = 1, \quad U^2 = 1 \text{ and } \delta^{\frac{q-1}{2}} = 1$$

by the relations

$$(\tau U)^3 = U^2, \quad (U\delta)^2 = U^2, \quad U^4 = 1 \text{ and } \delta^{\frac{q-1}{2}} = U^2$$

in the presentation in Theorem 55. Thus a presentation of $\mathrm{SL}(2, q)$ *is given by*

$$\begin{aligned}\{\tau, \delta, U \mid \tau_1 := \tau^{g(t)} = \prod_{i=0}^{e-1}(\tau^{\delta^i})^{\tilde{a_k}};\ & (\tau U)^3 = (U\delta)^2 = \delta^{(q-1)/2} = U^2, \\ & U^4 = (\tau_1 U\delta)^3 = \tau^p = [\tau, \tau_1] = [\tau_1, \tau^\delta] = \tau^{\mu(t)} = 1, \\ & \begin{cases} \tau^{\delta^m} = \tau\tau_1 \text{ and } \tau_1^{\delta^m} = \tau_1\tau^\delta, & \text{if } 1 + \omega \in \mathrm{GF}(q)^2, \\ \tau_1^{\delta^m} = \tau\tau_1 \text{ and } \tau^{\delta^{m+1}} = \tau_1\tau^\delta, & \text{otherwise} \end{cases}\}.\end{aligned}$$

This theorem is derived from [LGOB19], but the relation $(\tau U^{-1})^3 = U^2$ is replaced with $(\tau U)^3$. With this alternation we make sure that the generators of $\mathrm{SL}(2, q)$ of Theorem 53 fulfil the presentation.

Proof. The relations hold in SL$(2, q)$ and we prove first that $\langle U^2 \rangle$ is the centre of the presented group.

We have $(U^2)^U = \mathrm{id} \in \langle U^2 \rangle$. The relations $(U\delta)^2 = U^2$ and $U^4 = 1$ imply that

$$U^2\delta^{-1}U^2\delta = 1 \Leftrightarrow U^2\delta^{-1} = \delta^{-1}U^2 \Leftrightarrow (U\delta)^2\delta^{-1} = \delta^{-1}U^2$$
$$\Leftrightarrow \delta U\delta U = U^2 \Leftrightarrow U\delta U\delta U^4 = U^6 \Leftrightarrow (U\delta)^2 = U^2.$$

Thus U^2 and δ commute. Also $\tau \cdot U^2 = (\tau U^{-1})U^{-1} = (\tau U^{-1})U^2 \cdot U = (\tau U^{-1})^4 \cdot U = U^2\tau \cdot U^{-1} \cdot U = U^2\tau$, since $U^2 = U^{-2}$. Thus U^2 and τ also commute.

Since U^2 and δ commute, we have $(U\delta)^2 = U^2 \Leftrightarrow U\delta U = U^2\delta^{-1} \Leftrightarrow U^3\delta = \delta^{-1}U^3 \Leftrightarrow U\delta U^2 = \delta^{-1}U^3 \Leftrightarrow U\delta = \delta^{-1}U$. Thus the proof of the relation $(\tau_1 U\delta)^3 = 1$ for Theorem 55 is still correct. All the other relations were obtained without using the assumption that $U^2 = 1$ and thus the presentation is correct. □

If $q \equiv 3 \bmod 4$, then we can shorten the presentation for PSL$(2, q)$. The origin of the next theorem is Theorem 101.

Theorem 57 (Presentation of PSL$(2, q)$ for $q \equiv 3 \bmod 4$, [LGOB19], Theorem 3.3)**.** *We assume the requirements defined in Remark 54 and $q \equiv 3$ mod 4. If $1+\omega \in \mathrm{GF}(q)^2$, then we define $r := (q+1)/4$ and $r := (q-3)/4$ otherwise. Then* PSL$(2, q)$ *may be presented by*

$$\{\tau, \delta, U \mid (\tau U)^3 = (U\delta)^2 = U^2 = [\tau, \tau^{\delta^{(q+1)/4}}] = \tau^{\mu(t)} = 1,$$
$$\delta^{(q-1)/2} = \tau^p,\ \tau^{\delta^m} = [\tau^{-1}, \delta^r]\}.$$

Proof. Again we use the presentation in Theorem 101 and substitute the elements w, x, z with $U\tau^{-1}, \tau, \tau\delta^{-1}$. Then one obtains the relations

$$\{(U\tau^{-1})^3 = U^2 = (U\delta^{-1})^2 = \tau^{\mu(t)} = [\tau, (\tau\delta^{-1})^{(q+1)/4}\tau(\tau\delta^{-1})^{-(q+1)/4}] = 1,$$
$$(\tau\delta^{-1})^{(q-1)/2} = \tau^p,\ (\tau\delta^{-1})^m\tau(\tau\delta^{-1})^{-m}$$
$$= \tau(\tau\delta^{-1})^{(-1)^k(q+1)/4}\tau^{-1}(\tau\delta^{-1})^{(-1)^{k+1}(q+1)/4}\},$$

where $k := 2m + 1$.

Using the same arguments as in the proof of Theorem 55 we can replace the relations $(U\tau^{-1})^3 = 1$ and $(U\delta^{-1})^2 = 1$ by the relations $(\tau U)^3 = 1$ and $(U\delta)^2 = 1$. Similarly we have $(\tau\delta^{-1})^{(q+1)/4} = \delta^{-(q+1)/4}$ and thus we replace $[\tau, (\tau\delta^{-1})^{(q+1)/4}\tau(\tau\delta^{-1})^{-(q+1)/4}] = 1$ with $[\tau, \tau^{\delta^{(q+1)/4}}] = 1$. The relations $(\tau\delta^{-1})^{(q-1)/2} = \tau^p$ can be replaced by $\delta^{(q-1)/2} = \tau^p$, too. Likewise we have $(\tau\delta^{-1})^m\tau(\tau\delta^{-1})^{-m} = \tau^{\delta^m}$ and $(\tau\delta^{-1})^{(-1)^{k+1}(q+1)/4} = \delta^{(-1)^k(q+1)/4}$. If k is even, then we can replace this by $\delta^{(q+1)/4}$, otherwise by $\delta^{-(q+1)/4} = \delta^{(q-3)/4}$. □

Again we modify the presentation of the last theorem to obtain a presentation for SL$(2, q)$ in the special case that $q \equiv 3 \bmod 4$.

Theorem 58 (Presentation of $\mathrm{SL}(2,q)$ for $q \equiv 3 \bmod 4$, [LGOB19], Theorem 3.4)**.** *We assume the requirements that are established in Remark 54. Then a presentation for* $\mathrm{SL}(2,q)$ *is given by replacing the relations*

$$(\tau U)^3 = 1, \quad (U\delta)^2 = 1, \quad U^2 = 1 \text{ and } \delta^{\frac{q-1}{2}} = 1$$

by the relations

$$(\tau U)^3 = U^2, \quad (U\delta)^2 = U^2, \quad U^4 = 1 \text{ and } \delta^{\frac{q-1}{2}} = \tau^p U^2$$

in the presentation in Theorem 57.

The proof of this theorem is equivalent to that of Theorem 56.

Now we want to find a presentation for the case that $q = 2^e$ and use the presentation given in Theorem 102.

Theorem 59 (Presentation of $\mathrm{SL}(2,2^e)$, [LGOB19], Theorem 3.5)**.** *We assume the requirements as defined in Remark 54 with the exception that* p *is equal to* 2*. Furthermore we define* μ_{ω^2} *as the minimal polynomial of* ω^2 *over* $\mathrm{GF}(q)$*. Then* $\mathrm{SL}(2,2^e)$ *has the presentation*

$$\{\tau, \delta, U \mid (U\tau)^3 = U^2 = (U\delta)^2 = (\tau\delta)^{q-1} = \tau^2 = 1,\ \tau^{\delta^m} = [\tau,\delta],\ \tau^{\mu_{\omega^2}(t)} = 1\}.$$

Proof. We use Theorem 102 to prove this theorem and substitute w, x, z with $U\tau^{-1}, \tau$ and $\tau\delta^{-1}$. Thus we obtain the relations

$$\{(U\tau^{-1})^3 = U^2 = (U\delta^{-1})^2 = (\tau\delta)^{q-1} = \tau^2 = \tau^{\mu_{\omega^2}(t)} = \tau^{f(t)} = 1\}.$$

Now we can replace $(U\tau^{-1})^3 = 1$ and $(U\delta^{-1})^2 = 1$ by the relations $(U\tau)^3 = 1$ and $(U\delta)^2 = 1$ because $U^2 = 1$. And similarly $\tau^{f(t)} = 1$ by $\tau\tau^{\delta}\tau^{\delta^m} = 1 \Leftrightarrow \tau^{\delta^m} = [\tau,\delta]$. □

We need a small lemma that helps us to prove the correctness of the next presentation, which provides short presentations for the groups $SL(2,p)$ and $\mathrm{PSL}(2,p)$.

Lemma 60. *Let* $2,3 \neq p \in \mathbb{P}$ *be a prime number and* $\ell := \lfloor \frac{p}{3} \rfloor$*. Then* ℓ *is even for* $p \equiv 1$ *mod* 3 *and odd otherwise.*

Proof. We assume that $p \equiv 1 \bmod 3$. If ℓ would be odd, then we would find an element $k \in \mathbb{N}$ such that $\ell = 2k+1$ and thus $p = 3\ell+1 = 3(2k+1)+1 = 6k+4 = 2(3k+2) \notin \mathbb{P}$. Thus ℓ must be even.

On the other hand we assume that $p \not\equiv 1 \bmod 3$. We have $p \neq 3$, thus $p \equiv 2 \bmod 3$. If ℓ would be even, then we would find an element $k \in \mathbb{N}$ such that $\ell = 2k$ and thus $p = 3\ell + 2 = 3(2k) + 2 = 2(3k+1) \notin \mathbb{P}$. Consequentely the result follows. □

The presentation on the generating set of Theorem 99 can be found in Theorem 103. In the next theorem we state once again a modified version that is defined on the standard generators.

Theorem 61 (Presentation of $\mathrm{SL}(2,p)$ and $\mathrm{PSL}(2,p)$, [CR80], Theorem 3.6)**.** *We assume the requirements defined in Remark 54 and define $\ell := \lfloor p/3 \rfloor$. If $p \equiv 1$ mod 3 then $\mathrm{SL}(2,p)$ has the presentation*

$$\{\tau, U \mid U^2 = (U\tau U^2)^3,\ (U(\tau U^2)^4 U(\tau U^2)^{(p+1)/2})^2 (\tau U^2)^p U^{2l} = 1\},$$

else

$$\{\tau, U \mid U^{-2} = (U^{-1}\tau)^3,\ (U^{-1}\tau^4 U^{-1}\tau^{(p+1)/2})^2 \tau^p U^{-2l} = 1\}$$

A presentation for $\mathrm{PSL}(2,p)$ is given by adding the relation $U^2 = 1$.

Proof. Let $x := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $y := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We look at parts of the relations in Theorem 103:

$$x^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \left(\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\right)^3 = \left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)^3 = (xy)^3$$

and

$$(xy^4xy^{(p+1)/2})^2 = \left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & \frac{p+1}{2} \\ 0 & 1 \end{pmatrix}\right)^2$$

$$= \left(\begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & \frac{p+1}{2} \end{pmatrix}\right)^2 = \begin{pmatrix} -1 & -\frac{p+1}{2} \\ 4 & 1 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\,\mathrm{id}\,.$$

Also $y^p = \mathrm{id}$, $x^{2\ell} = \mathrm{id}$ for an even ℓ and $x^{2\ell} = -\,\mathrm{id}$ otherwise. Thus the relation $(xy^4xy^{(p+1)/2})^2 y^p x^{2\ell} = 1$ only holds if ℓ is odd. It follows from Lemma 60 that the relations are fulfilled for $p \not\equiv 1$ mod 3.

Now assume that $p \equiv 1$ mod 3. If we set $\tilde{y} := -y$ and $\tilde{x} := -x$ then we obtain $(\tilde{x}\tilde{y}^4\tilde{x}\tilde{y}^{(p+1)/2})^2 \tilde{y}^p \tilde{x}^{2\ell} = (xy^4xy^{(p+1)/2})^2(-y^p)x^{2\ell} = 1$, because ℓ is even according to Lemma 60. And also $\tilde{x}^2 = (\tilde{x}\tilde{y})^3 \Leftrightarrow x^2 = (xy)^3$, thus the relations in Theorem 103 hold.

Thus for $p \not\equiv 1$ mod 3 we have $x = U^{-1}$ and $y = \tau$ and $x = U$ and $y = \tau U^2$ otherwise. The matrices τ and U generate $\mathrm{SL}(2,p)$ and thus x and y generate $\mathrm{SL}(2,p)$. By substituting x and y in Theorem 103, we obtain the presentations in this theorem. □

6. Special Unitary Group $\mathrm{SU}(3, q)$

In this chapter we define unitary groups and present a generating set of the special unitary group of degree 3 in Section 6.2. In Section 6.3 we give a presentation of the special unitary group of degree 3 and prove its correctness in two steps. First we analyse the subgroup of upper triangular matrices and give a presentation and then we extend this presentation to obtain a presentation for the whole group.

6.1. Definition

Before we define the special unitary group, we need to define unitary forms and isometries on a vector space V with a unitary form ϕ.

Definition 62 (Unitary Form, [Hup67], page 233)**.** *Let $q \in \mathbb{N}$ be a prime power, V a $\mathrm{GF}(q^2)$-vector space and assume that $\bar{\cdot} : \mathrm{GF}(q^2) \to \mathrm{GF}(q^2)$ is a field automorphism of order 2. A map*

$$\phi : V \times V \to \mathrm{GF}(q^2), (v, w) \mapsto \phi(v, w)$$

*is called a **unitary form** on V, if it is additive, i.e.*

$$\phi(au + v, w) = a\phi(u, w) + \phi(v, w),$$

and

$$\phi(u, v) = \overline{\phi(v, u)}$$

for all $u, v, w \in V$ and $a \in \mathrm{GF}(q^2)$.

Definition 63 (Isometrie, [Hup67], page 233)**.** *Let V be a $\mathrm{GF}(q^2)$-vector space, ϕ a form on V and $\sigma \in \mathrm{Aut}(V)$ an automorphism on V, such that $\phi(v^\sigma, w^\sigma) = \phi(v, w)$ for all $v, w \in V$. Then we call σ an **isometry of** $\mathbf{V}$.*

Now we can define the unitary group $\mathrm{GU}(V)$ on a vector space V and its unitary form ϕ. Additionally we define the special unitary group and the projective special unitary group.

Definition 64 (Unitary Group, [Hup67], page 233)**.** *Assume that $\bar{\cdot}$ is a field automorphism of order 2 on the field $\mathrm{GF}(q^2)$. Furthermore, let ϕ be a unitary form on the $\mathrm{GF}(q^2)$-vector space. We call the group of isometries of V the **unitary group** $\mathrm{GU}(\mathbf{V})$ and the subgroup $\mathrm{GU} \cap \mathrm{SL}(V)$ the **special unitary group** $\mathrm{SU}(\mathbf{V})$. Additionally we define the **projective special linear group** $\mathrm{PSU}(\mathbf{V}) = \mathrm{SU}(V)/\mathrm{Z}(\mathrm{SU}(V))$, where $\mathrm{Z}(\mathrm{SU}(V))$ is the centre of the special unitary group.*

The next definition defines the vector space and unitary form that we use throughout the rest of this chapter.

Definition 65. *We define* $\bar{\cdot} : \mathrm{GF}(q^2) \to \mathrm{GF}(q^2), x \mapsto x^q$ *as the Frobenius automorphism on* $\mathrm{GF}(q^2)$*. Set* $V := \mathrm{GF}(q^2)^n$ *for* $n \in \mathbb{N}$*, and define the unitary form*

$$\phi : V \to V, (v,w) \mapsto v \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ \vdots & \iddots & \vdots & \vdots \\ 1 & \cdots & 0 & 0 \end{pmatrix} \overline{w},$$

where $\bar{\cdot}$ *is applied entry-wise. Then we write* $\mathrm{GU}(n,q)$ *instead of* $\mathrm{GU}(V)$ *for the unitary group and similarly* $\mathrm{SU}(n,q)$ *and* $\mathrm{PSU}(n,q)$*.*

Note that we write $\mathrm{SU}(n,q)$ for the group of unitary matrices of determinant 1 of degree n over the field $\mathrm{GF}(q^2)$. This is a common notation.

Lemma 66. *The centre of* $\mathrm{SU}(3,q)$ *is the subgroup*

$$\mathrm{Z}(\mathrm{SU}(3,q) = \{a\mathrm{I}_3 \in \mathrm{SU}(3,q) \mid a \in \mathrm{GF}(q^2) \text{ with } a^3 = 1\}.$$

Proof. It is $\mathrm{Z}(\mathrm{SU}(3,q)) = \mathrm{Z}(\mathrm{GL}(n,q^2)) \cap \mathrm{SU}(n,q)$ and [Hup67], page 177, states that $\mathrm{GL}(n,q^2) = \{a\mathrm{I}_n \mid a \in \mathrm{GF}(q^2)^\times\}$. Let $a \in \mathrm{GF}(q^2)^\times$ such that $a^3 = 1$, then the matrix $a\mathrm{I}_n$ is unitary and of determinant 1, thus the claim holds. □

We have defined all the groups that occur in this chapter. Before giving a generating set of the group $\mathrm{SU}(3,q)$ in the following section, we look at some elements of the special unitary group.

Throughout this chapter we frequently use the following notation.

Definition 67. *For* $\alpha, \beta \in \mathrm{GF}(q^2)$ *we set*

$$\nu(\alpha,\beta) := \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & -\alpha^q \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \Delta(\alpha) := \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^{q-1} & 0 \\ 0 & 0 & \alpha^{-q} \end{pmatrix}.$$

Note that $\det(\nu(\alpha,\beta)) = 1$ and $\Delta(\alpha)$ has determinant 1, if $0 \neq \alpha \in \mathrm{GF}(q^2)$. The matrix $\nu(\alpha,\beta)$ is a unitary matrix if the condition stated in the next lemma is satisfied.

Lemma 68. *Let* $\alpha, \beta \in \mathrm{GF}(q^2)$*. The matrix* $\nu(\alpha,\beta)$*, as defined in Definition 67, is a unitary matrix if and only if* $\mathrm{tr}(\beta) = -\alpha^{q+1}$*.*

Proof. We know that $\det(\nu(\alpha,\beta)) = 1$ for any $\alpha, \beta \in \mathrm{GF}(q^2)$. Thus we need to show that $\phi(v \cdot \nu(\alpha,\beta), w \cdot \nu(\alpha,\beta)) = \phi(v,w)$ for any $v, w \in \mathrm{GF}(q^2)^3$ if and only if

$\beta + \beta^q = -\alpha^{q+1}$. Observe that

$$\begin{aligned}
&\phi(v \cdot \nu(\alpha,\beta), w \cdot \nu(\alpha,\beta)) = \phi(v,w)\\
\Leftrightarrow\ & v \cdot \nu(\alpha,\beta) \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{w \cdot \nu(\alpha,\beta)}^{\top} = \phi(v,w)\\
\Leftrightarrow\ & v \cdot \nu(\alpha,\beta) \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{\nu(\alpha,\beta)}^{\top} \cdot \overline{w}^{\top} = \phi(v,w)\\
\Leftrightarrow\ & v \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & -\alpha^q \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & \alpha^q & \beta^q \\ 0 & 1 & -\alpha \\ 0 & 0 & 1 \end{pmatrix}^{\top} \overline{w}^{\top} = v \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{w}^{\top}\\
\Leftrightarrow\ & v \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & -\alpha^q \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ \alpha^q & 1 & 0 \\ \beta^q & -\alpha & 1 \end{pmatrix} \overline{w}^{\top} = v \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{w}^{\top}\\
\Leftrightarrow\ & v \begin{pmatrix} \beta^q + \alpha^{q+1} + \beta & \alpha^q - \alpha^q & 1 \\ -\alpha + \alpha & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{w}^{\top} = v \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{w}^{\top}.
\end{aligned}$$

Hence $\phi(v \cdot \nu(\alpha,\beta), w \cdot \nu(\alpha,\beta)) = \phi(v,w)$ if and only if $\beta + \beta^q = -\alpha^{q+1}$. □

Lemma 69. *Every upper unitriangular matrix $M \in \mathrm{SU}(3,q)$ is of the form $\nu(\alpha,\beta)$ for some $\alpha, \beta \in \mathrm{GF}(q^2)$.*

Proof. We define

$$M := \begin{pmatrix} 1 & m_{1,2} & m_{1,3} \\ 0 & 1 & m_{2,3} \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SU}(3,q)$$

and, since M is unitary, it follows that

$$\begin{aligned}
& M \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{M}^{\top} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\\
\Leftrightarrow\ & \begin{pmatrix} m_{1,3} + m_{1,2}^{q+1} + \overline{m_{1,3}} & m_{1,2} + \overline{m_{2,3}} & 1 \\ m_{2,3} + \overline{m_{1,2}} & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}
\end{aligned}$$

and the result follows directly. □

We obtain from Lemma 68 that the matrices $\nu(\alpha,\beta)$ defined in Definition 67 are elements of the group $\mathrm{SU}(3,q)$ if $\mathrm{tr}(\beta) = -\alpha^{q+1}$ (see Definition 10 and the subsequent lemma for a definition of the trace). We want to show that the same holds for the matrices $\Delta(\alpha)$, if $\alpha \neq 0$.

Lemma 70. *Let $\alpha \in \mathrm{GF}(q^2)$. The matrix $\Delta(\alpha)$, as defined in Definition 67, is a unitary matrix if and only if $\alpha \neq 0$.*

Proof. If $\alpha = 0$, then $\Delta(0) \notin \mathrm{SU}(3,q)$.

Let $\alpha \neq 0$. Then it is easy to determine that $\det(\Delta(\alpha)) = \alpha^0 = 1$. We have

$$\begin{aligned}
\Delta(\alpha)\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\overline{\Delta(\alpha)}^{\top} &= \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^{q-1} & 0 \\ 0 & 0 & \alpha^{-q} \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} \alpha^q & 0 & 0 \\ 0 & \alpha^{q(q-1)} & 0 \\ 0 & 0 & \alpha^{-1} \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & \alpha \\ 0 & \alpha^{q(q-1)} & 0 \\ \alpha^{-q} & 0 & 0 \end{pmatrix}\begin{pmatrix} \alpha^q & 0 & 0 \\ 0 & \alpha^{q(q-1)} & 0 \\ 0 & 0 & \alpha^{-1} \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & \alpha^0 \\ 0 & \alpha^0 & 0 \\ \alpha^0 & 0 & 0 \end{pmatrix}
\end{aligned}$$

and thus $\phi(v\Delta(\alpha), w\Delta(\alpha)) = \phi(v,w)$ and $\Delta(\alpha)$ is unitary and of determinant 1. □

Since we need to multiply many upper unitriangular matrices in the following proofs, we gather a few calculation rules in the next proposition.

Proposition 71. *Let $\alpha, \beta, \gamma, \delta \in \mathrm{GF}(q^2)$ and $\nu(\alpha,\beta)$ as defined in Definition 67. Then we have*

$$\nu(\alpha,\beta)\nu(\gamma,\delta) = \nu(\alpha+\gamma, \beta+\delta-\alpha\overline{\gamma}).$$

Immediate results are

(1) $\nu(\alpha,\beta)^n = \nu(n\alpha, n\beta - \frac{(n-1)n}{2}\alpha^{q+1})$ for any $n \in \mathbb{N}$,

(2) $\nu(\alpha,\beta)^{-1} = \nu(-\alpha, \overline{\beta})$ and

(3) $\nu(0,\delta)$ commutes with every other matrix $\nu(\alpha,\beta)$.

The proof of the last proposition can be verified easily by simple calculation except for result (1).

Proof. We prove result (1).
Base Case: Let $n := 1$. Then the statement holds.
Induction Hypothesis: We assume that the statement holds for some $n \in \mathbb{N}$.
Induction Step: Using the induction hypothesis, we obtain

$$\begin{aligned}
\nu(\alpha,\beta)^{n+1} &= \nu(\alpha,\beta)^n\nu(\alpha,\beta) = \nu(n\alpha, n\beta - \frac{(n-1)n}{2}\alpha^{q+1})\nu(\alpha,\beta) \\
&= \nu((n+1)\alpha, (n+1)\beta - \frac{(n-1)n}{2}\alpha - n\alpha^{q+1}) \\
&= \nu((n+1)\alpha, (n+1)\beta - \frac{n(n+1)}{2}\alpha)
\end{aligned}$$

and we have shown that the statement holds for all $n \in \mathbb{N}$. □

6.2. Generators

In this section we will define four matrices and show that they generate $\mathrm{SU}(3,q)$. This is needed for the presentation of the group given in the next section.

We start by defining the matrices in Definition 72. For the proof that they form a generating set of $\mathrm{SU}(3,q)$, which is given in Theorem 80 near the end of this section, we need several lemmata in preparation. At the end of this section we show two additional properties of the special unitary group that will be useful for the proof of the correctness of the presentation in Section 6.3.

Definition 72. *Let ω be a primitive element of $\mathrm{GF}(q^2)$, $\xi := (1+\omega^{q-1})^{-1}$, if q is even, and $\xi := -(1+1)^{-1}$ otherwise. Furthermore, define $\zeta := \omega^{(q+1)/2}$. Using the notation of Definition 67 we define the matrices*

$$\nu := \nu(1,\xi),\ \tau := \begin{cases} \nu(0,\zeta), & \text{if } q \text{ is odd} \\ \nu(0,1), & \text{if } q \text{ is even} \end{cases}, \Delta := \Delta(\omega) \text{ and } A := \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

In the remainder of this chapter we will use $\omega \in \mathrm{GF}(q^2)$ as a primitive element and write $-1/2 \in \mathrm{GF}(q^2)$ instead of $-(1+1)^{-1}$. Furthermore, we will use the matrices ν, τ, Δ and A without citing the definition each time.

Lemma 73. *The matrices defined in Definition 72 are elements of $\mathrm{SU}(3,q)$.*

Proof. We know by Lemma 70 that Δ is a unitary matrix of determinant 1.

Let q be odd. Then $-1/2 \in \mathrm{GF}(q)$ and thus the element lies in the fixed field of the map tr (see Lemma 11). It follows that $\xi + \xi^q = -1/2 + (-1/2)^q = -1$. Furthermore, $\zeta + \zeta^q = \omega^{\frac{q+1}{2}} + \omega^{\frac{q(q+1)}{2}} = \omega^{\frac{q+1}{2}}(1+\omega^{\frac{q^2-1}{2}}) = \omega^{\frac{q+1}{2}}(1-1) = 0$. We obtain with Lemma 68 that the matrices ν and τ are unitary and of determinant 1 if q is odd.

Now we assume that q is even. Then we have

$$\begin{aligned} \xi + \xi^q &= (1+\omega^{q-1})^{-1} + (1+\omega^{q-1})^{-q} = (1+\omega^{q-1})^{-1} + (1+\omega^{q(q-1)})^{-1} \\ &= (1+\omega^{q-1})^{-1} + (1+\omega^{1-q})^{-1} = (1+\omega^{q-1})^{-1} + (1+\omega^{1-q})^{-1} \\ &= (1+\omega^{1-q}+1+\omega^{q-1})(1+\omega^{1-q}+1+\omega^{q-1})^{-1} = 1 = -1^{q+1} \end{aligned}$$

and $1+1^q = 0$, thus ν and τ are unitary matrices of determinant 1 if q is even.

We need to show that A lies in $\mathrm{SU}(3,q)$. We have $\det(A) = 1$ and

$$\begin{aligned} A \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{A}^\top &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & (-1)^q & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & (-1)^q & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & (-1)^{q+1} & 0 \\ 1 & 0 & 0 \end{pmatrix}, \end{aligned}$$

since $(-1)^{q+1} = 1$ if q is odd, and $-1 = 1$ if q is even. Therefore we obtain that $\phi(vA, wA) = \phi(v,w)$ for all $v, w \in \mathrm{GF}(q^2)^3$ and thus A is also a unitary matrix. □

The next lemma uses the properties of unitary matrices of determinant 1 to deduce that a matrix is already a triangular matrix if one special entry of the matrix is zero.

Lemma 74. *Let $M \in \mathrm{SU}(3,q)$ be a unitary matrix of determinant 1 with $m_{1,3} = 0$. Then M is a lower triangular matrix.*

Proof. Let

$$M := \begin{pmatrix} m_{1,1} & m_{1,2} & 0 \\ m_{2,1} & m_{2,2} & m_{2,3} \\ m_{3,1} & m_{3,2} & m_{3,3} \end{pmatrix} \in \mathrm{SU}(3,q).$$

Then we have

$$\begin{gathered} \phi(vM, wM) = \phi(v,w) \\ \Leftrightarrow v \begin{pmatrix} m_{1,1} & m_{1,2} & 0 \\ m_{2,1} & m_{2,2} & m_{2,3} \\ m_{3,1} & m_{3,2} & m_{3,3} \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \overline{m_{1,1}} & \overline{m_{2,1}} & \overline{m_{3,1}} \\ \overline{m_{1,2}} & \overline{m_{2,2}} & \overline{m_{3,2}} \\ 0 & \overline{m_{2,3}} & \overline{m_{3,3}} \end{pmatrix} \overline{w}^\top = v \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{w}^\top \\ \Leftrightarrow v \begin{pmatrix} 0 & m_{1,2} & m_{1,1} \\ m_{2,3} & m_{2,2} & m_{2,1} \\ m_{3,3} & m_{3,2} & m_{3,1} \end{pmatrix} \begin{pmatrix} \overline{m_{1,1}} & \overline{m_{2,1}} & \overline{m_{3,1}} \\ \overline{m_{1,2}} & \overline{m_{2,2}} & \overline{m_{3,2}} \\ 0 & \overline{m_{2,3}} & \overline{m_{3,3}} \end{pmatrix} \overline{w}^\top = v \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{w}^\top \end{gathered}$$

for any $v, w \in \mathrm{GF}(q^2)^3$.

It follows that $m_{1,2}\overline{m_{1,2}} = 0 \Rightarrow m_{1,2} = 0$ and $m_{2,3}\overline{m_{1,1}} + m_{2,2}\overline{m_{1,2}} = 0 \Rightarrow m_{2,3}\overline{m_{1,1}} = 0$. We have $\det(M) = 1$ and $m_{1,3} = m_{1,2} = 0$, hence $m_{1,1} \neq 0$. Thus we obtain $m_{2,3} = 0$ and M is a lower triangular matrix. □

In Theorem 80 we take an arbitrary matrix $M \in \mathrm{SU}(3,q)$ and write this matrix as a product of the matrices defined in Definition 72. To achieve that, we want to multiply M with a matrix B (which should also be a product of the matrices of the generating set) to obtain a triangular matrix with the previous lemma.

The next lemmata show that we can write such a matrix B as a product of the claimed generators. We need to differentiate between odd and even q.

Lemma 75. *Let q be odd and $M := \begin{pmatrix} 1 & 0 & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SU}(3,q)$ with $\mathrm{tr}(\beta) = 0$. Then there exist $a_0, \ldots, a_k \in \mathbb{N}$ such that $M = \prod_{i=0}^{q-1} (\tau^{\Delta^i})^{a_i}$.*

Proof. We have

$$\begin{aligned}\tau^{\Delta^i} &= \begin{pmatrix} \omega^{-i} & 0 & 0 \\ 0 & \omega^{-i(q-1)} & 0 \\ 0 & 0 & \omega^{iq} \end{pmatrix} \begin{pmatrix} 1 & 0 & \zeta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \omega^{i} & 0 & 0 \\ 0 & \omega^{i(q-1)} & 0 \\ 0 & 0 & \omega^{-iq} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & \omega^{-i(q+1)}\zeta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.\end{aligned} \tag{6.1}$$

We define K as the smallest subfield of $\mathrm{GF}(q^2)$ which contains $\{\omega^{-i(q+1)}\zeta \mid i \in \mathbb{Z}\}$.

With $|\omega^{q+1}| = q-1$ it follows that ω^{q+1} is a primitive element of $\mathrm{GF}(q)$. Hence $\omega^{\frac{q+1}{2}} \in \mathrm{K}$ is not in $\mathrm{GF}(q)$. But K is a subfield of $\mathrm{GF}(q^2)$ and the largest non-trivial subfield of $\mathrm{GF}(q^2)$ is $\mathrm{GF}(q)$, thus we obtain $\mathrm{K} = \mathrm{GF}(q^2)$.

Therefore every element $\beta \in \mathrm{GF}(q^2)$ can be written as a sum $\beta = \sum_{i=1}^{q-1} a_i \omega^{-i(q+1)}\zeta$ and it follows with Equation 6.1 that $M = \prod_{i=1}^{q-1} (\tau^{\Delta^i})^{a_i}$. □

Lemma 76. *Let q be even and $M \in \mathrm{SU}(3,q)$. Then there exists a matrix $B \in \langle \nu, \tau, \Delta, A\rangle$ such that MB is a lower triangular matrix.*

Proof. We use that

$$\begin{aligned}\nu^{\Delta^i}\tau^{\Delta^j} &= \nu(\omega^{i(q-2)}, \omega^{-i(q+1)}\xi)\nu(0, \omega^{-j(q+1)}) \\ &= \nu(\omega^{i(q-2)}, \omega^{-i(q+1)}\xi + \omega^{-j(q+1)})\end{aligned} \tag{6.2}$$

holds for $i, j \in \mathbb{N}$.

If $m_{1,1} = 0$, then we set $M^{(2)} := MA$ and $m^{(2)}_{1,3} = 0$. Using Lemma 74, $M^{(2)}$ is a lower triangular matrix.

If $m_{1,1} \neq 0$, then we can choose $i, j \in \mathbb{N}$ such that $\nu^{\Delta^i}\tau^{\Delta^j} = \nu(-m_{1,2}m_{1,1}^{-1}, \beta) \in \mathrm{SU}(3,q)$ for some $\beta \in \mathrm{GF}(q^2)$, which follows from Equation 6.2. We set $M^{(1)} := M \cdot \nu(-m_{1,2}m_{1,1}^{-1}, \beta)$ and $m^{(1)}_{1,2} = 0$.

If $m^{(1)}_{1,3} = 0$, then $M^{(1)}$ is already a lower triangular matrix. Otherwise we choose $k, l \in \mathbb{N}$ such that $\nu^{\Delta^k}\tau^{\Delta^l} = \nu(\alpha, -m^{(1)}_{1,3}m^{(1)}_{1,1}) \in \mathrm{SU}(3,q)$ for some $\alpha \in \mathrm{GF}(q^2)$. We set $M^{(2)} := M^{(1)} \cdot \nu(\alpha, -m^{(1)}_{1,3}m^{(1)}_{1,1})$. Then $m^{(2)}_{1,3} = 0$ and $M^{(2)}$ is a lower triangular matrix with Lemma 74. □

In the previous two lemmata we have shown that we can multiply any matrix $M \in \mathrm{SU}(3,q)$ by a product of the matrices defined in Definition 72 and obtain a lower triangular matrix.

Lemma 77. *Let $M \in \mathrm{SU}(3,q)$ be a lower triangular matrix. Then M^A is an upper triangular matrix.*

Proof. We set $M := \begin{pmatrix} m_{1,1} & 0 & 0 \\ m_{2,1} & m_{2,2} & 0 \\ m_{3,1} & m_{3,2} & m_{3,3} \end{pmatrix}$. Then

$$\begin{aligned} M^A &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} m_{1,1} & 0 & 0 \\ m_{2,1} & m_{2,2} & 0 \\ m_{3,1} & m_{3,2} & m_{3,3} \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} m_{3,1} & m_{3,2} & m_{3,3} \\ -m_{2,1} & -m_{2,2} & 0 \\ m_{1,1} & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} m_{3,3} & -m_{3,2} & m_{3,1} \\ 0 & m_{2,2} & -m_{2,1} \\ 0 & 0 & m_{1,1} \end{pmatrix} \end{aligned}$$

and the result follows. □

We have shown that we can use the matrix A to convert a lower triangular matrix into an upper triangular matrix. The next step is to show that any upper triangular can be transformed into an upper unitriangular matrix (by multiplication with elements of Definition 72) and that any upper unitriangular unitary matrix of determinant 1 is already in $\mathrm{SU}(3,q)$.

Lemma 78. *Let $M \in \mathrm{SU}(3,q)$ be an upper triangular matrix. Then there exists a number $k \in \mathbb{N}$ such that $\Delta^{-k}M$ is an upper unitriangular matrix.*

Proof. Let $M := \begin{pmatrix} m_{1,1} & m_{1,2} & m_{1,3} \\ 0 & m_{2,2} & m_{2,3} \\ 0 & 0 & m_{3,3} \end{pmatrix} \in \mathrm{SU}(3,q)$. Similarly to Lemma 74 we use that M is a unitary matrix of determinant 1 to analyse the diagonal entries of M.

For any $v, w \in \mathrm{GF}(q^2)^3$ we have

$$\begin{aligned} &\phi(vM, wM) = \phi(v, w) \\ \Leftrightarrow\ & v \begin{pmatrix} m_{1,1} & m_{1,2} & m_{1,3} \\ 0 & m_{2,2} & m_{2,3} \\ 0 & 0 & m_{3,3} \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \overline{m_{1,1}} & 0 & 0 \\ \overline{m_{1,2}} & \overline{m_{2,2}} & 0 \\ \overline{m_{1,3}} & \overline{m_{2,3}} & \overline{m_{3,3}} \end{pmatrix} \overline{w}^\top = v \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{w}^\top \\ \Leftrightarrow\ & v \begin{pmatrix} m_{1,3} & m_{1,2} & m_{1,1} \\ m_{2,3} & m_{2,2} & 0 \\ m_{3,3} & 0 & 0 \end{pmatrix} \begin{pmatrix} \overline{m_{1,1}} & 0 & 0 \\ \overline{m_{1,2}} & \overline{m_{2,2}} & 0 \\ \overline{m_{1,3}} & \overline{m_{2,3}} & \overline{m_{3,3}} \end{pmatrix} \overline{w}^\top = v \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overline{w}^\top \end{aligned}$$

Thus we obtain $m_{3,3}\overline{m_{1,1}} = m_{2,2}\overline{m_{2,2}} = m_{1,1}\overline{m_{3,3}} = 1$.

We have $m_{1,1} \in \mathrm{GF}(q^2)$, hence there exists an element $k \in \mathbb{N}$ such that $m_{1,1} = \omega^k$. Then we can conclude that

$$\overline{m_{1,1}}m_{3,3} = 1 \Leftrightarrow m_{3,3} = \overline{\omega^k}^{-1} \Leftrightarrow m_{3,3} = \omega^{-kq}.$$

Furthermore there exists an element $r \in \mathbb{N}_0$ such that $m_{2,2} = \omega^r$. Then

$$m_{2,2}\overline{m_{2,2}} = \omega^r\omega^{rq} = \omega^{r(q+1)} = 1 \Leftrightarrow \omega^{r(q+1)} = \omega^0$$

and we can conclude that $r \in (q-1)\mathbb{N}_0$.

We also know that $\det(M) = m_{1,1}m_{2,2}m_{3,3} = \omega^k m_{2,2}\omega^{-kq} = 1 \Leftrightarrow m_{2,2} = \omega^{k(q-1)}$. Consequently

$$\begin{aligned}\Delta(\omega)^{-k}M &= \begin{pmatrix} \omega^{-k} & 0 & 0 \\ 0 & \alpha^{-k(q-1)} & 0 \\ 0 & 0 & \alpha^{kq} \end{pmatrix}\begin{pmatrix} \omega^k & m_{1,2} & m_{1,3} \\ 0 & \omega^{k(q-1)} & m_{2,3} \\ 0 & 0 & \omega^{-kq} \end{pmatrix} \\ &= \begin{pmatrix} \omega^0 & \omega^{-k}m_{1,2} & \omega^{-k}m_{1,3} \\ 0 & \omega^0 & \omega^{-k(q-1)}m_{2,3} \\ 0 & 0 & \omega^0 \end{pmatrix}\end{aligned}$$

and the result follows. □

Lemma 79. *Let $M \in \mathrm{SU}(3,q)$ be an upper unitriangular matrix. Then $M \in \langle \nu, \tau \rangle_{\langle \nu,\tau,\Delta\rangle}$.*

Proof. We know from Lemma 69 that there exist $\alpha, \beta \in \mathrm{GF}(q^2)$ such that $M = \nu(\alpha, \beta)$. Additionally we have

$$\begin{aligned}\nu^{\Delta^i}\tau^{\Delta^j} &= \nu(\omega^{i(q-2)}, \omega^{-i(q+1)}\xi)\nu(0, \omega^{-j(q+1)}) \\ &= \nu(\omega^{i(q-2)}, \omega^{-i(q+1)}\xi + \omega^{-j(q+1)})\end{aligned} \tag{6.3}$$

for $i, j \in \mathbb{N}$. Since the matrix in Equation 6.3 is a product of matrices in $\mathrm{SU}(3,q)$, it also lies in $\mathrm{SU}(3,q)$. For an arbitrary but fixed i, the first argument of ν in Equation 6.3 is fixed. There are q possible values for the second argument depending on j.

We choose i such that $\omega^{i(q-2)} = \alpha$, which is valid since ω^{q-2} has order q^2-1 and generates $\mathrm{GF}(q^2)^\times$. For any $\alpha \in \mathrm{GF}(q^2)$, there exist q elements $\beta \in \mathrm{GF}(q^2)$ such that $-\alpha^{q+1} = \beta + \beta^q$. Thus we can choose j such that $\omega^{-i(q+1)}\zeta + \omega^{-j(q+1)} = \beta$ and the result follows. □

Since we have shown that any upper triangular matrix can be written as a product of a power of Δ and an upper unitriangular matrix (which lies already in $\mathrm{SU}(3,q)$), we only need to summarise all the previous lemmata to prove that the matrices in Definition 72 form a generating set of $\mathrm{SU}(3,q)$.

Theorem 80. *Let ω be a primitive element of $\mathrm{GF}(q^2)$, $\xi := 1/(1+\omega^{q-1})$, if q is even, and $\xi := -1/2$ otherwise. Furthermore define $\zeta := \omega^{(q+1)/2}$. Using the notation in Definition 67 we define the matrices*

$$\nu := \nu(1,\xi),\ \tau := \begin{cases}\nu(0,\zeta), & \text{if } q \text{ is odd} \\ \nu(0,1), & \text{if } q \text{ is even}\end{cases},\ \Delta := \Delta(\omega) \text{ and } A := \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Then $\langle \nu, \tau, \Delta, A\rangle = \mathrm{SU}(3,q)$.

Proof. It follows from Lemma 73 that $\langle \nu, \tau, \Delta, A\rangle \subseteq \mathrm{SU}(3,q)$ holds.

We need to show the other inclusion and prove that every matrix M in $\mathrm{SU}(3,q)$ can be written as a product of ν, τ, Δ and A.

- If q is odd and $m_{3,3} \neq 0$, then we have shown in Lemma 75 that we can construct a matrix $B := \begin{pmatrix} 1 & 0 & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ with $\beta := -\frac{m_{1,3}}{m_{3,3}}$ as a product of τ and Δ. We obtain that
$$M^{(1)} = BM \in \mathrm{SU}(3,q)$$
is a unitary matrix of determinant 1 with $m^{(1)}_{1,3} = 0$. With Lemma 74 we can thus conclude that $M^{(1)}$ is a **lower triangular matrix**.

  If q is even, we know by Lemma 76 that we can write $M^{(1)} := BM$ for a matrix $B \in \langle \nu, \tau, \Delta, A\rangle$ where $M^{(1)}$ is a lower triangular matrix.

- Now we deduce from Lemma 77 that
$$M^{(2)} := (M^{(1)})^A \in \mathrm{SU}(3,q)$$
is an **upper triangular matrix**.

- With Lemma 78 it follows that there exists a natural number $k \in \mathbb{N}$ such that
$$M^{(3)} := \Delta^{-k} M^{(2)} \in \mathrm{SU}(3,q)$$
is an **upper unitriangular matrix**.

- Lemma 79 states that
$$M^{(3)} \in \langle \nu, \tau \rangle_{\langle \nu, \tau, \Delta\rangle}.$$

We have shown that M can be written as a product of ν, τ, Δ and A, hence $M \in \langle \nu, \tau, \Delta, A\rangle$ and $\langle \nu, \tau, \Delta, A\rangle = \mathrm{SU}(3,q)$. □

After having obtained a generating set for $\mathrm{SU}(3,q)$, we define the subgroup of all upper triangular matrices $H \leq \mathrm{SU}(3,q)$ and examine its order. The reader might know that H is a Borel subgroup of the special unitary group $\mathrm{SU}(3,q)$. In the next section we state a presentation for this subgroup and extend it to obtain a presentation for $\mathrm{SU}(3,q)$.

Lemma 81. *The subgroup $H := \langle \nu, \tau, \Delta\rangle \subseteq \mathrm{SU}(3,q)$ is the group of all upper triangular unitary matrices of determinant 1 of order $(q^2-1)q^3$, where the matrices are defined as in Theorem 80.*

Proof. From Lemma 78 and Lemma 79 we obtain that every upper triangular matrix can be written as a product of ν, τ and Δ. Furthermore ν, τ and Δ are upper triangular matrices and thus H is the subgroup of all upper triangular matrices of $\mathrm{SU}(3,q)$.

Any upper triangular matrix M is equal to $\Delta^k M^{(1)}$ for a natural number $k \in \mathbb{N}$ and an upper unitriangular matrix $M^{(1)}$ according to Lemma 78. Lemma 69 states that there exist $\alpha, \beta \in \mathrm{GF}(q^2)$ such that $M^{(1)} = \nu(\alpha, \beta)$, where ν is defined as in Remark 67.

Since M has determinant 1, none of the diagonal entries can be zero and thus $k \in \{1, \ldots, \mathrm{GF}(q)^2 - 1\}$. It follows that there are $q^2 - 1$ different possible values for the diagonal entries.

It holds that $\beta + \beta^q = -\alpha^{q+1}$. Since $-\alpha^{q+1} \in \mathrm{GF}(q)$, there exist q elements $\beta \in \mathrm{GF}(q^2)$ for any $\alpha \in \mathrm{GF}(q^2)$, such that $\beta + \beta^q = -\alpha^{q+1}$ (this follows from Lemma 11).

Thus there are $(q^2 - 1)q^3$ different upper triangular matrices $M \in \mathrm{SU}(3, q)$ and the result follows. □

The next result is needed to prove the correctness of the presentation of $\mathrm{SU}(3, q)$ which is obtained by extending the presentation of the subgroup H.

Lemma 82. *Let ν, τ, Δ and A as in Theorem 80 and $U := \langle \nu, \tau \rangle_H$, $D := \langle \Delta \rangle$, $L := \{A\}$ and $H := \langle \nu, \tau, \Delta \rangle$ the Borel subgroup as in Lemma 81. Then $\mathrm{SU}(3, q)$ is the disjoint union of the sets $UDLU$ and H.*

Proof. We have $UDLU, H \subseteq \mathrm{SU}(3, q)$, thus $UDLU \cup H \subseteq \mathrm{SU}(3, q)$. Let $M \in H$, then M is an upper triangular matrix. But

$$\nu(\alpha, \beta)\Delta^k A \nu(\gamma, \delta) = \begin{pmatrix} \omega^{-qk}\beta & -\omega^{(q-1)k}\alpha + \omega^{-qk}\beta\gamma & \omega^k + \omega^{(q-1)k}\alpha\gamma^q + \omega^{-qk}\delta\beta \\ -\omega^{-qk}\alpha^q & -\omega^{(q-1)k} - \omega^{-qk}\alpha^q\gamma & +\omega^{(q-1)k}\gamma^q - \omega^{-qk}\delta\alpha^q \\ \omega^{-qk} & \omega^{-qk}\gamma & \omega^{-qk}\delta \end{pmatrix} \tag{6.4}$$

for any $\alpha, \beta, \gamma, \delta \in \mathrm{GF}(q^2)$ and $k \in \mathbb{N}$. Thus $M \notin UDLU$. For every matrix $N \in UDLU$, we have $n_{3,1} \neq 0$, thus $N \notin H$ and $UDLU$ and H are disjoint.

The order of $\mathrm{GU}(n, q)$ is $q^{\frac{n^2-n}{2}} \prod_{i=1}^{n}(q^i - (-1)^i)$ (see [Nie19], Theorem 5.34). Let $M \in \mathrm{GU}(3, q)$, then we have $\det(M)\det(\overline{M}^\top) = 1$ since M is unitary. We define $\lambda := \det(M)$, then it follows that $\lambda^{q+1} = 1$.

Let $\lambda = \omega^k \in \mathrm{GF}(q^2)$ such that $\lambda \in \mathrm{Ker}(f)$ (see Lemma 12). Then it follows from the proof of Lemma 12, that $k = m(q - 1)$ for some $m \in \mathbb{N}$. Thus we can write the matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^{m(q-1)} & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GU}(3, q)$ and it follows that there exists a matrix $M \in \mathrm{SU}(3, q)$ for any $\lambda \in \mathrm{Ker}(f)$. Since f is a homomorphism, we obtain the order

$$|\mathrm{SU}(n, q)| = \frac{|\mathrm{GU}(n, q)|}{q + 1}.$$

Thus $|\mathrm{SU}(3, q)| = q^3(q^2 - 1)(q^3 + 1)$. Since $|H| = q^3(q^2 - 1)$ (see Lemma 81) and H and $UDLU$ are disjoint, we need to show that there are at least $|\mathrm{SU}(3, q)| - |H| = q^6(q^2 - 1)$ elements in $|UDLU|$.

Now let $M \in UDLU$ be an arbitrary matrix. Then M is equal to the structure of the matrix in Equation 6.4. The entry $m_{3,1}$ is different for $1 \leq k \leq q^2 - 1$. Since

$\nu(\alpha,\beta) \in \mathrm{SU}(3,q)$ implies that $-\alpha^{q+1} = \beta + \beta^q$, we obtain that for every $\alpha \in \mathrm{GF}(q^2)$ there are q possibilities for β. The same holds for γ and δ. If k, α, β, γ and δ are fixed, then the matrix M is already determined. Hence $|UDLU| = (q^2-1)q^6$.

Consequently $|UDLU \cup H| = |\mathrm{SU}(3,q)|$ and the result follows. □

6.3. Presentation

In this section we will prove the correctness of a presentation of $\mathrm{SU}(3,q)$, which is given in [LGOB19], Section 4.2.2. Our proof follows this paper by defining and proving the correctness of a presentation of the subgroup $H = \langle \nu, \tau, \Delta \rangle$ of order $(q^2-1)q^3$ first (see Lemma 81). Afterwards this presentation is extended to a presentation of the whole group $\mathrm{SU}(3,q)$.

6.3.1. Presentation of H

Before starting with a presentation of the subgroup H of $\mathrm{SU}(3,q)$ we cite two lemmata which will be used for the proof of the correctness of the presentation.

Lemma 83 ([Gur+08], Lemma 4.23)**.** *If $p^e =: q \neq 2,3,5$ for a prime p and $\omega \in \mathrm{GF}(q^2)$ a primitive element, then there exist integers x and y such that*

(1) $\omega^{x(q-2)} + \omega^{y(q-2)} = 1$

(2) $\omega^{-x(q+1)} + \omega^{-y(q+1)} = 1$

(3) $\mathrm{GF}(p)[\omega^{x(q+1)}] = \mathrm{GF}(q)$

(4) $\mathrm{GF}(p)[\omega^{x(q-2)}]$ *is equal to* $\mathrm{GF}(q^2)$ *or* GF.

Proof. The proof of this lemma can be found in [Gur+08], where ω^{-x} and ω^{-y} are replaced by elements $a, b \in \mathrm{GF}(q^2)$. □

Lemma 84 ([Gur+08], Lemma 4.5)**.** *Let U_0 and W_0 be subgroups of a group G, and let u, w, a, b be elements of G satisfying the following conditions:*

(1) $[a,b] = 1$

(2) $\langle u, u^a, U_0 \rangle = \langle u, u^b, U_0 \rangle = \langle u^a, u^b, U_0 \rangle$

(3) $\langle w, w^a, W_0 \rangle = \langle w, w^b, W_0 \rangle = \langle w^a, w^b, W_0 \rangle$

(4) $[u^a, w] = [u^b, w] = 1$

(5) U_0 *and* W_0 *are normalised by* $\langle a, b \rangle$

(6) $[U_0, w] = [u, W_0] = 1$.

Then $[\langle \{u^c \mid c \in \langle a,b \rangle\} \rangle, \langle \{w^c \mid c \in \langle a,b \rangle\} \rangle] = 1$.

Please refer to [Gur+08] for a proof of the last lemma. Now we have done all the preparation. The next theorem gives a presentation of the subgroup H defined in Lemma 81.

Theorem 85 ([LGOB19], Section 4.2.1)**.** *The set*

$$\{\nu, \tau, \Delta \mid R_1 \cup R_2 \cup R_3\}$$

is a presentation of a subgroup $H < \mathrm{SU}(3, q)$, where $q = p^e$ for a prime p, $\omega \in \mathrm{GF}(q^2)$ is a primitive element and $\omega_0 = \omega^{q+1} \in \mathrm{GF}(q)$.

The relations in R_1 are

(1) $\Delta^{q^2-1} = 1$

(2) $a := \Delta^x$ *and* $b := \Delta^y$ *for x and y satisfying Lemma 83*

(3) $\nu^p = 1$*, if p is odd, and* $\nu^2 = \tau$*, if p is even*

(4) $\tau^p = 1$*,*

the relations in R_2 are

(1) $\tau = \tau^a\tau^b$ *and, if p is odd, then* $\tau = \tau^b\tau^a$

(2) if $e > 1$, then $\tau^{\mu_1(a)} = 1$*, where μ_1 is the minimal polynomial of* ω_0^{-x} *over* $\mathrm{GF}(p)$

(3) if $e = 1$ *or* $\gcd(x, q^2 - 1) > 1$*, then* $\tau^\Delta = \tau^{\mu_2(a)}$*, where μ_2 is a polynomial of degree at most $e - 1$ over* $\mathrm{GF}(p)$ *and* $\omega_0^{-1} = \mu_2(\omega_0^{-x})$*.*

We define $W := \langle\tau\rangle_{\langle\nu,\tau,\Delta\rangle}$ as the normal closure of τ in the subgroup H and then the relations in R_3 are

(1) $\nu = \nu^a\nu^b w_1$ *for some* $w_1 \in W$ *and, if p is odd, then* $\nu = \nu^b\nu^a w_2$ *for some* $w_2 \in W$

(2) $[\nu^a, \tau] = [\nu^b, \tau] = 1$

(3) $[\nu, \nu^a] = w_3$ *for some* $w_3 \in W$

(4) if p is even and $e > 1$, then $[\nu^\Delta, \nu^a] = w_4$ *and* $[\nu^\Delta, \nu^b] = w_5$ *for some* $w_4, w_5 \in W$

(5) $\nu^{\mu_3(a)} = w_6$ *for some* $w_6 \in W$*, where μ_3 is a minimal polynomial of* $\omega^{x(q-2)}$ *over* $\mathrm{GF}(p)$

(6) if p is odd and $\gcd(x, q^2 - 1) > 1$*, then* $\nu^\Delta = \nu^{\mu_4(a)}w_7$ *for some* $w_7 \in W$*, where μ_4 is the polynomial of degree at most $2e - 1$ over* $\mathrm{GF}(p)$ *satisfying* $\omega^{q-2} = \mu_4(\omega^{x(q-2)})$*,*
otherwise, if p is even, then $\nu^{\Delta^2} = \nu^{\mu_5(a)}\nu^{\Delta\mu_6(a)}w_7$ *for some* $w_7 \in W$*, where μ_5 and μ_6 are polynomials of degree at most $e - 1$ over* $\mathrm{GF}(p)$ *satisfying* $\omega^{2q-4} = \mu_5(\omega^{x(q-2)}) + \omega^{q-2}\mu_6(\omega^{x(q-2)})$*.*

Note that $B^{p(a)}$ for elements B and a and a polynomial p is defined as in Remark 54.

We can identify the generators in Theorem 85 with the matrices in Theorem 80.

Proof. Let G be the presented group and H the subgroup of Lemma 81. We will prove that G is isomorphic to H and define $U := \langle \nu, \tau \rangle_H$ as the normal subgroup of H that contains all upper unitriangular matrices in H and $W := \langle \tau \rangle_H$ as the normal closure of τ. We follow Proposition 18 and prove first that the map

$$\varphi : G \to H, \tau \mapsto \tau, \nu \mapsto \nu, \Delta \mapsto \Delta$$

is a well-defined surjective homomorphism.

Relations $\mathbf{R_1}$ Relation (1) is satisfied, because $\mathrm{GF}(q^2)^\times$ has order $q^2 - 1$. Relation (2) actually defines new generators and the existence of numbers x and y is shown in Lemma 83.

For odd p we obtain with Lemma 71 that $\nu(1, \xi)^p = \nu(p, p\xi - \frac{p^2-p}{2}) = \mathrm{id}$, because the characteristic of the field is p. If p is even, we have $\nu^2 = \nu(2, 2\xi - 1) = \nu(0, 1) = \tau$.

For odd p, we have $\tau^p = \nu(0, p\zeta) = \mathrm{id}$ and for even p we obtain $\tau^p = \nu(0, p) = \mathrm{id}$. Thus relations (3) and (4) are satisfied.

Relations $\mathbf{R_2}$ We obtain with Lemma 83 that

$$\begin{aligned}
\tau^a \tau^b &= \Delta^{-x} \tau \Delta^{x-y} \tau \Delta^y \\
&= \begin{pmatrix} 1 & 0 & \zeta\omega^{-x(q+1)} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \zeta\omega^{-y(q+1)} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & \zeta(\omega^{-x(q+1)} + \omega^{-y(q+1)}) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \tau.
\end{aligned}$$

Similarly $\tau^b \tau^a = \mathrm{id}$, hence relation (1) holds.

If $e > 1$, then we define $\mu_1 : \mathrm{GF}(q^2) \to \mathrm{GF}(q^2), x \mapsto \sum_{i=0}^{e} c_i x^i$ as the minimal polynomial of ω_0^{-x} over $\mathrm{GF}(p)$. Then, with Remark 54, we obtain

$$\tau^{\mu_1(a)} = \begin{pmatrix} 1 & 0 & \zeta \sum_{i=0}^{e} c_i \omega^{-ix(q+1)} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \zeta\mu_1(\omega_0^{-x}) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathrm{id},$$

thus relations (2) holds.

Let $\mu_2 : \mathrm{GF}(q^2) \to \mathrm{GF}(q^2), x \mapsto \sum_{i=0}^{e-1} d_i x^i$ be a polynomial over $\mathrm{GF}(q)$ such that $\omega_0^{-1} = \mu_2(\omega_0^{-x})$. Then

$$\tau^{\mu_2(a)} = \begin{pmatrix} 1 & 0 & \zeta \sum_{i=0}^{e-1} d_i \omega^{-ix(q+1)} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \zeta\mu_2(\omega_0^{-x}) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & \zeta\omega_0^{-1} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \tau^{\Delta}.$$

Relations $\mathbf{R_3}$ The set $W := \langle\tau\rangle_H$ is the set of all matrices $M \in \mathrm{SU}(3,q)$ of the form $M = \begin{pmatrix} 1 & 0 & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ for $\beta \in \mathrm{GF}(q^2)$ with $\mathrm{tr}(\beta) = 0$. This follows from Lemma 75, because we have $\tau^\nu = \tau$. We also need Lemma 71 and $\nu^{\Delta^x} = \nu(\omega^{x(q-2)}, \omega^{-x(q+1)}\xi)$, which can be easily checked.

We know that

$$\nu^a\nu^b = \nu(\omega^{x(q-2)}, \omega^{-x(q+1)}\xi) \cdot \nu(\omega^{y(q-2)}, \omega^{-y(q+1)}\xi)$$
$$= \nu(\omega^{x(q-2)} + \omega^{y(q-2)},\ \omega^{-x(q+1)} + \omega^{-y(q+1)} - \omega^{x(q-2)+yq(q-2)})$$
$$= \nu(1, 1 - \omega^{(x+yq)(q-2)}) = \nu \cdot w_1$$

for a matrix $w_1 \in W$. Thus relation (1) holds.

We check that relation (2) is satisfied and obtain

$$[\nu^a, \tau] = (\tau\nu^a)^{-1}\nu^a\tau = (\nu(0,\zeta)\nu(\omega^{x(q-2)}, \omega^{-x(q+1)}\xi))^{-1} \cdot \nu(\omega^{x(q-2)}, \omega^{-x(q+1)}\xi)\nu(0,\zeta)$$
$$= \nu(\omega^{x(q-2)}, \zeta + \omega^{-x(q+1)}\xi)^{-1} \cdot \nu(\omega^{x(q-2)}, \omega^{-x(q+1)}\xi + \zeta) = \mathrm{id}\,.$$

Similarly, we obtain $[\nu^b, \tau] = \mathrm{id}$.

We have

$$[\nu, \nu^a] = (\nu^a\nu)^{-1}\nu\nu^a$$
$$= (\nu(\omega^{x(q-2)}, \omega^{-x(q+1)}\xi)\nu(1,\xi))^{-1} \cdot \nu(1,\xi)\nu(\omega^{x(q-2)}, \omega^{-x(q+1)}\xi)$$
$$= \nu(\omega^{x(q-2)} + 1, \omega^{-x(q+1)}\xi + \xi - \omega^{x(q-2)})^{-1} \cdot \nu(1 + \omega^{x(q-2)}, \xi + \omega^{-x(q+1)}\xi - \omega^{x(1-2q)})$$
$$= \nu(-\omega^{x(q-2)} - 1, -(\omega^{x(q-2)} + 1)^{q+1} - \omega^{-x(q+1)}\xi - \xi + \omega^{x(q-2)})$$
$$\cdot\nu(1 + \omega^{x(q-2)}, \xi + \omega^{-x(q+1)}\xi - \omega^{x(1-2q)})$$
$$= \nu(0,\gamma) \in W$$

for some $\gamma \in \mathrm{GF}(q^2)$, thus relation (3) holds.

Assuming that p is even and $e>1$, we obtain

$$\begin{aligned}[\nu^\Delta,\nu^a] &= (\nu^a\nu^\Delta)^{-1}\nu^\Delta\nu^a \\ = (\nu(\omega^{(q-2)x},\omega^{-(q+1)x}\xi)\nu(\omega^{(q-2)},\omega^{-(q+1)}\xi))^{-1}&\cdot\nu(\omega^{(q-2)},\omega^{-(q+1)}\xi)\nu(\omega^{(q-2)x},\omega^{-(q+1)x}\xi) \\ = \nu(\omega^{(q-2)x}+\omega^{(q-2)},\omega^{-(q+1)x}\xi+\omega^{-(q+1)}\xi-\omega^{(q-2)x}\omega^{(1-2q)})&^{-1} \\ \cdot\nu(\omega^{(q-2)}+\omega^{(q-2)x},\omega^{-(q+1)}\xi+\omega^{-(q+1)x}\xi-\omega^{(q-2)}\omega^{(1-2q)x}&) \\ = \nu(0,\gamma)\in W&\end{aligned}$$

similarly to the calculation in relation (3). Analogously we have $[\nu^a,\nu^\Delta]\in W$ and we obtain that the relations in (4) hold for the matrices ν,τ and Δ.

Let $\mu_3:\mathrm{GF}(q)\to\mathrm{GF}(q), x\mapsto\sum_{i=0}^{e-1}c_ix^i$ be the minimal polynomial of $\omega^{x(q-2)}$ over $\mathrm{GF}(p)$ (note that $\mathrm{GF}(p)[\omega^{x(q-2)}]=\mathrm{GF}(q)$ as stated in Lemma 83). We follows that $\nu^a=\nu(\omega^{x(q-2)},\omega^{-x(q+1)}\xi)$ and thus $\nu^{a^i}=\nu(\omega^{ix(q-2)},\omega^{-ix(q+1)}\xi)$. Then we obtain

$$\begin{aligned}\nu^{\mu_3(a)} &= \prod_{i=0}^{e-1}(\nu^{a^i})^{\tilde{c}_i}=\prod_{i=0}^{e-1}\nu(\omega^{ix(q-2)},\omega^{-ix(q+1)}\xi)^{\tilde{c}_i} \\ = \prod_{i=0}^{e-1}\nu(\tilde{c}_i\omega^{ix(q-2)},&\tilde{c}_i\omega^{-ix(q+1)}\xi-\frac{\tilde{c}_i{}^2-\tilde{c}_i}{2}\omega^{ix(q-2)(q+1)}) \\ &= \nu(\mu(\omega^{x(q-2)}),\gamma)\in W\end{aligned}$$

for some $\gamma\in\mathrm{GF}(q^2)$ and relation (5) holds.

Let p be odd, $\gcd(x,q^2-1)>1$ and $\mu_4:\mathrm{GF}(q^2)\to\mathrm{GF}(q^2), x\mapsto\sum_{i=0}^{2e-1}c_ix^i$ a polynomial over $\mathrm{GF}(p)$ such that $\mu_4(\omega^{x(q-2)})=\omega^{q-2}$. Then

$$\begin{aligned}\nu^{\mu_4(a)} &= \prod_{i=1}^{e-1}(\nu^{a^i})^{\tilde{c}_i}=\nu(\mu(\omega^{x(q-2)}),\gamma) \\ &= \mu(\omega^{q-2},\gamma)=\nu^\Delta w_7\end{aligned}$$

similarly to relation (5) for some $w_7\in W,\gamma\in\mathrm{GF}(q^2)$, since $\nu^\Delta=\nu(\omega^{q-2},\omega^{-q-1}\xi)$.

If p is even, then we define $\mu_5:\mathrm{GF}(q^2)\to\mathrm{GF}(q^2)$ and $\mu_6:\mathrm{GF}(q^2)\to\mathrm{GF}(q^2)$ as polynomials over $\mathrm{GF}(p)$ with degree at most $e-1$ such that $\mu_5(\omega^{x(q-2)})+\omega^{q-2}\mu_6(\omega^{x(q-2)})=\omega^{2q-4}$. Thus we obtain again

$$\begin{aligned}\nu^{\mu_5(a)}\nu^{\Delta\mu_6(a)} &= \nu(\mu_5(\omega^{x(q-2)}),\gamma_1)\nu(\mu_6(\omega^{x(q-2)})\omega^{q-2},\gamma_2) \\ = \nu(\mu_5(\omega^{x(q-2)})+\mu_5(\omega^{x(q-2)}\omega^{q-2}),\gamma_3)&=\nu(\omega^{2q-4},\gamma_3) \\ &= \nu^{\Delta^2}w_7\end{aligned}$$

for some $\gamma_1,\gamma_2,\gamma_3\in\mathrm{GF}(q^2)$ and $w_7\in W$, since $\nu^{\Delta^2}=\nu(\omega^{2q-4},\omega^{-2q-2}\xi)$. Thus the relations in (6) hold.

We have shown now that the relations $R_1 \cup R_2 \cup R_3$ hold for the matrices $\nu, \tau, \Delta \in H$ and thus the epimorphism φ is well-defined. Now we want to show that this epimorphism is already an isomorphism and prove this by considering the order of the generated group G. Lemma 81 states that H has order $q^3(q^2-1)$, hence we need to show that the order of the presented group G equals that of H.

We define $\tilde{U} := \{\langle \nu, \tau \rangle^c \mid c \in \langle a, b \rangle\}$ and $\tilde{W} := \langle \tau \rangle_G$, such that $\tilde{U}$ and $\tilde{W}$ are normal subgroups of G, and define $Z := \tilde{U}\tilde{W}/\tilde{W}$. With relations $R_3(1)$ and $R_3(2)$ we obtain that

$$[\nu, \tau] = \nu^{-1}\tau^{-1}\nu\tau = \nu^{-b}\nu^{-a}\tau\nu^a\nu^b\tau = 1,$$

thus $\tilde{W} = \langle \tau^c \mid c \in \langle \Delta \rangle \rangle$. Applying Lemma 84 with $U_0 = W_0 = \langle 1 \rangle$, $u = w = \tau$ and $a = \Delta^x, b = \Delta^y$, we obtain that

$$[\langle \tau^c \mid c \in \langle a, b \rangle \rangle, \langle \tau^c \mid c \in \langle a, b \rangle \rangle] = 1.$$

If $\gcd(x, q^2-1) = 1$, then we have $\Delta \in \langle a \rangle$. Otherwise it follows from relation $R_2(3)$ that $\tau^\Delta \in \langle \tau^c \mid c \in \langle a, b \rangle \rangle$ and thus $\langle \tau^c \mid c \in \langle a, b \rangle \rangle = \tilde{W}$ is abelian.

We set $u = w = \nu$, $a = \Delta^x, b = \Delta^y$, $U_0 = W_0 = \tilde{W}$ and check the conditions for Lemma 84. We have $[\Delta^x, \Delta^y] = 1$, $\langle \nu, \nu^a, \tilde{W} \rangle = \langle \nu, \nu^b, \tilde{W} \rangle = \langle \nu^a, \nu^b, \tilde{W} \rangle$ and $\tilde{W}$ is normalized by $\langle a, b \rangle$, since $\tilde{W}$ is normalized by Δ. The relation $[\nu^a, \nu] = [\nu^b, \nu] = 1$ is implied by relation $R_3(3)$. We have shown that ν and τ commute and thus $[\tilde{W}, \nu] = 1$ and the conditions are satisfied. It follows that

$$[\langle \nu^c \mid c \in \langle a, b \rangle \rangle, \langle \nu^c \mid c \in \langle a, b \rangle \rangle] = 1.$$

If $\gcd(x, q^2-1) = 1$, then we already know that $\Delta \in \langle a \rangle$ and $[\langle \nu^c \mid c \in \langle \Delta \rangle \rangle, \langle \nu^c \mid c \in \langle \Delta \rangle \rangle] = 1$. Otherwise it follows from relation $R_3(6)$ that $\nu^\Delta = \nu^{\mu_4(a)} w_7$ for some element $w_7 \in W$ and a polynomial $\mu_4(a)$.

It follows that Z is abelian and that we can write $Z = \langle \nu^c \mid c \in \langle a \rangle \rangle \tilde{W}/\tilde{W}$ (note that $c \in \langle a, b \rangle$ implies that $c \in \langle a \rangle$ is implied by relation $R_3(1)$). The elements ν and τ have order p and thus the order of every element in Z is a power of p. Hence Z is also elementary abelian.

We apply Lemma 83 again with $u = \tau$, $w = \nu$, $U_0 = \langle 1 \rangle$ and $W_0 = \tilde{W}$ and obtain

$$[\langle \tau^c \mid c \in \langle a, b \rangle \rangle, \langle \nu^c \mid c \in \langle a, b \rangle \rangle] = 1,$$

thus $\tilde{W} \trianglelefteq \tilde{U}$.

Odd Characteristic p Relation $R_3(6)$ states that $\nu^\Delta = \nu^{\mu_4(a)} w_7$ for an element $w_7 \in W$ and μ_4 a polynomial of degree at most $2e-1$, if $\gcd(x, q^2-1) > 1$. Otherwise we already know from Lemma 83 that there exists a polynomial of degree smaller or equal to $2e-1$ such that the same relation holds. Hence every element $z \in Z$ can be written as a product

$$z = \tilde{u}\tilde{w}\tilde{W} = \tilde{u}\tilde{W} = (\nu^{a^0})^{\ell_0}(\nu^{a^1})^{\ell_1} \cdots (\nu^{a^{2e-1}})^{\ell_{2e-1}}\tilde{W},$$

where $\ell_i \in \mathbb{N}$. Since ν has order p, we can deduce that there are $p^{2e} = q^2$ elements in Z. Similarly we can follow from relation $R_2(2)$ and $R_2(3)$ that $\tilde{W}$ has order $p^e = q$. Hence it is $Z = \tilde{U}/\tilde{W}$, where $\tilde{W} \trianglelefteq Z$. And thus $|Z| = |\tilde{U}|/|\tilde{W}| \Leftrightarrow q^2 = |\tilde{U}|/q \Leftrightarrow |\tilde{U}| = q^3$. Since $\tilde{U} = \langle \nu, \tau \rangle_G$, we obtain $|\langle \nu, \tau \rangle_G| = q^3$.

Even characteristic p The minimal polynomial of $\omega^{x(q-2)}$ has order e, since $\mathrm{GF}(p)[\omega^{x(q-2)}] = \mathrm{GF}(q)$ (see Lemma 83), hence we can use relation $R_3(5)$ in a similar way as above and obtain that Z has order q. Setting $u = \nu, w = \nu^\Delta$ and $U_0 = W_0 = \tilde{W}$ we can deduce with Lemma 84 that Z and Z^Δ commute. It also holds that $(z_1 z_2^\Delta)^\Delta \in Z \oplus Z^\Delta$ for any $z_1, z_2 \in Z$ because of relation $R_3(6)$. Consequently Δ normalises $Z \oplus Z^\Delta$. We apply Lemma 84 again with $u = \tau, w = \nu, U_0 = \langle 1 \rangle$ and $W_0 = \tilde{W}$ and obtain

$$[\langle \{\tau^c \mid c \in \langle a, b \rangle\} \rangle, \langle \{\nu^c \mid c \in \langle a, b \rangle\} \rangle] = 1.$$

Hence $\langle \nu, \tau \rangle_G$ normalizes $\tilde{W}$.

We obtain that $Z \oplus Z^\Delta = \langle \nu, \tau \rangle_G / \tilde{W}$, $|Z \oplus Z^\Delta| = q^2$, $|\tilde{W}| = q$ and hence $|\langle \nu, \tau \rangle_G| = q^3$.

Relation $R_1(1)$ defines the order of $\langle \Delta \rangle$ as $q^2 - 1$ and $\tilde{U} \trianglelefteq G$. Let $x \in \tilde{U} \cap \langle \Delta \rangle$. Then we have $x \in U$, thus $x^{p^d} = 1$ for some $d \in \mathbb{N}$. But $p \nmid q^2 - 1$, thus $d = 0$ and then x is already 1. It follows that $\tilde{U} \rtimes \langle \Delta \rangle = G$ and $|G| = |U||\Delta| = q^3(q^2 - 1)$.

We have shown that the presented group G has the same order as the subgroup H defined in Lemma 81 and knowing that φ is an epimorphism, we obtain that φ is an isomorphism and the presented group G is isomorphic to the subgroup H. Hence the correctness of the presentation is proven. □

6.3.2. Additional Relations for the Presentation of $\mathrm{SU}(3,q)$

After having proven a presentation of the subgroup H, we want to extend this presentation in the remainder of this chapter to obtain a presentation for the whole group $\mathrm{SU}(3,q)$. The proof of the extension follows [LGOB19], Section 4.2.2, which itself follows [HS11].

We start by defining relations called $P(u)$ of the form $u^A = u_L d A u_R$, where $u_L, u_R \in U$ and $d \in D$ depend on the upper unitriangular matrix $u \in U$. Note that U is the subgroup of upper unitriangular matrices in $\mathrm{SU}(3,q)$.

Lemma 86. *Let $\nu(\alpha, \beta) = u \in U$ be an upper unitriangular matrix in $\mathrm{SU}(3,q)$. Then the matrices $u_L := \nu(-\alpha, \beta^{-q}, \beta^{-1}) \in U$, $u_R := \nu(-\alpha\beta^{-1}, \beta^{-1}) \in U$ and $d := \mathrm{diag}(\beta^{-q}, \beta^{q-1}, \beta) \in \langle \Delta \rangle =: D$ fulfil the relation $u^A = u_L d A u_R$.*

Proof. This can be easily verified by multiplying the matrices. □

Next we define a group G via a presentation on four elements. We can deduce by observing the relations that the subgroup H is isomorphic to a subgroup of the presented group G.

Definition 87 (Presentation of $\mathrm{SU}(3,q)$, [LGOB19], page 14, and [HS11])**.** *Let $q = p^e$ be a prime power and $P(u)$ the relation $u^A = u_L dA u_R$ for $u, u_L, u_R \in U$ and $d \in D$ as in Lemma 86. Then we define the group*

$$G := \langle \nu, \tau, \Delta, A \mid R(1), R(2), \Delta^A = \Delta^{-q}, A^2 = 1 \rangle,$$

where $R(1)$ are the relations defined in Theorem 85 and $R(2) \subseteq \{P(u) \mid u \in U\}$.

Definition 88. *Let $R(2) \subseteq \{P(u) \mid u \in U\}$ be a set of relations as in Lemma 86. Then we define $V \subseteq U$ as the maximum set such that every relation $P(u)$ for $u \in V$ is implied by the relations in $R(2)$.*

The next threorem states that the group G defined in Definition 87 is isomorphic to the special unitary group $\mathrm{SU}(3,q)$ if certain conditions hold. More precisely $G \cong \mathrm{SU}(3,q)$ if every relation $P(u)$ is implied from $R(2)$ for any $u \in \mathrm{SU}(3,q)$.

Theorem 89. *We assume that G is the presented group of Definition 87 and $V \subseteq U$ as in Definition 88. If $V = U \backslash \{1\}$, then G is isomorphic to $\mathrm{SU}(3,q)$.*

Proof. Let $\tilde{H} \leq G$ be the group presented in Theorem 85, $\tilde{U} := \langle \nu, \tau \rangle_{\tilde{H}}, \tilde{D} := \langle \Delta \rangle$ and $\tilde{L} := \{A\}$ subgroups of the group G. Additionally, let U, D and L be the equivalents in the matrix group $\mathrm{SU}(3,q)$ (see Lemma 86 and $L := \{A\}$).

If $V = U \backslash \{1\}$, then a relation $u^A = u_L dA u_R$ is implied by $R(2)$ for every $u \in U \backslash \{1\}$. Thus $\tilde{U}\tilde{D}\tilde{L}\tilde{U} \cong UDLU$, since $U \cong \tilde{U}$ and $D \cong \tilde{D}$. The set $\tilde{H} \cup \tilde{U}\tilde{D}\tilde{L}\tilde{U}$ is a subgroup of G since $\mathrm{id} \in \tilde{H}$ and it is closed under multiplication: Let $a, b \in \tilde{H}$, then $ab \in \tilde{H}$. Let $a = u_1^A, b = u_2^A \in \tilde{U}\tilde{D}\tilde{L}\tilde{U}$, then $ab = (u_5 u_6)^A \in \tilde{H} \cup \tilde{U}\tilde{D}\tilde{L}\tilde{U}$. Let $a = u_1^A \in \tilde{U}\tilde{D}\tilde{L}\tilde{U}$ and $b \in \tilde{H}$, then there exist $u_2, u_3 \in \tilde{U}, d \in \tilde{D}$ such that $b = u_2 d u_3 = (u_2 dA\,\mathrm{id})(\mathrm{id}\,\mathrm{id}\,Au_3) = u_4^A$ for some $u_4 \in \tilde{U}$ and hence $ab = (u_1 u_4)^A \in \tilde{H} \cup \tilde{U}\tilde{D}\tilde{L}\tilde{U}$.

Furthermore all generators ν, τ, Δ, A are in $\tilde{H} \cup \tilde{U}\tilde{D}\tilde{L}\tilde{U}$, and thus we obtain $G = \tilde{H} \cup \tilde{U}\tilde{D}\tilde{L}\tilde{U} \cong H \cup UDLU = \mathrm{SU}(3,q)$ with Lemma 82. □

With the last theorem we have given a presentation of the special unitary group $\mathrm{SU}(3,q)$ and have proven its correctness. Since the obtained presentation is not yet short (as defined in Section 2.2), we show that only a limited number of relations $P(u)$ is needed.

A few properties of the set V and elements in $\mathrm{GF}(q^2)$ are stated in the subsequent lemmata.

Lemma 90. *The set V, as defined in Definition 88, is closed under conjugation by Δ. If $u, v \in V$ and u_R and v_L as in Lemma 86, then $uv \in V$ if and only if $u_R v_L \in V$.*

Proof. Let $u \in V$, then there is a relation $u^A = u_L dA u_R$ in $R(2)$. It follows with $\Delta^A = \Delta^{-q}$ and since U is closed under conjugation with Δ that

$$(u^\Delta)^A = (u^A)^{\Delta^A} = \Delta^q u_L dA u_R \Delta^{-q} = \tilde{u_L} \Delta^{-q} dA \Delta^q \tilde{u_R} = \tilde{u_L} \underbrace{\Delta^{-q} dAA \Delta^{-1}}_{\in D} A \tilde{u_R}.$$

Thus $u^\Delta \in V$.

Let $u, v \in V$ with $u^A = u_L dAu_R$ and $v^A = v_L d'Av_R$ for a number $k \in \mathbb{N}$. Then $(u_R v_L)^A = \tilde{u_L}\tilde{d}A\tilde{u_R}$ if and only if

$$(uv)^A = u^A v^A = (u_L dAu_R)(v_L \Delta^k A v_R) = u_L dA(Au_R v_L A)d'Av_R = \tilde{u_L}\tilde{d}Av_R$$

since $\Delta^A \in \langle\Delta\rangle$. □

Lemma 91. *Let $\beta, \eta \in \mathrm{GF}(q^2)$ with $\mathrm{tr}(\beta), \mathrm{tr}(\eta) \neq 0$. There exists an element $\gamma \in \mathrm{GF}(q^2)^\times$ with $\mathrm{tr}(\gamma) = 0$ and $\beta + \gamma \in \mathrm{GF}(q)^\times \eta$.*

Proof. We define $t := \mathrm{tr}(\beta)\,\mathrm{tr}(\eta)^{-1}$ and set $\gamma := t\eta - \beta$. Then we have $\mathrm{tr}(\gamma) = t\,\mathrm{tr}(\eta) - \mathrm{tr}(\beta) = 0$, since tr is $\mathrm{GF}(q)$-linear. Furthermore $t^q = \mathrm{tr}(\beta)^q\,\mathrm{tr}(\eta)^{-q} = (\beta + \beta^q)^q(\eta + \eta^q)^{-q} = \mathrm{tr}(\beta)\,\mathrm{tr}(\eta)^{-1} = t$, thus $t \in \mathrm{GF}(q)^\times$ and $\beta + \gamma = t\eta \in \mathrm{GF}(q)^\times \eta$. □

Lemma 92. *Let $\beta \in \mathrm{GF}(q^2)^\times \setminus \mathrm{GF}(q)$ and $\alpha \in \mathrm{GF}(q^2)$ such that $\nu(\alpha, \beta) \in \mathrm{SU}(3,q)$. If $q \equiv 2$ mod 3, then the cardinality of*

$$\{\nu(\alpha,\beta)^{\Delta^i} \mid i \in \mathbb{N}\}$$

is $(q+1)/3$, and $q^2 - 1$ otherwise.

Proof. We have $\nu(\alpha,\beta)^{\Delta^i} = \nu(\alpha\omega^{i(q-2)}, \beta\omega^{-i(q+1)})$. The cardinality of the defined set is equal to the smallest natural number $k \in \mathbb{N}$ such that $k(q-2) \equiv -k(q+1) \bmod q^2 - 1$. Let $q \equiv 2 \bmod 3$. Then $q - 2, q + 1 \equiv 0 \bmod 3$ and thus $3|\gcd(q-2, q+1)$ and, since $3|q^2 - 1$, the cardinality of the set is $(q^2-1)/3$. On the other hand we assume that $q \not\equiv 2 \bmod 3$. Then $\gcd(q-2, q+1) = 1$, thus $k = q^2 - 1$. □

The following two theorems show that we can reduce the number of relations in $R(2)$ to 3 relations, if $q \not\equiv 2 \bmod 3$, and 7 relations, otherwise.

Theorem 93 (Presentation of $\mathrm{SU}(3,q)$, [LGOB19], page 14)**.** *Suppose that $q \not\equiv 2$ mod 3. Let $\beta_0 = \omega\zeta$. Pick $\alpha_0 \in \mathrm{GF}(q^2)$ such that $\alpha_0^{q+1} = -\mathrm{tr}(\beta_0)$. By Lemma 91 there exists γ_0 with $\mathrm{tr}(\gamma_0) = 0$ and $\beta_0 + \gamma_0 \in \mathrm{GF}(q)^\times \omega^{-1}\zeta$.*

Let $\nu_0 = \nu(\alpha_0, \beta_0), \tau_0 = \nu(0, \gamma_0)$ and $\hat{U} = \{\nu_0, \tau_0, \nu_0\tau_0\}$. If $R(2) = \{P(u) \mid u \in \hat{U}\}$, then G is isomorphic to $\mathrm{SU}(3,q)$.

Proof. Again we define V as in Definition 88 and know that if $V = U \setminus \{1\}$, then the result follows. We define

$$U_i := \{\nu(\alpha,\beta) \mid \beta \in \mathrm{GF}(q)^\times \omega^{-i}\zeta, \alpha^{q+1} = \mathrm{tr}(\beta)\} \subset U$$

for $i \in \{0, \ldots, q\}$. Then the U_i are disjoint and it follows that

$$\nu(\alpha,\beta)^\Delta = \nu(\alpha\omega^{q-2}, \beta\omega^{-(q+1)}) \tag{6.5}$$

and for $\beta \in \mathrm{GF}(q)^\times \omega^{-i}\zeta$ we obtain that $\beta\omega^{-(q+1)} \in \mathrm{GF}(q)^\times \omega^{-i}\zeta$, since $\omega^{-(q+1)} \in \mathrm{GF}(q)^\times$. Thus each U_i is normalised by $\langle\Delta\rangle$.

There are $q - 1$ elements in U_0 (since $\mathrm{tr}(\beta) = a\,\mathrm{tr}(\zeta) = 0$ for $\beta \in \mathrm{GF}(q)^\times\zeta$, $a \in \mathrm{GF}(q)^\times$ and thus $\alpha = 0$) and $q^2 - 1$ elements in every U_i for $i \in \{1, \cdots, q\}$ (see

Lemma 92) and since the sets are disjoint, we have $|\cup_{i=0}^{q} U_i| = |U \setminus \{1\}|$. Hence the sets U_i form a partition on $U \setminus \{1\}$.

Let $i := 0$. We can deduce from Equation 6.5 that the order of $\{\tau_0^{\Delta^i} \mid i \in \mathbb{N}\}$ is $q-1$. Since $\mathrm{tr}(\gamma_0) = 0$, we obtain that $\tau_0 \in U_0$. Knowing that U_0 and V are closed under conjugation (see Lemma 90) it follows that $\{\tau_0^{\Delta^i} \mid i \in \mathbb{N}\} \subseteq U_0$. Since both sets have the same order, they are already equal. Thus $U_0 \subseteq V$.

Now we assume $i := 1$. We obtain

$$|\{(\nu_0\tau_0)^{\Delta^i} \mid i \in \mathbb{N}\}| = q^2 - 1$$

with Lemma 92 and since $\nu_0\tau_0 = \nu(\alpha_0, \beta_0 + \gamma_0)$ and $\beta_0 + \gamma_0 \in \mathrm{GF}(q)^\times \omega^{-1}\zeta$, we have $\nu_0\tau_0 \in U_1$. Similarly to the first case we can follow that $\{(\nu_0\tau_0)^{\Delta^i} \mid i \in \mathbb{N}\} \subseteq U_1$ and, for reasons of cardinality, both sets are equal.

Now let $i \in \{1, \ldots, q-1\}$ and assume that $U_i \subset V$. We set $\eta := \omega^{-i}\zeta$ and, since $\mathrm{tr}(\eta) \neq 0 \neq \mathrm{tr}(\beta_0)$, we can apply Lemma 91. We obtain that there exists an element $\gamma \in \mathrm{GF}(q^2)^\times$ such that $\beta_0 + \gamma \in \mathrm{GF}(q)^\times \omega^{-i}\zeta$ and $\mathrm{tr}(\gamma) = 0$.

By Lemma 11 it follows that there exist $q-1$ elements $\gamma \in \mathrm{GF}(q^2)^\times$ such that $\mathrm{tr}(\gamma) = 0$. Since $|U_0| = q-1$ we have $\nu(0, \gamma) \in U_0 \subseteq V$. Further we obtain that $\gamma \in \mathrm{GF}(q)^\times \zeta$.

Lemma 90 states that $\nu_0\nu(0,\gamma) \in V$ if and only if $(\nu_0)_R\nu(0,\gamma)_L \in V$ (see also Lemma 86). Hence we can derive that $(\nu_0)_R\nu(0,\gamma)_L = \nu(-\alpha_0\beta_0^{-1}, \beta_0^{-1})\nu(0,\gamma^{-1}) = \nu(-\alpha_0\beta_0^{-1}, \beta_0^{-1} + \gamma^{-1}) \in V$.

Furthermore $\beta_0\zeta \in \mathrm{GF}(q)^\times\omega\zeta$ and thus $\beta_0^{-1} + \gamma^{-1} = (\beta_0+\gamma)(\beta_0\gamma)^{-1} \in \mathrm{GF}(q)^\times\omega^{-(i+1)}\zeta$. Then $\nu(-\alpha_0\beta_0^{-1}, \beta_0^{-1} + \gamma^{-1}) \in U_{i+1}$ and since Δ normalises U_{i+1} and

$$|\{\nu(-\alpha_0\beta_0^{-1}, \beta_0^{-1} + \gamma^{-1})^{\Delta^i} \mid i \in \mathbb{N}\}| = q^2 - 1$$

(see Lemma92), it follows that $U_{i+1} \in V$.

Consequently $V = U \setminus \{1\}$ and the result follows. □

Corollary 94 ([LGOB19], page 15)**.** *Suppose that $q \equiv 2$ mod 3. Let $\beta_0 = \omega\zeta$. For $0 \leq i \leq 2$ pick $\alpha_i \in \omega^i(\mathrm{GF}(q^2)^\times)^3$ such that $\alpha_i^{q+1} = -\mathrm{tr}(\beta_0)$. By Lemma 91 there exists $\gamma_0 \in \mathrm{GF}(q^2)^\times$ with $\mathrm{tr}(\gamma_0)$ and $\beta_0 + \gamma_0 \in \mathrm{GF}(q)^\times\omega^{-1}\zeta$.*

Let $\nu_i = \nu(\alpha_i, \beta_0), \tau_0 = \nu(0, \gamma_0)$ and $\hat{U} = \{\nu_i, \tau_0, \nu_i\tau_0 \mid 0 \leq i \leq 2\}$. If $R(2) = \{P(u) \mid u \in \hat{U}\}$, then G is isomorphic to $\mathrm{SU}(3,q)$.

Proof. Let $\alpha_0 \in \mathrm{GF}(q^2)$ such that $\nu(\alpha_0, \beta_0) \in \mathrm{SU}(3,q)$. Then we obtain that $\nu(\alpha_1, \beta_0)$ and $\nu(\alpha_2, \beta_0)$ are matrices in $\mathrm{SU}(3,q)$ for $\alpha_1 := \alpha\omega^{q-1}$ and $\alpha_2 := \alpha\omega^{2(q-1)}$. Since $q - 1 \equiv 1 \bmod 3$, ω^{q-1} is not a cube in $\mathrm{GF}(q^2)^\times$ and the α_i lie in different cosets of $(\mathrm{GF}(q^2)^\times)^3$ in $\mathrm{GF}(q^2)^\times$. Possibly after swapping the indices, we obtain the α_i of this theorem.

We define the U_i for $i \in \{0, \ldots, q\}$ as in Theorem 93. Now it follows with Lemma 92, that the action of Δ on the U_i divides the set into three orbits for $i > 0$. For two matrices $\nu(\alpha,\beta), \nu(\gamma,\delta) \in U_i$ those matrices are in one orbit if and only if α and γ are in the same coset of $(\mathrm{GF}(q^2)^\times)^3$.

Now we follow the proof of Theorem 93 and obtain the result. □

We have obtained short presentations for the special unitary group $\mathrm{SU}(3,q)$. For completeness, we cite the presentations for the remaining special cases.

Theorem 95 ([LGOB19], page 15)**.** *A presentation for* $\mathrm{SU}(3,3)$ *is given by*

$$\{\nu,\tau,\Delta,A \mid \nu^3=1,\ A^2=1,\ \Delta^{-1}\nu^{-1}\Delta^{-1}\tau^{-1}\nu\Delta^2\nu^{-1}=1,\ \Delta^{-1}\nu\Delta^{-1}\tau^{-1}\nu^{-1}\Delta^2\nu=1,\\ \tau A\Delta^{-2}(\tau A)^2=1,\ \Delta\tau^{-1}\nu^{-1}A\Delta\tau^{-1}\nu\Delta A\nu\tau^{-1}A=1\}.$$

Theorem 96 ([LGOB19], page 15)**.** *A presentation for* $\mathrm{SU}(3,5)$ *is given by*

$$\{\nu,\tau,\Delta,A \mid \nu^5=1,\ \Delta\tau^2\Delta^{-1}\tau=1,\ \Delta^2\nu^2\Delta^{-2}\nu^{-1}=1,\ \Delta^5A\Delta A=1,\ \Delta^{-1}\nu A\nu^{-2}A\nu\Delta A=1,\\ \Delta\nu\Delta^{-1}\tau^{-1}\nu^{-1}\Delta\nu^{-1}\Delta^{-1}\nu=1,\ \nu^{-1}A\tau^{-1}\nu^{-1}A\Delta^{-1}\nu^2A\Delta\nu^{-1}A\Delta\tau^{-1}=1\}.$$

Theorem 97 ([LGOB19], page 15)**.** *A presentation for* $\mathrm{SU}(3,2)$ *is given by*

$$\{\nu,\nu',\Delta,A \mid a:=[\nu,A],\ b:=a^{2\nu},\ a^\nu=b^{-1},\ b^\nu=a\Delta,\ a^{\nu'}=aba,\\ b^{\nu'}=ab\Delta,\ \nu^2=\nu'^2=[\nu,\nu'],\ A=\nu^2a^2b\}.$$

Theorem 98 ([LGOB19], page 16)**.** *Assume that a presentation for* $\mathrm{SU}(3,q)$ *is given. Then a presentation for* $\mathrm{PSU}(3,q)$ *is obtained by adding the relation* Δ^{q^2-1}*.*

Proof. We have shown in Lemma 66 that the centre of $\mathrm{SU}(3,q)$ contains all matrices of the form $a\mathrm{I}_3$ with $a\in\mathrm{GF}(q^2)$ and $a^3=1$. Thus $|\mathrm{Z}(\mathrm{SU}(3,q))|=|\{a\in\mathrm{GF}(q^2)\mid a^3=1\}|=\gcd(q+1,3)$ and the result follows. □

7. Implementation

The presentations given in the previous chapters are implemented in GAP and the code and documentation can be found in [Ahr]. For each presentation there exists a function that takes a varying number of matrices $M_1, \ldots, M_k$ (or other elements that may be multiplied and inverted) and a natural number $d \in \mathbb{N}$ as arguments. The number d specifies the field over which the matrices are defined or the degree of the group. The function checks whether the matrices satisfy the relations of the particular presentation and returns `true` if the group $\langle M_1, \ldots, M_k \rangle$ is isomorphic to the presented group and `false` otherwise.

As an example, we look at the signature of the function for the presentation of the group $\mathrm{SU}(3, q)$ with $q \neq 2, 3, 5$. It is of the form

```
Bool : IsSU3( v, tau, delta, t, field ).
```

The function `IsSU3` checks whether `v, tau, delta` and `t` generate a group that is isomorphic to $\mathrm{SU}(3, q)$ where q equals `field`.

For the implementation of the presentations it is crucial to consider that the given matrices $M_1, \ldots, M_k$ are possibly of large dimension. If the matrix dimensions are large, then a single matrix multiplication might already be a very expensive computation. Additionally, we need to keep in mind that memory space is limited. These two limitations sometimes oppose each other. I analyse this conflict in the next sections.

7.1. Runtime Optimisation

There are two different approaches for optimising the runtime of the code. The first approach is to look at the problem from the mathematical side and try to reduce the length of the presentations (see Section 2.2). We have done this in the previous chapters successfully by obtaining short presentations.

The second approach is to analyse the problem from a computational viewpoint. I give an example for efficient computational optimisation in this section.

7.1.1. Square-and-Multiply Algorithm

The Square-and-Multiply Algorithm is a way to efficiently calculate powers of an arbitrary element a. The naive way to obtain a^n would be to compute

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ times}}$$

for $n \in \mathbb{N}$. Thus we need $n-1$ multiplications to calculate a^n and the program has linear runtime. In our case, the element a is a - possibly huge - matrix and thus linear runtime is not acceptable.

Another way to compute a^n is by looking at the binary representation of n. Let $n = (b_k \dots b_0)_2$. Then we obtain $a^n = a^{2^{b_k}} \cdots a^{2^{b_0}}$. Since $b_i \in \{0, 1\}$, we can calculate squares of a iteratively $(a, a^2, a^4, a^8, \dots)$ and multiply them together to obtain a^n.

See the code for the exact procedure of the algorithm.

```
# Calculates a^n in an efficient way by using square and multiply.
SquareAndMultiply := function( a, n )
    local exponents, current, result, i;

    # Calculates the binary representation of n and stores it in a list.
    exponents := CoefficientsQadic( n, 2 );

    current := a;
    result := a^0;

    # Calculates powers 2^i of a by calculating squares of a iteratively.
    # Multiplies the result by a^(2^i) if exponents[i] = 1.
    for i in [ 1 .. Length( exponents ) ] do
        if ( exponents[i] = 1 ) then
            result := result * current;
        fi;

        # Set current = a^(i+1)
        current := current^2;
    od;

    return result;
end;
```

The runtime of the Square-and-Multiply Algorithm is logarithmic since we need at most $2\log_2(n)$ multiplications to compute a^n for any element a. Refer to books like [Ott12] for background knowledge about measuring the runtime of an algorithm.

I have applied the idea of this algorithm several times to improve the efficiency of my code, e.g. for the presentation of the symmetric group. Relations of the presentation are V^n and $(UU^{V^j})^2$ for $2 \leq j \leq n/2$, see Theorem 28. In my code, I compute which powers V^j I have to remember in order to calculate V^d as a product of those powers. Then, I obtain V^j by multiplying $V^{j-1} \cdot V$ (since I need to obtain every V^j for $2 \leq j \leq n/2$) and multiply them directly to obtain V^d.

```
# First we calcate which values v^j should be remembered for the
# calculation of v^d.
powersToRemember := CoefficientsQadic( d, 2 );
```

```
for i in [ 1 .. Length( powersToRemember ) ] do
    if powersToRemember[i] <> 0 then
        powersToRemember[i] := 2^(i-1);
    fi;
od;

# Now we calculate v^j and remember it if necessary.
remember[1] := v;
remember[2] := e; # This is the neutral element of multiplication.

for i in [ 2 .. (d - (d mod 2))/2 ] do
    remember[1] := remember[1] * v;
    if ( i in powersToRemember ) then
        remember[2] := remember[2] * remember[1];
    fi;
    if ( ( u * u^(remember[1]) )^2 <> e ) then
        ...
    fi;
od;
```

7.2. Memory Consumption

In many of the obtained presentations specific generator products are used multiple times in various relations, for instance at the relations of the presentation of $\mathrm{SU}(3,5)$ in Theorem 96. For example, the matrices $\Delta^2, \nu^2, \nu^{-1}, \tau^{-1}$ and Δ^{-1} are frequently used and recomputation is expensive. But storing every reusable matrix is likely to cause memory problems.

Hence, it is important to consider in advance whether to store a matrix product or recompute it later.

Here again, there exists a way to optimise the storage usage. Assume a presentation that contains the relations $y^{-1}z^3 = 1$, $x^4y^{-1}z = 1$, $x^2yz = 1$ and $yz^2 = 1$. Note that I randomly chose these relations. It makes sense to verify the relations in such an order that the memory usage is minimised. See Figure 7.2 for a possible order of verification. The left-most column indicates the steps of the program, the right-most column states the relation that is being verified in this particular step and the columns in between illustrate the memory allocation.

After sorting the relations to obtain an optimal order, the function with the largest memory consumption needed to save a maximum of 12 matrices at the same time. The computation time was not affected by those changes. The memory consumption of the functions for the presentations of $\mathrm{SU}(3,q)$, $\mathrm{PSU}(3,q)$ and $\mathrm{SL}(2,q)$ are listed in Figure 7.2 and Figure 7.2 examplarily.

Time	Slot 1	Slot 2	Slot 3	Slot 4	Relation
0	x	y	z		
1	x^2	y	z		$x^2yz = 1$
2	x^4	y	z	y^{-1}	$x^4y^{-1}z = 1$
3	z^2	y	z	y^{-1}	$yz^2 = 1$
4	z^3			y^{-1}	$y^{-1}z^3 = 1$

Figure 7.1.: Examplary program flow and its memory allocation. The column *Time* denotes the steps of the program, the columns *Slot x* contain the current allocation of the memory space and the column *Relation* denotes which relation is checked.

Group	Memory (Number Of Matrices)
$\mathrm{SU}(3, q)$	12
$\mathrm{PSU}(3, q)$	12
$\mathrm{SU}(3, 2)$	9
$\mathrm{SU}(3, 3)$	8
$\mathrm{SU}(3, 5)$	9

Figure 7.2.: Memory consumption of the different presentations of $\mathrm{SU}(3, q)$ and $\mathrm{PSU}(3, q)$. The number indicates the maximum number of matrices stored simultaneously.

Presentation for	Memory (Number of Matrices)
$q = p^e$, p odd and $e > 1$	9
$q = p^e$, p odd and $e > 1$ and $q \equiv 3 \bmod 4$	5
p an odd prime and $p \equiv 1 \bmod 3$	7
p an odd prime and $p \not\equiv 1 \bmod 3$	6
$q = 2^e$	3
$q = 2$	2

Figure 7.3.: Memory consumption of the different presentations of $\mathrm{SL}(2, q)$. The number indicates the maximum number of matrices stored simultaneously.

This thesis has obtained *short* presentations for the symmetric group, the group of signed permutation matrices of determinant 1, the special linear group of degree 2, the special unitary group of degree 3 and related groups. The implementation of those presentations shows that only a limited number of matrix multiplications and memory space is needed. Hence, we have obtained a way to verify group isomorphisms for the analysed groups with an acceptable computational effort, and we can apply the implementations in the *matrix group recognition project*.

In future work it would be interesting to obtain and implement *short* presentations for the other finite classical and related groups (see [LGOB19]) to extend the number of groups for which we can test for isomorphy.

Bibliography

[Ahr] Emma Ahrens. *GAP Code of Presentations of Some Classical Groups*. Accessed: October 1, 2019. URL: https://github.com/emmakatherina.

[Beu94] Albrecht Beutelspacher. *Lineare Algebra*. 8th ed. Springer Spektrum, 1994.

[Bou13] Florian Bouyer. "Presentations of Groups". In: (2013).

[CR80] C. M. Campbell and E. F. Robertson. "A Deficiency Zero Presentation for SL(2, p)". In: *Bulletin of the London Mathematical Society* 12.1 (Jan. 1980), pp. 17–20.

[CRW90] C. Campbell, E. Robertson and P. Williams. "On presentation of $PSL(2, p^n)$". In: *Journal of The Australian Mathematical Society* 48 (Apr. 1990).

[Fra66] J. S. Frame. "Orthogonal Group Matrices of Hyperoctahedral Groups". In: (1966).

[GAP] The GAP Group. *GAP - Groups, Algorithms and Programming*. Version 4.10. 2019.

[Gur+08] Robert Guralnick et al. "Presentations of finite simple groups: A quantitative approach". In: *Journal of The American Mathematical Society - J AMER MATH SOC* 21 (July 2008), pp. 711–774. DOI: 10.1090/S0894-0347-08-00590-0.

[HEO05] Derek F. Holt, Bettina Eick and Eamonn A. O'Brien. *Handbook of Computational Group Theory*. CRC Press, 2005.

[HS11] Alexander Hulpke and Ákos Seress. "Short presentations for three-dimensional unitary groups". In: *Journal of Algebra* 245 (2011).

[Hup67] B. Huppert. *Endliche Gruppen 1*. Springer Verlag, 1967.

[Joh90] D. L. Johnson. *Presentations of Groups*. Cambridge University Press, 1990.

[Ker71] Adalbert Kerber. *Representationsof Permutation Groups 1*. Springer Verlag, 1971.

[Lee01] C. R. Leedham-Green. "The computational matrix group project". In: *Groups and computation, III (Columbus, OH, 1999)*. Vol. 8. Ohio State Univ. Math. Res. Inst. Publ. de Gruyter, Berlin, 2001, pp. 229–247.

[LGOB09] C. R. Leedham-Green and E. A. O'Brien. "Constructive recognition of classical groups in odd characteristic". In: *Journal of Algebra* 322 (2009).

[LGOB19] C. R. Leedham-Green and E. A. O'Brien. "Presentations on standard generators for classical groups". 2019.

[Moo96] E. H. Moore. *Concerning the abstract groups of order $k!$ and $\frac{1}{2}k!$ holohedrically isomorphic with the symmetric and the alternating substitution groups on k letters*. London Math. Soc., 1896.

[Nie18] Alice Niemeyer. *Vorlesungsskript Lineare Algebra, Computeralgebra und Algebra*. RWTH Aachen University, 2016-2018.

[Nie19] Alice Niemeyer. *Vorlesungsskript Gruppentheorie*. RWTH Aachen University, 2018/19.

[OBr19] E.A. O'Brien. "Towards effective algorithms for linear groups". In: (Sept. 2019).

[Ott12] Thomas Ottmann. *Algorithmen und Datenstrukturen*. Spektrum Akademischer Verlag, 2012.

A. Original Presentations of $\mathrm{SL}(2,q)$

In this chapter we list a generating set and presentations for $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$ that are obtained from [CRW90] and [CR80].

The following theorem lists four matrices that generate the special linear group of degree 2. The subsequent theorems give different presentations on the generating set in Theorem 99 for special cases of $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$. Please refer to [CRW90] or [CR80] for proofs of the correctness of those presentations.

Theorem 99 ([CRW90], Chapter 2)**.** *Let $\omega \in \mathrm{GF}(q)$ be a primitive element and*

$$w := \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ x := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ y := \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix},\ z := \begin{pmatrix} \omega & \omega^{-1} \\ 0 & \omega^{-1} \end{pmatrix}.$$

Then $w, x, y, z \in \mathrm{SL}(n,q)$ and those matrices generate $\mathrm{SL}(n,q)$.

Proof. We will show that every matrix in Theorem 53 can be generated by the matrices w, x, y and z by following [LGOB19], Chapter 3. We have $\tau = x$ and $z^{-1}x = \begin{pmatrix} \omega^{-1} & -\omega^{-1} \\ 0 & \omega \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \delta$. Also $wx = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = U$. Thus $\langle \tau, \delta, U \rangle \subseteq \langle w, x, y, z \rangle$.

On the other hand $w, x, y, z \in \mathrm{SL}(2,q)$ and thus the generated group is isomorphic to $\mathrm{SL}(2,q)$. □

Theorem 100 (Presentation of $\mathrm{PSL}(2,q)$, [CRW90], Theorem 2.2)**.** *We assume the requirements listed in Remark 54. Then $\mathrm{PSL}(2,q)$ has the presentation*

$$\begin{aligned}\{w, x, y, z \mid\ & w^3 = (wx)^2 = (wz)^2 = (wyz)^3 = x^p = y^p = z^{(q-1)/2} = [x, s_1] = [y, s_2] \\ & = s^{\mu(t)} = s^{t\mu(t)} = s^{f(t)} = s^{tf(t)} = 1\},\end{aligned}$$

where $s_{2i} := z^i x z^{-i}$ and $s_{2i+1} := z^i y z^{-i}$ for $1 \in \mathbb{N}$.

Theorem 101 (Presentation of $\mathrm{PSL}(2,q)$ for $q \equiv 3 \bmod 4$, [CRW90], Theorem 2.4)**.** *We assume the requirements defined in Remark 54 and $q \equiv 3$ mod 4. Then $\mathrm{PSL}(2,q)$ may be presented by*

$$\begin{aligned}\{w, x, z \mid\ & w^3 = (wx)^2 = (wz)^2 = s^{\mu(t)} = [x, z^l x z^{-l}] = 1, \\ & z^{\frac{q-1}{2}} = x^p,\ z^{\lfloor \frac{k}{2} \rfloor} x z^{-\lfloor \frac{k}{2} \rfloor} = x z^{(-1)^k l} x^{-1} z^{(-1)^{k+1} l}\},\end{aligned}$$

where $l := \frac{q+1}{4}$ and $s_{2i} := z^i x z^{-i}$ and $s_{2i+1} := z^i y z^{-i}$.

Theorem 102 (Presentation of $\mathrm{SL}(2,2^e)$, [CRW90], Theorem 3.2)**.** *We assume the requirements as defined in Remark 54 with the exception that p is now equal to 2. Then* $\mathrm{SL}(2,2^e)$ *has the presentation*

$$\{w,x,z \mid w^3=(wx)^2=(wz)^2=z^{q-1}=x^2=s^{\mu(t)}=s^{f(t)}=1\}.$$

Observe that the s_i for the relation $s^{\mu(t)}=1$ are not defined. Thus $s^{\mu(t)}=\prod_{i=0}^{k}(\tau^{\delta^k})^{\tilde{a_i}}$ for the minimal polynomial $\mu : \mathrm{GF}(q) \to \mathrm{GF}(q), x \mapsto \sum_{i=0}^{k} a_i x^i$ over $\mathrm{GF}(p)$.

Theorem 103 (Presentation of $\mathrm{SL}(2,p)$, [CR80], Chapter 3)**.** *We assume the requirements defined in Remark 54 and define $l := \lfloor p/3 \rfloor$. Then* $\mathrm{SL}(2,p)$ *has the presentation*

$$\{x,y \mid x^2=(xy)^3,\ (xy^4xy^{(p+1)/2})^2y^px^{2l}=1\}.$$

Acknowledgements

First and foremost I would like to express my deep gratitude to Prof. Dr. Alice C. Niemeyer and Dominik Bernhardt M.Sc. for their time, support and patience while supervising this work. Thanks to Prof. Dr. Wilhelm Plesken for kindly agreeing to read and grade my bachelor thesis.

I would also like to thank my friends that they were such good listeners and stood by me through stressful episodes. ;)

Special thanks to my family for encouraging and motivating me relentlessly and making this education possible for me!

Zentrales Prüfungsamt/Central Examination Office

Eidesstattliche Versicherung
Statutory Declaration in Lieu of an Oath

Name, Vorname/Last Name, First Name

Matrikelnummer (freiwillige Angabe)
Matriculation No. (optional)

Ich versichere hiermit an Eides Statt, dass ich die vorliegende Arbeit/Bachelorarbeit/ Masterarbeit* mit dem Titel
I hereby declare in lieu of an oath that I have completed the present paper/Bachelor thesis/Master thesis* entitled

selbstständig und ohne unzulässige fremde Hilfe (insbes. akademisches Ghostwriting) erbracht habe. Ich habe keine anderen als die angegebenen Quellen und Hilfsmittel benutzt. Für den Fall, dass die Arbeit zusätzlich auf einem Datenträger eingereicht wird, erkläre ich, dass die schriftliche und die elektronische Form vollständig übereinstimmen. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.
independently and without illegitimate assistance from third parties (such as academic ghostwriters). I have used no other than the specified sources and aids. In case that the thesis is additionally submitted in an electronic format, I declare that the written and electronic versions are fully identical. The thesis has not been submitted to any examination body in this, or similar, form.

Ort, Datum/City, Date

Unterschrift/Signature

*Nichtzutreffendes bitte streichen

*Please delete as appropriate

Belehrung:
Official Notification:

§ 156 StGB: Falsche Versicherung an Eides Statt
Wer vor einer zur Abnahme einer Versicherung an Eides Statt zuständigen Behörde eine solche Versicherung falsch abgibt oder unter Berufung auf eine solche Versicherung falsch aussagt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
Para. 156 StGB (German Criminal Code): False Statutory Declarations
Whoever before a public authority competent to administer statutory declarations falsely makes such a declaration or falsely testifies while referring to such a declaration shall be liable to imprisonment not exceeding three years or a fine.
§ 161 StGB: Fahrlässiger Falscheid; fahrlässige falsche Versicherung an Eides Statt
(1) Wenn eine der in den §§ 154 bis 156 bezeichneten Handlungen aus Fahrlässigkeit begangen worden ist, so tritt Freiheitsstrafe bis zu einem Jahr oder Geldstrafe ein.
(2) Straflosigkeit tritt ein, wenn der Täter die falsche Angabe rechtzeitig berichtigt. Die Vorschriften des § 158 Abs. 2 und 3 gelten entsprechend.
Para. 161 StGB (German Criminal Code): False Statutory Declarations Due to Negligence
(1) If a person commits one of the offences listed in sections 154 through 156 negligently the penalty shall be imprisonment not exceeding one year or a fine.
(2) The offender shall be exempt from liability if he or she corrects their false testimony in time. The provisions of section 158 (2) and (3) shall apply accordingly.

Die vorstehende Belehrung habe ich zur Kenntnis genommen:
I have read and understood the above official notification:

Ort, Datum/City, Date

Unterschrift/Signature