Utrecht University

The first Janko group J_1: simplicity and formalization

Author: Roxy van de Kuilen
Supervisor: Dr. Johan Commelin

Bachelor Thesis

Faculteit Bètawetenschappen
Mathematics

June 14, 2024

Abstract

In this thesis, we will examine the first Janko group J_1. It is a sporadic group, which means that it is a finite and simple group. The main goal of this thesis is to prove the simplicity of a finite group that contains an involution i such that the centralizer of i is isomorphic to $\langle i \rangle \times A_5$, that has no subgroups of index 2 and in which all Sylow 2-subgroups are abelian. As it turns out, the group J_1 satisfies these properties. Although the theorem has already been given and proven by Zvonimir Janko in 1965, we give an extensive and complete proof, which leaves few gaps for the reader to fill. Parts of the proof of the theorem will also be formalized in the proof assistant Lean. We want to emphasize that we will not prove that J_1 does possess the properties of the theorem in this thesis; we will only prove that groups that do satisfy them, are simple.

Contents

Introduction

Group theory is a large subject of mathematics. A fairly big branch of group theory focuses on finite simple groups. In this thesis, we will encounter one of the many finite simple groups, namely J_1. The group, named the first Janko group, is a sporadic group, which makes it an interesting and important group in mathematics.

In Chapter 1, we will briefly cover the history of the classification of finite simple groups. We will give the classification theorem, as well as some information about how it came into existence. Consequently, we will introduce all sporadic groups with some background information. This will provide us with some information about the value of this analysis and thesis.

Next, we will focus on the first Janko group, our main interest. Before we can prove results about this group, we need to examine how it is build. This will happen in Chapter 2. We will look at three different construction methods, the first originally being given by Zvonimir Janko. After that, we will give a representation of the Janko group given by Rob Curtis, followed by the definition of J_1 found in Robert Wilson's book.

In Chapter 3, we will give an extensive proof of a theorem given by Zvonimir Janko in the article where he first defined J_1. As it is a theorem about a general finite group G, the Janko group does not appear explicitly in the theorem. It states that a finite group G possessing three certain qualities has to be a simple group. In his article, Zvonimir Janko proved the theorem, after which he proved that J_1 satisfies the conditions of the theorem, whereby proving the simplicity of J_1. We want to make it clear that we will only prove the theorem in this thesis. For the proof that J_1 does indeed satisfy the properties, we refer to Janko's article *A New Finite Simple Group with Abelian Sylow 2-Subgroups and Its Characterization* [6].

In the last chapter, Chapter 4, we will give some information about the programming language Lean. It is a fairly new proof assistant, developed in 2013, with the latest version, Lean 4, released in 2021. In addition to giving the proof of the theorem on paper in Chapter 3, we formalized parts of this proof in Lean 4.

Before we begin with Chapter 1, I would like to express my gratitude to dr. Johan Commelin for his support, advice and answers to my questions. Without his help, I would not have progressed as much in Lean as I have now, for which I am endlessly grateful.

Chapter 1

Classification of finite simple groups

In group theory, there are a lot important theorems. Lagrange's Theorem or the Sylow Theorems are examples of well-known results. One particular big theorem is the Classification Theorem for Finite Simple Groups, which we will give after some history on the theorem. The theorem is commonly abbreviated as *CFSG* [2, p. 3]. Before we can start that section, we give the definition of a simple group to know what condition these groups apparently satisfy.

Definition 1.0.1. *[3, p. 102] A non-trivial group G is called simple if the only normal subgroups are the trivial ones; the trivial subgroup and G itself.*

Recall that a subgroup H of G is *normal* if and only if $g^{-1}Hg \subseteq H$ for all $g \in G$ [3, p. 82].

An elementary example of a simple group is a group G of prime order. One can easily see this using Lagrange's Theorem, as it implies that G only has the trivial group and itself as subgroup. These two groups are normal subgroups in every group. Therefore, such groups G with prime order will always be simple. [3, p. 102]

1.1 History of CFSG

In 1832, normal subgroups were introduced by Évariste Galois [1, p. 315], who is seen as the founder of group theory. Since then, group theory has evolved into an important branch of mathematics. After Galois' first notion of normal subgroups, multiple mathematicians came forward with new results in the nineteenth century. For example, in 1861, Émile Mathieu introduced the first two Mathieu groups, nowadays known as M_{11} and M_{12} [2, p. 1]. Twelve years later, he published another paper containing the constructions of the other three Mathieu groups, M_{22}, M_{23} and M_{24} [2, p. 1]. In 1870, Camille Jordan mentioned the importance of simple groups, as well as stated some that were already found; the alternating groups and the projective special linear groups [1, p. 315]. Then, in 1892, Otto Hölder published a paper proving that the order of a nonabelian finite simple group must consist of the product of at least four primes. He was able to prove this using only the Pigeonhole Principle and Sylow's Theorems, which were proven in 1872 [1, p. 315]. In his article, Hölder also asked for the classification of finite simple groups [1, p. 315]. This became known as *The Hölder Program*, which consists of two steps; classifying all finite simple groups, after which mathematicians should find all ways to form other groups out of these finite simple groups [3, p. 103]. This last step is also known as the *extension problem* [3, p. 104]. For some decades, no real progress was made on the Hölder Program. That is, until 1965, the discovery of the finite simple group J_1 by Zvonimir Janko. This caused a renewed interest in finite simple groups, which resulted in the discovery of twenty more finite simple groups in just ten years [1, p. 332]. In 1983, Daniel Gorenstein declared the Classification Project finished [1, p. 340], even though some articles containing relevant results had yet to be published. Thus, nearly a hundred years after its introduction, the proof of the following theorem is completed, resulting in the completion of the first step of The Hölder Program.

Theorem 1.1.1 (Classification Theorem for Finite Simple Groups)**.** *[2, p. 3] Every finite simple group is isomorphic to one of the following groups:*

- ◇ *a cyclic group of prime order;*
- ◇ *an alternating group of at least degree 5;*
- ◇ *a classical group;*
- ◇ *one of the 26 sporadic groups.*

In 1989 Michael Aschbacher noticed some flaws in a manuscript on particular groups, whereupon he was determined to fix this [1, p. 341]. In 2004, Aschbacher and Steve Smith published a 1221-page correction, filling this minor gap [4, p. 738]. Such gaps are not uncommon, as multiple gaps have been discovered from the 1980's until now [4, p. 736]. These flaws are sometimes hard to find, as the complete proof of Theorem 1.1.1 currently holds approximately 10000 pages, spread over more than 500 articles [3, p. 103]. And even these articles build onto another 2000 papers and articles [3, p. 103]. This makes the theorem unique in its size, as there is no other individual result with a proof so extensive as Theorem 1.1.1's in mathematics. This is also the reason we will not give any proof or outline.

Since the proof of Theorem 1.1.1 is so long, mathematicians feared that (parts of) it would eventually be lost. Daniel Gorenstein did so too, which is why he proposed an idea to present the proof via a global outline in the eighties. Ronald Solomon and Richard Lyons joined him to write it down in its completeness and simplify large parts of the proof [4, p. 736]. Given the size of the proof, it is not surprising that this project is not completed yet.

After finishing the Classification Theorem, it was time to focus on the next step of the Hölder Program. A more exact description of the extension problem is: when given two groups A and B, we want to describe and understand how to construct all groups G, such that it contains a normal subgroup N with $N \cong A$ and $G/N \cong B$ [3, p. 104]. This turned out to be difficult, maybe even more complicated than the first part of the Hölder Program. In practice, when faced with a finite group, mathematicians mostly deconstruct the problem to a smaller problem about finite simple groups [4, p. 737]. This is where the classification of simple groups becomes truly useful, as it gives us a lot of information we need to solve these smaller questions [4, p. 737]. This method for solving problems in group theory is a successful one; almost all unsolved problems from before 1980 are now solved [4, p. 737]. Finite groups are not only convenient in group theory, they are also applicable in other subject of mathematics [4, p. 737]. This once more shows the importance of the Classification Theorem and finite simple groups.

1.2 Sporadic groups

In Theorem 1.1.1, we have seen that every finite simple group is isomorphic to a member of 3 infinite families or to one of the sporadic groups. Since finite group theory is an important branch of mathematics, we will briefly look at the 26 sporadic groups.

The first sporadic groups to be discovered were the Mathieu groups. As stated before, M_{11} and M_{12} were introduced in 1861 by Émile Mathieu and the construction of the groups M_{22}, M_{23} and M_{24} followed twelve years later in 1873. The latter three are also known as the large Mathieu groups, which makes the first two part of the small Mathieu groups [2, p. 183]. The group M_{11} is the smallest of the five with a cardinality of 7920 [2, p. 202]. The order of M_{24} is $|M_{24}| = 244823040$, by which it is the largest of the Mathieu groups [2, p. 187].

For almost a century, no other sporadic group was discovered. Finally, in 1965 Zvonimir Janko publicated an article on the construction of J_1, the first Janko group [2, p. 2]. In that article, Janko also predicted the existence of the groups J_2 and J_3. The construction of J_2 was later given by Marshall Hall [1, p. 332]. The group J_3 was eventually constructed by Higman and McKay [2, p. 268]. The final Janko group, J_4, was discovered by Zvonimir Janko in 1974 [1, p. 336].

The way the second Janko group was constructed, as a rank 3 permutation group, provided opportunities for other finite simple groups to be discovered. As a result, four groups of similar construction were discovered soon after J_2; the Higman-Sims group HS, the McLaughlin group McL, the Rudvalis group Ru and the Suzuki group Suz [1, p. 332]. The latter was introduced in 1973, the first three were discovered in 1969 [1, p. 336].

Zvonimir Janko inspired three more sporadic groups to be discovered. Both the Held group as the

Lyons group, as well as the O'Nan group were identified after Janko's study of involutions in the sixties [1, p. 332]. The first mentioned, He, is of order 4030387200 and was discovered while the mathematician Dieter Held tried to characterize M_{24} [2, p. 264]. The Lyons group, denoted by Ly, was discovered by Richard Lyons and Charles Sims in 1973 when they tried to classify simple groups with a certain property [2, p. 274]. Sims was also involved in the discovery of the O'Nan group [2, p. 272], which is named after Michael O'Nan. The group has order 460815505920 and J_1 is a subgroup of $O'N$ [2, p. 184,272].

John Conway, a British mathematician, constructed three sporadic groups around 1968 [2, p. 183]. These are called the Conway groups, denoted by Co_1, Co_2 and Co_3 [1, p. 332]. The first group is the biggest of the three, with more than four quintillion elements (which is $4 \cdot 10^{18}$) [2, p. 205]. Both Co_2 and Co_3 are isomorphic to a subgroup of Co_1 [2, p. 211]. Although the Conway groups were discovered after the Higman-Sims group and McLaughlin group, the latter two are contained in Co_2 and Co_3 [2, p. 183].

Somewhere between 1969 and 1971, Bernd Fischer constructed three sporadic groups, which were called the Fischer groups [1, p. 336]. The groups Fi_{22}, Fi_{23} and Fi'_{24} were discovered after Fischer studied 3-transposition groups [1, p. 336]. A 3-transposition group is a group generated by the conjugacy class of involutions, such that the product of any two involutions has order equal to 1, 2 or 3 [2, p. 234]. The group Fi'_{24} is especially interesting, as it plays an important role in the discovery of the baby monster group and monster group.

Fischer dove deeper into the transposition groups after finding the Fischer groups. This led him to the suspicion of the existence of the baby monster group B in 1973 [1, p. 336]. This is a group of order 4154781481226426191177580544000000 [2, p. 260], i.e. more than four decillion elements. Through this enormous group, another, even larger, group M was discovered by Bernd Fischer and Robert Griess in 1974 [1, p. 340]. The monster group, also called the Friendly Giant, contains more than $8 \cdot 10^{53}$ elements [2, p. 251]. In Griess' article proving the existence of the monster group, he divides the sporadic groups in two parts, the groups that are contained in the Friendly Giant and those that do not [5, p. 91].

The last two sporadic groups that we have not spoken about yet are the Thompson group Th and the Harada–Norton group HN. These two groups are subgroups of the monster group [1, p. 336]. The Thompson group however, was already constructed by P. Smith and John Thompson some years before the discovery of the monster group [2, p. 260]. The group HN is named after its discoverers. The group is of order 273030912000000 [2, p. 262].

1.2.1 Happy Family

Robert Giess stated in 1982 that certainly twenty sporadic groups are subgroups of the Friendly Giant, but that it was not yet determined if the first Janko group is contained in M [5, p. 91]. Since then, a proof has been found that J_1 is indeed not a subgroup of the monster group [2, p. 184].

In his article, Giess gives a name to the set of the twenty sporadic groups that are contained in the Friendly Giant; the *Happy Family*. This set consists of the following groups [5, p. 3]:

- ◇ the Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24};
- ◇ the Janko group J_2;
- ◇ the Held group He;
- ◇ the Higman-Sims group HS;
- ◇ the McLaughlin group McL;
- ◇ the Suzuki group Suz;
- ◇ the Conway groups Co_1, Co_2, Co_3;
- ◇ the Fischer groups Fi_{22}, Fi_{23}, Fi'_{24};

- ◇ the Harada-Norton group HN;
- ◇ the Thompson group Th;
- ◇ the baby monster group B;
- ◇ the monster group M.

1.2.2 Pariahs

Since twenty sporadic groups are subgroups of the monster group, there are six sporadic groups that do not. Giess called these groups the *Pariahs* [5, p. 91]. This set consists of the following sporadics [5, p. 3]:

- ◇ the Janko groups J_1, J_3, J_4;
- ◇ the Lyons group Ly;
- ◇ the O'Nan group $O'N$;
- ◇ the Rudvalis group Ru.

For the Lyons group and the Janko group J_4, proving that they are an element of the Pariahs is quite easy. Using Lagrange's Theorem, we can prove that these are not a subgroup of M, since the order of Ly and the order of J_4 are not a divisor of $|M|$. Showing that the other four sporadics are pariahs requires more work, which can be seen in Giess article [5].

Chapter 2

Constructions of the first Janko group

In the following chapters, we will focus on the first Janko group J_1, a group containing 175560 elements [2, p. 267]. As we have seen in Chapter 1, the group is a sporadic group, in particular a pariah. This also means that it is a simple group, which we will prove in the next chapter. Now, we will look at three ways to construct this simple group J_1. We will see a construction given by Zvonimir Janko [6], Rob Curtis [7] and Robert Wilson [2]. These constructions are entirely different, yet they all define the same Janko group.

2.1 Construction by Zvonimir Janko

We will begin with the original construction of J_1 by Zvonimir Janko. He is reportedly the first person to give a construction of the group. In his article, *A New Finite Simple Group with Abelian Sylow 2-Subgroups and Its Characterization* [6], Janko presents the first Janko group as a subgroup of $GL(7, \mathbb{F}_{11})$. He states that J_1 is generated by the following two matrices A and B

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} -3 & 2 & -1 & -1 & -3 & -1 & -3 \\ -2 & 1 & 1 & 3 & 1 & 3 & 3 \\ -1 & -1 & -3 & -1 & -3 & -3 & 2 \\ -1 & -3 & -1 & -3 & -3 & 2 & -1 \\ -3 & -1 & -3 & -3 & 2 & -1 & -1 \\ 1 & 3 & 3 & -2 & 1 & 1 & 3 \\ 3 & 3 & -2 & 1 & 1 & 3 & 1 \end{pmatrix}.$$

In the article, Janko gives and proves Theorem 2.1.1, after which he proves that his definition of J_1 satisfies the properties given in the theorem. Recall that the *centralizer* of an element i is given by the set of all elements that commute with said element, i.e. $C(i) = \{g \in G : ig = gi\}$. Sometimes the centralizer is denoted by $C_G(i)$ to indicate that it is a subgroup of G. We also want to remember the definition of an involution: an element of a group G is called an *involution* if its order equals two. In other words, an involution is its own inverse.

Theorem 2.1.1. *[6, p. 147] Let G be a finite group with the following properties:*

1. *The Sylow 2-subgroups of G are abelian;*
2. *G contains an involution i such that the centralizer $C(i)$ is isomorphic to $\langle i \rangle \times A_5$;*
3. *G has no subgroup of index 2.*

Then G is a simple group.

In his work, Janko also gives characterizations and properties of the group J_1, accompanied by proofs of his claims [6].

2.2 Construction by Rob Curtis

In later works and books, mathematicians use other constructions for the first Janko group. Rob Curtis, for example, gives a definition where J_1 is not generated by two matrices. Curtis claims that the group

$$G = \frac{2^{*11} : PSL(2, \mathbb{F}_{11})}{(\sigma_{018} t_0)^5} \tag{2.1}$$

is isomorphic to J_1 as defined by Zvonomir Janko, or G is the trivial group [7]. If we look at the construction in (2.1), we see that it is constructed from multiple groups. Among others, we see 2^{*11}, the free product of eleven times the cyclic group C_2. This group can also be written as $2^{*11} \cong \langle t_1, t_2, \ldots, t_{11} \mid {t_i}^2 = 1 \rangle$. Furthermore, we see $PSL(2, \mathbb{F}_{11})$, the projective special linear group in two dimensions over a field with eleven elements, in the definition of G in (2.1). Curtis forms the group $2^{*11} : PSL(2, \mathbb{F}_{11})$ as a split extension of 2^{*11} by $PSL(2, \mathbb{F}_{11})$. The group that is isomorphic to J_1 is obtained by factoring by $(\sigma_{018} t_0)^5$, which is a relation that says that an element of order 6 in $PSL(2, \mathbb{F}_{11})$, multiplied by a symmetric generator in its 3-cycle, has order 5. [7, p. 355–358]
In his paper, Rob Curtis proves that this group G is simple and that it contains 175560 elements.

2.3 Construction by Robert Wilson

Another representation of J_1 is given in Robert Wilson's book *The Finite Simple Groups* [2]. He defines it as a group of automorphisms of the octonions over the field $\mathbb{F}_{11}$ [2, p. 267]. Recall that octonions can be seen as an octatuple $(1, i_0, i_1, i_2, \ldots, i_6)$ with subscripts modulo 7 of (in this case) elements of $\mathbb{F}_{11}$ such that for every t the following identities hold $i_t i_{t+1} = i_{t+3}$, $i_{t+1} i_{t+3} = i_t$ and $i_{t+3} i_t = i_{t+1}$ [2, p. 119].
In his book, Wilson starts with the group named 2^3:7:3, which he forms from the octonions by automorphisms a, b and c. Automorphism a is a sign change on i_0, i_3, i_5 and i_6, automorphisms b and c are coordinate permutations given by $b = (0, 1, 2, 3, 4, 5, 6)$ and $c = (1, 2, 4)(3, 6, 5)$ [2, p. 267]. To get a group isomorphic to J_1, Wilson adjoins an involution d to 2^3:7:3 which inverts b and commutes with c [2, p. 267]. After some arguments, Wilson concludes that the involution has to be the map

$$d : i_t \mapsto 9i_{-t} + (i_{t-1} + i_{2-t} + i_{4-t}) + 3(i_{3-t} + i_{6-t} + i_{5-t}). \tag{2.2}$$

Wilson claims that the group that follows from these steps would be isomorphic to J_1 [2, p. 267].
In *The Finite Simple Groups*, Wilson describes the structure of the subgroups of J_1 briefly as well as some properties of the groups. Additionally, he compares his definition of J_1 with groups of similar constructions, showing that there are some useful similarities between those groups [2, p. 267–268].

2.4 Advantage of various constructions

An advantage of multiple constructions of the same group is that the properties of the group can be given and proven in a different, and sometimes more comprehensible, way. In the construction of Rob Curtis for example, it is easier to see that the projective special linear group $PSL(2, \mathbb{F}_{11})$ is contained in J_1 than in the construction of Wilson. Nevertheless can the latter be useful, as the manner of constructing gives us parallel groups from which we can find properties of J_1 [2, p. 267]. Additionally, multiple definitions of a group can help for the understanding of said group. The study of the group is made more accessible as it can be viewed from various perspectives. When someone does not understand the first definition, the other two could maybe offer a solution.

Now that we have had a first introduction to the first Janko group, we can dive deeper into the mathematics of the group. As mentioned before, J_1 is a finite simple group, which we will see in the following chapter.

Chapter 3

Simplicity of the first Janko group

In this chapter, we will prove the following theorem, which we had already seen at the construction of Zvonimir Janko in Chapter 2.

Theorem 3.0.1. *[6, p. 147] Let J be a finite group with the following properties:*

1. *The Sylow 2-subgroups of J are abelian;*
2. *J contains an involution i such that $C(i) \cong \langle i \rangle \times A_5$;*
3. *J has no subgroup of index 2.*

Then J is a simple group.

From now on, if we denote a group by J, we implicitly mean a group J that satisfies the properties of Theorem 3.0.1.

The theorem has already been proved by mathematicians such as Zvonomir Janko [6] and Claude Chevalley [8]. Their proofs are very compact and leave quite some gaps for the reader to fill. The outline of the proof that we will provide originates from Chevalley's article [8], but the details were found and proven by us. At this stage, we want emphasize again that we only prove Theorem 3.0.1 in this thesis. For a proof that J_1 indeed satisfies the properties given in the theorem, we refer to Janko's article [6].
As the theorem has a complex proof, using multiple approaches and steps, we will cover it in four sections. The first is targeted at the fact that involutions in a group J are conjugated. After that, we will prove that normal subgroups of a group J cannot have odd order. The next step is to prove that J does not contain a normal subgroup of odd index. After proving those three claims, we will be ready to prove Theorem 3.0.1 in the last section. However, we begin by giving the first two Sylow theorems (without proof, as those can be found in Dummit and Foote's book *Abstract Algebra* [3]), as they will play a key role in the proofs we will provide. Recall that for a group G with order $p^n m$, with p a prime and $p \nmid m$, a maximal p-subgroup of order p^n is called a *Sylow p-subgroup* of G [3, p 139].

Theorem 3.0.2 (First Sylow Theorem)**.** *[3, p. 139–140] Given a finite group G of order $p^n m$, with p a prime and $p \nmid m$, the group G has a subgroup of order p^n.*

This theorem tells us that Sylow p-subgroups of a group G will always exists, provided that p is a prime number that is a divisor of the cardinality of G. From now on, we will not refer to this theorem. Henceforth, when we speak of a Sylow p-subgroup, we implicitly use Theorem 3.0.2 to justify our use of Sylow subgroups. The next theorem is the Second Sylow Theorem, which states that the Sylow p-subgroups of a group G are conjugated.

Theorem 3.0.3 (Second Sylow Theorem)**.** *[3, p. 139–140] Given a finite group G, and prime number p in the prime factorization of the order of G, all Sylow p-subgroups are conjugates. That is, for every Sylow p-subgroup S and S' of G, there exists some $g \in G$ such that $g^{-1}Sg = S'$.*

This theorem will be useful for proving Theorem 3.0.1, which is why we denote it here explicitly. Furthermore, we will give Lagrange's Theorem. Although it is a well-known result in group theory, we give it here formally for completeness.

Theorem 3.0.4 (Lagrange's Theorem)**.** *[3, p. 89] Let G be a finite group, with subgroup H. Then the order of H divides the order of G, with $|G| = [G : H]|H|$.*

Recall that $[G : H]$ is a notation for the *index* of the subgroup H. This is equal to the number of cosets of H in G [3, p. 90]. From now on, we will refer to Theorem 3.0.4 as Lagrange's Theorem. A corollary that follows from Lagrange's Theorem, which we will use often, is given next.

Corollary 3.0.5. *[3, p. 90] Let G be a finite group. For every element $g \in G$, the order of g is a divisor of the cardinality of G.*

Likewise, we will mostly not refer to this corollary explicitly. Lastly, we give another important notable theorem in group theory.

Theorem 3.0.6 (Cauchy's Theorem)**.** *[3, p. 93] Let G be a finite group. If p is a prime dividing the cardinality of G, the group contains an element of order p.*

Just as with Lagrange's Theorem, we will usually refer to this result as Cauchy's Theorem.

3.1 All involutions of J are conjugated

As the title suggests, this section is concentrated on proving that all involutions of a group J are conjugated. We once again want to remember that we mean a group that satisfies the properties given in Theorem 3.0.1 when we denote J. We aim to prove the next lemma in this section, using introductory lemmas that will follow. The proof of Lemma 3.1.1 is given in section 3.1.5.

Lemma 3.1.1. *In a group J like in Theorem 3.0.1, all involutions are conjugates.*

3.1.1 Sylow 2-subgroups of J are of the type $[2, 2, 2]$

In this subsection, we will give a lemma about a useful property of Sylow 2-subgroups of J. Recall that we call a group of the *type* $[a, b, c, \cdots]$ if it is isomorphic to the direct product of the cyclic groups C_a, C_b, C_c, and so on, where $C_k = \langle x \mid x^k = 1\rangle$ [3, p. 163]. Therefore a group of type $[2, 2]$ is isomorphic to $C_2^2 = \langle x, y \mid x^2 = y^2 = 1,\ xy = yx\rangle$ and a group of type $[2, 2, 2]$ is isomorphic to the group $C_2^3 = \langle x, y, z \mid x^2 = y^2 = z^2 = 1,\ xy = yx,\ yz = zy,\ xz = zx\rangle$.

Lemma 3.1.2. *The Sylow 2-subgroup S of a group J that contains the involution i for which property 2 of Theorem 3.0.1 holds, is of type $[2, 2, 2]$, i.e. consists of seven involutions and the trivial element.*

Proof. Let S be the Sylow 2-group of J containing an involution i such that $C(i) \cong \langle i\rangle \times A_5$. Since S is abelian, we have that $S \subseteq \langle i\rangle \times A_5$. It is known that the maximal 2-group, i.e. the Sylow 2-group, of A_5 is of the type $[2, 2]$. Therefore, S must be of the type $[2, 2, 2]$. □

This lemma will mostly not be used explicitly in our proofs, but it will justify our use of involutions.

3.1.2 Sylow 2-subgroups and their centralizers

We will give a preliminary lemma to get one step closer to our desired result. In Chapter 2, we had seen the definition for a centralizer of an element. Now, we want to recall a definition that is similar. The *centralizer* of a subgroup H of G is given by all elements $g \in G$ such that $gh = hg$ for all $h \in H$ [3, p. 49]. We will denote this subgroup with $C_G(H)$ or $C(H)$ if there cannot be any confusion in which group the centralizer lives. Similarly, the *normalizer* of a subgroup H is given by the set $\{g \in G : gH = Hg\}$, which we will denote by $N_G(H)$ or $N(H)$ [3, p. 50]. We are now ready for the following lemma.

Lemma 3.1.3. *Let H be a subgroup of a group G. Then the centralizer of H in G is a normal subgroup of the normalizer of H in G.*

Proof. Using the definitions, it is easy to see that $C_G(H) \subseteq N_G(H)$.
Take some $x \in N_G(H)$ and $c \in C_G(H)$. To prove the normality of $C_G(H)$ in $N_G(H)$, we must prove that $x^{-1}cx \in C_G(H)$. Take some arbitrary $h \in H$. Then, we have

$$(x^{-1}cx)^{-1}h(x^{-1}cx) = x^{-1}c^{-1}(xhx^{-1})cx.$$

Since $x \in N_G(H)$, we have that $xhx^{-1} \in H$, which therefore commutes with c. By this, we find that

$$(x^{-1}cx)^{-1}h(x^{-1}cx) = x^{-1}(c^{-1}(xhx^{-1})c)x = x^{-1}(xhx^{-1})x = h,$$

thus proving that $x^{-1}cx$ is an element of $C_G(H)$. By definition, this means that $C_G(H)$ is a normal subgroup of $N_G(H)$. □

After this general lemma, we will give a lemma that says something about the group J.

Lemma 3.1.4. *In a group J, the Sylow 2-subgroup of J that contains the involution for which property 2 of Theorem 3.0.1 holds, is its own centralizer.*

Proof. Denote the Sylow 2-subgroup of J by S and let i be the involution of S such that $C(i) \cong \langle i \rangle \times A_5$. By definition, we have that $C_J(S) = \{j \in J : js = sj \ \forall s \in S\}$. In particular, we have that $ji = ij$ for all $j \in C_J(S)$ as $i \in S$. Therefore, we conclude that $C_J(S) \subseteq \langle i \rangle \times A_5$. It is known that the centralizer of a Sylow 2-group in A_5 is equal to itself, which means that S is its own centralizer, i.e. $S = C_J(S)$. □

3.1.3 Normalizers act faithfully on Sylow 2-subgroups

In this subsection, we will prove just one lemma. Using Lemma 3.1.4, we can prove the following result fairly quick. First, we recall that a group G *acts faithfully* on a set A if two distinct elements of G act on A as two distinct automorphisms [3, p. 43]. This is a property that we will need for the following lemma.

Lemma 3.1.5. *Let J be a group satisfying the properties of Theorem 3.0.1 and let S be a Sylow 2-subgroup of J containing the involution i for which the centralizer is isomorphic to $\langle i \rangle \times A_5$. Denote the normalizer of S in J by N. Then N/S acts faithfully on S via automorphisms.*

Proof. Firstly, observe that for all $n \in N$ the map $\phi_n : S \to S$, defined as $\phi_n(s) = n^{-1}sn$ is a well defined automorphism. Since N was assumed to be the normalizer of S, $n^{-1}Sn = S$ for all $n \in N$. It is clear that ϕ_n is a homomorphism. For bijectivity, we observe that

$$\phi_{n_1 \cdot n_2}(s) = (n_1 \cdot n_2)^{-1}sn_1n_2 = n_2^{-1}n_1^{-1}sn_1n_2 = n_2^{-1}\phi_{n_1}(s)n_2 = \phi_{n_2} \circ \phi_{n_1}(s) \tag{3.1}$$

for all $s \in S$. We also see that $\phi_1(s) = s = \mathrm{id}(s)$. Using (3.1) we see that

$$\phi_n \circ \phi_{n^{-1}}(s) = \phi_{n^{-1} \cdot n}(s) = \phi_1(s) = \mathrm{id}(s) \tag{3.2}$$

for all $s \in S$. With (3.2), we see that $\phi_{n^{-1}}$ is the inverse of ϕ_n, by which we can conclude that ϕ_n is a bijection. Thus, ϕ_n is a bijective homomorphism from S to itself, hence an automorphism.
The map $\psi : N \to S$, $\psi(n) = \phi_n$ defines a group action on S. The kernel of ψ consists of all elements of N that commute with every element of S, which is precisely the centralizer of S. In Lemma 3.1.4 we had seen that S is its own centralizer in J. Then we find that $\psi : N/S \to \mathrm{Aut}(S)$, defined as $\psi(x) = \phi_x$ is an injective map. By definition, this means that N/S acts faithfully on S via automorphisms. □

3.1.4 The order of the normalizer of a Sylow 2-subgroup

Before we can continue our progress to the last lemma of this section, we need to give a definition of the term *p-normal*. But before that, we recall that the *center* of a group G is given by $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$, the subgroup of elements of G that commute with all elements of G [3, p. 50].

Definition 3.1.6. *[9, p. 205] Let G be a group and p be a prime number. We call G a p-normal group if the center of a Sylow p-subgroup of G is the center of all Sylow p-subgroups containing $Z(S)$.*

In other words: if for all Sylow p-subgroups S and S' of G with $Z(S) \subseteq S'$, we have that $Z(S') = Z(S)$, we call G p-normal. As will be shown in the next lemma, the group J satisfies that condition for Sylow 2-subgroups and is hence 2-normal.

Lemma 3.1.7. *A group J like in Theorem 3.0.1 is 2-normal.*

Proof. Since S is abelian by the first property of Theorem 3.0.1, we have that $Z(S) = S$. Take S' to be a Sylow 2-subgroup of J that contains $Z(S) = S$. Since S and S' are by definition both maximal in J and thus of the same cardinality, we can conclude that $S = S'$. Then $Z(S') = Z(S)$ holds. Using Definition 3.1.6, we hereby see that J is 2-normal. □

Now that we have established that J is a 2-normal group, we will give the Second Theorem of Grün, which can be found in *The Theory of Groups* [9]. This theorem states a useful property of p-normal groups, which we will use to prove the last theorem of this section.

Theorem 3.1.8 (Second Theorem of Grün)**.** *[9, p. 215] Let G be a p-normal group. Let G' be the smallest normal subgroup of G such that G/G' is an abelian p-group. Let S be a Sylow p-subgroup of G, with center Z. Denote the normalizer of Z by H. Let H' be the smallest normal subgroup of H such that H/H' is an abelian p-group. Then $G/G' \cong H/H'$.*

We will not give the proof of this theorem, as it can be found on page 215 and 216 of Marshall Hall's book [9]. However, we will give a corollary of the Second Theorem of Grün, with proof.

Corollary 3.1.9. *Let G be a p-normal group. Let S be a Sylow p-subgroup of G, with center Z. Denote the normalizer of Z by H. Let H' be the smallest normal subgroup of H such that H/H' is an abelian p-group. If H has a subgroup of index p that contains H', then G also has an index p subgroup.*

Proof. Let $G' \subseteq G$ be the smallest normal subgroup such that G/G' is an abelian p-group. Since G is p-normal, we can apply Theorem 3.1.8 to see that $G/G' \cong H/H'$.
Denote the index p subgroup of H by H''. We then have $H' \subseteq H'' \subseteq H$, with H' and H'' normal in H. We can define the map $\phi : H/H' \to H/H''$ by $\phi(xH') = xH'H'' = xH''$. It is easy to see that this is a homomorphism.
Since G' is normal in G, there exists a homomorphism $\psi : G \to G/G'$, the quotient map. We had already seen that $G/G' \cong H/H'$, by which we can write $\psi : G \to H/H'$. Now we observe that $\phi \circ \psi : G \to H/H''$ is a homomorphism. By the First Isomorphism Theorem [3, p. 97], we see that $G/\mathrm{Ker}(\phi \circ \psi) \cong H/H''$. As H'' was an index p subgroup of H, G also has an index p subgroup, namely $\mathrm{Ker}(\phi \circ \psi)$. □

We had already seen in Lemma 3.1.7 that J is a 2-normal group. Therefore, Corollary 3.1.9 can be applied to J. We will do so in the next lemma.

Lemma 3.1.10. *The normalizer N of a Sylow 2-subgroup S of the group J containing an involution i such that $C(i) \cong \langle i \rangle \times A_5$, is of order 168.*

Proof. By Lemma 3.1.3 we have that $C_J(S) = S$ is a normal subgroup of N. We know that S is a maximal 2-group of J, so by Lagrange's Theorem we have that $|N/S|$ must be odd. We see that N/S acts faithfully on S via automorphisms by Lemma 3.1.5. Thus, $N/S \subseteq \mathrm{Aut}(S)$. We know that the automorphism group of a group of type $[2,2,2]$ equals the general linear group of degree 3 over $\mathbb{F}_{11}$. Since S was proven to be a group of type $[2,2,2]$ in Lemma 3.1.2, we can write $\mathrm{Aut}(S) \cong \mathrm{GL}_3(\mathbb{F}_2)$, therefore $|\mathrm{Aut}(S)| = 8 \cdot 3 \cdot 7$. Since $|N/S|$ is odd, $|N/S|$ must divide $3 \cdot 7$. We know that the normalizer of a Sylow 2-subgroup of A_5 is equal to A_4 and has order $2^2 \cdot 3$. By Cauchy's Theorem, we know that such normalizer must contain an element of order 3. Therefore, N and N/S also need to contain an element of order 3, hence 3 divides $|N/S|$. Using this and the fact that $|N/S|$ is a divisor of $3 \cdot 7$, we have either $|N/S| = 21$ or $|N/S| = 3$.
We will now prove by contradiction that the case $|N/S| = 3$ is not possible. Suppose that $|N/S| = 3$, then we have that $|N| = |S||N/S| = 2^3 \cdot 3$. We know that both N and A_5 (and thus $\langle i \rangle \times A_5$ also), contain an element of order 3. We also have that $S \subseteq \langle i \rangle \times A_5$, since S is abelian. Therefore, $N \subseteq \langle i \rangle \times A_5$ holds in this case. Using the order of N we found and the fact that $|\langle i \rangle \times A_5| = 2^3 \cdot 3 \cdot 5$, we find that $|N \cap A_5| = 2^2 \cdot 3$. Therefore, we have that $[N : N \cap A_5] = 2$. In Lemma 3.1.7, we have seen that J is 2-normal. Let H' be the smallest normal subgroup of N such that N/H' is an abelian 2-group. One can easily see that the intersection of normal subgroups $H'' \subseteq H$ such that H/H'' is an abelian 2-group also yields a normal subgroup that possesses that property. Using this, we see that the smallest subgroup H' must be contained in all those subgroups H''. We had already established that $N \cap A_5$ is an index 2 subgroup of N, thus it is a normal subgroup such that $N/(N \cap A_5)$ is an abelian 2-group (as it contains only 2 elements). Therefore, $H' \subseteq N \cap A_5$. When we apply Corollary 3.1.9, we see that J must also have an index 2 subgroup. This contradicts property 3 of Theorem 3.0.1, by which we can conclude that our assumption that $|N/S| = 3$ is impossible.
Therefore, $|N/S| = 21$ has to hold. By Lagrange's Theorem, we have $|N| = |N/S||S| = 21 \cdot 8 = 168$. □

For our next lemma, we need the definitions of orbits and stabilizers. If G is a group acting on a set X by conjugation, we define the *orbit* of an element $x \in X$ as $\mathrm{orb}(x) = \{y \in X : \exists g \in G : y = g^{-1}xg\}$ [3, p. 45]. The *stabilizer* of an element $x \in X$ is defined as $\mathrm{stab}(x) = \{g \in G : g^{-1}xg = x\}$ [3, p. 51]. We also use the Orbit-Stabilizer Theorem [3, p. 114], which states that for all $x \in X$ the following identity holds: $|G| = |\mathrm{orb}(x)| \cdot |\mathrm{stab}(x)|$.

Lemma 3.1.11. *The normalizer N of a Sylow 2-subgroup S of the group J containing an involution i such that $C(i) \cong \langle i \rangle \times A_5$ contains an element that permutes all non-trivial elements of S.*

Proof. Since the order of N is 168 by Lemma 3.1.10, we have $7 \mid |N|$. By Cauchy's Theorem, N contains an element x of order 7. Since $x \notin S$, as $7 \nmid |S| = 8$, we see that $xS \neq S$ and $xS \in N/S$ with $\mathrm{ord}(xS) = 7$. In Lemma 3.1.5, we have seen that N/S acts faithfully on S. This means that $n^{-1}sn = s$ for all $s \in S$ implies that $n = 1$. Since xS has order 7, we know that there exists some non-trivial $s_1 \in S$ such that $(xS)^{-1}s_1xS \neq s_1$. This also means that $x^{-1}s_1x \neq s_1$.
Now we will look at the cyclic group generated by x; the group $\langle x \rangle$ is of order 7. We can let this group act on S by conjugation. Then, by the Orbit-Stabilizer Theorem [3, p. 114], we have that

$$7 = |\langle x \rangle| = |\mathrm{orb}(s_1)| \cdot |\mathrm{stab}(s_1)|,$$

where $\mathrm{orb}(s_1)$ is the orbit of s_1 in S and $\mathrm{stab}(s_1)$ is the stabilizer of s_1 in $\langle x \rangle$. Since 7 is a prime, we know that either $|\mathrm{orb}(s_1)|$ or $|\mathrm{stab}(s_1)|$ is 7 and the other is equal to 1. By our assumption that $x^{-1}s_1x \neq s_1$, we see that $|\mathrm{stab}(s_1)| < 7$, which means that $|\mathrm{stab}(s_1)| = 1$, hence $|\mathrm{orb}(s_1)| = 7$. We see that $1 \neq \mathrm{orb}(s_1)$, otherwise $s_1 = 1$ would have to hold. This means that $\mathrm{orb}(s_1)$ contains all non-trivial elements of S, hereby proving that $x \in N$ permutes all non-trivial elements of S. □

3.1.5 Proof of Lemma 3.1.1

After we have proven all lemmas from previous subsections, we are ready to prove Lemma 3.1.1, which states that all involutions of the group J are conjugated.

Proof of Lemma 3.1.1. Let S denote the Sylow 2-subgroup of J that contains an involution i such that $C(i) \cong \langle i \rangle \times A_5$. Lemma 3.1.11 then tells us that there exists some x in the normalizer of S that permutes all involutions of S by conjugation.
To show that all involutions of J are conjugated, we take some arbitrary involutions i_1 and i_2 of J. Suppose that $i_1 \in S'$ and $i_2 \in S''$ for Sylow 2-subgroups S' and S'' of J. Since all Sylow 2-subgroup are conjugated (Theorem 3.0.3), there exist some $j_1, j_2 \in J$ such that $j_1^{-1} i_1 j_1 \in S$ and $j_2^{-1} i_2 j_2 \in S$. As x permutes all non-trivial elements of S transitively, there exist some $g_1, g_2 \in J$, powers of x, such that $g_1^{-1} j_1^{-1} i_1 j_1 g_1 = i$ and $g_2^{-1} j_2^{-1} i_2 j_2 g_2 = i$. Substituting the second equality in the first, we get that $g_1^{-1} j_1^{-1} i_1 j_1 g_1 = g_2^{-1} j_2^{-1} i_2 j_2 g_2$. Rewriting this expression to $j_2 g_2 g_1^{-1} j_1^{-1} i_1 j_1 g_1 g_2^{-1} j_2^{-1} = i_2$, lets us see that i_1 and i_2 are conjugated. Since these involutions were chosen arbitrary, we can conclude that all involutions of J are conjugated. □

With this proof, we conclude this section. We have seen the definition of p-normal, as well as a proof that J is 2-normal. Additionally, we have proven that all Sylow 2-subgroups of J are of the type $[2, 2, 2]$. Via some other lemmas, we have proven that the order of the normalizer of a Sylow 2-subgroup of J is 168, by which we have proven that all involutions of J are conjugated.

3.1.6 On centralizers of involutions of J

In the previous subsection, we were able to prove that all involutions of J are conjugates. The lemmas in Section 3.1 on which the proof of Lemma 3.1.1 is build, were primarily based on the assumption that S was a Sylow 2-subgroup that contained the involution i such that $C(i) \cong \langle i \rangle \times A_5$. In this subsection, we will prove that this is the case for all involutions of J. We begin by proving a lemma about the conjugate of a subgroup.

Lemma 3.1.12. *Let G be a group and H be a subgroup of G. For all $g \in G$, $g^{-1}Hg$ is a subgroup of G with $g^{-1}Hg \cong H$.*

Proof. Firstly, we will prove that $g^{-1}Hg$ is a subgroup of G. We note that the identity of G is contained in H, by which we find that $g^{-1}1g = 1 \in g^{-1}Hg$. Now, we take some arbitrary $x, y \in g^{-1}Hg$ to prove that it is closed under multiplication and inverses. First off, we observe that there exist some $x', y' \in H$ such that $x = g^{-1}x'g$ and $y = g^{-1}y'g$. With this, we see that $x^{-1} = g^{-1}(x')^{-1}g$. Since $x' \in H$, we have that $(x')^{-1} \in H$ and thus $x^{-1} \in g^{-1}Hg$. Now we find that $xy = g^{-1}x'gg^{-1}y'g = g^{-1}x'y'g$. Since H is a subgroup of G, we have that $x'y' \in H$, by which we conclude that $xy \in g^{-1}Hg$. As a result, $g^{-1}Hg$ is non-empty and closed under inverses and multiplication, hence a subgroup of G.
To prove that H and $g^{-1}Hg$ are isomorphic, we define the map $\phi : H \to g^{-1}Hg$ as $\phi(h) = g^{-1}hg$. We see that this is a homomorphism; $\phi(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = \phi(x)\phi(y)$. It is also an injection. Suppose $x, y \in H$ for which $\phi(x) = \phi(y)$ holds. Then we have that $g^{-1}xg = g^{-1}yg$, from which we can conclude that $x = y$, using cancellation laws. Furthermore, ϕ is a surjective map. Take some arbitrary $x \in g^{-1}Hg$. By definition, this means that there exists some $h \in H$ such that $x = g^{-1}hg$. Now, we see that $\phi(h) = g^{-1}hg = x$, hence ϕ is surjective.
Thus, we have found ϕ to be both injective and surjective, by which it is a bijection. Therefore, we have found a isomorphism between H and $g^{-1}Hg$, concluding our proof that $H \cong g^{-1}Hg$. □

With this lemma, we can prove the next lemma, that will justify our use of involutions in the future.

Lemma 3.1.13. *Let J be a group satisfying the properties of Theorem 3.0.1. Then $C(i) \cong \langle i \rangle \times A_5$ holds for all involutions i of J.*

Proof. Let j be the involution of J such that its centralizer $C(j)$ is isomorphic to $\langle j \rangle \times A_5$, as given in property 2 of Theorem 3.0.1. Let i be another involution of J. By Lemma 3.1.1, we see that there exists some $g \in J$ such that $g^{-1}jg = i$.
Now, take some element $c \in C(i)$. By definition, we have that $ci = ic$. Substituting $g^{-1}jg = i$, we get $cg^{-1}jg = g^{-1}jgc$. Multiplying with g from the left and with g^{-1} from the right, we get $gcg^{-1}j = jgcg^{-1}$. Using the definition of a centralizer again, we see that $gcg^{-1} \in C(j)$, i.e. $c \in g^{-1}C(j)g$. Since c was chosen arbitrarily from $C(i)$, we have that $C(i) \subseteq g^{-1}C(j)g$.
In a similar way, we have that

$$c \in g^{-1}C(j)g \implies gcg^{-1}j = jgcg^{-1} \implies cg^{-1}jg = g^{-1}jgc \implies ci = ic \implies c \in C(i).$$

Therefore, we find that $g^{-1}C(j)g \subseteq C(i)$. This leads us to the conclusion that $C(i) = g^{-1}C(j)g$. With Lemma 3.1.12, we find that $C(i) = g^{-1}C(j)g \cong C(j)$. Since j was assumed to satisfy property 2 of Theorem 3.0.1, we find that $C(i) \cong C(j) \cong \langle j \rangle \times A_5$.
If we apply Lemma 3.1.12 one more time, we see that $\langle j \rangle \cong g^{-1}\langle j \rangle g$. Using our knowledge of a cyclic group, we see that $g^{-1}\langle j \rangle g = \{1, g^{-1}jg\}$. When we substitute $g^{-1}jg = i$ in this equality, we have that $g^{-1}\langle j \rangle g = \{1, i\} = \langle i \rangle$. Thus, we find that $\langle j \rangle \cong \langle i \rangle$, by which we can conclude that $C(i) \cong \langle i \rangle \times A_5$. Since i was an arbitrarily chosen involution of J, we can conclude that for all involutions q of J, we have that $C(q) = \langle q \rangle \times A_5$. □

Now we have proven this result, we can draw conclusions about our previous lemmas. We see that Lemma 3.1.2, Lemma 3.1.4, Lemma 3.1.5 and Lemma 3.1.10 are more generally applicable. In these four lemmas, wherever a Sylow 2-subgroup of J containing an involution i such that $C(i) \cong \langle i \rangle \times A_5$ is mentioned, we can generalize it to just some Sylow 2-subgroup of J. That is, because Lemma 3.1.13 tells us that all involutions satisfy the property that is demanded. Since Sylow 2-subgroups are a 2-group, they must contain an element of order 2 by Cauchy's Theorem. Therefore, all Sylow 2-subgroups of J contain an involution i such that $C(i) \cong \langle i \rangle \times A_5$. From now on, if we refer to one of the four lemmas mentioned, we will mean the more generalized version of the lemma.

3.2 On normal subgroups of J of odd order

The main objective of our work is to prove the simplicity of a group J such as in Theorem 3.0.1. As we had already seen in Definition 1.0.1, this means that J has no normal subgroups other than the trivial group and J itself. In this section, we will prove the following lemma:

Lemma 3.2.1. *A group like J in Theorem 3.0.1 cannot have a non-trivial normal subgroup H of odd order.*

3.2.1 Homomorphisms without non-trivial fixed points

Before we can prove the claim in Lemma 3.2.1, we need to give a lemma which tells us something about the properties of homomorphisms that satisfy $\phi \circ \phi = \mathrm{id}$ and have no non-trivial fixed points. Recall that x is a *fixed point* of ϕ if $\phi(x) = x$ holds.

Lemma 3.2.2. *Let G be a finite group and the map $\phi : G \to G$ be a homomorphism. If $\phi \circ \phi = id_G$ and ϕ has no non-trivial fixed points, then $\phi(x) = x^{-1}$ and G is abelian.*

Proof. Take the map $\gamma(x) = x^{-1}\phi(x)$. We claim that γ is bijective. First, we prove its injectivity.
Assume $x^{-1}\phi(x) = y^{-1}\phi(y)$ for some $x, y \in G$. Then, we can rewrite the expression to get $\phi(x)\phi(y)^{-1} = xy^{-1}$. By the properties of homomorphisms, we get $\phi(xy^{-1}) = xy^{-1}$. It was presumed that ϕ has no non-trivial fixed points, thus $1 = xy^{-1}$. Therefore, $y = x$ and ϕ is injective. Since ϕ is an injective map from a finite group G to itself, we can conclude that it is a bijection. This means that every element of G can be written as $x^{-1}\phi(x)$ for some $x \in G$.
Take an arbitrary $g \in G$. Then there exists some $x \in G$ such that $g = x^{-1}\phi(x)$. When we apply ϕ at both sides, we get $\phi(g) = \phi(x^{-1})\phi(\phi(x)) = \phi(x)^{-1}x$. Multiplying both sides with g gives us $g\phi(g) = x^{-1}\phi(x)\phi(x)^{-1}x = 1$. Thus we conclude that $\phi(g) = g^{-1}$ for all $g \in G$.
Now we can prove that G is abelian. We observe that $\phi(gh) = (gh)^{-1} = h^{-1}g^{-1}$, but also that $\phi(gh) = \phi(g)\phi(h) = g^{-1}h^{-1}$ by the properties of homomorphisms. Then, we get that $h^{-1}g^{-1} = g^{-1}h^{-1}$, i.e. $gh = hg$, thus G is abelian. □

Primarily the first conclusion of this lemma, that $\phi(x) = x^{-1}$ holds when ϕ satisfies the assumptions, will be used, as we will see later on.

3.2.2 Proof of Lemma 3.2.1

Since we had found that a Sylow 2-subgroup S of J is of the type $[2, 2, 2]$, it is evident that there exists two distinct involutions i_1 and i_2 in S. Considering J is assumed to satisfy the properties in Theorem 3.0.1, in particular the first, S is abelian. By this, we see that there exist two distinct involutions in a Sylow 2-subgroup that commute with each other. Now, we are ready to prove the main lemma of this section.

Proof of Lemma 3.2.1. Suppose H is a normal subgroup of J of odd order. Let i be an involution of J, by Lemma 3.1.13 we have that $C(i) \cong \langle i \rangle \times A_5$. Then we have that $H \cap C(i) = \{1\}$, since A_5 (and thus $\langle i \rangle \times A_5$) has no non-trivial normal subgroup of odd order. Hence, conjugating with i induces an automorphism without a non-trivial fixed element in H. Using Lemma 3.2.2, we get that such an automorphism maps each element of H to its inverse.

When i_1 and i_2 are different involutions of J that are commuting, then $i_1 i_2$ is also an involution, as $(i_1 i_2)^2 = i_1 i_2 i_1 i_2 = i_1 i_1 i_2 i_2 = 1$. With Lemma 3.2.2, we see that for $x \in H$ $i_1 i_2(x) = i_1(x^{-1}) = x$. Using the properties of automorphisms and that the inverse of an involution equals itself, we also get $i_1 i_2(x) = i_1(x^{-1}) = i_1(x)^{-1} = i_1(x) = x^{-1}$. Therefore $x = x^{-1}$ for all $x \in H$, thus all elements of H are their own inverse as $x^2 = 1$. This means that $\mathrm{ord}(x) \mid 2$, implying $\mathrm{ord}(x) = 1$ or $\mathrm{ord}(x) = 2$ for all $x \in H$. By Corollary 3.0.5, we have that $\mathrm{ord}(x) \mid |H|$. Since H was assumed to have odd order, $\mathrm{ord}(x) = 1$ is the only possibility. Thus $H = \{1\}$ has to hold if it is a normal subgroup of J of odd order. □

With this lemma and proof, we are one step closer to proving that J is a simple group. We have seen a lemma on homomorphisms without non-trivial fixed points with the property $\phi \circ \phi = \mathrm{id}$. With this, we have eliminated the possibility of a non-trivial normal subgroup of J of odd order.

3.3 On normal subgroups of J of odd index

In this section, we will focus on proving that a normal subgroup H of odd index of a group J as in Theorem 3.0.1 has to be equal to J. Yet again, we will denote a group with J if we want the group to possess the properties from Theorem 3.0.1. To have an indication what we intend to prove exactly in this section, we give the most important lemma of this section, the proof will follow in Section 3.3.4.

Lemma 3.3.1. *Let J be a group satisfying the properties of Theorem 3.0.1. If H is a normal subgroup of J of odd index, the identity $H = J$ has to hold.*

3.3.1 Frattini's Argument

Our first lemma in this section is called Frattini's Argument. It can be proven by a fairly short demonstration, but it is a useful lemma nonetheless. Recall that we mean the *product of group subsets* by the notation AB for A and B subsets of a group G. This set is defined as $\{ab \mid a \in A,\ b \in B\}$ and is not necessarily a subgroup of G [3, p. 93]. It can be proven that AB is a subgroup of G if and only if $AB = BA$.

Lemma 3.3.2 (Frattini's Argument)**.** *[3, p. 193] Let G be a finite group with a normal subgroup H. If S is a Sylow p-subgroup of H, then $G = N_G(S)H$. In other words, G is equal to the product of the subsets $N_G(S)$ and H.*

Proof. [3, p. 193] Let $g \in G$ be arbitrary. Since S is a subgroup of H, the following holds $g^{-1}Sg \subseteq g^{-1}Hg$. We had assumed H to be normal in G, thus $g^{-1}Hg = H$. Therefore $g^{-1}Sg \subseteq H$ is a Sylow p-subgroup of H. By Theorem 3.0.3, there exists an element $h \in H$ such that $h^{-1}Sh = g^{-1}Sg$. With this, we see that $gh^{-1}Shg^{-1} = S$. By definition, this means that $gh^{-1} \in N_G(S)$, hence $g \in N_G(S)H$. Since $g \in G$ was an arbitrary element, we can conclude that $G = N_G(S)H$. □

3.3.2 The centralizers of involutions are contained in H

In this subsection, we will work towards proving that $C(i)$, the centralizer of an involution i of J, is contained in all normal subgroups H of odd index in J. Before we commence with that result, we give some introductory lemmas. For example, the next one gives us information about a homomorphism if the orders of the domain and codomain are known.

Lemma 3.3.3. *Let $\phi : G \to H$ be a group homomorphism. If G has even order and H has odd order, ϕ cannot be injective.*

Proof. Suppose to the contrary that ϕ is injective. Then every element $g \in G$ is mapped to a distinct element in H. Thus, $|Im(\phi)| = |G|$. We know that $Im(\phi)$ has to be a subgroup of H. By Lagrange's Theorem, we have that $|Im(\phi)| \mid |H|$. However, this is impossible as $|Im(\phi)| = |G|$ is even and $|H|$ is odd. Therefore, ϕ cannot be injective. □

The next lemma also involves a homomorphism. It gives us a neat condition by which we can check the injectivity of homomorphisms. Recall that the *kernel* of a homomorphism is given by all the elements of the domain that are mapped to the identity of the codomain [3, p. 40].

Lemma 3.3.4. *Let $\phi : G \to H$ be a group homomorphism. Then ϕ is injective if and only if $Ker(\phi) = \{1\}$.*

Proof. First, we will prove the implication to the right. Therefore, ϕ is assumed to be injective. Let $\phi(x) = 1$ hold for some $x \in G$. We know that $\phi(1) = 1$ must hold. Therefore, $\phi(x) = \phi(1) = 1$. By the injectivity of ϕ, we have that $x = 1$, thus proving that the kernel of ϕ is trivial.
Now we will prove the left implication, thus assume that $\mathrm{Ker}(\phi)$ is trivial. If we have that $\phi(x) = \phi(y)$ for some $x, y \in G$, we have that $\phi(x)\phi(y)^{-1} = 1$. By the properties of homomorphisms, we have that $\phi(xy^{-1}) = 1$. Since the kernel was assumed to be trivial, we must have that $xy^{-1} = 1$, thus $x = y$, proving the injectivity of ϕ. □

The next lemma is also concentrated on homomorphisms, the order of the image in particular. Apparently, for a homomorphism ϕ, the order of $\phi(x)$ is a divisor of the order of x. We will also state and prove a corollary of the next lemma.

Lemma 3.3.5. *Let $\phi : G \to H$ be a homomorphism. Denote the order of an element $x \in G$ by n. Then $ord(\phi(x)) \mid n$.*

Proof. By our assumptions, we have $x^n = 1$. Using the properties of a homomorphism, we get

$$\phi(x)^n = \phi(x^n) = \phi(1) = 1.$$

By definition, this means that $\text{ord}(\phi(x)) \mid n$. □

Corollary 3.3.6. *Let H be a normal subgroup of a finite group G and G/H be the quotient group of G by H. For all $g \in G$, the order of gH divides the order of g.*

Proof. Recall that the map $\phi : G \to G/H$, defined as $\phi(g) = gH$ is a group homomorphism. Using Lemma 3.3.5, we see that $\text{ord}(\phi(g)) \mid \text{ord}(g)$, thus $\text{ord}(gH) \mid \text{ord}(g)$. □

The next lemma requires some more effort to prove than the preceding ones. It gives us information about the normal subgroups of a group that is equal to the direct product of two simple groups.

Lemma 3.3.7. *Let $G = H_1 \times H_2$ be a group composed of the direct product of the distinct simple groups H_1 and H_2. The only normal subgroups of G are precisely $\{1\}$, $H_1 \times \{1\}$, $\{1\} \times H_2$ and $H_1 \times H_2$.*

Proof. Let N be a normal subgroup of G. Define $\pi_1 : G \to H_1$ as the projection of G onto H_1. This is a surjective map, thus $\pi_1(N)$ is a normal subgroup of H_1. Since H_1 is a simple group, we have two possibilities: $\pi_1(N) = \{1\}$ or $\pi_1(N) = H_1$.
If $\pi_1(N) = \{1\}$, N is a subgroup of H_2. As $N \subseteq H_2 \subseteq G$ holds, and $N \trianglelefteq G$, we have that $N \trianglelefteq H_2$. The group H_2 was assumed to be simple, thus $N = \{1\}$ or N is isomorphic to H_2.
If $\pi_1(N) = H_1$, we can look at the kernel of π_1. We see that $\text{Ker}(\pi_1) = H_2$ in this case. Now define $L = \text{Ker}(\pi_1) \cap N = H_2 \cap N$. Since L is an intersection of normal subgroups of G, L is also normal in G. Thus, we have $L \subseteq H_2 \subseteq G$ with $L \trianglelefteq G$. This implies that L is normal in H_2. Since H_2 is simple, we have $L = H_2 \cap N = \{1\}$ or $L = H_2 \cap N = H_2$. In the first case, we have that N is isomorphic to H_1. In the second case we see that $H_2 \subseteq N$ as well as $H_1 \subseteq N$. Since both H_1 and H_2 are normal in G, we see that they are normal in N. As N is a subset of $H_1 \times H_2$, all elements can be uniquely written as a product of an element form H_1 and an element of H_2. By our assumption, $H_1 \cap H_2 = \{1\}$. By this, we see that $N \cong H_1 \times H_2$ has to hold, concluding our proof. □

This lemma can be applied to the centralizer of a involution i of J, as Lemma 3.1.13 tells us that $C(i) \cong \langle i \rangle \times A_5$. Both $\langle i \rangle$ and A_5 are simple groups. Therefore Lemma 3.3.7 is applicable, as we will see in the following lemma.

Lemma 3.3.8. *Let J be a group possessing the properties of Theorem 3.0.1. If H is a normal subgroup of J such that J/H is of odd order and i is an involution of J, then $C(i) \subseteq H$ must hold.*

Proof. Define a group homomorphism $\varphi : C(i) \to J/H$ as the composition of the inclusion map and the quotient map. It is known that $\text{Ker}(\varphi)$ is a normal subgroup of $C(i)$. By Lemma 3.1.13, $C(i)$ is a direct product of two simple groups. By Lemma 3.3.7, we find that $\text{Ker}(\varphi)$ can be equal to $\{1\} \times \{1\}$, $\{1\} \times A_5$, $\langle i \rangle \times \{1\}$ or $\langle i \rangle \times A_5$. Since $C(i)$ is of even order and J/H is assumed to be of odd order, with Lemma 3.3.3, we conclude that φ is not injective. By Lemma 3.3.4, we find that $\text{Ker}(\varphi)$ is not trivial and thus not equal to $\{1\} \times \{1\}$. We know that A_5 contains an element of order 2, which we will denote by x. Then, by Lemma 3.3.5, we find that $\text{ord}(\varphi(1, x)) \mid 2$, hence $\text{ord}(\varphi(1, x)) = 1$ or $\text{ord}(\varphi(1, x)) = 2$. The latter is impossible, as $\text{ord}(\varphi(1, x)) \mid |J/H|$ and the order of J/H is odd. Therefore $\text{ord}(\phi(1, x)) = 1$ has to hold. Then $\varphi(1, x) = 1$ in J/H, so, by definition, we have $(1, x) \in \text{Ker}(\varphi)$. This means that $\text{Ker}(\varphi) \neq \langle i \rangle \times \{1\}$. We know that $\langle i \rangle$ also contains an involution. With a similar reasoning, we can find

that $\mathrm{Ker}(\varphi) \neq \{1\} \times A_5$. Therefore, we can conclude that $\mathrm{Ker}(\varphi) = C(i)$. By definition, this means that $C(i) \subseteq H$. □

This lemma thus tells us that for every normal subgroup H of J of odd index, the centralizer of an involution of J is contained in H. This is helpful information for proving Lemma 3.3.1.

3.3.3 On the intersection of subgroups H of index 2

For this subsection, we do not only need the normal subgroup H of odd index of J, but we also need to define another subgroup H'. Let H' be the intersection of subgroups of H of index 2.

3.3.3.1 The quotient group H/H' is a 2-group

We recall that a subgroup A of G is called *characteristic* if A is mapped to itself under every automorphism of G [3, p. 135]. As follows from the next lemma, H' is characteristic in H.

Lemma 3.3.9. *Let H be the intersection of subgroups of index $n \in \mathbb{N}$ of G. Then H is characteristic in G.*

Proof. Let $\phi : G \to G$ be an automorphism. Let K be a subgroup of G such that $[G : K] = n$. Since ϕ is a bijection, $\phi(K) \subseteq G$ has the same number of elements as K. Then

$$[G : \phi(K)] = \frac{|G|}{|\phi(K)|} = \frac{|G|}{|K|} = [G : K] = n.$$

Therefore, $\phi(K)$ is contained in the collection of subgroups of G with index n. Since ϕ is a bijection, it is certainly an injection. Therefore we have

$$\phi\Big(\bigcap_{\substack{K\subseteq G\\ [G:K]=n}} K\Big) = \bigcap_{\substack{K\subseteq G\\ [G:K]=n}} \phi(K).$$

We have defined H to be the intersection of subgroups of index n of G, therefore we see that

$$\phi(H) = H,$$

by which we conclude that H is characteristic in G. □

We want to mention that conjugation by an element of G, i.e. the map $\phi : G \to G$, defined as $\phi(x) = g^{-1}xg$, is an automorphism for all $g \in G$. This means that for a characteristic subgroup H of a group G the following holds: $\phi(H) = g^{-1}Hg = H$ for all $g \in G$, which is exactly the definition for a normal subgroup. With this, we see that H' is not only characteristic in H, it is also a normal subgroup of H.
Before we can draw conclusions about H and H' in J, we need to look at another lemma. This is an interesting lemma for our current situation, as it tells us that all squares of H are contained in index 2 subgroups, hence in H', the intersection of all index 2 subgroups of H.

Lemma 3.3.10. *Let H be a normal subgroup of a group G of index n. Then $x^n \in H$ for all elements x of G.*

Proof. Suppose $x \in H$, then by the properties of groups, $x^n \in H$ holds.
Suppose $x \notin H$. Then, xH is a proper element of the quotient group G/H. We know that $|G/H| = [G : H] = n$, so by Lagrange's Theorem, we have $(xH)^n = H$. Since H is normal in G, we also see that

$$(xH)^n = xHxHxH \cdots xH = x^nH. \tag{3.3}$$

This leads us to the conclusion that $x^nH = H$ holds, by which we see that x^n is an element of H. □

Now, we are well enough prepared to prove the following lemma. Essentially, it says that the quotient of H by H' as defined before is a 2-group when H is of odd index in G.

Lemma 3.3.11. *Let J be a group possessing the properties of Theorem 3.0.1, and H be a normal subgroup of J such that $|J/H|$ is odd. We define H' as the intersection of subgroups of H of index 2. Then $|H/H'| = 2^k$ for some natural number k.*

Proof. Take an element of H/H' and denote the representative for that element in H by x. By Lemma 3.3.10, we see that x^2 is contained in every subgroup of H of index 2, hence $x^2 \in H'$. This means that x^2 is trivial in H/H'. Therefore, $\mathrm{ord}(xH')$ is a divisor of 2. Since we had taken an arbitrary element of H/H', we see that all elements of H/H' are of the order 1 or 2. This means that H/H' has to be a 2-group, i.e. $|H/H'| = 2^k$ for some natural number k. □

With this lemma, we are almost ready to prove the main goal of this section; J attains no normal subgroups of odd index. But first, we have to prove one other lemma, which will happen in the next subsection.

3.3.3.2 Sylow 2-subgroups intersected with H' are not trivial

In this subsection, we once more take H to be a normal subgroup of J such that J/H is of odd order. We again define H' to be the intersection of all index 2 subgroups of H. The following lemma gives us interesting and useful information about H' in J.

Lemma 3.3.12. *Let K be a characteristic subgroup of H and let H be normal in G. Then K is normal in G.*

Proof. Since H is normal in G, $\gamma_g : G \to G$ defined as $\gamma_g(x) = g^{-1}xg$ for some $g \in G$ is an automorphism of H, as $g^{-1}Hg \subseteq H$. We can restrict the automorphism to H to get $\gamma_g : H \to H$. Since K is characteristic in H, we have $\gamma_g(K) = K$, thus $g^{-1}Kg = K$ for all $g \in G$. By definition, this means that K is normal in G. □

In Lemma 3.3.9, we had seen that H' is characteristic in H. Additionally, H was assumed to be normal in J. By Lemma 3.3.12, we therefore see that H' is a normal subgroup of J. Now we will look at a result that tells us something about the elements in a subgroup of index n.

Lemma 3.3.13. *Let H be a subgroup of G of index n. Then all elements of order coprime to n must be contained in H.*

Proof. Let $g \in G$ be an element, such that $\mathrm{ord}(g)$ is coprime to n. we have that $\mathrm{ord}(g) \mid |G|$ by Lagrange's Theorem. It is also known that

$$|G/H| = \frac{|G|}{|H|} = [G : H] = n.$$

Since $\mathrm{ord}(g)$ is coprime to n, $\mathrm{ord}(g) \nmid |G/H|$. Therefore, g has to be an element of H. □

The next two lemmas address results about Sylow p-subgroups of a group G and a normal subgroup H of G. The next one in particular tells us that all Sylow p-subgroups of G are subgroups of H in the case that the index of H is not divisible by p.

Lemma 3.3.14. *Let p be a prime and H be a normal subgroup of G such that the index of H is not divisible by p. Then the Sylow p-subgroups of G are contained in H.*

Proof. Let S be a Sylow p-subgroup of G. Take some arbitrary $s \in S$. Since S is a p-group, we have that $\text{ord}(s) = p^n$ for some positive integer n. As the index of H is not divisible by p, we can use Lemma 3.3.13 to find that $s \in H$ has to hold. Since s was chosen arbitrary in S, we can conclude that $S \subseteq H$. □

The following lemma focuses on the intersection of a Sylow 2-subgroup of a group G and a normal subgroup H of G. This will prove itself useful in the last lemma of this section, as well as in the final proof of Theorem 3.0.1.

Lemma 3.3.15. *Let H be a normal subgroup of G and S a Sylow 2-subgroup of G. Then $S \cap H = \{1\}$ implies that $|H|$ is odd.*

Proof. We assume to the contrary that H has even order. Then, by Cauchy's Theorem, there exists an element $h \in H$ of order 2. This element is contained in a Sylow 2-subgroup of G, which we will denote by S'. We know that all Sylow 2-subgroups are conjugates by Theorem 3.0.3. Therefore, we can find a $g \in G$ such that $g^{-1}S'g = S$. Therefore, $g^{-1}hg \in S$. Since H is normal in G, $g^{-1}hg \in H$ holds. This leads to a contradiction, which shows our desired result. □

The last lemma of this subsection will demonstrate that the intersection of H' as defined before and a Sylow 2-subgroup of J is not trivial. This is also the last preliminary lemma needed to prove J cannot have a proper normal subgroup of odd index.

Lemma 3.3.16. *Let J be a group with the properties of Theorem 3.0.1. Let H be a normal subgroup of J such that J/H is of odd order. Define H' as the intersection of subgroups of H of index 2. Then $H' \cap S$, for S a Sylow 2-subgroup of J, contains a non-trivial element.*

Proof. By Lemma 3.3.9, H' is characteristic in H. We took H to be normal in J, so by Lemma 3.3.12, H' is normal in J.
By Lemma 3.3.14, H contains a Sylow 2-subgroup S of J. Assume to the contrary that $S \cap H' = \{1\}$. This implies that H' has to have odd order by Lemma 3.3.15. So H' is a normal subgroup of J of odd order. By Lemma 3.2.1, we see that $H' = \{1\}$. Then, by Lemma 3.3.13, H cannot have an element of odd order other than 1. If H would contain non-trivial elements of odd order, such elements would be contained in all index 2 subgroups of H by Lemma 3.3.13, and thus in the intersection of index 2 subgroups of H. However, H' is the trivial subgroup, hence H has no non-trivial elements of odd order. By Cauchy's Theorem, the order of H needs to be a power of 2. This means that H is a 2-group. By Lemma 3.3.8, we know that $C(i) \subseteq H$. This however gives us a contradiction, as $C(i)$ is not a 2-group and thus can't possibly be contained in a 2-group. Therefore, our assumption that $S \cap H' = \{1\}$ holds cannot be true. □

3.3.4 Proof of Lemma 3.3.1

As stated before, this subsection aims to prove that J has no proper normal subgroups of odd index. Using our preparatory lemmas, this is relatively easy to prove.

Proof of Lemma 3.3.1. Define H' to be the intersection of subgroups of H of index 2. Using Lemma 3.3.16, we see that $S \cap H'$ contains a non-trivial element. Since S is of the type $[2, 2, 2]$ as seen in Lemma 3.1.2, $H' \cap S$ contains an involution. This means that H' also has to contain an involution. Since all involutions in J are conjugated (see Lemma 3.1.1) and H' is normal in J (see Lemma 3.3.12), i.e. closed under conjugation, H' must contain all involutions of J as it contains at least one. As S consists of involutions and the trivial element, $S \subseteq H'$. A Sylow 2-subgroup is maximal, which means that H/H' will have odd order. By Lemma 3.3.11, we see that $|H/H'| = 2^k$ for some natural number k. Therefore,

$|H/H'| = 1$ has to hold and thus $H = H'$. This implies that H has no subgroup of index 2. We also know that the Sylow 2-subgroups of H, which are the same as the Sylow 2-subgroups of J, are abelian and that there exists an involution $i \in H$ for which $C(i) \cong \langle i \rangle \times A_5$ (see Lemma 3.3.8). Therefore H satisfies the properties of Theorem 3.0.1. It is known that $N_H(S) \subseteq N_J(S)$. By Lemma 3.1.10, we see that $N_H(S)$ has order 168, as does $N_J(S)$. Therefore, we can conclude that $N_J(S) = N_H(S)$. Using Lemma 3.3.2, we see that $J = N_J(S)H = N_H(S)H$. Since $N_H(S) \subseteq H$, we get that $N_H(S)H = H$. Now, we can conclude that $J = H$. □

This lemma concludes this section. We have seen Frattini's Argument, as well as multiple lemmas about homomorphisms and their properties. We have seen a lemma about normal subgroups of a direct product of simple groups. We have furthermore seen results about characteristic subgroups, in addition to lemmas telling us about properties of subgroups of certain indices. It became apparent that $C(i) \subseteq H$, that H/H' is a 2-group and that $H' \cap S \neq \{1\}$, by which we could prove that J contains no non-trivial normal subgroup of odd index.

3.4 Proof of simplicity

Now, we have arrived at the point where we are ready to prove our main theorem. Since we have done a lot of preliminary work with a lot of lemmas and results, completing the proof of Theorem 3.0.1 will be quite easy. For clarity, we will write the theorem here once more, followed by its proof.

Theorem 3.4.1. *[6, p. 147] Let J be a finite group with the following properties:*

1. *The Sylow 2-subgroups of J are abelian;*
2. *J contains an involution i such that $C(i) \cong \langle i \rangle \times A_5$;*
3. *J has no subgroup of index 2.*

Then J is a simple group.

Proof. Let H be a normal subgroup of J. With Lemma 3.2.1, we have seen that H is trivial when it is of odd order. Lemma 3.3.1 tells us that H is equal to J if $|J/H|$ is odd. Lastly, we need to look at the case where $H \neq \{1\}$, $H \neq J$ and both H and J/H are of even order.
Let S be a Sylow 2-subgroup of J. Then $H \cap S \neq S$, otherwise J/H would have odd order as S is a maximal 2-group. We also see that $H \cap S \neq \{1\}$ by Lemma 3.3.15. This means that there exist some $x, y \in S$ such that $xH = H$ and $yH \neq H$. We know that x and y are involutions (by Lemma 3.1.2) and that those are conjugated in J, which means that there is a $j \in J$ such that $j^{-1}xj = y$. Then we have that $yH = j^{-1}xjH$. Since H is normal in J, we find that $yH = j^{-1}xHj = j^{-1}Hj = H$, which is a contradiction. This means that J has no non-trivial normal subgroups, hence J is simple. □

Chapter 4

Formalization

In addition to proving the simplicity of J_1 on paper, we also attempt to start the formalization of the proof of Theorem 3.0.1. This will happen in the programming language *Lean*. In this chapter, we will give an introduction to the proof assistant Lean, as well as an insight in our progress to formalize the theorem in Lean.

4.1 Lean

Lean is a proof assistant that was first developed in 2013 [10, p. 625]. Leonardo de Moura designed a programming language that ensures mathematical correctness if a result is properly formalized [13, p. 251]. Lean can ensure this, as it checks the proofs from the logical foundations of mathematics [11]. Nevertheless, it is not necessary for users of Lean to prove theorems and lemmas from these foundations as there exist an online 'library' of definitions and theorems already defined and proven, called *mathlib* [10, p. 625]. We will see more about this later on.

Lean is a programming language based on dependent type theory, which means that every expression in Lean is associated to a certain *Type* [14]. These types are dependent on variables, which explains the name of the theory. An especially useful example of types are *Type Classes*. If we continuously need to use an argument `a` of `type A`, we can save us some work by defining a `class` where this argument is already specified [14]. Then, if we summon `a`, we do not need to specify its type again.

Another useful feature in Lean is the possibility to formalize theorems, temporarily without their proof. For example, if we know that a lemma is true, but cannot prove it yet for some reason, we write `sorry`, which will automatically produce a 'proof' of the statement [15]. This so-called proof is obviously not conclusive, otherwise nothing would need to be proven anymore. Usually, users use `sorry` to build the frame of a (long) proof in Lean [15], as it is a good indicator if there are enough increments and if these are placed correctly.

4.1.1 Mathlib

Four years after the start of the Lean project, users created *mathlib*, a mathematical library for Lean [10, p. 625]. As of June 2024, mathlib contains more than 79000 definitions and 150000 theorems ready for use [16]. It is an ever growing collection of files that users provide. Every Lean user can expand mathlib by making a *Pull Request* of their modified local file [12]. Before that change is final, the lines of code need to be checked by mathlib maintainers to ensure that the mathematics is correct and complete [12]. After passing another test called *Continuous Integration*, the changes can be uploaded to mathlib [12]. This is also called committing the changes to the master, where the master branch is the "production" version of mathlib [12]. All these checks and testing ensure that there are no faulty files (for example files containing `sorry` as a proof) merged to the master.

Mathlib can be accessed via every browser[i]. Most of the mathematics in mathlib is at an undergraduate level [17, p. 2]. It contains, but is not limited to, (linear) algebra, category theory, geometry, analysis and topology [17, p. 2].

[i] https://leanprover-community.github.io/mathlib4_docs/

4.2 Formalization of Theorem 3.0.1

For the formalization of Theorem 3.0.1, we started with coding almost all of our results in Chapter 3 using `sorry`. We maintained the layout of Chapter 3. All the lemmas we were unable to implement in Lean, are mentioned as comments in the file. From there, we were able to prove our theorem, stating that a group `G` possessing the three properties is simple. After that, we began replacing `sorry` of the preliminary lemmas with their actual proof.

We did not finish formalizing the theorem in Lean completely. Some lemmas, mostly the lemmas containing a statement about p-normal groups, are not implemented in Lean yet. Additionally, the lemmas stated in Chapter 3.1, need to be modified. In the written lemmas, we use the Sylow 2-subgroup that contains the involution such that its centralizer satisfies property 2 of Theorem 3.0.1. The implementation of these lemmas in Lean is too general now, as they use any Sylow 2-subgroup. Due to the lack of knowledge about Lean, as we only learned about it six months ago, we were not able to make these changes.

The final product of our formalization can be found on *GitHub* via the link https://github.com/roxyvdk/theorem-Janko1-Lean.

Bibliography

[1] R. Solomon, A brief history of the classification of the finite simple groups, *Bulletin of the American Mathematical Society*, **38** (2001), no. 3, p. 315–352.

[2] R. Wilson, *The Finite Simple Groups*, Springer, Londen, 2009.

[3] D. Dummit & R. Foote, *Abstract Algebra*, John Wiley & Sons Inc, Hoboken, 2004.

[4] M. Aschbacher, The Status of the Classification of the Finite Simple Groups, *Notices of the American Mathematical Society*, **51** (2004), no. 7, p. 736–740.

[5] R. Giess, The Friendly Giant, *Invent Math*, **69** (1982), p. 1–102.

[6] Z. Janko, A New Finite Simple Group with Abelian Sylow 2-Subgroups and Its Characterization, *Journal of Algebra*, **3** (1966), p. 147–186.

[7] R. Curtis, Symmetric generation and existence of the Janko group J_1, *Journal of Group Theory*, **2** (1999), p. 355–366.

[8] C. Chevalley, "Le groupe de Janko", in: Séminaire Bourbaki (red), *Séminaire Bourbaki: années 1966/67 1967/68, exposés 313-346*, Ch. 331, Paris, 1968.

[9] M. Hall Jr, *The Theory of Groups*, The Macmillan Company, New York, 1963.

[10] L. de Moura & S. Ullrich, "The Lean 4 Theorem Prover and Programming Language" in: A. Platzer (red), *Automated Deduction – CADE 28*, p. 625–635, Cham, 2021.

[11] *Lean Community*, https://leanprover-community.github.io/ (consulted June 9, 2024).

[12] *How to contribute to mathlib*, https://leanprover-community.github.io/contribute/index.html (consulted June 9, 2024).

[13] F. van Doorn, G. Ebner & R. Lewis, "Maintaining a Library of Formal Mathematics", in: C. Benzmüller (red), *Intelligent Computer Mathematics*, p. 251–267, Cham, 2020.

[14] *Theorem Proving in Lean 4: Inductive Types*, https://lean-lang.org/theorem_proving_in_lean4/inductive_types.html (consulted June 9, 2024).

[15] *Theorem Proving in Lean 4: Propositions and Proofs*, https://lean-lang.org/theorem_proving_in_lean4/propositions_and_proofs.html (consulted June 9, 2024).

[16] *Mathlib statistics*, https://leanprover-community.github.io/mathlib_stats.html (consulted June 9, 2024).

[17] The mathlib Community, *The Lean Mathematical Library*, Association for Computing Machinery, New York, 2020.