Diploma Thesis

On The Groups Of Cube-Free Order

by

Heiko Dietrich

Tutor
Professor Dr. Bettina Eick

Institute Computational Mathematics
Technical University Carolo-Wilhelmina at Braunschweig
Pockelsstr.14
38106 Braunschweig

Germany

Braunschweig, March 18, 2005

Statement of Originality (Eidesstattliche Erklärung)

I certify that this thesis, and the research to which it refers, are the product of my own work, and that any ideas or quotations from the work of other people, published or otherwise, are fully acknowledged in accordance with the standard referencing practices of the discipline.

(Deutsch) Hiermit bestätige ich an Eides statt, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Hilfsmittel verfasst habe.

Braunschweig, March 18, 2005

(Signature)

Contents

Chapter 1

Introduction

"The mathematical sciences particularly exhibit order, symmetry, and limitation; and these are the greatest forms of the beautiful."
Aristotle (383 B.C. – 322 B.C.)

Nowadays the theory of groups has applications in the most branches of mathematics and also in many areas of science, for example quantum theory, crystallography, and cryptography. Therefore it is a natural ambition to know as much as possible about the different structures of groups and it is an interesting problem in group theory to construct all groups of a certain order up to isomorphism.

The general idea of classification is to find for a given order n an explicit list of groups so that every group of order n is isomorphic to a group in the list and no two groups in the list are isomorphic to each other. The primary difficulty is not to determine a list containing all possible isomorphism types but to reduce this list to isomorphism type representatives.

In this thesis we consider the special type of groups whose order factorizes in a certain form: the groups of cube-free order or the so-called cube-free groups; that is, we investigate the groups of order n where the prime-power factorization of n is of the form $n = p_1^{e_1} \cdots p_r^{e_r}$ with $e_i \in \{1, 2\}$. Hence, the aims of this thesis are to describe the structure of the groups of cube-free order and to develop an algorithm to construct all groups of a given cube-free order up to isomorphism.

Unless otherwise noted, all considered groups are finite.

1.1 Approach and results

Depending on the structure or significant properties of the considered groups - for example p-groups or solvable groups - there exist different approaches to classify them. For more details see [4, 5].

The approach of this thesis to construct the groups of cube-free order is based on the *Frattini extension method.* This method is also described in [4, 5] and has been used to construct the groups of order at most 2 000. It follows a brief survey of this method.

Let G be a finite group. The Frattini subgroup $\Phi(G)$ of G is defined to be the intersection of all maximal subgroups of G. Since the Frattini factor $G/\Phi(G)$ has a trivial Frattini subgroup, every finite group is an extension of a Frattini-free group by its Frattini subgroup. In particular, a group G is a Frattini extension of a group H by an H-module M if there exists a normal subgroup $N \trianglelefteq G$ with $N \cong M$ and $G/N \cong H$ such that $G/\Phi(G) \cong H/\Phi(H)$.

Thus the main idea to construct all groups of cube-free order n is as follows:

1. Determine the list $\mathcal{F}$ of all possible Frattini factors up to isomorphism.
2. For each $F \in \mathcal{F}$ determine the list $\mathcal{E}_F$ of all Frattini extensions of order n of F up to isomorphism.

Then the union of all elements in $\mathcal{E}_F$, $F \in \mathcal{F}$, forms a complete and irredundant list of groups of order n.

Motivated by this method, the following three main theorems will be proved in this thesis; see Theorem 2.7, Theorem 7.8, and Corollary 7.13.

Theorem 1: *The group G is a simple group of cube-free order if and only if $G \cong C_p$ for a prime p or $G \cong PSL(2, r)$ for a prime $r > 3$ with $r + 1$ and $r - 1$ cube-free.*

Theorem 2: *Every cube-free group is either solvable or it is a direct product of a non-abelian simple group with a solvable group.*

Theorem 3: *There is a one-to-one correspondence between the solvable cube-free groups of order $n = p_1^{e_1} \dots p_r^{e_r}$ (prime-power factorization) and the solvable Frattini-free groups F with $|F| \mid n$ and $p_1 \dots p_r \mid |F|$.*

Taunt [28] has also considered the solvable groups of cube-free order, since he has investigated solvable groups with abelian Sylow subgroups. Compared to the approach of Taunt, the approach of this thesis has the advantage that it translates to an effective construction algorithm – which is the second aim of this thesis.

An implementation of this algorithm is available in GAP [29], see [10], and a published version of some of the results of this thesis can be found in [11].

1.2 Structure of the thesis

The above algorithm – that is, the Frattini extension method – motivates the steps of this thesis:

As a preliminary step, Chapter 2 investigates the cube-free groups within the classes of simple and nilpotent groups, respectively. Some special matrix groups of cube-free order are examined in Chapter 3. For this purpose a brief introduction into module theory is needed. Chapter 4 gives an introduction into the theory of group extensions and cohomology groups. We go back to the results of these chapters in later examinations.

The construction of all possible Frattini factors relies on [16], where Gaschütz prepared the classification of the Frattini-free groups. For this purpose Chapter 5 examines the Frattini subgroup of a group. The theory of Frattini-free groups is presented in Chapter 6. In particular, we examine the socle of a group and the Fitting-free groups, and then provide a theorem of Gaschütz. Applying this theorem, we investigate the structure of the cube-free Frattini-free groups.

The cube-free groups are discussed in Chapter 7. We investigate Frattini extensions and exhibit the main results of this thesis. Therefore Chapter 7 completes our theoretical examinations of the cube-free groups.

A group whose order is not divisible by any prime-square is called a square-free group. Chapter 8 applies the results of Chapter 6 to the case of groups of square-free order.

Chapter 9 gives a summary of the results and an outlook on further possible investigations.

Finally, in Chapter 10 the algorithm to construct all groups of a given cube-free order is presented. Also a report on experiments with the implementation of this algorithm is included.

1.3 Historical remarks

The origins of the axiomatic group theory are settled in the middle of the 18th century. At this time, mathematicians like Joseph Louis Lagrange (1736 – 1813), Paulo Ruffini (1765 – 1822), and Évariste Galois (1811 – 1832) investigated the theory of algebraic equations and the corresponding permutations of roots of polynomials. In 1854 Arthur Cayley (1821 – 1895) developed the concept of an abstract group. He denoted the group elements by abstract symbols and defined the group operation in an abstract way. Some years later Walther von Dyck (1856 – 1934) introduced the presentations of groups.

The idea to construct all groups of a given order has been initiated by Cayley [7] and it has developed a long history since then. We refer to [5] for an overview. Historically, the approaches to this problem involved a large number of hand-computations and case distinctions. Therefore many of them contained significant errors.

It follows a small selection of some papers dealing with groups whose order factorizes in a certain way. The symbols p, q, and r denote distinct primes.

Introducing the idea of an abstract group, Cayley [7, 8] considered the cyclic groups and groups of order 4, 6, and 8 in the middle of the 19th century. In 1893 Hölder [19] examined the groups of order p^3, p^2q, pqr, and p^4.

The groups of square-free order have been known for a long time; Hölder [21] investigated the square-free groups in the year 1895.

The groups of order p^5 were investigated for example by Bagnera [2], Miller [22], Schreier [26] and Bender [3].

Western [34] considered groups of order p^3q and Le Vavasseur [31, 32] examined groups of order p^2q^2.

In the beginning of the 20th century Tripp [30] considered groups of order p^3q^2 and Potron [23, 24] was engaged in groups of order p^6. In 1988 Wilkinson [35] examined groups of order p^7.

As mentioned before, Taunt [28] discussed the solvable groups of cube-free order in the middle of the 20th century.

In 1938 Fitting [14] developed a concept to construct all finite groups. Fifteen years later Gaschütz acted on this suggestion and modified this concept in [16]. The results of Gaschütz play a fundamental role in this thesis.

Chapter 2

Special types of cube-free groups

In this chapter we consider some special classes of groups and determine the cube-free groups in them. We will utilize most of these results in later investigations.

2.1 Nilpotent groups

As a first step, we examine the structure of cube-free p-groups. The m-fold direct product of cyclic groups of order n is denoted with C_n^m.

2.1. Lemma: *Let G be a group with $|G| \in \{p, p^2\}$ for a prime p. Then $G \cong S$ for some $S \in \{C_p, C_{p^2}, C_p^2\}$.*

Proof: This is well-known: One can show readily that G has to be abelian, see [25], Proposition 1.6.15, and then the assertion follows from [25], Proposition 4.2.10. •

We recall that $P \leq G$ is a Sylow p-subgroup of the finite group G if P is a p-group and $p \nmid [G : P]$. Further, a finite group is nilpotent if and only if it is a direct product of its Sylow subgroups; that is, if and only if every Sylow subgroup is normal. Together with Lemma 2.1 this implies the following theorem.

2.2. Theorem: *Let G be a nilpotent group of cube-free order. It follows that $G \cong S_{p_1} \times \ldots \times S_{p_r}$ for distinct primes $p_1, \ldots, p_r$ and $S_p \in \{C_p, C_p^2, C_{p^2}\}$ for every prime p.*

2.2 Simple groups

A group $G \neq \{1\}$ is said to be simple if $\{1\}$ and G are the only normal subgroups of G. The classification of the finite simple groups was one of the major projects in the theory of finite groups in the last century. The existent proof is divided into over 500 papers, which were published between 1950 and 1980, and there is no complete proof published yet. For more details and a list of all finite simple groups up to isomorphism we refer to [9] and [17].

We recall that every finite group G has a composition series; that is, there exists a sequence of subgroups $G = G_1 \rhd G_2 \rhd \ldots \rhd G_l \rhd G_{l+1} = \{1\}$ with simple composition factors G_i/G_{i+1} for $1 \leq i \leq l$. It follows that every composition factor of a cube-free group is a simple group of cube-free order. Thus the simple groups of cube-free order are the basic building blocks for all groups of cube-free order and, consequently, the results of this section will be used as a basis for later investigations.

As a preliminary step some comments concerning the notation follow. Let $n \in \mathbb{N}$. With A_n and S_n we denote the alternating group and the symmetric group of degree n, respectively. For a prime power q the symbol $\mathrm{GL}(n, q)$ denotes the group of invertible $n \times n$ matrices over the finite field $\mathbb{F}_q$ with q elements. The subgroup $\mathrm{SL}(n, q) \leq \mathrm{GL}(n, q)$ consists of all matrices with determinant 1. If G is a group, then $\zeta(G) = \{g \in G \mid \forall h \in G : hg = gh\}$ denotes its center.

2.3. Lemma: *Let $Z = \zeta(GL(n, q))$. The projective linear group is defined by $PGL(n, q) = GL(n, q)/Z$ and the projective special linear group is given by $PSL(n, q) = SL(n, q)/(Z \cap SL(n, q))$. Let $k = \gcd(q-1, n)$ and $l = n(n-1)/2$.*

a) $|PSL(n, q)| = q^l(q^n - 1) \cdots (q^2 - 1)/k$,

b) $|PGL(n, q)| = k|PSL(n, q)|$,

c) $PSL(2, 4) \cong PSL(2, 5) \cong A_5$.

Proof: Proofs can be found in [20], Theorems (II, 6.2) and (II, 6.14). •

Using the classification theorem of the finite simple groups, it is straightforward to determine the simple groups of cube-free order. Nevertheless, we are able to provide an alternative proof not based on the classification theorem. Our proof uses the Odd-Order Theorem of Feit and Thompson.

2.4. Theorem (ODD-ORDER THEOREM)**:** *Every group of odd order is solvable.*

Proof: The proof of this important theorem is about 254 journal pages and can be found in [13]. •

We recall that a group G acts on a group H if there exists a group homomorphism $\psi : G \to \mathrm{Aut}(H)$ from G into the group of automorphisms of H. Usually one identifies $g^\psi = g$ and writes $h^g = h^{(g^\psi)}$ for $g \in G$ and $h \in H$.

2.5. Corollary: *The order of a non-abelian simple group is divisible by 4.*

Proof: Let G be a group of order n. Since G acts on itself via right multiplication, there is a mapping $G \to S_n$, $g \mapsto \overline{g}$, and thus a homomorphism $\sigma : G \to \{\pm 1\}$, $g \mapsto \text{sign}(\overline{g})$. Let $g \in G$ be an element of order r and let $\{g_1, \ldots, g_k\}$ be a left transversal to $\langle g \rangle$ in G; that is, $k = n/r$. One can observe that $\overline{g}$ written as a permutation has the form

$$\overline{g} = (g_1, g_1 g, g_1 g^2, \ldots, g_1 g^{r-1}) \ldots (g_k, g_k g, g_k g^2, \ldots, g_k g^{r-1})$$

and, as $\text{sign}((g_i, g_i g, g_i g^2, \ldots, g_i g^{r-1})) = (-1)^{r-1}$, we have $g^\sigma = \left((-1)^{r-1}\right)^k$.
Now let G be non-abelian simple. By the Odd-Order Theorem it follows that $2 \mid n$. Suppose that $4 \nmid n$; that is, $n = 2k$ and k is odd. Then there is $g \in G$ with $|g| = 2$ and $n/|g| = k$ is odd; that is, $g^\sigma = -1$. The Isomorphism Theorem shows that $G/\ker \sigma \cong \{\pm 1\}$ and therefore $\ker \sigma$ is a normal subgroup of G of index 2. This is a contradiction and thus $4 \mid n$. •

It follows that the order of a cube-free non-abelian simple group G has the form $|G| = 4k$ and k is odd. The next theorem classifies this special type of simple groups.

2.6. Theorem: *If G is a non-abelian simple group with $|G| = 4k$ and k is odd, then $G \cong PSL(2, q)$ for some prime-power q.*

Proof: A proof can be found in [18], Theorem 2. •

The main result of this section follows.

2.7. Theorem: *The group G is a simple cube-free group if and only if*

a) $G \cong C_p$ for a prime p or

b) $G \cong PSL(2, p)$ for a prime $p > 3$ with $p + 1$ and $p - 1$ cube-free.

Proof: We observe that $|\text{PSL}(2, p)| = p(p-1)(p+1)/2$ and $\gcd(p-1, p+1) = 2$ for an odd prime p. Hence, by [20], Theorem (II, 6.11), it follows that the groups listed in a) and b) are simple groups of cube-free order, and it is left to show that these are the only groups with this property.

Every abelian simple group is isomorphic to a group in a). By Theorem 2.6, every non-abelian simple group G of cube-free order is isomorphic to a group $\text{PSL}(2, q)$ for some prime-power $q = p^r$. Then the order of G is given by $|G| = q(q^2 - 1)/k$ where $k = \gcd(q - 1, 2)$. Suppose that this order is cube-free. Then:

- $r \in \{1, 2\}$ holds: If $r \geq 3$, then $p^3 \mid q$ and $|G|$ is not cube-free.
- $r = 1$ holds if p is odd: If $r = 2$, then $|G| = q(q + 1)(q - 1)/2 = q(q + 1)$ $(p-1)(p+1)/2$ holds and hence $8 \mid |G|$ follows, since $4 \mid p - 1$ or $4 \mid p + 1$.
- Now $p \in \{2, 3\}$ can be ignored: $\text{PSL}(2, 2)$ and $\text{PSL}(2, 3)$ are not simple and $\text{PSL}(2, 4) \cong \text{PSL}(2, 5)$ is covered by b).

- Now p is odd and $r = 1$ holds. Thus $|G| = p(p+1)(p-1)/2$ with $\gcd(p+1, p-1) = 2$. Hence $|G|$ is cube-free if and only if $p+1$ and $p-1$ are cube-free.

This completes the proof. •

Chapter 3

Subgroups of GL$(2, p)$

Let p be a prime and let $G \leq \mathrm{GL}(2,p)$ be a subgroup such that $p^2|G|$ is cube-free. If $\mathbb{F}_p^2$ is the natural G-module, then the group $G \ltimes \mathbb{F}_p^2$ is cube-free and a prototype for later constructions. Thus, as a preliminary step, the examination of these matrix subgroups follows. We will exhibit that each of these groups is solvable.

3.1 Module theory

First, we recall some notations and an important representation theoretical theorem of Maschke to which we also refer in later investigations. A more detailed description and proofs can be found in [25], Section 8.1. All considered vector spaces are finite-dimensional.

3.1. Definition: Let G be a finite group.

a) An abelian group $(A, +)$ is a *G-module* if G acts on A; that is, there exists a homomorphism $\psi : G \to \mathrm{Aut}(A)$. One often identifies $g^\psi = g$ for $g \in G$.

b) Let A and B be G-modules and let $\psi : A \to B$ be a group homomorphism. If $(a^g)^\psi = (a^\psi)^g$ holds for all $a \in A$ and $g \in G$, then ψ is a *G-module homomorphism.* The set of all G-module homomorphism from A to B is denoted by $\mathrm{Hom}_G(A, B)$.

c) Let A be a G-module and let $B \leq A$. If $b^g \in B$ for all $b \in B$ and $g \in G$, then B is a *G-submodule* of A.

d) If the only G-submodules of a G-module A are $\{0\}$ and A, then A is called *irreducible.*

It is well-known that $\mathrm{Hom}_G(A, B)$ has the structure of an abelian group.

3.2. Lemma: *Let A be a G-module. If G is a simple group, then G is either isomorphic to a subgroup of $Aut(A)$ or A is trivial as a G-module.*

Proof: Denote with $\psi : G \to \mathrm{Aut}(A)$ the action of G on A. As G is simple, it follows that $\ker\psi \in \{G, \{1\}\}$. If $\ker\psi = \{1\}$, then, by the Isomorphism Theorem, it follows that $G \cong G^\psi \leq \mathrm{Aut}(A)$. The case $\ker\psi = G$ implies that G acts trivially on A. •

Obviously, if $G \cong C_p \cong A$ for a prime p, then A is trivial as a G-module.

Now we recall the definition of an R-module for a ring R with identity element.

3.3. Definition: Let R be a ring with identity element.

a) An abelian group $(A, +)$ is an *R-module* if there is a mapping $R \times A \to A$, $(r, a) \mapsto ra$, such that the following holds for all $a, b \in A$ and $r, s \in R$:

- $r(a + b) = ra + rb$,
- $(r + s)a = ra + sa$,
- $(rs)a = r(sa)$, and
- $1a = a$ where $1 \in R$.

b) An R-module A is a *free R-module* if A has an R-basis; that is, there exists $\{a_1, \ldots, a_m\} \subseteq A$ such that every $a \in A$ can be written uniquely as $a = \sum\limits_{i=1}^{m} r_i a_i$ with $r_i \in R$.

c) If M is a non-empty set, then the set of all formal sums

$$\sum_{m\in M} r_m m \quad \text{with} \quad r_m \in R$$

together with the following rules of addition

$$\sum_{m\in M} r_m m + \sum_{m\in M} r'_m m = \sum_{m\in M} (r_m + r'_m) m$$

and multiplication

$$r(\sum_{m\in M} r_m m) = \sum_{m\in M} r r_m m, \quad (r \in R),$$

forms a free R-module with basis M.

d) Let A, B be R-modules and let $\psi : A \to B$ be a group homomorphism. If $(ra)^\psi = r(a^\psi)$ holds for all $a \in A$ and $r \in R$, then ψ is called an *R-module homomorphism*. The abelian group of all these homomorphisms is denoted by $\mathrm{Hom}_R(A, B)$.

e) An *exact sequence* of R-modules is a sequence of R-modules $(A_i)_{i\in\mathbb{N}_0}$ together with a sequence of mappings $(\mu_i)_{i\in\mathbb{N}}$ with $\mu_i \in \mathrm{Hom}_R(A_i, A_{i-1})$ and $\ker\mu_i = \mathrm{im}\,\mu_{i+1}$ for $i \geq 1$.

The next definition considers a special type of a ring which is induced by a group.

3.4. Definition: Let G be a finite group.

a) Let R be a ring with identity element. The *group ring* $RG = \{\sum_{g\in G} r_g g \mid r_g \in R\}$ is the free R-module with basis G together with the rule of multiplication

$$(\sum_{g\in G} r_g g)(\sum_{h\in G} r'_h h) = \sum_{g\in G}(\sum_{g=yz} r_y r'_z)g.$$

b) Let F be a field. The *group algebra of* G *over* F is the group ring FG together with the F-module structure given by

$$(\sum_{x\in G} f_x x)^f = \sum_{x\in G}(ff_x)x, \quad (f \in F).$$

Obviously, the group ring RG is a ring with identity element and the group algebra FG, in addition to be a ring, is a vector space over F with $(uv)^f = u^f v = uv^f$ for all $u, v \in FG$ and $f \in F$. We identify $g \in G$ with $1g \in RG$ and $1g \in FG$, respectively.

In particular, if A is a G-module, then we define an action of $\sum\limits_{g\in G} z_g g \in \mathbb{Z}G$ on $a \in A$ by

$$\sum_{g\in G} z_g a^g = \sum_{g\in G} \operatorname{sign}(z_g)\,\underbrace{(a^g + \ldots + a^g)}_{|z_g|\text{ times}} \in A,$$

which furnishes A with the structure of a $\mathbb{Z}G$-module. Conversely, every $\mathbb{Z}G$-module structure on A yields a G-module structure on A. Thus it is common to write Hom_G instead of $\mathrm{Hom}_{\mathbb{Z}G}$.

3.5. Definition: Let G be a group and let F be a field. An F-vector space A is called an *FG-module* if A is an FG-module in the sense of Definition 3.3a) together with the property that $g(a^f) = g^f a = (ga)^f$ for all $g \in FG$, $f \in F$ and $a \in A$.

An important example is the field $\mathbb{F}_p$, a matrix group $G \leq \mathrm{GL}(n,p)$ and the n-dimensional F-vector space $\mathbb{F}_p^n$. Using the well-known multiplications, the group $\mathbb{F}_p^n$ is the so-called natural $\mathbb{F}_pG$-module.

3.6. Definition: We consider a group G, a field F, and an FG-module A.

a) A subspace $B \leq A$ of the F-vector space A is an *FG-submodule* if $gb \in B$ for all $b \in B$ and $g \in FG$.

b) Let A be the *sum* of two FG-submodules U and V; that is, $A = U + V = \{u + v \mid u \in U,\ v \in V\}$. If $U \cap V = \{1\}$, then A is the *direct sum* of U and V and we write $A = U \oplus V$.

c) If $\{0\}$ and A are the only FG-submodules of A, then A is called *irreducible*.

d) The FG-module A is called *completely reducible* if every FG-submodule B of A has a complement; that is, there exists an FG-submodule $C \leq A$ with $A = B \oplus C$.

Similar to vector spaces, the intersection and sum of two FG-submodules are FG-submodules. Next, it follows a useful equivalence.

3.7. Lemma: *Let A be an FG-module. Then A is completely reducible if and only if A is the direct sum of irreducible FG-submodules.*

Proof: "$\Rightarrow$" Let $S = S_1 + \ldots + S_r$ be the sum of all irreducible FG-submodules of A. If $S < A$, then there exists an FG-submodule $T \neq \{0\}$ with $A = S \oplus T$. Since T contains an irreducible FG-submodule of A, we obtain a contradiction to the choice of S and hence it follows that $A = S$. Let $W \leq A$ be maximal with respect to be a direct sum of some S_i. If $W < A$, then there exists $1 \leq j \leq r$ with $S_j \not\leq W$ and $U = W \oplus S_j$ is an FG-submodule of A with $W < U$. This contradiction yields that $A = W$.

"$\Leftarrow$" Let $A = S_1 \oplus \ldots \oplus S_r$ be the direct sum of irreducible FG-submodules and let $V \leq A$ be an arbitrary FG-submodule. Since A is finite-dimensional, there is an FG-submodule U being maximal with respect to $U \cap V = \{0\}$. If $U \oplus V < A$, then there exists $1 \leq j \leq r$ with $S_j \cap (U \oplus V) = \{0\}$ and $U < U \oplus S_j$. If $v = u + s \in V \cap (U \oplus S_j)$ with $u \in U$ and $s \in S_j$, then $v - u \in S_j \cap (U \oplus V)$ and hence $v - u = 0$. This shows that $v = u \in V \cap U = \{0\}$ and thus $V \cap (U \oplus S_j) = \{0\}$ which contradicts the choice of U. Hence the assertion follows. •

Now we can phrase Maschke's Theorem, see also [25], Proposition 8.1.2, and the examination of the required matrix groups follows.

3.8. Theorem (Maschke)**:** *Let G be a finite group and let F be a field whose characteristic does not divide the order of G. Then every FG-module is completely reducible.*

Proof: Let V be an FG-module and let $W \leq V$ be an FG-submodule. There is a subspace $U \leq V$ with $V = U \oplus W$ (as subspaces). The aim is to modify the subspace U to obtain an FG-submodule and for this purpose we define

$$\Theta : V \to W,\ v \mapsto \frac{1}{|G|} \sum_{g \in G} g^{-1} \pi(gv)$$

where

$$\pi : V = U \oplus W \to W,\ v = u + w \mapsto w.$$

Note that $|G|$ is invertible in F by assumption. One can check readily that Θ is a linear mapping with $\Theta(hv) = h\Theta(v)$ for all $v \in V$ and $h \in G$. Therefore

$L = \ker\Theta$ is an FG-submodule of V which complements W in V: Let $v \in V$ with $\Theta(v) = w$. Then $l = v - w$ satisfies $\Theta(l) = \Theta(v) - \Theta(w) = w - w = 0$ and thus $l \in L$. This shows that $v = l + w \in L + W$ and $V = L + W$. If $w \in L \cap W$, then $0 = \Theta(w) = w$ and hence $L \cap W = \{0\}$. Together we have $V = L \oplus W$ and V is completely reducible. •

3.2 Matrix groups

For a prime p we consider a subgroup $G \leq \mathrm{GL}(2,p)$ and the corresponding group algebra $\mathbb{F}_pG$. As mentioned before, the $\mathbb{F}_p$-vector space $\mathbb{F}_p^2$ can be considered as the natural $\mathbb{F}_pG$-module. It follows readily that the $\mathbb{F}_pG$-submodules of $\mathbb{F}_p^2$ are exactly the subgroups of $\mathbb{F}_p^2$ which are invariant under the action of G; these subgroups are called G-invariant. Thus the irreducible $\mathbb{F}_pG$-submodules are exactly the minimal G-invariant subgroups.

For the sake of completeness we recall that the group algebra $\mathbb{F}_pG$ acts (or is) reducible if there exists a proper non-trivial $\mathbb{F}_pG$-submodule of $\mathbb{F}_p^2$. Equivalently, we also say that G acts (or is) reducible if there exists a proper non-trivial G-invariant subgroup of $\mathbb{F}_p^2$. Otherwise, $\mathbb{F}_pG$ and G, respectively, are said to act (or to be) irreducible.

As a preliminary step, some useful definitions follow. With $N_G(U) = \{g \in G \mid U^g = U\}$ we denote the normalizer of a subgroup $U \leq G$ in G.

3.9. Definition: Let p be a prime.

a) The subgroup of all diagonal matrices of $\mathrm{GL}(2,p)$ is denoted by $\mathrm{D}(2,p)$.

b) The subgroup of all *monomial matrices* of $\mathrm{GL}(2,p)$ is defined as

$$\mathrm{M}(2,p) = \langle \mathrm{D}(2,p), a\rangle \quad \text{where} \quad a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

c) Let $\mathrm{S}(2,p) \leq \mathrm{GL}(2,p)$ and $\mathrm{N}(2,p) \leq \mathrm{GL}(2,p)$ be defined by

$$\mathrm{S}(2,p) = \langle b\rangle \quad \text{with} \quad b = \begin{pmatrix} 0 & 1 \\ -\alpha^{p+1} & \alpha + \alpha^p \end{pmatrix}$$

and

$$\mathrm{N}(2,p) = \langle b, c\rangle \quad \text{with} \quad c = \begin{pmatrix} 1 & 0 \\ \alpha + \alpha^p & -1 \end{pmatrix}$$

where α is a generator of the multiplication group of the field $\mathbb{F}_{p^2}$. The group $\mathrm{S}(2,p)$ is called a *Singer cycle* of $\mathrm{GL}(2,p)$.

3.10. Lemma: *The Singer cycle $S(2,p)$ is cyclic of order $p^2 - 1$. The group $N(2,p)$ is the normalizer of $S(2,p)$ in $GL(2,p)$ and $[N(2,p) : S(2,p)] = 2$.*

Proof: A proof and a more detailed description can be found in [27], Theorems 2.3.5 and 2.3.6, and in [15], Section 4. •

Now we can examine the required matrix groups.

3.11. Lemma: *Let p be a prime and let $G \leq GL(2,p)$ be a subgroup with $p \nmid |G|$. Further, let $V = \mathbb{F}_p^2$ be the natural $\mathbb{F}_pG$-module.*

a) The group V is a direct product of G-invariant subgroups.

b) If G is reducible, then G conjugates into the group $D(2,p)$.

Proof: a) By Theorem 3.8, the $\mathbb{F}_pG$-module V is the direct sum of irreducible $\mathbb{F}_pG$-submodules; that is, the group V is the direct product of G-invariant subgroups.

b) Since G is reducible, there exists a non-trivial $\mathbb{F}_pG$-submodule $U < V$. Thus, by Theorem 3.8, the group V is the direct product of two proper G-invariant subgroups and therefore G is conjugated in $\mathrm{GL}(2,p)$ to a subgroup of $\mathrm{D}(2,p)$. •

It remains to consider the irreducible cube-free subgroups of $\mathrm{GL}(2,p)$. These subgroups are determined up to conjugacy by Flannery and O'Brien in [15], Section 4, and we use this to obtain the following.

3.12. Theorem: *Let p be a prime and let $G \leq GL(2,p)$. If G has cube-free order with $p \nmid |G|$, then G is conjugated in $GL(2,p)$ to a subgroup of $M(2,p)$ or to a subgroup of $N(2,p)$.*

Proof: If G is reducible, then it conjugates into the group $\mathrm{D}(2,p) \leq \mathrm{M}(2,p)$ by Lemma 3.11. Therefore let G be irreducible. By [15], Theorems 4.1 – 4.4, the group G is either conjugated in $\mathrm{GL}(2,p)$ to a subgroup of $\mathrm{N}(2,p)$ or $\mathrm{M}(2,p)$, or it has a central quotient $G/\zeta(G)$ of isomorphism type in $\{A_4, S_4, A_5, \mathrm{PSL}(2,p), \mathrm{PGL}(2,p)\}$. If $G/\zeta(G) \cong S_4$, then $8 \mid |G|$ and G is not cube-free. If $p > 5$ and $G/\zeta(G)$ is of the isomorphism type A_4 or A_5, then, by [15], Theorem 4.5 and Theorem 4.8, respectively, the group G has a center of even order and thus $8 \mid |G|$. One can check readily that the same holds in the case of $p \in \{2,3,5\}$. Since $p \mid |\mathrm{PSL}(2,p)|$ and $p \mid |\mathrm{PGL}(2,p)|$, the theorem is proved. •

It is obvious that $U \in \{\mathrm{M}(2,p), \mathrm{N}(2,p)\}$ is solvable; that is, U has a series $U = U_1 \geq \ldots \geq U_l \geq U_{l+1} = \{1\}$ of normal subgroups $U_i \trianglelefteq U$ with abelian factors U_i/U_{i+1} for $1 \leq i \leq l$. As a subgroup of a solvable group is solvable as well, it follows that every cube-free group $G \leq \mathrm{GL}(2,p)$ with $p \nmid |G|$ is solvable.

For the sake of completeness we recall an equivalent definition of a solvable group: A group U is solvable if and only if there exists $i \in \mathbb{N}$ with

$$U = U^{(0)} \rhd \ldots \rhd U^{(i+1)} = \{1\}$$

where $U^{(j+1)} = (U^{(j)})'$ and $G' = \langle g^{-1}h^{-1}gh \mid g, h \in G \rangle$ denotes the commutator subgroup of a group G. The integer i is called the derived length of U.

Chapter 4

Extensions

It follows an introduction into the theory of group extensions. Then we provide some useful results on cohomology theory. We will use these results in later investigations.

4.1 Group extensions

First, we recall the definition of an extension.

4.1. Definition: Let G, H, and M be finite groups. The group G is an *extension* of H by M, if there exists $N \trianglelefteq G$ with $N \cong M$ and $G/N \cong H$.

Obviously, if G is an extension of H by M, then one can identify N and M as well as G/N and H.

Now we introduce some notations and recall several well-known facts concerning group extensions. For further background we refer to [25], Chapter 11, and [20], Sections I.14 and I.16.

Let H be a group and let $(A, +)$ be an H-module. For an arbitrary mapping $\gamma : H \times H \to A$ with

$$\forall h, k, l \in H : \quad \gamma(h, k) + \gamma(l, hk) = \gamma(lh, k) + \gamma(l, h)^k$$

we define a group

$$G_\gamma = \{(h, a) \mid h \in H, a \in A\}$$

with group operation

$$(h_1, a_1)(h_2, a_2) = (h_1 h_2, a_1^{h_2} + a_2 + \gamma(h_1, h_2)).$$

Then G_γ has a normal subgroup $A \cong \{1\} \times A$ with factor group $G_\gamma/A = H \times \{1\} \cong H$; that is, G_γ is an extension of H by A.

Conversely, if G is an extension of a group H by an abelian group A with $A \trianglelefteq G$ and $G/A = H$, then the action

$$H \to \mathrm{Aut}(A), \;\; gA \mapsto (A \to A, \; a \mapsto a^g)$$

furnishes A with the structure of an H-module and there exists a mapping $\gamma : H \times H \to A$ as above with $G \cong G_\gamma$. This partly motivates the following definition.

4.2. Definition: For a group H and an H-module A let

$$\begin{aligned} C^2(H,A) &= \{\gamma : H \times H \to A \mid \forall h \in H : \; \gamma(1,h) = \gamma(h,1) = 0\}, \\ Z^2(H,A) &= \{\gamma \in C^2(H,A) \mid \forall h,k,l \in H : \\ &\qquad\qquad \gamma(h,k) + \gamma(l,hk) = \gamma(lh,k) + \gamma(l,h)^k\}, \\ B^2(H,A) &= \{\gamma \in C^2(H,A) \mid \exists \delta : H \to A \; \forall k,h \in K : \\ &\qquad\qquad \gamma(k,h) = \delta(kh) - \delta(k)^h - \delta(h)\}. \end{aligned}$$

The elements of $Z^2(H,A)$ and $B^2(H,A)$ are called 2-*cocycles* and 2-*coboundaries*, respectively.

Obviously, $C^2(H,A)$ has the structure of an abelian group where the group operation is given by

$$(\gamma + \delta) : H \times H \to A, \;\; (h,k) \mapsto (\gamma + \delta)(h,k) = \gamma(h,k) + \delta(h,k),$$

and it follows that $B^2(H,A) \leq Z^2(H,A) \leq C^2(H,A)$.

4.3. Definition: Let H be a group and let A be an H-module.

a) The second *cohomology group* of H in A is defined by

$$\widehat{H}^2(H,A) = Z^2(H,A)/B^2(H,A).$$

b) The symbol $\mathcal{E}(H,A)$ denotes the set of all extensions of H by A up to isomorphism.

Originally the second cohomology group is denoted by $H^2(H,A)$, but for technical reasons we will temporarily use the "hat"-notation $\widehat{H}^2(H,A)$.

As indicated above, there is an important connection between the second cohomology group of H in A and the set $\mathcal{E}(H,A)$:

4.4. Theorem: *Let H be a group and let A be an H-module. For an extension G of H by A let $\overline{G} \in \mathcal{E}(H,A)$ be defined by $G \cong \overline{G}$. Then the mapping*

$$\widehat{H}^2(H,A) \to \mathcal{E}(H,A), \;\; \gamma + B^2(H,A) \mapsto \overline{G_\gamma}$$

is well-defined and onto.

Proof: This follows from [25], Proposition 11.1.4. •

Since the mapping of Theorem 4.4 does not have to be injective, it may occur that distinct elements of $\widehat{H}^2(H,A)$ induce isomorphic extensions of H by A:

4.5. Example: Let $H = V_4$ and let $A = C_2$. Then A is trivial as an H-module and one can show that $Z^2(H,A) \cong C_2^3$ and $B^2(H,A) = \{0\}$; that is, $|\widehat{H}^2(H,A)| = 8$. A complete and irredundant list of isomorphism types of groups of order 8 is given by

$$\begin{aligned} &C_8, \qquad C_2^3, \qquad C_4 \times C_2, \\ &D_8 = \langle x, y \mid x^4 = y^2 = x^y x = 1 \rangle, \\ &Q_8 = \langle x, y \mid x^4 = y^2 x^{-2} = x^y x = 1 \rangle. \end{aligned}$$

Since C_8 is not an extension of H by A, one obtains that $|\mathcal{E}(H,A)| = 4$.

This isomorphism problem is difficult to solve in general, but we will find an improvement of the situation.

4.6. Definition: Let G_i be an extension of a group H by an H-module A and let $A_i \trianglelefteq G_i$ be the subgroup corresponding to A for $i \in \{1,2\}$. Then G_1 and G_2 are *strongly isomorphic* if there exists an isomorphism $\iota : G_1 \to G_2$ with $A_1^\iota = A_2$.

The following theorem yields a criterion when two extensions are strongly isomorphic. The restriction of a mapping $f : A \to B$ to a subset $U \subseteq A$ is denoted as $f|_U$.

4.7. Theorem: *Let G_i be an extension of a finite group H by an H-module A via the cocycle ψ_i for $i \in \{1,2\}$. Denote with $\overline{h} \in Aut(A)$ the action of $h \in H$ on A and let T be the group of* compatible pairs*; that is,*

$$T = \{(\alpha,\beta) \in Aut(H) \times Aut(A) \mid \forall h \in H : \ \overline{h^\alpha} = (\overline{h})^\beta\},$$

which acts on $\widehat{H}^2(H,A)$ via

$$\gamma + B^2(H,A) \mapsto \gamma^{(\alpha,\beta)} + B^2(H,A)$$

where

$$\gamma^{(\alpha,\beta)} = \left[(l,h) \mapsto \gamma(l^\alpha, h^\alpha)^{\beta^{-1}}\right].$$

Then G_1 is strongly isomorphic to G_2 if and only if there exists an element $(\alpha,\beta) \in T$ such that $\psi_1^{(\alpha,\beta)} \equiv \psi_2 \bmod B^2(H,A)$.

Proof: We identify $G_i = G_{\psi_i}$ and $A = \{1\} \times A \leq G_i$ for $i \in \{1,2\}$. It is straightforward, but technical, to prove that T is a group which acts on $\widehat{H}^2(H,A)$ via the above defined operation. A more detailed description and references can be found in [4], Section 4.2.1.

"$\Rightarrow$" Let $\iota : G_1 \to G_2$ be a strong isomorphism. Since $A^\iota = A$, the restriction $\iota|_A = \beta^{-1}$ is an automorphism of A. Therefore ι induces an automorphism $\iota|_{G_1/A} = \alpha^{-1}$ on $H = G_1/A = G_2/A$. Let $(1, a), (h, 0) \in G_1$. The 2-cocycle condition yields that

$$\psi_1(h^{-1}, h) = \psi_1(h, h^{-1})^{\overline{h}}$$

and since

$$(h, a)^{-1} = (h^{-1}, -\psi_1(h, h^{-1}) - a^{\overline{h^{-1}}})$$

it follows that

$$(1, a)^{(h,0)} = (h, 0)^{-1}(1, a)(h, 0) = (1, a^{\overline{h}}).$$

The equation

$$(1, a)^{(h,0)^\iota} = ((h, 0)^{-1})^\iota (1, a)(h, 0)^\iota = (1, a)^{\iota^{-1}(h,0)\iota}$$

together with

$$(1, a)^{(h,0)^\iota} = (1, a^{\overline{h^{\alpha^{-1}}}}) \quad \text{and} \quad (1, a)^{\iota^{-1}(h,0)\iota} = (1, a^{\beta\overline{h}\beta^{-1}})$$

implies that $(\alpha^{-1}, \beta^{-1}) \in T$ and thus also $(\alpha, \beta) \in T$.

Let the mapping $\eta : H \to A$, $h \mapsto a_h$, be defined by

$$(h^\alpha, 0)^\iota = (h, a_h) \in G_2$$

and, as $a_1 = 0$, let $\gamma : H \times H \to A$, $(g, h) \mapsto a_{gh} - (a_g)^{\overline{h}} - a_h$, be the coboundary corresponding to η. The aim is to show that $\psi_1^{(\alpha,\beta)} + \gamma = \psi_2$. Let $g, h \in H$. It follows that

$$\begin{aligned}
((g^\alpha, 0)(h^\alpha, 0))^\iota &= (g^\alpha, 0)^\iota (h^\alpha, 0)^\iota \\
&= (g, 0)(1, a_g)(h, 0)(1, a_h) \\
&= (g, 0)(h, 0)(1, (a_g)^{\overline{h}})(1, a_h).
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
((g^\alpha, 0)(h^\alpha, 0))^\iota &= ((g^\alpha h^\alpha, 0)(1, \psi_1(g^\alpha, h^\alpha)))^\iota \\
&= (gh, a_{gh})(1, \psi_1(g^\alpha, h^\alpha)^{\beta^{-1}}) \\
&= (gh, 0)(1, a_{gh})(1, \psi_1^{(\alpha,\beta)}(g, h)).
\end{aligned}$$

Combining the results of these two equations, one obtains that

$$\begin{aligned}
(1, \psi_2(g, h)) &= (gh, 0)^{-1}(g, 0)(h, 0) \\
&= (1, a_{gh})(1, \psi_1^{(\alpha,\beta)}(g, h))(1, a_h)^{-1}(1, (a_g)^{\overline{h}})^{-1} \\
&= (1, \psi_1^{(\alpha,\beta)}(g, h))(1, a_{gh})(1, -a_h)(1, -(a_g)^{\overline{h}})
\end{aligned}$$

$$= \quad (1, \psi_1^{(\alpha,\beta)}(g,h) + \gamma(g,h))$$

which yields the first part of the equivalence.

"$\Leftarrow$" Let $(\alpha,\beta) \in T$ and $\gamma \in B^2(H,A)$ with $\psi_1^{(\alpha,\beta)} + \gamma = \psi_2$. By definition, there exists a function $\eta : H \to A$, $h \mapsto a_h$ corresponding to the coboundary γ, and we define

$$\iota : G_1 \to G_2,\ (h,a) \mapsto (h^{\alpha^{-1}}, a_{h^{\alpha^{-1}}} + a^{\beta^{-1}}).$$

If $(h,a),(g,b) \in G_1$, then it follows from the assumptions that

$$\begin{aligned}
(h,a)^\iota (g,b)^\iota &= (h^{\alpha^{-1}}, a_{h^{\alpha^{-1}}} + a^{\beta^{-1}})(g^{\alpha^{-1}}, a_{g^{\alpha^{-1}}} + b^{\beta^{-1}}) \\
&= ((hg)^{\alpha^{-1}}, (a_{h^{\alpha^{-1}}})^{\overline{g^{\alpha^{-1}}}} + (a^{\beta^{-1}})^{\overline{g^{\alpha^{-1}}}} + a_{g^{\alpha^{-1}}} + \\
&\qquad + b^{\beta^{-1}} + \psi_2(h^{\alpha^{-1}}, g^{\alpha^{-1}})) \\
&= ((hg)^{\alpha^{-1}}, (a_{h^{\alpha^{-1}}})^{\overline{g^{\alpha^{-1}}}} + a^{\overline{g}\beta^{-1}} + a_{g^{\alpha^{-1}}} + b^{\beta^{-1}} + \\
&\qquad + \psi_1(h,g)^{\beta^{-1}} - (a_{h^{\alpha^{-1}}})^{\overline{g^{\alpha^{-1}}}} - a_{g^{\alpha^{-1}}} + a_{(hg)^{\alpha^{-1}}}) \\
&= ((hg)^{\alpha^{-1}}, a^{\overline{g}\beta^{-1}} + b^{\beta^{-1}} + \psi_1(h,g)^{\beta^{-1}} + a_{(hg)^{\alpha^{-1}}}) \\
&= (hg, a^{\overline{g}} + b + \psi_1(h,g))^\iota \\
&= ((h,a)(g,b))^\iota
\end{aligned}$$

and therefore ι is a group homomorphism. As $a_1 = 0$, it is easy to see that ι is injective and hence, because $|G_1| = |G_2|$, it has to be surjective as well. Since $A^\iota = A$, it is shown that ι is a strong isomorphism from G_1 to G_2. •

Thus the T-orbits on $\widehat{H}^2(H,A)$ correspond one-to-one to the strong isomorphism classes of extensions of H by A.

Now we consider a special type of extensions.

4.8. Definition: An extension G of a group H by an H-module A is a *split extension* if $G \cong H \ltimes A$ where $H \ltimes A = G_{\gamma_0}$ with $\gamma_0 : H \times H \to A, (g,h) \mapsto 0$.

In particular, a group G is a split extension of $A \trianglelefteq G$ if and only if there is a subgroup $H \leq G$ with $G = HA$ and $H \cap A = \{1\}$. Then one also says that G splits over A. In this case $G \cong H \ltimes A$ where H acts on A via conjugation. The group H is called a complement to A in G.

4.9. Theorem: *Let H be a group and let A be an H-module. An extension of H by A is a split extension if and only if the corresponding element of $\widehat{H}^2(H,A)$ is trivial.*

Proof: A proof can be found in [25], Proposition 11.1.4. •

The investigation of the special case when H and A are cyclic with prime order follows.

4.10. Lemma: *Let $H \cong C_p$ be a group of prime order and let $h \in H$ be a generator. Let $A \cong C_p$ be trivial as an H-module.*

a) The mapping

$$\alpha : Z^2(H,A) \to A,\ \gamma \mapsto \sum_{i=1}^{p-1} \gamma(h, h^i)$$

is an epimorphism with kernel $B^2(H,A)$.

b) For $t \in A$ let

$$\gamma_t : H \times H \to A,\ (h^i, h^j) \mapsto \begin{cases} 0 & : \overline{i} + \overline{j} < p \\ t & : \overline{i} + \overline{j} \geq p \end{cases}$$

where $\overline{z} = z \bmod p$ for $z \in \mathbb{Z}$. Then $\gamma_t \in Z^2(H,A)$ and $\gamma_t^\alpha = t$.

c) The group $\widehat{H}^2(H,A)$ is of the isomorphism type C_p.

Proof: a) The mapping α is a homomorphism and it follows from b) that it is surjective. Let $\gamma \in B^2(H,A)$ and let $\delta : H \to A$ be the function corresponding to the coboundary γ. Then

$$\sum_{i=1}^{p-1} \gamma(h, h^i) = \sum_{i=1}^{p-1} \big(\delta(h^{i+1}) - \delta(h^i) - \delta(h)\big) = -\sum_{i=1}^{p} \delta(h) = 0$$

and thus $B^2(H,A) \leq \ker \alpha \leq Z^2(H,A)$.

Now let $\gamma \in \ker \alpha$. Then the corresponding group extension G_γ contains a subgroup

$$U = \langle (h, 0) \rangle = \{(h^j, \sum_{i=1}^{j-1} \gamma(h, h^i)) \mid 0 \leq j \leq p-1\}$$

of order p which complements $A = \{1\} \times A$ in G_γ. Therefore G_γ is a split extension of H by A and hence $\gamma \in B^2(H,A)$ by Theorem 4.9.

b) Let $t \in A$ and $0 \leq i, j, l \leq p-1$ be arbitrary. An elementary computation with case distinctions shows that

$$\gamma_t(h^i, h^j) + \gamma_t(h^l, h^{i+j}) = \gamma_t(h^{l+i}, h^j) + \gamma_t(h^l, h^i)$$

and hence $\gamma_t \in Z^2(H,A)$. Further, one obtains that

$$\gamma_t^\alpha = \sum_{i=1}^{p-1} \gamma_t(h, h^i) = \gamma_t(h, h^{p-1}) = t.$$

c) From a) it follows that

$$Z^2(H,A)/B^2(H,A) = Z^2(H,A)/\ker\alpha \cong A \cong C_p$$

and thus the lemma is proved. •

4.2 Cohomology groups

This section provides some properties of the second cohomology group and for this purpose we introduce a generalized definition of cohomology groups. For proofs and further background we refer to [20], Section (I, §16), as well as [1], Chapters 2 and 3, and [33], Chapters 1 – 3.

Throughout this section the action of a mapping f on an element x is written as $f(x)$; further, all considered modules are left modules.

Let $H \neq \{1\}$ be a finite group with a subgroup $P \leq H$ and let A be an H-module. We consider $\mathbb{Z}$ as a $\mathbb{Z}H$-module where the action of H on $\mathbb{Z}$ is trivial. By [20], Theorem (I, 16.11), there exists a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}H$-module; that is, an exact sequence

$$\ldots \to X_n \overset{\mu_n}{\to} X_{n-1} \to \ldots \to X_0 \overset{\mu_0}{\to} \mathbb{Z} \to 0$$

with free $\mathbb{Z}H$-modules X_i. In particular, this exact sequence is also a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}P$-module: Let X be a free $\mathbb{Z}H$-module with basis $\{x_1,\ldots,x_r\}$ and let $\{h_1,\ldots,h_k\}$ be a right transversal to P in H. Then $\mathbb{Z}H$ can be considered as a free $\mathbb{Z}P$-module with basis $\{h_1,\ldots,h_k\}$. Consequently, X is a free $\mathbb{Z}P$-module with basis $\{h_jx_i \mid 1 \leq i \leq r,\ 1 \leq j \leq k\}$.

Next, for every $i \in \mathbb{N}_0$ we define a homomorphism

$$\delta^i : \begin{cases} \mathrm{Hom}_H(X_{i-1},A) \to \mathrm{Hom}_H(X_i,A), \\ f \mapsto [x \mapsto f(\mu_i(x))]\,. \end{cases}$$

and obtain a sequence

$$\mathrm{Hom}_H(X_0,A) \overset{\delta^1}{\to} \mathrm{Hom}_H(X_1,A) \overset{\delta^2}{\to} \mathrm{Hom}_H(X_2,A) \to \ldots$$

of $\mathbb{Z}$-modules with $\mathrm{im}\ \delta^j \leq \ker\delta^{j+1}$ for all $j \in \mathbb{N}$ since $\ker\mu_j = \mathrm{im}\ \mu_{j+1}$.

4.11. Definition: With the above notations, for $n \in \mathbb{N}$ we define

$$H^n(H,A) = \ker\delta^{n+1}/\mathrm{im}\ \delta^n$$

as the nth *cohomology group* of the H-module A.

By [20], Theorem (I, 16.8), the definition of $H^n(H, A)$ does not depend on the choice of the free resolution of $\mathbb{Z}$. In particular, throughout this section we use the following free resolution to define $H^n(H, A)$:

For $i \in \mathbb{N}$ let X_i be the free $\mathbb{Z}H$-module generated by all elements of

$$\underbrace{H \setminus \{1\} \times \ldots \times H \setminus \{1\}}_{i \text{ times}},$$

and let $X_0 \cong \mathbb{Z}$ be the free $\mathbb{Z}H$-module generated by the abstract symbol $()$. Next, for $i \in \mathbb{N}$ we describe a $\mathbb{Z}H$-module homomorphism $\mu_i : X_i \to X_{i-1}$ via its action on the basis elements $(g_1, \ldots, g_i) \in X_i$ of X_i: We set

$$\mu_i(g_1, \ldots, g_i) \quad = \quad (g_2, \ldots, g_i) + \sum_{k=1}^{i-1} \varepsilon_k^i(g_1, \ldots, g_i) + (-1)^i g_i(g_1, \ldots, g_{i-1})$$

where

$$\varepsilon_k^i(g_1, \ldots, g_i) = \begin{cases} (-1)^k(g_1, \ldots, g_{k-1}, g_k g_{k+1}, g_{k+2}, \ldots, g_i) & : \text{if } g_k g_{k+1} \neq 1, \\ 0 & : \text{otherwise} \end{cases}$$

and further we define $\mu_0 : X_0 \to \mathbb{Z}$ via

$$\mu_0 : X_0 \to \mathbb{Z}, \ () \mapsto 1.$$

Then, by [1], Sections 16.1, 16.2, and 19.2, this yields a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}H$-module, which is called the normalized standard free resolution.

4.12. *Remark:* If one applies these definitions to the case $H = \{1\}$, then one obtains that $H^n(H, A) = \{0\}$ for all $n \in \mathbb{N}$.

4.13. Theorem: *If H is a group and A is an H-module, then*

$$H^2(H, A) \cong \widehat{H}^2(H, A).$$

Proof: Since a homomorphism is described completely by its action on a basis, one can observe that the mapping

$$\psi : \mathrm{Hom}_H(X_2, A) \to C^2(H, A), \ f \mapsto \widehat{f},$$

where

$$\widehat{f}\big|_{X_2} = f \quad \text{and} \quad \widehat{f}(1, h) = \widehat{f}(h, 1) = 0 \ \ (\forall h \in H)$$

is an isomorphism. Identifying $\mathrm{Hom}_H(X_2, A)$ with $C^2(H, A)$, it is straightforward to check that the induced second cohomology group $H^2(H, A)$ coincides with $\widehat{H}^2(H, A)$. •

4.14. Lemma: *Let $H \neq \{1\}$ be a group and let A be an H-module. If A is a p-group and $n \in \mathbb{N}$, then $H^n(H,A)$ is a p-group as well.*

Proof: Let $l = (|H|-1)^n$ and $n \in \mathbb{N}$. As in the proof of Theorem 4.13, one can identify $\mathrm{Hom}_H(X_n, A)$ with

$$C^n(H,A) = \{f : H^n \to A \mid f(h_1, \ldots, h_n) = 0 \text{ if there is } h_i = 1\}.$$

Since the mapping

$$C^n(H,A) \to A^l,\ \gamma \mapsto (\gamma(h_1, \ldots, h_n))_{h_1, \ldots, h_n \in H \setminus \{1\}}$$

is an isomorphism, one obtains that $|\mathrm{Hom}_H(X_n, A)| = |A|^l$ and thus $H^n(H,A)$ is a p-group. •

The next theorems define three useful mappings between cohomology groups and then partially translate them to the special case when the second cohomology group is defined as in Definition 4.3. Since much more theory is necessary to prove this theorem, we only refer to a proof.

4.15. Theorem: *Let H be a group and let A be an H-module. We consider a subgroup $P \leq H$ and a left transversal $\{h_1, \ldots, h_k\}$ to P in H. Let $n \in \mathbb{N}$.*

a) The inclusion $\widehat{res}^n(P,H) : Hom_H(X_n, A) \hookrightarrow Hom_P(X_n, A)$ induces a homomorphism

$$res^n(P,H) : H^n(H,A) \to H^n(P,A),$$

the so-called restriction-mapping.

b) For $g \in H$ let

$$\widehat{con}^n(P,g) : \begin{cases} Hom_P(X_n, A) \to Hom_{gPg^{-1}}(X_n, A) \\ f \mapsto \left[x \mapsto g(f(g^{-1}x))\right]. \end{cases}$$

Then $\widehat{con}^n(P,g)$ induces a homomorphism

$$con^n(P,g) : H^n(P,A) \to H^n(gPg^{-1}, A)$$

which is called the conjugation-mapping.

c) The mapping

$$\widehat{cor}^n(H,P) : \begin{cases} Hom_P(X_n, A) \to Hom_H(X_n, A) \\ f \mapsto \left[x \mapsto \sum\limits_{i=1}^{k} h_i(f(h_i^{-1}x))\right] \end{cases}$$

is independent of the choice of the transversal and it induces a homomorphism

$$cor^n(H,P) : H^n(P,A) \to H^n(H,A).$$

This is called the corestriction-mapping.

Proof: A proof can be found in [6], Section (XII, §8), or [33], Sections 2.3 and 2.4. •

As a consequence of the definitions, for $P_1 \leq P_2 \leq H$ and $x \in H$ and all $\gamma \in H^n(P_2, A)$ we have

$$\mathrm{con}^n(P_1, x)\mathrm{res}^n(P_1, P_2)(\gamma) = \mathrm{res}^n(xP_1x^{-1}, xP_2x^{-1})\mathrm{con}^n(P_2, x)(\gamma)$$

and

$$\mathrm{res}^n(P_1, P_2)\mathrm{res}^n(P_2, H)(\gamma) = \mathrm{res}^n(P_1, H)(\gamma).$$

4.16. Theorem: *With the notations of Theorem 4.15 one can observe the following:*

a) If one defines $H^2(P, A)$ via the normalized standard free resolution of $\mathbb{Z}$ as a $\mathbb{Z}P$-module and identifies $H^2(P, A)$ with $\widehat{H}^2(P, A)$, then the action of $x \in N_H(P)$ on $H^2(P, A)$ via $con^2(P, x)$ translates to an action on $\widehat{H}^2(P, A)$; written exponentially, that is to say

$$\gamma = f + B^2(P, A) \ \mapsto \ \gamma^x = f^x + B^2(P, A)$$

where

$$f^x = \left[(s, t) \mapsto f(xsx^{-1}, xtx^{-1})^x\right].$$

b) For $h \in H$ let $\widetilde{h} \in \{h_1, \ldots, h_k\}$ be defined by $hP = \widetilde{h}P$. Written exponentially, the explicit formula for $cor^2(H, P)$ in terms of the normalized standard free resolution is given by

$$cor^2(H, P) : \gamma + B^2(P, A) \mapsto \widehat{\gamma} + B^2(H, A)$$

where

$$\widehat{\gamma}(u, v) = \sum_{i=1}^{k} \gamma(\widetilde{uh_i}^{-1} uh_i, \widetilde{vuh_i}^{-1} v\widetilde{uh_i})^{h_i^{-1}}.$$

Proof: The proof is based on the more elaborated theory of cohomology groups presented in [33], Chapters 1 – 3, and can be found in [33], Propositions 2.5.1 and 2.5.2. •

Now we exhibit some useful properties of the mappings defined in Theorem 4.15.

4.17. Lemma: *With the notations of Theorem 4.15 it follows that*

$$cor^n(H, P)res^n(P, H)(\gamma) = [H : P]\gamma = \underbrace{\gamma + \ldots + \gamma}_{k \ times}, \qquad (\gamma \in H^n(H, A)).$$

Proof: Let $\gamma \in H^n(H,A)$; that is, $\gamma = f + \mathrm{im}\ \delta^n$ for some $f \in \mathrm{Hom}_H(X_n, A)$. Now the assertion follows from

$$\widehat{\mathrm{cor}}^n(H,P)\widehat{\mathrm{res}}^n(P,H)(f):\ x \mapsto \sum_{i=1}^{k} h_i(f(h_i^{-1}x)) = \sum_{i=1}^{k} f(x).$$

•

In particular, we have the following corollary.

4.18. Corollary: *Let H be a group and let A be an H-module. The order of $\gamma \in H^n(H,A)$, $n \in \mathbb{N}$, is a divisor of $|H|$.*

Proof: Since $H^n(\{1\},A) = \{0\}$, we have $\mathrm{res}^n(\{1\},H)(\gamma) = 0$. Now the assertion follows from Lemma 4.17 with $P = \{1\}$. •

The next aim is to show that for a p-group A with an H-module structure one can determine $H^2(H,A)$ from $H^2(P,A)$ where $P \leq H$ is a Sylow p-subgroup of H. For this issue some preliminaries are needed:

4.19. Definition: We consider a group H, an H-module A, and a subgroup $P \leq H$. An element $\gamma \in H^n(P,A)$ is *stable* if for every $x \in H$ we have

$$\mathrm{res}^n(P \cap xPx^{-1}, P)(\gamma) = \mathrm{con}^n(x^{-1}Px \cap P, x)\mathrm{res}^n(x^{-1}Px \cap P, P)(\gamma)$$

or equivalently

$$\mathrm{res}^n(P \cap xPx^{-1}, P)(\gamma) = \mathrm{res}^n(xPx^{-1} \cap P, xPx^{-1})\mathrm{con}^n(P,x)(\gamma).$$

The proof of the following lemma can be found in [6], Proposition (XII, 9.4).

4.20. Lemma: *With the notations of Definition 4.19 it follows that*

$$res^n(P,H)\,cor^n(H,P)(\gamma) = [H:P]\gamma$$

for every stable element $\gamma \in H^2(P,A)$.

Proof: Let H be written as a disjoint union of double cosets $H = \bigcup_i Px_iP$ with $x_i \in H$. We define $W_i = P \cap x_iPx_i^{-1}$ and consider a representation of P as a disjoint union of left W_i cosets; that is, $P = \bigcup_j y_{ji}W_i$ with $y_{ji} \in P$. Hence one can write

$$Px_i = \bigcup_j y_{ji}(Px_i \cap x_iP)$$

and

$$Px_iP = \bigcup_j y_{ji}(Px_iP \cap x_iP) = \bigcup_j y_{ji}x_iP.$$

This union is still disjoint: If $y_{j_1 i}x_i p_1 = y_{j_2 i}x_i p_2$ for some $p_1, p_2 \in P$, then $y_{j_2} \in y_{j_1 i}x_i P x_i^{-1}$. Now $y_{j_2 i}W_i = y_{j_1 i}W_i$ shows that $y_{j_2 i} = y_{j_1 i}$. Therefore H is the disjoint union of left P cosets

$$H = \bigcup_{i,j} y_{ji}x_i P$$

and it follows that

$$[H : P] = \sum_i [P : W_i]. \tag{4.1}$$

Let X_n be a part of the normalized standard free resolution of $\mathbb{Z}$ as a $\mathbb{Z}H$-module. If $f \in \mathrm{Hom}_P(X_n, A)$, then, by using the above transversals and the definitions, one can check readily that

$$\widehat{\mathrm{res}}^n(P,H)\widehat{\mathrm{cor}}^n(H,P)(f) = \sum_i \widehat{\mathrm{cor}}^n(P,W_i)\widehat{\mathrm{res}}^n(W_i, x_i P x_i^{-1})\widehat{\mathrm{con}}^n(P,x_i)(f)$$

Passing to cohomology, for a stable element $\gamma \in H^2(P,A)$ one obtains that

$$\begin{aligned}
&\mathrm{res}^n(P,H)\mathrm{cor}^n(H,P)(\gamma)\\
&\quad= \sum_i \mathrm{cor}^n(P, P\cap x_iPx_i^{-1})\mathrm{res}^n(P\cap x_iPx_i^{-1}, x_iPx_i^{-1})\mathrm{con}^n(P,x_i)(\gamma)\\
&\quad= \sum_i \mathrm{cor}^n(P, P\cap x_iPx_i^{-1})\mathrm{res}^n(P\cap x_iPx_i^{-1}, P)(\gamma),
\end{aligned}$$

and Lemma 4.17 proves the assertion:

$$\mathrm{res}^n(P,H)\mathrm{cor}^n(H,P)(\gamma) = \sum_i [P : P\cap x_iPx_i^{-1}]\gamma \overset{(4.1)}{=} [H : P]\gamma.$$

●

The proof of the next theorem is taken from [6], Proposition (XII, 10.1).

4.21. Theorem: *Let P be a Sylow p-subgroup of the group H and let A be a p-group with an H-module structure. Then $res^n(P,H)$ maps $H^n(H,A)$ monomorphically to $H^n(P,A)$ and the image consists of the stable elements of $H^n(P,A)$.*

Proof: From Lemma 4.14 it follows that $H^n(H,A)$ is a p-group and hence every element of $H^n(H,A)$ has p-power order. If $\gamma \in \ker \mathrm{res}^n(P,H)$, then, by Lemma 4.17, one obtains that

$$0 = \mathrm{cor}^n(H,P)\mathrm{res}^n(P,H)(\gamma) = [H : P]\gamma$$

and thus $\gamma = 0$ since $p \nmid [H : P]$. Therefore $\mathrm{res}^n(P,H)$ is a monomorphism from $H^n(H,A)$ to $H^n(P,A)$.

Let $\gamma = \mathrm{res}^n(P,H)(\delta)$ be an element of the image of $\mathrm{res}^n(P,H)$ and let $x \in H$ be arbitrary. Then $\mathrm{con}^n(H,x)(\delta) = \delta$ and thus

$$\begin{aligned}\mathrm{con}^n(P,x)(\gamma) &= \mathrm{con}^n(P,x)\mathrm{res}^n(P,H)(\delta) = \mathrm{res}^n(xPx^{-1},H)\mathrm{con}^n(H,x)(\delta)\\ &= \mathrm{res}^n(xPx^{-1},H)(\delta).\end{aligned}$$

It follows that

$$\begin{aligned}\mathrm{res}^n(xPx^{-1}\cap P, xPx^{-1})\mathrm{con}^n(P,x)(\gamma) &= \mathrm{res}^n(xPx^{-1}\cap P, H)(\delta)\\ &= \mathrm{res}^n(xPx^{-1}\cap P, P)\mathrm{res}^n(P,H)(\delta)\\ &= \mathrm{res}^n(xPx^{-1}\cap P, P)(\gamma)\end{aligned}$$

and therefore γ is stable.

Now suppose that $\gamma \in H^n(P,A)$ is stable. Then Lemma 4.20 shows that

$$\mathrm{res}^n(P,H)\mathrm{cor}^n(H,P)(\gamma) = [H:P]\gamma.$$

As $\gcd([H:P],|P|) = 1$, there exist $i,j \in \mathbb{Z}$ with $i[H:P] = 1 + j|P|$, and from Corollary 4.18 it follows that

$$\mathrm{res}^n(P,H)\big(i\mathrm{cor}^n(H,P)(\gamma)\big) = (1+j|P|)\gamma = \gamma \in \mathrm{im}\ \mathrm{res}^n(P,H).$$

•

Now we can state an important corollary.

4.22. Corollary: *Let $P \cong C_p$ be a Sylow p-subgroup of H and let $A \cong C_p$ be an H-module. Then*

$$\widehat{H}^2(H,A) \cong \{\gamma \in \widehat{H}^2(P,A) \mid \forall x \in N_H(P):\ \gamma = \gamma^x\}$$

with γ^x as in Theorem 4.16a).

Proof: It follows from Theorem 4.21 that the group $H^2(H,A)$ is isomorphic to $\{\gamma \in H^2(P,A) \mid \gamma \text{ stable}\}$. Since $\mathrm{res}^2(P,P) = [\gamma \mapsto \gamma]$ and $\mathrm{res}^2(\{1\},P) = [\gamma \mapsto 0]$, as $H^2(\{1\},P) = \{0\}$, one obtains that

$$H^2(H,A) \cong \{\gamma \in H^2(P,A) \mid \forall x \in N_H(P):\ \gamma = \mathrm{con}^2(P,x)(\gamma)\}.$$

Identifying $H^2(H,P)$ with $\widehat{H}^2(H,P)$ and using Theorem 4.16a), the assertion follows. •

4.23. *Remark:* From now on the group $H^2(H,A)$ will be identified with $\widehat{H}^2(H,A)$.

4.3 The Schur multiplicator

For the purpose of further examinations another cohomology theoretical theorem follows. We recall that every group G has a presentation; that is, there exists a free group F and a normal subgroup $R \trianglelefteq F$ with $G \cong F/R$.

4.24. Definition: For a group G with presentation $R \trianglelefteq F$ we define

$$\mathrm{M}(G) = (F' \cap R)/[F, R]$$

where

$$[F, R] = \langle f^{-1}r^{-1}fr \mid f \in F, r \in R\rangle.$$

The isomorphism type of $\mathrm{M}(G)$ is called the Schur multiplicator of G and it is independent from the presentation. For a more detailed description we refer to [25], Theorem 11.4.15, and to [20], Theorem (V, 23.5).

Denote with $\mathrm{Hom}(G, A)$ the abelian group of all group homomorphisms from the group G to the group A.

4.25. Theorem: *If G is a non-abelian simple group and A is trivial as a G-module, then*

$$H^2(G, A) \cong Hom(M(G), A).$$

Proof: This is a corollary of the Universal Coefficients Theorem; see [25], Theorem 11.4.18. •

The following corollary will be useful later.

4.26. Corollary: *Let $G = PSL(2, q)$ for a prime $q > 3$ and let $A \cong C_p$ for a prime $p > 2$ be a G-module. Then $H^2(G, A) = \{0\}$.*

Proof: By [9], Section 3.3, one obtains that $|\mathrm{M}(G)| = 2$, and therefore $\mathrm{Hom}(\mathrm{M}(G), A) = \{0\}$. Since G is simple and A is trivial as a G-module by Corollary 3.2, the assertion follows from Theorem 4.25. •

Chapter 5

The Frattini subgroup

As indicated in the introduction of this thesis, it is essential to study the structure and the properties of the Frattini subgroup of a group. Therefore this chapter yields some important propositions concerning the Frattini subgroup.

All proofs in this chapter can also be found in [16] or [20, 25].

As a first step, we recall the definition. Let $U < G$ be a proper subgroup of a group G. If there exists no subgroup $V < G$ with $U < V < G$, then U is called a maximal subgroup of G and this is denoted with $U <_m G$.

5.1. Definition: Let G be a group.

a) The *Frattini subgroup* $\Phi(G)$ of G is defined to be the intersection of all maximal subgroups of G.

b) If $\Phi(G) = \{1\}$, then G is called *Frattini-free.*

A subgroup $U \leq G$ is called characteristic if $U^\alpha = U$ holds for all $\alpha \in \mathrm{Aut}(G)$. Since group automorphisms map maximal subgroups on maximal subgroups, it follows from the definition that $\Phi(G)$ is a characteristic subgroup of G.

The Frattini subgroup $\Phi(G)$ has the characterizing property to consist of all elements of G which are unnecessary in every generating set of G; such elements are called non-generators of G.

5.2. Theorem: *The Frattini subgroup $\Phi(G)$ consists of all non-generators of G.*

Proof: Let $g \in \Phi(G)$. If g is not a non-generator of G, then there is $X \subseteq G$ with $\langle X, g\rangle = G$ and $\langle X\rangle < G$. Let $M < G$ be maximal with respect to $X \subseteq M$ and $g \notin M$. If $M < H \leq G$, then $g \in H$ and thus $H = G$. It follows that $H <_m G$. Since $g \in \Phi(G) \leq H$, this is a contradiction.

Now let $g \in G$ be a non-generator. If $g \notin \Phi(G)$, then there is $M <_m G$ with $g \notin M$. Hence it follows that $G = \langle M, g\rangle$ and since g is a non-generator, one obtains that $G = M$. This is a contradiction and it follows that $g \in \Phi(G)$. •

An immediate consequence is the following corollary.

5.3. Corollary: *Let $N \trianglelefteq G$. There is a subgroup $U < G$ with $G = UN$ if and only if $N \not\leq \Phi(G)$.*

The next lemmas list some more properties of the Frattini subgroup.

5.4. Lemma: *Let $N \trianglelefteq G$ be a normal subgroup. Then the following holds:*

a) $\Phi(G)N/N \leq \Phi(G/N)$.

b) If $N \leq \Phi(G)$, *then* $\Phi(G)/N = \Phi(G/N)$.

Proof: a) It is well-known that a subgroup $U \leq G/N$ has the form $U = V/N$ where $N \leq V \leq G$. One can prove immediately that $V/N <_m G/N$ if and only if $V <_m G$. Therefore $V/N <_m G/N$ implies that $\Phi(G)N \leq V$ and the assertion follows.

b) Part a) yields that $\Phi(G)/N \leq \Phi(G/N)$. If $M <_m G$, then $N \leq \Phi(G) \leq M$ and thus $M/N <_m G/N$. Hence it follows that $\Phi(G/N) \leq \Phi(G)/N$. •

In particular, Lemma 5.4 shows that the Frattini factor $G/\Phi(G)$ of a group G is always Frattini-free.

5.5. Lemma: *Let σ be a group homomorphism of G. Then $\Phi(G)^\sigma \leq \Phi(G^\sigma)$.*

Proof: Let $U <_m G^\sigma$ be a maximal subgroup and let $U^\star \leq G$ be the preimage of U under σ. If $U^\star < H \leq G$, then $U < H^\sigma \leq G^\sigma$ and thus $H^\sigma = G^\sigma$. Since $\ker\sigma \leq H$, it follows that $H = G$ and hence $U^\star <_m G$. The equation

$$(A \cap B)^\star = A^\star \cap B^\star$$

holds for all subgroups $A, B \leq G^\sigma$ and therefore

$$(\Phi(G^\sigma))^\star = \bigcap_{V <_m G^\sigma} V^\star.$$

This shows $\Phi(G) \leq (\Phi(G^\sigma))^\star$ and the assertion follows. •

One can observe that $\Phi(G)^\sigma \neq \Phi(G^\sigma)$ in general:

5.6. Example: Let $G = \langle a, b \mid a^5 = b^4 = a^{-1}b^{-1}a^2b = 1\rangle$. By Lagrange, the groups $\langle b\rangle$ and $\langle ab\rangle$ are maximal subgroups of G and it follows that G is Frattini-free. If $\sigma : G \to G/\langle a\rangle$, $g \mapsto g\langle a\rangle$, is the natural epimorphism, then $\Phi(G^\sigma) \cong \Phi(\langle b\rangle) = \langle b^2\rangle$ and thus $\Phi(G)^\sigma < \ \Phi(G^\sigma)$.

We provide two well-known lemmas:

5.7. Lemma: *Let $M \trianglelefteq G$. If $N \leq M$ is a characteristic subgroup of M, then $N \trianglelefteq G$.*

Proof: Since $\mathrm{Inn}(G)|_M = \{\alpha|_M \mid \alpha \in \mathrm{Inn}(G)\}$ is a subgroup of $\mathrm{Aut}(M)$, the group N is invariant under $\mathrm{Inn}(G)$ and hence $N \trianglelefteq G$. •

5.8. Lemma (Dedekind's Modular Law)**:** *Let $A, B, C \leq G$ with $A \leq C$ and $C \leq AB$. Then $C = AB \cap C = A(B \cap C)$.*

Proof: The equation $C = AB \cap C$ holds obviously. Let $c = ab \in C$ with $a \in A$ and $b \in B$. It follows that $b = a^{-1}c \in C$ and thus $c \in A(B \cap C)$. Conversely, if $c = ad \in A(B \cap C)$ with $a \in A$ and $d \in B \cap C$, then $c \in C$. •

Now we can prove the following:

5.9. Lemma: *Let $U \leq G$ be a subgroup and $N \trianglelefteq G$.*

a) If $N \leq \Phi(U)$, then $N \leq \Phi(G)$.

b) $\Phi(N) \leq \Phi(G)$.

Proof: a) If $N \not\leq \Phi(G)$, then there is a maximal subgroup $M <_m G$ with $N \not\leq M$. Hence $G = NM$ and Lemma 5.8 yields that $U = N(M \cap U)$. Since $N \leq \Phi(U)$, Lemma 5.2 applies and thus $U = M \cap U$ and $N \leq U \leq M$. This is a contradiction and therefore $N \leq \Phi(G)$.

b) Since $\Phi(N) \leq N$ is a characteristic subgroup, the assertion follows from Lemma 5.7 and a). •

If $U \leq G$ is not normal, then $\Phi(U) \not\leq \Phi(G)$ in general. An example is $D_8 = \langle(1,2,3,4),(1,4)(2,3)\rangle \leq S_4$ with $\Phi(D_8) = \langle(1,3)(2,4)\rangle$ and $\Phi(S_4) = \{()\}$.

5.10. Lemma: *If $G = G_1 \times G_2$, then $\Phi(G) = \Phi(G_1) \times \Phi(G_2)$.*

Proof: By Theorem 5.9, it follows that $\Phi(G_i) \leq \Phi(G_1 \times G_2)$ for $i \in \{1, 2\}$, and hence $\Phi(G_1) \times \Phi(G_2) \leq \Phi(G_1 \times G_2)$. The equation

$$\bigcap_{M <_m G_1 \times G_2} M \;\leq\; \bigcap_{A <_m G_1} (A \times G_2) \;\cap\; \bigcap_{B <_m G_2} (G_1 \times B),$$

implies that $\Phi(G_1 \times G_2) \leq \Phi(G_1) \times \Phi(G_2)$. •

5.11. Lemma: *If $A \trianglelefteq G$ is an abelian normal subgroup with $A \cap \Phi(G) = \{1\}$, then G splits over A.*

Proof: One can assume that $A < G$. Let $H \leq G$ be minimal with respect to $G = HA$. Since A is an abelian normal subgroup of G, it follows that $H \cap A \trianglelefteq HA = G$. If $H \cap A \leq \Phi(H)$, then $H \cap A \leq \Phi(G) \cap A = \{1\}$ by Lemma 5.9 and thus G splits over A. Conversely, if $H \cap A \not\leq \Phi(H)$, then there is $M <_m H$ with $H = M(A \cap H)$. It follows that $G = HA = MA$ which contradicts the choice of H. •

This yields the following important corollary. We recall that a minimal normal subgroup of G is a non-trivial normal subgroup that does not contain a smaller non-trivial normal subgroup of G.

5.12. Corollary: *Let $N \trianglelefteq G$ be an abelian minimal normal subgroup. There is a complement to N in G if and only if $N \not\leq \Phi(G)$.*

Proof: If $N \leq \Phi(G)$, then N is non-complemented in G by Corollary 5.3. If $N \not\leq \Phi(G)$, then G splits over N by Lemma 5.11. •

The next lemma is often referred to as the Frattini argument and, as a corollary, one obtains that the Frattini subgroup is always nilpotent. We recall that $\mathrm{Syl}_p(G)$ denotes the set of all Sylow p-subgroups of a group G and that all elements of $\mathrm{Syl}_p(G)$ are conjugated in G.

5.13. Lemma (Frattini argument)**:** *If $H \trianglelefteq G$ is a normal subgroup and $P \in Syl_p(H)$, then $G = N_G(P)H$.*

Proof: Let $g \in G$. It follows that $P^g \in \mathrm{Syl}_p(H)$ and thus there exists an element $h \in H$ with $P^g = P^h$. Then $gh^{-1} \in N_G(P)$ and $g \in N_G(P)H$. Since $N_G(P)H \leq G$, the assertion is proved. •

5.14. Corollary: *The Frattini subgroup $\Phi(G)$ of G is nilpotent.*

Proof: If $P \in \mathrm{Syl}_p(\Phi(G))$ is an arbitrary Sylow p-subgroup of $\Phi(G)$, then Lemma 5.13 and Theorem 5.2 yield that $G = N_G(P)\Phi(G) = N_G(P)$. It follows that every Sylow p-subgroup of $\Phi(G)$ is normal and hence $\Phi(G)$ is nilpotent. •

The following lemma provides an important property concerning the order of the Frattini subgroup.

5.15. Lemma: *If $p \mid |G|$ for a prime p, then $p \mid |G/\Phi(G)|$.*

Proof: Suppose that $p \nmid |G/\Phi(G)|$ and let $P \in \mathrm{Syl}_p(\Phi(G))$. The fact that $\Phi(G)$ is nilpotent implies that $P \leq \Phi(G)$ is a characteristic subgroup. Hence $P \trianglelefteq G$ and $\gcd(|P|, |G/P|) = 1$. By the Theorem of Schur-Zassenhaus, see [20], Theorem (I, 18.1), there exists a complement Q to P in G. Since $P \leq \Phi(G)$, it follows that $G = Q$, and this contradiction shows that $p \mid |G/\Phi(G)|$. •

As a final result of this section, Lemma 5.15 implies a corollary concerning the structure of the Frattini subgroup of a cube-free group.

5.16. Corollary: *If G is a cube-free group, then $\Phi(G) \cong C_{p_1} \times \ldots \times C_{p_k}$ for distinct primes $p_1, \ldots, p_k$.*

Proof: It follows from Lemma 5.15 that $|\Phi(G)|$ is square-free; that is, $|\Phi(G)| = p_1 \cdots p_k$ for distinct primes $p_1, \ldots, p_k$. The assertion holds, because $\Phi(G)$ is nilpotent. •

Chapter 6

Frattini-free groups

The main aim of this chapter is to provide a theorem of Gaschütz which classifies the groups with trivial Frattini subgroup. It turns out that every group F with trivial Frattini subgroup has the form $F = K \ltimes S$ where S is contained in the so-called socle of F and $K \leq \mathrm{Aut}(S)$. Hence, as a first step, we define and examine the structure of the socle of a group. Then we investigate the structure of the cube-free Frattini-free groups.

Concerning our aim to implement an algorithm to construct the cube-free Frattini-free groups of a given order, Section 6.5 supplies some notes on the construction of $K \leq \mathrm{Aut}(S)$ by so-called subdirect products.

6.1 Completely reducible groups

First, we recall the definition of the socle of a group.

6.1. Definition: The *socle* $\mathrm{Soc}(G)$ of a group G is the subgroup generated by all minimal normal subgroups of G.

In particular, the socle of a group is a characteristic subgroup since group automorphisms map minimal normal subgroups on minimal normal subgroups.

The group of inner automorphisms of G is defined by

$$\mathrm{Inn}(G) = \{\alpha \in \mathrm{Aut}(G) \mid \exists g \in G : \ \alpha = (G \to G, \ h \mapsto h^g)\}$$

and $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

The next definition generalizes the concept of a group. This is useful to prove the following theorem of Remak in a more general context.

6.2. Definition: An *operator group* is a triple (G, Ω, α) consisting of a group G, a set Ω called the *operator domain*, and a function $\alpha : G \times \Omega \to G$ such that $g \mapsto (g, \omega)^\alpha$ is a group endomorphism of G for every $\omega \in \Omega$. If the function α is understood, then we write g^ω for $(g, \omega)^\alpha$ and speak of the Ω-group G.

Thus an operator group is a group with a set of operators which act on the group like endomorphisms. In particular, every group is an operator group with empty operator domain.

Analogue to groups one can define Ω-subgroups: If G is an Ω-group, an Ω-subgroup of G is a subgroup $H \leq G$ such that $h^\omega \in H$ for all $h \in H$ and $\omega \in \Omega$. One can check readily that the intersection of a set of Ω-subgroups is an Ω-subgroup.

An Ω-subgroup $\{1\} < H \leq G$ is called Ω-simple if H has only the trivial normal Ω-subgroups. If $\Omega = \mathrm{Inn}(G)$, then the Ω-simple subgroups of G are exactly the minimal normal subgroups of G. If $\Omega = \emptyset$, then the Ω-simple subgroups of G coincide with the simple subgroups of G.

Next, we provide two theorems concerning the decomposition of a group. The proofs are basically from [25], Section 3.3.

6.3. Theorem (Remak)**:** *Let $G = G_1 \times \ldots \times G_n$ be an Ω-group where G_i is Ω-simple for $1 \leq i \leq n$. Suppose that N is a normal Ω-subgroup of G.*

a) There exists $M = \{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$ with $G = N \times G_{i_1} \times \ldots \times G_{i_t}$ and hence N is a direct product of Ω-simple groups.

b) If $\zeta(G) = \{1\}$, then N is the direct product of some G_i.

Proof: a) If $N = G$, then we take M to be empty. Now we assume that $N \neq G$ and hence there exists a group $G_i \not\leq N$. Since G_i is Ω-simple, it follows that $NG_i \cong N \times G_i$. Let $M \subseteq \{1, \ldots, n\}$ be maximal with regard to the property that

$$G_M = \langle N, G_j \mid j \in M \rangle \cong N \times \prod_{j \in M} G_j.$$

For every $j \in \{1, \ldots, n\} \backslash M$ it follows that $G_j \cap G_M \neq \{1\}$ and thus $G_j \leq G_M$. Therefore $G = G_M$ and a) is proved.

b) Factoring out any G_j contained in N, one can assume that $G_i \cap N = \{1\}$ for all $1 \leq i \leq n$. Since N and all G_i are normal in G, it follows that $[N, G_i] \leq N \cap G_i = \{1\}$; that is, elements of N commutate with elements of G_i for $1 \leq i \leq n$. This implies that $N \leq \zeta(G) = \{1\}$ and b) is proved. •

6.4. Theorem: *Let G be a group.*

a) A product of minimal normal subgroups of G is a direct product of some of them.

b) A minimal normal subgroup of G is a direct product of simple groups.

c) If G decomposes into a direct product of simple subgroups and $\zeta(G) = \{1\}$, then this decomposition is unique up to the order of the factors.

d) Let $H \leq N \leq G$ with $H, N \trianglelefteq G$. If N is a direct product of non-abelian simple groups, then there exists $M \trianglelefteq G$ with $M \leq N$ and $N = H \times M$, and M is a direct product of non-abelian simple groups.

Proof: a) Let $N = N_1 \cdots N_k$ be a product of minimal normal subgroups of G and let $P \leq N$ be maximal with respect to be a direct product of some N_i. If $P < N$, then there exists $N_j \not\leq P$ and thus $PN_j \cong P \times N_j$. This contradicts the choice of P and therefore $N = P$.

b) Let M be a minimal normal subgroup of G. By Lemma 5.7, the group M is characteristic simple; that is, M contains no smaller non-trivial characteristic subgroup of G. Let $U \leq M$ be a minimal normal subgroup of M and therefore $U^\alpha \cap U \in \{U, \{1\}\}$ for all $\alpha \in \mathrm{Aut}(M)$. Since M and $\mathrm{Aut}(M)$ are finite, it follows that

$$A = \langle U^\alpha \mid \alpha \in \mathrm{Aut}(M) \rangle = U^{\alpha_1} \times \ldots \times U^{\alpha_t}$$

for some $\alpha_1, \ldots, \alpha_t \in \mathrm{Aut}(M)$ and, as M is characteristic simple, one obtains that $A = M$. If there exists $\{1\} \lhd H \lhd U^{\alpha_j}$ for some $j \in \{1, \ldots, t\}$, then $H \lhd M$ which contradicts the choice of $U^{\alpha_j} \cong U$. Hence the groups $U^{\alpha_1}, \ldots, U^{\alpha_t}$ are simple and M is a direct product of simple groups.

c) A proof can be found in [25], Theorem 3.3.10.

d) Since $\zeta(N) = \{1\}$, part c) yields that the decomposition of N into simple groups is unique up to the order of the factors. Then, by Theorem 6.3, there exists an unique complement $M \trianglelefteq N$ of H in N. For all $g \in G$ it follows that

$$H \times M = N = N^g = H \times M^g$$

and thus $M = M^g$; that is, $M \trianglelefteq G$. •

In particular, every product N of minimal normal subgroups of a group G is completely reducible; that is, N is a direct product of simple groups. The following definition extends the definition of a completely reducible group.

6.5. Definition: Let G be a group and let $\mathrm{Inn}(G) \leq \Gamma \leq \mathrm{Aut}(G)$.

a) The group G is *completely reducible* if G is a direct product of simple groups.

b) A *minimal* Γ*-subgroup* of G is a subgroup $U \leq G$ which is minimal with respect to $U^\alpha = U$ for all $\alpha \in \Gamma$. The group G is called Γ*-completely reducible* if G is a product of minimal Γ-subgroups.

c) Let $N \trianglelefteq G$. Then N is G*-completely reducible*, if N is Γ-completely reducible for $\Gamma = \mathrm{Inn}(G)|_N$.

It follows from the definition that the socle of a finite group G is the largest normal subgroup of G which is G-completely reducible.

6.6. Lemma: *Let G be a group and let $N \trianglelefteq G$. Then the following properties are equivalent:*

a) N is G-completely reducible.

b) N is a direct product of minimal normal subgroups of G.

c) For every $M \trianglelefteq G$ with $M \leq N$ there exists $K \trianglelefteq G$ with $N = M \times K$.

Proof: "a)⇒ b)" This follows from Theorem 6.4a).

"b) ⇒ c)" This follows from Theorem 6.3.

"c) ⇒ a)" Let $M = N_1 \cdots N_t$ be the product of all minimal normal subgroups $N_i \trianglelefteq G$ with $N_i \leq N$. If $M < N$, then there exists $K \trianglelefteq G$ with $N = M \times K$ which contradicts the choice of M. It follows that $M = N$ and N is G-completely reducible. •

We recall that the class of nilpotent groups is closed under forming subgroups and that the product of two normal nilpotent subgroups is a normal nilpotent subgroup; see [20], Theorem (III, 4.1). This allows the following definition.

6.7. Definition: Let G be a group.

a) The Fitting subgroup $\mathrm{Fit}(G)$ of G is the unique largest normal nilpotent subgroup of G.

b) If $\mathrm{Fit}(G) = \{1\}$, then G is called *Fitting-free.*

It is easy to see that G is Fitting-free if and only if every abelian normal subgroup of G is trivial. Often this property is also called semisimple.

Since the socle of a group is completely reducible, the next theorem examines its structure.

6.8. Theorem: *Let S be a completely reducible group and let Rad(S) be the unique largest solvable normal subgroup of S.*

a) The group Rad(S) is a direct product of cyclic groups of prime order. In particular, Rad(S) is the product of all abelian minimal subgroups of S.

b) There exists an unique subgroup N$(S) \leq S$ with $S =$ Rad$(S) \times$ N(S). The group N(S) is Fitting-free and a direct product of non-abelian simple groups.

Proof: a) By Theorem 6.3, it follows that $\mathrm{Rad}(S)$ is a direct product of solvable simple groups. A solvable simple group H is abelian since it has a trivial commutator subgroup. Therefore H is cyclic of prime order. Now it follows from the definition that $\mathrm{Rad}(S)$ is the product of all abelian minimal normal subgroups of S.

b) Let N be the product of all non-abelian minimal normal subgroups of S. By Theorems 6.4a) and 6.3, the group N is Fitting-free and it follows that $N \cap \mathrm{Rad}(S) = \{1\}$ and thus $S = N \times \mathrm{Rad}(S)$. If K is a complement to $\mathrm{Rad}(S)$ in N, then $K \cong N$ and K is a direct product of non-abelian simple groups. Hence $K = N$ and we define $\mathrm{N}(S) = N$. •

6.9. Definition: Let S be a completely reducible group. The groups $\mathrm{Rad}(S)$ and $\mathrm{N}(S)$ in Theorem 6.8 are called the *abelian* and *Fitting-free components* of S.

In particular, $\mathrm{Rad}(S)$ and $\mathrm{N}(S)$ are characteristic subgroups of S.

Finally, we exhibit an important result of this section.

6.10. Theorem: *A completely reducible group S has cube-free order if and only if S has the form $S \cong A \times B \times C$ with*

- $A \in \{PSL(2,r) \mid r > 3$ *prime with* $r+1$ *and* $r-1$ *cube-free*$\} \cup \{\{1\}\}$,
- $B = C_{p_1} \times \ldots \times C_{p_n}$ *for different primes* $p_1, \ldots, p_n$ *with* $p_i^2 \nmid |A|$, *and*
- $C = C_{q_1}^2 \times \ldots \times C_{q_m}^2$ *for different primes* $q_1, \ldots, q_m \nmid |A||B|$.

Proof: The assertion follows from Theorem 2.7 together with the fact that $4 \mid |\mathrm{PSL}(2,p)|$ for every prime $p > 3$. •

6.2 Finite Fitting-free groups

We provide some useful propositions about Fitting-free groups. The main result of this section is the following theorem which will be used in later investigations.

6.11. Theorem: *Let S be a direct product of non-abelian simple groups and let A and B be groups with $Inn(S) \leq A, B \leq Aut(S)$. If there is a group isomorphism $\alpha : A \to B$, then there exists an element $\Theta \in Aut(S)$ with $a^\Theta = a^\alpha$ for all $a \in A$.*

Theorem 6.11 is proved by the subsequent theorems. We recall that the center of a direct product is the direct product of the centers. If G is a group and $M \subseteq G$ is a subset, then the centralizer of M in G is defined by $C_G(M) = \{g \in G \mid \forall m \in M: \ mg = gm\}$.

The proof of the next theorem is partially from [25], Proposition 3.3.18.

6.12. Theorem: *Let H be a finite Fitting-free group and $S = Soc(H)$.*

a) The socle S is a direct product of non-abelian simple groups.

b) The centralizer $C_H(S)$ of S in H is trivial.

c) There exists $Inn(S) \leq K \leq Aut(S)$ with $K \cong H$.

d) If T is a direct product of non-abelian simple groups and K is a group with $Inn(T) \leq K \leq Aut(T)$, then K is a finite Fitting-free group with socle $Soc(K) = Inn(T) \cong T$.

Proof: a) It follows from the assumptions that $\mathrm{Rad}(S) = \{1\}$. By Theorem 6.8b), the group $S = \mathrm{N}(S)$ is a direct product of non-abelian simple group.

b) Since S is normal in H, it follows that $C_H(S) \trianglelefteq H$. If $C_H(S) \neq \{1\}$, then there exists a minimal normal subgroup N of H in $C_H(S)$. Therefore

$N \leq S \cap C_H(S) = \zeta(S) = \{1\}$ which yields a contradiction.

c) Let $\tau : H \to \mathrm{Aut}(S)$ be the conjugation homomorphism; that is, τ maps $h \in H$ onto $h^\tau = (S \to S, s \mapsto s^h)$. It follows that $\ker \tau = C_H(S) \overset{\text{b)}}{=} \{1\}$ and hence H is isomorphic to $K = H^\tau$ with $\mathrm{Inn}(S) \leq K \leq \mathrm{Aut}(S)$.

d) Due to the fact that $\zeta(T) = \{1\}$ is the kernel of the conjugation homomorphism $\tau : T \to \mathrm{Inn}(T)$, it follows that $T \cong T^\tau = \mathrm{Inn}(T)$. Obviously, the group K is finite. If $\alpha \in C = C_{\mathrm{Aut}(T)}(\mathrm{Inn}(T))$, then the following equation holds for all $t \in T$:

$$t^\tau = \alpha^{-1} t^\tau \alpha = (t^\alpha)^\tau.$$

As τ is injective, it follows that $t = t^\alpha$ for all $t \in T$. Therefore $\alpha = 1$ and $C = \{1\}$. If $A \trianglelefteq K$ is an abelian normal subgroup, then $A \cap \mathrm{Inn}(T)$ is normal in $\mathrm{Inn}(T)$. Since $\mathrm{Inn}(T) \cong T$ is Fitting-free by Theorem 6.3, one obtains that $A \cap \mathrm{Inn}(T) = \{1\}$. Hence $A\mathrm{Inn}(T) = A \times \mathrm{Inn}(T)$ as A and $\mathrm{Inn}(T)$ are both normal in K. It follows that $A \leq C = \{1\}$ and therefore K is Fitting-free. In particular, the socle of K is a direct product of non-abelian simple groups.

The group $I = \mathrm{Inn}(T) \cap \mathrm{Soc}(K)$ is normal in K. By Theorem 6.4d), there exists a normal subgroup $M_1 \trianglelefteq K$ with $\mathrm{Inn}(T) = M_1 \times I$. It follows that

$$\mathrm{Soc}(K) \cap M_1 = \mathrm{Soc}(K) \cap M_1 \cap \mathrm{Inn}(T) = I \cap M_1 = \{1\}$$

and thus

$$\mathrm{Soc}(K)\mathrm{Inn}(T) = \mathrm{Soc}(K) I M_1 = \mathrm{Soc}(K) \times M_1$$

is a direct product of non-abelian simple groups. Applying Theorem 6.4d) again, there exists a normal subgroup $M_2 \trianglelefteq K$ with

$$\mathrm{Soc}(K)\mathrm{Inn}(T) = M_2 \times \mathrm{Inn}(T).$$

This shows that $M_2 \leq C = \{1\}$ and hence $\mathrm{Soc}(K) \trianglelefteq \mathrm{Inn}(T)$. Now there exists $M_3 \trianglelefteq K$ with $\mathrm{Inn}(T) = \mathrm{Soc}(K) \times M_3$. Since $M_3 \leq C_K(\mathrm{Soc}(K)) \overset{\text{a)}}{=} \{1\}$, it follows that $\mathrm{Soc}(K) = \mathrm{Inn}(T)$. •

Since isomorphic groups have isomorphic socles, the next theorem classifies the finite Fitting-free groups having a fixed isomorphism type of socle; see [25], Proposition 3.3.19.

6.13. Theorem: *Let S be a direct product of non-abelian simple groups and*

$$\mathcal{A} = \{H \mid \mathit{Inn}(S) \leq H \leq \mathit{Aut}(S)\}.$$

If $\mathcal{R}$ is a complete and irredundant list of conjugacy class representatives of $\mathcal{A}$ in Aut(S), then $\mathcal{R}$ is also a complete and irredundant list of isomorphism type representatives of

$$\mathcal{B} = \{H \mid H \text{ a finite Fitting-free group with } \mathit{Soc}(H) \cong S\}.$$

Proof: From Theorem 6.12d) it follows that $\mathcal{R} \subseteq \mathcal{A} \subseteq \mathcal{B}$. As a first step, we show that the isomorphism classes of $\mathcal{A}$ are exactly the conjugacy classes of $\mathcal{A}$ in $\mathrm{Aut}(S)$. Obviously, conjugated elements are isomorphic. Now let $H_1, H_2 \in \mathcal{A}$ be isomorphic groups with a group isomorphism $\alpha : H_1 \to H_2$. Since $\mathrm{Soc}(H_1) = \mathrm{Inn}(S) = \mathrm{Soc}(H_2)$ by Theorem 6.12d), one obtains that the restriction $\alpha|_{\mathrm{Inn}(S)}$ is an automorphism. Further, the conjugation homomorphism $\tau : S \to \mathrm{Inn}(S)$ is an isomorphism and hence

$$\Theta = \tau\alpha\tau^{-1} : S \to S, \quad s \mapsto s^{\tau\alpha\tau^{-1}},$$

is an automorphism with $\Theta\tau = \tau\alpha$. For all $s \in S$ and $f \in \mathrm{Aut}(S)$ we observe that

$$(s^f)^\tau = f^{-1} s^\tau f. \tag{6.1}$$

If $s \in S$ and $h \in H_1 \leq \mathrm{Aut}(S)$, then

$$\begin{aligned} (s^{\Theta^{-1}h\Theta})^\tau &= ((s^{\Theta^{-1}h})^\tau)^\alpha \overset{(6.1)}{=} (h^{-1}(s^{(\Theta^{-1})})^\tau h)^\alpha = (h^\alpha)^{-1} s^{\Theta^{-1}\tau\alpha} h^\alpha \\ &= (h^\alpha)^{-1} s^\tau h^\alpha \overset{(6.1)}{=} (s^{(h^\alpha)})^\tau. \end{aligned}$$

Since the mapping τ is injective and $s \in S$ was chosen arbitrarily, it follows that $\Theta^{-1}h\Theta = h^\alpha$. Hence $\Theta^{-1}H_1\Theta = H_1^\alpha = H_2$, and H_1 and H_2 are conjugated in $\mathrm{Aut}(S)$. It remains to show that every $M \in \mathcal{B}$ is isomorphic to a group $N \in \mathcal{A}$ and this follows from Theorem 6.12c). •

Finally, Theorem 6.11 is a corollary of Theorem 6.13.

6.3 A theorem of Gaschütz

Using the results of the last sections, we now provide the announced theorem of Gaschütz which permits a classification of the Frattini-free groups. The theory and proofs of this section are mainly from [16].

As isomorphic groups have isomorphic socles, we consider a fixed isomorphism type S of socle and classify all Frattini-free groups with socle isomorphic to S. Thus throughout this section let $S = R \times N$ be a fixed completely reducible group with $R = \mathrm{Rad}(S)$ and $N = \mathrm{N}(S)$.

Since R and N are characteristic in S, one can identify $\mathrm{Inn}(S) = \mathrm{Inn}(N)$ and observe that $\mathrm{Inn}(N) \cong N$. Further, there is an isomorphism

$$\mathrm{Aut}(S) \to \mathrm{Aut}(R) \times \mathrm{Aut}(N), \ \beta \mapsto (\beta|_R, \beta|_N),$$

and every $s \in S$ and $\gamma \in \mathrm{Aut}(S)$ can be written uniquely as

$$s = s_\alpha s_\eta \qquad \text{with } s_\alpha \in R \text{ and } s_\eta \in N, \text{ and}$$

$$\gamma = \gamma_\alpha \gamma_\eta \qquad \text{with } \gamma_\alpha = \gamma|_R \in \mathrm{Aut}(R) \ \text{ and } \ \gamma_\eta = \gamma|_N \in \mathrm{Aut}(N).$$

Consequently, for a subgroup $\Gamma \leq \mathrm{Aut}(S)$ let

$$\Gamma_\alpha = \{\gamma_\alpha \mid \gamma \in \Gamma\} \quad \text{and} \quad \Gamma_\eta = \{\gamma_\eta \mid \gamma \in \Gamma\}.$$

By definition, Γ_α and Γ_η act trivially on N and R, respectively, and elements of Γ_α commutate with elements of Γ_η.

As a preliminary step, some useful lemmas follow.

6.14. Lemma: *If Inn*$(S) \leq \Gamma \leq$ *Aut*(S)*, then the mapping*

$$\Gamma/C_\Gamma(\mathit{Inn}(S)) \to \Gamma_\eta, \quad \gamma C_\Gamma(\mathit{Inn}(S)) \mapsto \gamma_\eta$$

is a group isomorphism.

Proof: It is sufficient to prove that the homomorphism $\varphi : \Gamma \to \Gamma_\eta$, $\gamma \to \ \gamma_\eta$ has kernel $C_\Gamma(\mathrm{Inn}(S))$. For this purpose let $\tau : N \to \mathrm{Inn}(N) = \mathrm{Inn}(S)$ be the conjugation isomorphism and observe that the following equation holds for all $n^\tau \in \mathrm{Inn}(S)$ and $\beta \in \ker\varphi$:

$$\forall x \in S: \ x^{n^\tau \beta} = (n^{-1})^\beta x^\beta n^\beta = n^{-1} x^\beta n = x^{\beta n^\tau}.$$

Hence it follows that $\ker\varphi \leq C_\Gamma(\mathrm{Inn}(S))$. Now let $\beta \in C_\Gamma(\mathrm{Inn}(S))$. If $n \in N$, then

$$\forall x \in S: \ (x^\beta)^{(n^{\beta\tau})} = x^{n^\tau \beta} = x^{\beta n^\tau} = (x^\beta)^{(n^\tau)}.$$

Since $\beta : S \to S$ is an isomorphism, it follows that $n^{\beta\tau} = n^\tau$ and, because τ is injective, one obtains that $n^\beta = n$. Since $n \in N$ was chosen arbitrarily, this shows $\beta \in \ker\varphi$ and thus $C_\Gamma(\mathrm{Inn}(S)) = \ker\varphi$ •

6.15. Lemma: *Let Inn*$(S) \leq \Gamma \leq$ *Aut*(S) *and* $\delta \in$ *Aut*(S)*. If* R *is* Γ*-completely reducible, then* R *is* Γ^δ*-completely reducible.*

Proof: First, one can observe that $\mathrm{Inn}(S) \leq \Gamma^\delta \leq \mathrm{Aut}(S)$ for all $\delta \in \mathrm{Aut}(S)$. If $R = R_1 \cdots R_n$ is a product of minimal Γ-subgroups, then $R = R^\delta = R_1^\delta \cdots R_n^\delta$ is a product of Γ^δ-subgroups. It is easy to show that R_i^δ is a minimal Γ^δ-subgroup for $1 \leq i \leq n$ and hence R is Γ^δ-completely reducible. •

For the remaining part of this section let $\mathrm{Inn}(S) \leq \Gamma \leq \mathrm{Aut}(S)$ such that R is Γ-completely reducible. Further, for this Γ a group F_Γ is defined by

$$F_\Gamma = \Gamma \ltimes R.$$

6.16. Lemma: *The socle Soc*(F_Γ) *of* F_Γ *is isomorphic to* S*.*

Proof: Since $\mathrm{Inn}(S)$ acts trivially on R and $\mathrm{Inn}(S)$ is normal in $\mathrm{Aut}(S)$, the group

$$S^\star = \mathrm{Inn}(S) \times R$$

is a normal subgroup of F_Γ with $S^\star \cong S$, as $\mathrm{Inn}(S) = \mathrm{Inn}(N) \cong N$. Next, we show that $S^\star = \mathrm{Soc}(F_\Gamma)$. The fact that R is abelian and Γ-completely reducible yields that $\{1\} \times R$ is a product of minimal normal subgroups of F_Γ. The same holds for $\mathrm{Inn}(S) \times \{1\}$ since $\mathrm{Inn}(S)_\alpha = \{1\}$ and since $\mathrm{Inn}(S) = \mathrm{Inn}(N) \overset{6.12d)}{=} \mathrm{Soc}(\Gamma_\eta)$ is a product of minimal normal subgroups of Γ_η. Therefore

$$S^\star = (\mathrm{Inn}(S) \times \{1\})(\{1\} \times R)$$

is a product of minimal normal subgroups of F_Γ and hence $S^\star \leq \mathrm{Soc}(F_\Gamma)$.
If $(\gamma, b) \in C_{F_\Gamma}(S^\star)$ and $(\sigma, a) \in S^\star$, then

$$(\gamma, b)(\sigma, a) = (\gamma\sigma, b^\sigma a) = (\sigma\gamma, a^\gamma b) = (\sigma, a)(\gamma, b). \tag{6.2}$$

We note that $b^\sigma = b$ and since R is abelian, Equation (6.2) yields that $\gamma_\alpha = 1$ and $\gamma = \gamma_\eta$. Hence

$$\gamma \in C_{\mathrm{Aut}(N)}(\mathrm{Inn}(N)) \overset{6.12b)}{=} \{1\}$$

and it follows that $C_{F_\Gamma}(S^\star) \leq S^\star$. If $B \trianglelefteq F_\Gamma$ is a minimal normal subgroup of F_Γ with $B \not\leq S^\star$, then $BS^\star = B \times S^\star$ and hence $B \leq C_{F_\Gamma}(S^\star) \leq S^\star$. This is a contradiction and thus $\mathrm{Soc}(F_\Gamma) \leq S^\star$. •

6.17. Lemma: *Let G be a group with socle S. Then G is Frattini-free if and only if G splits over R.*

Proof: "⇒" By Theorem 6.8a), it follows that R is an abelian normal subgroup of G with $R \cap \Phi(G) = \{1\}$, as $\Phi(G) = \{1\}$. Therefore G splits over R by Lemma 5.11.

"⇐" Let $\Phi(G) \neq \{1\}$ and assume, for a contradiction, that there exists a complement H to R in G. Let N be a minimal normal subgroup of G in $\Phi(G)$. Since N is nilpotent, it follows that N is abelian and thus $N \leq R$. By Lemma 6.6c), there exists $M \leq R$ with $R = N \times M$ and thus $G = HR = HNM$. This shows that $|G| = |H||N||M|$ and $MH < G$, and Corollary 5.3 yields that $N \not\leq \Phi(G)$. This contradiction proves the assertion. •

6.18. Lemma: *The group F_Γ has a trivial Frattini subgroup.*

Proof: Lemma 6.16 yields that $\mathrm{Soc}(F_\Gamma) = \mathrm{Inn}(S) \times R \cong N \times R$ and therefore

$$A = \mathrm{Rad}(\mathrm{Soc}(F_\Gamma)) = \{1\} \times R.$$

If one defines $H = \Gamma \times \{1\} \leq F_\Gamma$, then

$$F_\Gamma = HA \quad \text{and} \quad H \cap A = \{1\},$$

and the assertion follows from Lemma 6.17. •

After all this preparations we can state the main theorem of this chapter.

6.19. Theorem (GASCHÜTZ)**:** *Let $S = R \times N$ be a completely reducible group with $R = Rad(S)$ and $N = N(S)$. Let $\mathcal{L}$ be a complete and irredundant list of conjugacy class representatives of subgroups of $Aut(S)$ in $Aut(S)$. If $\mathcal{R}$ is the set of all $\Gamma \in \mathcal{L}$ with*

$$\text{(i) } Inn(S) \leq \Gamma \quad \text{and} \quad \text{(ii) } R \text{ is } \Gamma\text{-completely reducible,}$$

then $\{F_\Gamma \mid \Gamma \in \mathcal{R}\}$ is a complete and irredundant list of isomorphism type representatives of Frattini-free groups with socle isomorphic to S.

Proof: Lemma 6.15 yields that the definition of $\mathcal{R}$ is independent from the choice of $\mathcal{L}$. Further, Lemma 6.16 and Lemma 6.18 show that the groups F_Γ, $\Gamma \in \mathcal{R}$, are Frattini-free and have the socle

$$S^\star = \mathrm{Inn}(S) \times R \cong S$$

with $\mathrm{Rad}(S^\star) = \{1\} \times R$ and $\mathrm{N}(S^\star) = \mathrm{Inn}(S) \times \{1\}$.

The remaining proof is divided into three parts. Let $\Gamma_1, \Gamma_2 \in \mathcal{R}$.

(1) We show: If $F_{\Gamma_1} \cong F_{\Gamma_2}$, then Γ_1 and Γ_2 are conjugated in $\mathrm{Aut}(S)$.

Let $\Lambda : F_{\Gamma_1} \to F_{\Gamma_2}$ be an isomorphism. Hence $\Lambda|_{S^\star}$ is an automorphism and $\mathrm{Rad}(S^\star)^\Lambda = \mathrm{Rad}(S^\star)$. One can observe the following:

- If $a \in R$, then $(1, a)^\Lambda = (1, a^{\lambda_1})$ for some $\lambda_1 \in \mathrm{Aut}(R)$ induced by Λ.
- If $\gamma \in \Gamma_1$, then $(\gamma, 1)^\Lambda = (\gamma^{\widetilde{\Lambda}}, c_{\Lambda,\gamma})$ for some $c_{\Lambda,\gamma} \in R$ and a mapping $\widetilde{\Lambda} : \Gamma_1 \to \Gamma_2$ induced by Λ.

Thus Λ acts on $(\gamma, a) \in F_{\Gamma_1}$ via

$$(\gamma, a)^\Lambda = (\gamma, 1)^\Lambda (1, a)^\Lambda = (\gamma^{\widetilde{\Lambda}}, a^{\lambda_1} c_{\Lambda,\gamma}).$$

Let $\gamma \in \Gamma_1$. For every $a \in R$ it follows that

$$\begin{aligned}(\gamma^{\widetilde{\Lambda}}, a^{\gamma\lambda_1} c_{\Lambda,\gamma}) &= (\gamma, a^\gamma)^\Lambda = ((1, a)(\gamma, 1))^\Lambda \\ &= (1, a)^\Lambda (\gamma, 1)^\Lambda = (1, a^{\lambda_1})(\gamma^{\widetilde{\Lambda}}, c_{\Lambda,\gamma}) \\ &= (\gamma^{\widetilde{\Lambda}}, a^{\lambda_1 \gamma^{\widetilde{\Lambda}}} c_{\Lambda,\gamma})\end{aligned}$$

and therefore

$$(\gamma^{\widetilde{\Lambda}})_\alpha = (\lambda_1^{-1} \gamma \lambda_1)_\alpha = \lambda_1^{-1} \gamma_\alpha \lambda_1. \tag{6.3}$$

The mapping

$$\widetilde{\Lambda} : \Gamma_1 \to \Gamma_2,\ \gamma \mapsto \gamma^{\widetilde{\Lambda}},$$

is an isomorphism: The fact that Λ is an isomorphism yields that $\widetilde{\Lambda}$ is an epimorphism. If $\gamma \in \ker \widetilde{\Lambda}$, then $(\gamma, 1)^{\Lambda} \in \mathrm{Rad}(S^\star)$ and thus $(\gamma, 1) \in \mathrm{Rad}(S^\star)$. It follows that $\gamma = 1$ and $\widetilde{\Lambda}$ is injective.

Let $\varphi : \mathrm{Aut}(S) \to \mathrm{Aut}(N)$, $\gamma \mapsto \gamma_\eta$. By Lemma 6.14, it follows that

$$(\Gamma_i)^\varphi = (\Gamma_i)_\eta \cong \Gamma_i / C_{\Gamma_i}(\mathrm{Inn}(S)),\ \ i \in \{1, 2\},$$

and thus there are isomorphisms

$$\varphi_i : \Gamma_i / C_{\Gamma_i}(\mathrm{Inn}(S)) \to (\Gamma_i)_\eta,\ \gamma C_{\Gamma_i}(\mathrm{Inn}(S)) \mapsto \gamma_\eta,\ \ i \in \{1, 2\}.$$

We recall that $\mathrm{N}(S^\star)^\Lambda = \mathrm{Inn}(S) \times \{1\}$ and thus $\mathrm{Inn}(S)^{\widetilde{\Lambda}} = \mathrm{Inn}(S)$. It follows that

$$(C_{\Gamma_1}(\mathrm{Inn}(S)))^{\widetilde{\Lambda}} = C_{\Gamma_2}(\mathrm{Inn}(S))$$

and $\widetilde{\Lambda}$ induces an isomorphism

$$\Lambda^\star : \begin{cases} \Gamma_1 / C_{\Gamma_1}(\mathrm{Inn}(S)) \to \Gamma_2 / C_{\Gamma_2}(\mathrm{Inn}(S)) \\ \gamma C_{\Gamma_1}(\mathrm{Inn}(S)) \mapsto \gamma^{\widetilde{\Lambda}} C_{\Gamma_2}(\mathrm{Inn}(S)). \end{cases}$$

Defining the projections $\pi_i : \Gamma_i \to \Gamma_i / C_{\Gamma_i}(\mathrm{Inn}(S))$, $i \in \{1, 2\}$, one obtains the following commutative diagram:

$$\begin{tikzcd}
(\Gamma_1)_\eta \arrow[dr, "\varphi_1^{-1}", "\cong"'] & \Gamma_1 \arrow[r, "\widetilde{\Lambda}", "\cong"'] \arrow[d, "\pi_1"] & \Gamma_2 \arrow[d, "\pi_2"'] & (\Gamma_2)_\eta \\
 & \Gamma_1 / C_{\Gamma_1}(\mathrm{Inn}(S)) \arrow[r, "\Lambda^\star", "\cong"'] & \Gamma_2 / C_{\Gamma_2}(\mathrm{Inn}(S)) \arrow[ur, "\varphi_2", "\cong"'] &
\end{tikzcd}$$

This implies an isomorphism

$$\widetilde{\Lambda}^\star : (\Gamma_1)_\eta \to (\Gamma_2)_\eta,\ \gamma_\eta \mapsto (\gamma^{\widetilde{\Lambda}})_\eta.$$

Since $\mathrm{Inn}(N) \leq (\Gamma_1)_\eta, (\Gamma_2)_\eta \leq \mathrm{Aut}(N)$, Theorem 6.11 applies and there is an element $\Theta \in \mathrm{Aut}(N)$ with

$$\forall \gamma_\eta \in (\Gamma_1)_\eta : \ \ \Theta^{-1} \gamma_\eta \Theta = (\gamma_\eta)^{\widetilde{\Lambda}^\star} = (\gamma^{\widetilde{\Lambda}})_\eta. \tag{6.4}$$

Finally, we define $\lambda = \lambda_1 \Theta \in \mathrm{Aut}(S)$ with $\lambda_1 \in \mathrm{Aut}(R)$ and $\Theta \in \mathrm{Aut}(N)$ as in (6.3) and (6.4), respectively. If $\gamma \in \Gamma_1$, then

$$\gamma^\lambda = (\gamma_\alpha)^{\lambda_1} (\gamma_\eta)^\Theta = (\gamma^{\widetilde{\Lambda}})_\alpha (\gamma^{\widetilde{\Lambda}})_\eta = \gamma^{\widetilde{\Lambda}},$$

and thus $(\Gamma_1)^\lambda = (\Gamma_1)^{\widetilde{\Lambda}} = \Gamma_2$.

(2) We show: If $(\Gamma_1)^\lambda = \Gamma_2$ for some $\lambda \in \operatorname{Aut}(S)$, then $F_{\Gamma_1} \cong F_{\Gamma_2}$.

Let

$$\Psi : F_{\Gamma_1} \to F_{\Gamma_2}, \quad (\gamma, a) \mapsto (\gamma^\lambda, a^\lambda) = (\lambda^{-1}\gamma\lambda, a^\lambda).$$

Since $\lambda \in \operatorname{Aut}(S)$ and the conjugation with λ in $\operatorname{Aut}(S)$ is bijective, it follows immediately that Ψ is bijective. Now let $(\gamma, a), (\delta, b) \in F_{\Gamma_1}$. One can observe that

$$\begin{aligned}(\gamma, a)^\Psi(\delta, b)^\Psi &= (\gamma^\lambda\delta^\lambda, a^{\lambda(\lambda^{-1}\delta\lambda)}b^\lambda) = ((\gamma\delta)^\lambda, a^{\delta\lambda}b^\lambda) = (\gamma\delta, a^\delta b)^\Psi \\ &= ((\gamma, a)(\delta, b))^\Psi,\end{aligned}$$

and hence Ψ is an isomorphism.

(3) We show: If F is a finite Frattini-free group with $\operatorname{Soc}(F) \cong S$, then $F \cong F_\Gamma$ for some $\Gamma \in \mathcal{R}$.

W.l.o.g. one can assume that $\operatorname{Soc}(F) = S$ and $\operatorname{Rad}(\operatorname{Soc}(F)) = R$. By Lemma 6.17, there is V to R in F. Let $\sigma : V \to \operatorname{Aut}(S)$ be the conjugation homomorphism and

$$\Gamma = V^\sigma = \{S \to S,\ s \mapsto s^v \mid v \in V\} \leq \operatorname{Aut}(S).$$

An abelian minimal normal subgroup $B \trianglelefteq F$ is contained in R and for every $f = av \in F$ with $a \in R$ and $v \in V$ it follows that $B = B^f = B^{av} = B^v$. Therefore B is a Γ-subgroup and it is easy to show that B is minimal with this property. As R is the product of all abelian minimal normal subgroups of F, the abelian component R of S is Γ-completely reducible.

Let $\tau : N \to \operatorname{Inn}(S)$ be the conjugation homomorphism and let $n = av \in N$ with $a \in R$ and $v \in V$. Since R is abelian, the element v commutates as well as the element n with every element of R. Hence n^τ maps $s = s_\alpha s_\eta \in S$ onto $s_\alpha^n s_\eta^{av} = s_\alpha s_\eta^v$ and it follows that $n^\tau = v^\sigma$. Thus $\operatorname{Inn}(S) \leq \Gamma$ and Γ satisfies the conditions (i) and (ii). In particular, one can assume that $\Gamma \in \mathcal{R}$.

Next, we consider an element $v \in \ker\sigma = C_V(S) = C_F(S) \cap V$ and the normal closure $[v] = \{v\}^F$ of $\{v\}$ in F; that is,

$$[v] = \langle v^g \mid g \in F\rangle \trianglelefteq F.$$

Let $g \in F$ and $s \in S$. Since $v \in C_F(S)$ and $S \trianglelefteq F$, it follows that

$$v^g s = (v\widetilde{s})^g = (\widetilde{s}v)^g = sv^g$$

with $\widetilde{s} = gsg^{-1} \in S$. Hence $v^g \in C_F(S)$ and thus $[v] \leq C_F(S)$. For all $f = wa \in F$ with $w \in V$ and $a \in R \leq S$ it follows that

$$([v] \cap V)^f = ([v] \cap V)^{wa} = ([v] \cap V)^a = [v] \cap V$$

and therefore $v \in [v] \cap V \trianglelefteq F$. Since $[v]$ is the smallest normal subgroup containing v, one obtains that $[v] \leq V$.

If $[v] \neq \{1\}$, then there is a minimal normal subgroup B of F in $[v]$. Since R contains all abelian minimal normal subgroups of F and $V \cap R = \{1\}$, the group B has to be non-abelian. This is a contradiction to $B \leq S$ and $B \leq [v] \leq C_F(S)$. Hence $[v] = \{1\}$ which shows that $\sigma : V \to \Gamma$ is an isomorphism.

Since F splits over R, one can identify $F = V \ltimes R$. Next, we define

$$\vartheta : F \to F_\Gamma,\ (v, a) \mapsto (v^\sigma, a).$$

If $(v, a), (u, b) \in F$, then

$$\begin{aligned}(v,a)^\vartheta (u,b)^\vartheta &= (v^\sigma, a)(u^\sigma, b) = (v^\sigma u^\sigma, a^{(u^\sigma)} b) = ((vu)^\sigma, a^u b) \\ &= (vu, a^u b)^\vartheta = ((v,a)(u,b))^\vartheta.\end{aligned}$$

Obviously, ϑ is bijective and hence $F \cong F_\Gamma$.

Finally, (1), (2), and (3) complete the proof. •

Theorem 6.19 yields a method to construct all cube-free Frattini-free groups with a socle isomorphic to a completely reducible S. This intention will be concretized in the following section.

6.20. Example: We determine the isomorphism types of Frattini-free groups having a socle isomorphic to $V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle \leq S_4$. First, one can observe that S_4, A_4, and V_4 are Frattini-free groups with

$$\mathrm{Soc}(S_4) = \mathrm{Soc}(A_4) = \mathrm{Soc}(V_4) = V_4.$$

If one identifies $\mathrm{Aut}(V_4) = S_3$, then

$$K_1 = \{()\},\ K_2 = \langle (1,2) \rangle,\ K_3 = \langle (1,2,3) \rangle, \text{ and } K_4 = S_3$$

is a complete and irredundant list of conjugacy class representatives of subgroups of $\mathrm{Aut}(V_4)$. Further, one can observe that $\{1\} = \mathrm{Inn}(V_4) \leq K_i$ for $1 \leq i \leq 4$. Now the only possibilities to write V_4 as a product of different subgroups are

$$\begin{aligned}V_4 &= \langle (1,2)(3,4) \rangle \langle (1,3)(2,4) \rangle = \langle (1,2)(3,4) \rangle \langle (1,4)(2,3) \rangle \\ &= \langle (1,3)(2,4) \rangle \langle (1,4)(2,3) \rangle\end{aligned}$$

In particular, the group V_4 is K_1-, K_3-, and K_4-completely reducible, but not K_2-completely reducible. Hence Theorem 6.19 yields that

$$\begin{aligned}&F_{K_4} = K_4 \ltimes V_4 \cong S_4, \\ &F_{K_3} = K_3 \ltimes V_4 \cong A_4, \qquad \text{and} \\ &F_{K_1} = K_1 \ltimes V_4 \cong V_4\end{aligned}$$

are all isomorphism types of Frattini-free groups having a socle isomorphic to V_4.

6.4 Frattini-free groups of cube-free order

Based on Theorem 6.19, we investigate the structure of the cube-free Frattini-free groups. We recall that the socle S of a cube-free group has the form $S = A \times B \times C$ with A, B, and C as in Theorem 6.8, and we use this notation throughout this section. In particular, $\mathrm{Rad}(S) = B \times C$ and $\mathrm{N}(S) = A$.

First, it is necessary to examine the automorphism group of S.

6.21. Lemma: *If $S = A \times B \times C$ is a completely reducible group of cube-free order, then the following holds:*

a) $Aut(S) = Aut(A) \times Aut(B) \times Aut(C)$,

b) $Inn(S) \cong Inn(A) \cong A$ and $[Aut(A) : Inn(A)] \mid 2$,

c) $Aut(B) = \prod_i Aut(C_{p_i}) \cong C_{p_1-1} \times \ldots \times C_{p_n-1}$,

d) $Aut(C) = \prod_i Aut(C_{q_i}^2) \cong GL(2, q_1) \times \ldots \times GL(2, q_m)$.

Proof: The groups S, B, and C decompose into direct products of characteristic subgroups and thus also $\mathrm{Aut}(S)$, $\mathrm{Aut}(B)$, and $\mathrm{Aut}(C)$ decompose accordingly. This shows a) and the first parts of c) and d).

For $i \in \{1, 2\}$ we consider $C_p^i \cong \mathbb{F}_p^i$ as an $\mathbb{F}_p$-vector space and observe that $\mathrm{Aut}(\mathbb{F}_p^i)$ can be identified with $\mathrm{GL}(i, p)$. Obviously, $\mathrm{GL}(1, p) \cong C_{p-1}$, and thus c) and d) are proved.

The isomorphisms in b) are already shown in the previous sections. The group A is either trivial or $A = \mathrm{PSL}(2, r)$ for some prime r. If $A = \mathrm{PSL}(2, r)$, then [9], Section 3.3, yields that $|\mathrm{Aut}(A)/\mathrm{Inn}(A)| = 2$. •

6.22. Theorem: *Let $S = A \times B \times C$ be a completely reducible group of cube-free order.*

a) The group F is a Frattini-free group of cube-free order with socle S if and only if $F \cong A \times (K \ltimes (B \times C))$ with $K \leq Aut(B \times C)$ such that $|K||S|$ is cube-free.

b) Two Frattini-free groups $F_i = A \times (K_i \ltimes (B \times C))$, $i \in \{1, 2\}$, are isomorphic if and only if K_1 is conjugated to K_2 in $Aut(B \times C)$.

Proof: a) "⇒" By Theorem 6.19, it follows that $F \cong L \ltimes (B \times C)$ for some $\mathrm{Inn}(S) \leq L \leq \mathrm{Aut}(S)$. Thus the case $A = \{1\}$ follows directly and it remains to consider the case $A \neq \{1\}$. By Lemma 6.21b), one can identify $A = \mathrm{Inn}(A) = \mathrm{Inn}(S)$. Thus $4 \mid |\mathrm{Inn}(A)|$ and it follows that $2 \nmid [L : \mathrm{Inn}(A)]$ as L has cube-free order. Now $[\mathrm{Aut}(A) : \mathrm{Inn}(A)] = 2$ implies that

$$\mathrm{Inn}(A) \; \leq \; L \; \leq \; \mathrm{Inn}(A) \times \mathrm{Aut}(B) \times \mathrm{Aut}(C).$$

Let $\lambda : L \to \mathrm{Aut}(\mathrm{Inn}(A))$ be the conjugation homomorphism and note that $L^\lambda = \mathrm{Inn}(\mathrm{Inn}(A))$. Denote with $\delta : L \to L/\mathrm{Inn}(A)$ the natural epimorphism and let

$$\mu : L \to \mathrm{Inn}(\mathrm{Inn}(A)) \times L/\mathrm{Inn}(A),\ l \mapsto (l^\lambda, l^\delta),$$

be the combination of these two mappings. We show that μ is bijective. Let $(a^\lambda, b^\delta) \in \mathrm{Inn}(\mathrm{Inn}(A)) \times L/\mathrm{Inn}(A)$ with $a, b \in L$. Then there are $x, y \in \mathrm{Inn}(A)$ with $x^\lambda = a^\lambda$ and $y^\lambda = (b^\lambda)^{-1}$. It follows that $(byx)^\mu = (a^\lambda, b^\delta)$ and μ is surjective. If $l \in \ker \mu$, then $l \in \mathrm{Inn}(A)$. Since $\mathrm{Inn}(A)$ is non-abelian simple, the conjugation homomorphism $\mathrm{Inn}(A) \to \mathrm{Inn}(\mathrm{Inn}(A))$ is injective and thus $l = 1$. Hence μ is an isomorphism and it follows that

$$L \cong \mathrm{Inn}(\mathrm{Inn}(A)) \times K \cong \mathrm{Inn}(A) \times K$$

for some $K \leq \mathrm{Aut}(B) \times \mathrm{Aut}(C)$. Therefore

$$F \cong L \ltimes (B \times C) \cong (\mathrm{Inn}(A) \times K) \ltimes (B \times C) \cong A \times (K \ltimes (B \times C)).$$

"$\Leftarrow$" Let $F \cong A \times (K \ltimes (B \times C))$ with $K \leq \mathrm{Aut}(B \times C)$ and $|K||S|$ cube-free. Then $F \cong L \ltimes (B \times C)$ with $L = A \times K$ and, by Lemma 6.21b), one can identify $L = \mathrm{Inn}(S) \times K$. Thus L is a cube-free group with $\mathrm{Inn}(S) \leq L \leq \mathrm{Aut}(S)$. The image of the projection $K \to \mathrm{GL}(2, q_i) \leq \mathrm{Aut}(B \times C)$ is a cube-free subgroup $K_i \leq \mathrm{GL}(2, q_i)$ with $q_i \nmid |K_i|$ for $1 \leq i \leq m$. Hence Theorem 3.11a) applies and it is easy to show that C is K-completely reducible. Further, B is K-completely reducible by the definition of B. Since $\mathrm{Inn}(S)$ acts trivial on $B \times C$, it follows that $B \times C$ is L-completely reducible. Now a) is proved by Theorem 6.19.

b) As shown in part a), one can identify $F_i = (\mathrm{Inn}(S) \times K_i) \ltimes (B \times C)$ for $i \in \{1, 2\}$. Since $\mathrm{Inn}(S) \times K_1$ and $\mathrm{Inn}(S) \times K_2$ are conjugated in $\mathrm{Aut}(S)$ if and only if K_1 and K_2 are conjugated in $\mathrm{Aut}(B \times C)$, the assertion follows directly from Theorem 6.19. •

Thus every cube-free Frattini-free group F with socle $S = A \times B \times C$ has the form $F = A \times (K \ltimes (B \times C))$ with a cube-free $K \leq \mathrm{Aut}(B \times C)$. By Lemma 6.21, the group K can be identified with a cube-free subgroup of

$$C_{p_1 - 1} \times \ldots \times C_{p_n - 1} \times \mathrm{GL}(2, q_1) \times \ldots \times \mathrm{GL}(2, q_m).$$

Every projection of K into a direct factor is solvable by Theorem 3.12. Since K is a subgroup of the direct product of these projections, K and hence also $K \ltimes (B \times C)$ are solvable. In particular, it follows a corollary concerning the structure of cube-free Frattini-free groups.

6.23. Corollary: *A Frattini-free group F of cube-free order decomposes into a direct product $F = A \times L$ where A is either trivial or a non-abelian simple group and L is solvable. If A is non-trivial, then $4 \mid |A|$ and $|L|$ is odd.*

This yields a method to construct the Frattini-free groups of a given cube-free order n up to isomorphism. First, all possible completely reducible groups $S = A \times B \times C$ of order dividing n are determined using Theorem 6.8. Then all subgroups K of $\mathrm{Aut}(B \times C)$ with $|S||K| = n$ are computed up to conjugacy in $\mathrm{Aut}(B \times C)$. By Lemma 6.21, such a group K is a subgroup of a direct product of groups of the type C_{p-1} and $\mathrm{GL}(2, q)$. As it will be shown in the following section, the possible groups K can be determined up to conjugacy from their projections into the direct factors using a so-called subdirect product construction. The possible projections into a group of the type C_{p-1} can be determined readily and the possible projections into a group of the type $\mathrm{GL}(2, q)$ are considered in Lemma 3.12. Once all possible groups K are determined, it is straightforward to construct all products $A \times (K \ltimes (B \times C))$.

6.5 Subdirect products

We investigate the question how one can compute all subgroups of a direct product having given projections into the direct factors. Such subgroups are called subdirect products of these projections and this section outlines their construction. The theory of this section is based on [12], Section 2.2.1.

First of all, we specify the definition of a subdirect product. All direct products are to be regarded as internal direct products.

6.24. Definition: Let $D = D_1 \times \ldots \times D_n$ be a direct product of groups $D_1, \ldots, D_n$ and let $\pi_i : D \to D_i$ for $i \in \{1, \ldots, n\}$ be the corresponding projections. A *subdirect product* of $D_1, \ldots, D_n$ is a subgroup $U \leq D$ such that $U^{\pi_i} = D_i$ for $1 \leq i \leq n$.

In particular, it is sufficient to consider the case $n = 2$. For this purpose we analyze the situation and assume that $U \leq D_1 \times D_2$ is a subdirect product of D_1 and D_2. Then $\ker \pi_1 = U \cap D_2$ and $\ker \pi_2 = U \cap D_1$ are normal in U and hence also in D_2 and D_1, respectively. If $M = (U \cap D_1)(U \cap D_2)$, then $M^{\pi_i} \leq M$ for $i \in \{1, 2\}$. Since $U/M \to D_iM/M$, $uM \mapsto u^{\pi_i}M$, is bijective for $i \in \{1, 2\}$, it follows that

$$D_1/U \cap D_1 \;\cong\; D_1M/M \;\cong\; U/M \;\cong\; D_2M/M \;\cong\; D_2/U \cap D_2$$

and

$$U/M \cap D_1M/M \;\cong\; \{1\} \;\cong\; U/M \cap D_2M/M.$$

Therefore the following lemma reduces the investigations to subdirect products U of D_1 and D_2 with trivial intersections; this means that $D_1 \cap U$ and $D_2 \cap U$ are trivial.

6.25. Lemma: *Let $U \leq D_1 \times D_2$ and $M = (U \cap D_1)(U \cap D_2)$. Then U is a subdirect product of D_1 and D_2 if and only if U/M is a subdirect product of D_1M/M and D_2M/M.*

Proof: Since $U \cap D_1$ and $U \cap D_2$ are the kernels of the projections $U \to D_2$ and $U \to D_1$, respectively, the assertion follows immediately. •

Consequently, the first step to determine all subdirect products of D_1 and D_2 is the computation of all candidates for the intersections $U \cap D_1$ and $U \cap D_2$; that is, one has to determine all pairs (N_1, N_2) with $N_i \trianglelefteq D_i$, $i \in \{1,2\}$, and $D_1/N_1 \cong D_2/N_2$. Then one computes all subdirect products V of D_1/N_1 and D_2/N_2 with trivial intersections $V \cap D_i/N_i$, $i \in \{1,2\}$. The final step is to lift V to its preimage concerning the projection

$$D_1 \times D_2 \ \to \ D_1/N_1 \times D_2/N_2 = (D_1 \times D_2)/(N_1 \times N_2).$$

Thus it remains to examine the subdirect products with trivial intersections.

6.26. Lemma: *If $\psi : D_1 \to D_2$ is an isomorphism, then*

$$U_\psi = \{(g,h) \mid g \in D_1,\ h \in D_2,\ g^\psi = h\} \leq D_1 \times D_2$$

is a subdirect product of D_1 and D_2 with trivial intersections $U_\psi \cap D_1$ and $U_\psi \cap D_2$.

Proof: The assertion follows from the construction. A more generalized version of this lemma can be found in [20], Theorem (I, 9.11). •

If U is a subdirect product of D_1 and D_2 with trivial intersections, then the projections $\pi_i : U \to D_i$, $i \in \{1,2\}$, are isomorphisms. Therefore $\psi = \pi_1^{-1}\pi_2 : D_1 \to D_2$ is an isomorphism and $U = U_\psi$ as in Lemma 6.26. Since different isomorphisms yield different subdirect products, there is a bijection between all isomorphisms $D_1 \to D_2$ and all subdirect products U of D_1 and D_2 with trivial intersections $D_1 \cap U$ and $D_2 \cap U$. This completes the described algorithm to compute all subdirect products of D_1 and D_2.

In the context of this thesis it is necessary to reduce these subdirect products of D_1 and D_2 to conjugacy class representatives in a group $G = G_1 \times G_2$ with $D_1 \times D_2 \leq G$. This requires some extra propositions and we refer to [12], Section 2.2.1, for more details and some comments concerning an implementation. As the algorithm to construct all subdirect products indicates, the main runtime of this function is spent to the computation of group isomorphisms.

6.27. Example: We construct all subdirect products of $G = \langle g \mid g^8 = 1\rangle$ and $H = \langle h \mid h^4 = 1\rangle$. First, all pairs (N, M) of normal subgroups $N \trianglelefteq G$ and $M \trianglelefteq H$ with $G/N \cong H/M$ are determined:

(i) $(\langle g\rangle, \langle h\rangle)$,
(ii) $(\langle g^2\rangle, \langle h^2\rangle)$, and
(ii) $(\langle g^4\rangle, \langle 1\rangle)$.

If $(N, M) = (\langle g\rangle, \langle h\rangle)$, then $\widetilde{G} = G/N \cong \{1\} \cong H/M = \widetilde{H}$ and the identity mapping is the only isomorphism from $\widetilde{G}$ to $\widetilde{H}$. Hence $U_{\mathrm{id}} = \{(1N, 1M)\}$ and this induces the direct product:

$$U_1 = G \times H.$$

If $(N, M) = (\langle g^2\rangle, \langle h^2\rangle)$, then $\widetilde{G} = G/N \cong C_2 \cong H/M = \widetilde{H}$ and, again, the identity mapping is the only isomorphism from $\widetilde{G}$ to $\widetilde{H}$. Now $U_{\mathrm{id}} = \langle (gN, hM)\rangle$ induces the subdirect product of order 16:

$$U_2 = \langle (g^7, h^3), (g^2, 1)\rangle.$$

If $(N, M) = (\langle g^4\rangle, \langle 1\rangle)$, then $\widetilde{G} = G/N \cong C_4 \cong H/M = H$. There are two isomorphisms from $\langle gN\rangle$ to H, that is to say

$$\begin{aligned} \psi_1 &: gN \mapsto h \quad \text{and} \\ \psi_2 &: gN \mapsto h^3. \end{aligned}$$

Thus $U_{\psi_1} = \langle (gN, h)\rangle$ and $U_{\psi_2} = \langle (gN, h^3)\rangle$ and the subdirect products of order 8 follow:

$$\begin{aligned} U_3 &= \langle (g, h)\rangle, \quad \text{and} \\ U_4 &= \langle (g, h^3)\rangle. \end{aligned}$$

Finally, $U_1, \ldots, U_4$ are the only subdirect products of G and H, and since $G \times H$ is abelian, no two of these subdirect products are conjugated in $G \times H$.

Chapter 7

Cube-free Frattini extensions

We discusses the second step in the algorithm to construct all groups of a given cube-free order up to isomorphism: Assuming that a Frattini-free group F of cube-free order is given, we want to determine all Frattini extensions G of F with cube-free order up to isomorphism.

At first we define and investigate Frattini extensions. Then we introduce the main results of this thesis.

7.1 Frattini extensions

First, we specify the definition of a Frattini extension.

7.1. Definition: Let G, H, and M be finite groups.

a) The group G is a *Frattini extension* of H by M, if G is an extension of H by M and $G/\Phi(G) \cong H/\Phi(H)$.

b) The group G is a *minimal Frattini extension* of H by M, if G is a Frattini extension of H by M and there exists a minimal normal subgroup $N \trianglelefteq G$ with $N \cong M$ and $G/N \cong H$.

7.2. Lemma: *If G is a Frattini extension of a Frattini-free group F by a normal subgroup $M \trianglelefteq G$, then $\Phi(G) = M$.*

Proof: It follows from Lemma 5.4a) that

$$\Phi(G)M/M \leq \Phi(G/M) \cong \Phi(F) = \{1\}$$

and thus $\Phi(G) \leq M$. Since $G/\Phi(G) \cong G/M$, one obtains that $M = \Phi(G)$. •

Now we consider the minimal Frattini extensions.

7.3. Lemma: *Let G be an extension of H by an H-module M; that is, we assume that $M \trianglelefteq G$ and $G/M = H$. Then G is a minimal Frattini extension of H by M, if and only if M is a minimal non-complemented normal subgroup of G.*

Proof: "⇒" Suppose M is a complemented. Then Corollary 5.12 yields that $M \cap \Phi(G) = \{1\}$, and it follows from $\Phi(G)M/M \leq \Phi(G/M)$ that

$$\frac{|H|}{|\Phi(H)|} = \frac{|G/M|}{|\Phi(G/M)|} \leq \frac{|G|}{|\Phi(G)M|} < \frac{|G|}{|\Phi(G)|}.$$

Thus $H/\Phi(H) \ncong G/\Phi(G)$ and G is not a Frattini extension of H by M. This is a contradiction and hence M has to be non-complemented.

"⇐" It follows from Corollary 5.12 that $M \leq \Phi(G)$ and this shows that $\Phi(H) = \Phi(G/M) = \Phi(G)/M$. Hence $H/\Phi(H) \cong (G/M)/\Phi(G/M) \cong G/\Phi(G)$ and G is a minimal Frattini extension of H by M. •

As a consequence, one obtains the following corollary.

7.4. Corollary: *The minimal Frattini extensions of a group H are exactly the non-split extensions of H by an irreducible H-module M.*

In particular, it follows from Theorem 4.9 that there is no minimal Frattini extension of H by M if $H^2(H, M) = \{0\}$.

7.2 Reduction to minimal Frattini Extensions

Now we examine the cube-free Frattini extensions. By Corollary 5.16, the Frattini subgroup of a cube-free group G has the form

$$\Phi(G) \cong C_{p_1} \times \ldots \times C_{p_s}$$

for distinct primes $p_1, \ldots, p_s$. Let p be a prime. If $M \cong C_p$ is an F-module, then, by Corollary 7.4, every non-split extension of F by M is a Frattini extension of F. Conversely, Corollary 5.16 indicates that these extensions are essentially all possible extensions which can occur.

Hence as a first step, we show that it is sufficient to consider minimal Frattini extensions. For this purpose we introduce the following notation. If $G_1, \ldots, G_s$ are extensions of F by $N_1, \ldots, N_s$, respectively, then the subdirect product

$$G_1 \curlywedge \ldots \curlywedge G_s \leq G_1 \times \ldots \times G_s$$

is defined by

$$G_1 \curlywedge \ldots \curlywedge G_s = \{(g_1, \ldots, g_s) \mid g_1 N_1 = \ldots = g_s N_s\}$$

where we identify $G_i/N_i = F$.

Further, for a group $M \cong C_{p_1} \times \ldots \times C_{p_s}$ we define $M_i \leq M$ by $M_i \cong C_{p_i}$ and $M(i) \leq M$ by

$$M(i) \cong C_{p_1} \times \ldots \times C_{p_{i-1}} \times C_{p_{i+1}} \times \ldots \times C_{p_s}.$$

Thus one can identify $M = M_1 \times \ldots \times M_s = M(i) \times M_i$ for $1 \leq i \leq s$.

7.5. Theorem: *Let F be a cube-free Frattini-free group and let M be an F-module of isomorphism type $C_{p_1} \times \ldots \times C_{p_s}$.*

a) If G is a Frattini extension of F by M, then $G/M(i)$ is a minimal Frattini extension of F by M_i for $1 \leq i \leq s$.

b) If $G_1, \ldots, G_s$ are minimal Frattini extensions of F by $M_1, \ldots, M_s$, respectively, then the group $G_1 \curlywedge \ldots \curlywedge G_s$ is a Frattini extension of F by M.

c) If G is a Frattini extension of F by M, then $G/M(1) \curlywedge \ldots \curlywedge G/M(s) \cong G$.

Proof: a) Obviously, $G/M(i)$ is an extension of F by M_i. By Lemma 7.2, one can identify $\Phi(G) = M$. Then $\Phi(G/M(i)) = \Phi(G)/M(i) = M/M(i)$ and thus $(G/M(i))/\Phi(G/M(i)) \cong G/M = G/\Phi(G) \cong F$.

b) Let $D = G_1 \curlywedge \ldots \curlywedge G_s$. Since $F \cong G_1/M_1$ and because the mapping $\mu : D \to G_1/M_1$, $(g_1, \ldots, g_s) \mapsto g_1M_1$, is an epimorphism with kernel M, it follows that that $D/M \cong F$. Next, we show that $M = \Phi(D)$. The group

$$J_i = \{1\} \times \ldots \times \{1\} \times M_i \times \{1\} \times \ldots \times \{1\}$$

is a minimal normal subgroup of D and

$$\overline{J_i} = M_1 \times \ldots \times M_{i-1} \times \{1\} \times M_{i+1} \times \ldots \times M_s$$

is a complement to J_i in M. Since $\gcd(|M/J_i|, |J_i|) = 1$, the Schur-Zassenhaus Theorem shows that this complement is unique; see [25], Theorem 9.1.2. Suppose, for a contradiction, that there exists a complement R to J_i in D. Then $\psi_i : R \to D/J_i$, $r \mapsto rJ_i$, is an isomorphism. If K_i is the preimage of M/J_i under ψ_i, then $K_i \cap J_i \leq R \cap J_i = \{1\}$ and $K_iJ_i = M$. Hence K_i complements J_i in M and thus $K_i = \overline{J_i}$. Let $\nu_i : D \to D/K_i$ be the natural epimorphism. Then R^{ν_i} complements $J_i^{\nu_i}$ in D/K_i as R is a complement to J_i in D and $K_i \leq R$. By Corollary 5.12, this contradicts $\Phi(D/K_i) = \Phi(D/\overline{J_i}) = J_i^{\nu_i}$, and it follows that J_i has no complement R in D. Now Corollary 5.12 shows that $J_i \leq \Phi(D)$ and thus $M = J_1 \cdots J_s \leq \Phi(D)$. Using the projection $\mu_i : D \to G_i$, Lemma 5.5 yields that $\Phi(D)^{\mu_i} \leq \Phi(D^{\mu_i}) = \Phi(G_i) = M_i$ and therefore $\Phi(D) \leq M$. In summary, it follows that $\Phi(D) = M$.

c) By a), the group $G_i = G/M(i)$ is a minimal Frattini extension of F by M_i. Let

$$\psi : G \to G_1 \times \ldots \times G_s,\ g \mapsto (gM(1), \ldots, gM(s)).$$

If $g^\psi = 1$, then $g \in \bigcap_{i=1}^s M(i) = \{1\}$ and hence ψ is a monomorphism. Since $M(i)M_i = M$, one obtains that $G^\psi \leq G_1 \curlywedge \ldots \curlywedge G_s$. This proves the assertion because $|G| = |F||M| = |G_1 \curlywedge \ldots \curlywedge G_s|$. •

One can observe that Theorem 7.5 reduces the construction of cube-free Frattini extensions of F by a module of the isomorphism type $C_{p_1} \times \ldots \times C_{p_s}$ to the construction of minimal Frattini extensions of F by a module of the isomorphism type C_{p_i}.

It follows a comment on the minimal Frattini-extensions in the cube-free case.

7.6. *Remark:* We have given a cube-free Frattini-free group F and an F-module M of the isomorphism type C_p. The aim is to construct a cube-free Frattini extension of F by M. For this purpose one has to assume that there is a Sylow p-subgroup $P \in \mathrm{Syl}_p(F)$ with $P \cong C_p$; see Lemma 5.15. Let P be generated by $g \in P$. Let $\{h_1, \ldots, h_k\}$ be a left transversal to P in F and for $f \in F$ define $\widetilde{f} \in \{h_1, \ldots, h_k\}$ by $fP = \widetilde{f}P$. We recall that $\mathrm{res}^2(P, F)$ maps $H^2(F, M)$ monomorphically to the subgroup of stable elements of $H^2(P, M)$. To guarantee the existence of a Frattini extension of F by M, one has to assume that $H^2(F, M) \neq \{0\}$. In this case every element of $H^2(P, M)$ has to be stable and thus $H^2(F, A) \cong C_p$. Let $0 \neq t \in M$. As shown in Lemma 4.10b), the cocycle

$$\gamma_t : P \times P \to M,\ (g^i, g^j) \mapsto \begin{cases} 0 & : \overline{i} + \overline{j} < p \\ t & : \overline{i} + \overline{j} \geq p \end{cases}$$

yields a generator $\gamma_t + B^2(P, M)$ of $H^2(P, M) \cong C_p$. If follows from Lemma 4.20 that

$$\widehat{\gamma}_t + B^2(F, M) = k^{-1}\mathrm{cor}^2(F, P)(\gamma_t + B^2(P, M))$$

is a generator of $H^2(F, M)$. By Theorem 4.16b), we have an explicit formula for $\mathrm{cor}^2(F, P)$ in terms of the normalized standard free resolution and hence

$$\widehat{\gamma}_t : F \times F \to M,\ (u, v) \mapsto k^{-1} \sum_{i=1}^{k} \gamma_t(\widetilde{uh_i}^{-1} uh_i, \widetilde{vuh_i}^{-1} v\widetilde{uh_i})^{h_i^{-1}}.$$

Obviously, the cocycle $\widehat{\gamma}_t \in Z^2(F, M)$ induces a minimal Frattini extension of F by M.

7.3 A direct product decomposition

This section provides the first main result of this thesis: We show that every cube-free group is either solvable or it is a direct product of a non-abelian simple group with a solvable group.

For this purpose we reduce to the construction of solvable minimal Frattini extensions of cube-free order. We recall that, by Corollary 6.23, a cube-free Frattini-free group F has the form $F = A \times L$, where A is non-abelian simple or trivial and L is solvable. The following theorem addresses the case that A is non-abelian simple.

7.7. Theorem: *Let $F = A \times L$ be a Frattini-free group of cube-free order such that A is non-abelian simple and L is solvable. Let G be a cube-free Frattini extension of F by an F-module $M \cong C_p$. Then $G = A \times H$ and H is a solvable Frattini extension of L by M.*

Proof: Theorem 2.7 yields that $A \cong \mathrm{PSL}(2,q)$ for some prime $q > 3$. Since $4 \mid |A|$ and $G/M \cong A \times L$, it follows that $p \neq 2$. Now Corollary 4.26 shows that $H^2(A,M) = \{0\}$. Let $\psi : G \to G/M \cong F$ be the natural epimorphism and let $A^\star \trianglelefteq G$ and $H \trianglelefteq G$ be preimages of A and L under ψ, respectively. Due to the fact that $H^2(A,M)$ is trivial, the group $A^\star$ is a split extension of A by M, and, because M is trivial as an A-module by Lemma 3.2, one can identify $A^\star = M \times A$. Since $(A^\star)' = A$ is a characteristic subgroup of $A^\star$, it follows that $A \trianglelefteq G$ and $H \cap A = \{1\}$. Thus $G = A \times H$ and, as $\Phi(A) = \{1\}$,

$$M = \Phi(G) = \Phi(A) \times \Phi(H) = \Phi(H).$$

Hence it follows that $H/\Phi(H) \cong L$. Therefore H is a solvable Frattini extension of L by M. Figure 1 summarizes the situation. •

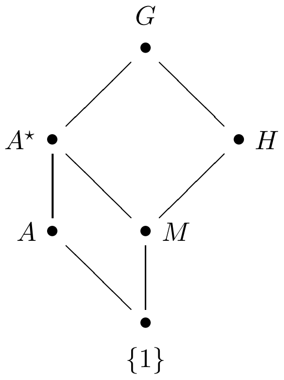

Figure 1.

The main result of this section is implied by Theorems 7.5 and 7.7:

7.8. Theorem: *A group G of cube-free order decomposes into a direct product $G = A \times L$ where A is either trivial or a non-abelian simple group and L is solvable. If A is non-trivial, then $4 \mid |A|$ and $|L|$ is odd.*

7.4 Uniqueness of Frattini extensions

By Theorem 7.7, it is sufficient to consider cube-free Frattini extensions of a solvable group L by an L-module M of the isomorphism type C_p. The following theorem shows that the existence and uniqueness of such Frattini extensions depend on the module structure of M.

If M and P are N-modules with a group isomorphism $\psi : M \to P$ and $(m^n)^\psi = (m^\psi)^n$ for all $m \in M$ and $n \in N$, then M and P are isomorphic as N-modules. This is denoted by $M \cong_N P$.

7.9. Theorem: *Let G be a group and let $P \in Syl_p(G)$. Suppose that $P \cong C_p$ and let $N = N_G(P)$ the Sylow normalizer. Let $M \cong C_p$ be a G-module.*

a) If $M \cong_N P$, then up to isomorphism there exists exactly one Frattini extension of G by M.

b) If $M \ncong_N P$, then there exists no Frattini extension of G by M.

Proof: Lemma 4.10c) yields that $H^2(G, M) \cong C_p$. Let $P = \langle g \rangle$ and $M = \langle m \rangle$. It follows from Lemma 4.10a) that

$$\alpha : Z^2(P, M) \to M,\ \gamma \mapsto \sum_{i=1}^{p-1} \gamma(g, g^i)$$

is an epimorphism with kernel $B^2(P, M)$. As in Lemma 4.10b), for an arbitrary $t \in M$ let

$$\gamma_t : P \times P \to M,\ (g^i, g^j) \mapsto \begin{cases} 0 & : \overline{i} + \overline{j} < p \\ t & : \overline{i} + \overline{j} \geq p \end{cases}$$

where $\overline{z} = z \bmod p$ for $z \in \mathbb{Z}$. Then $\gamma_t \in Z^2(P, M)$ and $\gamma_t^\alpha = t$. Since $\gamma_{t_1} \equiv \gamma_{t_2} \bmod B^2(P, M)$ implies $t_1 = t_2$, the set $\{\gamma_s \mid s \in M\}$ is a transversal to $B^2(P, M)$ in $Z^2(P, M)$; that is, every element $\gamma \in Z^2(P, M)$ can be written uniquely as $\gamma = \gamma_t + \delta$ for some $t \in M$ and $\delta \in B^2(P, M)$.
The group N acts on P with kernel $C = C_G(P) = C_N(P)$ and therefore one obtains that $N/C \hookrightarrow \mathrm{Aut}(P) \cong C_{p-1}$ and thus $N = \langle x, C \rangle$ for some $x \in N \backslash C$. Let the operation of x on P and M, respectively, be denoted by

$$\begin{array}{llll} x^{-1} & : & P \to P, & g \mapsto g^a, \\ x & : & P \to P, & g \mapsto g^b, \qquad \text{and} \\ x & : & M \to M, & m \mapsto cm \end{array}$$

with $a, b, c \in \{1, \ldots, p-1\}$ and $ab \equiv 1 \bmod p$.
As mentioned in Theorem 4.16a), an element $l \in N$ acts on $Z^2(P, M)$ via

$$\gamma \mapsto \gamma^l = \left[(s, t) \mapsto \gamma(s^{l^{-1}}, t^{l^{-1}})^l \right]$$

and there is an induced action of N on $H^2(P, M)$. The subgroup of all fixed points is denoted by

$$\mathrm{Fix}_N(H^2(P, M)) = \{\gamma \in H^2(P, M) \mid \forall l \in N :\ \gamma^l = \gamma\}.$$

Let $0 \neq t \in M$. Then $\gamma_t^x \equiv \gamma_t \bmod B^2(P, M)$ if and only if $(\gamma_t^x)^\alpha = \gamma_t^\alpha = t$. For $k \in \{1, \ldots, p-1\}$ one obtains that

$$\gamma_t^x(g, g^k) = \gamma_t(g^{x^{-1}}, (g^k)^{x^{-1}})^x = \gamma_t(g^a, g^{\overline{ak}})^x = \begin{cases} 0 & : a + \overline{ak} < p \\ ct & : a + \overline{ak} \geq p \end{cases},$$

and it follows that

$$(\gamma_t^x)^\alpha = \sum_{i=1}^{p-1} \gamma_t^x(g, g^i) = \lambda ct,$$

where $\lambda = |\{k \in \{1, \ldots, p-1\} \mid \overline{ak} \geq p - a\}|$.
Using $l = \overline{b^{-1}k}$ one obtains that $\overline{ak} = \overline{abl} = l$ and thus $\lambda = a$. It follows that $\gamma_t^x \equiv \gamma_t \bmod B^2(P, M)$ if and only if $ac \equiv 1 \bmod p$; that is, if and only if x acts on P as on M. Since C acts trivially on P, the equation $(\gamma_t^y)^\alpha = t^y$ holds for all $y \in C$. Therefore $\gamma_s^n \equiv \gamma_s \bmod B^2(P, M)$ for every $s \in M$ and $n \in N$ if and only if $M \cong_N P$. Since $\{\gamma_s \mid s \in M\}$ is a transversal to $B^2(P, M)$ in $Z^2(P, M)$, one obtains the following equivalence:

$$\text{(7.1)} \qquad \mathrm{Fix}_N(H^2(P, M)) = H^2(P, M) \iff M \cong_N P.$$

a) Corollary 4.22 and Equation (7.1) yield that

$$H^2(G, M) \cong \mathrm{Fix}_N(H^2(P, M)) = H^2(P, M) \cong C_p.$$

Denote with $\overline{j} \in \mathrm{Aut}(M)$ the action of $j \in G$ on M. As in Theorem 4.7 let

$$T = \{(\alpha, \beta) \in \mathrm{Aut}(G) \times \mathrm{Aut}(M) \mid \forall j \in G: \ \overline{j^\alpha} = (\overline{j})^\beta\}$$

be the group of compatible pairs which acts on $H^2(G, M)$ via

$$\gamma \mapsto \gamma^{(\alpha,\beta)} = \left[(l, h) \mapsto \gamma(l^\alpha, h^\alpha)^{\beta^{-1}}\right].$$

As $\mathrm{Aut}(M)$ is abelian, it follows that

$$\widehat{T} = \{(1, \beta) \mid \beta \in \mathrm{Aut}(M)\} \leq T.$$

By construction, there are two orbits in $H^2(G, M)$ under the action of $\widehat{T}$: the trivial orbit $\{0\}$ and the orbit $H^2(G, M) \setminus \{0\}$ of size $p - 1$. Thus by Theorem 4.7, this yields that there are two isomorphism types of extensions of G by M: the split extension which corresponds to the trivial orbit and a non-split extension which corresponds to the non-trivial orbit. By Corollary 7.4, the non-split extension is the only Frattini extension of G by M.

b) From Corollary 4.22 and Equation (7.1) it follows that $H^2(G, M) = \{0\}$, and thus, by Corollary 7.4, there exists no Frattini extension of G by M . •

In particular, if there exists a unique Frattini extension, then Remark 7.6 indicates the structure of the corresponding cocycle.

Finally it remains to investigate the question how many G-modules M with $M \cong C_p$ and $M \cong_N P$ exist up to G-isomorphism. The next theorem solves this problem in our considered case. As a preliminary step, we provide the following lemma. The symbol A^G denotes the normal closure of a subset $A \subseteq G$ in the group G.

7.10. Lemma: *Let G be a group and let $A, B \leq G$ and $N \trianglelefteq G$.*

a) $(AN)^G = A^G N$.

b) If $N \leq A$, then $(A/N)^{G/N} = A^G/N$.

c) If $N \leq A$, then

$$A/N \cap BN/N = (A \cap BN)/N = (A \cap B)N/N.$$

Proof: a) The group $A^G N$ is a normal subgroup of G with $AN \leq A^G N$; that is, $(AN)^G \leq A^G N$. Since $A, N \leq (AN)^G$, it follows that $A^G N = (AN)^G$.

b) The group A^G/N is a normal subgroup of G/N with $A/N \leq A^G/N$ and it follows that $(A/N)^{G/N} \leq A^G/N$. Let $M \trianglelefteq G$ be defined by $(A/N)^{G/N} = M/N$. Then $A^G \leq M$ and thus $A^G/N = (A/N)^{G/N}$.

c) Obviously, $(A \cap BN)/N \leq A/N \cap BN/N$. Let $mN \in A/N \cap BN/N$; that is, there exist $a \in A$ and $b \in BN$ with $mN = aN = bN$. Then there is $n \in N$ with $b = an \in A \cap BN$ and thus $mN = anN \in (A \cap BN)/N$. This shows the first equation.

If $a = bn \in A \cap BN$ with $a \in A$, $b \in B$, and $n \in N$, then $b = an^{-1} \in A \cap B$ and thus $A \cap BN \leq (A \cap B)N$. If $cn \in (A \cap B)N$ with $c \in A \cap B$ and $n \in N$, then $cn \in A \cap BN$. This implies the second equation. •

7.11. Theorem: *Let G be a cube-free group and let $P \in Syl_p(G)$ such that $P \cong C_p$. Denote $N = N_G(P)$ and $Z = C_G(P)$ and let $R = Z^G$ be the normal closure of Z in G.*

a) There exists a G-module M with $M \cong_N P$ if and only if $R \cap N = Z$.

b) If M is a G-module with $M \cong_N P$, then M is unique up to G-isomorphism.

c) If G is solvable, then $R \cap N = Z$.

Proof: One can observe that $R \trianglelefteq G$ and $Z \leq R \cap N$. Since $N = N_G(P)$ and $P \in \mathrm{Syl}_p(R)$, the Frattini argument yields that $G = RN$; see Lemma 5.13. Thus the situation is as displayed in Figure 2; see page 61.

a) "$\Rightarrow$" Let M be a G-module with $M \cong_N P$ and let $H = C_G(M) \trianglelefteq G$ be the kernel of the operation of G on M. Since M is trivial as a P-module by Lemma 3.2, it follows that $P \leq H$ and the Frattini argument yields that $G = HN$. The group P is trivial as a Z-module and, because $P \cong_Z M$, it follows that $Z \leq H \trianglelefteq G$ and $R = Z^G \leq H$. Since $H \cap N = C_N(M) = C_N(P) = C_G(P) = Z \leq R \cap N$, the equation

$$|G| = \frac{|H||N|}{|H \cap N|} = \frac{|N||R|}{|N \cap R|}$$

shows that $|H| \leq |R|$ and therefore $R = H$. Hence $R \cap N = H \cap N = Z$ is proved.

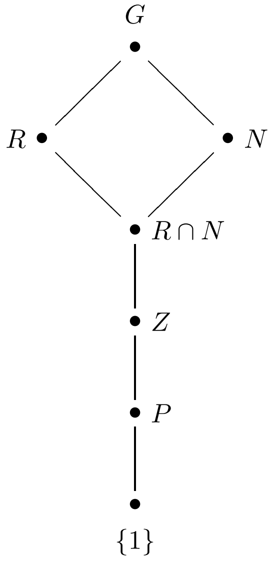

Figure 2.

"$\Leftarrow$" Let $G = RN$ and $R \cap N = Z$, and denote the action of N on P by $\alpha : N \to \mathrm{Aut}(P)$. If $g = r_1n_1 = r_2n_2 \in G$ with $r_1, r_2 \in R$ and $n_1, n_2 \in N$, then $n_1n_2^{-1} \in N \cap R = Z$ and thus $n_1^\alpha = n_2^\alpha$. Let $g \in P$ be a generator of P. We define $M = \langle m \rangle \cong C_p$ and $\delta : \mathrm{Aut}(P) \to \mathrm{Aut}(M)$, $(g \mapsto g^i) \mapsto (m \mapsto m^i)$, and observe that the operation

$$\beta : G \to \mathrm{Aut}(M),\ h = rn \mapsto (n^\alpha)^\delta,$$

of G on M is well defined. Obviously, β is a homomorphism and the mapping $P \to M$, $g \mapsto m$, induces an N-module isomorphism from P to M. In particular, M is a G-module with $M \cong_N P$.

b) Suppose there are two G-modules M_1 and M_2 with $M_1 \cong_N P \cong_N M_2$. Let $H_i = C_G(M_i)$ be the kernel of the operation of G on M_i for $i \in \{1, 2\}$. The proof of a) shows that $H_1 = R = H_2$ and, since $G = RN$, it follows that M_1 and M_2 are isomorphic as G-modules.

c) We use induction on $|G|$. The case $G = P$ is trivial and thus one can assume that $P < G$. Let Q be a minimal normal subgroup of G. Since G is solvable, the group Q is an elementary abelian q-group for a prime q. If $q = p$, then $Q = P$ and $N = G$ and $R \cap N = Z$. Hence one can assume $p \neq q$ in the following. Then $P \cap Q = \{1\}$. For a subgroup $U \leq G$ we define $\overline{U} = UQ/Q$.
First, we show that $Q \leq R$ holds. Suppose that $Q \not\leq R$; that is, $R \cap Q = \{1\}$ as Q is a minimal normal subgroup. It follows that $[Q, P] \leq [Q, R] \leq R \cap Q = \{1\}$ and hence $Q \leq Z$. But $Z \cap Q \leq R \cap Q = \{1\}$ now implies that Q is trivial which contradicts the choice of Q.

Next, we note that $\overline{N} = N_{\overline{G}}(\overline{P})$ holds, since the Frattini argument yields that $NQ = N_G(PQ)$.
Further, we show that $\overline{Z} = C_{\overline{G}}(\overline{P})$ holds. It follows from the construction that $\overline{Z} \leq C_{\overline{G}}(\overline{P})$. Let $cQ \in C_{\overline{G}}(\overline{P})$. As $C_{\overline{G}}(\overline{P}) \leq N_{\overline{G}}(\overline{P}) = \overline{N}$, one can write $c = hn$ for some $h \in Q$ and $n \in N$. Then for every $k \in P$ it follows that $[c, k] = [hn, k] = [h, k]^n[n, k] \in QP$. On the other hand $cQ \in C_{\overline{G}}(\overline{P})$ implies that $[c, k] \in Q$. Thus $[n, k] \in Q \cap P = \{1\}$ for every $k \in P$. This implies $n \in Z$ and thus $cQ = nQ \in \overline{Z}$. In summary, this yields that $\overline{Z} = C_{\overline{G}}(\overline{P})$.
Now $\overline{R} \cap \overline{N} = \overline{Z}$ follows from the induction hypothesis and the fact that $\overline{R} = \overline{Z}^{\overline{G}}$ by Lemma 7.10a),b).
Finally, we show that $R \cap N = Z$ holds. For this purpose, note that $N \cap Q$ and P are both normal in N. Thus $[N \cap Q, P] \leq N \cap Q \cap P = \{1\}$ and $N \cap Q \leq Z \cap Q$. Hence $N \cap Q = Z \cap Q$ follows. We recall that $Q \leq R$. Since $N \cap Q = Z \cap Q \leq Z \leq R$, it follows from Lemma 7.10c) that $Z/Z \cap Q \cong \overline{Z} = \overline{R} \cap \overline{N} = \overline{R \cap N} \cong R \cap N/R \cap N \cap Q \cong R \cap N/N \cap Q$ and thus $R \cap N = Z$. •

In particular, the Theorems 7.5 - 7.11 yield a proof for the following theorem.

7.12. Theorem (Main Theorem)**:** *Let F be a Frattini-free group of cube-free order and write $F = A \times L$ where A is non-abelian simple or trivial and L is solvable, as in Corollary 6.23. Let $\{p_1, \ldots, p_r\}$ be a set of primes such that $p_i \mid |F|$ and $p_i^2 \nmid |F|$ for $1 \leq i \leq r$ and let $M \cong C_{p_1} \times \ldots \times C_{p_r}$.*

a) There exists a Frattini extension of F by M if and only if $p_i \mid |L|$ for $1 \leq i \leq r$. In this case there exists exactly one F-module structure on M which allows Frattini extensions and for this unique F-module structure on M there exists exactly one Frattini extension up to isomorphism.

b) If G is a Frattini extension of F by M, then $G = A \times H$ where H is a Frattini extension of L by M.

It follows an important corollary.

7.13. Corollary: *Let $n = p_1^{e_1} \cdots p_r^{e_r}$ with distinct primes $p_1, \ldots, p_r$ and $e_1, \ldots, e_r \in \{1, 2\}$. There is a one-to-one correspondence between the groups of cube-free order n and the Frattini-free groups $F = A \times L$, as in Corollary 6.23, with $|F| \mid n$ and $p_1 \cdots p_r \mid |L|$.*

In particular, there is a one-to-one correspondence between the solvable groups of cube-free order $n = p_1^{e_1} \cdots p_r^{e_r}$ and the solvable Frattini-free groups F with $|F| \mid n$ and $p_1 \cdots p_r \mid |F|$.

Chapter 8

Square-free groups

A group G has square-free order if $p^2 \nmid |G|$ for every prime p. As mentioned in the introduction of this thesis, the groups of square-free order are known for a long time; Hölder [21] has investigated them at the end of the 19th century.

Now we exhibit what follows from the approach of this thesis; that is, from the Frattini extension method.

8.1. Lemma: *A group of square-free order is Frattini-free.*

Proof: This follows from Lemma 5.15. •

This implies that step two of the Frattini extension method is omitted as one has not to construct any Frattini extension.

8.2. Lemma: *If G is a square-free group, then $Soc(G) \cong C_{p_1} \times \ldots \times C_{p_k}$ for distinct primes $p_1, \ldots, p_k$.*

Proof: This follows from Theorem 6.10. •

Since groups of square-free order are Frattini-free, one can modify Theorem 6.19 to construct them:

8.3. Theorem: *Let $n = p_1 \ldots p_m$ for distinct primes $p_1, \ldots, p_m$. Let $\mathcal{S}$ be the list of all subgroups of $C_{p_1} \times \ldots \times C_{p_m}$ and for every $S \in \mathcal{S}$ define $\mathcal{K}_S$ to be the list of all subgroups K of $Aut(S)$ with $|K||S| = n$. Then*

$$\{K \ltimes S \mid S \in \mathcal{S},\ K \in \mathcal{K}_S\}$$

is a complete and irredundant list of isomorphism type representatives of groups of order n.

Proof: Let S be the socle of a group of order n. It follows from Lemma 8.2 that S and $\mathrm{Aut}(S)$ are abelian and thus $\mathrm{Inn}(S) = \{1\}$. Hence no two subgroups of $\mathrm{Aut}(S)$ are conjugated in $\mathrm{Aut}(S)$. Since S is Γ-completely reducible for every $\Gamma \leq \mathrm{Aut}(S)$, the assertion follows from Theorem 6.19. •

In particular, one has to construct *all* subgroups K of the abelian group $\mathrm{Aut}(S)$. Concerning this computation it is another advantage over the cube-free case that $\mathrm{Aut}(S)$ is a direct product of cyclic groups.

Moreover, one obtains that every group of square-free order is solvable with derived length at most 2. Groups with this property are also called metabelian.

Now we present a construction algorithm and an isomorphism test for square-free groups:

The following algorithm takes as input a square-free integer $n = p_1 \ldots p_m$ and returns a list of all groups of order n up to isomorphism.

```
**SquareFreeGroups**($n$)
initialize *Groups* as empty list
for every $s \mid n$ do
    write $s$ as $s = p_{i_1} \cdots p_{i_l}$
    define $S := C_{p_{i_1}} \times \ldots \times C_{p_{i_l}}$ and $\mathrm{Aut}(S) := C_{p_1 - 1} \times \ldots \times C_{p_l - 1}$
    define $\mathcal{G} := \{\Gamma \ltimes S \mid \Gamma \leq \mathrm{Aut}(S) \text{ with } |\Gamma| = n/s\}$
    append $\mathcal{G}$ to *Groups*
return the list *Groups*
```

By Theorem 8.3, a square-free group G with socle S has the form $G \cong \Gamma \ltimes S$ for an unique subgroup $\Gamma \leq \mathrm{Aut}(S)$. One can determine Γ from G and S: Let $T \leq G$ be a complement to S in G; that is, $G \cong T \ltimes S$. As $C_G(S) = S$, the group T acts faithfully on S and therefore can be identified with a subgroup $\widehat{\Gamma} \leq \mathrm{Aut}(S)$. Then $G \cong \widehat{\Gamma} \ltimes S$ and, as Γ is unique, it follows that $\widehat{\Gamma} = \Gamma$.

The next algorithm decides whether two square-free groups G_1 and G_2 are isomorphic.

```
**IsomorphismTestSF**($G_1$,$G_2$)
if $|G_1| \neq |G_2|$ then return *false*
compute $S_i := \mathrm{Soc}(G_i)$ for $i \in \{1, 2\}$
if $|S_1| \neq |S_2|$ then return *false*
determine $\Gamma_i \leq \mathrm{Aut}(S_i)$ such that $G_i \cong \Gamma_i \ltimes S_i$ for $i \in \{1, 2\}$
identify $S_1 = S_2$ and $\mathrm{Aut}(S_1) = \mathrm{Aut}(S_2)$ and hence $\Gamma_1, \Gamma_2 \leq \mathrm{Aut}(S_1)$
if $\Gamma_1 \neq \Gamma_2$ then
    return *false*
else
    return *true*
```

This completes our examination of the square-free groups.

Chapter 9

Cube-free groups

This chapter outlines the main results of this thesis.

As a first step, we have investigated the nilpotent, simple, and completely reducible groups of cube-free order; see Theorems 2.2, 2.7, and 6.10.

(1) The group G is a nilpotent group of cube-free order if and only if $G \cong S_{p_1} \times \ldots \times S_{p_r}$ for distinct primes $p_1, \ldots, p_r$ and $S_p \in \{C_p, C_p^2, C_{p^2}\}$ for every prime p.

(2) The group G is a simple group of cube-free order if and only if $G \cong C_p$ for a prime p or $G \cong \mathrm{PSL}(2, r)$ for a prime $r > 3$ with $r+1$ and $r-1$ cube-free.

(3) The group S is a completely reducible group of cube-free order if and only if $S \cong A \times B \times C$ with

- $A \in \{\mathrm{PSL}(2,r) \mid r > 3 \text{ prime with } r+1 \text{ and } r-1 \text{ cube-free}\} \cup \{\{1\}\}$,
- $B = C_{p_1} \times \ldots \times C_{p_n}$ for different primes $p_1, \ldots, p_n$ with $p_i^2 \nmid |A|$, and
- $C = C_{q_1}^2 \times \ldots \times C_{q_m}^2$ for different primes $q_1, \ldots, q_m \nmid |A||B|$.

Since every group G is an extension of its Frattini factor $G/\Phi(G)$ by its Frattini subgroup $\Phi(G)$, we have examined the structure of the possible Frattini subgroups and Frattini-free groups; see Corollary 5.16 and Theorem 6.22.

(4) Let G be a cube-free group. Then $\Phi(G) \cong C_{r_1} \times \ldots \times C_{r_k}$ for distinct primes $r_1, \ldots, r_k$ with $r_i^2 \mid |G|$ for $1 \leq i \leq k$.

(5) Let $S = A \times B \times C$ be a cube-free completely reducible group as in (3). The group F is a Frattini-free group of cube-free order with socle isomorphic to S if and only if

$$F \cong A \times L \quad \text{with} \quad L = (K \ltimes (B \times C))$$

for some $K \leq \mathrm{Aut}(B \times C)$ such that $|K||S|$ is cube-free.

Further, two cube-free Frattini-free groups $F_1 = A \times (K_1 \ltimes (B \times C))$ and $F_2 = A \times (K_2 \ltimes (B \times C))$ are isomorphic if and only if K_1 and K_2 are conjugated in $\mathrm{Aut}(B \times C)$.

The required groups $K \leq \mathrm{Aut}(B \times C)$ have been considered in Theorem 3.12 and it follows that K is a subdirect product of subgroups of groups of the type C_p, $\mathrm{N}(2,p)$, and $\mathrm{M}(2,p)$. In particular, every cube-free Frattini-free group F has the form $F = A \times L$ where A is non-abelian simple or trivial and L is solvable.

Next, we have examined the cube-free Frattini extensions; see Theorem 7.12. Let $F = A \times L$ be a cube-free Frattini-free group as in (5) and let $r_1, \ldots, r_k$ be distinct primes with $r_i \mid |F|$ and $r_i^2 \nmid |F|$ for $1 \leq i \leq k$. Let $M \cong C_{r_1} \times \ldots \times C_{r_k}$.

(6) There exists a Frattini extension of F by M if and only if $r_1 \ldots r_k \mid |L|$. In this case there is exactly one F-module structure on M which allows Frattini-extensions and for this unique F-module structure on M there exists exactly one Frattini extension G up to isomorphism.

(7) The unique isomorphism type of the extension G in (6) is given by

$$G \cong A \times (G_1 \Yup \ldots \Yup G_k)$$

where G_i is the unique minimal Frattini extension of L by $M_i \cong C_{r_i}$ for $1 \leq i \leq k$ (compare Remark 7.6) and

$$G_1 \Yup \ldots \Yup G_k = \{(g_1, \ldots, g_k) \in G_1 \times \ldots \times G_k \mid g_1 M_1 = \ldots = g_k M_k\}.$$

In particular, $G_1 \Yup \ldots \Yup G_k$ is solvable.

For the sake of completeness we note a consequence; see Theorem 7.8.

(8) Let G be a cube-free group with Frattini factor $F \cong A \times L$ as in (5) and Frattini subgroup $M \cong C_{r_1} \times \ldots \times C_{r_k}$ as in (4). Then G has the form

$$G \cong A \times (G_1 \Yup \ldots \Yup G_k)$$

as in (7).

Therefore a cube-free group is either solvable or a direct product of a non-abelian simple group with a solvable group.

As an important result of this thesis one obtains the the following:

(9) By (6) and (8), there is a one-to-one correspondence between the cube-free groups of order $n = r_1^{e_1} \ldots r_k^{e_k}$ (prime-power factorization) and the cube-free Frattini-free groups $F = A \times L$, as in (5), with $|F| \mid n$ and $r_1 \cdots r_k \mid |L|$; see Corollary 7.13.

Since the Frattini-free groups are classified by Theorem 6.19, this may yield a classification of the cube-free groups.

Furthermore, the approach of this thesis gives rise to an algorithm to construct the groups of a given cube-free order n up to isomorphism. This algorithm is also very efficient to compute groups of square-free order.

Further investigations may consider the explicit classification of the cube-free groups as well as the improvement of the construction algorithm.

The approach of this thesis may also be applied to investigate the groups of order n with $p^4 \nmid n$ for all primes p; even though the theory to work on this case seems to be much more difficult to handle.

Chapter 10

Algorithms and implementation

This chapter gives a summary of the algorithm to construct all groups of a given cube-free order up to isomorphism. Further, a report on experiments with an implementation is given.

10.1 The construction of cube-free groups

The function *CubeFreeGroups*(n) takes as input a cube-free n and returns a list of all groups of order n up to isomorphism.

```
**CubeFreeGroups**$(n)$
initialize Groups and Simple as empty lists
for every prime $p > 3$ with $p+1$ and $p-1$ cube-free do
    if $p(p+1)(p-1)/2 \mid n$ then
        add $\mathrm{PSL}(2,p)$ to Simple
for every $A$ in Simple do
    append $\{A \times L \mid L \in CubeFreeSolvableGroups(n/|A|)\}$ to Groups
return the list Groups
```

The function *CubeFreeSolvableGroups*(n) takes as input a cube-free n and returns a list of all solvable groups of order n up to isomorphism. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime-power factorization of n.

```
**CubeFreeSolvableGroups**$(n)$
initialize Groups as empty list
for every $m \mid n$ with $p_1 \cdots p_r \mid m$ do
    for every $L$ in CubeFreeSolvableFFGroups$(m)$ do
        add CubeFreeSolvableFExtension$(L,n/m)$ to Groups
return the list Groups
```

The function *CubeFreeSolvableFFGroups*(n) takes as input a cube-free n and returns a list of all solvable Frattini-free groups of order n up to isomorphism.

```
CubeFreeSolvableFFGroups($n$)
initialize Groups as empty list
for every $m \mid n$ do
    write $m$ as $m = p_1 \cdots p_k p_{k+1}^2 \cdots p_l^2$ (prime-power factorization)
    define $B := C_{p_1} \times \ldots \times C_{p_k}$ and $C := C_{p_{k+1}^2} \times \ldots \times C_{p_l}^2$
    define $\mathcal{M} := \{K \ltimes (B \times C) \mid K \in CubeFreeAutGrps(B \times C, n/m)\}$
    append $\mathcal{M}$ to Groups
return the list Groups
```

The next algorithm takes a solvable cube-free group L and a square-free $n = p_1 \cdots p_k$ with $p_i \mid |L|$ and $p_i^2 \nmid |L|$ for $1 \leq i \leq k$ and computes the unique cube-free Frattini extension of L by $M \cong C_{p_1} \times \ldots \times C_{p_k}$.

```
CubeFreeSolvableFExtension($L$,$n$)
write $n = p_1 \cdots p_k$
for $i$ in $\{1, \ldots k\}$ do
    compute a Sylow $p_i$-subgroup $P$ of $L$
    determine $N := N_L(P)$ and $R := C_L(P)^L$
    for $l \in L$ choose $\overline{l} = n$ if $l = rn \in RN$.
    define $M_i \cong P$ as an $L$-module via $m \mapsto m^l = m^{\overline{l}}$
    compute a non-trivial $\gamma_i \in H^2(L, M_i)$
    compute the extension $E_i$ of $L$ by $M_i$ via $\gamma_i$
return $E := E_1 \curlywedge \ldots \curlywedge E_k$
```

It remains to compute the subgroups of

$$\mathrm{Aut}(B \times C) \cong C_{p_1 - 1} \times \ldots \times C_{p_k - 1} \times \mathrm{GL}(2, p_{k+1}) \times \ldots \times \mathrm{GL}(2, p_l)$$

of a given order m up to conjugacy. These subgroups can be determined from their projections into the direct factors. Hence, by Theorem 3.12, we compute all possible projections $Z_i \leq C_{p_i - 1}$ and $G_j \leq \mathrm{GL}(2, p_j)$, respectively, up to conjugacy. Using a subdirect product construction, see Section 6.5 and [12], we determine all subdirect products U of $Z_1 \times \ldots \times Z_k \times G_{k+1} \times \ldots \times G_l$ of order m up to conjugacy in $\mathrm{Aut}(B \times C)$.

A list of all possible irreducible subgroups of $\mathrm{GL}(2, p)$ up to conjugacy can be extracted from [15], Section 4. By Theorem 3.12, the required reducible subgroups of $\mathrm{GL}(2, p)$ are determined as the cube-free subgroups of the group of diagonal matrices of $\mathrm{GL}(2, p)$.

The function *CubeFreeAutGrps*$(B \times C$,$m)$ takes as input an abelian socle $B \times C$ and a cube-free m and returns a list of all subgroups of $\mathrm{Aut}(B \times C)$ of order m up to conjugacy. All groups in the following algorithm are determined up to conjugacy.

```
CubeFreeAutGrps($B \times C$,$m$)
initialize Groups as empty list
for $p_i \mid |B| = p_1 \cdots p_l$ and $p_j \mid |C| = p_{l+1}^2 \cdots p_t^2$ do
    compute a list $\mathcal{L}_i$ of all cube-free $U \leq C_{p_i - 1}$
    compute a list $\mathcal{L}_j$ of all cube-free $U \leq \mathrm{GL}(2, p_j)$ with $p_j \nmid |U|$
for all groups $D := D_1 \times \ldots \times D_t$ with $D_i \in \mathcal{L}_i$ do
    compute a list SubDir of all subdirect products $U \leq D$ with $|U| = m$
    append SubDir to Groups
return the list Groups
```

This completes the algorithm to construct all groups of a given cube-free order.

10.2 Implementation and performance

The algorithm described above is implemented in the computer algebra system Gap [29]; see [10]. All runtimes are given in seconds.

10.2.1 Cube-free groups of order at most 10 000

We have constructed all isomorphism types of cube-free groups of order at most 10 000 using a modified algorithm: When computing the cube-free groups of order n we can assume that the Frattini-free groups of cube-free order $m < n$ are known. This means that we have stored the cube-free Frattini-free groups of order m during the previous computations. Nevertheless, the Frattini-free groups of order n have to be computed. In particular, every square-free group has a trivial Frattini subgroup by Lemma 8.1.

We note that there are 8 319 cube-free integers between 1 and 10 000 and 6 083 of them are square-free.

The following table contains a description of this computation:

• # Isomorphism types of cube-free groups:	58 312.
Runtime to compute these groups:	17 752.
• # Isomorphism types of square-free groups:	16 615.
Runtime to compute these groups:	2 009.
• # Isomorphism types of cube-free but not square-free groups:	41 697.
Runtime to compute these groups:	15 741.

As the runtimes indicate, the algorithm is also very efficient to construct the groups of square-free order. This is indeed not surprising in regard to the theory presented in Chapter 8. In particular, when computing the groups of a square-free order, the algorithm **CubeFreeGroups** automatically degenerates to the algorithm **SquareFreeGroups**; see page 64.

The following table lists the top orders with respect to the number of different isomorphism types. We use the non-modified algorithm to compute these groups.

Order	Factorized order	# Groups	Runtime
8 820	$2^2 \cdot 3^2 \cdot 5 \cdot 7^2$	672	197
6 300	$2^2 \cdot 3^2 \cdot 5^2 \cdot 7$	570	158
9 900	$2^2 \cdot 3^2 \cdot 5^2 \cdot 11$	492	131
7 644	$2^2 \cdot 3 \cdot 7^2 \cdot 13$	378	93
8 892	$2^2 \cdot 3^2 \cdot 13 \cdot 19$	303	82
9 324	$2^2 \cdot 3^2 \cdot 7 \cdot 37$	303	89
6 084	$2^2 \cdot 3^2 \cdot 13^2$	298	96
3 276	$2^2 \cdot 3^2 \cdot 7 \cdot 13$	268	69
4 788	$2^2 \cdot 3^2 \cdot 7 \cdot 19$	259	71
5 460	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	238	61
7 260	$2^2 \cdot 3 \cdot 5 \cdot 11^2$	234	71

10.2.2 Some large applications

Now we consider some larger cube-free orders. The results are given in the following table. The first part of the table contains genuine cube-free orders, while the second part contains some larger square-free orders.

Factorized order	# Groups	Runtime
$5^2 \cdot 7 \cdot 13^2 \cdot 67^2 \cdot 97 \cdot 107$	12	178
$19^2 \cdot 23^2 \cdot 29 \cdot 37 \cdot 67 \cdot 73^2 \cdot 107^2$	24	1 720
$167 \cdot 191^2 \cdot 233^2 \cdot 241$	4	17
$29 \cdot 31 \cdot 37 \cdots 83 \cdot 89 \cdot 97$ (primes)	4	48
$19 \cdot 461 \cdot 6\,449 \cdot 8\,779 \cdot 9\,907$	2	271
$13 \cdot 241 \cdot 6\,449 \cdot 20\,051$	2	148

Compared to the runtimes to compute the groups of order at most 2 000, see [5], one can observe that the Frattini extension method restricted to the cube-free or square-free case is a very efficient method to construct these groups. In particular, one is able to compute groups of a much larger order when using this algorithm in the cube-free case.

10.2.3 Bottlenecks

Since the irreducible subgroups of $\mathrm{GL}(2,p)$ are given explicitely in [15], the runtime of the algorithms divides predominantly into the computation of the subdirect products, see algorithm **CubeFreeAutGrps**, and into the determination of the Frattini extensions, see algorithm **CubeFreeSolvableFExtension**.

Acknowledgments

First and foremost, I would like to thank my supervisor, Prof. Dr. Bettina Eick, for the great ongoing encouragement and numerous helpful discussions and advice. I am highly thankful for her inspiring collaboration and for making this work and especially the published version of this work possible.

Furthermore, I am grateful to Andreas Distler, Dörte Feichtenschlager, Dr. Harm Pralle, and Christian Sievers for proofreading and helping me when I had questions.

As this thesis completes my time as a student, I would like to thank quite a number of different people.

First of all, I am deeply indebted to Gabriele, Wolfgang, and Anja Dietrich and the remainder of my family, who made my study possible and who assisted me steadily during the last years. Thank you for all.

Sincere thanks to Prof. Dr. Heiko Harborth for his encouragement and collaboration, as well as the numerous interesting occupational and also private discussions.

I would like to thank my student colleagues, especially Thomas Möstl and Andreas Wörner, for the interesting and helpful discussions besides the study.

Last but not least, I would like to thank my friends, especially Alina, Anja, Steffi, and Thomas, for their patience and for always being there for me.

Heiko Dietrich

Bibliography

[1] A. Babakhanian. *Cohomological Methods in Group Theory.* Marcel Dekker, Inc., New York, 1972.

[2] G. Bagnera. La Composizione dei Gruppi finiti il cui Grado él la quinta Potenza di un Numero primo. *Ann. Mat. Pura Appl.*, **1**(3): 137 – 228, 1898.

[3] H. A. Bender. A Determination of the Groups of Order p^5. *Ann. Math.*, **29**(2): 61 – 72, 1927.

[4] H. U. Besche and B. Eick. Construction of finite Groups. *J. Symb. Comput.*, **27**: 387 – 404, 1999.

[5] H. U. Besche, B. Eick, and E. A. O'Brien. A Millenium Project: Constructing small Groups. *Intern. J. Alg. and Comput.*, **12**: 623 – 644, 2002.

[6] H. Cartan and S. Eilenberg. *Homological Algebra.* Princeton, 1956.

[7] A. Cayley. On the Theory of Groups, as depending on the Symbolic Equation $\theta^n = 1$. *Philos. Mag.*, **4**(7): 40 – 47, 1854.

[8] A. Cayley. On the Theory of Groups, as depending on the Symbolic Equation $\theta^n = 1$ - Part III. *Philos. Mag.*, **4**(18): 34 – 37, 1859.

[9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups.* Clarendon Press, Oxford, 1985.

[10] H. Dietrich and B. Eick. The GAP-package *cfgroups* available under. *http://www.icm.tu-bs.de/ag_algebra/software/dietrich/cfgroups/.*

[11] H. Dietrich and B. Eick. On the Groups of Cube-Free Order. To appear in *J. Alg.*, 2005.

[12] B. Eick. Charakterisierung und Konstruktion von Frattinigruppen und Anwendungen in der Konstruktion endlicher Gruppen. Aachener Beiträge zur Mathematik, 1996. Dissertation, RWTH Aachen.

[13] W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, **13**: 775 – 1029, 1963.

[14] H. Fitting. Beiträge zur Theorie der Gruppen endlicher Ordnung. *Jahresbericht der DMV*, **48**: 77 – 145, 1938.

[15] D. L. Flannery and E. A. O'Brien. The linear groups of small degree over finite fields. To appear in *Intern. J. Alg. and Comput.*, 2004.

[16] W. Gaschütz. Über die Φ-Untergruppe endlicher Gruppen. *Math. Z.*, **58**: 160 – 170, 1953.

[17] D. Gorenstein, R. Lyons, and R. Solomon. *The Classification of the Finite Simple Groups.* Mathematical Surveys and Monographs 40.1. Amer. Math. Soc., Providence, 1994.

[18] D. Gorenstein and J. H. Walter. The Characterization of Finite Groups with Dihedral Sylow 2-Subgroups. *J. of Algera*, **2**: 85 – 151, 1964.

[19] O. Hölder. Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4. *Math. Ann.*, **43**: 301 – 412, 1893.

[20] B. Huppert. *Endliche Gruppen I.* Springer Heidelberg, 1967.

[21] O. Hölder. Die Gruppen mit quadratfreier Ordnung. *Nachr. Königl. Ges. Wiss. Göttingen Math.-Phys. K* **1**: 211 – 229, 1895.

[22] G. A. Miller. Report on Recent Progress in the Theory of Groups of a Finite Order. *Bull. Amer. Math. Soc.*, **5**: 227 – 249, 1899.

[23] M. Potron. Sur Quelques Groupes d'Ordre p^6, 1904. Ph.D. Thesis, Gauthier-Villars, Paris.

[24] M. Potron. Sur Quelques Groupes d'Ordre p^6. *Bull. Soc. Math. France*, **32**: 296 – 300, 1904.

[25] D. J. S. Robinson. *A Course in the Theory of Groups.* Springer-Verlag, New York, Heidelberg, Berlin, 1982.

[26] O. Schreier. Über die Erweiterung von Gruppen. II. *Abh. Math. Sem. Univ. Hamburg*, **4**: 47 – 71, 1926.

[27] M. W. Short. *The primitive Soluble Permutation Groups of Degree less than 256.* Lecture Notes in Math. 1519. Springer-Verlag, 1992.

[28] D. R. Taunt. Remarks on the Isomorphism Problem in Theories of Construction of finite Groups. *Proc. Cambridge Philos. Soc*, **51**: 16–24, 1955.

[29] The GAP Group. *GAP – Groups, Algorithms and Programming.* http://www.gap-system.org, 2000.

[30] M. O. Tripp. Groups of Order p^3q^2, 1909. Ph.D. Thesis, Columbia University.

[31] R. L. Vavasseur. Les Groupes d'Ordre p^2q^2, p étant un Nombre premier plus grande que le Nombre premier q. *C. R. Acad. Sci. Paris Vie Académique*, **128**: 26 – 27, 1899.

[32] R. L. Vavasseur. Les Groupes d'Ordre p^2q^2, p étant un Nombre premier plus grande que le Nombre premier q. *Ann. de l'Éc. Norm.*, **19**(3): 335 – 355, 1902.

[33] E. Weiss. *Cohomology of Groups*, volume 34 of *Pure and Applied Mathematics.* Academic Press, Inc., New York, 1969.

[34] A. E. Western. Groups of Order p^3q. *Proc. London Math. Soc.*, **30**(1): 209 – 263, 1899.

[35] D. Wilkinson. The Groups of Exponent p and Order $p \geq 7$ (p any Prime). *J. Algebra*, **118**: 109 – 119, 1988.

Index

The numbers refer to the page where the corresponding expressions are defined or used first.