SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

A Classification of Certain Finite Groups

av

Armin Novin

2024 - No K18

A Classification of Certain Finite Groups

Armin Novin

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Wushi Goldring

2024

Abstract

This paper classifies finite groups whose order has a particularly simple prime factorization.

Abstract

Detta arbete presenterar en klassificering av ändliga grupper vars ordning har en enklare primtalsfaktorisering.

Acknowledgements

A sincere thank you

to Wushi Goldring, for his courtesy, attention to detail and insightful feedback in supervising me

to Kilian Liebe, for the undeserved amount of help I have received from him during my education

and to Kristina, for her patience as I put myself through school, fifteen years later.

Contents

1 Introduction

The problem of classifying distinct finite groups is seemingly not too involved. After all, the axioms of groups are quite simple, and conceptually they aren't difficult objects. But the methods of classification can range quickly from simple to very intricate. For example, there is only *one* group of order 11, up to isomorphism. This result is obtained by an application of Lagrange's theorem. For groups of order 4, one can deduce that there are *two* such distinct groups by studying group tables. But for order 16, there are *fourteen* distinct groups, requiring more advanced methods of classification.

It is a fascination with this that motivates the present paper, which will give a basic classification of a number of finite groups. Specifically, we will consider the prime factorisations p, p^2, p^3 and pq where p and q are distinct prime numbers. For each factorisation, a classification will be given for some or all of the groups of corresponding order.

Section 2 treats the very basics of group theory. Section 3 introduces concepts that are more involved in the procedure of classification. Some results in this section will be proven, while the proof of other results will be left out. Section 4 treats the classification itself.

A word on notation

Throughout this paper, whenever a group is said to have order p or q, it invariably means prime numbers. Sometimes the word p-group will be used, referring to some group of prime order p. When groups of arbitrary orders are discussed, the letters m and n will be used.

2 Preliminary notions

2.1 Groups: basic definitions and properties

Definition 2.1. A group is a non-empty set G together with a function $f : G \times G \to G$ such that the following hold:

- *(Associativity)* $f(a,(b,c)) = f((a,b),c)$ for all a,b,c in G
- *(Identity)* There exists an element $e \in G$ such that $f(e,g) = f(g,e) = g$, for all $g \in G$. This element is called the identity element.
- *(Invertibility)* For every $g \in G$ there exists an element g^{-1} such that $f(g,g^{-1}) = f(g^{-1},g) = e$. The element g^{-1} is called the inverse of g.

The notation $f(a,b)$ will from here on be substituted with ab and be referred to as the *product* of a and b. A consequence of the associative law is that when multiplying a group element by itself several times, we are free to parenthesize the product as we wish, which motivates the use of a multiplicative notation

$$\underbrace{ggg\ldots g}_{\text{n times}} = g^n$$

Example 2.1. The set $(\mathbb{Z},+)$ of positive integers numbers with the operation of addition constitutes a group. The identity element in this group is the integer 0.

Example 2.2. The set $(\mathbb{R}^+,\times)$ of positive real numbers with the operation of multiplication constitutes a group. The identity element in this group is the real number 1.

Example 2.3. The set of integers modulo n, denoted $\mathbb{Z}/n\mathbb{Z}$ is a group under addition, with 0 as the identity element.

Example 2.4. the set $V_4 = \{1,a,b,c\}$, with operation defined by $v^2 = 1$ for all $v \in V_4$, and where any pair among a,b,c gives the third element constitutes a group. This group is called the Klein-4 group.

We now prove some consequences of the definition.

Proposition 2.1. Let G be a group. The following hold.

1. The identity element e is unique.
2. The inverse of an element is unique.
3. $(ab)^{-1} = b^{-1}a^{-1}$.
4. $(g^n)^{-1} = g^{-n}$.

Proof. 1. Suppose e and e' are two distinct identity elements and let $g \in G$. Then

$$\begin{aligned} & ge = ge' \\ \Leftrightarrow \quad & e = e' \end{aligned}$$

since we can multiply both sides on the left by g^{-1}.

2. Suppose b and c are both inverses of an element g. Then

$$\begin{aligned} b &= b(ca) \\ &= b(ac) \\ &= (ba)c \\ &= ec \\ &= c. \end{aligned}$$

3. Notice that for the product ab, the element $b^{-1}a^{-1}$ has the property that

$$ab(b^{-1}a^{-1}) = (b^{-1}a^{-1})ab = e.$$

4. Because

$$g^n = \underbrace{ggg\dots g}_{\text{n times}} \qquad \text{and} \qquad g^{-1} = \underbrace{g^{-1}g^{-1}g^{-1}\dots g^{-1}}_{\text{n times}}$$

we get

$$\begin{aligned} g^n g^{-n} &= (ggg\dots g)(g^{-1}g^{-1}\dots g^{-1}) \\ &= (gg^{-1})(gg^{-1})(gg^{-1})\dots(gg^{-1}) \\ &= e. \end{aligned}$$

□

Definition 2.2. The order of a group element g is the smallest positive integer n for which $g^n = e$, if this number exists. We denote this $|g| = n$. If $g^n \neq e$ for no n then g is said to have infinite order and we denote it $|g| = \infty$. The identity element is the only element that has order 1.

Remark. If $|g| = n$ and m is a multiple of n, then $g^m = 1$, because $g^k = g^{kn}$ for some factor k, implying $g^{kn} = g^{nk} = (g^n)^k = 1^k = 1$.

Proposition 2.2. Let G be a finite group. Then every element $g \in G$ has finite order.

Proof. Suppose $|g| = \infty$. Given that G is finite, it is impossible that powers of g be distinct. Hence $g^i = g^j$ for $i \neq j$. This implies $g^{i-j} = e$. □

Proposition 2.3. Let G be a finite and group and let $g \in G$ with $|g| = n$. Then powers of g are distinct up to the order of g.

Proof. If $g^i = g^j$ for $j < i < n$ and $i \neq j$ then $g^{i-j} = e$ implies that the order of g is at most $i - j$, but could be smaller. □

2.2 Subgroups

A subgroup is a subset of a group which itself acts like a group. The following definition is particular to finite groups.

Definition 2.3. Let G be a finite group and let H be a non-empty subset of G. Then H is a subgroup of G, written $H \leq G$, if it closed under the operation defined on G.

To check that a subset H is indeed a subgroup G the following suffices.

Proposition 2.4. Let G be a finite group and let H be a subset of G. Then H is a subgroup of G if and only if $H \neq \emptyset$ and $x, y \in H \implies xy \in H$.

Proof. If H is a subgroup then the rest follows immediately. Conversely, suppose H is non-empty and closed under products, and Let $x \in H$. By closure, the set $\{x, x^2, \ldots, x^{n-1}, x^n\} \subseteq H$. In particular $x^n = 1 \in H$ and $x^{n-1} \in H$, the latter of which being equal to the inverse of x, since

$$\begin{aligned} xx^{n-1} &= x^{n-1}x \\ &= x^{n-1+1} \\ &= x^n \\ &= 1. \end{aligned}$$

□

Finally, Associativity is inherited from G.

Centers, Centralisers and Normalizers

The following are an important class of subgroups which will be used later. They provide various aspects on the property of commutativity and are related to one another.

Definition 2.4. Let G be a group. The *center* of G, denoted $Z(G)$ is the set

$$Z(G) = \{g \in G \mid ga = ag \ \ \forall a \in G\}.$$

In other words, the center of G is the set of elements that commute with *all other* elements of G.

Proposition 2.5. The set $Z(G)$ is a subgroup of G.

Proof. The set $Z(G)$ is non-empty, since $1 \in Z(G)$. Suppose $x, y \in Z(G)$ and let g be any element of G. It follows that

$$\begin{aligned}(xy)g &= x(yg)\\ &= x(gy)\\ &= (xg)y\\ &= (gx)y\\ &= g(xy).\end{aligned}$$

□

Remark. If G is abelian then $Z(G) = G$.

Definition 2.5. Let G be a group with an element g. The *Centraliser* of g in G denoted $C_G(g)$ is the set

$$C_G(g) = \{x \in G \mid xg = gx\}$$

of all elements in G that commute with g.

Proposition 2.6. The centraliser of an element is a subgroup of a G.

Proof. The proof is identical to the previous proof. □

The centraliser can be defined for subsets of G as well, where if A is a subset, $C_G(A)$ is taken to mean the set of elements in G that commute with *every* element of A. In particular $C_G(G) = Z(G)$, and in general $Z(G) \subseteq C_G(g)$ for every $g \in G$.

For the next subgroup, we define the notion of conjugation.

Definition 2.6. Let $H = \{h_1, h_2, \ldots, h_n$ be a subset of a group G. For an arbitrary element $g \in G$ define

$$gHg^{-1} = \{gh_1g^{-1}, gh_2g^{-1}, \ldots, gh_ng^{-1}\}$$

The set gHg^{-1} is said to be *conjugate* to H, or that H has been *conjugated* by g. Conjugation can be defined for individual elements as well.

Definition 2.7. Let G be a group with a subset A. Define

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

The set $N_G(A)$ is called the *normaliser* of A in G.

That $gAg^{-1} = A$ for an element g means that A is stable under conjugation by g: no element of the form ga_ig^{-1}, where $a_i \in A$ leaves the set A. In the case of the centraliser, if $g \in C_G(A)$ then gAg^{-1} fixes every element of A. We may thus think of the normaliser as a relaxed form of the centraliser. In fact, the latter is contained in the former, and for individual elements they coincide. If g is an element of a group G then

$$\begin{aligned} N_G(g) &= \{x \in G \mid xgx^{-1} = x\} \\ &= \{x \in G \mid xg = gx\} \\ &= C_G(g). \end{aligned}$$

Proposition 2.7. Let A be a subset of a group G. Then $N_G(A) \leq G$.

Proof. Since $e \in N_G(A)$, $N_G(A)$ is non-empty. If $x, y \in N_G(A)$ then

$$\begin{aligned} xyA(xy)^{-1} &= xyAy^{-1}x^{-1} \\ &= x(yAy^{-1})x^{-1} \\ &= xAx^{-1} \\ &= A. \end{aligned}$$

□

We finally define the notion of a normal subgroup.

Definition 2.8. A subgroup H of G is called *normal* in G if $N_G(H) = G$. This is written $N \trianglelefteq G$.

Proposition 2.8. Let G be a group and let A be a non-empty subset of G. Then

1. $Z(G) \leq C_G(A) \leq N_G(A)$
2. If G is abelian, then $Z(G) = C_G(A) = N_G(A) = G$

Proof. We have already shown the inclusions as sets. Since each is a subgroup of G, the closure property ensures that they are indeed subgroups in the presented manner. If G is abelian, we know that $Z(G) = G$ and (1) forces the latter two subgroups to be equal to G, although this can be deduced by looking at each of them individually. □

Subgroups generated by subsets

Proposition 2.9. Let $H_1, H_2, \ldots, H_n$ be a collection of subgroups of a group G. Then the intersection of all these subgroups is a subgroup of G.

Proof. Let

$$I = \bigcap_{i=1}^{n} H.$$

Since $e \in H_i$ for all i, I is non-empty. If $x, y \in H_i$ for all i, then since every H_i is a group, $ab \in H_i$ for all i. Thus $ab \in I$ and $I \leq G$ by Proposition 2.4. □

Definition 2.9. Let K be a subset of a group G and let

$$\langle K \rangle = \bigcap_{\substack{K \subseteq H \\ H \leq G}} H$$

that is, the interserction of all subgroups that contain K. We call $\langle K \rangle$ the subgroup of G generated by K. It has the property of being the smallest subgroup of G that contains K: for if there was a smaller such subgroup $\langle K' \rangle$, the implication is that there is an element x in $\langle K \rangle$ that is not in $\langle K' \rangle$. But by definition, x is in the intersection of all subgroups that contain K, which simply forces it to be in $\langle K' \rangle$.

A more involved way of constructing this subgroup is by defining the closure $\bar{K}$ of a set K as

$$\bar{K} = \{k_1^\epsilon k_2^\epsilon \dots k_n^\epsilon\}$$

where $k_i \in K$ and $\epsilon = \pm 1$ so that $\bar{K}$ is the set of finite products of elements in K and their inverses. We also define $\bar{\emptyset} = \{1\}$.

Proposition 2.10. $\bar{K} = \langle K \rangle$.

Proof. By previous results, $\bar{K}$ is non-empty. If $k, q \in \bar{K}$ where $k = k_1^\epsilon k_2^\epsilon \dots k_n^\epsilon$ and $q = q_1^\delta q_2^\delta \dots q_m^\delta$ then $kq \in \bar{K}$ in the finite case since

$$kq = k_1^\epsilon k_2^\epsilon \dots k_n^\epsilon \cdot q_1^\delta q_2^\delta \dots q_m^\delta$$

is just a product of elements of K raised to 1 or -1. The same is true in the general case. Because every element of K can be written k^1, $K \subseteq \bar{K}$ and $\langle K \rangle \subseteq \bar{K}$. But because $\langle K \rangle$ contains K and is closed under the group operation, $\langle K \rangle$ contains all elements of the form $k_2^\epsilon \dots k_n^\epsilon$, implying $\bar{K} \subseteq \langle K \rangle$ and $\bar{K} = \langle K \rangle$. □

2.3 Different types of groups

In this section we give definitions of the following

Direct products of groups

The Cyclic group C_n

The Symmetric group S_n

The Dihedral group D_{2n}

The Quaternion group Q_8

The direct product of groups

Definition 2.10. The direct product of n groups $G_1, G_2, \ldots, G_n$ is the Cartesian product

$$G_1 \times G_2 \times \ldots \times G_n.$$

An element in this set is the n-tuple $(g_1, g_2, \ldots, g_n)$, where the i :th component is an element of G_i. If we define an operation on the direct product by

$$\begin{aligned} & (g_1, g_2, \ldots, g_n) \circ (h_1, h_2, \ldots, h_n) \\ = \quad & (g_1 h_1, g_2 h_2, \ldots, g^{n-1} h^{n-1}) \end{aligned}$$

that is, *componentwise*, then the direct product is a group under this operation.

The cyclic group

Definition 2.11. The cyclic group C_n of order n is the group that is generated by a single element $\langle x \rangle = \{1, x, x^2, \ldots, x^{n-1}\}$.

Remark. The cyclic group is a special case of a subgroup being generated by a subset, namely, when the subset is a single element.

The dihedral group

Suppose we have the group elements r $\in C_n$ and $s \in C_2$. We wish to create a group, for now denoted D, with r and s as generators. First we impose the condition that $r^n = s^2 = 1$. Noting that $sr^\alpha \neq sr^\beta$ for $\alpha \neq \beta$ and $\alpha, \beta < n$, there are *at least* $2n$ elements in D. These are

$$D = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}.$$

Next we require that $sr = r^{-1}s$. This implies $sr^i = r^{-i}s$ for any i, since

$$sr^i = (\underbrace{s\,r)r\ldots r}_{i \text{ times}}$$

$$= r^{-1}s\,\underbrace{rr\ldots r}_{i-1 \text{ times}} \qquad \text{since } sr^1 = r^{-1}s.$$

Continuing in this manner results in a right hand side that is equal to $r^{-i}s$. Let z be an element in D consisting of an arbitrary product of powers of r and powers of s

$$z = r^{\alpha_1}s^{\alpha_1}r^{\alpha_2}s^{\alpha_2}\ldots r^{\alpha_k}s^{\alpha_k}$$

with no particular conditions placed on the exponents α_i. The requirement that $sr = r^{-1}s$ implies $z = s^k r^i$ where k and i have been obtained by the successive interchanging of r and i. We conclude that any element in the group can be written in this form. And since k is counted modulo 2 and i is counted modulo n there are *at most* $2n$ elements in the group. We conclude that there are exactly $2n$ elements.

Definition 2.12. The Dihedral group D_{2n} is the group generated by the elements r and s subject to the relations

$$r^n = s^2 = 1 \qquad \text{and} \qquad sr = r^{-1}s.$$

Remark. There is a geometric interpretation of the group D_{2n}. For $n \in \mathbb{Z}$, $n \geq 3$, consider a regular n-gon centered at the origin. A *symmetry* on the n-gon is either a rotation of $2\pi/n$ about the origin, or a reflection along any symmetry axes, or indeed any composition of the two. With a labeling of vertices from 1 to n the symmetries can be uniquely described as permutations on the set of vertices.

The symmetric group

For a non-empty set X, the set of bijections from X to itself constitutes a group. A bijection has a 2-sided inverse, and the composition of bijections is another bijection. Furthermore, the composition of functions in general is associative, and there is a bijection that fixes all elements of X.

Definition 2.13. For a non-empty set X, symmetric group S_X is the group of bijections of X. When X is a subset of the natural numbers of the form $\{1, 2, \ldots, n\}$ the symmetric group is denoted S_n.

The Quaternion group

As with the dihedral group we begin with a motivation. Let $a \in C_4$ and $b \in C_4$. We wish to create a group, for now denoted Q with a and b as genereators. The First condition imposed is $a^4 = 1$. Secondly, $a^2 = b^2$. This implies that $b^4 = a^2a^2 = a^4 = 1$. Lastly, we require that $ab = b^{-1}a$. With this, we have at least 8 elements

$$Q = \{1, a, a^2, a^3, b, b^3, ab, ba\}$$

which is reasonable, because supposing that $ab = ba$ implies ulitmately that $b^2 = a^2 = 1$. Similarly, supposing that $ab = a^k$ implies either that $b = 1, b = b^2$ or $b = a$.

The relation $ab = b^{-1}a$ allows us, as in the case of the dihedral group, to write any element uniquely as a product a^ib^j, both i and j being counted modulo 4. Hence there are at most, and therefore exactly 8 elements in this group.

Definition 2.14. The Quaternion group Q_8 is the group generated by the elements a, b subject to the relations

$$a^4 = 1 \quad a^2 = b^2 \quad ab = b^{-1}a$$

Exploring the consequences of the relations reveals that

$$(ab)^2 = abab = b^{-1}a^2b = b^{-1}b^2b = b^2 = a^2$$

which also holds for ba. Letting

$$\begin{array}{ccc} a = i & b = j & ab = k \\ a^3 = -i & b^3 = -j & ba = -k \end{array}$$

and $a^2 = b^2 = (ab)^2 = (ba)^2 = -1$, the group can be expressed as

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with the notable properties

$$(-1)(-1) = 1 \quad (-1)a = a(-1) = -a \quad \forall a \in Q_8$$

$$\begin{array}{c} i^2 = j^2 = k^2 = -1 \\ ij = k \quad , ji = -k \\ jk = i, \quad kj = -i \\ ki = j, \quad ik = -j \end{array}$$

2.4 Group Isomorphisms

A group isomorphism is best described by first defining a group *homomorphism*.

Definition 2.15. Let G and H be groups. A mapping $\phi : G \to H$ is a homomorphism if

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$$

for all $g_1, g_2 \in G$. An isomorphism is simply a homomorphism that is bijective. Two isomorphic groups are structurally identical. The only difference is what we choose to name them and their elements.

2.5 Group actions

Definition 2.16. A group action of a group G on a set X is a mapping $G \times X \to X$ such that

(1) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all g_1, g_2 in G and all x in X.
(2) $1 \cdot x = x$ for all x in X.

Two properties of group actions are that for every given $g \in G$, the associated map σ_g is a permutation of X, and that the map from G to S_X defined by $g \mapsto \sigma_g$ is a homomorphism. To show the first property, we observe that permutations are bijections from a set to itself and will therefore need to show that the map σ_g has a two-sided inverse. Let x be any element of X:

$$\begin{aligned}
(\sigma_{g^{-1}} \circ \sigma_g)(x) &= \sigma_{g^{-1}}(\sigma_g(x)) && \text{by associativity of function composition} \\
&= g^{-1} \cdot (g \cdot x) && \text{by definition of } \sigma_g \text{ and } \sigma_{g^{-1}} \\
&= (g^{-1} g) \cdot x && \text{by property (1)} \\
&= 1 \cdot x = x && \text{by property (2).}
\end{aligned}$$

The above shows that $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map in X. Because g can be any given element in G, we may interchange the places of g and g^{-1} to arrive at $\sigma_g \circ \sigma_{g^{-1}}$ being the identity map in X as well. Therefore the map σ_g has a two-sided inverse and is a permutation of X.

Now let $\phi : G \to S_X$ be defined by $\phi(g) = \sigma_g$ and observe that

$$\begin{aligned}
\phi(g_1 g_2)(x) &= \sigma_{g_1 g_2}(x) && \text{by definition of } \phi \\
&= (g_1 g_2) \cdot x && \text{by definition of } \sigma_{g_1 g_2} \\
&= g_1 \cdot (g_2 \cdot x) && \text{by property (1)} \\
&= \sigma_{g_1}(\sigma_{g_2}(x)) && \text{by definition of } \sigma_{g_1}, \sigma_{g_2} \\
&= (\phi(g1) \circ \phi(g_2))(a) && \text{by definition of } \phi
\end{aligned}$$

This shows that $\phi : G \to S_X$ is a homomorphism. Conversely, if $\phi : G \to S_X$ is any homomorphism, then the map $G \times X \to X$ defined by $g \cdot x = \phi(g)(x)$ satisfies

$$\begin{aligned}(g_1g_2)\cdot x &= \phi(g_1g_2)(x)\\ &= \phi(g_1)\phi(g_2)(x)\\ &= (\sigma_{g_1}\circ\sigma_{g_2})\cdot x\\ &= \sigma_{g_1}\cdot(\sigma_{g_2}\cdot x)\\ &= g_1\cdot(g_2\cdot x)\end{aligned}$$

and

$$\begin{aligned}1\cdot x &= \phi(1)(x)\\ &= 1(x)\\ &= 1.\end{aligned}$$

Example 2.5. Let G be a group and let $g, h \in G$. Define a map $G \times G \to G$ by $g \cdot h = gh$. This constitutes a group action (we put $X = G$), since $1 \cdot h = h$ for all $h \in G$, and

$$\begin{aligned}g_1\cdot(g_2\cdot h) &= g_1(g_2h)\\ &= (g_1g_2)h\\ &= (g_1g_2)\cdot h.\end{aligned}$$

This action is called the *left multiplication* by G on itself, and will be used later to prove Lagrange's theorem.

Example 2.6. Let G be a group and let $g, h \in G$. Define a map $G \times G \to G$ by $g \cdot h = ghg^{-1}$. This constitutes a group action (we put $X = G$), since $1 \cdot ehe^{-1} = h$ for all $h \in G$, and

$$\begin{aligned}g_1\cdot(g_2\cdot h) &= g_1(g_2hg_2^{-1})g_1^{-1}\\ &= g_1g_2h(g_1g_2)^{-1}\\ &= (g_1g_2)\cdot h.\end{aligned}$$

This action is called *conjugation* by G on itself.

3 Some structure theory

3.1 Group tables: a doomed approach

The idea of a group table is a simple one, and might hint at a combinatorical method of classifying groups. However, as the order of a group grows larger the concept becomes unwieldy. It is included in this paper to show just how quickly (Example 3.1) it falls apart.

Definition 3.1. Let G be a group. The *group table* of G is the cartesian product $G \times G$, where an element $(a, b) \in G \times G$ is the result of the product ab in G.

A pictorial presentation of the group table of $V_4 = \{1, a, b, c\}$ is given by the labeled array

	1	**a**	**b**	**c**
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Now in the group $\mathbb{Z}/4\mathbb{Z}$, if we assigned new names to the elements, specifically $0 = 1, 1 = a, 2 = b, 3 = c$, then the corresponding presentation of $\mathbb{Z}/4\mathbb{Z}$ gives us the array

	1	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

The structural difference between them is in some sense laid bare in these presentations. With the notion of a group table introduced, we point out that any jumble of a finite elements within an array does not constitute a group table. A special property that group tables have is that they are so called *latin squares*.

Definition 3.2. A Latin square is an $n \times n$ array populated by n distinct elements, such that each row of the array contains an element exactly once, and each column contains each element exactly once.

To prove that the group table of a group G is a latin sqare, we observe that the row corresponding to the element g_i contains the elements

$$g_i g_1 \quad g_i g_2 \quad \cdots \quad g_i g_n.$$

These are all unique, since if $g_i g_t = g_i g_r$, left cancellation implies that $g_t = g_r$. Similarly, right cancellation implies that every element in a column is unique. The group table of G is thus a latin square.

Somewhat surprisingly, this doesn't necessarily hold in the other direction: a latin square doesn't necessarily represent a group table.

Example 3.1. Let $S = \{1, a, b, c, d\}$ be a set equipped with an operation $\circ$ such that the table of the operation is given by the array

	1	**a**	**b**	**c**	**d**
1	1	a	b	c	d
a	a	1	d	b	c
b	b	c	1	d	a
c	c	d	a	1	b
d	d	b	c	a	1

It is clear that this table is a latin square. It is not, however, a group: Consider the product aab. We should have that $(aa)c = a(ac)$. But $(aa)c = c$ and $a(ac) = d$ according to the table. The associative property does not hold.

3.2 Lagrange's Theorem

Lagrange's theorem relates the order of a group to the order of its subgroup in a very useful way.

Proposition 3.1. Let G be a group and X a set, and let G act on X. Define a relation on X given by

$$x_1 R x_2 \Leftrightarrow x_1 = g \cdot x_2 \quad \text{for some } g \in G$$

then R is an equivalence relation.

Proof. Reflexivity is shown by taking $g = 1$, as then $x_1 = 1 \cdot x_1$, implying that x_1 is related to itself. For symmetry, if xRy then $x = g \cdot y$ for some $g \in G$. Letting g^{-1} act on both sides we obtain $g^{-1} \cdot x = (g^{-1}g) \cdot y = y$, which shows that yRx. Lastly, if xRy and yRz then

$$x = g_1 \cdot y \quad \text{and} \quad y = g_2 \cdot z$$

then $g^{-1} \cdot x = g_2 \cdot z$, implying that $x = (g_1 g_2) \cdot z$ and hence xRz which shows transitivity. □

The set $\mathcal{O} = \{y \in X \mid y = g \cdot x \text{ for some } g \in G\}$ of all the images of x under the action of G is called *orbit* of x. Having shown that group actions partition the set that is acted upon, we will show a narrower but important case.

Proposition 3.2. Let G be a group and $H \leq G$. Let H act on G by left multiplication. For an arbitrary $g \in G$, let $\mathcal{O}$ be the orbit of g under the action of H. Then $|H| = |\mathcal{O}|$

Proof. Define a map $H \to \mathcal{O}$ by $h \mapsto hg$. We will show that this mapping is bijective. It is injective, because $h_1 g = h_2 g$ implies that $h_1 = h_2$. It is surjective, since by definition every element in $\mathcal{O}$ is of the form hg for some $h \in H$. Hence it is bijective. □

The proposition shows that a subgroup H partitions a group G into sets of equal size, from which follows

Theorem 3.1. (Lagrange) Let G be a finite group and H be a subgroup of G. Then the order of H divides the order G.

Proof. Let $|H| = m$. By Proposition 3.1, H partitions G through the action of left multiplication. Let k be the number of these. Since they are of equal size, $|G| = km$ and hence the order of H divides the order of G. □

A partial converse to Lagrange's theorem is Cauchy's theorem. We leave out the proof.

Theorem 3.2. (Cauchy)
If G is a finite group and p divides $|G|$, then G has an element of order p.

3.3 The Orbit-Stabilizer Theorem

Definition 3.3. Let G be a group acting on a set X. For a fixed element $x \in X$, the *stabilizer* of x in G is the set $G_x = \{g \in G \mid g \cdot x = x\}$.

Note that the set G_x is a subgroup of G, since if $g_1, g_2 \in G_x$ then $g_2^{-1}g_1 \in G_x$ because

$$\begin{aligned}(g_2^{-1}g_1) \cdot x &= g_2^{-1} \cdot (g_1 \cdot x) \\ &= g_2^{-1} \cdot x \\ &= x.\end{aligned}$$

We can thus let G_x act on G by right multiplication. As we have shown, this action partitions G into k equal parts, namely, the left cosets of G_x in G. Let G/G_x denote the set of these cosets, and let $\mathcal{O}$ be the orbit of x as introduced previously. We arrive at the following result.

Theorem 3.3. (Orbit-stabilizer) Let the group G act on a set X, and fix $x \in X$. Then $|\mathcal{O}| = [G : G_x]$.

Proof. Let $f : G/G_x \to \mathcal{O}$ be a map defined by $gG_x \mapsto g \cdot x$. We will show that this map is well-defined and bijective. The equality $f(g_1G_x) = f(g_2G_x)$ is equivalent to $g_1 \cdot x = g_2 \cdot x$ from which follows that $(g_2^{-1}g_1) \cdot x = x$, meaning that $g_2^{-1}g_1 \in G_x$ which implies $g_1G_x = g_2G_x$. This shows injectivity.

Now if y is any element of $\mathcal{O}$, then $y = g \cdot x$ for some $g \in G$. Consider the coset gG_x: by definition of f this coset maps to $g \cdot x = y$. The map is therefore surjective, and hence a bijection.

Finally, the domain of f is G, but since G is constant on left cosets of G_x in G, it descends to a map whose domain G/G_x and is hence well-defined.

□

3.4 The Class Equation

Definition 3.4. Let G be a group. Two elements x and y are said to be conjugate if there is some $g \in G$ such that $y = gxg^{-1}$. Similarly, two sets X and Y are conjugate if for some g, $Y = gXg^{-1}$. In both cases, conjugation is equivalent to the two objects being in the same orbit of G under the action of conjugation on itself. These orbits are called *conjugacy classes*.

Theorem 3.4. Let G be a finite group with $g_1, g_2, \ldots, g_n$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

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

Proof. See Dummit and Foote, page 124. □

Corollary 3.4.1. Let P be a group of order $p^\alpha, \alpha \geq 1$. Then $Z(P) \neq 1$.

Proof. Note that the order of the centraliser $C_P(g)$ of any element $g \in P$ cannot be P itself, else the result follows trivially. Hence $1 \leq |C_P(g)| \leq p^{\alpha-1}$. Whatever the case, p divides $|P : C_P(g)|$ for all $g \in P$. It also divides $|P|$. Hence by the class equation

$$|P| = |Z(P)| + \sum_{i=1}^{n} |P : C_P(g_i)|$$

$$\Leftrightarrow \quad |P| - \sum_{i=1}^{n} |P : C_P(g_i)| = |Z(P)|.$$

Since p divides the left hand side, it must also divide the right, implying $Z(P)$ is non-trivial. □

3.5 Sylow's Theorems

Sylow's theorem provides a partial converse to Lagrange's theorem. Before stating it we introduce some notation. We refer to page 139 of Dummit and Foote for the proof.

Definition 3.5. Let G be a p-group.

- Subgroups of G that are p-groups are called p-subgroups.
- If G is a group of order $p^\alpha m$ where $p \nmid m$ then a subgroup of order p^α is called a *Sylow p-subgroup* of G.
- The set of Sylow p-subgroups of G is called $Syl_p(G)$ and their cardinality is called n_p.

Theorem 3.5. Let G be a group of order $p^\alpha m$ where $p \nmid m$. Then

- $Syl_p(G) \neq \emptyset$
- if $P \in Syl_p(G)$ and Q is a p-subgroup then Q is contained in a conjugate of P, $Q \leq gPg^{-1}$ for some $g \in G$. In particular, any two Sylow p-subgroups are conjugate in G.
- The number n_p satisfies $n_p \equiv 1 \pmod{p}$. Moreover, it is the index of $N_G(P)$ in G for any Sylow p-subgroup P and hence divides m.

Note that $n_p = 1$ implies that a Sylow p-subgroup of G is normal in G

3.6 Quotient groups

Definition 3.6. Let G be a group and N be a normal subgroup of G. The quotient group G/N is defined as the group of left cosets of N in G with group operation defined as

$$(aN)(bN) = (ab)N.$$

For proof that G/N is indeed a group we refer to page 81 of Dummit and Foote.

The First isomorphism theorem

Proposition 3.3. Let G and H be groups and let $\phi : G \to H$ be a homomorphism. Then

$$G/\ker\phi \cong \mathrm{im}\phi$$

Proof. See Dummit and foote, page 97. □

3.7 Automorphisms

The notion of automorphisms are relevant to the use of semidirect products.

Definition 3.7. Let G be a group. An isomorphism $\phi : G \to G$ is called an automorphism. The set of automorphisms of G is denoted $\mathrm{Aut}(G)$

We leave out the proof that $\mathrm{Aut}(G)$ is itself a group under composition of automorphisms, called the automorphism group of G.

In classifying certain finite groups in section 4, we need the automorphism groups of a certain kind of group. This is given by the following proposition

Proposition 3.4. The automorphism group of the cyclic group of order p^n is itself cyclic of order $p^{n-1}(p-1)$.

Proof. See Dummit and Foote, page 136. □

Example 3.2. For C_p We have $\mathrm{Aut}(C_p) \cong C_{p-1}$ and $\mathrm{Aut}(C_{p^2}) \cong C_{p(p-1)}$

3.8 Relation between indicies and normality

Proposition 3.5. Let G be a group let H be a subgroup G. Then if H has index 2, it is a normal subgroup.

Proof. The two cosets of H in G are H itself and gH for some $g \in G$. A subgroup is normal if and only if its right cosets are equal to its left cosets. Suppose then that $gH \neq Hg$. The possibilities for Hg are restricted to H, implying g is the identity. □

The following proposition generalizes the previous one.

Proposition 3.6. Let G be a group and let H be a subgroup of G with index p, where p is the smallest prime dividing $|G|$. Then H is normal in G.

Proof. Let G act on the set of left cosets of H by left multiplication, $x \cdot (gH) = (xg)H$. The action affords a homomorphism ϕ from G into S_p. The kernel K is contained in H, and the quotient G/K is isomorphic to a subgroup of S_p. It is therefore the case that $|G/K|$ divides both $p!$ and $|G|$ implying $|G/K| = p$. We now note that

$$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = p\frac{|H|}{|K|}$$

forces H/K to be the trivial group. Hence $K = H$ and the latter is normal. □

3.9 Semidirect products

This section introduces the notion of the semidirect product, which will be used heavily in classifying groups in section 4. We will also show how it relates to the direct product that was introduced in Section 1. We begin by studying some consequences of normality as it relates to subgroups: for two subgroups H and K of a group G, we want to know under what circumstances the set $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G.

Proposition 3.7. Let G be a group. For any finite subgroups H, K of G, the set defined as

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

has cardinality

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. We first observe that HK is a union of left cosets of K

$$HK = \bigcup_{h \in H} hK = h_1K \cup h_2K \cup \ldots \cup h_sK. \qquad (1)$$

By Proposition 3.2 $|hK| = |K|$ for any h. We need to find the distinct number of cosets of K. For two identical cosets we have the equivalence

$$\begin{aligned} & h_1K = h_2K \\ \Leftrightarrow \quad & h_2^{-1}h_1K = K \\ \Leftrightarrow \quad & h_2^{-1}h_1 \in K \\ \Leftrightarrow \quad & h_2^{-1}h_1 \in H \cap K \\ \Leftrightarrow \quad & h_2^{-1}h_1(H \cap K) = H \cap K \\ \Leftrightarrow \quad & h_1(H \cap K) = h_2(H \cap K). \end{aligned}$$

We may thus count the distinct number of cosets $h(H \cap K)$ for $h \in H$. By Lagrange's theorem this number is given by $\frac{|H|}{|H \cap K|}$. Hence the union in (1) consists of $\frac{|H|}{|H \cap K|}$ distinct cosets of K, each of size $|K|$, which proves the statement. □

Corollary 3.5.1. Let H, K be subgroups of a group G with $|H \cap K| = 1$. Then every element of HK can be expressed uniquely as a product hk for some $h \in H, k \in K$.

Proof. Suppose $h_1k_1 = h_2k_2$. Equivalently $h_2^{-1}h_1 = k_2k_1^{-1}$. Clearly the left hand side is an element of H and the right hand side an element of K. This implies $h_2^{-1}h_1 \in H \cap K$. Since the latter is assumed to be trivial $h_1 = h_2$. It now follows that also $k_1 = k_2$. □

Proposition 3.8. The set HK in Proposition 3.7 is a subgroup of G if and only if $HK = KH$, that is, if at least one of H or K is normal in G.

Proof. Suppose that $HK = KH$ with $x, y \in HK$. We will show that $xy^{-1} \in HK$. If $x = h_1k_1$ and $y = h_2k_2$ for $h_i \in H, k_i \in K$ then $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Write $k_3 = k_1k_2^{-1}$ and $h_3 = h_2^{-1}$. Then $xy^{-1} = h_1k_3h_3$. The property $HK = KH$ ensures that $k_3h_3 = h_4k_4$ for some $h_4 \in H, k_4 \in K$. Hence

$$xy^{-1} = (h_1h_4)k_4 \in HK$$

Conversely, if $HK \leq G$ and both $H, K \leq G$ then by closure $KH \subseteq HK$. Now suppose $hk \in HK$. Write $hk = h_ik_j$ for some $(h_ik_j)^{-1} \in HK$. Then

$$hk = k_i^{-1}h_i^{-1} \in KH.$$

□

Now that we know when the set HK is a subgroup of G, the following proposition shows that one more assumption implies that the subgroup HK is isomorphic to the direct product of H and K.

Proposition 3.9. Let G be a group and let H, K be subgroups of G such that

- $H \cap K$=1
- *Both* H and K are normal in G

Then the subgroup HK is isomorphic to $H \times K$.

Proof. We know from Proposition 3.8 that HK is a subgroup. By the normality both H and K, the element $h^{-1}k^{-1}hk$ is a member of both H and K. This can be seen by parenthesizing appropriately

$$\underbrace{(h^{-1}k^{-1}h)}_{\in K}k \qquad h^{-1}\underbrace{(k^{-1}hk)}_{\in H}.$$

Since $H \cap K = 1$ this implies that $h^{-1}k^{-1}hk = 1$, and further that $hk = kh$. Hence all elements of H commute with all elements of K. By Corollary 3.5.1, every element in HK is a unique product hk for some $h \in H$ and $k \in K$. Thus the map $\phi : HK \to H \times K$ defined by $hk \mapsto (h, k)$ is well-defined. We now see that

$$\begin{aligned}
\phi(h_1k_1h_2k_2) &= \phi(h_1h_2k_1k_2) \qquad \text{Since H and K commute} \\
&= (h_1h_2, k_1k_2) \\
&= (h_1, k_1, k_1, k_2) \\
&= \phi(h_1k_1)\phi(h_2k_2)
\end{aligned}$$

is a homomorphism. Since every $hk \in HK$ can be uniquely expressed, it follows that there is one for every $(h, k) \in HK$ and hence ϕ is a homomorphism.

□

If, in Proposition 3.9, we add the condition that $HK = G$, we have that $G \cong H \times K$, and we would say that G is a direct product of its subgroups H and K.

So far, we have presupposed that G contains subgroups H and K fulfilling the conditions of the previous propositions. The idea of a semidirect product is to approach the matter from the other way. We begin with two general groups H and K, with a homomorphism $\phi : K \to \mathrm{Aut}(H)$ and then define a group G such that the conditions of Proposition 3.7 hold.

Theorem 3.6. Let H and K be groups. Let ϕ be a homomorphism from K into $\mathrm{Aut}(H)$, and G the set of ordered pairs (h, k). Define an operation on G by

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$

where $\cdot$ is the left action of of K on H as determined by ϕ. This makes G a group of order $|H||K|$.

Proof. The identity element is $(1_H, 1_K)$ since

$$\begin{aligned}(1_H, 1_K)(h, k) &= (1_H 1_k \cdot h, 1_H k) \\ &= (1_H h, 1_K k) \\ &= (h, k) \\ &= (hk \cdot 1_H, k 1_K) \\ = (h, k)(1_H, 1_K).&\end{aligned}$$

for all $(h, k) \in G$.

Let $(x, y) \in G$ and consider $(h, k)(x, y) = (hk \cdot x, ky)$. For (x, y) to be the inverse of (h, k) we require that

$$\begin{aligned}(hk \cdot x, ky) &= (1_H, 1_K) \\ \Leftrightarrow \qquad hk \cdot x &= 1_H, \quad ky = 1_K\end{aligned}$$

The first equation is equivalent to $x = k^{-1}h^{-1}$ and the second to $y = k^{-1}$. Hence $k^{-1}h^{-1}, k^{-1}$ is the inverse of (h, k). That they commute can be easily checked. Associativity is shown by

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

Lastly, it is clear that the order of G is the product of the orders of H and K. □

The following proposition shows that there are isomorphic copies of H and K in G.

Proposition 3.10. The sets $\{(h,1) \mid h \in H\}$ and $\{(k,1) \mid k \in K\}$ are subgroups of G such that

$$H \cong \{(h,1) \mid h \in H\} \qquad K \cong \{(k,1) \mid k \in K\}$$

Proof. We show that the finite, that $\{(h,1) \mid h \in H\}$ is closed under the group operation of G. Consider two elements $(h_1,1)$ and $(h_2,1)$. Their product is

$$\begin{aligned}(h_1,1)(h_2,1) &= (h_1 1 \cdot h_2, 11)\\ &= (h_1 h_2, 1),\end{aligned}$$

with the closure of H implying $(h_1h_2,1)$ is in the set. Clearly, $|H| = |\{(h,1) \mid h \in H\}|$ and the map $\phi : H \to \{(h,1) \mid h \in H\}$ defined by $\phi(h) = (h,1)$ has the property that

$$\begin{aligned}\phi(h_1h_2) &= (h_1h_2, 1)\\ &= (h_1 1 \cdot h_2, 11)\\ &= \phi(h_1)\phi(h_2)\end{aligned}$$

and is hence a homomorphism. It is clearly surjective and, by the two sets having equal cardinality, also injective and thus an isomorphism. □

Proposition 3.11. Identifying H and K with their isomorphic copies in G from the previous theorem, we have that

1. $H \cap K = 1$
2. $khk^{-1} = k \cdot h = \phi(k)\phi(h)$ for all $h \in H, k \in K$
3. $H \trianglelefteq G$

Proof. That $H \cap K = 1$ is clear, since otherwise some h would be an element of K or vice versa. To identify conjugation of H by K with the homomorphism ϕ we consider

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

Finally, the normality of H can be seen by noting that both $K \leq N_G(H)$, $N \leq N_G(H)$ and that $HK = G$. □

Definition 3.8. Let H and K be groups. Let ϕ be a homomorphism from K into $\mathrm{Aut}(H)$. The group G from theorem 3.6 is called the semidirect product of H and K with respect to ϕ, denoted $H \rtimes_\phi K$ or just $H \rtimes K$ when ϕ is unambiguous.

The last proposition in this section shows how the semidirect product is a generalisation of the direct product.

Proposition 3.12. Let H, K and ϕ be as in Theorem 3.6. If ϕ is the trivial homorphism then

$$H \rtimes K \cong H \times K$$

Proof. Consider any product in the group $H \rtimes K$

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2).$$

If ϕ is the trivial homorphism then $\phi_k(h) = h$ for all $k \in K$. Hence

$$(h_1 k_1 \cdot h_2, k_1 k_2) = (h_1 h_2, k_1 k_2)$$

and the semidirect product coincides with the direct product. □

4 Classification of finite groups

We have seen Example 2.3 and Example 2.4 that the groups V_4 and $\mathbb{Z}/4\mathbb{Z}$ both have order 4. Yet they have differences. For instance, in $\mathbb{Z}/4\mathbb{Z}$ the element 2 is the only non-trivial element that is equal to its own inverse, since $2 + 2 = 0$ modulo 4. But in V_4, *every* element is equal to it's own inverse. It raises a question if there are other groups of order 4 that are different from these two, and if so, how many? This will be explored in the present section.

4.1 A note on cyclic groups

For every $n \in \mathbb{Z}^+$ there exists a cyclic group C_n of order n. An example of this is the group $\mathbb{Z}/n\mathbb{Z}$ with generator 1. In the following classifications, we will only look at the non-cyclic isomorphism classes of a group G of some finite order, referring to this subsection as needed.

4.2 Groups of order p

Suppose G is a group and $|G| = p$. Let $x \in G$ be any non-trivial element, and consider the cyclic subgroup $\langle x \rangle$ generated by x. Lagrange's theorem dictates that the order of x be a divisor of p. But p being prime and x being non-trivial, the only possibility is $|\langle x \rangle| = p$, implying that $\langle x \rangle = G$. If a group has prime order, then it must be cyclic.

4.3 Groups of order p^2

In this subsection we classify groups of order p^2. We start by developing a necessarily result.

Lemma 4.1. Let G be a group of order p^2. Then G is abelian.

Proof. By Lagrange, and that $Z(G)$ is non-trivial by Corollary 3.4.1, $|Z(G)|$ is restricted to p or p^2. If the latter is true then $Z(G) = G$ and we are done. Suppose then that $|Z(G)| = p$. The quotient group $G/Z(G)$ has order $\frac{p^2}{p} = p$ and hence is cyclic: there is an element $x \in G$ such that

$$\langle xZ(G)\rangle = G/Z(G)$$

so that every $g \in G$ can be written $g = x^n z$, for some $z \in Z(G)$ and some $n \in \mathbb{Z}$. If $g_1 = x^n z_1$ and $g_2 = x^m z_2$, then

$$\begin{aligned} g_1 g_2 &= x^n z_1 x^m z_2 \\ &= x^m z_2 x^n z_1 \\ &= g_2 g_1 \end{aligned}$$

using that $z_1, z_2 \in Z(G)$ and that any element commutes with powers of itself. Note that this means $G/Z(G)$ is trivial: if G is abelian, then $Z(G) = G$, implying $G/Z(G) = G/G = 1$. □

Proposition 4.1. Let G be a non-cyclic group of order p^2 for a prime number p. Then G is isomorphic to $C_p \times C_p$.

Proof. Let a and b be distinct non-trivial elements of G and let $A = \langle a\rangle$, $B = \langle b\rangle$ be the respective cyclic subgroups they generate. Note that these subgroups have a trivial intersection, and each have order p. Since G is abelian, every subgroup is normal and hence AB is a subgroup of G, by Proposition 3.8. We have that

$$|AB| = \frac{|A||B|}{|A \cap B|} = \frac{p \cdot p}{1} = p^2$$

hence $AB = G$. Now define a map $\phi : AB \to A \times B$ by $ab \mapsto (a, b)$. Letting a_1, a_2, b_1, b_2 all be elements of G it follows that

$$\begin{aligned} \phi(a_1 b_1 a_2 b_2) &= \phi(a_1 a_2 b_1 b_2) && \text{Since } G \text{ is abelian.} \\ &= (a_1 a_2, b_1 b_2) \\ &= (a_1, b_1)(a_2, b_2) && \text{by the operation in } A \times B. \\ &= \phi(a_1 b_1)\phi(a_2 b_2). \end{aligned}$$

Since $|A \times B| = |A||B| = p^2$, ϕ is an isomorphism and hence $G \cong C_p \times C_p$. □

Recalling attention to the discussion of the V_4-group and group tables, we conclude that these are the only groups of order 4, up to isomorphism.

4.4 Groups of order p^3

The case p = 2

We begin with the non-abelian subcase, and will derive generators whose orders will determine the isomorphism type.

In a group G of order 8, the possible orders of its elements are $1, 2, 4, 8$ by Lagrange's Theorem. We know that no element can have order 8, since it implies G is cyclic, and hence abelian. The following proposition helps us show that G must have an element of order 4, by assuming all elements have order at most 2.

Proposition 4.2. Let G be a group and suppose that $|x| = 2$ for every non-identity element $x \in G$. Then G is abelian.

Proof. That $|x| = 2$ implies $x^{-1} = x$. Generally speaking, a product xy has inverse

$$(xy)^{-1} = y^{-1}x^{-1}$$

but since every element is its own inverse, the left hand side may simply be written as xy. For the same reason, we can replace y^{-1} with y and x^{-1} with x in the right hand side

$$\begin{aligned} & (xy)^{-1} = y^{-1}x^{-1} \\ \Leftrightarrow \qquad & xy = yx \end{aligned}$$

hence G is abelian. □

The proposition shows that not all elements of G can have order 2: there exists an element x of order 4. Let $X = \langle x \rangle = \{x^0, x^1, x^2, x^3\}$ and $y \in G - X$. Because $\langle x, y \rangle$ contains $\langle x \rangle$, its order is divisible by 4. Since it also contains $\langle y \rangle$, its order is greater than the order of $\langle x \rangle$. Hence $\langle x, y \rangle$ generates G.

We now examine the generators x and y. Note that the element $z = yxy^{-1}$ is in X, since X has index 2 and hence is normal. It cannot be that $z = x^0 = 1$ since that implies $x = 1$ and $\langle x, y \rangle$ won't generate G. If $z = x^1 = x$ then x and y commute, implying that the generated group G is abelian, contradicting our assumption. The only possibilty is that $z = x^3$, meaning $|z| = 4$. With this we consider the order of y.

If $|y| = 2$ then $G \cong D_8$ because G is then given by the relation

$$G = \langle x, y \mid x^4 = s^2 = 1, yx = x^{-1}y \rangle.$$

If $|y| = 4$ then $G \cong Q_8$ because G is then given by the relation

$$G = \langle x, y \mid x^4 = 1, \quad x^2 = y^2, \quad yx = x^{-1}y \rangle.$$

For an abelian group G of order 8 we will use the theory of semidirect products to classify its isomorphism types. Assuming that G is non-cyclic, no element can have order 8. Hence for non-trivial elements, the possible orders are 2 and

4. Suppose G has no element of order 4. Then every non-trivial element must have order 2. Let x, y, z be three such elements. Define

$$H = \langle x \rangle \cong C_2 \qquad \text{and} \qquad H = \langle y, z \rangle \cong C_2 \times C_2$$

The normality of H follows from G being abelian, and we also have that $K \cap H = 1$. Thus the criterion of Proposition 3.7 are fulfilled, and we can look at automorphims ϕ from $K \to \mathrm{Aut}(H)$ or equivalently

$$\begin{aligned} & \phi : C_2 \times C_2 \to \mathrm{Aut}(C_2) \\ \Leftrightarrow \qquad & C_2 \times C_2 \to C_2 \end{aligned}$$

Hence G is isomorphic to the semidirect product $C_2 \times C_2 \rtimes C_2$ for different homomorphisms ϕ. But since the only possible homomorphism is the trivial one, $G \cong C_2 \times C_2 \times C_2$.

If G does have an element of y of order 4, let $K = \langle y \rangle \cong C_4$ and let H be as previously. We thus look at autmorphisms

$$\phi : C_4 \to \mathrm{Aut}(y) = C_2.$$

Since here too, the only possible homomorphism is the trivial one, the semidirect product coincides with the direct product, and $G \cong C_4 \times C_2$.

4.4.1 The case p ≠ 2

For the case when p is an odd prime, we introduce an object known as a commutator. Intuitively it can be thought of as a measure of how 'non-abelian' a group is. The following four proposition develop its properties that will be used later.

Definition 4.1. Let G be a group and let $g, h \in G$. The *commutator* $[g, h]$ of g and h is defined as

$$[g, h] = g^{-1}h^{-1}gh.$$

Proposition 4.3. Let g and h be as in the above definition. The following is true.

1. $gh = hg[g, h]$
2. $gh = hg$ if and only if $[g, h] = 1$
3. $[g, h]^{-1} = [h, g]$.

Proof. (1) By definition $[g, h] = g^{-1}h^{-1}gh$. Thus the right hand side becomes

$$\begin{aligned} hg(g^{-1}h^{-1}gh) &= h(gg^{-1})h^{-1}gh \\ &= hh^{-1}gh \\ &= gh. \end{aligned}$$

(2) If $[g, h] = g^{-1}h^{-1}gh = 1$ then we can multiply on the left by $h^{-1}g^{-1}$ and obtain $gh = h^{-1}g^{-1} = (gh)^{-1}$ implying that g and h commute. Conversely. If $gh = hg$ then by (1) $[g, h] = 1$.

(3) follows if we compute the products $[g, h][h, g]$ and $[h, g][g, h]$. □

Proposition 4.4. Let G be a group and let $a, b, c \in G$. Then

1. $[a, bc] = [a, c](c^{-1}[a, b]c)$
2. $[ab, c] = (b^{-1}[a, c]b)[b, c]$

Proof. For a proof of 1, consider the right hand side: rewriting the leftmost commutator gives us

$$\begin{aligned} [a, c](c^{-1}[a, b]c) &= a^{-1}c^{-1}ac(c^{-1}[a, c]c) \\ &= a^{-1}c^{-1}a(cc^{-1})[a, b]c \\ &= a^{-1}c^{-1}a[a, b]c. \end{aligned}$$

Rewriting the commutator that is left then gives

$$\begin{aligned} a^{-1}c^{-1}a[a, b]c &= a^{-1}c^{-1}a(a^{-1}b^{-1}ab)c \\ &= a^{-1}c^{-1}(aa^{-1})b^{-1}abc \\ &= a^{-1}c^{-1}b^{-1}abc \\ &= a^{-1}(bc)^{-1}abc \\ &= [a, bc] \end{aligned}$$

hence the two sides are equal. The proof of 2 is analogous. □

Lemma 4.2. let g and h be elements of the group G. Suppose that g and h commute with $[g, h]$. Then

$$[g^2, h] = [g, h^2] = [g, h]^2$$

Proof. The result follows from applying proposition 4.4, letting the squared element take the role of ab or bc. □

Proposition 4.5. Suppose $g, h \in G$, both of which commute with $[g, h]$. Then

$$(gh)^n = g^n h^n [h, g]^{\frac{n(n-1)}{2}}$$

for all positive integers n.

Proof. The proof follows from induction on n. Notice that for $n = 2$, $\frac{n(n-1)}{2} = 1$ and so

$$\begin{aligned}
(gh)^n &= ghgh \\
&= ghhg[g, h] \quad \text{By (1) of Proposition 4.3} \\
&= gh^2 g[g, h] \\
&= ggh^2[h^2, g][g, h] \quad \text{By the same property} \\
&= g^2 h^2 [h, g]^2 [h, g]^{-1} \quad \text{By Corollary 4.4.1 and Property (3) of Proposition 4.3} \\
&= g^2 h^2 [h, g].
\end{aligned}$$

Suppose now that the result holds for the first $n - 1$ integers

$$(gh)^{n-1} = g^{n-1} h^{n-1} [h, g]^{\frac{(n-1)(n-2)}{2}}$$

Multiplying both sides on the right by gh we obtain

$$\begin{aligned}
(gh)^n &= g^{n-1} h^{n-1} [h, g]^{\frac{(n-1)(n-2)}{2}} gh \\
&= g^{n-1} h^{n-1} gh [h, g]^{\frac{(n-1)(n-2)}{2}}
\end{aligned}$$

since both g and h commute with $[g, h]$. to reach the induction step we now shift g and h a number of times, giving rise to additional commutators as in the base case:

$$\begin{aligned}
g^{n-1} h^{n-1} gh [h, g]^{\frac{(n-1)(n-2)}{2}} &= g^{n-1} h^{n-1} hg [g, h] [h, g]^{\frac{(n-1)(n-2)}{2}} \quad \text{By (1) of Proposition 4.3} \\
&= g^{n-1} h^n g [g, h] [h, g]^{\frac{(n-1)(n-2)}{2}} \\
&= g^{n-1} gh^n [h^n, g] [g, h] [h, g]^{\frac{(n-1)(n-2)}{2}} \\
&= g^n h^n [h, g]^n [h, g]^{-1} [h, g]^{\frac{(n-1)(n-2)}{2}} \quad \text{By Corollary 4.4.1} \\
&= g^n h^n [h, g]^{\frac{(n-1)(n-2)}{2} + n - 1} \\
&= g^n h^n {}^{\frac{n(n-1)}{2}}
\end{aligned}$$

□

Proposition 4.6. Let G be a group and $H \trianglelefteq G$. If G/H is abelian then $G' \leq H$.

Proof. See Dummit and Foote, page 169 (point 4 of Proposition 7.) □

Proposition 4.7. Let p be an odd prime, and P a non-abelian group of order p^3. Then $P' = Z(P)$.

Proof. By proposition 4.6, $P' \leq Z(P)$. Note that $|Z(P)| = p^3$ implies P is abelian. By Lemma 4.3, $|Z(P)| = p^2$ also implies P is abelian. Finally, we know by Corollary 3.4.1 that $Z(P)$ is non-trivial. Hence the only possibility is $|Z(P)| = p$, hence by Lagrange's Theorem $P' = Z(P)$. □

Proposition 4.8. Let p be an odd prime, and P a non-abelian group of order p^3. Then the map ϕ defined by $x \mapsto x^p$ is a homomorphism from P into $Z(P)$. Furthermore, the kernel of ϕ has order p^2 or p^3.

Proof. We first show that the image of ϕ is contained in $Z(P)$. Consider the image x^p for an arbitrary $x \in P$. For any other element $y \in P$

$$\begin{aligned} x^p y &= y x^p [x^p, y] \\ &= y x^p [x, y]^p \qquad \text{By Lemma 4.4.1} \\ &= y x^p \end{aligned}$$

since $P' = Z(P)$ and $|P'| = p$ by Proposition 4.7. Next we show that ϕ is a homomorphism. By definition $\phi(xy) = (xy)^p$, and by Proposition 4.5

$$(xy)^p = x^p y^p [y, x]^{\frac{p(p-1)}{2}}.$$

Since p is odd, $\frac{p-1}{2}$ is an even integer. Thus p divides $p \cdot \frac{(p-1)}{2}$ and $[y, x]^{\frac{p(p-1)}{2}} = 1$. Hence ϕ is a homomorphism.

To show that the kernel of ϕ has order p^2 or p^3, we rule out other possibilities. If $|\ker \phi| = 1$ then ϕ is injective, implying $|P| = |Z(P)|$, contradicting the assumption that P is non-abelian. By the First Isomorphism Theorem

$$P/\ker \phi \cong \text{im}\phi \leq Z(P).$$

Since $\text{im}\phi$ divides $|Z(P)|$, the only possibilities are $|\ker \phi| = p^2$ or $|\ker \phi| = p^3$. □

Remark. The equation $(xy)^p = x^p y^p [y, x]^{\frac{p(p-1)}{2}}$ would not have been satisfied if p were even, because then $p - 1$ would be odd, and the denominator would halve p itself.

We can now go on to the classification itself. Let P be a non-cyclic group of order p^3. Proposition 4.8 showed that the map ϕ defined by $x \mapsto x^p$ is a homomorphism from P into $Z(P)$, and that $\ker \phi$ has order p^2 or p^3. The first possibility implies P has an element of order p^2: there exist non-trivial elements outside of $\ker \phi$. These cannot have order p^3 since P is non-cyclic. The second possibility implies every non-trivial element has order p, since the whole group is contained in $\ker \phi$. In this paper we will confine ourselves to the first case.

P has an element of order p^2

Let x be an element of order p^2 and let $H = \langle x \rangle$. Note that since H index p, it is normal in G. If E is the kernel of the pth power map, then in this case $E \cong Z_p \times Z_p$ and $E \cap H = \langle x^p \rangle$. Let y be any element of $E - H$ and let $K = \langle y \rangle$, a cyclic group of order p. By construction, $H \cap K = 1$, and both K and H are normal in G. Hence G is isomorphic to the semidirect product $C_p \ltimes C_{p^2}$ for various homomorphisms from K into $\mathrm{Aut}(H)$, the latter being isomorphic to $C_{p(p-1)}$ by By Sylow's Theorem, $\mathrm{Aut}(H)$ has a unique subgroup of order p, so any non-trivial homomorphism must map K to this subgroup. Let γ be a generator. Then, for $x \in H$

$$\begin{aligned}
\gamma(x) &= x^{1+p} \\
\gamma^2(x) &= x^{(1+p)(1+p)} \\
&= x^{1+2p} \\
&\vdots \\
\gamma^p(x) &= x^{p^2+1} \\
&= x
\end{aligned}$$

Up to choice of generator of the cyclic group K there is only one non-trivial homomorphism ϕ from K into $\mathrm{Aut}(H)$, given by $\phi(y) = \gamma$; hence up to isomorphism there is a unique non-abelian group $K \ltimes H$. This group is given by the presentation

$$\langle x, y \mid x^{p^2} = y^p = 1, yxy^{-1} = x^{1+p} \rangle.$$

4.5 Groups of order pq

4.5.1 The case p ∤ q-1

Suppose G is a group of order pq, with $p < q$. Sylow's theorem asserts that $Syl_q(G)$ and $Syl_p(G)$ are non-empty. Let $Q \in Syl_q(G)$. Between them, the conditions

$$\begin{aligned} &n_q = 1 + kq \quad \text{for } k \geq 0 \\ &n_q \mid p \\ &p < q \end{aligned}$$

imply $k = 0$. Hence $n_q = 1$ and $Q \trianglelefteq G$. If we can show that additionally, $P \trianglelefteq G$ then the conditions of Proposition 3.9 are satisfied. Assume for now this is the case. We prove the following.

Lemma 4.3. $C_m \times C_n \cong C_{mn}$ if and only if m and n are coprime.

Proof. □

The normality of P depends on p and q. By Sylow, n_p divides q, so $n_p = 1$ or q. If $p \nmid q - 1$ then $n_p \neq q$. Hence $P \trianglelefteq G$ and we have proven that

Proposition 4.9. Let G be a group of order pq, with $p < q$. If $p \nmid q - 1$ then G is cyclic.

Remark. Stated in terms of semidirect products, $G \cong P \rtimes Q$, the condition $p \nmid q - 1$ implies the only homormophism from P to $\mathrm{Aut}(Q)$ is the trivial one.

4.5.2 The special case p | q-1 and $p = 2$

Lemma 4.4. For an abelian group G, the inversion map ϕ given by $x \mapsto x^{-1}$ is an automorphism of G.

Proof. For x_1, x_2 in G, the abelian property assures that

$$\begin{aligned} \phi(x_1 x_2) &= x_2^{-1} x_1^{-1} \\ &= x_1^{-1} x_2^{-1} \\ &= \phi(x_1)\phi(x_2) \end{aligned}$$

□

If $p = 2$ then $p \mid q - 1$ implies $p = 2$ and $q - 1 = 2m$ for some integer m. Let γ be a generator of $\mathrm{Aut}(Q)$ and let $x \in P$. There exists a non-trivial homomorphism $\phi : P \to \mathrm{Aut}(Q)$ given by $x \mapsto \gamma^m$ as can be seen by

$$\begin{aligned} \phi(x^2) &= \phi(e) \\ &= \gamma^m \gamma^m \\ &= \phi(x)\phi(x). \end{aligned}$$

The associated action has the property that, for every $y \in Q$, $x \cdot y = y^{-1}$. The element x thus acts as the inversion map of Q. Hence multiplication in the semidirect product takes the form

$$\begin{aligned}(y_1, x_1)(y_2, x_2) &= (y_1 x_1 \cdot y_2, x_1 x_2) \\ &= (y_1 y_2^{-1}, x_1 x_2)\end{aligned}$$

for $y \in Q$, $x \in P$.

Proposition 4.10. Let $P \ltimes Q$ be the group as discussed above. Let $(y, 1) = r$ and $(1, x) = s$. Then r and s satisfy the relation

$$r^q = s^2 = 1 \quad \text{and} \quad sr = r^{-1}s$$

i.e the semidirect product $P \ltimes Q$ is isomorphic to the dihedral group D_{2n}.

Proof. That $r^q = s^2 = 1$ follows from composing the elements the respective number of times. The other relation can be shown as follows

$$\begin{aligned}sr &= (1, x)(y, 1) \\ &= (1x \cdot y, x) \\ &= (y^{-1}, x) \\ &= (y^{-1}, 1)(1, x) \\ &= r^{-1}s.\end{aligned}$$

□

Depending on the choice of generator of $\mathrm{Aut}(Q)$ there are seemingly different homomorphisms from P into $\mathrm{Aut}(Q)$. That these are isomorphic to each other will not be shown in this paper.

5 References

Dummit, D.S. and Foote, R.M. (2004) Abstract Algebra. 3rd Edition, John Wiley Sons, Inc.