Palindromes in Finite Groups

Dagur Tómas Ásgeirsson

Faculty of Physical Sciences
University of Iceland
2019

PALINDROMES IN FINITE GROUPS

Dagur Tómas Ásgeirsson

10 ECTS thesis submitted in partial fulfillment of a
Baccalaureus Scientiarum degree in Mathematics

Advisors
Patrick Devlin
Rögnvaldur G. Möller

Examiner
Anders Claesson

Faculty of Physical Sciences
School of Engineering and Natural Sciences
University of Iceland
Reykjavik, February 2019

Palindromes in Finite Groups
10 ECTS thesis submitted in partial fulfillment of a B.Sc. degree in Mathematics

Faculty of Physical Sciences
School of Engineering and Natural Sciences
University of Iceland
Dunhagi 5
107, Reykjavik
Iceland

Telephone: 525 4000

Bibliographic information:
Dagur Tómas Ásgeirsson, 2019, Palindromes in Finite Groups, B.Sc. thesis, Faculty of Physical Sciences, University of Iceland.

Printing: Háskólaprent, Fálkagata 2, 107 Reykjavík
Reykjavik, Iceland, February 2019

Abstract

In this work, we begin by giving an overview of some topics in group theory, namely semidirect products, nilpotent groups and wreath products. We use wreath products to prove Schur's theorem which says that if the order and index of a normal subgroup A of a group G are relatively prime, then the A has a complement in G. Next, we introduce the notion of a *civic group*: a group with the property that every subset which is closed under taking palindromes is a subgroup. We prove that civic groups satisfy the property that its *palindromic width* is equal to one and then we reduce the classification of civic groups to the odd order case. More precisely, we show that every civic group is a direct product of a cyclic 2-group and a civic group of odd order. Further, we show that a minimal group of odd order having palindromic width greater than 1 is a semidirect product of two elementary abelian groups, or a p-group. This is also the form of the minimal non-civic groups of odd order. Finally, we show that for solving the so-called Magnus-Derek game [6, 8] on general finite groups, it suffices to consider the odd order case. We give a solution of the game for civic groups of odd order, as well as other groups having sufficiently large subgroups. Moreover, we make progress on the solution of the game in general groups by giving a solution in terms of a maximal subset closed under taking palindromes. We conjecture that such subsets can in fact always be chosen to be subgroups, but that question remains open for now.

Contents

Acknowledgement

First and foremost, I would like to thank Professor Patrick Devlin of Yale University for meeting with me during his stopover in Iceland last summer and suggesting this interesting research project. I am greatly indebted to him for his help and patience with all my questions and I hope that we will continue our collaboration on this project and other research in the future.

Secondly, I am grateful to Professor Rögnvaldur G. Möller of the University of Iceland for encouraging me to write a bachelor's thesis about this project, for reading many preliminary versions of it and making many helpful remarks.

I would also like to thank Professor Anders Claesson of the University of Iceland for acting as examiner and reading, and listening to me present, the thesis.

Introduction

The main topic of this thesis are groups which we call *civic groups*:

Definition. We say that a group G is *civic* if any subset P of G satisfying the properties

- $1 \in P$
- $a, b \in P \Rightarrow aba \in P$

is a subgroup of G. We say that a subset P satisfying the above properties is *palindromic* in G.

The idea of this definition came up when the author, along with his advisor and collaborator Professor Patrick Devlin of Yale University, was trying to solve the Magnus-Derek game [6, 8] on general groups. The game is played by two players called Magnus and Derek. A token starts at some given group element and Magnus moves it around the group by specifying a group element g while Derek gets to decide whether to right multiply the current position by g or g^{-1}. Magnus's goal is to maximize the number of elements visited while Derek's is to minimize this number. Gerbner [6] solved the game for abelian groups and a few other cases. In Section 2.2, a partial solution of this game in a general group is given. Civic groups and palindromes in groups, are treated in Section 2.1.

We found a solution to the Magnus-Derek game for civic groups of odd order, and at first, we conjectured that all groups of odd order are in fact civic. That conjecture turned out to be wrong; one of the non-abelian groups of order 27 is a small counterexample. However, the study of civic groups of odd order is of interest, because a classification of them would imply a classification of all civic groups, see Theorem 2.1.12. Some work has been done on palindromes in groups, see e.g. [5], where Fink and Thom prove results on palindromes in simple groups. That paper gave us the idea of *reversibility* of a group with respect to some generating set (see Definition 2.1.13 in Section 2.1). We give a solution to the game in terms of maximal palindromic sets, and in the cases when those coincide with subgroups, we have quite a satisfactory solution to the game. This happens, for instance, in nilpotent groups, which are the topic of Section 1.2, and other groups which have a subgroup whose index is the smallest prime divisor of the order of the group. This is substantial progress compared to what was known before.

In Section 2.1 civic groups of both even and odd order are treated in detail. We prove that the classification of them reduces to the odd order case by showing that every civic group is the direct product of a cyclic 2-group and an odd order civic group (Theorem 2.1.12). Then we go on to make progress on the classification of odd order civic groups by giving the form of minimal, non-civic groups of odd order: $(\mathbb{Z}/p\mathbb{Z})^r \rtimes (\mathbb{Z}/q\mathbb{Z})$, with $r \in \mathbb{N}$, and p and q distinct primes, or a non-civic p-group. The study of civic groups is of course related to the study of palindromes in groups. We show that the set of all palindromes in a group with a fixed generating set, has size dividing the order of the group, that a group consisting of palindromes such that every subgroup also consists of palindromes (i.e. has *palindromic width* 1 with respect to any generating set – see Definition 2.1.2) is civic, and that civic groups consist of palindromes (in the sense of Definition 2.1.2).

We begin, however, by studying some interesting topics in group theory – namely, semidirect products, nilpotent groups and wreath products. In chapter 1 we give the definitions of these, and prove a few results which we wish to use in the subsequent chapter.

1. Topics in Group Theory

This chapter will serve as an introduction to some topics in group theory, usually not covered at the undergraduate level. The choice of topics is motivated by the content of chapter 2; the aim is to prove as many as possible of the non-trivial results used there. Most of the contents of this chapter is based on the text of *Abstract Algebra* by Dummit and Foote [3]. In Section 1.3, we choose the approach of Kargapolov and Merzljakov [7] to prove Schur's theorem, instead of following Dummit and Foote.

1.1. Semidirect Products

Let G be a group with subgroups H and K such that H is a normal subgroup of G. Then it is well-known that the set

$$HK = \{hk : h \in H, k \in K\}$$

is a subgroup of G. If we add the assumption that $H \cap K = \{1\}$, we have a bijection between HK and the cartesian product (H, K) (we use this notation to avoid confusion with the direct product of groups, which will be introduced shortly) by mapping $hk \mapsto (h, k)$. We want to define binary operation on the set (H, K) which makes it into a group, isomorphic to HK; this we will call the *semidirect product* of H and K. Moreover, we will see that we do not need the restriction that H, K be subgroups of some given group G.

Now, take two elements $hk, h'k'$ of HK. We will use the following as a model when constructing our operation on $H \times K$:

$$\begin{aligned}(hk)(h'k') &= hkh'(k^{-1}k)k' \\ &= h(kh'k^{-1})kk' \\ &= h''k'',\end{aligned}$$

where $h'' = h(kh'k^{-1})$ and $k'' = kk'$. It is clear that $k'' \in K$; to see that $h'' \in H$ recall that H is a normal subgroup of G so $kh'k^{-1} \in H$, thus $h'' = h(kh'k^{-1}) \in H$.

Let H, K be arbitrary groups. We want to mimic the above to construct a group with underlying set (H, K), which contains a normal subgroup isomorphic to H and a subgroup isomorphic to K. To define the operation

$$\text{“}(h,k)(h',k') = (h(kh'k^{-1}), kk')\text{”}$$

on $H \times K$, we need to define what $kh'k^{-1}$ *means* in this context — after all, H and K are completely arbitrary groups whose elements cannot simply be multiplied with each other — to do this, we will need the notion of a *group action*.

Definition 1.1.1. A *group action* of G on a set A is a map $\cdot : G \times A \to A$ satisfying the properties (i) and (ii) below. Instead of $\cdot(g, a)$ we will write $g \cdot a$.

(i) For all $g, g' \in G$ and all $a \in A$, $g \cdot (g' \cdot a) = (gg') \cdot a$

(ii) For all $a \in A$, $1 \cdot a = a$

We are particularly interested in the case when A is also a group. Then we have the following result and definition.

Proposition 1.1.2. *Suppose A is a group and $\varphi : G \to \mathrm{Aut}(A)$ is a group homomorphism. Define a map $\cdot : G \times A \to A$ by $g \cdot a = \varphi(g)(a)$. Then $\cdot$ is an action of G on A called the **left action of G on A determined by φ**. In addition, if $a, a' \in A$ and $g \in G$, then*

$$(g \cdot a)(g \cdot a') = g \cdot (aa').$$

Proof. Take $g, g' \in G$ and $a \in A$. Then

$$\begin{aligned} g \cdot (g' \cdot a) &= \varphi(g)(\varphi(g')(a)) \\ &= (\varphi(g) \circ \varphi(g'))(a) \\ &= \varphi(gg')(a) \\ &= (gg') \cdot a \end{aligned}$$

where the third equality follows from the fact that φ is a group homomorphism. Also, since φ is a homomorphism we have that $\varphi(1)$ is the identity element of $\mathrm{Aut}(A)$, i.e. the identity map, Therefore,

$$1 \cdot a = \varphi(1)(a) = a.$$

For the last part, note that since φ is an automorphism,

$$\begin{aligned}(g \cdot a)(g \cdot a') &= \varphi(g)(a)\varphi(g)(a') \\ &= \varphi(g)(aa') \\ &= g \cdot (aa').\end{aligned}$$

□

Returning briefly to the case where H, K are subgroups of G with H normal in G and $H \cap K = \{1\}$, we see that since H is normal, for a fixed $k \in K$ the map

$$\sigma_k : H \to H, \quad h \mapsto khk^{-1}$$

is an automorphism of H. Further, the map

$$\varphi : K \to \mathrm{Aut}(H), \quad k \mapsto \sigma_k$$

is a group homomorphism. Going back to considering arbitrary groups H and K, this suggests the definition included in the following theorem.

Theorem 1.1.3. *Let H and K be groups and $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Let $\cdot$ denote the left action of K on H determined by φ. Denote by $H \rtimes_\varphi K$ the set (H, K) of pairs (h, k) with $h \in H$ and $k \in K$ along with the multiplication*

$$(h, k)(h', k') = (h(k \cdot h'), kk').$$

(i) $H \rtimes_\varphi K$ is a group called the ***semidirect product*** *of H and K with respect to φ.*

(ii) The subgroups

$$\widetilde{H} = \{(h, 1) : h \in H\} \quad \text{and} \quad \widetilde{K} = \{(1, k) : k \in K\}$$

are isomorphic to the groups H and K respectively, via the isomorphisms $h \mapsto \tilde{h}$ and $k \mapsto \tilde{k}$, where for $h \in H$ and $k \in K$ we define $\tilde{h} = (h, 1)$ and $\tilde{k} = (1, k)$.

(iii) $\widetilde{H}$ is a normal subgroup of $H \rtimes_\varphi K$, and $H \rtimes_\varphi K = \widetilde{H}\widetilde{K}$.

Proof. (i) By Proposition 1.1.2, $k \cdot h' \in H$ and thus $h(k \cdot h') \in H$. Also $kk' \in K$. Therefore, $H \rtimes_\varphi K$ is closed under the multiplication defined above.

For associativity, note that if $a, b, c \in H$ and $x, y, z \in K$, then we can use Proposition 1.1.2 to obtain:

$$\begin{aligned}
((a,x)(b,y))(c,z) &= (a(x\cdot b), xy)(c,z) \\
&= (a(x\cdot b)((xy)\cdot c), xyz) \\
&= (a(x\cdot b)(x\cdot (y\cdot c)), xyz) \\
&= (a(x\cdot (b(y\cdot c))), x(yz)) \\
&= (a,x)(b(y\cdot c), yz) \\
&= (a,x)((b,y)(c,z)).
\end{aligned}$$

To see that $(1,1)$ is the identity element of $H \rtimes_\varphi K$, note that $\varphi(k)(1) = 1$ since $\varphi(k)$ is an automorphism on H, and if $h \in H$ and $k \in K$,

$$\begin{aligned}
(h,k)(1,1) &= (h(k\cdot 1), k) \\
&= (h\varphi(k)(1), k) \\
&= (h,k) \\
&= (1(1\cdot h), k) \\
&= (1,1)(h,k).
\end{aligned}$$

Finally, we show that $(k^{-1}\cdot h^{-1}, k^{-1})$ is the inverse of (h,k):

$$\begin{aligned}
(h,k)(k^{-1}\cdot h^{-1}, k^{-1}) &= (h(k\cdot (k^{-1}\cdot h^{-1})), kk^{-1}) \\
&= (h((kk^{-1})\cdot h^{-1}), 1) \\
&= (h(1\cdot h^{-1}), 1) \\
&= (hh^{-1}, 1) \\
&= (1,1)
\end{aligned}$$

and

$$\begin{aligned}
(k^{-1}\cdot h^{-1}, k^{-1})(h,k) &= ((k^{-1}\cdot h^{-1})(k^{-1}\cdot h), kk^{-1}) \\
&= (k^{-1}\cdot (hh^{-1}), 1) \\
&= (k^{-1}\cdot 1, 1) \\
&= (1,1).
\end{aligned}$$

(ii) It suffices to note the following: For $a, b \in H$ we have

$$\tilde{a}\tilde{b} = (a,1)(b,1) = (a(1\cdot b), 1) = (ab, 1) = \widetilde{ab}$$

and for $x, y \in K$ we have

$$\tilde{x}\tilde{y} = (1, x)(1, y) = (1(x \cdot 1), xy) = (1, xy) = \widetilde{xy}.$$

(iii) To see that $H \rtimes_\varphi K = \widetilde{H}\widetilde{K}$, note that for any (h, k),

$$(h, k) = (h(1 \cdot 1), 1k) = (h, 1)(1, k).$$

Now, recall that the *normalizer* of $\widetilde{H}$ in $H \rtimes_\varphi K$ is the largest subgroup $N(\widetilde{H})$ of $H \rtimes_\varphi K$ such that $\widetilde{H}$ is normal in $N(\widetilde{H})$, i.e. $N(\widetilde{H}) = \{g : g\widetilde{H}g^{-1} = \widetilde{H}\}$. Note that for $h \in H$ and $k \in K$, we have

$$\begin{aligned}
\tilde{k}\tilde{h}\tilde{k}^{-1} &= (1, k)(h, 1)(1, k^{-1}) \\
&= (1(k \cdot h), k)(1, k^{-1}) \\
&= ((k \cdot h)(k \cdot 1), kk^{-1}) \\
&= (k \cdot h, 1) = \widetilde{k \cdot h} \in \widetilde{H}.
\end{aligned}$$

Thus, $\widetilde{K} \subseteq N(\widetilde{H})$. Now certainly $\widetilde{H} \subseteq N(\widetilde{H})$ and since $N(\widetilde{H})$ is a subgroup, we have $H \rtimes_\varphi K = HK \subseteq N(\widetilde{H})$. Thus $H \rtimes_\varphi K$ is the normalizer of $\widetilde{H}$ and therefore $\widetilde{H}$ is a normal subgroup.

□

From now on, we will simply identify H, K with their isomorphic copies $\widetilde{H}, \widetilde{K}$ in the semidirect product. When there is no risk of confusion, we will write $H \rtimes K$ for a semidirect product of H and K. Note, however, that we can have different semidirect products of H and K by choosing different homomorphisms

$$\varphi : K \to \mathrm{Aut}(H).$$

This is best illustrated by the following example.

Example 1.1.4. Let H be any abelian group and $\mathbb{Z}/2\mathbb{Z} = \langle x : x^2 = 1 \rangle$ be the group of order 2. Since H is abelian, the map $\sigma : H \to H$, $\sigma(h) = h^{-1}$ is an automorphism of H. Moreover, the map

$$\varphi_1 : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(H),\ x \mapsto \sigma$$

is a homomorphism, since σ is its own inverse. Also, let φ_2 be the trivial map $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(H)$ which maps everything in $\mathbb{Z}/2\mathbb{Z}$ to the identity map on H. Then, we can define the semidirect products $H \rtimes_{\varphi_1} \mathbb{Z}/2\mathbb{Z}$ and $H \rtimes_{\varphi_2} \mathbb{Z}/2\mathbb{Z}$. In general, they are not isomorphic. For instance, when H is cyclic of order $n > 2$, the semidirect product $H \rtimes_{\varphi_1} \mathbb{Z}/2\mathbb{Z}$ is isomorphic to the dihedral group D_{2n}, which is not abelian, while $H \rtimes_{\varphi_2} \mathbb{Z}/2\mathbb{Z}$ is abelian.

In the example above, we saw a special case of the so-called *direct product* of groups. The direct product of two groups H, K is the special case of the semidirect product, when the homomorphism $\varphi : K \to \mathrm{Aut}(H)$ is trivial (i.e. when K *acts trivially* on H). There are three equivalent definitions of the direct product as the next theorem shows.

Theorem 1.1.5. *Let H and K be groups and $\varphi : K \to \mathrm{Aut}(H)$ a homomorphism. Then the following three conditions are equivalent.*

(i) The homomorphism $\varphi : K \to \mathrm{Aut}(H)$ is trivial.

(ii) K is a normal subgroup of $H \rtimes K$ (here, K is identified with what we denoted as $\widetilde{K}$ in theorem 1.1.3).

(iii) The operation on $H \rtimes K$ is given with $(h,k)(h',k') = (hh',kk')$.

Proof. We begin by showing the equivalence of (i) and (ii) and then we prove the equivalence of (i) and (iii).

Suppose (i) holds. As we saw in the proof of Theorem 1.1.3(iii), we have (with the identifications $H = \widetilde{H}$, $K = \widetilde{K}$, $h = \tilde{h}$ and $k = \tilde{k}$) $k \cdot h = khk^{-1}$ for $k \in K$, $h \in H$. Since the action of K on H is trivial, $k \cdot h = h$, and thus $h = khk^{-1}$, so $hkh^{-1} = k \in K$. Therefore, since $H \rtimes K = HK$, we have $K \lhd H \rtimes K$, which gives (ii).

Now suppose (ii) holds and let h, k be elements of H, K respectively. Since $H \lhd H \rtimes K$, we have $kh^{-1}k^{-1} \in H$ and since $K \lhd H \rtimes K$, we have $hkh^{-1} \in K$. Therefore, the commutator $[h,k] = hkh^{-1}k^{-1} \in H \cap K = \{1\}$ is trivial, i.e. $k \cdot h = khk^{-1} = h$. This means that the action of K on H is trivial, i.e. the homomorphism φ is trivial.

Now if (iii) holds, $hh' = h(k \cdot h')$, i.e. $k \cdot h' = h'$ for all $k \in K$ and $h' \in H$. Thus the action of K on H is trivial, yielding (i). Reversing this argument gives that (i) implies (iii). $\square$

To emphasize, we state the following definition.

Definition 1.1.6. A semidirect product $H \rtimes K$ satisfying the three equivalent conditions of Theorem 1.1.5 is called the *direct product* of H and K and is denoted $H \times K$.

To identify when a group G (has a subgroup which) is isomorphic to a semidirect product of two groups, we can use the following theorem.

Theorem 1.1.7. *Let G be a group with a normal subgroup H and another subgroup K such that $H \cap K = \{1\}$. Let $\varphi : K \to \mathrm{Aut}(H)$ be the homomorphism which is obtained by mapping k to the automorphism $h \mapsto khk^{-1}$ of H. Then $HK \cong H \rtimes K$. Further, if K is also normal in G, we have $HK \cong H \times K$.*

Proof. The first part follows from the calculations in the beginning of this section, and the proof of Theorem 1.1.3(iii).

The second part follows from the first and Theorem 1.1.5. □

Definition 1.1.8. Let H be a subgroup of a group G. A subgroup K of G is called a *complement* for H if $G = HK$ and $H \cap K = \{1\}$.

With this terminology, Theorem 1.1.7 gives that to show that a given group G is a semidirect product of some subgroups, it suffices to find a normal subgroup H which has a complement K in G. Section 1.3 will partially answer the question about when a given normal subgroup of a group, has a complement in the given group.

1.2. Nilpotent Groups

An interesting class of groups that lies strictly between abelian and solvable groups is the class of nilpotent groups:

Definition 1.2.1. For a group G, we define a sequence, called the *upper central series* of G, of normal subgroups

$$Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots ,$$

in the following way:

$$Z_0(G) = \{1\}, \quad Z_1(G) = Z(G)$$

and if $Z_i(G)$ has been defined, we define

$$Z_{i+1}(G) = \pi^{-1}(Z(G/Z_i(G))$$

where $\pi : G \to G/Z_i(G)$ is the canonical projection. This means that

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

If there exists an integer n such that $G = Z_n(G)$, then we say that G is *nilpotent*.

Remark 1.2.2. It is not obvious that $Z_i(G)$ is normal in G for all G, so that needs to be proved:

Proof. We use induction on i. For $i = 0, 1$ it is clear. Suppose $Z_i(G) \lhd G$. Then since

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)),$$

we have that $Z_{i+1}(G)/Z_i(G) \lhd G/Z_i(G)$, and by the fourth isomorphism theorem (cf. Theorem A.1.4(v) in Appendix A.1), $Z_{i+1}(G) \lhd G$. $\square$

We immediately note an equivalent definition of nilpotence, via *central series*:

Definition 1.2.3. Let G be a group. A normal series

$$G = K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_0 = \{1\}$$

(i.e. such that K_i is a normal subgroup of G for all i) is called a *central series* of G if K_{i+1}/K_i is contained in the center of G/K_i for $i = 0, \ldots, n-1$.

Proposition 1.2.4. *A group G is nilpotent if and only if it possesses a central series.*

Proof. Clearly, if G is nilpotent then since $G = Z_n(G)$ for some integer n, we can let $K_i = Z_i(G)$ for $i = 0, \ldots, n$ to obtain a central series of G.

For the other direction, suppose G has a central series

$$G = K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_0 = \{1\}.$$

We will show that $K_i \subseteq Z_i(G)$ for all i. This will imply that $G \subseteq Z_n(G)$, i.e. that the upper central series of G terminates, which is the definition of nilpotence of G. We use induction on i It is clear that $K_0 \subseteq Z_0(G)$. Now suppose $K_i \subseteq Z_i(G)$ for some i. We want to show that $K_{i+1} \subseteq Z_{i+1}(G)$. We have $K_{i+1}/K_i \subseteq Z(G/K_i)$. Define the subgroup H of G such that $Z(G/K_i) = H/K_i$; then $K_{i+1} \subseteq H$. We will show that $H \subseteq Z_{i+1}(G)$. Now take $h \in H$. Then $hK_i \in H/K_i = Z(G/K_i)$ and thus for all $g \in G$, we have $ghK_i = hgK_i$, i.e.

$$hgh^{-1}g^{-1} \in K_i \subseteq Z_i(G).$$

Thus $ghZ_i(G) = hgZ_i(G)$ for all $g \in G$ and thus

$$hZ_i(G) \in Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G),$$

hence $h \in Z_{i+1}(G)$, and we are done. □

Lemma 1.2.5. *If G is nilpotent, then every subgroup and quotient of G is nilpotent.*

Proof. Let H be a subgroup of G and

$$G = K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_0 = \{1\}$$

a central series of G. Then we claim that

$$H = H \cap K_n \supseteq H \cap K_{n-1} \supseteq \cdots \supseteq H \cap K_0 = \{1\}$$

is a central series of H. It is clearly a normal series. Now, let i be given and $\varphi : H/(H \cap K_i) \to HK_i/K_i$ be the natural isomorphism (given by $h(H \cap K_i) \mapsto hK_i$). Since $H \cap K_i \subseteq K_i \subseteq K_{i+1}$, we have

$$\varphi((H \cap K_{i+1})/(H \cap K_i)) = H(H \cap K_{i+1})/K_i \subseteq K_{i+1}/K_i \subseteq Z(G/K_i)$$

and thus

$$\begin{aligned}
\varphi((H \cap K_{i+1})/(H \cap K_i)) &\subseteq (HK_i/K_i) \cap Z(G/K_i) \\
&\subseteq Z(HK_i/K_i) \\
&= Z(\varphi(H/(H \cap K_i))) \\
&= \varphi(Z(H/(H \cap K_i)))
\end{aligned}$$

since the isomorphism φ preserves the center. Since φ is an isomorphism, we see that

$$(H \cap K_{i+1})/(H \cap K_i) \subseteq Z(H/(H \cap K_i)),$$

as desired.

To show that every quotient of G is nilpotent, it suffices to show that every homomorphic image of G is nilpotent. So let φ be a homomorphism from G to some group; we want to show that $\varphi(G)$ is nilpotent. Let a central series of G,

$$G = K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_0 = \{1\},$$

be given as before. We want to show that

$$\varphi(G) = \varphi(K_n) \supseteq \varphi(K_{n-1}) \supseteq \cdots \supseteq \varphi(K_0) = \{1\},$$

is a central series for $\varphi(G)$, i.e. that it is a normal series and, given i, we have $\varphi(K_{i+1})/\varphi(K_i) \subseteq Z(\varphi(G)/\varphi(K_i))$. It is clear that $\varphi(K_i) \lhd \varphi(G)$ since

$$\varphi(g)\varphi(K_i)\varphi(g)^{-1} \subseteq \varphi(gK_ig^{-1}) \subseteq \varphi(K_i)$$

(because K_i is normal in G). Now take some $\varphi(k)\varphi(K_i) \in \varphi(K_{i+1})/\varphi(K_i)$ where $k \in K_{i+1}$. We want to show that if $g \in G$, then $\varphi(g)\varphi(k)\varphi(K_i) = \varphi(k)\varphi(g)\varphi(K_i)$. Now, since $gkK_i = kgK_i$ for all $g \in G$, and φ is a homomorphism, this is clear. Thus we have

$$\varphi(K_{i+1})/\varphi(K_i) \subseteq Z(\varphi(G)/\varphi(K_i)).$$

□

Lemma 1.2.6. *If G is a non-trivial p-group, then the center $Z(G)$ is non-trivial.*

Proof. We have the class equation,

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|,$$

where $g_1, \ldots, g_r$ are representatives for the distinct conjugacy classes that lie outside the center (see Appendix A.2). Since $g_i \notin Z(G)$, we have that the centralizer $C_G(g_i)$ is not all of G, hence p divides $|G : C_G(g_i)|$. Since G is non-trivial, p also divides $|G|$, and then the equation gives that p divides $|Z(G)|$. In particular, $|Z(G)| > 1$. □

Definition 1.2.7. A *characteristic subgroup* of a group G is a subgroup H such that $\alpha(H) \subseteq H$ for all $\alpha \in \mathrm{Aut}(G)$. In other words, a subgroup of G is characteristic if it is invariant under all automorphisms of G.

Remark 1.2.8. All characteristic subgroups are normal subgroups, since normal subgroups are those subgroups which are invariant under all *inner* automorphisms of G.

Remark 1.2.9. If H is a characteristic subgroup of G, and α is an automorphism of G, then $\alpha(H) = H$. To see that, note that α^{-1} is an automorphism of G, so $\alpha^{-1}(H) \subseteq H$ and hence

$$H = \alpha(\alpha^{-1}(H)) \subseteq \alpha(H).$$

Lemma 1.2.10. *Let A, B, C be groups such that A is a characteristic subgroup of B, which in turn is a normal subgroup of C. Then A is a normal subgroup of C.*

Proof. For any $c \in C$, the map $b \mapsto cbc^{-1}$ is an automorphism of B (since B is normal in C. Thus A is invariant under this map, implying that $cAc^{-1} = A$ for all $c \in C$. But that means precisely that A is normal in C. □

Lemma 1.2.11. *Let P be a Sylow p-subgroup of G. Then the following are equivalent:*

(i) P is the unique Sylow p-subgroup of G;

(ii) P is normal in G;

(iii) P is characteristic in G.

Proof. Suppose (i) holds. Since for all $g \in G$, gPg^{-1} is a Sylow p-subgroup of G, we have $gPg^{-1} = P$ for all $g \in G$ and hence $P \lhd G$, i.e. (ii). Suppose (ii) holds. Then, take any Sylow p-subgroup Q of G and note that by Sylow's theorem (cf. Appendix A.3, Theorem A.3.2(ii)) there exists $g \in G$ such that $Q = gPg^{-1} = P$, since $P \lhd G$. This gives (i).

Suppose (ii) holds. By the above argument, P is the unique Sylow p-subgroup of G. Take an automorphism α of G. Then $\alpha(P)$ is a Sylow p-subgroup of G and hence $\alpha(P) = P$, so P is characteristic in G, yielding (iii).

Finally, (iii) obviously implies (ii). □

Now we can prove the following theorem, which gives convenient characterizations of *finite* nilpotent groups.

Theorem 1.2.12. *Let G be a finite group and let $p_1, \ldots, p_s$ be the distinct prime divisors of $|G|$. Let P_i be a Sylow p_i-subgroup of G for $i = 1, \ldots, s$. Then the following conditions are equivalent:*

(i) G is nilpotent,

(ii) if H is a proper subgroup of G, then H is a proper subgroup of $N_G(H)$, its normalizer in G,

(iii) $P_i \lhd G$ *for* $i = 1, \ldots, s$*,*

(iv) $G \cong P_1 \times \cdots \times P_s$*,*

(v) G *has a normal subgroup of order* d *for every divisor* d *of* $|G|$*.*

Proof. We will first show $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$ establishing equivalence of the first four statements, and then we will show that (v) is equivalent to them as well.

1. $(i) \Rightarrow (ii)$: We use induction on $|G|$. The statement is vacuously true if G is trivial, settling the base case. Since G is nilpotent, its center is non-trivial. Clearly, $H \lhd \langle H \cup Z(G) \rangle$ (since $zhz^{-1} = h$ for all $z \in Z(G), h \in H$), and if $Z(G) \nsubseteq H$ then H is properly contained in $\langle H \cup Z(G) \rangle$, which we just saw is contained in the normalizer $N_G(H)$.

   Now, if $Z(G) \subseteq H$, then by the inductive hypothesis we have that $H/Z(G)$ is properly contained in its normalizer in $G/Z(G)$ (since $G/Z(G)$ is nilpotent by Lemma 1.2.5). By the third isomorphism theorem (cf. Theorem A.1.3 in Appendix A.1) we have that $H/Z(G) \lhd N_G(H)/Z(G)$ and

   $$N_G(H)/H \cong \frac{N_G(H)/Z(G)}{H/Z(G)} \supseteq \frac{N_{G/Z(G)}(H/Z(G))}{H/Z(G)},$$

   so $N_G(H)/H$ is non-trivial, as desired. Here, we used that

   $$N_G(H)/Z(G) \supseteq N_{G/Z(G)}(H/Z(G)),$$

   which needs to be proved. Write $N_{G/Z(G)}(H/Z(G)) = M/Z(G)$. Then it suffices to prove that $H \lhd M$, but that is clear from the fourth isomorphism, (cf. part (v) of Theorem A.1.4 in Appendix A.1), since $H/Z(G) \lhd M/Z(G)$.

2. $(ii) \Rightarrow (iii)$: Let some i be given and denote P_i by P and p_i by p. Since $N_G(P) \subseteq G$, we have that P is a normal Sylow p-subgroup of $N_G(P)$ and thus by Lemma 1.2.11 we have that P is characteristic in $N_G(P)$. By Lemma 1.2.10 we then have that $P \lhd N_G(N_G(P))$. Therefore, $N_G(N_G(P)) \subseteq N_G(P)$ so $N_G(P)$ is its own normalizer and thus since (ii) holds we have that $N_G(P) = G$, which means that $P \lhd G$.

3. $(iii) \Rightarrow (iv)$: We will show by induction on r that

   $$P_1 P_2 \cdots P_r \cong P_1 \times P_2 \times \cdots \times P_r.$$

The base case is obvious. Since $P_i \lhd G$ by (iii) for all i we have that $P_1 P_2 \cdots P_{r-1} \cdot P_r$ is a subgroup of G. Now the orders of $P_1 \cdots P_{r-1}$ and P_r are relatively prime and hence their intersection is trivial. Therefore, by Theorem 1.1.7 we have that $P_1 \cdots P_r \cong P_1 \cdots P_{r-1} \times P_r$, and by the inductive hypothesis, $P_1 \cdots P_{r-1} \cong P_1 \times \cdots \times P_{r-1}$, so we are done.

4. $(iv) \Rightarrow (i)$: We will use induction on $|G|$. Since both (i) and (iv) hold for the trivial group, the base case is clear. Now, it is easy to see that

$$Z(P_1 \times \cdots \times P_s) = Z(P_1) \times \cdots \times Z(P_s)$$

and

$$G/Z(G) = (P_1/Z(P_1)) \times \cdots \times (P_s/Z(P_s)). \qquad (*)$$

Since G is non-trivial, some P_i is non-trivial and hence $Z(P_i)$ is non-trivial by Lemma 1.2.6. Thus, $G/Z(G)$ is smaller than G and satisfies (iv) by $(*)$. Therefore, $G/Z(G)$ is nilpotent by the inductive hypothesis. Thus, there exists n such that $Z_n(G/Z(G)) = G/Z(G)$ where $(Z_i(G/Z(G)))_{i \geq 0}$ denotes the upper central series of $G/Z(G)$. Now, $Z_2(G)/Z(G) = Z(G/Z(G)) = Z_1(G/Z(G))$. We will show by induction on i that

$$Z_i(G)/Z(G) = Z_{i-1}(G/Z(G)).$$

Now, by induction and repeated use of the third isomorphism theorem,

$$\begin{aligned}
Z_{i-1}(G/Z(G))/Z_{i-2}(G/Z(G)) &= Z((G/Z(G))/Z_{i-2}(G/Z(G))) \\
&= Z((G/Z(G))/Z_{i-1}(G)/Z(G)) \\
&\cong Z(G/Z_{i-1}(G)) \\
&= Z_i(G)/Z_{i-1}(G) \\
&\cong (Z_i(G)/Z(G))/(Z_{i-1}(G)/Z(G)) \\
&= (Z_i(G)/Z(G))/Z_{i-2}(G/Z(G)),
\end{aligned}$$

i.e.

$$Z_i(G)/Z(G) = Z_{i-1}(G/Z(G))$$

as desired. Thus,

$$Z_{n+1}(G)/Z(G) = Z_n(G/Z(G)) = G/Z(G),$$

i.e. $Z_{n+1}(G) = G$, so G is nilpotent.

5. Suppose G is nilpotent, i.e. that $(i) - (iv)$ hold. We will use induction on $|G|$ to show that (v) holds. If G is trivial, then the statement that G has a

normal subgroup of any order dividing $|G|$ is of course true. Suppose G is non-trivial. Since G is nilpotent, it has non-trivial center. Let d be a divisor of $|G|$ and take some prime p dividing $|Z(G)|$. Then there exists an element $g \in Z(G)$ of order p. Since $N = \langle g \rangle \subseteq Z(G)$, we have that $N \lhd G$. The group G/N then has a subgroup of any given order dividing $|G|/|N| = |G|/p$. If p divides d, then G/N has a subgroup H/N of order d/p, so H is a subgroup of G of order d. So suppose p does not divide d. Then d divides $|G/N|$ and thus G/N has a subgroup H/N of order d; H is then a subgroup of G of order pd. Now, if H is a proper subgroup of G then we are done, since then H has a subgroup of order d, which is also a subgroup of G. Finally, assume $H = G$. Then G has order dp with d, p relatively prime. We can assume $p = p_s$. Since all Sylow subgroups of G are normal, then we have that $P_1 \cdots P_{s-1}$ is normal in G, of order d, and we are done.

6. $(v) \Rightarrow (iii)$: Take the highest power of p_i dividing $|G|$ to obtain a Sylow p_i-subgroup of G which is normal in G.

□

1.3. Wreath Products and a Theorem of Schur

What follows in this section is mainly based on the text of Kargapolov and Merzljakov [7], but Keith Conrad's notes [2] were also helpful. The aim is to prove the following theorem of Schur

Theorem 1.3.1. *(Schur) Let G be a finite group and $H \lhd G$. If $|H|$ and $|G/H|$ are relatively prime, then H has a complement in G.*

We begin with a few definitions.

Definition 1.3.2. Let A and B be groups. Then the set $A^{[B]}$ of all maps $B \to A$ forms a group with the operation defined as follows: for $f, g \in A^{[B]}$, we define $fg : B \to A$ with $(fg)(b) = f(b)g(b)$ for all $b \in B$.

We should check that the operation defined above on $A^{[B]}$ satisfies the group axioms. Indeed, associativity follows directly from associativity of the operation of A, the identity element is the trivial map which maps every element of B to the identity 1 of A. Finally, the multiplicative inverse of $f : B \to A$ is the map $g : B \to A$, $g(x) = (f(x))^{-1}$.

For each $f \in A^{[B]}$, we can define another map $f^b : B \to A$ by setting

$$f^b(x) = f(b^{-1}x)$$

for all $x \in B$.

Proposition 1.3.3. *The map* $\hat{b} : A^{[B]} \to A^{[B]}$, $f \mapsto f^b$, *is an automorphism. Moreover, the map* $B \to \mathrm{Aut}(A^{[B]})$, $b \mapsto \hat{b}$, *is a homomorphism.*

Proof. Note that $\hat{b}$ is an endomorphism, since for all $x \in B$ and $f, g \in A^{[B]}$, we have

$$\hat{b}(fg)(x) = (fg)(b^{-1}x) = f(b^{-1}x)g(b^{-1}x) = \hat{b}(f)(x)\hat{b}(g)(x).$$

Further, the inverse of $\hat{b}$ is clearly $\widehat{b^{-1}}$, and thus $\hat{b}$ is an automorphism.

To see that $b \mapsto \hat{b}$ is a group homomorphism, note that for all $b_1, b_2, x \in B$ and $f \in A^{[B]}$,

$$\begin{aligned}
\widehat{b_1 b_2}(f)(x) &= f^{b_1 b_2}(x) \\
&= f((b_1 b_2)^{-1}x) \\
&= f(b_2^{-1} b_1^{-1} x) \\
&= f^{b_2}(b_1^{-1}x) \\
&= (f^{b_2})^{b_1}(x) \\
&= \widehat{b_1}(f^{b_2})(x) \\
&= (\widehat{b_1} \circ \widehat{b_2})(f)(x),
\end{aligned}$$

so we have $\widehat{b_1 b_2} = \widehat{b_1} \circ \widehat{b_2}$ □

Now we can use the homomorphism φ from Proposition 1.3.3 to define a semidirect product of $A^{[B]}$ and B, called the wreath product of A and B.

Definition 1.3.4. Let A and B be groups and let $\varphi : B \to \mathrm{Aut}(A^{[B]})$ be the homomorphism defined by $\varphi(b) = \hat{b}$. Then the semidirect product $A^{[B]} \rtimes_\varphi B$ is called the *wreath product* of A and B and is denoted $A \text{ Wr } B$.

Let us now see how the multiplication in a wreath product behaves. Let two elements $(f_1, b_1), (f_2, b_2) \in A$ Wr B be given. Recall that f_1, f_2 are maps $A \to B$. The action of the element b_1 on f_2 is given with

$$b_1 \cdot f_2 = \varphi(b_1)(f_2) = \hat{b_1}(f_2) = f_2^{b_1},$$

i.e. $f_2^{b_1}$ is the map

$$x \mapsto f_2(b_1^{-1}x), x \in B.$$

So we have

$$(f_1, b_1)(f_2, b_2) = (f_1(b_1 \cdot f_2), b_1 b_2) = (f_1 f_2^{b_1}, b_1 b_2)$$

Definition 1.3.5. We say that a group G is an *extension of* A *by* B if A is a normal subgroup of G and $B = G/A$.

Definition 1.3.6. An *embedding* of a group G *into* another group Γ is an injective homomorphism $\varphi : G \to \Gamma$. If an embedding $G \to \Gamma$ exists, we say that G can be *embedded* in Γ.

Now we are ready for a lemma, crucial to proving Schur's theorem (1.3.1).

Theorem 1.3.7. *(Kaluznin-Krasner) Every extension of a group A by a group B can be embedded in the wreath product $W = A$ Wr B.*

Proof. Let G be an extension of A by B, i.e. $A \lhd G$ and $B = G/A$. Define a *transversal* $\tau : B \to G$, i.e. a map which takes every element xA of $B = G/A$ to an element $\tau(xA) \in xA$. For every g in G, define a map $f_g : B \to A$ by

$$f_g(xA) = (\tau(xA))^{-1} g \tau(g^{-1}xA).$$

We need to show that f_g indeed maps B into A. But since $\tau(xA) = xa_1$ for some $a_1 \in A$, and $\tau(g^{-1}xA) = a_2$ for some $a_2 \in G$, we have

$$f_g(xA) = (xa_1)^{-1} g(g^{-1}xa_2) = a_1^{-1}a_2 \in A,$$

that fact is clear.

Note that if $g, h \in G$ and $xA \in B$, then

$$\begin{aligned}(f_g f_h^{gA})(xA) &= f_g(xA) f_h(g^{-1}xA)\\ &= (\tau(xA))^{-1} g\tau(g^{-1}xA)(\tau(g^{-1}xA))^{-1} h\tau(h^{-1}g^{-1}xA)\\ &= (\tau(xA))^{-1} gh\tau((gh)^{-1}xA)\\ &= f_{gh}(xA).\end{aligned}$$

This fact enables us to define the homomorphism

$$\psi : G \to W = A \text{ Wr } B,\ \psi(g) = (f_g, gA).$$

To see that it is a homomorphism, note that

$$\begin{aligned}\psi(g)\psi(h) &= (f_g, gA)(f_h, hA)\\ &= (f_g f_h^{gA}, ghA)\\ &= (f_{gh}, ghA)\\ &= \psi(gh).\end{aligned}$$

Finally, we conclude the proof by showing that ψ is injective. Take $g \in \operatorname{Ker}\psi$. Then (f_g, gA) is the identity element of W, i.e. f_g is the trivial map and $gA = A$. Therefore, $g \in A$ and $f_g(xA) = 1$ for all $xA \in B$, i.e.

$$(\tau(xA))^{-1} g\tau(xA) = 1$$

for all $x \in B$, which implies $g = 1$. Thus $\operatorname{Ker}\psi = \{1\}$, i.e. ψ is injective and hence an embedding of G into W. $\square$

Let ψ be the embedding from Theorem 1.3.7 and $W = A \text{ Wr } B$. Then it is easy to see that $W = A^{[B]}\psi(G)$: We want to write any element (f, xA) as

$$(f', A)\psi(g) = (f', A)(f_g, gA) = (f' f_g^A, gA) = (f' f_g, gA)$$

for some $g \in G$ (here, we have, as usual, identified $A^{[B]}$ with the group which was denoted $\widetilde{A^{[B]}}$ in theorem 1.1.3). But that is easy, take $g = x$ and $f' = f f_x^{-1}$.

Moreover, we have that $\psi(G) \cap A^{[B]} \cong A$. To see that, note that elements in $\psi(G)$ have the form (f_g, gA) for $g \in G$, and elements in $A^{[B]}$ have the form (f, A) where $f : B \to A$ is a map. Therefore, the elements of the intersection have the form (f_a, A) where $a \in A$. Now the desired isomorphism $\psi(G) \cap A^{[B]} \to A$ is given by $(f_a, A) \mapsto a$. It is clearly bijective, and to see that it is operation-preserving, note that $(f_{a_1}, A)(f_{a_2}, A) = (f_{a_1 a_2}, A)$, since $a_1, a_2 \in A$.

Lastly, for proving Schur's theorem, we need a lemma which is proved using representation theory, in particular Maschke's theorem (see Appendix A.4).

Lemma 1.3.8. *Let H be a normal elementary abelian p-subgroup of a group G, i.e. $H \cong (\mathbb{Z}/p\mathbb{Z})^n$ for some $n \in \mathbb{N}$, where p is a prime. Suppose further that p does not divide $|G : H|$. If K is a normal subgroup of G contained in H, then there exists a normal subgroup L of G such that $H = K \times L$*

Proof. We define a vector space structure on H over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and an action of G on H making H into an $\mathbb{F}_p(G/H)$-module. Define addition of $h_1, h_2 \in H$ by $h_1 + h_2 = h_1 h_2$ and multiplication by a scalar $\lambda \in \{0, 1, \ldots p-1\}$ as $\lambda h = h^\lambda$. With this notation, it is clear that the action of G/H on H by conjugation, i.e. $(gH) \cdot h = ghg^{-1}$ for all $g \in G$, $h \in H$, satisfies the properties of the definition of an FG-module (cf. Appendix A.4). This action is well defined, since if $g_1 H = g_2 H$, and $h \in H$, there exists $h_0 \in H$ such that $g_1 = g_2 h_0$, and $g_1 h g_1^{-1} = g_2 h_0 h h_0^{-1} g_2^{-1} = g_2 h g_2^{-1}$, since H is abelian. Since p does not divide $|G/H|$, Maschke's theorem (A.4.3) is applicable here. The action of G/H on H was defined as conjugation, and hence the submodules of H as an $\mathbb{F}_p(G/H)$-module are exactly the subgroups of H which are normal in G. So let K be a subgroup of H which is normal in G, i.e. an $\mathbb{F}_p(G/H)$-submodule of H. Then Maschke's theorem gives that there exists a submodule L of H, i.e. a normal subgroup L of G contained in H, such that $H = K \oplus L = K \times L$. $\square$

Now we are ready to prove the main theorem. We state it again:

Theorem 1.3.9. *(Schur) Let G be a finite group and $A \lhd G$. If $|A|$ and $|G/A|$ are relatively prime, then A has a complement in G.*

Proof. We divide the proof into two parts, 1 and 2. In part 1, we will settle the case where A is elementary abelian, and then in part 2 we will reduce the general case to the case of part 1 by induction.

1. Suppose A is an elementary abelian p-group and let $B = G/A$. By the Kaluznin-Krasner Theorem (1.3.7), we can embed G in the wreath product $W = A \text{ Wr } B$. Identify G with its isomorphic copy inside W and recall that
$$W = A^{[B]}G.$$
We also had $A \cong G \cap A^{[B]}$ and we make the identification
$$A = G \cap A^{[B]}.$$
Now A, B are finite and $A^{[B]}$ is just the direct product of A with itself $|B|$ times. Therefore, $A^{[B]}$ is an elementary abelian p-group as well. Since A is normal in both $A^{[B]}$ and G, we have that A is normal in $W = A^{[B]}G$. Thus by Lemma 1.3.8 we have a normal subgroup C of W such that $A^{[B]} = A \times C$. Now, since $G \cap A^{[B]} = A$ and $W = A^{[B]}G$, we have $W = CG$. Further, by the second isomorphism theorem (see Appendix A.1),
$$W/C = CG/C \cong G/(C \cap G) \cong G.$$

Moreover, we have $B \cap C \subseteq B \cap A^{[B]} = \{1\}$, so by the second isomorphism theorem again,

$$CB/C \cong B/B \cap C \cong B,$$

but BC/C is a subgroup of W/C and so B is (isomorphic to) a subgroup of G, concluding this case.

2. For the general case, we proceed by induction on $|G|$. Suppose G is a minimal counterexample, i.e. that the theorem is true of all proper subgroups and quotients of G, but not of G. To obtain a contradiction, it suffices to show that G has a subgroup of order $|B| = |G : A|$, since subgroups of relatively prime orders have trivial intersection and thus, since A is a normal subgroup of G, their product is the whole group G. Let p be a prime divisor of $|A|$ and P a Sylow p-subgroup of A. Since A and $|G : A|$ are relatively prime, p does not divide $|G : A|$ and thus P is a Sylow p-subgroup of G. Since $A \lhd G$, all conjugates of P are contained in A and therefore, by Sylow's theorem (A.3.2), all Sylow p-subgroups of G are contained in A. Further, the number of Sylow p-subgroups of A is equal to the number of Sylow p-subgroups of G, so by Sylow's theorem, we have

$$|G : N_G(P)| = |A : N_A(P)|.$$

Clearly, we have $N_A(P) = A \cap N_G(P)$. Thus we have

$$|G : N_G(P)| = |A : A \cap N_G(P)|,$$

i.e.

$$|G|/|N_G(P)| = |A|/|A \cap N_G(P)|,$$

i.e.

$$|G : A| = |N_G(P) : A \cap N_G(P)| \tag{1.1}$$

Now, suppose P is not normal in G, i.e. $N_G(P) \neq G$. Since $A \cap N_G(P)$ is a normal subgroup of $N_G(P)$, and its order is relatively prime to its index in $N_G(P)$ by equation 1.1, the group $N_G(P)$ along with the subgroup $A \cap N_G(P)$ satisfies the conditions of the theorem. Thus $N_G(P)$ has a subgroup of order $|G : A|$, which is then also a subgroup of G, so we have our contradiction.

Assume P is normal in G. Then by the third isomorphism theorem, the group A/P is normal in G/P and $(G/P)/(A/P) \cong G/A$; in particular, $|G/P : A/P| = |G : A|$. Thus the theorem is true for the group G/P along with the subgroup A/P and hence there exists a subgroup H of G containing P, such that

$$|H : P| = |H/P| = |G : A|. \tag{1.2}$$

In particular, $|H : P|$ is not divisible by p. Since P is a non-trivial p-group, it has non-trivial center Z by Lemma 1.2.6. Clearly, $Z \lhd H$, and so by the third isomorphism theorem we have that $P/Z \lhd H/Z$ and

$$|H/Z : P/Z| = |H : P| = |G : A|$$

by equation 1.2. So P/Z is a p-group while its index in H/Z is not divisible by p. Hence the theorem is true for the groups H/Z and P/Z, so H contains a subgroup K which contains Z, such that $|K/Z| = |H : P| = |G : A|$. Now, $Z \lhd K$, Z is a p-group and

$$|K : Z| = |K/Z| = |G : A|$$

so the group K along with its subgroup Z satisfy the hypotheses of the theorem. If $K \neq G$, we conclude that K, and hence G, has a subgroup of order $|K : Z| = |G : A|$, a contradiction. Hence $K = G$. Thus, since $K \subseteq H$, we have $H = G$ and since $|G : P| = |H : P| = |G : A|$ we conclude that $A = P$.

Now suppose A is non-abelian. Then we can go through the whole argument again replacing P with A and H with G, and obtain a subgroup K/Z of G/Z of order $|G : A|$ (here, again, $Z = Z(P) = Z(A)$). Then $|K| = |Z||G : A|$. Since A is non-abelian, $|Z| < |A|$ and thus $|K| < |G|$, so K is a proper subgroup of G and we have a contradiction as before.

Suppose A is abelian. Consider the subgroup $A_p = \{a \in A : a^p = 1\}$. This is a subgroup of A (necessarily normal, since A is abelian), and we can replace Z in the above paragraph by A_p, so if A_p is a proper subgroup of A, we again have a contradiction.

We conclude that $A_p = A$, i.e. A is an elementary abelian p-group, which was dealt with in part 1 of this proof, and we are done.

□

2. Palindromes and Games

In this chapter, the results of research on palindromes in finite groups is presented (Section 2.1), along with an application where palindromes in groups are used to partially solve the Magnus-Derek game (Section 2.2).

2.1. Civic groups

Definition 2.1.1. We say that a group G is *civic* if any subset P of G satisfying the properties

- $1 \in P$
- $a, b \in P \Rightarrow aba \in P$

is a subgroup of G. We say that a subset P satisfying the above properties is *palindromic* in G.

Definition 2.1.2. Let $G = \langle X \rangle$ be a group. A *palindrome in* X or X*-palindrome* (or simply *palindrome* if there is no confusion about the generating set) is a word in the alphabet $X \cup X^{-1}$ which reads the same from left to right and from right to left. Denote by $l_X(g)$ the smallest natural number k such that g can be written as a product of k palindromes in the alphabet $X \cup X^{-1}$. The number $l_X(g)$ is called the *palindromic length* of g. The *palindromic width* of G with respect to X is denoted by $\mathrm{pw}(G, X)$ and defined as the upper bound of the set of palindromic lengths of the elements of G, i.e.

$$\mathrm{pw}(G, X) = \sup_{g \in G} l_X(g).$$

Finally, when we simply talk about the *palindromic width* of G and use the notation $\mathrm{pw}(G)$, it should be taken to mean the supremum of palindromic widths over all possible generating sets of G, i.e.

$$\mathrm{pw}(G) = \sup\{\mathrm{pw}(G, X) : X \subseteq G \text{ and } G = \langle X \rangle\}.$$

Lemma 2.1.3. *Let G be a finite group and $P \subseteq G$ palindromic. Suppose $a \in P$. Then $a^k \in P$ for all k.*

Proof. The statement is clearly true for $k = 0, 1$. Suppose $k \geq 2$ and $a^m \in G$ for all $m < k$. Then $a^k = a(a^{k-2})a \in P$. Hence by induction, $a^k \in P$ for all k. □

A palindromic subset P of a finite group G like in Defintion 2.1.1 is closed under taking inverses (because of Lemma 2.1.3). To show that a group is civic, it therefore suffices to prove that any such set is closed under the group operation.

Proposition 2.1.4. *A civic group G has palindromic width 1 (with respect to all generating sets).*

Proof. Suppose $G = \langle X \rangle$ is civic. Let $P(X)$ be the set of all X-palindromes in G. Then clearly $P(X)$ is palindromic in G and hence a subgroup. Then since $X \subseteq P(X)$, we have $\langle X \rangle \subseteq P(X)$ and therefore $P(X) = G$. Since the generating set X was chosen arbitrarily, the result is clear. □

Proposition 2.1.5. *If G is civic, then all subgroups and quotients of G are civic.*

Proof. Take a subgroup H of G and a palindromic subset $P \subseteq H$. Then P is a subgroup of G and hence of H.

For quotients, it suffices to show that any homomorphic image of G is civic. Take a homomorphism φ from G to some group. Suppose $P \subseteq \varphi(G)$ is palindromic. Then if $a, b \in \varphi^{-1}(P)$, we have $\varphi(a), \varphi(b) \in P$, and thus $\varphi(aba) = \varphi(a)\varphi(b)\varphi(a) \in P$ which implies $aba \in \varphi^{-1}(P)$. Therefore $\varphi^{-1}(P)$ is palindromic in G and since G is civic, $\varphi^{-1}(P)$ is a subgroup of G; hence $P = \varphi(\varphi^{-1}(P))$ is a subgroup of $\varphi(G)$. □

As the next two lemmas show, all abelian groups of odd order are civic, while in the even order case there is a very small counterexample.

Lemma 2.1.6. *If G is an abelian group of odd order, then G is civic.*

Proof. Let P be a palindromic subset of G. It suffices to show that $a, b \in P$ implies that $ab \in P$. Let $2m - 1 = \mathrm{ord}(b)$. Then $b^m \in P$ by Lemma 2.1.3, and hence

$$ab = ab^{2m} = b^m a b^m \in P.$$

□

Lemma 2.1.7. *The Klein 4-group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not civic.*

Proof. The group has presentation $\langle a, b : a^2 = b^2 = aba^{-1}b^{-1} = 1 \rangle$. It is easy to check that the set $\{1, a, b\}$ is palindromic but not a subgroup. □

Lemma 2.1.8. *If G is a group such that $G/Z(G)$ is cyclic, then G is abelian.*

Proof. Suppose $G/Z(G) = \langle xZ(G) \rangle$ where $x \in G$. Then every element of G can be written in the form $x^r z$ where r is an integer and $z \in Z(G)$. Take two elements $x^r z_1, x^s z_2 \in G$, where $z_1, z_2 \in Z(G)$. Then

$$(x^r z_1)(x^s z_2) = x^{r+s} z_2 z_1 = (x^s z_2)(x^r z_1)$$

so G is abelian. □

Theorem 2.1.9. *If G is a 2-group, then G civic if and only if it is cyclic.*

Proof. Any finite cyclic group is obviously civic.

For the other direction, let G be a minimal counterexample, i.e. a non-cyclic, civic 2-group such that every smaller civic 2-group is cyclic. Since G is a 2-group, it is nilpotent and hence has non-trivial center. By minimality of G, $G/Z(G)$ is cyclic and hence G is abelian by Lemma 2.1.8. Therefore, G is a non-cyclic, abelian 2-group and hence contains a subgroup isomorphic to the Klein 4-group, which is not civic by Lemma 2.1.7, so G is not civic, contradiction. □

To study civic groups further, Theorem 2.1.9 allows us to consider only groups with cyclic Sylow 2-subgroup; if a group has a non-cyclic Sylow 2-subgroup, then said Sylow 2-group is a non-civic subgroup, and by Theorem 2.1.5, the group G must be non-civic itself.

Burnside proved the following (see [1, 10])

Lemma 2.1.10. *Let G be a finite group and p the smallest prime divisor of $|G|$. If G has a cyclic Sylow p-subgroup H, then $G = KH$ where K is a normal subgroup of order prime to p.*

Lemma 2.1.10 implies that any civic group must be a semidirect product of an odd order normal subgroup, and a cyclic 2-group. We will show that for the group to be civic, this product must in fact be direct.

Proposition 2.1.11. *Suppose $G = H \times K$ with $gcd(|H|, |K|) = 1$. Then G is civic if and only if H and K are civic.*

Proof. If G is civic, then H and K are too since they are subgroups.

For the other direction, suppose $P \subseteq H \times K$ is palindromic, and let $(a, b) \in P$. Since P is palindromic, it is closed under raising to positive powers, so $(a^m, b^m) \in P$ for all m. So if $m = \mathrm{ord}(b)$, then $(a^m, 1) \in P$. But since $\gcd(m, \mathrm{ord}(a)) = 1$, there exists n such that $a^{nm} = a$ and hence $(a, 1) \in P$. A similar argument shows that $(1, b) \in P$.

Thus, $(a, b) \in P$ implies $(a, 1)$ and $(1, b) \in P$. So if $(a, b), (a', b') \in P$, then we have $(a, 1), (a', 1) \in P$ and $(1, b), (1, b') \in P$. Because H is civic, we have that $\{x : (x, 1) \in P\}$ is a subgroup of H (since the image of palindromic sets is palindromic). Thus $(aa', 1) \in P$ and similarly $(1, bb') \in P$.

Without loss of generality, suppose $|H|$ is odd ($|H|$ and $|K|$ cannot both be even). So

$$(aa', 1)^m (1, bb')(aa', 1)^m = ((aa')^{2m}, bb') \in P$$

for all m, and (because $|H|$ is odd) we can choose m such that $2m - 1 = \mathrm{ord}(aa')$. Thus, $(aa', bb') \in P$, which shows P is closed under multiplication and hence a subgroup (since G is finite). □

Theorem 2.1.12. *A finite group G is civic if and only if $G = N \times H$ where N is civic of odd order and H is a cyclic 2-group.*

Proof. Suppose $G = N \times H$ where N is civic of odd order and H is a cyclic (and hence civic) 2-group. Then by Proposition 2.1.11, G is civic.

Suppose G is civic. We know that G is a semidirect product, $G = N \rtimes H$ with N and H as above, by Lemma 2.1.10. Suppose G is a minimal counterexample, i.e. with the semidirect product not direct. Let $H = \langle a \rangle$ and let $K = N \times H_1$ where $H_1 = \langle a^2 \rangle$.

First we show that H_1 is the unique subgroup in K of order $|H_1| = 2^{n-1}$. suppose there is another subgroup H_2 of the same order. Then H_1, H_2 are both Sylow 2-subgroups of K and thus conjugate (see Theorem A.3(ii) in the appendix). Therefore, there exists $g \in K$ such that $H_2 = gH_1g^{-1} = H_1$, since H_1 is normal in K. This implies that H_1 is characteristic in K (by Lemma 1.2.11) and hence normal in G (by Lemma 1.2.10).

Next we show that H is normal in G. Take some $g \in G$. We want to show that $gag^{-1} = a^k$ for some integer k. Since $g\langle a^2 \rangle g^{-1} = \langle a^2 \rangle$, there exists an integer k such that $(gag^{-1})^2 = ga^2g^{-1} = a^{2k}$ and hence $gag^{-1} = a^k$ or $gag^{-1} = a^{k+2^{n-1}}$.

Since N and H have relatively prime orders, $H \cap N = \{1\}$ and since both subgroups are normal in G, we are done. $\square$

Now we have reduced the classification of civic groups to the classification of odd order civic groups. The aim of the rest of this section is to understand those better.

Definition 2.1.13. Let G be a group and fix a generating set X. Let w be a word in the alphabet $X \cup X^{-1}$. Denote by $|w|$ the corresponding group element. Define $\overline{w}$ as the word obtained by reversing the word w. We say that a group is *reversible* with respect to X or X-*reversible* if it satisfies the property

$$|\overline{w_1}| = |\overline{w_2}| \Leftrightarrow |w_1| = |w_2|$$

for all words w_1, w_2.

Remark 2.1.14. Let $G = \langle X \rangle$ be a group and suppose that G is X-reversible. Let $g \in G$. If w_1 and w_2 are words such that $|w_1| = |w_2| = g$, then we know that $|\overline{w_1}| = |\overline{w_2}|$. Therefore we will use the notation $\overline{g}$ for the unique group element which is obtained by reversing any word that gives g. In general however, many different group elements can be obtained from g by writing it as different words and reversing them.

Lemma 2.1.15. *Let $P(X)$ be the set of all X-palindromes in a group $G = \langle X \rangle$ of odd order. Suppose there exists a nontrivial normal subgroup H of G such that $H \subseteq P(X)$. Then $pw(G, X) = pw(G/H, X/H)$, where $X/H = \{xH : x \in X\}$.*

Proof. Obviously, $\mathrm{pw}(G, X) \geq \mathrm{pw}(G/H, X/H)$.

Next we show that $\mathrm{pw}(G,X) \leq \mathrm{pw}(G/H, X/H)$. Let $k = \mathrm{pw}(G/H, X/H)$. Then one can write every element of G/H as $p_1 \cdots p_k H$ where $p_1, \ldots, p_k \in P(X)$. Therefore, every element of G can be written in the form $p_1 \cdots p_k h$ where $h \in H$. Now it suffices to show that $p_k h \in P(X)$. Note that we can write $p_k = p^2$ where $p \in P(X)$ since G has odd order (in fact, $p = p_k^{(\mathrm{ord}(p_k)+1)/2}$). Thus

$$p^2 h = p(php^{-1})p \in P(X)$$

since $php^{-1} \in H$ by normality, and since $H \subseteq P(X)$ we have that php^{-1}, and thus also $p(php^{-1})p$, is a palindrome. $\square$

Let $G = \langle X \rangle$ be a group. Fink and Thom [5, Proposition 3] show that the set $H = \{|\overline{w}| \in G : w \text{ is a word in } X \text{ and } |w| = 1\}$ is a normal subgroup of G. If G is not X-reversible, then that subgroup is non-trivial. Since the word $w\overline{w}$ is an X-palindrome, and $|\overline{w}w| = |\overline{w}||w| = |\overline{w}|$ if $|\overline{w}| \in H$, Lemma 2.1.15 allows us to restrict our attention to reversible groups in some minimal cases. In particular, if G is a minimal example of a group of odd order and palindromic width > 1, then there must be some generating set X with respect to which G is reversible: otherwise by minimality of G, G/H has palindromic width 1, where H is defined as above, contradicting that G has greater palindromic width by Lemma 2.1.15.

Lemma 2.1.16. *Let $G = \langle X \rangle$ be a group of odd order and suppose that G is X-reversible, let $N = \{g \in G : \overline{g} = g^{-1}\}$ and let $P(X)$ be the set of X-palindromes of G. Then every element of G can be written uniquely as pn where $p \in P(X)$ and $n \in N$.*

Proof. Since every palindrome is the square of a palindrome (as we saw in the proof of Lemma 2.1.15), we can write $g\overline{g} = p^2$ with $p \in P(X)$. Hence $g = p(p\overline{g}^{-1})$. Write $k = p\overline{g}^{-1}$. Then $p^2 = g\overline{g} = pk\overline{pk} = pk\overline{k}\overline{p} = pk\overline{k}p$ implying $k\overline{k} = 1$ and hence $k \in N$.

For uniqueness, suppose $pn = qm$ where $p, q \in P(X)$ and $n, m \in N$. Then $\overline{pn} = \overline{qm}$, i.e. $\overline{n}p = \overline{m}p$. Thus $pn\overline{n}p = qm\overline{m}q$ so $p^2 = q^2$ and hence $p = q$. This in turn implies that $n = m$. $\square$

As a bonus, we obtain the following corollary:

Corollary 2.1.17. *The number of X-palindromes of an odd order group $G = \langle X \rangle$ divides the order of the group.*

Proof. Suppose G is X-reversible. First we show that the set $N \subseteq G$ defined in Lemma 2.1.16 is a subgroup of G. Indeed, if $n_1, n_2 \in N$, then

$$\overline{(n_1 n_2)} = \overline{n_2}\,\overline{n_1} = n_2^{-1} n_1^{-1} = (n_1 n_2)^{-1}$$

and

$$\overline{(n_1^{-1})} = (\overline{n_1})^{-1} = (n_1^{-1})^{-1},$$

as desired. Now the result follows from Lemma 2.1.16.

If G is not X-reversible, then take the normal subgroup

$$H = \{|\overline{w}| \in G : w \text{ is a word in } X \text{ and } |w| = 1\} \lhd G$$

and consider the group G/H. If G/H is X/H-reversible, then the number of X/H-palindromes in G/H divides $|G|/|H|$ as shown above, and for any X/H-palindrome rH of G/H we obtain $|H|$ different X-palindromes $r|w\overline{w}| = |w|r|\overline{w}|$ of G (where $|w\overline{w}| = |\overline{w}| \in H$, since $|w| = 1$). If G/H is not X/H-reversible, we repeat and take the quotient by the group

$$H_2 = \{|\overline{w}| \in G/H : w \text{ is a word in } (X/H) \text{ and } |w| = 1\}.$$

Eventually, this process must stop since we are start with a finite group. □

We need the following Lemma, which is proved in Robinson [9, p. 148].

Lemma 2.1.18. *If G is a non-trivial finite solvable group and H a minimal normal subgroup, then $H = (\mathbb{Z}/p\mathbb{Z})^r$ for some integer $r \geq 1$ and prime p.* □

In the rest of this section, G will denote a minimal odd order group with respect to the property $\mathrm{pw}(G) > 1$, i.e. a group of odd order such that $\mathrm{pw}(G) > 1$ and $\mathrm{pw}(H) = 1$ whenever H is a quotient or subgroup of G. We may assume $\mathrm{pw}(G, X) > 1$ where $G = \langle X \rangle$ is X-reversible, as noted above (follows from Lemma 2.1.15). To clarify: G will have palindromic width 1 with respect to every generating set, with respect to which G is not reversible. The goal is to arrive at Theorem 2.1.26, i.e. prove that G is a p-group for some prime p, or that $G = (\mathbb{Z}/p\mathbb{Z})^r \rtimes (\mathbb{Z}/q\mathbb{Z})$ for distinct primes q, p.

Lemma 2.1.19. *If $G = \langle X \rangle$ is X-reversible and civic, then G is abelian.*

Proof. Take $x, y \in X$. Then there exists an X-palindrome w such that $xy = |w|$. Then $yx = |\overline{w}| = |w| = xy$, hence G is abelian. □

Lemma 2.1.20. *For any non-trivial normal subgroup H of G, the quotient G/H is abelian.*

Proof. For any nontrivial normal subgroup H of G, G/H is X/H-reversible with palindromic width 1, since $xy = \overline{xy} = yx$ for generators $x, y \in X/H$ ($\overline{xy}$ is uniquely determined because G/H is X/H-reversible), and thus G/H is abelian. □

Lemma 2.1.21. *The derived subgroup $G' = \langle \{xyx^{-1}y^{-1} : x, y \in G\} \rangle$ of G is elementary abelian, i.e. $G' = (\mathbb{Z}/p\mathbb{Z})^r$ for some integer r and prime p.*

Proof. By the Feit-Thompson theorem [4], G is solvable, so if H is a minimal normal subgroup, we have $H = (\mathbb{Z}/p\mathbb{Z})^r$ for some integer r by Lemma 2.1.18. Thus it suffices to show that G' is a minimal normal subgroup of G. It is well-known to be normal. Since G is not abelian, G' is nontrivial. Further, it is contained in any non-trivial normal subgroup H of G since for all $x, y \in G$, Lemma 2.1.20 gives that $xyH = yxH$ i.e. $x^{-1}y^{-1}xyH = H$ i.e. $x^{-1}y^{-1}xy \in H$. □

Lemma 2.1.22. *Every proper subgroup of G is civic.*

Proof. Let H be a proper subgroup of G. Note that H has palindromic width 1, and every subgroup of H has palindromic width 1. We want to show that H is civic. Take a palindromic subset P of H. Since $\mathrm{pw}(\langle P \rangle, P) = 1$, every element of $\langle P \rangle$ can be written as a palindrome in the letters of P, but these are precisely the elements of P (since P is palindromic). Hence $P = \langle P \rangle$ is a subgroup of H. Therefore H is civic. □

Lemma 2.1.23. *If r, s are two non-commuting X-palindromes, then $G = \langle r, s \rangle$.*

Proof. Suppose there exist non-commuting X-palindromes r, s such that

$$H = \langle r, s \rangle \neq G.$$

By minimality of G, the set of $\{r, s\}$-palindromes is a palindromic subset and hence a subgroup of H, since H is civic by Lemma 2.1.22.

Now we show that H is $\{r, s\}$-reversible. Let w, v be words in X such that $r = |w\overline{w}|$ and $s = |v\overline{v}|$. Suppose u is a word in the alphabet $\{r, s\}$. Let u' be the word in X obtained from u by replacing each occurence of r and s in u with the words $w\overline{w}$ and $v\overline{v}$ respectively. Then, since $\overline{w\overline{w}} = w\overline{w}$ and $\overline{v\overline{v}} = v\overline{v}$, we obtain that $|\overline{u}| = |\overline{u}'|$.

We conclude that H is civic and reversible, and hence abelian (by Lemma 2.1.19, contradicting the assumption that r, s do not commute. Therefore, $G = \langle r, s \rangle$. $\square$

Lemma 2.1.24. *The center $Z(G)$ contains no non-trivial X-palindromes.*

Proof. Let $P(X)$ be the set of X-palindromes in G and let $H = P(X) \cap Z(G)$. It suffices to show that H is a normal subgroup of G, since $H \subseteq P(X)$ and then by Lemma 2.1.15, H being nontrivial would contradict the fact that $\mathrm{pw}(G, X) > 1$. Take $g_1, g_2 \in H$. Since $g_1, g_2 \in Z(G)$, we have that $g_1 g_2 = g_2 g_1 = \overline{g_1 g_2}$ is a palindrome. Thus H is closed under multiplication. Clearly it is also closed under inverses. This means that H is a subgroup of G, and since it is contained in the center, it is normal in G, and we are done. $\square$

Lemma 2.1.25. *The number of X-palindromes of G is at least $|C_x||C_y|$ where x, y are non-commuting palindromes of G and $C_x = \{g \in G : gx = xg \text{ and } g = \overline{g}\}$ is the set of X-palindromes commuting with x.*

Proof. First we show that C_x forms an abelian group. Note that C_x is contained in $C_G(x)$, the centralizer of x in G, which is a proper subgroup of G since $y \notin C_G(x)$. Let $g_1, g_2 \in C_x$. Then $\langle g_1, g_2 \rangle \subseteq C_G(x) \neq G$ and hence the X-palindromes g_1, g_2 do not generate the whole group G. Therefore they commute and hence $g_1 g_2$ is an X-palindrome (because G is X-reversible), so $g_1 g_2 \in C_x$. Obviously $g_1^{-1} \in C_x$, and we obtain that C_x is an abelian subgroup of G.

Since $Z(G)$ contains no X-palindromes by Lemma 2.1.24, it is clear that if x, y are non-commuting palindromes, $C_x \cap C_y = \{1\}$. Further, $C_x = C_g$ for all $g \in C_x$ such that $g \neq 1$.

To show that the number of palindromes of G is at least $|C_x||C_y|$ where x, y are non-commuting palindromes, we will show that if $a, b \in C_x$ and $c, d \in C_y$ then $aca = bdb$ if and only if $a = b$ and $c = d$, implying that the set

$$\{aca : a \in C_x, c \in C_y\},$$

which consists of X-palindromes, has $|C_x \times C_y| = |C_x||C_y|$ different elements.

Suppose $aca = bdb$ and define $z = ab^{-1}$. Then $d = b^{-1}acab^{-1} = ab^{-1}cab^{-1} = zcz$. It suffices to show that $z = 1$. Now $cd = dc$ so $czcz = zczc$ implying $cz = zc$ since the order of G is odd. Therefore $z \in C_x \cap C_c = C_x \cap C_y = \{1\}$. $\square$

Now let N be as in Lemma 2.1.16. Take $n \in N$ and write $n = x^2$. Then $x \in N$ so $x = \overline{x}^{-1}$. Since G/G' is abelian, $xG' = \overline{x}G'$ so $nG' = x^2G = \overline{x}^{-1}xG' = G'$. Hence $N \subseteq G'$.

Consider two cases

(i) Suppose $N = G'$. Then N is a normal subgroup of G. Take a generator $x \in X$ and let $h \in N$. We have

$$N \ni x^{-1}h^{-1}x = \overline{xhx^{-1}} = (xhx^{-1})^{-1} = xh^{-1}x^{-1}$$

and hence

$$x^2h = hx^2.$$

Therefore, $N \subseteq Z(G)$ since $|G|$ is odd and is thus G is generated by the squares of any given generators. There must exist two non-commuting X-palindromes, since otherwise the group would be abelian. Let x, y be non-commuting X-palindromes of G. By Lemma 2.1.23, $G = \langle x, y\rangle$. Thus G/G' is generated by xG' and yG', so $|G/G'|$ divides $\mathrm{ord}(x)\mathrm{ord}(y)$. Recall that $|G/G'|$ is the number of palindromes. Further, we have that the number of palindromes is at least $|C_x||C_y|$ by Lemma 2.1.25. Therefore,

$$|C_x||C_y| \leq |G/G'| \leq \mathrm{ord}(x)\mathrm{ord}(y) \leq |C_x||C_y|,$$

implying equality everywhere. We conclude that $|G/G'| = \mathrm{ord}(x)\mathrm{ord}(y)$. Further, the palindrome xyx does not commute with x or y. To see that, suppose xyx commutes with x. Then $x^2yx = xyx^2$, and hence $xy = yx$, contradiction. If xyx commutes with y, then $xyxy = yxyx$ and hence $xy = yx$ since the group has odd order, again a contradiction. We conclude that there exist at least three pairwise non-commuting palindromes. We now claim that all X-palindromes have the same prime order q. Indeed, let p be an X-palindrome not commuting with x or y. Then $G = \langle p, x\rangle = \langle p, y\rangle$ and thus

$$|G/G'| = \mathrm{ord}(x)\mathrm{ord}(y) = \mathrm{ord}(p)\mathrm{ord}(y) = \mathrm{ord}(p)\mathrm{ord}(y),$$

which implies

$$\mathrm{ord}(x) = \mathrm{ord}(y) = \mathrm{ord}(p).$$

To see that $\mathrm{ord}(x)$ is prime, take some m such that $x^m \neq 1$. Then x^m is a palindromes not commuting with y and thus $G = \langle x^m, y\rangle$. Therefore, as before,

$$\mathrm{ord}(x^m) = \mathrm{ord}(x).$$

If $\mathrm{ord}(x)$ had a divisor m greater than 1, then $\mathrm{ord}(x^m) < \mathrm{ord}(x)$, proving that $\mathrm{ord}(x)$ is prime.

(ii) Suppose N is properly contained in G'. Note that G is then necessarily centerless, otherwise $Z(G) \supseteq G'$ (since G' is a minimal normal subgroup of G) properly contains N and therefore $Z(G)$ contains some nontrivial palindromes, contradicting Lemma 2.1.24. Since G' is abelian, in particular all the palindromes of G' commute, and thus every element of G' can be written uniquely as zn where $z \in C_x$ for some palindrome $x \in G'$ and $n \in N$. It's easy to see that these z's form a subgroup H of C_x. Hence $G' = HN$. Since any pair of non-commmuting palindromes will generate the whole group G by Lemma 2.1.23, we have that $G/G' = \langle yG' \rangle$ where y is a palindrome not commuting with x. Hence $|G|$ divides $|N||H|\mathrm{ord}(y)$. Recall that $|G|/|N|$ is the number of palindromes and

$$|C_x||C_y| \leq |G|/|N| \leq |H|\mathrm{ord}(y) \leq |C_x||C_y|.$$

Thus the number of palindromes is equal to $|H|\mathrm{ord}(y)$ for any palindrome y not commuting with x. As before, all such palindromes y have the same prime order, call it q.

In both of the above cases, we find that G/G' is elementary abelian of order dividing q^2 (order q^2 in the former case and q in the latter). Recall also that G' is elementary abelian of order p^r for some integer r.

If $p \neq q$, it follows directly from Schur's Theorem (1.3.9), that G is the semi-direct product of two elementary abelian groups: $(\mathbb{Z}/p\mathbb{Z})^r$ and $(\mathbb{Z}/q\mathbb{Z})^j$ where $j \in \{1, 2\}$, p is the prime dividing the order of G' and r is some integer. It is in the former case that $j = 2$, but then we actually have a central series for G: $\{1\}, Z(G), G$. Therefore G is nilpotent, and by Theorem 1.2.12 it is the direct product of its Sylow subgroups. Hence in our case, G is abelian, and therefore civic.

Otherwise G is a p-group for some prime p. In conclusion:

Theorem 2.1.26. *A minimal odd order group G having the property $pw(G) > 1$ is either a p-group or of the form $(\mathbb{Z}/p\mathbb{Z})^r \rtimes (\mathbb{Z}/q\mathbb{Z})$ for distinct primes q, p.* □

Corollary 2.1.27. *A minimal non-civic group of odd order is either a p-group or of the form $(\mathbb{Z}/p\mathbb{Z})^r \rtimes (\mathbb{Z}/q\mathbb{Z})$ for distinct primes q, p.*

Proof. This follows from Theorem 2.1.26 and Lemma 2.1.22. □

We end this section by giving examples of civic and non-civic groups.

Example 2.1.28. We want to show that of the five groups of order 27, four are civic and one is not. The five groups of order 27 are (see [3, p. 179-184])

- $G_1 = \mathbb{Z}/27\mathbb{Z}$;
- $G_2 = (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$;
- $G_3 = (\mathbb{Z}/3\mathbb{Z})^3$;
- $G_4 = \langle x, y : x^3 = y^9 = 1, xyx^{-1} = y^4 \rangle$;
- $G_5 = \langle x, a, b : x^3 = a^3 = b^3 = 1, ab = ba, xax^{-1} = ab, xbx^{-1} = b \rangle$.

The groups G_1, G_2 and G_3 are all civic because of Lemma 2.1.6.

Next we show that G_4 is civic. Note that $xy = y^4 x$, but $yx \neq xy^4$. Hence, G_4 is not $\{x, y\}$-reversible. Since every proper subgroup and quotient of G_4 is abelian, this implies that $\mathrm{pw}(G_4, \{x, y\}) = 1$. Now take some $X \subseteq G_4$ such that $G_4 = \langle X \rangle$. We want to show that $\mathrm{pw}(G_4, X) = 1$. Suppose $\mathrm{pw}(G_4, X) > 1$. Then we may assume G_4 is X-reversible and G_4 is thus a minimal odd order group of the type that was studied on the preceding pages. Since G_4 is a 3-group, it cannot be centerless and thus $N = G_4'$ where N is defined as in Lemma 2.1.16. Note that $y^3 = xyx^{-1}y^{-1}$, and thus $\langle y^3 \rangle \subseteq G_4'$. Also, $xy^3x^{-1} = y^{12} = y^3$ so $\langle y^3 \rangle \lhd G_4$. Since G_4' is a minimal normal subgroup of G_4, we now have $\langle y^3 \rangle = G_4'$. Every element of G_4 can be written as the product of an X-palindrome p and an element $n \in N$ by Lemma 2.1.16. Therefore, there exists an X-palindrome p and integer m such that

$$y = (y^3)^m p,$$

which implies that $y^{1-3m} = p$ is an X-palindrome. This is a contradiction, since then $y^3 \in N$ is an X-palindrome. We conclude that $\mathrm{pw}(G_4, X) = 1$ and thus G_4 is civic.

Finally, we show that G_5 is not civic. Note that $G_5 = \langle a, x \rangle$, since $b = xax^{-1}a^{-1}$. We will show that the set of all $\{a, x\}$-palindromes in G_5 is

$$P = \{a^r x^s a^r : 0 \leq r, s \leq 2\}$$

which is a proper subset of G_5. This implies that $\mathrm{pw}(G_5, \{a, x\}) > 1$. Take some word w in the alphabet $\{a, x\}$ and suppose w is a palindrome. By "peeling off" the leftmost and rightmost letter of w and repeating, one eventually ends up with a word w' such that $|w'| \in P$. Therefore, if we can show that for any $p \in P$, both

$apa \in P$ and $xpx \in P$, we are done. Obviously $apa \in P$. Note that the relations of the group G_5 give

$$xa^r = a^r x b^r \text{ and } a^r x = x a^r b^{-r} \quad (*)$$

(if $a^r \neq 1$). Let $p = a^r x^s a^r$ where $r, s \in \{0, 1, 2\}$. If $r = 0$, then clearly $xpx \in P$. Otherwise, using $(*)$ above, we obtain

$$xpx = xa^r x^s a^r x = a^r x b^r x^s x a^r b^{-r} = a^r x^{s+2} a^r b^r b^{-r} = a^r x^{s+2} a^r \in P,$$

and we are done.

2.2. Application to the Magnus-Derek Game

In [8], Nedev and Muthukrishnan introduced the so-called Magnus-Derek game. It is played by two players called Magnus and Derek, on a circular table with n labeled positions. Magnus moves a token around the table by specifying how many positions he will move the token, while Derek gets to decide in which direction he moves it. Magnus's goal is to maximize the number of positions visited while Derek's is to minimize this number. Later, Gerbner [6] generalized the game such that the positions are the elements of a finite group. Then Magnus chooses a group element g and Derek decides whether to multiply the current position with g or g^{-1} from the right. In the same paper, Gerbner solved the game for abelian groups and a few other cases. Of course, the original game is equivalent to Gerbner's game in $\mathbb{Z}/n\mathbb{Z}$.

Denote by $f(G)$ the number of group elements that will be visited assuming optimal play in a group G. For G an abelian group, Gerbner [6] showed that

$$f(G) = \begin{cases} |G|, & \text{if } |G| \text{ is a power of 2,} \\ |G|(1 - 1/p), & \text{where } p \text{ is the smallest odd prime factor dividing } |G|. \end{cases}.$$

Let Γ be the subgroup of G generated by the elements of G whose order is a power of 2, and P be a maximal palindromic proper subset of G/Γ. Since G is abelian, Γ is in fact the Sylow 2-subgroup of G. Further, G/Γ is abelian of odd order, and hence civic by Lemma 2.1.6, so P will be a maximal subgroup of G/Γ, and $|(G/\Gamma) : P| = p$ where p is the smallest odd prime divisor of $|G|$ (by Theorem 1.2.12). Thus $|P| = \frac{|G|/|\Gamma|}{p}$ and the above formula for $f(G)$ gives

$$f(G) = \begin{cases} |G|, & \text{if } |G| \text{ is a power of 2,} \\ |G| - |\Gamma||P|, & \text{otherwise.} \end{cases}$$

We claim that this is the case for all groups, not just abelian ones. To prove that claim, we need to show that $f(G) = |G| - |P|$ where G is a group of odd order, since it suffices to consider groups of odd order, as the next three lemmas show.

Lemma 2.2.1. *Let G be a finite group and $\Gamma \subseteq G$ be the subgroup of G generated by all the elements whose orders are powers of 2. Then $\Gamma \lhd G$ and $|G/\Gamma|$ is odd.*

Proof. First note that $|G|/|\Gamma|$ is odd since Γ contains a (in fact every) Sylow 2-group of G. To see that $\Gamma \lhd G$, let $x \in \Gamma$ and write $x = t_1 t_2 \cdots t_k$, where each t_i has order a power of 2. Then conjugating we see

$$gxg^{-1} = g\left(\prod_{i \le k} t_i\right) g^{-1} = \prod_{i \le k} (g t_i g^{-1}),$$

and since conjugation does not change order of an element, each $g t_i g^{-1}$ has order a power of 2. $\square$

Lemma 2.2.2. *If Γ is generated by elements whose orders are powers of 2, then $f(\Gamma) = |\Gamma|$.*

Proof. Suppose the token is currently at x and t is an element of order 2^k. We will show that Magnus has a strategy to move the token from x to xt. With this, it will follow that Magnus has a strategy to move the token to $x t_1 t_2 \cdots t_k$ for any elements t_i whose orders are powers of 2, and since such elements generate Γ, this would complete the proof.

For Magnus to move the token from x to xt, he performs the following algorithm:

- Magnus chooses t^1, t^2, t^4, t^8, $\ldots$, $t^{2^{k-1}}$ in order until the token is at xt.

If Magnus follows this strategy, we claim that one of Derek's responses necessarily moves the token to xt. Otherwise Derek's first reply must be

$$x \mapsto xt^{-1} = xt^{1-2}$$

(since otherwise the token would land on xt). Similarly, the second reply must be

$$xt^{1-2} \mapsto (xt^{1-2})t^{-2} = xt^{1-4}.$$

And in general, Derek's response to t^{2^i} must be

$$xt^{1-2^i} \mapsto xt^{1-2^{i+1}}.$$

Thus, his response to $t^{2^{k-1}}$ must be $xt^{1-2^{k-1}} \mapsto xt^{1-2^k}$. But this is equal to xt since $t^{2^k} = 1$. $\square$

Lemma 2.2.3. *If $K \lhd G$, then $f(K)f(G/K) \leq f(G) \leq |K|f(G/K)$.*

Proof. For the lower bound, Magnus's strategy is as follows:

(a) Each time the token arrives in a new left coset gK, Magnus chooses only elements of K (thereby staying within that coset) until he has moved the token to as many new positions within gK as he can.

(b) By playing as if in G/K, Magnus moves the token to a new (left) coset if possible.

If Magnus follows this strategy, the token will visit at least $f(K)$ elements within each coset, and it will visit at least $f(G/K)$ cosets.

For the upper bound, Derek can follow a strategy as if playing in G/K, and making every decision with the singular goal that the token reaches at most $f(G/K)$ cosets. □

The previous three lemmas show that for any group G, with Γ defined like in Lemma 2.2.1, we have

$$f(G) = |\Gamma| f(G/\Gamma).$$

Therefore, it suffices to find $f(G/\Gamma)$. Further, the order of the group G/Γ is always odd. Hence we have reduced the problem to the odd order case.

Now suppose G is a group of odd order. We define the *open Magnus-Derek game* as follows:

Derek first picks a set $N \subseteq G$ and *tells Magnus what that set is.* Derek's goal is to pick as large a set as possible so that he can be certain to keep the token out of N. In this version, Magnus's only goal is to move the token into N.

We define $\tilde{f}(G) = |G| - \max_N |N|$, where the maximum is taken over all sets N for which Derek can win this modified game.

Conveniently, it turns out the open Magnus-Derek game is equivalent to the original Magnus-Derek game in finite groups.

Lemma 2.2.4. *If N is a maximal set for which Derek can win the open game, then Magnus can reach every element outside of N. Moreover, for all x and g, if $xg \in N$ and $xg^{-1} \in N$, then $x \in N$ as well.*

Proof. Let $y \in G \setminus N$. By the maximality of N, Derek cannot win the game if he claims the set $N \cup \{y\}$. Hence Magnus can reach some element of $N \cup \{y\}$, however Derek plays. When Derek claims the set N, he will play a strategy that prevents Magnus from reaching any element of N, so if Magnus plays the strategy that would allow him to reach some element of $N \cup \{y\}$ had Derek claimed that set, then he must eventually reach some element of that set, and that element must be y since Derek is preventing him from reaching N.

For the second part, suppose $x \notin N$. Then by the first part of this lemma, Magnus can reach x and then choose g. Then he reaches either xg or xg^{-1}, contradicting the fact that both belong to N. Hence $x \in N$. □

Proposition 2.2.5. *For any finite group G, $\tilde{f}(G) = f(G)$.*

Proof. In the original game, Derek can pick a maximal set N for which he can win the open game without telling Magnus, and play as if playing the open game. Thus $f(G) \leq \tilde{f}(G)$.

Now we consider the original game from Magnus's point of view. Suppose that N is the set of elements the token hasn't visited, at the current step. Note that if $|N| > |G| - \tilde{f}(G)$, then Magnus can pretend that Derek has picked the set N, and play as in the open game to make the token reach some element of N (he can do that, since otherwise we would have found a bigger set for which Derek can win the open game). Eventually, the size of N will shrink to $|G| - \tilde{f}(G)$, which means that the token will have reached $\tilde{f}(G)$ elements. Thus $f(G) \geq \tilde{f}(G)$. □

Definition 2.2.6. Let G be a group of odd order. We say that an element $b \in G$ is *between* elements $a, c \in G$ if there exist $x, g \in G$ such that $a = xg$, $b = x$, $c = xg^{-1}$.

It is straightforward to see that there is a unique element between any two elements. Since G has odd order, every element is a square and indeed, $b = cd$, where d is the (unique) square root of $c^{-1}a$, is the unique element between a and c. With this terminology, Lemma 2.2.4 states that for any two elements in N, the element between them also belongs to N. Define a map $b : G \times G \to G$ such that $b(x, y)$ is the element between x and y.

Lemma 2.2.7. *Let G be a group of odd order and let $N \subseteq G$ be a set with the property $x, y \in N \Rightarrow b(x, y) \in N$. Then the following holds: if $a \in N$ and $ax \in N$ then $ax^k \in N$ for all integers k.*

Proof. Denote the square root of x by $s(x)$ and s^k the composition of s with itself k times. Observe that s is the inverse of the map $x \mapsto x^2$. Let $x \in N$ and m be the order of x.

Consider the sequence $(x^{2^i})_{i\in\mathbb{N}}$. It is periodic since the sequence $(2^i \bmod m)_{i\in\mathbb{N}}$ is periodic; call its period p. Then the finite sequence $(s^i(x))_{i=0}^p$ is obtained by reversing the order of the finite sequence $(x^{2^i})_{i=0}^p$. To see that, note that

$$x^{2^i} = s^{-i}(x) = s^{p-i}(x),$$

since $x \mapsto x^2$ is the inverse of the map s, as noted above.

Now, since $as(x) = b(a, ax)$ we have that the sequence $(as^i(x))_{i=0}^p$ is fully contained in N. Hence the sequence $(ax^{2^i})_{i=0}^p$ is contained in N. Suppose 2^r is the largest power of 2 which does not exceed m. Let $t \leq r$ be an integer and observe that $ax^k \in N$ for all integers k between 2^{t-1} and 2^t — simply keep taking the "between" elements. Hence $\{ax^k\}_{k=0}^{2^r} \subseteq N$, i.e. more than half of all the powers ax^k are contained in N. For each integer q between 1 and $\frac{m+1}{2}$, we have

$$b(ax^{q-1}, ax^q) = ax^{q-1}s(x) =: ax^k$$

where $k > \frac{m+1}{2}$. Further, for the $\frac{m+1}{2}$ different choices of q we get $\frac{m+1}{2}$ different values of k. We are done, since $\frac{m+1}{2} < 2^r$ and hence $ax^q \in N$ for all these choices of q. $\square$

Corollary 2.2.8. *Let N and G be as in Lemma 2.2.7. Then there exists $a \in G$ such that $N = aP$ where P is a palindromic subset of G.*

Proof. Fix some $a \in N$. We want to show that the set $a^{-1}N$ is palindromic in G. Note that $1 \in a^{-1}N$ and take some $x, y \in a^{-1}N$. By Lemma 2.2.7, the fact that $a, ay \in N$ implies that

$$ax(x^{-1}y^{-1}) = ay^{-1} \in N.$$

Since $ax, ax(x^{-1}y^{-1}) \in N$, Lemma 2.2.7 again implies that

$$axyx = ax(x^{-1}y^{-1})^{-1} \in N,$$

i.e. $xyx \in a^{-1}N$. $\square$

To prove that that our claim (that $f(G) = |G| - |P|$ where P is a maximal proper palindromic subset of G) is true, it now only remains to show that for any palindromic subset of G, Derek can win the game if he pick a set of the same size and win:

Proposition 2.2.9. *Let $P \subsetneq G$ be a palindromic subset of an odd order group G. Then there exists $a \in G$ such that Derek can prevent the token from reaching aP.*

Proof. Suppose b is the element where the token starts, and let a be some element such that $b \notin aP$. First we show that $b(ax, ay) = ap$, where $p \in G$ is an $\{x, y\}$-palindrome. Indeed, suppose n is the order of y and $2m - 1$ is the order of $y^{-1}x$. Then $(y^{-1}x)^m$ is the square root of $y^{-1}x$ and

$$\begin{aligned} b(ax, ay) &= ay((ay)^{-1}ax)^m \\ &= ay(y^{-1}a^{-1}ax)^m \\ &= ay(y^{-1}x)^m \\ &= ax\, \underbrace{y^{-1}x \cdots xy^{-1}x}_{m-1 \text{ factors of } y^{-1}x} \\ &= ax\, \underbrace{y^{n-1}x \cdots xy^{n-1}x}_{m-1 \text{ factors of } y^{n-1}x} \\ &= ap \end{aligned}$$

where $p = x(y^{n-1}x)^m$ is clearly an $\{x, y\}$-palindrome. Therefore, aP satisfies the property that for any $x, y \in P$, $b(ax, ay) \in aP$. Taking the contrapositive, we see that if $b(ax, ay) \notin aP$, then $ax \notin P$ or $ay \notin P$.

If the token is at $g \in G \setminus aP$, then for any $h \in G$,

$$g = b(gh, gh^{-1}).$$

Thus, either $gh \notin aP$, or $gh^{-1} \notin aP$. Hence, if the token is currently at an element g outside of aP, then whatever element h Magnus chooses, Derek can send the token to an element outside aP. □

Theorem 2.2.10. *In the Magnus-Derek game, if G has odd order, then*

$$f(G) = |G| - |P|,$$

where P is a maximal palindromic proper subset of G. In particular,

$$f(G) \leq |G|(1 - 1/p),$$

where p is the smallest prime dividing $|G|$.

Proof. From Corollary 2.2.8 it follows that

$$f(G) \geq |G| - |P|,$$

and from Proposition 2.2.9 that

$$f(G) \leq |G| - |P|.$$

The fact that

$$f(G) \leq |G|(1 - 1/p)$$

follows from Corollary 2.1.17, which applies since P is the set of all P-palindromes of the subgroup $\langle P \rangle$ of G. $\square$

Note that this upper bound is reached in nilpotent groups, since subgroups are palindromic subsets and a nilpotent group has a subgroup of any given order dividing its order. In fact, the upper bound is reached in all groups with a subgroup of index p where p is the smallest prime dividing the order of the group. Note also that if G is civic, then we know that any set P like in Theorem 2.2.10 is a subgroup. We conjecture that every group of odd order satisfies a weaker property than being civic, namely that it has a proper subgroup at least as large as any proper palindromic subset, but the question of whether that is true remains open.

A. Basic Results in Group- and Representation Theory

Here, we present some notions and results in elementary group theory, which the reader should be familiar with. The proofs of the theorems can be found in most algebra textbooks, for instance [3]. Also, we state the one theorem from representation theory that is used, Maschke's theorem.

A.1. Isomorphism Theorems

Theorem A.1.1. *(The first isomorphism theorem) Let G, H be groups and $\varphi : G \to H$ a group homomorphism. Then the kernel* $\operatorname{Ker}\varphi$ *is a normal subgroup of G and*

$$G/\operatorname{Ker}\varphi \cong \varphi(G).$$

□

Theorem A.1.2. *(The second isomorphism theorem) If G is a group, H a subgroup of G and N a normal subgroup of G, then $H \cap N$ is normal in H and*

$$HN/N \cong H/(H \cap N).$$

In fact, there is a natural isomorphism $\varphi : H/(H \cap N) \to HN/N$ given by

$$\varphi(h(H \cap N)) = hN.$$

□

Theorem A.1.3. *(The third isomorphism theorem) If G is a group and N, M are normal subgroups of G such that $M \subseteq N$, then N/M is normal in G/M and*

$$(G/M)/(N/M) \cong G/N.$$

□

Theorem A.1.4. *(The fourth isomorphism theorem) Let G be a group and N a normal subgroup of N. Then there is a bijection from the set of those subgroups A of G such that $N \subseteq A$, to the set of subgroups of G/N. In particular, every subgroup of G/N is of the form A/N for some subgroup A of G containing N. The bijection $A \mapsto A/N$ has the following properties: for all subgroups $A, B \subseteq G$ such that $N \subseteq A$ and $N \subseteq B$,*

(i) $A \subseteq B$ *if and only if* $A/N \subseteq B/N$,

(ii) *if* $A \subseteq B$, *then* $|B : A| = |B/N : A/N|$,

(iii) $\langle A \cup B \rangle /N = \langle A/N \cup B/N \rangle$,

(iv) $(A \cap B)/N = (A/N) \cap (B/N)$ *and*

(v) $A \lhd G$ *if and only if* $A/N \lhd G/N$.

□

A.2. The Class Equation

Definition A.2.1. Let G be a group, $A \subseteq G$ and $a \in G$. Then we define

- the *centralizer* of $a \in G$ as $C_G(a) = \{g \in G : ga = ag\}$,
- the *normalizer* of A in G as $N_G(A) = \{g \in G : gA = Ag\}$

Note that $C_G(a) = N_G(\{a\})$.

Definition A.2.2. Let G be a group. The *conjugacy class* of $x \in G$ is the set

$$x^G = \{gxg^{-1} : g \in G\}.$$

In the language of group actions, we could say that the conjugacy class of x is the orbit of x in the action of G on itself by conjugation.

The size of the conjugacy class x^G is related to the centralizer of x in the following way:

Proposition A.2.3. *For all $x \in G$, we have*

$$|x^G| = |G : C_G(x)|$$

□

Now if $x \in Z(G)$, we have that $gxg^{-1} = x$ for all $g \in G$ and hence $x^G = \{x\}$, in accordance with Proposition A.2.3. Moreover it is easy to see that the conjugacy classes of G form a partition of G. Thus we have the following

Theorem A.2.4. *(The class equation). Let G be a finite group and $g_1, \ldots, g_r$ be representatives for each of the distinct conjugacy classes that lie outside of $Z(G)$. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

□

A.3. Sylow's Theorem

Definition A.3.1. Let p be a prime and P a group. Then if $|P| = p^n$ for some integer n, we say that P is a *p-group*. Now suppose G is a finite group and P a subgroup of G which is a p-group with p not dividing the index $|G : P|$. Then P is called a *Sylow p-subgroup* of G. The set of Sylow p-subgroups of G is denoted $\mathrm{Syl}_p(G)$ and we let $n_p = |\mathrm{Syl}_p(G)|$

Theorem A.3.2. *(Sylow) Let G be a group of order $p^\alpha m$ where p is a prime not dividing m.*

(i) There exists a Sylow p-subgroup of G, i.e. $Syl_p(G) \neq \varnothing$.

(ii) If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \subseteq gPg^{-1}$. In particular, if Q is also a Sylow p-subgroup of G, then $Q = gPg^{-1}$. Then we say that P and Q are ***conjugate****.*

(iii) The number n_p of Sylow p-subgroups of G is of the form $1 + kp$ for some integer k. Further, $n_p = |G : N(P)|$ for any Sylow p-subgroup P of G (here $N(P)$ denotes the normalizer of P in G); in particular n_p divides m.

□

A.4. FG-Modules and Maschke's Theorem

Definition A.4.1. Let G be a group acting on a vector space V over a field F. If the action satisfies the properties (i) and (ii), we say that V is an *FG-module.* Let $u, v \in V$ be vectors and $\lambda \in F$ a scalar.

(i) $g \cdot (\lambda v) = \lambda(g \cdot v)$,

(ii) $g \cdot (u + v) = g \cdot u + g \cdot v$.

Definition A.4.2. Let V be an FG-module and $W \subseteq V$ a subspace. If W satisfies the property that, for all $w \in W$ and all $g \in G$, $g \cdot w \in W$, we say that W is an *FG-submodule* of G.

Theorem A.4.3. *(Maschke) Let G be a finite group, F be a field such that $|G|$ does not divide the characteristic of F. Let V be an FG-module and U an FG-submodule of V. Then there exists another FG-submodule W of V such that*

$$V = U \oplus W.$$

□

A.5. Solvable Groups

Definition A.5.1. We say that a group is *solvable* if there exists a subnormal series

$$\{1\} = K_0 \lhd K_1 \lhd \cdots \lhd K_n = G$$

such that the quotient K_i/K_{i-1} is abelian for all i.

The following major result in finite group theory was proved by Feit and Thompson in 1963 [4].

Theorem A.5.2. *(Feit-Thompson) Every group of odd order is solvable.*

Bibliography

[1] W. Burnside. Notes on the Theory of Groups of Finite Order. *Proc. Lond. Math. Soc.*, 26:191–214, 1894/95.

[2] K. Conrad. The Schur-Zassenhaus Theorem.

[3] D. S. Dummit and R. M. Foote. *Abstract Algebra.* John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[4] W. Feit and J. G. Thompson. Solvability of Groups of Odd Order. *Pacific J. Math.*, 13:775–1029, 1963.

[5] E. Fink and A. Thom. Palindromic Words in Simple Groups. *Internat. J. Algebra Comput.*, 25(3):439–444, 2015.

[6] D. Gerbner. The Magnus-Derek Game in Groups. *Discrete Math. Theor. Comput. Sci.*, 15(3):119–126, 2013.

[7] M. I. Kargapolov and J. I. Merzljakov. *Fundamentals of the Theory of Groups*, volume 62 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979. Translated from the second Russian edition by R. G. Burns.

[8] Z. Nedev and S. Muthukrishnan. The Magnus-Derek Game. *Theoret. Comput. Sci.*, 393(1-3):124–132, 2008.

[9] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1996.

[10] R. Solomon. A Brief History of the Classification of the Finite Simple Groups. *Bull. Amer. Math. Soc. (N.S.)*, 38(3):315–352, 2001.