MT300: Groups of a Square-Free Order

Iordan Ganev
Royal Holloway, University of London
Supervisor: Dr. Benjamin Klopsch

Spring 2009
Updated January 2010*

Abstract

Hölder's formula for groups of a square-free order is an early advance in the enumeration of finite groups. We aim to elucidate this classical result through a structural approach, emphasizing topics such as nilpotency, the Fitting subgroup, and extensions. These topics, which are usually not covered in undergraduate group theory, feature in the proof of Hölder's result and have wide applicability in group theory. Finally, we remark on further results and conjectures in the enumeration of finite groups.

Contents

*An abbreviated version of this report has been accepted for publication in the Spring 2010 issue of the Rose-Hulman Undergraduate Mathematics Journal.

1 Introduction

How many non-isomorphic groups are there of order n? This is one of the simplest yet most mysterious questions in group theory. Groups of order 16 or less were classified in the late nineteenth century as part of early advances in group theory. It has been clear from even earlier that for any prime p, there is only one group of order p. In general, however, the tabulation of the non-isomorphic groups of order n requires careful consideration of the prime-power factorization of n, and the constraints on group structure imposed by the relationships between the divisors of n. Up to date, the groups of order less than 2048 have been tabulated [5].

Throughout this project, $f(n)$ denotes the number of groups, up to isomorphism, of order n. Group theorists agree that there is no hope for a precise formula for the group number function $f(n)$ in general. Nonetheless, there have been several remarkable asymptotic estimates due to Pyber which use the classification of finite simple groups, Hall systems, and combinatorial estimates. Moreover, for certain types of orders it is possible to determine explicit formulas, precise estimates, or other characterizations of $f(n)$. Much of the current research in the enumeration of finite groups attempts to extend the known results to more types of orders [3, Chapter 22].

One of the first mathematicians to make advances in the enumeration of finite groups was Otto Hölder. In 1893, he described groups of order p^3 and p^4 [14]. Shortly thereafter, he derived a remarkable formula for the number of groups of order n where n is square-free [15]:

$$f(n) = \sum_{m|n} \prod_{p} \frac{p^{c(p)} - 1}{p - 1}$$

where p is a prime divisor of n/m and $c(p)$ is the number of prime divisors q of m that satisfy $q \equiv 1 \pmod{p}$.

The aim of this project is to elucidate this classical result through a structural approach, demonstrating that what makes the formula possible is that a group of square-free order has restricted structure as a Sylow tower group. In order to render the result more accessible and to illustrate my progress through the term, we include introductory explanations of concepts used in this project that are beyond a standard undergraduate group theory course. Hence we devote much attention to topics such as nilpotency, the Fitting subgroup, and extensions. In addition, our approach emphasizes notions that have wide application in other areas of group theory and relate to open research problems.

The presentation of the advanced concepts in sections 3 to 7 relies heavily on Rotman [21]. For the derivation of Hölder's formula (section 8), Blackburn et al. [3] give an argument that we follow, but their comments are not a complete proof and warrant more explanation in our view. We also examine briefly Hölder's original proof and an argument given in Conway et al. [4]. First, let us remind ourselves of basic terminology from group theory.

2 Preliminaries

If $xy = yx$ for all elements x, y in a group G, then G is said to be *abelian*. The *center* $Z(G)$ of a group G is the set of elements that commute with any element of G, that is, $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$. Clearly $Z(G) = G$ if and only if G is abelian. For an element a in G, the *centralizer* $C_G(a)$ of a in G is the set of all elements that commute with a; in notation, $C_G(a) = \{g \in G \mid ga = ag\}$. The centralizer of a subgroup H of G is defined analogously: $C_G(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$.

For elements x, y in any group G, the conjugate of x under y is conventionally written as $x^y := y^{-1}xy$. The *normalizer* $N_G(H)$ of a subgroup H in G is the set $\{g \in G \mid g^{-1}Hg = H\}$, where $g^{-1}Hg = \{ghg^{-1} \mid h \in H\}$. A subgroup N of G is *normal* if $g^{-1}Ng = N$ for all $g \in G$, that is, if $N_G(N) = G$; in this case we write $N \trianglelefteq G$. It is trivial to verify that $Z(G)$ is a normal subgroup[1] in G and that, more generally, any subgroup of the center is normal. One can also verify that for any normal subgroup N of G, $C_G(N) \trianglelefteq G$ and $Z(N) \trianglelefteq G$. A *simple* group has exactly two normal subgroups: the identity subgroup $\{1\}$ and the group itself.

We will also make use of factor groups, products of groups, the Chinese Remainder Theorem, the Fundamental Theorem of Finite Abelian Groups (also known as the Basis Theorem), and the Sylow Theorems. Please refer to [11] and [21] for more details.

A *homomorphism of groups* is a map f from a group G to a group H with the property that for any $x, y \in G$, $f(xy) = f(x)f(y)$. The kernel of f is the pre-image of the identity of H: $\ker(f) = f^{-1}(1_H)$. Note that the identity of G is always mapped to the identity of H, so $1_G \in \ker(H)$. Also, $\ker(f)$ is a normal subgroup of G. The image $\mathrm{im}(f)$ of f in H is a subgroup of H.

An *isomorphism of groups* $f : G \to H$ is a bijective homomorphism. When an isomorphism exists from G to H, we write $G \cong H$ to indicate that the groups are *isomorphic*. An isomorphism from a group G to itself is called an *automorphism*. The set of automorphisms of G, denoted $\mathrm{Aut}(G)$, forms a group under the operation of composition of functions. Conjugation by an element $g \in G$ is an example of an automorphism. A subgroup H of G is a *characteristic subgroup* if $\phi(H) = H$ for all automorphisms ϕ of G. Hence, all characteristic subgroups of G are normal in G.

For a homomorphism $f : G \to H$, the *First Isomorphism Theorem* states that $G/\ker(f) \cong \mathrm{im}(f)$. If f is surjective, then its image is H and $G/\ker(f) \cong H$.

A cyclic group of finite order n consists of all powers of an element x, with the defining condition that $x^n = 1$. The generic cyclic group of order n is denoted here as C_n. The integers modulo n, denoted $\mathbb{Z}/n\mathbb{Z}$, form a cyclic group of order n under addition. The subset $U(n)$ of $\mathbb{Z}/n\mathbb{Z}$ consisting of elements relatively prime to n forms a group under multiplication modulo n. It is well-known that $\mathrm{Aut}(C_n) \cong U(n)$.

We prove the following proposition (known as the N/C Lemma) before completing this revision.

Proposition 1. *If H is a subgroup of G, then $C_G(H) \trianglelefteq N_G(H)$ and the quotient $N_G(H)/C_G(H)$ is isomorphic to a subgroup of* $\mathrm{Aut}(H)$.

Proof. Let $\gamma_g|_H$ denote conjugation by $g \in G$ restricted to H, that is $\gamma_g|_H : H \to G$, $x \mapsto g^{-1}xg$. If $g \in N_G(H)$, then $\gamma_g|_H$ is an automorphism of H, from the definition of the normalizer. Hence let $\phi : N_G(H) \to \mathrm{Aut}(H)$ be the homomorphism which maps g to $\gamma_g|_H$. Then,

$$g \in \ker(\phi) \;\Leftrightarrow\; \gamma_g = \mathrm{id}|_H \;\Leftrightarrow\; g^{-1}xg = x \text{ for all } x \in H \;\Leftrightarrow\; g \in C_G(H).$$

Since the kernel of a homomorphism in normal in the domain, $C_G(H) \trianglelefteq N_G(H)$. By the First Isomorphism Theorem,

$$N_G(H)/C_G(H) = N_G(H)/\ker(\phi) \cong \mathrm{im}(\phi) \leq \mathrm{Aut}(H).$$

□

3 Commutators

Let G be a group. For any two elements x and y in G, define the *commutator* of x and y to be $[x, y] := x^{-1}y^{-1}xy = x^{-1}x^y$. Similarly, if H and K are subgroups of G then $[H, K]$ denotes the

[1] In fact, $Z(G)$ is characteristic in G.

subgroup of G generated by all commutators $[h,k]$ with $h \in H$ and $k \in K$. Since $[h,k] = [k,h]^{-1}$, $[H,K] = [K,H]$. The *commutator subgroup* $G' := [G,G]$ of G is generated by the set $\{[x,y] \mid x,y \in G\}$. This subgroup is also known as the derived subgroup of G.

Proposition 2. *The derived subgroup G' of a group G is characteristic (hence normal) in G. Furthermore, for any normal subgroup N in G,*

$$G/N \text{ abelian } \Leftrightarrow G' \subseteq N.$$

In other words, G' is the smallest normal subgroup in G with an abelian factor group.

Proof. To prove that G' is characteristic in G, we show that any automorphism ϕ of G maps elements of the generating set for G', $\{[x,y] \mid x,y \in G\}$, to other elements in the generating set:

$$\phi([x,y]) = \phi(x^{-1}y^{-1}xy) = \phi(x)^{-1}\phi(y)^{-1}\phi(x)\phi(y) = [\phi(x),\phi(y)].$$

Taking ϕ to be conjugation by an element of G verifies that G' is normal.

Let $N \trianglelefteq G$. For any $x,y \in G$,

$$\begin{aligned} G/N \text{ abelian } &\Leftrightarrow xN \cdot yN = yN \cdot xN \Leftrightarrow xyN = yxN \Leftrightarrow x^{-1}y^{-1}xyN = N \\ &\Leftrightarrow [x,y] = x^{-1}y^{-1}xy \in N \Leftrightarrow G' \subseteq N. \end{aligned}$$

□

A nonidentity group with the property $G = G'$ is called *perfect*. For any group G, the *derived series* $\{G^{(i)}\}_{i\in\mathbb{N}}$ is a descending sequence defined as

$$G^{(0)} := G,\ G^{(1)} := G',\ G^{(2)} := [G',G'],\ \ldots\ , G^{(i)} := [G^{(i-1)}, G^{(i-1)}],\ \ldots$$

of successive commutators. If G is finite, then the orders of the groups in this sequence are finite and non-increasing. Hence there exists an integer d such that $G^{(d)} = G^{(d+1)}$, and consequently $G^{(d)} = G^{(s)}$ for all $s \geq d$. Observe that such a $G^{(d)}$ is a perfect group when it contains more than the identity. If $G^{(d)}$ is only the identity $\{1\}$, then the original group G is called *solvable*. The smallest positive integer d for which $G^{(d)} = \{1\}$, is the *derived length* of G. Let G be non-trivial and solvable with derived length d. Then it must be that $G^{(d-1)}$ is abelian since $G^{(d-1)} \cong G^{(d-1)}/\{1\} = G^{(d-1)}/G^{(d)}$ is abelian (Proposition 2). Note that any subgroup of a solvable group is solvable.

Example 1. The commutator subgroup of any abelian group is trivial, so abelian groups are solvable. ⋄

Example 2. Consider D_4, the dihedral group of order 8. What is $D_4' = [D_4, D_4]$? Recall that D_4 has presentation $\langle a,b \mid a^4 = b^2 = (ab)^2 = 1\rangle$. Rather than looking for

- an explicit list of elements of D_4', or
- an explicit list of all commutators $[x,y] = x^{-1}y^{-1}xy$, or
- an explicit shorter list of generators for D_4',

we look for an explicit list of generators of D_4' as a normal subgroup. This list will have to imply that the quotient D_4/D_4' is abelian. Since the generators for D_4 are a and b, the generators of

D_4/D_4' are the cosets $\overline{a}$ and $\overline{b}$. Furthermore, $\overline{a}$ and $\overline{b}$ must commute, so we deduce the relation $[\overline{a},\overline{b}] = \overline{1}$. As a consequence,

$$\overline{[a,b]} = \overline{1} \quad \Rightarrow \quad a^{-1}b^{-1}ab \in D_4' \quad \Rightarrow \quad a^{-2} \in D_4' \quad \Rightarrow \quad a^2 \in D_4'.$$

The second implication follows from the relations in our presentation of D_4: $b^{-1} = b$ and $bab = a^{-1}$. The single relation $[\overline{a},\overline{b}] = \overline{1}$ is sufficient because if the generators of D_4/D_4' commute, then it is abelian.

Thus, D_4' is equal to the smallest subgroup of D_4 generated by a^2 and its conjugates. To compute the conjugates it is enough to consider repeated conjugation of a^2 by the generators of D_4: $(a^2)^a = a^2$ and $(a^2)^b = ba^2b = a^{-2} = a^2$, using the relations cited above. Finally we have that $D_4' = \langle a^2 \rangle = \{1, a^2\}$. Observe that the quotient here is the abelian group $C_2 \times C_2$. Since D_4' is abelian, $D_4'' = \{1\}$, so D_4 is solvable.

A natural generalization is to ask: for which n is D_n solvable? The argument above, with a few modifications, shows that for any n, $D_n' = \langle a^2 \rangle$ and $D_n'' = \{1\}$, so dihedral groups are solvable in general.

If n is odd, $D_n' = \langle a^2 \rangle = \langle a \rangle$, so $[D_n : D_n'] = 2n/n = 2$ and $D_n/D_n' \cong C_2$. If n is even, then $D_n/D_n' \cong C_2 \times C_2$. Indeed, $[D_n : D_n'] = 2n/(n/2) = 4$, and the three nonidentity elements have order 2. The order of $\overline{a}$ and $\overline{b}$ is 2 in D_n/D_n', and from the abelian property of the quotient, the order of their product $\overline{a}\overline{b}$ is the least common multiple of the orders of $\overline{a}$ and $\overline{b}$, which is again 2. $\diamond$

Non-abelian simple groups are perfect, but not all perfect groups are simple. A simple counterexample is $\mathrm{Alt}(5) \times \mathrm{Alt}(5)$ which has three proper normal subgroups: $\mathrm{Alt}(5) \times \{1\}$, $\{1\} \times \mathrm{Alt}(5)$, and the identity $\{1\}$. In each case the quotient is nonabelian, and so $(\mathrm{Alt}(5) \times \mathrm{Alt}(5))' = \mathrm{Alt}(5) \times \mathrm{Alt}(5)$.

Proposition 3. *Let N be a normal subgroup of a group G. If N is solvable and G/N is solvable, then G is solvable.*

Proof. For any subgroup K of G write $\overline{K}$ of the subgroup K/N in G/N. Let c and d be the derived lengths of $G/N = \overline{G}$ and N, respectively, so that:

$$\overline{G} \supseteq \overline{G}' \supseteq \overline{G}'' \supseteq \cdots \supseteq \overline{G}^{(c)} = \{1\} \quad \text{and}$$
$$N \supseteq N' \supseteq N'' \supseteq \cdots \supseteq N^{(d)} = \{1\}.$$

First we show by induction that $\overline{G}^{(i)} = \overline{G^{(i)}}$ for each i. Indeed,

$$\begin{aligned} &\text{Base step, } i = 0: \ \overline{G}^{(0)} = \overline{G} = \overline{G^{(0)}} \\ &\text{Induction step, } i \geq 1: \ \overline{G}^{(i)} = [\overline{G}^{(i-1)}, \overline{G}^{(i-1)}] = [\overline{G^{(i-1)}}, \overline{G^{(i-1)}}] \\ &\qquad\qquad = \overline{[G^{(i-1)}, G^{(i-1)}]} = \overline{G^{(i)}}. \end{aligned}$$

Therefore, the first series above implies that the derived series for G enters N (the pre-image of the identity in $\overline{G}$ under the natural homomorphism) after at most c steps. Combining this conclusion with the second series reveals that the derived series of G includes the identity:

$$G, \ G', \ G'', \ \ldots \ , G^{(c)} \subseteq N, \ G^{(c+1)} \subseteq N', \ \ldots \ , \ G^{(c+d)} \subseteq N^{(d)} = \{1\}.$$

Hence G is solvable with derived length at most $c + d$. $\square$

The *solvable radical* of a finite group G is the largest normal solvable subgroup of G. It was recently proved that the solvable radical of a finite group G is equal to the set of all elements $g \in G$ such that for any $x \in G$, the subgroup generated by g and x is solvable [13]. The solvable radical also occurs and has an important role in the theory of linear groups.

4 Nilpotent Groups

Another important descending sequence for a group G is the *lower central series*:

$$G = \ \gamma_1(G) \supseteq \gamma_2(G) \supseteq \cdots \supseteq \gamma_i(G) \ \ldots$$

where $\gamma_{i+1}(G) := [\gamma_i(G), G] = \langle x^{-1}y^{-1}xy \mid x \in \gamma_i(G), y \in G\rangle$. Note that $\gamma_2(G) = G'$.

Proposition 4. *For each i, $\gamma_i(G)$ is a characteristic subgroup of G.*

Proof. We argue by induction on i. Clearly $\gamma_1(G) = G$ is characteristic in G.

Suppose $\gamma_i(G)$ is characteristic in G for some $i \geq 1$. The generating set for $\gamma_{i+1}(G)$ is $\{[x, g] \mid x \in \gamma_i(G),\ g \in G\}$. Similar to the proof of Proposition 2, we show that any automophism ϕ of G maps elements of this set to other generators. Let $\phi \in \mathrm{Aut}(G)$, $x \in \gamma_i(G)$, and $g \in G$. Then

$$\phi([x, g]) = \phi(x^{-1}g^{-1}xg) = \phi(x)^{-1}\phi(g)^{-1}\phi(x)\phi(g) = [\phi(x), \phi(g)].$$

Since $\gamma_i(G)$ is characteristic, $\phi(x) \in \gamma_i(G)$, so $\phi([x, g])$ is in the generating set for $\gamma_{i+1}(G)$. □

Proposition 5. *The group $\gamma_i(G)/\gamma_{i+1}(G)$ is central in $G/\gamma_{i+1}(G)$, i.e. all of its elements commute with all other elements of the factor group.*

Proof. For any $x \in \gamma_i(G)$ and $g \in G$, $[x, g] \in \gamma_{i+1}(G)$ implies equality between the cosets $(xg)\gamma_{i+1}(G)$ and $(gx)\gamma_{i+1}(G)$ in $G/\gamma_{i+1}(G)$. □

Lemma 5 explains the name "lower central series": each member is central in G modulo its successor. If G is finite, then the orders of the groups $\gamma_i(G)$ are finite and non-increasing. If there exists a d such that $\gamma_{d+1}(G) = \{1\}$, then G said to be *nilpotent*. The *nilpotency class* of a nilpotent group G is the smallest such d, and we write $\mathrm{nc}(G) = d$. Note that nilpotent groups are solvable, and that subgroups of nilpotent groups are also nilpotent.

Example 3. We calculate the lower central series for D_4 and show that D_4 is nilpotent. Indeed,

$$\begin{aligned}
&\gamma_1(D_4) = D_4;\\
&\gamma_2(D_4) = D_4' = \langle a^2\rangle = \{1, a^2\};\\
&\gamma_3(D_4) = [\{1, a^2\}, D_4] = \{1\};
\end{aligned}$$

since, using the relations from Example 2, $a^{-2}a^{-1}a^2a = 1$ and $a^{-2}b^{-1}a^2b = a^2a^{-2} = 1$. The nilpotency class of D_4 is 2.

In general, $\gamma_2(D_n) = D_n' = \langle a^2\rangle$, and to calculate $\gamma_3(D_n) = [\langle a^2\rangle, D_n]$ we use the fact that $\langle a^2\rangle/\gamma_3(D_n)$ is central in $D_n/\gamma_3(D_n)$. The first group is generated by $\overline{a}^2$ and the second by $\overline{a}$ and $\overline{b}$, hence we realize that

$$[\overline{a}^2, \overline{a}] = \overline{1} \quad \text{and} \quad [\overline{a}^2, \overline{b}] = \overline{a}^{-2}\overline{b}^{-1}\overline{a}^2\overline{b} = \overline{a}^{-4}$$

are trivial in $D_n/\gamma_3(D_n)$. The second condition implies $a^4 \in \gamma_3(D_n)$. As before, conjugation of a^4 by a and b gives a^4 and a^{-4}, respectively. Thus, $\gamma_3(D_n) = \langle a^4\rangle$.

Inductively we can show that $\gamma_k(D_n) = \langle a^{2^{k-1}}\rangle$. Indeed, the inductive hypothesis implies that $[\overline{a}^{2^{k-1}}, \overline{b}] = \overline{1}$ in $D_n/\gamma_{k+1}(D_n)$, but this means that $a^{-2^{k-1}}a^{-2^{k-1}} = a^{-2^k} \in \gamma_{k+1}(D_n)$, so also $a^{2^k} \in \gamma_{k+1}(D_n)$. The conjugates remain in $\langle a^{2^k}\rangle$, so this is $\gamma_{k+1}(D_n)$.

Now, the order of a in D_n is n, and $\langle a^{2^k}\rangle = \{1\}$ for some k if and only if the order of a is a power of 2. Hence, the nilpotent dihedral groups are precisely the groups D_n where $n = 2^d$. In this case, the nilpotency class is d. ⋄

A characterization of finite nilpotent groups is given in the following theorem, whose proof is omitted here. See Rotman [21, Theorem 5.39].

Theorem 6. *A finite group G is nilpotent if and only if it is the direct product of its Sylow subgroups. That is*

$$G \text{ nilpotent} \Leftrightarrow G = S_{p_1} \times S_{p_2} \times \cdots \times S_{p_r}, \tag{1}$$

where $p_1, p_2, \ldots, p_r$ are the prime divisors of $|G|$ and S_{p_i} are Sylow subgroups of G.

Finite nilpotent groups can also be characterized in terms of two-variable Engel words [20, Theorem 12.3.4], and there is an analogous description of finite solvable groups [1]. Unlike the Sylow subgroups in the theorem above, Engel words can also be used to study infinite groups, though the characterizations mentioned above for finite nilpotent and finite solvable groups do not carry over to the infinite case [20, § 12.3] .

5 The Fitting Subgroup

Nilpotent subgroups have several important properties given in the Lemmas 7 and 8 that will allow us to construct a group's maximal nilpotent subgroup, called the Fitting subgroup. This subgroup is the nilpotent analogue of the solvable radical and is important in the structural decomposition of a group. It relates, for example, to research questions about infinite polycyclic groups [12, 22, 2], though here it features in the proof of Hölder's formula for finite groups of a square-free order.

Lemma 7. *If G is nilpotent and $N \trianglelefteq G$, then G/N is nilpotent.*

Proof. Let $\overline{G} := G/N$. We will first show by induction that $\overline{\gamma_i(G)} = \gamma_i(\overline{G})$. The base step is clear: $\overline{\gamma_1(G)} = \overline{G} = \gamma_1(\overline{G})$. For the induction step, if $i \geq 2$ then

$$\begin{aligned}
\overline{\gamma_i(G)} &= \overline{[\gamma_{i-1}(G), G]} = \overline{\langle [x,y] \mid x \in \gamma_{i-1}(G),\ y \in G \rangle} \\
&= \langle \overline{[x,y]} \mid x \in \gamma_{i-1}(G),\ y \in G \rangle \\
&= \langle [\overline{x}, \overline{y}] \mid x \in \gamma_{i-1}(G),\ y \in G \rangle \\
&= \langle [a,b] \mid a \in \overline{\gamma_{i-1}(G)},\ b \in \overline{G} \rangle \\
&= \langle [a,b] \mid a \in \gamma_{i-1}(\overline{G}),\ b \in \overline{G} \rangle = \gamma_i(\overline{G}).
\end{aligned}$$

Hence, if $\gamma_{d+1}(G)$ is trivial for some d, then $\gamma_{d+1}(\overline{G}) = \overline{\gamma_{d+1}(G)}$ is also trivial. In addition, this shows that $\mathrm{nc}(\overline{G}) \leq \mathrm{nc}(G)$. □

Now, the product of two subgroups N and M of G is defined to be $NM = \langle ab \mid a \in N, b \in M \rangle = \langle N \cup M \rangle$. If $N \trianglelefteq G$ and M is another subgroup of G, then $NM = \{xy \mid x \in N,\ y \in M\}$. To see why, let $x_1, x_2 \in N$ and $y_1, y_2 \in M$. Then $x_1 y_1 x_2 y_2 = (x_1 x_2^{y_1^{-1}})(y_1 y_2) \in \{xy \mid x \in N, y \in M\}$ since $N \trianglelefteq G$.

Moreover, if both N and M are normal in G, then NM is also normal in G. Indeed, if $g \in G$, $x \in N$, and $y \in M$, then $(xy)^g = g^{-1}xyg = (g^{-1}xg)(g^{-1}yg) = x^g y^g \in NM$ since both subgroups are normal.

Lemma 8. *For normal subgroups A, B, and C, of a group G,*

(i) $[AB, C] = [A, C][B, C]$

(ii) $[A, BC] = [A, B][A, C]$.

Proof. Let a, b, and c be elements of A, B, and C, respectively. Then $[ab, c] = b^{-1}a^{-1}c^{-1}abc = b^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = [a, c]^b[b, c] \in [A, C]^b[B, C]$. Now, both A and C are normal, so $[A, C]^b = [A, C]$, giving the inclusion $[AB, C] \subseteq [A, C][B, C]$. Conversely, $[A, C]$ and $[B, C]$ are both contained in $[AB, C]$, so the product $[A, C][B, C]$ is contained in $[AB, C]$ as well, giving the first result.

The second identity follows from equation (3) and (i):

$$[A, BC] = [BC, A] = [B, A][C, A] = [A, B][A, C].$$

□

This operation of taking products of groups preserves normality and nilpotency, as verified in the next theorem. In proving the result, we will use "left-normed commutators":

$$[X_1, X_2, X_3, \ldots, X_n] := [\ldots[[X_1, X_2], X_3], \ldots, X_n].$$

In this notation, $\gamma_i(G) = [G, G, \ldots, G]$ (i times).

Theorem 9. *If N and M are nilpotent normal subgroups of a group G, then NM is nilpotent and normal in G. Moreover, $nc(NM) \leq nc(N) + nc(M)$.*

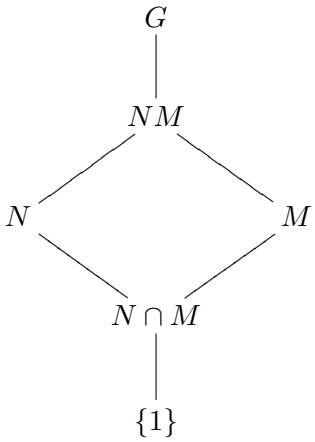
Proof. We already showed that $NM \trianglelefteq G$. Let c and d be the nilpotency classes of M and N, respectively, and let $r = c + d$. Then, applying Lemma 8,

$$\begin{aligned}\gamma_{r+1}(MN) &= [MN, MN, \ldots, MN] \\ &= \prod [X_1, X_2, \ldots, X_{r+1}],\end{aligned}$$

where the product includes all tuples

$$(X_1, X_2, \ldots, X_{r+1}) \in \{M, N\}^{r+1} = \{M, N\}^{c+d+1}.$$

In each term, either at least $c{+}1$ of the X_i's are equal to M or at least $d{+}1$ of them are equal to N. In the first case, the corresponding group is contained in $\gamma_{c+1}(M) = \{1\}$; in the second case, it is contained in $\gamma_{d+1}(N) = \{1\}$. Therefore, $\mathrm{nc}(NM) \leq c + d = \mathrm{nc}(N) + \mathrm{nc}(M)$.



□

Using this result, we can find a unique maximal nilpotent normal subgroup $F(G)$ in a finite group G, which is referred to as the *Fitting subgroup* of G. Equivalently, $F(G)$ is the subgroup generated by the maximal normal p-subgroups of a finite group G, where p runs over all prime divisors of $|G|$.

Theorem 10. *If G is a finite solvable group, then $C_G(F(G)) = Z(F(G))$.*

Proof. For convenience, let $F = F(G)$, $C = C_G(F(G))$, and $Z = Z(F(G))$. Now, $Z \trianglelefteq C$ and $Z \trianglelefteq G$. The former follows since $Z \leq F$ and elements in C commute with those in F. To see why $Z \trianglelefteq G$, let $z \in Z$, $f \in F$, and $g \in G$. Because F is normal in G, z^g and $f_1 := f^{g^{-1}}$ belong to F. Meanwhile, $z^g \in C$ since

$$z^g f = g^{-1}zgfg^{-1}g = g^{-1}zf_1g = g^{-1}f_1zg = g^{-1}f_1gg^{-1}zg = fz^g.$$

Thus, $z^g \in C \cap F = Z$.

Suppose, for a contradiction, that Z is strictly contained in C and let M/Z be a minimal nontrivial normal subgroup of G/Z that is contained in C/Z. Since G is solvable, M/Z is solvable.

We show that $(M/Z)' \trianglelefteq G/Z$. Since M/Z is normal in G/Z, conjugation by an element $g \in G/Z$ is an automorphism of M/Z. Also, $(M/Z)'$ is characteristic in M/Z (Proposition 2) , so conjugation by g maps $(M/Z)'$ to itself.

Therefore, $(M/Z)' \trianglelefteq G/Z$. By the minimality of M/Z, $(M/Z)'$ must equal either 1 or M/Z. But M/Z is solvable, so $(M/Z)' = 1$ equivalently $M' \leq Z$. Since $M \subseteq C$ and $M' \subseteq Z \subseteq F$, we have that $\gamma_3(M) = [M', M] \subseteq [C, F] = 1$.Therefore M nilpotent and normal in G, which implies that $M \subseteq F$ from the definition of the Fitting subgroup. But $M \leq C$, so $M \subseteq C \cap F = Z$. Then M/Z is trivial, contradicting the choice of M. This means that there are no nontrivial normal subgroups between Z and C, giving the result $Z = C$. □

6 Split Extensions

Let H and K be groups. The *direct product* $H \times K$ of H and K is the set of ordered pairs $\{(h, k) \mid h \in H, k \in K\}$ with operation $(h_1, k_1)\cdot(h_2, k_2) = (h_1 \cdot h_2,\ k_1 \cdot k_2)$. In terms of presentations, if

$$H = \langle h_1, h_2, \dots \mid r_1, r_2, \dots \rangle \text{ and } K = \langle k_1, k_2, \dots \mid s_1, s_2, \dots \rangle,$$

then a presentation for $H \times K$ is

$$\langle h_1, h_2, \dots, k_1, k_2, \dots \mid r_1, r_2, \dots, s_1, s_2, \dots, h_ik_j = k_jh_i \text{ for all } i, j\rangle.$$

More generally, let $\phi : H \to \mathrm{Aut}(K)$ be a homomorphism[2]. The *semidirect product* $H \ltimes K$ with respect to ϕ is defined as the set $\{(h, k) \mid h \in H, k \in K\}$ with operation $(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot h_2,\ k_1^{\phi(h_2)} \cdot k_2)$.

If $G = H \ltimes K$, then G is also known as a *split extension* of K by H and sometimes the notation $G = H : K$ appears. By means of the natural embeddings $K \to G$, $k \mapsto (1, k)$, and $H \to G$, $h \mapsto (h, 1)$ we may regard K and H as subgroups of G. Then K is a normal subgroup of G, H is a subgroup of G disjoint from K except for the identity, and H and K generate the entire group G. The subgroup H is called a *complement* of K in G, while the normal subgroup K is called a *normal complement* of H in G.

[2]A remark on notation: here ϕ is written on the left as $\phi(h)$, while elements in $\mathrm{Aut}(K)$ are written on the right, so if $\sigma \in \mathrm{Aut}(K)$, then we write k^σ for the image of k under σ.

Note that extensions of groups need not be split. If K is a normal subgroup of group G, then K may or may not admit a complement[3] in G.

Theorem 11 (Schur-Zassenhaus Lemma, 1973)**.** *Let K be a normal subgroup in G. If $[G : K]$ and $|K|$ are coprime, then K has a complement H in G. That is, G is a split extension of K by H.*

We will not prove or use this result, only mention it briefly later. See [21, Theorem 7.41] for a proof.

Example 4. The alternating group of degree 4, Alt(4), is isomorphic to $C_3 \ltimes (C_2 \times C_2)$. Indeed, we may take

$$H = \{(1), (123), (132)\} \cong C_3,$$
$$K = \{(1), (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2.$$

In this case, K is isomorphic to the Klein four group. For convenience, we will write $K \cong \{e, i, j, k\}$ so that

$$\mathrm{Aut}(K) = \{(1), (ij), (ik), (jk), (ijk), (ikj)\} \leq \mathrm{Sym}(K).$$

Since elements of order 3 in H must be mapped to elements of order 3 or the identity in $\mathrm{Aut}(K)$, there are three possibilities for $\phi : H \to \mathrm{Aut}(K)$, namely

- The trivial homomorphism $\phi_1((1)) = \phi_1((123)) = \phi_1((132)) = (1)$ which leads to $C_3 \times (C_2 \times C_2) \cong C_6 \times C_2$.
- $\phi_2((1)) = (1)$, $\phi_2((123)) = (ijk)$, $\phi_2((132)) = (ikj)$.
- $\phi_3((1)) = (1)$, $\phi_3((123)) = (ikj)$, $\phi_3((132)) = (ijk)$.

Relabeling of i as j and j as i reveals that ϕ_2 and ϕ_3 lead to isomorphic groups. In fact, ϕ_2 is the correct one for our choice of K since $i^{\phi((123))} = (123)^{-1}[(12)(34)](123) = (13)(24) = k = i^{\phi_3((123))}$. $\diamond$

Example 5. The dihedral group D_n of order $2n$ is the semidirect product $C_2 \ltimes C_n$ of cyclic groups. The homomorphism ϕ from $C_2 = \{1, \sigma\}$ to $\mathrm{Aut}(C_n) \cong U(n)$ sends σ to multiplication by -1.

For example, if $n = 5$, then D_5 is the group of symmetries of a regular pentagon. The normal subgroup isomorphic to C_5 is the set of rotations $\{R_0, R_\alpha, R_{2\alpha}, R_{3\alpha}, R_{4\alpha}\}$, where $\alpha = \frac{2\pi}{5} = 72°$. The image of σ under homomorphism ϕ is the automorphism that sends R_α to $R_{-\alpha} = R_{4\alpha}$. The geometric interpretation of multiplication by -1 is reflection across an axis between an vertex and the midpoint of the opposite side. $\diamond$

7 The Transfer Homomorphism

Suppose we want to know whether a group G is solvable. Clearly we must search for a proper, nontrivial normal subgroup in G (unless $G \cong C_p$). If G can be written as the split extension of a normal subgroup K by a complement Q, then according to Proposition 3, we can reduce to studying K and $Q \cong G/K$. Therefore, a common strategy to prove that a group is solvable is to begin with an accessible subgroup Q and, if possible, construct a homomorphism from G to Q, whose kernel will be a normal complement of Q in G. This homomorphism is known as the *transfer*. For the next few results, let Q be a subgroup of G with finite index n.

[3] In infinite polycyclic groups one finds *almost complements* and *almost split extensions*

Lemma 12. *Let $\{l_1, \ldots, l_n\}$ and $\{h_1, \ldots, h_n\}$ be two left coset representatives of Q in G. For any fixed $g \in G$ and each $i \in \{1, ..., n\}$, there is a unique $\sigma(i) \in \{1, .., n\}$ and a unique $x_i \in Q$ such that $gh_i = l_{\sigma(i)}x_i$. Moreover, σ is a permutation of $\{1, ..., n\}$ (i.e. $\sigma \in \mathrm{Sym}(n)$).*

Proof. The left cosets partition G, so gh_i is contained in exactly one left coset l_jQ. Hence $\sigma(i) = j$ and $x_i = l_j^{-1}gh_i \in Q$ are unique such that $gh_i = l_{\sigma(i)}x_i$.

To prove that σ is a permutation, note that it is a map from the finite set $\{1, \ldots, n\}$ to itself, so it is enough to prove that σ is injective. Suppose $\sigma(i) = \sigma(k) = j$. Then $gh_i = l_jx_i$ and $gh_k = l_jx_k$, which implies

$$gh_ix_i^{-1} = gh_kx_k^{-1} \Rightarrow h_i^{-1}h_k = x_i^{-1}x_k \in Q \Rightarrow h_iQ = h_kQ \Rightarrow i = k.$$

□

In the case where the two coset representatives are the same ($l_i = h_i$ for all $i \in \{1, ..., n\}$), the previous lemma guarantees a unique x_i such that $x_i = l_{\sigma(i)}^{-1}gl_i$ for each $g \in G$ and $i \in \{1, ..., n\}$. With this x_i in mind, define the function $V : G \to Q/Q'$ where

$$V(g) = \prod_{i=1}^{n} x_iQ'.$$

This function is known as the *transfer* [4].

Proposition 13. *The transfer function V is a homomorphism whose definition does not depend on the choice of a left transversal of Q in G.*

Proof. Let $\{l_1, ..., l_n\}$ and $\{h_1, ..., h_n\}$ be two left coset representatives of Q in G. By Lemma 12, for each $g \in G$ we have x_i, $y_i \in Q$ and σ, $\tau \in \mathrm{Sym}(n)$ such that

$$gl_i = l_{\sigma(i)}x_i \qquad gh_i = h_{\tau(i)}y_i$$

To prove that the transfer is independent of the choice of left transversal, we shall show that

$$\prod_{i=1}^{n} x_iQ' = \prod_{i=1}^{n} y_iQ'.$$

Setting $g = 1$ in Lemma 12, we have $\alpha \in \mathrm{Sym}(n)$ and $z_i \in Q$ such that $h_i = l_{\alpha(i)}z_i$ forall i. Fix i. Define $j := \alpha^{-1}\sigma\alpha(i)$ so $h_j = l_{\sigma\alpha(i)}z_j$. Then

$$gh_i = gl_{\alpha(i)}z_i = l_{\sigma\alpha(i)}x_iz_i = h_jz_j^{-1}x_iz_i$$

By the uniqueness assertion in Lemma 12 and the definition of j,

$$j = \tau i \quad \text{and} \quad y_i = z_j^{-1}x_iz_i = z_{\alpha^{-1}\sigma\alpha(i)}^{-1}x_iz_i.$$

Consider

$$\prod_{i=1}^{n} y_iQ' = \prod_{i=1}^{n} z_{\alpha^{-1}\sigma\alpha(i)}^{-1}x_iz_iQ'.$$

[4]The letter V abbreviates the original German term $Verlagerung$.

The order of multiplication is irrelevant since Q/Q' is abelian. Furthermore, $\alpha^{-1}\sigma\alpha$ is a permutation of $\{1,\dots,n\}$, so the inverse of each z_i appears and cancels z_i. Hence,

$$\prod_{i=1}^{n} y_i Q' = \prod_{i=1}^{n} x_i Q'$$

as desired. Hence the definition of V does not depend on the choice of left transversal.

To prove that V is a homomorphism, let $g, g' \in G$ and let x_i and y_i be the unique elements in Q such that $x_i = l_{\sigma(i)}^{-1} g l_i$ and $y_i = l_{\tau(i)}^{-1} g' l_i$. Then

$$gg' l_i = g l_{\tau(i)} y_i = l_{\sigma\tau(i)} x_{\tau(i)} y_i.$$

Using the facts that Q/Q' is abelian and that $\tau \in \mathrm{Sym}(n)$,

$$V(gg') = \prod_{i=1}^{n} x_{\tau(i)} y_i Q' = \left(\prod_{i=1}^{n} x_{\tau(i)} Q'\right)\left(\prod_{i=1}^{n} y_i Q'\right) = \left(\prod_{i=1}^{n} x_i Q'\right)\left(\prod_{i=1}^{n} y_i Q'\right).$$

Thus V is a homomorphism. □

Lemma 14. *Let Q be a subgroup of G with finite index n and left coset representatives $\{l_1,\dots,l_n\}$. For any fixed $g \in G$, there exist $m \in \mathbb{N}$; $h_1,\dots,h_m \in G$; and positive integers $n_1,\dots,n_m$ with*

(i) *$h_i \in \{l_1,\dots,l_n\}$ for all i;*

(ii) *$h_i^{-1} g^{n_i} h_i$ belongs to Q;*

(iii) *$\sum_{i=1}^{m} n_i = n$; and*

(iii) *$V(g) = \prod_{i=1}^{m} (h_i^{-1} g^{n_i} h_i) Q'$.*

Proof. Lemma 12 provides unique $\sigma \in \mathrm{Sym}(n)$ and unique $x_s \in Q$ such that $x_s = l_{\sigma(s)}^{-1} g l_s$ for all $s \in \{1,\dots,n\}$. Factorize σ as the product of disjoint cycles, including a 1-cycle for each fixed point: $\sigma = \alpha_1 \dots \alpha_m$. Then for a fixed $i \in \{1,\dots,m\}$, the cycle α_i is of the form[5] $(j_1,\dots,j_r)$ and

$$\begin{aligned} & x_{j_1} = l_{\sigma(j_1)}^{-1} g l_{j_1}, \quad x_{j_2} = l_{\sigma(j_2)}^{-1} g l_{j_2}, \quad \dots, \quad x_{j_r} = l_{\sigma(j_r)}^{-1} g l_{j_r} \\ \Rightarrow\ & x_{j_1} = l_{j_2}^{-1} g l_{j_1}, \quad x_{j_2} = l_{j_3}^{-1} g l_{j_2}, \quad \dots, \quad x_{j_r} = l_{j_1}^{-1} g l_{j_r} \\ \Rightarrow\ & x_{j_r} \dots x_{j_2} x_{j_1} = (l_{j_1}^{-1} g l_{j_r}) \dots (l_{j_3}^{-1} g l_{j_2})(l_{j_2}^{-1} g l_{j_1}) = l_{j_1}^{-1} g^r l_{j_1}, \end{aligned}$$

which is in Q. Define $h_i := l_{j_1}$ and $n_i := r$. Then (i) and (ii) follow immediately. The sum of the n_i's is the sum of the length of the cycles of σ – a permutation of n elements. Hence, (iii) holds. Finally, to show (iv),

$$\begin{aligned} \prod_{i=1}^{m} (h_i^{-1} g^{n_i} h_i) Q' &= \prod_{i=1}^{m} (l_{j_1}^{-1} g^r l_{j_1}) Q' = \prod_{i=1}^{m} x_{j_r} \dots x_{j_2} x_{j_1} Q' \\ &= \prod_{i=1}^{m} \prod_{k=1}^{n_i} x_{j_k} Q' = \prod_{s=1}^{n} x_s Q' = V(g), \end{aligned}$$

where each s corresponds to one of $\sum_{i=1}^{m} n_i = n$ combinations of i and k, i.e. one for each coset of Q. The final equality holds because the product includes all the x_s's of the necessary form. □

[5] The j's and r depend on i, but additional notation is omitted.

Corollary 15. *Let Q be a subgroup of G of finite index n. If $Q \leq Z(G)$, then $V(g) = g^n$ for all $g \in G$.*

Proof. Any subgroup of the center is normal (see Section 2), so Q is a normal subgroup of G. Also, Q' is trivial because Q is abelian, and we may regard the transfer as a homomorphism $V : G \to Q$. If $g, h \in G$ satisfy $h^{-1}g^r h \in Q$ for some integer r, then $g^r = h(h^{-1}g^r h)h^{-1} \in Q$ since Q is normal. But Q is in the center, so $h^{-1}g^r h = g^r$.

By parts (iii) and (iv) of Lemma 14,

$$V(g) = \prod_{i=1}^{m} h_i^{-1} g^{n_i} h_i = \prod_{i=1}^{m} g^{n_i} = g^{\sum_{i=1}^{m} n_i} = g^n.$$

□

We now turn our attention to Sylow subgroups.

Proposition 16. *Let Q be a Sylow subgroup of a finite group G, and let h and k be elements of $C_G(Q)$. If h and k are conjugate in G, then they are conjugate in $N_G(Q)$.*

Proof. Suppose $k = g^{-1}hg$ for some $g \in G$. Then $k \in g^{-1}C_G(Q)g$. Now,

$$\begin{aligned} g^{-1}C_G(Q)g &= \{g^{-1}ag \in G \mid a \in G \text{ and } ax = xa \text{ for all } x \in Q\} \\ &= \{b \in G \mid gbg^{-1}x = xgbg^{-1} \text{ for all } x \in Q\} \\ &= \{b \in G \mid bg^{-1}xg = g^{-1}xgb \text{ for all } x \in Q\} \\ &= \{b \in G \mid by = yb \text{ for all } y \in g^{-1}Qg\} \\ &= C_G(g^{-1}Qg). \end{aligned}$$

Hence, $k \in C_G(g^{-1}Qg)$. By hypothesis, $Q \subseteq C_G(k)$ and now we have shown that $g^{-1}Qg \subseteq C_G(k)$. Since conjugation is an automorphism, $|g^{-1}Qg| = |Q|$; thus, both groups are Sylow subgroups of $C_G(k)$. By the third Sylow Theorem (see [11, Theorem 24.5]), there exists a $c \in C_G(k)$ such that $Q = c^{-1}g^{-1}Qgc$. Then $gc \in N_G(Q)$ and $c^{-1}g^{-1}hgc = c^{-1}kc = k$. □

Theorem 17 (Burnside, 1900)**.** *Let G be a finite group and let Q be an abelian Sylow subgroup with the property that $Q \leq Z(N_G(Q))$, i.e. Q is contained in the center of its normalizer. Then Q has a normal complement K in G.*

Proof. Since Q is abelian, $Q' = \{1\}$ and we may regard the transfer as a homomorphism $V : G \to Q$. We will show that V is surjective and that $K = \ker(V)$ is the desired complement.

Let $g \in Q$. Then, using Lemma 14,

$$V(g) = \prod_{i=1}^{m} h_i^{-1} g^{n_i} h_i$$

with

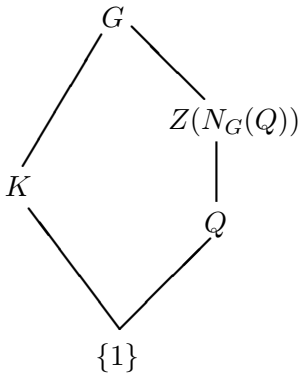
$$h_i^{-1} g^{n_i} h_i \in Q$$

for all $i \in \{1, \ldots, m\}$. For any i, g^{n_i} and $h_i^{-1}g^{n_i}h_i$ are elements of Q which are conjugate in Q. Note that g^{n_i} and $h_i^{-1}g^{n_i}h_i$ belong to $C_G(Q)$. This is because Q is abelian, and hence $Q \leq C_G(Q)$. By Proposition 16, g^{n_i} and $h_i^{-1}g^{n_i}h_i$ are already conjugate in $N_G(Q)$, i.e. there exists $c_i \in N_G(Q)$

with $h_i^{-1} g^{n_i} h_i = c_i^{-1} g^{n_i} c_i$. But $Q \leq Z(N_G(Q))$, so g^{n_i} commutes with c_i and, combining several steps,

$$V(g) = \prod_{i=1}^{m} h_i^{-1} g^{n_i} h_i = \prod_{i=1}^{m} c_i^{-1} g^{n_i} c_i = \prod_{i=1}^{m} g^{n_i} = g^{\sum_{i=1}^{m} n_i} = g^n,$$

where $n = [G : Q]$, as before. Let $|Q| = q$. Then $\gcd(n, q) = 1$, since Q is a Sylow subgroup. There are integers a and b such that $an + bq = 1$. V is surjective because for any $g \in Q$, we have that $g = g^{an+bq} = g^{an} g^{bq} = (g^a)^n = V(g^a)$.



By the First Isomorphism Theorem, $G/K \cong Q$. It remains to show that $K \cap Q$ is trivial. Indeed, as seen above, V restricted to Q is exponentiation by n. Since n is relatively prime to $q = |Q|$, this shows that V restricted to Q is injective, hence $K \cap Q = 1$. We conclude that $G = Q \ltimes K$ and K is the desired complement of Q in G. □

Theorem 18. *Let G be a finite group, and let p be the smallest prime divisor of $|G|$. Let Q be a Sylow p-subgroup of G. If Q is cyclic, then Q has a normal complement in G.*

Proof. Let $N = N_G(Q)$ and $C = C_G(Q)$. From Proposition 1, $C \trianglelefteq N$ and N/C is isomorphic to a subgroup of $\mathrm{Aut}(Q)$. What can we say about $|N/C|$?

Say $|Q| = p^m$ for some m. Then $\mathrm{Aut}(Q) \cong U(p^m)$ because Q is cyclic (see Section 2), and it is easy to show that $|U(p^m)| = p^{m-1}(p-1)$. Thus, $|N/C|$ divides $p^{m-1}(p-1)$. Since Q is abelian, $Q \leq C$ and Q is the Sylow p-subgroup of C. Hence p does not divide $|N/C|$ and so $|N/C|$ divides $p - 1$. Finally, $N \leq G$, and therefore $|N/C| = |N|/|C|$ divides $|G|$. But p is the smallest prime divisor of $|G|$; therefore $|N/C| = 1$, which means $N = C$.

Because Q is abelian, $Q \leq Z(C)$, which implies $Q \leq Z(N)$. By Theorem 17, Q has a normal complement in G. □

Corollary 19. *Let G be a finite group, and let p be the smallest prime divisor of $|G|$. Let Q be a Sylow p-subgroup of G. If Q is cyclic, then G is a split extension of a normal subgroup by Q.*

8 Groups of a Square-Free Order

As mentioned in the Introduction, it is a difficult task in general to determine $f(n)$, the number of groups of finite order n. In this section, we restrict our attention to cases when n is *square-free*. In

other words, $n = p_1 p_2 \cdots p_r$ where the p_i's are distinct primes. This is a very special situation of the broader problem, and lends itself to relatively straightforward results, most notably Hölder's formula. We begin with an algebraic classification of groups whose order is the product of two primes, then prove two general results for groups of square-free order before considering Hölder's formula.

Example 6: Classification of groups with order *pq*. For the case when $r = 2$, denote $p := p_1$ and $q := p_2$ with $p < q$. By the third Sylow Theorem, the number of Sylow q-subgroups of G has the form $qa + 1$ for some integer a with $qa + 1$ dividing the order of the group. Thus $qa + 1$ must equal one of 1, p, q, or pq, the divisors of pq. But since $q > p$, it follows that there is precisely one (normal) Sylow q-subgroup. (We will see below by a different argument that in a group G of square-free order, the largest prime divisor of the order of the group always has a unique Sylow subgroup.)

Similarly, the number of p-subgroups of G has the form $pa + 1$ for some integer a with $pa + 1$ dividing the order of the group. Thus $pa + 1$ must equal one of 1, p, q, or pq, the divisors of pq. Here we have two cases: (i) p divides $q - 1$ and (ii) p does not divide $q - 1$.

In the second case, $a = 0$ is the only possibility, and G has only one Sylow p-subgroup. Both Sylow subgroups are normal as a consequence of the third Sylow Theorem, and both are cyclic, so let x and y be a their respective generators. Also note that their intersection $\langle x \rangle \cap \langle y \rangle$ is trivial. But

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}(x^y) \in \langle x \rangle,$$
$$[x, y] = x^{-1}y^{-1}xy = (y^x)y \in \langle y \rangle.$$

So $[x, y] = \{1\}$. Therefore, $xy = yx$ so the order of xy is pq, the product of the orders of x and y. Hence G is cyclic and $f(pq) = 1$ when $p < q$ and p does not divide $q - 1$.

In the other case, if p divides $q - 1$ then $f(pq) = 2$. This is because there is either 1 Sylow p-subgroup, which leads to the cyclic group of order pq, as above; or there are q Sylow p-subgroups.

Extensions give another approach to classify groups with order pq. Since there is a unique normal Sylow q-subgroup S_q, we may regard G as the extension of S_q by a Sylow p-subgroup S_p. To determine the isomorphism class, we must specify a corresponding map $\phi : S_p \to \mathrm{Aut}(S_q)$. One option is that ϕ maps S_p to the identity, and this possibility gives the cyclic group C_{pq}. The other possibility is for the image of S_p in $\mathrm{Aut}(S_q)$ to be a subgroup of size p. Since $\mathrm{Aut}(S_q) \cong \mathrm{Aut}(C_q) \cong U(q)$ is cyclic of order $q - 1$, it has a subgroup of order p if and only if p divides $q - 1$. This subgroup of order p, if it exists, is unique in $\mathrm{Aut}(S_q)$. Since it has several generators, the group S_p can be mapped to it in different ways, but up to composition with an automorphism of S_p there is only one choice. Therefore, if p divides $q - 1$, there is a second non-abelian isomorphism class for groups of order pq in addition to the cyclic one. $\diamond$

Let G be a group of square-free order n. All Sylow subgroups have prime order and are therefore cyclic. Also, if G is abelian, it must be the product of cyclic groups of prime order by the Fundamental Theorem of Finite Abelian Groups [11, Theorem 11.1]. Hence G is abelian if and only if it is cyclic.

Before continuing the classification of groups of square-free order, we now prove that such groups are solvable (a result due to Frobenius [10]) and that they are so-called Sylow tower groups.

Proposition 20. *Every group of square-free order is solvable.*

Proof. Let p be the smallest prime divisor of $|G|$ with S_p a Sylow p-subgroup of G. Then S_p is cyclic, solvable, and has a normal complement K in G (Theorem 18). Then $|K|$ is square-fee, and,

by induction on the order of the group, K is solvable. Also, $G/K \cong S_p$ is solvable, so by Proposition 3, G is solvable. □

We remark that this proposition is consistent with the Classification of Finite Simple Groups. In particular, from the classification one can deduce that 4 divides the order of any non-abelian finite simple group[6]. Let G be a group of square-free order. Clearly 4 cannot divide $|G|$. So if G is simple, G must be abelian and hence solvable. If G is not simple, it has a proper normal subgroup N such that $|G/N|$ and $|N|$ are square-free, and it follows by induction that G is solvable.

If G is abelian with square-free order it may be simple (e.g. $G \cong C_p$ for a prime p) but it is solvable (Example 1). Clearly 4 cannot divide the square-free order of G, so a nonabelian group of square-free order isn't simple. Thus it has a normal subgroup whose factor group has square-free order and the result follows by induction.

A finite group G is a *Sylow tower group* if there exists a series of normal subgroups of G

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\},$$

such that G_{i-1}/G_i is a Sylow p_i-subgroup of G/G_i where p_i is the largest prime divisor of $|G/G_i|$.

Theorem 21. *Groups of square free order are Sylow tower groups.*

Proof. Let $|G| = p_1 p_2 \cdots p_r$ with $p_i < p_{i+1}$. By Theorem 18 a Sylow p_1-subgroup S_{p_1} has a normal complement G_1 in $G = G_0$, with $|G_1| = p_2 \cdots p_r$. Similarly, the Sylow p_2-subgroup of G_1 has a normal complement G_2 in G_1, with $|G_2| = p_3 p_4 \cdots p_r$. For $i = 1, \ \ldots \ , r-1$ define G_i to be the normal complement of the Sylow p_i-subgroup of G_{i-1}, where $G_0 := G$. Then $G_i \trianglelefteq G_{i-1}$ and in particular $G_1 \trianglelefteq G_0 = G$. Also, $|G_i| = p_{i+1} p_{i+2} \ldots p_r$. We prove by induction that $G_i \trianglelefteq G$.

Suppose G_{i-1} is normal in G for some $i \geq 1$. Then conjugation by $g \in G$ is an automorphism of G_{i-1}. Therefore, the image of G_i under conjugation by $g \in G$, denoted $\gamma_g(G_i)$, is a subgroup of G_{i-1} with order $p_{i+1} p_{i+2} \ldots p_r$. Now consider $\gamma_g(G_i)G_i/G_i$, the corresponding subgroup of G_{i-1}/G_i. The order of the subgroup $\gamma_g(G_i)G_i/G_i$ must divide $p_{i+1} p_{i+2} \ldots p_r$ (the order of $\gamma_g(G_i)$ in G_{i-1}) as well as p_i (the order of the group G_{i-1}/G_i). But $\gcd(p_{i+1} p_{i+2} \ldots p_r, \ p_i) = 1$ implies that $\gamma_g(G_i)G_i/G_i$ is trivial, hence $\gamma_g(G_i) \subseteq G_i$. Since this is true for all $g \in G$, G_i is normal in G for $i \in \{1, 2, \ \ldots \ r-1\}$.

For each i, $1 \leq i \leq r$, p_i is the largest prime divisor of $|G/G_i| = p_1 p_2 \cdots p_i$, while $|G_{i-1}/G_i| = p_i$. Hence G_{i-1}/G_i is the Sylow p_i-subgroup of G/G_i and the result follows. □

The proof of the theorem shows that for the largest prime factor p of $|G|$, the Sylow p-subgroup S_p is unique in G. Also, one can algebraically build groups of square-free order as iterated split extensions by cyclic groups of prime order.

Finally, we turn our attention to Hölder's classical result [15]:

Theorem 22 (Hölder, 1895)**.** *The number of groups of order n, where n is square-free is given by*

$$f(n) = \sum_{m|n} \prod_{p} \frac{p^{c(p)} - 1}{p - 1}$$

where p runs over all prime divisors of n/m and $c(p)$ is the number of prime divisors q of m that satisfy $q \equiv 1 \pmod{p}$.

[6]By the Feit-Thompson Theorem, 2 divides the order of any non-abelian finite simple group, so groups of odd order are not simple.

Suppose G is a non-abelian group such that 2 divides its order but 4 does not. Then its Sylow 2-subgroup is cyclic and has a normal complement in G by Theorem 18. Hence G is not simple. Another way to arrive at this result is to show that the set of elements of G with odd order form a normal subgroup.

We explain the derivation of this formula expanding on the comments given by Blackburn *et al.* [3]. Let G be a group of square-free order n and let m be the order of the Fitting subgroup $F(G)$. Since $F(G)$ is nilpotent, it is the product of its Sylow subgroups by Theorem 6. But these are all cyclic and their orders are distinct primes, so $F(G)$ is cyclic by the Chinese Remainder Theorem. Moreover, $\gcd(F(G), [G : F(G)]) = 1$ since $|G|$ is square-free. By Theorem 11, $F(G)$ has a complement $H \cong G/F(G)$ and G can be regarded as a split extension $F(G)$ by H. This shows that G is a split metacyclic group. We will give a direct proof which also shows that H is cyclic.

Lemma 23. *In a group G of square-free order, $F(G)$ admits a cyclic complement H.*

Proof. By the above comments, $F(G)$ is cyclic and, in particular, $\mathrm{Aut}(F(G))$ is abelian. Let $\gamma_g : F(G) \to F(G)$ denote conjugation by $g \in G$ — an automorphism since $F(G)$ is a normal subgroup of G. Consider the map $\phi : G \to \mathrm{Aut}(F(G))$ with $g \mapsto \gamma_g$. The kernel of ϕ is

$$\{g \in G \mid x = g^{-1}xg \text{ for all } x \in F(G)\} = C_G(F(G)) = Z(F(G)) = F(G),$$

the penultimate equality following from Theorem 10 (G is solvable). Hence $G/F(G)$ is isomorphic to a subgroup of the abelian group $\mathrm{Aut}(F(G))$. This makes $G/F(G)$ abelian, and it is also cyclic since it is of square-free order (see above).

Choose an element $g \in G$ such that $G/F(G) = \langle \overline{g} \rangle$. As $G/F(G)$ and $F(G)$ have coprime orders we may replace g by a suitable power of g so that $\langle g \rangle \cap F(G) = 1$. Then $H = \langle g \rangle$ is the desired complement of $F(G)$ in G. □

Since $F(G)$ is cyclic, $C_G(F(G)) = F(G)$ (Theorem 10) and $\mathrm{Aut}(F(G))$ is abelian. Consider a map ϕ from H to $\mathrm{Aut}(F(G))$ in which h is mapped to conjugation by h, denoted $\gamma_h : F(G) \to F(G)$. The map ϕ is injective since its kernel is trivial:

$$\begin{aligned} h \in \ker \phi \;&\Leftrightarrow \gamma_h = \mathrm{id} \;\Leftrightarrow\; h^{-1}xh = x \text{ for all } x \in F(G) \\ &\Leftrightarrow h \in C_G(F(G)) = F(G) \;\Leftrightarrow\; h \in F(G) \cap H = \{1\}. \end{aligned}$$

Hence G embeds into the holomorph $\mathrm{Aut}(F(G)) \ltimes F(G)$. We need to understand the isomorphism classes of certain subgroups of this holomorph.

Proposition 24. *Suppose K is a finite cyclic group (equivalently K is abelian with $\mathrm{Aut}(K)$ abelian). Let H_1 and H_2 be subgroups of $\mathrm{Aut}(K)$, and consider $H_1 \ltimes K$ and $H_2 \ltimes K$ as subgroups of $\mathrm{Aut}(K) \ltimes K$. Then an isomorphism*

$$\phi : H_1 \ltimes K \xrightarrow{\cong} H_2 \ltimes K \quad \text{with } \phi(K) = K$$

exists if and only if $H_1 = H_2$.

Proof. "⇐" : trivial.
"⇒" : Conversely, suppose there exists an isomorphism

$$\phi : H_1 \ltimes K \xrightarrow{\cong} H_2 \ltimes K \quad \text{with } \phi(K) = K.$$

Step 1: We may assume that $\phi|_K = \mathrm{id}_K$.
Subproof. Write $\alpha := \phi|_K \in \mathrm{Aut}(K)$, and consider

$$\tilde{\phi} : H_1 \ltimes K \xrightarrow{\phi} H_2 \ltimes K \xrightarrow{\psi} \alpha H_2 \alpha^{-1} \ltimes K$$

where $\psi(h,k) = (\alpha h \alpha^{-1}, k^{\alpha^{-1}})$. As $\mathrm{Aut}(K)$ is abelian, we have $\alpha H_2 \alpha^{-1} = H_2$. Moreover, $\tilde{\phi} : H_1 \ltimes K \overset{\cong}{\to} H_2 \ltimes K$ with $\tilde{\phi}|_K = \mathrm{id}_K$, for $\tilde{\phi}(k) = \psi(\phi(k)) = (k^\alpha)^{\alpha^{(-1)}} = k$.

Step 2: For $h \in H_1$ we have $\phi(h) = \psi(h) \cdot x_h$ where

$$\psi : H_1 \hookrightarrow H_1 \ltimes K \overset{\phi}{\to} H_2 \ltimes K \overset{\mathrm{proj}}{\to} H_2$$

and $x_h \in K$. Since K is abelian we deduce that $k^h = \phi(k^h) = (\phi(k))^{\phi(h)} = k^{\psi(h)x_h} = k^{\psi(h)}$ for all $k \in K$. Thus $h = \psi(h)$, and consequently $H_1 = H_2$. □

Therefore the isomorphism class of the extension $G = H \ltimes F(G)$ is determined by the image of H in $\mathrm{Aut}(F(G))$. In other words, the number of nonisomorphic groups of square-free order n whose Fitting subgroup has order m is the number of distinct groups of size n/m in $\mathrm{Aut}(F(G)) \cong U(m)$. Now, write $m = q_1 q_2 \dots q_k$ where each distinct prime q_j equals p_i for some i. Then, using the Chinese Remainder Theorem,

$$\begin{aligned}\mathrm{Aut}(F(G)) &\cong U(m) \cong U(q_1) \times U(q_2) \times \cdots \times U(q_k) \\ &\cong C_{q_1-1} \times C_{q_2-1} \times \cdots \times C_{q_k-1}.\end{aligned}$$

Suppose p divides n/m. How many subgroups of size p does $\mathrm{Aut}(F(G))$ have? A factor C_{q_j-1} has a subgroup of size p if and only if p divides $q_j - 1$, i.e. if and only if $q \equiv 1 \pmod{p}$ and these subgroups are unique. For each prime divisor p of n/m, let $c(p)$ denote the number of primes q dividing m such that $q \equiv 1 \pmod{p}$. Hence $\mathrm{Aut}(F(G))$ has a subgroup isomorphic to

$$C_p \times C_p \times \cdots \times C_p = C_p^{c(p)}$$

and all subgroups of $\mathrm{Aut}(F(G))$ with order p are contained in this subgroup. This subgroup has $\frac{p^{c(p)}-1}{p-1}$ subgroups of order p. This is because any of the $p^{c(p)} - 1$ nonzero elements in $C_p^{c(p)}$ generates a subgroup of order p, but each such subgroup has $p - 1$ generators. Hence we obtain Hölder's formula.

Hölder's original proof is similar in some ways. He uses the maximal normal cyclic subgroup H of G, which turns out in this case to coincide with the Fitting subgroup $F(G)$, and establishes that G/H is cyclic. From there he determines the possible relations for generators of G. The explanation given in Conway et al. [4] also focuses on the generators and relations of a group.

9 Further Results and Conjectures

A natural question that arises from Hölder's formula is: for n square-free, can we relate $f(n)$ to n more explicitly? McIver and Neumann [16] determined that $f(n) \leq n^4$ for n square-free. A better bound, given in [17], is $f(n) \leq \phi(n)$, where ϕ is Euler's function. For square-free $n = p_1 p_2 \cdots p_r$ and greater than 1, this last result implies that

$$f(n) \leq \phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1) < n.$$

Furthermore, if n is even and square-free, then $p_1 = 2$ and $f(n) \leq \phi(n) = 1(p_2 - 1) \cdots (p_r - 1) < n/2$.

Murty and Srinivasan [18] proved a more detailed result: there exist real numbers A, $B > 0$ such that

$$f(n) \leq O\left(\frac{n}{(\log n)^{A \log\log\log n}}\right)$$

for all square-free n and

$$f(n) > \frac{n}{(\log n)^{B \log\log\log n}}$$

for infinitely many square-free n. Such results are based on our understanding of the distribution of prime numbers. In this sense they are more number theoretic than the arguments presented in this report.

A positive integer n is cube-free if no cube divides n. Similarly, a positive integer n is $(k+1)$-free if it is not divisible by any $(k+1)$-th power greater than 1. It is tempting to think that Hölder's result generalizes in some way to groups of cube-free order, or even to groups whose order is a $(k+1)$-free integer. A general explicit formula is very unlikely, however, since such groups are not necessarily solvable, and if solvable need not be Sylow tower groups. A more promising direction, therefore, is to understand the asymptotic behavior of $f(n)$ when n is $(k+1)$-free. In this light, define

$$M(k) := \overline{\lim_{n\to\infty}} \frac{\log f(n)}{\log n}$$

where the limit superior ranges just over $(k+1)$-free integers n. For the square-free case ($k = 1$), Erdös, Murty, and Murty [8] have shown that $M(1) = 1$; their proof uses Dirichlet's Theorem on primes in arithmetic progressions, among other techniques. The following conjecture for the cube-free case ($k = 2$) is attributed to Peter Neumann.

Conjecture 25. *With $M(k)$ defined as above, $M(2) = 2$.*

A proof of Conjecture 25 may also use Dirichlet's Theorem, and will likely invoke several known properties of groups of cube-free order. For a start, McIver and Neumann have shown that $f(n) \leq n^8$ for n cube-free [16]. In any group, the solvable residual is the smallest normal subgroup with solvable factor group, and recall that the solvable radical is that largest normal subgroup. Although groups of cube-free order are not solvable in general, they are the product of the solvable radical and the solvable residual [3, Proposition 21.15], so their structure can be studied through these two subgroups. It may be feasible to determine estimates for the number of groups of cube-free order since a large part of any such group is normal with a Sylow tower structure.

A natural extension of Conjecture 25 is to find the value of $M(k)$ for other small k. Such results may provide insight into another problem: what are good bounds for $M(k)$? For general k, one can verify that $M(k) \leq k^2 + k + 2$ using results of McIver and Neumann [16]. Also, Pyber's theorem [19] gives $M(k) \leq \frac{2}{27}k^2 + O(k^{3/2})$, which may turn out to be the best asymptotic bound.

Another, more significant conjecture in the enumeration of finite groups is Graham Higman's PORC conjecture. In order to describe it, let us first define a polynomial on residue classes (PORC). The residue class of k with respect to N is $R_N(k) = \{n \in \mathbb{Z} \mid n \equiv k \pmod N\}$. Let f be a function defined on a set of integers. Suppose that for some integer N and for each k, there is a polynomial f_k such that whenever $n \in R_N(k) \cap \mathrm{dom}(f)$, we have $f_k(n) = f(n)$. Then the function f is said to be PORC. Now we state the conjecture:

Conjecture 26 (Higman's PORC conjecture)**.** *Let $g_n(p) = f(p^n)$ where p is a prime and f is the group number function. For a fixed n, the function g_n is PORC as a function of p.*

The result has been verified in some limited cases. Combining the work of several researchers, it can be shown by means of sophisticated computation that g_n is PORC for n less than or equal to 7. Using cohomology theory and algebraic representations of algebraic groups, Evseev has verified the result for a related function $\phi_n(p)$ which counts the number of groups of order p^n whose Frattini group is central [9]. Marcus du Sautoy has applied zeta functions of finitiely generated torsion-free

nilpotent groups to this problem [7]. His approach features algebraic groups, p-adic Lie groups, p-adic integration, among others. Based on these advances, it is clear that the techniques necessary to prove the PORC conjecture would have a profound impact on several areas of mathematics. If $f(p^k)$ is confirmed PORC, there will likely be relevant implications for $f(n)$. Maybe there are other classes of orders for which $f(n)$ is PORC? It has also been suggested that the function that counts metabelian or even metacyclic groups of a given order is PORC.

We mention one final, curious conjecture in the enumeration of finite groups:

Conjecture 27. *The group enumeration function is surjective.*

That is, for every positive integer m, the conjecture asserts that there exists n such that $f(n) = m$. This conjecture may well be resolved through consideration of square-free n, largely because of Hölder's formula. Indeed, it has been verified that every m less than 10,000,000 is equal to $f(n)$ for some square-free n, and a forthcoming paper by R. Keith Dennis promises to shed more light on the topic [5, 6].

Hölder's formula was a ground-breaking result in the early development of group theory, and it continues to influence research today. In this project, we have seen how a structural approach to the formula can be used to re-interpret the classical result using more recent ideas. In addition, understanding the formula can serve as an introduction to topics in graduate-level group theory and to current research topics.

References

[1] T. Bandman, G.-M. Greuei, F. Grunewald, B. Kunyavski, G. Pfister, and E. Plotkin. Identities for finite solvable groups and equations in finite simple groups. *Compositio Mathematica*, 142(3):734–764, 2006.

[2] O. Baues and F. J. Grunewald. Automorphism groups of polycyclic-by-finite groups and arithmetic groups. *Publications Mathématiques de l'IHÉS*, 104:213–268, 2006.

[3] S. R. Blackburn, P. M. Neuman, and G. Venkatarmaman. *Enumeration of Finite Groups*. Cambridge Tract in Mathematics, 173. Cambridge University Press, Cambridge, UK, 2007.

[4] J. Conway, H. Burgiel, and C. Goodman-Strauss. *The Symmetries of Things*. A K Peters, Ltd., Wellesley, Massachusetts, 2008.

[5] J. Conway, H. Dietrich, and E. A. O'Brien. Counting groups: gnus, moas and other exotica. *Mathematical Intelligencer*, 30(2):6–15, 2008.

[6] R. K. Dennis. The number of groups of order n. In preparation.

[7] M. du Sautoy. Counting subgroups in nilpotent groups and points on elliptic curves. *Journal für die reine und angewandte Mathematik (Crelle's Journal)*, 549(1-21), 2002.

[8] P. Erdös, M. R. Murty, and V. K. Murty. On the enumeration of finite groups. *Journal of Number Theory*, 25:360–378, 1987.

[9] A. Evseev. On Higman's PORC Conjecture. Preprint, Mathematical Institute, Oxford, 2005.

[10] Frobenius. Über auflösbare Gruppen. *Sitzungsberichte der Königlichen Preussischen Akademie der Wissenschaften zu Berlin*, pages 337–345, 1893.

[11] J. A. Gallian. *Contemporary Abstract Algebra*. Houghton Mifflin, Boston, Massachusetts, 6th edition, 2006.

[12] F. J. Grunewald, P. R. Pickel, and D. Segal. Finiteness theorems for polycycic groups. *Bulletin of the American Mathematical Society (New Series)*, 1(3):575–578, 1979.

[13] R. Guralnick, B. Kunyavski, E. Plotkin, and A. Shalev. Thompson-like characterizations of the solvable radical. *Journal of Algebra*, 300:363–375, 2006.

[14] O. Hölder. Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4. *Mathematische Annalen*, 43:301–412, 1893.

[15] O. Hölder. Die Gruppen mit quadratfreier Ordnungszahl. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-Physikalische Klasse*, pages 211–219, 1895.

[16] A. McIver and P. M. Neuman. Enumerating finite groups. *Quarterly Journal of Mathematics Oxford*, 38(2):473–488, 1987.

[17] M. R. Murty and V. K. Murty. On the number of groups of a given order. *Journal of Number Theory*, 18(178-191), 1984.

[18] M. R. Murty and S. Srinivasan. On the number of groups of a squarefree order. *Canadian Mathematics Bulletin*, 30:412–420, 1987.

[19] L. Pyber. Enumerating finite groups of a given order. *Annals of Mathematics*, 137:203–220, 1993.

[20] D. J. S. Robinson. *A Course in the Theory of Groups*. Springer, New York, second edition, 1996.

[21] J. J. Rotman. *An Introduction to the Theory of Groups*. Springer, New York, fourth edition, 1995.

[22] D. Segal. *Polycyclic Groups*. Cambridge University Press, Cambridge, UK, 2005.