On Sylow's Theorems

Master's Thesis

Hayley Poutiainen

2437451

Department of Mathematical Sciences

University of Oulu

Autumn 2015

Contents

1 Introduction

The earliest study of groups seems to have taken place in parallel threads around the world. It has been suggested that the convergence of all these developments into what formed a more uniform theory took place in 1870 and was the result of a book produced by C. Jordan called, *Traité des substitutions et des équations algébriques*. The following paper explores the theorems produced by Peter Sylow, a Norwegian mathematician, whose discoveries were too late to be included in the publication by Jordan. Sylow had proved his theorems as early as 1870, but he withheld them from publication for at least two years until Jordan, assured Sylow that the theorems were both new and significant. In 1872, Sylow published a 10-page paper presenting the theorems that now bear his name. The Sylow Theorems (5.4, 5.5) form a fundamental part of finite group theory and have very important applications in the classification of finite simple groups.

Two key mathematicians play a role in this paper alongside Sylow, as a result of their influence on Sylow's development of his theory. The first being Lagrange, whose Theorem (2.15) states that the order of a subgroup must always divide the order of the group itself. The corollary to Lagrange's Theorem does not in fact hold true for all groups. That is there may not exist a subgroup whose order is a divisor of the main groups order. The simplest example of this is the Alternative Group, A_4, of order 12, which has no subgroup of order 6. The Sylow's Theorems provide a partial converse to this problem. Cauchy proved that for every prime p that divides the or-

der of a finite, abelian group, there is an element of order p that exists in the group. Cauchy's Theorem (4.2) was a direct inspiration for the theorems which Sylow developed, which were later shown to hold true for any finite group. Sylow's original proof operated within a subgroup of the symmetric group, just as Cauchy's had.

The paper follows the logical progression of the mathematical knowledge needed in order to solve Sylow's Theorems. The first major theorem explored in the paper is Lagrange's Theorem 2.15 in Chapter 2 which then leads into the development of Cauchy's Theorem 4.2 in Chapter 4. Two different proofs for Cauchy's Theorem are illustrated in Chapter 2. Cauchy's Theorem leads us to the final chapter in which Sylow's Theorems are explored. The theorems have been re-proved by a variety of mathematicians over the years. This paper explores three different versions of proof, with regard to the first statement of the Theorem (5.4), this being the theorem of existence of the subgroups. After the proofs, some of the resulting consequences that Sylow's Theorems provide are discussed. The paper finishes off with a few examples showing the practical importance the theorems play in the study of finite groups and group theory in general. Enjoy your read.

1.1 Notations

$\mathbb{Z}$ - Set of integers

$\mathbb{N}$ - Set of positive integers

$\mathbb{Q}$ - Set of rational numbers

$\mathbb{R}$ - Set of real numbers

$\mathbb{C}$ - Set of complex numbers

gcd - Greatest Common Divisor

$m \mid n$ - m divides n

$m \nmid n$ - m does not divide n

$A \subseteq G$ - A is a subset of G

$f : X \to Y$ - Function from set X to set Y

$i : X \to X, i_X$ - The identity function on X

$A \leq G$ - A is a subgroup of G

$A \trianglelefteq G$ - A is a normal subgroup of G

$|G|$ - Order of group G

$e_G = 1_G$ - Identity element of group G

$[G : H]$ - index of H in G, Number of distinct cosets of H in G.

$\langle H \rangle$ - H is a cyclic group.

S_n - Symmetric group of degree n.

$H \cong G$ - H is isomorphic to G

G/H - Factor group of G by N.

$Syl_p(G)$ - Sylow p-subgroup of G

N_p - The number of Sylow p-subgroups in G.

1.2 Useful Number Theory

Definition 1.1. *Least Integer Axiom*: There is a smallest integer in every nonempty subset C of natural numbers $\mathbb{N}$. C being nonempty simply means that there is a least one integer in C

Theorem 1.2. *(Division Algorithm) Given integers a and b with $a \neq 0$, there exist unique integers q and r with $b = qa + r$ and $0 \leq r < |a|$*

Example 1.3. If p is a prime and b is any integer, then

$$gcd(p, b) = \begin{cases} p & if\ p|b \\ 1 & otherwise \end{cases}$$

Proof. ([7], p. 40) A common divisor c of p and b is a divisor of p. But the only positive divisors of p are p and 1, and so $gcd(p, b) = p$ or 1, It is p if $p|b$, and it is 1 otherwise. □

Proposition 1.4. *If p is a prime not dividing an integer r, then for all $m \geq 1$, then $p \nmid \binom{p^m r}{p^m}$.*

Proof. Expanding the binomial coefficient:
$\binom{p^m r}{p^m} = \frac{p^m r}{p^m} \cdot \frac{(p^m r - 1)}{(p^m - 1)} \cdots \frac{p^m r - i}{p^m - i} \cdots \frac{p^m r - p^n + 1}{p^m - p^n + 1}$

For each term $\frac{p^m r - i}{p^m - i}$ of this product we make all possible cancellations of common divisors of the numerator and denominator.

For $i = 0$, we are left with r, and we know that $p \nmid r$. So the result holds when $i = 0$

For $i > 0$, let $i = p^l q$, where l is non-negative integer,and q is a positive integer not divisible by p, then $l < m$. So $\frac{p^m r - i}{p^m - i} = \frac{p^m r - p^l q}{p^m - p^l q} = \frac{p^{m-l} r - q}{p^{m-l} - q}$.
Now $p \nmid p^{m-l} r - q$ and $p \nmid p^{m-l} - q$, since $m - l > 0$.

Showing p does not divide into the product of the simplified numerators and denominators of the binomial coefficient. We can therefore conclude that $p \nmid \binom{p^m r}{p^m}$. □

Theorem 1.5. *If a and b are integers, then their gcd is a linear combination of a and b.*

Proof. ([7], p.40) We may assume that at least one of a and b is not zero (otherwise, the gcd is 0 and the result is obvious). Consider the set I of all linear combinations:

$$I = \{sa + tb : s, t \in \mathbb{Z}\}$$

Now a and b are in I (take $s = 1$ and $t = 0$ or vice versa). It follows that I contains positive integers(if $a \neq 0$, then I contains $\pm a$) and hence the set P of all those positive integers that lie in I is nonempty. By the Least Integer Axiom, P contains a smallest positive integer, say, d; we claim that d is the gcd of a and b. Since d is in I, it is a linear combination of a and b: there are integers s and t with

$$d = sa + tb \quad .$$

Let us show that d is a common divisor by trying to divide each of a and b by d. The division algorithm gives $a = qd + r$, where $0 \leq r < d$. If $r > 0$, then

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + (-qt)b \text{ is in P,}$$

contradicting d being the smallest element of P. Hence $r = 0$ and $d|a$; a similar argument shows that $d|b$.

Finally, if c is a common divisor of a and b, then $a = ca'$ and $b = cb'$, so that c divides d, for $d = sa + tb = c(sa' + tb')$. But if $c|d$, then $|c| \leq d$ and so d is the gcd of a and b. □

Corollary 1.6. *Let I be a subset of $\mathbb{Z}$ such that*

1. *0 is in I*
2. *if a and b are in I, then $a - b$ is in I*
3. *if a is in I and q is in $\mathbb{Z}$, then qa is in I*

Then there is a nonnegative integer d in I with I consisting precisely of all the multiples of d.

Proof. ([7], p.41) If I consists of only the single integer 0, take $d = 0$. If I contains a nonzero integer a, then $(-1)a = -a$ is in I, by (3). Thus, I contains $\pm a$, one of which is positive. By the Least Integer Axiom, I contains a smallest positive integer; call it d.

We claim that every element a in I is a multiple of d. The division algorithm gives integers q and r with $a = qd + r$, where $0 \leq r < d$. Since d is in I, so is qd, by (3), and so (2) gives $r = a - qd$ in I. But $r < d$, the smallest positive element of I, and so $r = 0$, thus, a is a multiple of d. □

Theorem 1.7 (Euclid's Lemma)**.** *If p is a prime and $p|ab$, then $p|a$ or $p|b$. More generally, if a prime p divides a product $a_1a_2...a_n$, then it must divide at least one of the factors of a_i. Conversely, if $m \geq 2$ is an integer such that $m|ab$ always implies $m|a$ or $m|b$, then m is a prime.*

Proof. ([7], p.41) Assume that $p \nmid a$; we must show that $p|b$. Now the $\gcd(p, a) = 1$ (see Example 1.3). By Theorem 1.5, there are integers s and t with $1 = sp + ta$, and so

$$b = spb + tab \quad .$$

Since $p|ab$, we have $ab = pc$ for some integer c, so that $b = spb+tpc = p(sb+tc)$ and $p|b$. The second statement now follows easily by induction on $n \geq 2$.

We prove the contrapositive: If m is composite, then there is a product ab divisible by m. Since m is composite, $m = ab$, where $a < m$ and $b < m$. Thus, m divides ab, but m divides neither factor, since if $m|a$, then $m < a$ □

1.3 Sets

Definition 1.8. A family of sets $\mathcal{P}$ is pairwise disjoint, if for all $A, B \in \mathcal{P}$, either $A = B$ or $A \cap B = \emptyset$

Definition 1.9. A *partition* of a set X is a family of non-emply, *pairwise disjoint* subsets (*blocks*), whose union is all of X.

Example 1.10. Let X be a finite set and $A_1, A_2, ..., A_n$ is a partition of the set X., then:

1. $X = A_1 \cup A_2 \cup ... \cup A_n$, and
2. $|X| = |A_1| + |A_2| + ...|A_n|$

1.4 Relations and Functions

Let $a, b \in S$, a *relation* is a statement, such as aRb, indicating the relationship, R, between the elements a and b from the set S.

Example 1.11. Let $\mathbb{I}$ be the set of integers, then operations such as $=$, $<$ and $\leq$ are all relations on $\mathbb{I}$.

Definition 1.12. If $a, b, c \in S$ then the relation defined by $\equiv$ is known as an *equivalence relation* if it is satisfies the following three criteria:

1. Reflexivity: $a \equiv a$
2. Symmetry: $a \equiv b \Rightarrow b \equiv a$
3. Transivity: $a \equiv b, b \equiv c \Rightarrow a \equiv c$

Example 1.13. [7], [2] Define the relation *congruence modulo* n by

$$a \equiv b \bmod n, \text{ if } n|(a-b), \text{ for } n \geq 0.$$

The *congruence modulo* n relation is in fact an equivalence relation since:

1. $n \mid 0$ and $0 = a - a \Rightarrow a \equiv a \bmod n$
2. Since $n|(a-b) \Rightarrow n|(b-a)$ we have that $a \equiv b \bmod n$ and $b \equiv a \bmod n$
3. If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $n|(a-b)$ and $n|(b-c)$. Therefore $n|((a-b)+(b-c))$, which means that $n|(a-c) \Rightarrow a \equiv c \bmod n$

Hence we have shown that, *congruence modulo* n is an equivalence relation since it is reflexive by (1), symmetric by (2) and transitive by (3).

Definition 1.14. If $\equiv$ is an equivalence relation on a set S, then $[a]$, the *equivalence class* of a, is defined by $[a] = \{b \in S | b \equiv a\} \subseteq S$

Theorem 1.15. *If $\equiv$ is an equivalence relation on a set S, then $a \equiv b$ if and only if $[a] = [b]$*

Proof. ([7], p.101) Assume that $a \equiv b$. If $c \in [a]$, then $c \equiv a$, and so transitivity gives, $c \equiv b$, hence $[a] \subseteq [b]$. By symmetry, $b \equiv a$, and this gives the reverse inclusion $[b] \subseteq [a]$. Thus $[a] = [b]$.

Conversley if $[a] = [b]$, then $a \in [a]$, by reflexivity , and so $a \in [a] = [b]$, therefore $a \equiv b$. □

Theorem 1.16. *If $\equiv$ is an equivalence relation on a set X, then the equivalence classes form a partition of X. Conversely, given a partition S of X, then there is an equivalence relation on X whose equivalence classes are the blocks in S.*

Proof. ([7], p.102). Assume that an equivalence relation $\equiv$ on X is given. Each $x \in X$, lies in the equivalence class $[x]$ because it is reflexive, it follows that the equivalence classes are non empty subsets whose union is X.

To prove pairwise disjointness, assume that $a \in [x] \cap [y]$, so that $a \equiv x$ and $a \equiv y$. By symmetry, $x \equiv a$, and so transivity gives $x \equiv y$. Therefore $x = y$, by Theorem 1.15, and so equivalence classes form a partition on X.

Conversely, let S be a partition of X. If $x, y \in X$, define $x \equiv y$ if there is $A \in S$, with $x \in A$ and $y \in A$. It is plain that $\equiv$ is reflexive and symmetric. To see that $\equiv$ is transitive, assume that $x \equiv y$ and $y \equiv z$; that is, there are $A, B \in S$ with $x, y \in A$ and $y, z \in B$. Since $y \in A \cap B$, pairwise disjointness gives $A = B$. So $x, z \in A$, that is $x \equiv z$, showing that $\equiv$ is an equivalence relation.

Now we show that the equivalence classes are subsets in S. If $x \in X$, then $x \in A$ for some $A \in S$. By definition of $\equiv$, if $y \in A$, then $y \equiv x$ and $y \in [x]$, hence $A \subseteq [x]$. For the reverse inclusion, let $z \in [x]$, so that $z \equiv x$. There is

some B with $x \in B$ and $z \in B$; thus, $x \in A \cap B$. By pairwise disjointness, $A = B$, so that $z \in A$, and $[x] \subseteq A$. Hence $[x] = A$. □

Definition 1.17. Let X and Y be sets, a *function* f from X to Y, denoted by $f : X \mapsto Y$, is a relation f from X to Y such that for every $x \in X$ there is a unique $y \in Y$ such that the ordered pair $(x, y) \in f$. For the $y \in Y$ we write the function as $y = f(x)$.

A function, in simple terms is known as a *mapping* of elements from one set to another.

Definition 1.18. The *image* of a function, such as the defined function in Definition 1.17 is set $f(Y)$ or $imgf$. It is said that y is the *image* of x under f and that x is the *preimage* of y under the function f.

A function needs to be a *well-defined*. For a function to be well defined one needs to be able to show that if there are 2 elements that are the same in X, then their image in Y needs to be the same as well. Showing the uniquness of the mapping from every element in the primage to the elements in the image. More formally, let $x, x' \in X$, then only if $f(x) = f(x')$, the relation is considered *well defined*, hence a function.

Definition 1.19. $f : X \to Y$ is an *injective(one-to-one)* function, if for every pair $x, x' \in X$, we have: $f(x) = f(x') \implies x = x'$.

Definition 1.20. $f : X \to Y$ is *surjective (onto)* if for each $y \in Y$, there is some $x \in X$, with $y = f(x)$ or alternatively $imf = Y$.

Definition 1.21. $f : X \to Y$ is *bijective* if it is both *injective* (1.19) and *surjective* (1.20). There is a one-to-one correspondence between the elements of sets X and Y.

Proposition 1.22. *Let X and Y be sets, and let $f : X \to Y$ be a function. Then*

1. *If $T \subseteq S$ are subsets of X, then $f(T) \subseteq f(S)$, and if $U \subseteq V$ are subsets of Y, then $f^{-1}(U) \subseteq f^{-1}(V)$.*

2. *If $U \subseteq Y$, then $ff^{-1}(U) \subseteq U$; if f is a surjection then $ff^{-1}(U) = U$.*

3. *If $T \subseteq X$, then $T \subseteq f^{-1}f(T)$; if f is an injection, then $T = f^{-1}f(T)$.*

Proof. ([7], p.98) See Proposition 2.14. □

Example 1.23. $f : \mathbb{N} \mapsto \mathbb{Z}$ be defined by, $f : x \mapsto 2x$.

1. f is *well-defined*. If $x = x' \implies 2x = 2x'$, in other words $f(x) = f(x')$.

2. f is *injective*. If $f(x) = f(x')$, then $2x = 2x' \implies x = x'$

3. f is not *surjective*. The image of f is the set $im(f) = \{2, 4, 6, 8, ...\}$ and $im(f) \neq \mathbb{Z}$.

2 Groups

2.1 Preliminaries

Definition 2.1. : Group Axioms: A non-empty set G, is a group if there is a defined operation $*$ on G such that:

1. For all $a, b \in G$, $a * b \in G$ (Closure)

2. For $a, b, c \in G$, $(a * b) * c = a * (b * c)$ (Associativity)

3. There exists $e \in G$ such that, for all $a \in G$ the following $a*e = e*a = a$ holds. (Existence of an identity element, identified as e_G)

4. For every $a \in G$, there exists $b \in G$, such that, $a*b = b*a = e$ (Inverse, $b = a^{-1}$)

Definition 2.2. G is a *finite group* if it has a finite number of elements. The number of elements in G is called the *order* of G and is denoted by $|G|$. If $a \in G$, then the order of the element a is the least positive integer n such that $a^n = e$.

Lemma 2.3. *Let G be a group and assume that $a \in G$ has a finite order k. If $a^n = 1$, then $k|n$. In fact, $\{n \in \mathbb{Z} : a^n = 1\}$ is the set of all multiples of k*

Proof. ([7], p.136)
It is easy to see that $I = \{n \in \mathbb{Z} : a^n = 1\} \subset \mathbb{Z}$ satisfies the hypothesis of Corollary 1.6: $a^0 = 1$; if $a^n = 1$, and $a^m = 1$, then $a^{n-m} = a^n a^{-m} = 1$; if $a^n = 1$ and if q is any integer, then $a^{qn} = (a^n)^q = 1$. Therefore, I consists of all the multiples of k, where k is the smallest positive integer in I. But the smallest positive k in I is, by definition, the order of a. Therefore, if $a^n = 1$, then $N \in I$, and so n is a multiple of k. □

Definition 2.4. A group G is called *abelian* if it satisfies the commutative law. That is $a * b = b * a$ for every $a, b \in G$

Definition 2.5. A non-empty subset H of a group G is a *subgroup* if, under the operation $*$:

1. $e \in H$

2. if $a, b \in H$, then $a * b \in H$

3. if $a \in H$, then $a^{-1} \in H$

If the above properties hold, H is a subgroup of G and denoted by $H \leq G$.

Remark 2.6. :

1. $\{e\}$ and G are always subgroups of a group G, where $\{e\}$ denotes the subset consisting of the single element e. They are known as *trivial* subgroups.

2. H a subgroup of G is called a *proper* subgroup if $H \neq G$, denoted by $H < G$

3. H a subgroup of G is called a *nontrivial* subgroup if $H \neq \{1\}$

Example 2.7. Let $A \subset \mathbb{Q} \setminus \{0\}$, where $A = \{1, -1\}$. It is known that $\mathbb{Q} \setminus \{0\}$ is a group under multiplication. Then $(A, \cdot) \leq (\mathbb{Q} \setminus \{0\}, \cdot)$, since the *subgroup* properties as defined in Definition 2.5 hold. That is, (1) $e = 1 \in A$ is the identity under multiplication, (2) $1 \cdot -1 = -1 \in A$ and lastly (3) $1 \cdot -1 = -1 = e \in A$, hence they are each others inverse and are in A.
However if the defined operation is addition. We have that $(A, +) \not\leq (\mathbb{Q}, +)$. Closure (2) is not met, since $1 + (-1) = 0 \notin A$. Hence $A \not\leq \mathbb{Q}$ under the operation of addition.

Theorem 2.8. *The intersection $\cap_{i \in I} H_i$ of any family of subgroups of a group G is a subgroup of G. In particular if H and K are subgroups of G then $(H \cap K) \leq G$.*

Proof. ([7], p.152)

Let $D = \cap_{i \in I} H_i$.

(1) $D \neq \emptyset$, since $e \in H_i$ for all $i \implies e \in D$.

(2) If $x, y \in D$, then $x, y \in H_i$ for all i, hence since each H_i is a subgroup for each i then the product $xy \in H_i$ for each $i \implies xy \in D$.

(3) If $x \in D$, then $x \in H_i$, for all i, since each H_i is a subgroup of each i then $x^{-1} \in H_i$ for all $i \implies x^{-1} \in D$.

Showing that $D = \cap_{i \in I} H_i$ satisfies the criteria for a subgroup as laid out in definition 2.5 and so $\cap_{i \in I} H_i \leq G$ □

If $H \leq G$, Lagrange's Theorem 2.15 claims that the order of the subgroup H is a divisor of the order of the finite group G . It is clear that $|H| \leq |G|$. In order to prove Lagrange's Theorem, the concept of *cosets* is introduced.

2.2 Cosets and Lagrange's Theorem

Definition 2.9. *Cosets*

1. Let H be a sugroup of group G, where the operation defined on G is $*$. If $a \in G$, define a *left coset* as $aH = \{a * h | h \in H\}$ and a *right coset* as $H * a = \{ha | h \in H\}$.

2. The set of all left cosets is denoted by G/H, as is the set of all right cosets of H in G.

Example 2.10. The set $H = \langle [5] \rangle = \{[0], [5], [10], [15]\}$ is a subgroup of the cyclic group $\mathbb{Z}_{20}$. The distinct cosets of H in $\mathbb{Z}_{20}$ are:

$[0] + H = \{[0], [5], [10], [15]\}$

$[1] + H = \{[1], [6], [11], [16]\}$

$[2] + H = \{[2], [7], [12], [17]\}$

$[3] + H = \{[3], [8], [13], [18]\}$

$[4] + H = \{[4], [9], [14], [19]\}$

Not all the cosets are subgroups of $\mathbb{Z}_{20}$. Only $[0] + H$ is a subgroup of $\mathbb{Z}_{20}$. The different cosets of the example are *pairwise disjoint*. In fact the cosets *partition* $\mathbb{Z}_{20}$

$|H| = 4$ and $|\mathbb{Z}_{20}| = 20$, and $20 \div 4 = 5$ which is the number of distinct cosets of H in $\mathbb{Z}_{20}$.

We are now at a point where we can introduce an *equivalence relation* which is used in the proving of Lagrange's Theorem 2.15. It is a special case of the previous *congruence modulo n*, Example 1.13.

Definition 2.11. If H is a subgroup of group G. Define a relation on G by $a \equiv b$ if $a^{-1}b \in H$.

Example 2.12. The relation, $\equiv$, as defined above is infact an *equivalence relation* on G, since it satisfies the following:

Proof. :

1. Reflexivity: If $a \in G$, then $a^{-1}a = e \in H \implies a \equiv a$.

2. Symmetry: If $a \equiv b$, then $a^{-1}b \in H$. Since H is a subgroup of G, and subgroups are closed under inverses, $(a^{-1}b)^{-1} = b^{-1}a \in H \implies b \equiv a$

3. Transitivity: If $a \equiv b$ and $b \equiv c$, then $a^{-1}b, b^{-1}c \in H$, since H is a subgroup of G, and subgroups are closed under multiplication, $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}c \in H \implies a \equiv c$

□

Proposition 2.13. *Cosets are equivalency classes. Let G be a group, $H \leq G$, $a \in G$ and $[a]$ the equivalency class under $\equiv$. Then $[a] = aH$*

Proof. Suppose $x \in [a]$. Then $x \equiv a$, so $a^{-1}x \in H$. There is some $h \in H$ with $a^{-1}x = h$ with $x = ah \in aH$ which means $[a] \subseteq aH$. Now, let $x \in aH$, then $x = ah$, for some $h \in H$. Then $a^{-1}x = a^{-1}(ah) = eh = h \in H$. Showing $aH \subseteq [a]$. Hence proving that $aH = [a]$. □

Lemma 2.14. *Let H be a subgroup of a group G, and let $a, b \in G$*

1. *$aH = bH$ if and only if $b^{-1}a \in H$. In particular, $aH = H$ if and only if $a \in H$.*
2. *If $aH \cap bH \neq \varnothing$, then $aH = bH$*
3. *$|aH| = |H|$ for all $a \in G$.*

Proof. :

1. $aH = bH \iff [a] = [b]$ (Proposition 2.13) $\iff a \equiv b \iff a^{-1}b \in H$. The second statement follows because $H = 1H$, we have $aH = H = eH \iff a = e^{-1}a \in H$
2. If $x \in aH \cap bH$, then $x = ah = bh^{'}$ for some $h, h^{'} \in H$, and so $b^{-1}a = h^{'}h^{-1} \in H$. Therefore, $aH = bH$. Recall Theorem 1.16, the equivalence classes, form a partition of set S, by Proposition 2.13, so to do the cosets partition G.

3. Define a function $f : H \to aH$, given by $f(h) = ah$. f is injective since if $f(h_1) = f(h_2)$, then $ah_1 = ah_2$ hence, $h_1 = h_2$. Further, take $y \in ah$, then $y = ah$ for some $h \in H$. So $f(h) = ah = y$, thus f is surjective. Which means that f is a bijection from H to aH, hence $|aH| = |H|$.

□

We now get to the first major theorem in the development of the theory leading up to the Sylow's Theorems, Lagranges's Theorem.

Theorem 2.15 (Lagrange's Theorem)**.** *If H is a subgroup of a finite group G, then $|H|$ is a divisor of $|G|$.*

Proof. ([7], p.156)
Let $a_1H, a_2H, ..., a_tH$ be the family of all the distinct left cosets of H in G. Then

$$G = a_1H \cup a_2H \cup .... \cup a_tH$$

because $g \in G$ lies in the coset gH and $gH = a_iH$ for some i. Moreover Lemma 2.14 (2), shows that distinct cosets a_iH and a_jH are disjoint. It follows that

$$|G| = |a_1H| + |a_2H| + ... + |a_tH| \quad .$$

But $|a_iH| = |H|$ for all i, by Lemma 2.14 (3), so that $|G| = t \cdot |H|$, as desired. □

Remark 2.16. t represents the number of distinct left cosets of H in G.

Definition 2.17. Let G be a group and $H \leq G$, the *index* of H in G is the number of distinct left cosets of H in G. The *index* is denoted by $[G : H]$. $|G| = t \cdot |H| = [G : H] \cdot |H| \implies [G : H] = |G|/|H|$

Remark 2.18. Looking at Example 2.10. The strength of Lagrange's Theorem is clear. Since,

1. In this example the 5 cosets as laid out in the example are distinct and partition the set $\mathbb{Z}_{20}$.

2. Each coset has the same cardinality as H,
   $|H| = |[0] + H| = |[1] + H| = ... = 4$

3. The number of left cosets from the example above is 5 and the index is $[G : H] = \frac{|G|}{|H|} = \frac{20}{4} = 5$.

Proposition 2.19. *If $H \leq G$ and $[G : H] = 2$, then $g^2 \in G$ for every $g \in G$.*

Proof. See [7], Proposition 2.97(i), p. 167. □

2.3 Cyclic Groups and Related Properties

Definition 2.20. If G is a group and $a \in G$, write

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\text{all powers of } a\ \}$$

$\langle a \rangle$ is called the *cyclic* subgroup of G generated by a. If $G = \langle a \rangle$ is a cyclic group with generator a, then G is generated by the subset $X = \{a\}$. Cyclic groups are abelian (Definition 2.4) groups.

Theorem 2.21. *A group G of prime order is cyclic.*

Proof. ([2], p.60) Let $H \leq G$, then by Lagrange's Theorem 2.15, $|H|$ divides $|G|$. However since $|G| = p$, with p being a prime, this means that $|H| = 1$ or $|H| = |G| = p$.

So if $H \neq \langle e \rangle$, then $H = G$.

Take $a \in G$, with $a \neq e$, the powers of a form a subgroup $\langle a \rangle$ of G, different from $\langle e \rangle$. So this subgroup is all of G. Meaning that any $x \in G$ is of the form $x = a^n$. Hence, G is cyclic by Definition 2.20. □

Refer to the difference between the order of a group and the order of an element as outlined in Definition 2.2. Now we can add that the order of a is the number of elements in $|\langle a \rangle|$.

Theorem 2.22. *If G is a finite group and $a \in G$, then the order of a divides $|G|$.*

Proof. The order of element a is $|\langle a \rangle|$. Since $\langle a \rangle \leq G$, by Lagrange's Theorem 2.15, $|\langle a \rangle|$ / G □

2.4 Homomorphisms and Isomorphisms

Identifying homomorphic and isomorphic relationships between two groups is a way of determining whether or not two groups are in any way the same.

Definition 2.23. if $(G, *)$ and $(H, \circ)$ are groups, then a function $f : G \to H$ is a *homomorphism* if:

$$f(x * y) = f(x) \circ f(y)$$

for all $x, y \in G$.

A homomorphism preserves the operation of G, but need not be injective.

If f is a bijection (Definition 1.21), then f is called an *isomorphism*. Two groups G and H are called isomorphic, denoted by $G \cong H$, if there exists an isomorphism $f : G \to H$.

Example 2.24. Let the two groups be $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$, where addition in $\mathbb{Z}_n$ is defined by $[a] + [b] = [a + b]$.

Define $f : \mathbb{Z} \to \mathbb{Z}_n$ by $f(a) = [a]$. So

$$f(a + b) = [a + b] = [a] + [b] = f(a) + f(b) \quad .$$

Showing that f is a *homomorphism* from $\mathbb{Z}$ to $\mathbb{Z}_n$

Example 2.25. Let G and Hbe finite cyclic groups of the same order m and assume that $G = \{1, a, a^2, ..., a^{m-1}\} = \langle a \rangle$ and $H = \{1, b, b^2, ..., b^{m-1}\} = \langle b \rangle$.

Define $f : G \to H$ by $f(a^i) = b^i$ for $a \leq i < m$. It follows that f is a bijection.

To see that f is a homomorphism (hence an isomorphism), we need to show that $f(a^i a^j) = f(a^i)f(a^j)$ for all i and j with $0 \leq i, j < m$.

If $i + j < m$, then

$$f(a^i a^j) = f(a^{i+j}) = b^{i+j} = b^i b^j = f(a^i)f(a^j).$$

Now if $i + j \geq m$, then $i + j = m + r$, where $0 \leq r < m$, so that $a^{i+j} = a^{m+r} = a^m a^r = a^r$, since $a^m = 1$, similarly $b^{i+j} = b^r$.

So for $i + j \geq m$ we can show that

$$f(a^i a^j) = f(a^{i+j}) = f(a^r) = b^r = b^{i+j} = b^i b^j = f(a^i)f(a^j) \quad .$$

This shows that f is an isomorphism and $G \cong H$. Now following from Theorem 2.21 , any two groups of prime order are isomorpic.

Proposition 2.26. *If f is a homomorphism of G onto H, then:*

1. $f(e_G) = e_H$

2. $f(a^{-1}) = f(a)^{-1}$ *for all* $a \in G$

Proof. See [2], Hernstein, Pg 70, Lemma 2.5.2 □

Definition 2.27. If $f : G \to H$, define

$$kernel f = ker f = \{x \in G | f(x) = 1_H\}$$
$$image f = im f = \{h \in H | h = f(x) \text{ for some } x \in G\}$$

Proposition 2.28. *Let* $f : G \to H$ *be a homomorphism.*

1. $ker f \leq G$ *and* $im f \leq H$

2. *If* $x \in ker f$ *and if* $a \in G$, *then* $axa^{-1} \in ker f$

3. f *is an injection if and only if* $ker f = \{1\}$

Proof. See [7], Rothman, Pg 164, Proposition 2.93 □

2.5 Normal Subgroups

Definition 2.29. A subgroup H of a group G is called a *normal subgroup* if $h \in H$ and $g \in G$ imply $ghg^{-1} \in H$. If H is a *normal* subgroup of G one writes $H \trianglelefteq G$.

Definition 2.30. The subgroup H of G is said to be a *normal subgroup* of G if $aHa^{-1} \subset H$ for every $a \in G$.

A subgroup H, of group, G, is a normal subroup, if and only if every left coset is equal to every right coset in the group. The following theorem formalises this assertion.

Theorem 2.31. *H is a subgroup of G, now $H \trianglelefteq G$ if and only if $aH = Ha$ for every $a \in H$.*

Proof. ([7], p.178) (1) Assume $H \trianglelefteq G$. Let $ah \in aH$. Since H is normal, then $aha^{-1} \in H$. Let $aha^{-1} = h' \in H$, then $ah = (aha^{-1})a = h'b \in Ha$. Showing $aH \subseteq Ha$.

Now take $ha \in Ha$. Since H is normal, $(a^{-1})h(a^{-1})^{-1} = a^{-1}ha \in H$. Let $a^{-1}ha = h" \in H$, Then , $ha = a(a^{-1}ha)bh" \in aH$ showing that $Ha \subseteq aH$. Showing that if H is normal in G, then $aH = Ha$.

(2) Assume that $aH = Ha$ for all $a \in G$. If $h \in H$, then $ah \in aH = Ha$; hence, there is $h' \in H$ such that $ah = h'a$, so that $aha^{-1} = h' \in H$. Showing that $H \rhd G$ □

Remark 2.32. (1) It is clear from Proposition 2.28 (2) that the $kerf \trianglelefteq G$

(2) If a group G is an abelian group, then every subgroup H, is infact a normal subgroup. Since $h \in H$ and $g \in G$, then $ghg^{-1} = gg^{-1}h = h \in H$

2.6 Factor Groups

Theorem 2.33. *Let $G/K = \{[a] : a \in G\} = \{aK | a \in G\}$ denote the family of all the cosets of a subgroup K of G. If $K \trianglelefteq G$, then G/K is a group under the operation $aKbK = abK$ for all $a, b \in G$.*

Proof. See [7], Rotman, Pg 179, Theorem 2.113 □

The group G/K is called the *Factor (Quotient) Group* G mod K. When G is finite, its order $|G/K| = |G|/|K|$, that is the *index* of K in G, the number of distinct cosets of K in G.

Example 2.34. ([1], p.97) The group $H = \{[0], [5], [10], [15]\}$ is a normal subgroup of the additive abelian group $\mathbb{Z}_{20}$.

The distinct cosets in the factor group $\mathbb{Z}_{20}/H$ are:

$[0] + H = \{[0], [5], [10], [15]\} = H$,

$[1] + H = \{[1], [6], [11], [16]\}$,

$[2] + H = \{[2], [7], [12], [71]\}$,

$[3] + H = \{[3], [8], [13], [18]\}$ and

$[4] + H = \{[4], [9], [14], [19]\}$

The operation is coset addition. E.g.

$([3] + H) + ([4] + H) = ([3] + [4]) + H = [3 + 4] + H = [7] + H = [2] + H$.

$|H| = 4$, $\mathbb{Z}_{20} = 20$

The index of H in $\mathbb{Z}_{20} = |\mathbb{Z}_{20}|/|H| = 4|20 = 5 =$ the number of distinct cosets in the factor group $\mathbb{Z}_{20}/H$

Theorem 2.35. *Every normal subgroup is the kernel of some homomorphism. In other words, if $K \trianglelefteq G$, then there exists a homomorphism, $f : G \to G/K$ such that $kerf = K$.*

Proof. If $K \trianglelefteq G$. Define the most natural mapping $f : G \to G/K$ as $f(a) = aK$. With the product as defined in G/K, that is $aKbK = abK$. Now $f(a)f(b) = aKbK = abK = f(ab)$. Thus f is a (surjective) homomorphism. Since K is the identity element in G/K, we have $kerf = \{a \in G | f(a) = K\} = \{a \in G | aK = K\} = K$, by Lemma 2.14 □

2.7 Homomorphism Theorems

The next logical step towards developing the Sylow Theorems is to study the relationships between the groups and subgroups. In doing this we can establish the relationships that develop as a result.

The *First Isomorphism Theorem* shows that every homomorphism gives rise to an isomorphism and that factor groups are merely constructions of homomorphic images. Let G be a group and $f : G \to H$ is a homomorphism. If K is the kernel of f, then we know $K \trianglelefteq G$, so the subgroup G/K can be formed. The *First Isomorphism Theorem* shows the relationship between H and G/K.

Theorem 2.36. ***(First Isomrphism Theorem).***

If $f : G \to H$ is a homomorphism, then

$$kerf = K \trianglelefteq G \text{ and } G/K = G/kerf \cong imf$$

In more detail, if $kerf = K$, then the function $g : G/K \to imf \leq H$, given by $g(aK) = f(a)$, is an isomorphism.

Proof. It is clear that $kerf = K \trianglelefteq G$, (Remark 2.32).

If $aK = bK$ then $a = bk$ for some $k \in K$. Hence $f(a) = f(bk) = f(b)f(k)$, since f is well defined. Since $k \in K$, so $f(k) = e_H$. Hence $f(a) = f(b)$, so by the defintion of the mapping of g this means that $g(aK) = g(bK)$, showing that g is well defined.

Since f is a homomorphism and $g(aK) = f(a)$, we have $g((aK)(bK)) = g(abK) = f(ab) = f(a)f(b) = g(aK)g(bK)$. Showing that g is a homomorphism.

It is clear that the $img \leq imf$.

For the reverse inclusion, note that $y = f(a)$ for some $a \in G$, so $y = f(a) = g(aK)$, thus g is surjective.

Finally, to show g is injective. Suppose that $g(aK) = g(bK)$, then $f(a) = g(aK) = g(bK) = f(b)$. Hence we have

$e_H = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \implies ab^{-1} \in Kerf = K$

from Proposition 2.26 and Lemma 2.14 (1). This means that $aK = bK$, showing g is injective.

Showing that $g : G/K \to imf \leq H$ is an isomorphism. □

The *Correspondence Theorem*, is then an extension of the First Isomorphism Theorem. It shows there is a 1-1 corresnpondence between subgroups of G and those subgroups of G that contain K.

Theorem 2.37. ***(Correspondence Theorem).***

Let $f : G \to G'$ be a homomorphism of G onto G' where $kerf = K$. If $H' \leq G'$ and $H = \{a \in G | f(a) \in H'\}$ then

(1) $H \leq G$,

(2) $K \subset H$ and

(3) $H/K \cong H'$ and

(4) if $H' \trianglelefteq G'$, then $H \trianglelefteq G$.

Proof. (1) Showing that H is a subgroup of G: $e \in H$, so $H \neq \emptyset$. If $a, b \in H$, then $f(a), f(b) \in H'$. Hence $f(a)f(b) = f(ab) \in H'$, since $H' \leq G'$, proving $ab \in H$. That is H is closed. Finally, If $a \in H$, then $f(a) \in H'$. Hence $f(a^{-1}) = f(a)^{-1} \in H'$ (Proposition 2.26). Since $H' \leq G'$, then $a^{-1} \in H$.

(2) $f(K) = \{e'\} \subset H'$, where e' is the unit element of G', therefore $K \subset H$.

(3) Since $K \trianglelefteq G$ and $K \subset H$, we have that $K \trianglelefteq H$. The mapping f restricted to H, defines a homomorphism of H onto H', with $Kerf = K$. Therefore by The First Isomorphism Theorem 2.36 we get $H/K \cong H'$

(4) If $H' \trianglelefteq G'$ and if $a \in G$, then $f(a)^{-1}H'f(a) \subset H'$. So $f(a^{-1})H'f(a) \subset H'$ (Proposition 2.26). This tells us that $f(a^{-1}Ha) \subset H'$, so $a^{-1}Ha \subset H$. So by Definition 2.30, $H \trianglelefteq G$. □

3 Group Actions

Definition 3.1. If G is a group and $a \in G$, then a *conjugate* of g is any element in G of the form aga^{-1}, where $a \in G$. Define $g^a = aga^{-1}$ as the conjugate of g in G.

Note that a subgroup $H \leq G$ is a normal subgroup if and only if it contains all the conjugates of its elements.

Definition 3.2. Let $\emptyset \neq H \subset G$, then the set defined by $H^g = \{h^g | h \in H\}$ is the conjugate set of H in G. Now if H is a subgroup of a group G, then a conjugate set of H is a subgroup of the form

$$H^a = aHa^{-1} = \{aha^{-1} : h \in H\} \quad ,$$

where $a \in G$.

Example 3.3. *Conjugacy* is infact an equivalence relation and thus an equivalency class as defined in Definition 1.14 .

Proof. Define the relation $x \sim y$ for $x, y \in G$ as follows: $\exists a \in G$ such that $x^a = axa^{-1} = y$.

1. $x^1 = 1x1^{-1} = x \implies x \sim x$

2. $x \sim y \implies x^a = y \implies y^{a^{-1}} = x \implies y \sim x$

3. $x \sim y$ and $y \sim z \implies x^a = y$ and $y^b = z \implies (x^a)^b = z \implies x^{ab} = z \implies x \sim z$

□

Definition 3.4. If G is a group and $g \in G$, then define *conjugation* $\gamma_g : G \to G$ by $\gamma_g(a) = gag^{-1}, \forall a \in G$.

Definition 3.5. If G acts on X and $x \in X$, then the *orbit* of x, denoted by $\mathcal{O}(x)$ is the subset of X

$$\mathcal{O}(x) = \{gx : g \in G\} \subseteq X;$$

If G acts on X and $x \in X$, then the *stabilizer* of x, denoted by G_x, is

$$G_x = \{g \in G : gx = x\} \leq G$$

Lemma 3.6. *If G acts on a set X, then X is the disjoint union of the orbits. If X is finite, then*

$$|X| = \textstyle\sum_i \mathcal{O}(x_i) \quad ,$$

where one x_i is chosen from each orbit.

Proof. ([7], p.185) If $x \in X$, then $x = 1x \in \mathcal{O}(x)$, and so $X = \bigcup_{x \in G} \mathcal{O}(x)$. If $z \in \mathcal{O}(x) \cap \mathcal{O}(y)$, then there are $g, h \in G$ with $gz = z = hy$; hence, $x = g^{-1}hy$ and $y = h^{-1}gx$. We claim that $\mathcal{O}(x) = \mathcal{O}(y)$. If $u \in \mathcal{O}(x)$, then $u = g'x$ for some $g' \in G$, and so $u = g'ghy \in \mathcal{O}(y)$; thus $\mathcal{O}(x) \subset \mathcal{O}(y)$. For the reverse inclusion, if $v \in \mathcal{O}(y)$, then $v = h'y = h'h^{-1}gx \in \mathcal{O}(x)$. Therefore, $\mathcal{O}(x) = \mathcal{O}(y)$, and so distinct orbits are disjoint.

The count given in the second statement is correct: Since the orbits are disjoint, no element in X is counted twice. □

Corollary 3.7. *If a finite group G acts on a set* X*, then the number of elements in any orbit is a divisor of $|G|$*

Proof. This follows from Lagrange's Theorem 2.15. □

Example 3.8. Let $X = \{1, 2, 3, 4, 5\}$. S_5 is a group of all permutations on X. If $G \leq S_5$, then G is a permutation group of degree 5.

The following can be shown to be an equivalence relation on set X:

$$i \sim j \iff \exists g \in G \text{ such that } g(i) = j$$

Based on Theorem 1.16, Example 1.10 and Lemma 3.6, we can then infer that X is made up of its equivalency classes $T_1, T_2, ...T_r$ (where each $T_i = \mathcal{O}(x_i)$). Thus

$$X = \bigcup_{i=1}^{r} T_i \text{ and } |X| = \sum_{i=1}^{r} |T_i| \quad .$$

Note that T represents the orbits of G in X with $j \in T$, and $T = \{g(j) | g \in G\}$.

Now let $G = \langle (123) \rangle = \{(1), (123), (132)\}$

The *orbits* of G in S_5 are:

$T_1 = \{1, 2, 3\}$, $T_2 = \{4\}$ and $T_3 = \{5\}$.

Thus,

$X = T_1 \cup T_2 \cup T_3 = \{1, 2, 3, 4, 5\}$ and

$|X| = |T_1| + |T_2| + |T_3| = 3 + 1 + 1 = 5$.

It is clear that the number of elements in each the orbits divide into $|G| = 3$, confirming Corollary 3.7.

The *stabiliser* for $G_1 = \{(1)\}$ and for $G_4 = \{(1), (123), (132)\}$. Note that $|G_1| = 1$ and $|G_4| = 3$.

The following theorem connects the orbit ($\mathcal{O}(x)$) size for each $x \in G$, to the index size of the stabiliser (G_x) of an element in G, that is $[G : G_x]$.

Theorem 3.9. *If G acts on a set X and $x \in X$, then*

$$|\mathcal{O}(x)| = [G : G_x]$$

Proof. ([7], p.199) Let G/G_x denote the family of all the cosets of G_x in G. We will exhibit a bijection $f : \mathcal{O}(x) \to G/G_x$, and this will give the result since $|G/G_x| = [G : G_x]$ by Lagranges Theorem 2.15.
If $y \in \mathcal{O}(x)$, then $y = gx$ for some $g \in G$; define $f(y) = gG_x$.
Now f is single-valued: if $y = hx$ for some $h \in G$, then $h^{-1}gx = x$ and $h^{-1}g \in G_x$; hence $hG_x = gG_x$.
To see that f is injective, suppose that $f(y) = f(z)$; then there are $g, h \in G$ with $y = gx$, $z = hx$, and $gG_x = hG_x$; that is $h^{-1}g \in G_x$. It follows that $h^{-1}gx = x$, and so $y = gx = hx = z$
Finally f is a surjection: if $gG_x \in G/G_x$, then let $y = gx \in \mathcal{O}(x)$ and note that $\mathcal{O}(y) = gG_x$. □

Example 3.8 continued. Since $|\mathcal{O}(x)| = [G : G_x] = \frac{|G|}{|G_x|}$. We can use this to help us find the size of the orbits or stabilisers in G. Confirming the findings above, we have:
(1) $|T_1| = \frac{|G|}{|G_1|} = \frac{3}{1} = 3$, 3 elements in the orbit of the element 1.
(2) With a bit of manipulation, $|G_1| = \frac{|G|}{|T_1|} = \frac{3}{3} = 1$, confirming the stabilizer of 1 has 1 element in it.

Definition 3.10. If $H \leq G$, then the *normalizer* of H in G is the subgroup

$$N_G(H) = \{a \in G : H^a = aHa^{-1} = H\}$$

Remark 3.11. (1) $H \rhd N_G(H)$,(2) $N_G(H) \leq G$

Definition 3.12. let $\emptyset \neq H \subset G$. The *centraliser* is the set defined as:

$$C_G(H) = \{g \in G | gh = hg, \forall h \in H\}$$

Remark 3.13. (1) $C_G(H) \leq G$, (2) $C_G(H) \trianglelefteq N_G(H)$.

Definition 3.14. Let a group G act on itself by conjugation as described in Definition 3.4. If $x \in G$, then $\mathcal{O}(x) = \{y \in G | y = axa^{-1}$, for some $a \in G\}$. $\mathcal{O}(x)$ is called the *conjugacy class* of x, often denoted by x^G.

If $x \in G$, then the stabilizer of G_x of x is $C_G(x) = \{g \in G | gxg^{-1} = x\}$. This subgroup of G, consisting of all $g \in G$ that commute with x, is called the *centralizer* of $x \in G$

Proposition 3.15. *If x lies in a finite group G, then the number of conjugates of x is the index of its centralizer:*

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

and hence it is a divisor of G.

Proof. Theorem 3.9 states that $|\mathcal{O}(x)| = [G : G_x]$. Definition 3.14 states that $x^G = \mathcal{O}(x)$ and $C_G(x) = G_x$. □

Definition 3.16. The *center* of a group is denoted by $Z(G)$ and is defined to be $Z(G) = \{z \in G : zg = gz, \forall g \in G\}$

The center of a group is used in many of the coming sections. A few of its basic properties are:

(1) $Z(G)$ contains all the elements that commute with all the other elements in G.

(2) A group is abelian if and only if $Z(G) = G$.

(3) A group is centerless if $Z(G) = 1_G$.

(4)

$$\begin{aligned} Kerf &= \{a \in G | f(a) = e_G\} \\ &= \{a \in G | axa^{-1} = x, \forall x \in G\} \\ &= \{a \in G | ax = xa, \forall x \in G\} \\ &= Z(G). \end{aligned} \tag{1}$$

Now since $kerf \trianglelefteq G \implies Z(G) \trianglelefteq G$.

(5) If the congugacy class x^G of an element x in a group consits of x alone, then x commutes with every $g \in G$, for $gxg^{-1} = x$, that is $x \in G$.

Conversely, if $x \in Z(G)$, then $x^G = \{x\}$.

Therefore, the center $Z(G)$ consists of all those elements in G where $|x^G| = 1$.

Definition 3.17. The *class equation* of a finite group G is:

$$|G| = |Z(G)| + \textstyle\sum_i [G : C_G(x_i)]$$

Where x_i is selected from each conjugacy class having more than one element.

Example 3.18. The following example will verify the class equation for S_3.

(1) Firstly we will find the congugacy classes for S_3:

In the symmetric group, conjugacy preserves the cycle type. Hence by specifyig a cycle type it is the same as specifying a partition of n.

Two-cycles in S_3 are conjugate $\iff$ They have the same cycle length.

$S_3 = \{(1), (12), (21), (23), (123), (132)\}$, $|S_3| = 3! = 6$.

S_3 has 3 conjugacy classes. Those being:

$\{(1)\}$, $\{(12), (13), (23)\}$ and $\{(123), (132)\}$

Thus:

$Z(S_3) = (1)$, $|Z(S_3)| = 1$,

$C_{S_3}((12)) = \{(12), (13), (23)\}$, $|C_{S_3}((12)| = 3$,

$C_{S_3}((123)) = \{(123, (132))\}$, $|C_{S_3}((123))| = 2$.

(2) Verifying the class equation:

$|Z(S_3)| = 1$

$[S_3 : C_{S_3}((12))] = \frac{6}{3} = 2$

$[S_3 : C_{S_3}((123))] = \frac{6}{2} = 3$

Showing that:

$|S_3| = Z(S_3) + [S_3 : C_{S_3}((12))] + [S_3 : C_{S_3}((123))] = 1 + 2 + 3 = 6$.

Proposition 3.19. *Let y be a group element of order m; if $m = pt$ for some prime p, then y^t has order p.*

Proof. $y^m = 1$ and $m = pt$. Now $y^m = y^{pt} = (y^t)^p = 1$, showing that the order of $y^t = p$. □

Theorem 3.20. *If G is a group of order p^n, where p is a prime, then $Z(G)$, the center of G, is not trivial (i.e. there exists an element $a \neq e$ in G such that $ax = xa$ for all $x \in G$)*

Proof. We shall use the class equation (Definition 3.17) to carry out the proof. Let $z = |Z(G)|$; Where z is the number of elements in G whose conjugacy class has only one element. Since $e \in Z(G)$, $z \geq 1$. For any element

b outside $Z(G)$, its conjugacy class contains more than one element and $|C_G(b)| < |G|$. Moreover, since $|C_G(b)|$ divides $|G|$ by Lagranges Theorem 2.15, $|C_G(b)| = p^{n(b)}$, where $1 \leq n(b) < n$. We divide the pieces of the class equation into two parts: that coming from the center, and the rest. We get, this way,

$$p^n = |G| = z + \sum_{b \notin Z(G)} \frac{|G|}{|C_G(b)|} = z + \sum_{n(b)<n} \frac{p^n}{p^{n(b)}} = z + \sum_{n(b)<n} p^{n-n(b)}$$

Clearly, p divides the left-hand side, p^n, and divides $\sum_{n(b)<n} p^{n-n(b)}$. The net result of this is that $p|z$, and since $z \geq 1$, we have that z is at least p. So since $z = |Z(G)|$, there must be an element $a \neq e$ in $Z(G)$, which proves the theorem. □

4 Cauchy's Theorem

Cauchy's Theorem (Theorem 4.2 and Theorem 4.5) shows that if a prime p divides the order of a *finite* group G, then G contains an element of order p. Part (1) of Proposition 4.1 below is similar to Cauchy's Theorem, however the requirements in Proposition 4.1 are that G needs to be *finite* as well as *abelian*. Proposition 4.1 is included as it illustrates a general technique which involves pulling back information from G/N to get information about G.

Proposition 4.1. *Let G be a finite abelian group.*

1. *When p is a prime divisor of $|G|$, then G contains an element of order p.*

2. *G has a subgroup of order d for every divisor of $|G|$.*

Proof. ([7], p.185)
(1) We prove, by induction on $n = |G|$, that for every prime divisor p of $|G|$, there is an element of order p in G.
The base step $n = 1$ is true, for there are no prime divisors of 1.
For the inductive step, choose $a \in G$ of order $k > 1$. If $p|k$, say $k = pl$, then Proposition 3.19 says that a^l has order p. If $p \nmid k$, consider the cyclic subgroup $H = \langle a \rangle$. Now $H \trianglelefteq G$, because G is abelian (Remark 2.32 (2)), and so the quotient group G/H exists. Note that $|G/H| = n/k$ is divisible by p, and so the inductive hypothesis gives an element $bH \in G/H$, with $|bH| = p$. If b has order m then $(bH)^m = b^m H = H$ in G/H, and so Lemma 2.3 gives $p|m$. We have returned to the first case.
(2) We prove the general result by induction on $d \geq 1$.

The base step $d = 1$ is obviously true. So we may assume that $d > 1$, that is, that d has a prime divisor say, p.

By induction, G contains a subgroup H of order p. Since G is abelian, we have $H \trianglelefteq G$, and so the quotient group is defined.

Moreover $|G/H| = |G|/p$, so that $(d/p) \mid |G/H|$.

The inductive hypothesis gives a subgroup $S^* \leq G/H$, where $S^* = d/p$. By The Correspondence Theorem 2.37, there is an intermediate subgroup S with $S^* = S/H$, $(H \leq S \leq G)$. Therefore, $|S| = p|S^*| = p \cdot (d/p) = d$. □

Theorem 4.2. *(Cauchy). If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. ([7], p.200) We prove the theorem by induction $|G|$, the base step $|G| = 1$ is true as there are no prime divisors of 1. If $x \in G$, then the number of conjugates of x is $|x^G| = [G : C_G(x)]$, where $C_G(x)$ is the centralizer of x in G. As noted above, if $x \notin Z(G)$, then x^G has more than one element, and so $|C_G(x) < |G|$. If $p \mid |C_G(x)|$ for some noncentral x, then the inductive hypothesis says there is an element of order p in $C_G(x) \leq G$, and we are done. Therefore, we may assume that $p \nmid |C_G(x)|$ for all noncentral $x \in G$. Better, since $|G| = [G : C_G(x)]|C_G(x)|$, Euclid's Lemma 1.7 gives

$$p \mid [G : C_G(x)].$$

After recalling that $Z(G)$ consists of all those elements $x \in G$ with $|x^G| = 1$, we may use Lemma 3.6 to see

$$|G| = |Z(G)| + \textstyle\sum_i [G : C_G(x_i)],$$

where one x_i is selected from each conjugacy class having more than one element. Since $|G|$ and all $[G : C_G(x_i)]$ are divisible by p, it follows that

$|Z(G)|$ is divisible by p. But $Z(G)$ is abelian, and so Lemma 4.1 says that $Z(G)$, and hence G contains an element of order p. □

James McKay [4] provided an alternative method to proving Cauchy's Theorem which makes use of the notion of group actions. The proof appeared in the American Mathematical Monthly in 1959.

Definition 4.3. (An extension of the equivalence relation as defined in Example 3.8 which is used in the proof below.)

Let X be a set, let $f \in S_n$.

Define a relation on X as follows:

$$x \sim y \text{ if } x = f^i(y), \text{ for some integer } i$$

This is an *equivalence relation* on X.

The equivalence class of x, $[x]$ is called the *orbit* of x under f, denoted by $\mathcal{O}(x)$.

X is the disjoint union of the orbits of its elements.

If $f^k(x) = x$, then $f^{tk}(x) = x$, for some t, k integers.

Lemma 4.4. *If $f \in S_n$ is of order p, p being a prime, then the orbit of any element of the set X under f has 1 or p elements.*

Proof. Let $x \in X$; if $f(x) = x$, then the orbit of x under f consists merely of x itself, so has one element. Suppose that $f(x) \neq x$. Consider the elements $x, f(x), f^2(x), ..., f^{p-1}(x)$; we claim that these p elements are distinct and constitute the orbit of x under f. If not, then $f^i(x) = f^j(x)$ for some $0 \leq i < j \leq p-1$, which gives us that $f^{j-1}(x) = x$. Let $m = j-i$; then $0 < m \leq p-1$ and $f^m(x) = x$ and since $p \nmid m$, $ap + bm = 1$ for some integers a and b. Thus

$f^1(x) = f^{ap+bm}(x) = f^{ap}(f^{bm}(x)) = f^{ap}(x) = x$, since $f^m(x) = f^p(x) = x$. This contradicts that $f(x) \neq x$. Thus the orbit of x under f consists of $x, f(x), f^2(x), ..., f^{p-1}(x)$, so as p elements. □

Theorem 4.5. *(Cauchy, proof by McKay) If p is a prime and divides the order of G, then G contains an element of order p.*

Proof. ([4] as shown in [2], p.89) If $p = 2$, there is an element $a \neq e$ such that $a = a^{-1}$ which results in $a^2 = e$. Proving the theoremen statement holds true when $p = 2$.

Assume that $p \neq 2$. Let $X = \{(a_1, a_2, ..., a_{p-1}, a_p) : a_1a_2...a_{p-1}a_p = e\}$,the set of *ordered* p-tuples, where $a_1, a_2, ..., , a_p \in G$.

Claim: $|X| = n^{p-1}$ when $n = |G|$.

We can choose $a_1, ..., a_{p-1}$ arbitrarily in G, and by putting $a_p = (a_1a_2...a_{p-1})^{-1}$, the p-tuple $(a_1, a_2, ..., a_{p-1}, a_p)$ then satisfies

$$a_1a_2...a_{p-1}a_p = a_1a_2...a_{p-1}(a_1a_2...a_{p-1}^{-1}) = e,$$

so is in X. Thus X has n^{p-1} elements.

If $a_1a_2...a_{p-1}a_p = e$ then, $a_pa_1a_2...a_{p-1} = e$ (for if $xy = e$ in a group, then $yx = e$). So the mapping $f : X \to X$ defined by $f(a_1, ..., a_p) = (a_p, a_1, a_2, ..., a_{p-1})$ is in S_n. Note that $f \neq i_X$, the identity map on X, and that $f^p = i_X$, so f is of order p.

If the orbit of x under f has one element, then $f(x) = x$. On the other hand, if $f(x) \neq x$, we know that the orbit of x under f consists precisely of p distinct elements, this we have by Lemma 4.4.

Now when is $f(x) \neq x$?

We claim that $f(x) \neq x$ if and only if when $x = (a_1, a_2, ..., a_p)$, then for some

$i \neq j$, $a_i \neq a_j$. So $f(x) = x$ if and only if $x = (a, a, ..., a)$ for some $a \in G$.

Let m be the number of $x \in X$ such that $f(x) = x$; since for $x = (e, e, ..., e)$, $f(x) = x$, we know that $m \geq 1$. On the other hand if $f(x) \neq x$, the orbit of x consists of p elements, and these orbits are disjoint, for they are equivalence classes. If there are k such orbits where $f(x) \neq x$, we get that $n^{p-1} = m + kp$, for we have accounted this way for every element of X.

But $p|n$ by assumption and $p|(kp)$. So we must have $p|m$, since $m = n^{p-1} - kp$. Because $m \neq 0$ and $p|m$, we get that $m > 1$. This says that there is an $x = (a, a, ..., a) \neq (e, e, ..., e)$ in X; from the definition of X this implies that $a^p = e$. Since $a \neq e$, a is the required element of order p. $\square$

5 Sylow's Theorems

5.1 Theory and Theorems of Sylow's

Definition 5.1. :

1. *p-group* : If p is a prime, then a *p-group* is a group of order p^n for some $n \geq 0$

2. Subgroup $M < G$ is a *maximal subgroup* of G when: $M < H \leq G \implies H = G$

3. Let p be prime. A Sylow p-subgroup of a finite group G is a *maximal p-subgroup* P. That is if $Q \leq G$ is a p-subgroup and $P \leq Q$ then $P = Q$.

Proposition 5.2. *Let $H \trianglelefteq G$ be a finite group, let p be a prime. Then if both H and G/H are p-groups, then $|G|$ is a p-group.*

Lemma 5.3. *Let P be a Sylow p-subgroup of a finite group G.*

1. *Every conjugate of P is a Sylow p-subgroup*

2. *$p \nmid |N_G(P)/P|$.*

3. *If $a \in G$ has order some power of p and if $aPa^{-1} = P$, then $a \in P$.*

Proof. ([7], p. 492) (1) If $a \in G$, then aPa^{-1} is a p-subgroup of G, if it is not a maximal such, then there is a p-subgroup Q with $aPa^{-1} < Q$. Hence $P < a^{-1}Qa$, contradicting the maximality of P.
(2) If p divides $|N_G(P)/P|$, then Cauchy's Theorem 4.2 shows that $N_G(P)/P$ contains an element aP of order p, and hence $N_G(P)/P$ contains a subgroup

$S' = \langle aP \rangle$ of order p. By the Correspondence Theorem (Theorem 2.37) there is a subgroup S with $P \leq S \leq N_G(P)$ such that $S/P \cong S'$. By Proposition 5.2 S is a p-subgroup of $N_G(P) \leq G$ strictly larger than P, and this contradicts the maximality of P. We conclude that p does not divide $|N_G(P)/P|$.
(3) By Definition 3.10, the element a lies in $N_G(P)$. If $a \notin P$, then the coset aP is a non trivial element of $N_G(P)/P$ having order some power of p, in light of part (ii), this contradicts Lagrange's Theorem 2.15 □

Since every conjugate of a Sylow p-subgroup is itself a subgroup, it seems natural to let G act by conjugation (Definition 3.4) on a set of Sylow p-subgroups. We have now developed the theory to a point where we are able to go through the 'three parts' which constitute Sylow's Theorems.

For the first Theorem we provide proof of existence of the subgroups. Over the years since Sylow first proved the existence of the subgroups Sylow's Theorems have been re-proved using a variety of techniques. In this paper we provide three different proofs. The first is outlined by Rotman [7], the second is laid out as in Hernstein [2], while the third is a proof constructed by Wielandt [11], in 1959 and is based on based on combinatorial arguments and an application of group action methods. Wielands proof does not make use of Cauchy's Theorem.

Theorem 5.4. *Sylow*

If G is a finite group of order $p^l m$, where p is a prime and $p \nmid m$, then every Sylow p-group P of G has order p^l.

Proof 1 ([7], p.493)

We first show that $p \nmid [G : P]$. Now

$$[G : P] = [G : N_G(P)][N_G(P) : P]$$

.

The first factor, $[G : N_G(P)] = r$, is the number of conjugates of P in G, and we know that $r \equiv 1 \ mod \ p$; hence, p does not divide $[G : N_G(P)]$. The second factor is $[N_G(P) : P] = |N_G(P)/P|$; this, too, is not divisible by p, by Lemma 5.3(2). Therefore, p does not divide $[G : P]$, by Euclid's Lemma 1.7. Now $|P| = p^k$ for some $k \leq e$, and so

$$[G : P] = |G|/|P| = p^l m/p^k = p^{l-k} m$$

. Since $p \nmid [G : P]$, we must have $k = l$, thus $|P| = p^l$.

□

Proof 2 ([2], p.105)

If $l = 0$, this is trivial.

We therefore assume that $l \geq 1$. We proceed by induction on $|G|$, assuming the result to be true for all groups H such that $|H| < |G|$.

Suppose that the result is false for G. Then by our induction hypothesis, p^l cannot divide $|H|$ for any subgroup H of G if $H \neq G$. In particular, if $a \notin Z(G)$, then $C_G(a) \neq G$, hence $p^l \nmid |C_G(a)|$. Thus p divides $|G|/|C_G(a)| = [G : C_G(a)]$ for $a \notin Z(G)$.

Write down the class equation, definition 3.17, for G following the lines of the argument in Theorem 3.20. If $|Z(G)| \geq 1$ and

$$p^l m = |G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C_G(a)]$$

.

However $p|[G : C_G(a)]$ if $a \notin Z(G)$, so $p| \sum_{a \notin Z(G)} [G : C_G(a)]$. Since $p|p^n m$,

we get $p||Z(G)|$. By Cauchy's Theorem 4.2 there is an element a of order p in $Z(G)$. If A ia the subgroup generated by a, then $|A| = p$ and $A \trianglelefteq G$, since $a \in Z(G)$.

Consider $B = G/A$; $|B| = |G|/|A| = p^n m/p = p^{n-1}m$. Since $|B| < |G|$, by our induction hypothesis B has a subgroup M of order p^{n-1}. However by the Correspondence Theorem 2.37 there is a subgroup P of G such that $P \supset A$ and $P/A = M$. Therefore, $|P| = |M||A| = p^{n-1}p = p^l$ and P is the sought after subgroup of G of order p^l, contradicting our assumption that G has no such subgroup.

□

Proof 3 ([11], as reproduced by [7], p.494)

If X is the family of all subsets of G having exactly p^e elements, then $|X| = \binom{p^l m}{p^l}$; by Proposition 1.4, $p \nmid |X|$.

Now G acts on X: define gB, for $g \in G$ and $B \in X$, by $gB = \{gb : b \in B\}$. If p divides $|\mathcal{O}(B)|$ for every $B \in X$, then p is a divisor of $|X|$, for X is the disjoint union of orbits, by Lemma 3.6. As $p \nmid |X|$, there exists a subset B with $|B| = p^l$ and with $|\mathcal{O}(B)|$ not divisible by p. If G_B is the stabilizer of this subset B, then Theorem 3.9 gives $[G : G_B] = |\mathcal{O}(B)|$, and so $|G| = |G_B| \cdot |\mathcal{O}(B)|$.

Since $p^l \mid |G|$ and $p \nmid |\mathcal{O}(B)|$, repeated application of Euclid's Lemma 1.7 gives $p^l \mid |G_B|$. Therefore, $p^l \leq |G_B|$.

For the reverse inequality, choose an element $b \in B$ and define a function $f : G_B \to B$ by $g \mapsto gb$. Note that $f(g) = gb \in bB = B$, for $g \in G_B$, the stabilizer of B. If $g, h \in G_B$ and $h \neq g$, then $f(h) = hb \neq gb = f(g)$, that is

f is an injection. We conclude that $|G_B| \leq |B| = p^e$ and so G_B is a subgroup of G of order p^e.

□

The last theorem we present as two sections. Their discovery was and still is vital when one is working with finite groups whose properties are unknown. They provide information about the subgroups themselves.

Theorem 5.5. *Sylow*

Let G be a finite group, and let P be a Sylow p-subgroup for some prime p.

1. *Every Sylow p-subgroup is conjugate to P.*
2. *If there are r Sylow p-subgroups, then r is a divisor of $|G|/p^l$ and*
   $r \equiv 1 \mod p$

Proof. ([7], p.492) Let $X = \{P_1, ..., P_r\}$ be the set of all conjugates of Q, where we have denoted P by P_1. If Q is any Sylow$p$-subgroup of G, then Q acts on X by conjugation (3.4): if $a \in Q$, then it sends
$\gamma_a(P_i) = \gamma_a(g_i P g_i^{-1}) \mapsto a(g_i P g_i^{-1})a^{-1} = (ag_i)P(ag_i)^{-1} \in X$.
By Corollary 3.7, the number of elements in any orbit is a divisor of $|Q|$, that is, every orbit has size some power of p (because Q is a p-group) . If there is an orbit of size 1, then there is some P_i with $aP_ia^{-1} = P_i$ for all $a \in Q$. By Lemma 5.3, we have $a \in P_i$ for all $a \in Q$, that is, $Q \leq P_i$. But Q, by being a Sylow p-subgroup, is a maximal p-subgroup of G, and so $Q = P_i$. In particular, if $Q = P_1$, then every orbit has size a power of p except one, the orbit consisting of P_1 alone. We conclude that $|X| = r \equiv 1 \; mod \; p$.

Suppose now that there is some Sylow p-subgroup Q that is not a conjugate of P ; thus, $Q \neq P_i$ for any i. Again, we let Q act on X, and again, we ask if there is an orbit of size 1, say $\{P_j\}$. As in the previous paragraph, this implies $Q = P_j$, contrary to our present assumption that $Q \notin X$. Hence, there are no orbits of size 1, which says that each orbit has a size of p. It follows that $|X| = r$ is a multiple of p, that is, $r \equiv 0 \ mod \ p$, which contradicts the congruence $r \equiv 1 \ mod \ p$. Therefore, no such Q can exist, and so all Sylow p-subgroups are conjugate to P.

Finally, since all Sylow p-subgroups are conjugate, we have

$r = [G : N_G(P)]$, and so r is a divisor of $|G| = p^l m$. However $(r, p) = 1$ since $r \equiv 1 \ mod \ p$, showing that $r|p^l m \implies r|m$, that is $r \mid |G| \ /p^l$ □

5.2 Practical Consequences of Sylow's

In this section we outline a number of the practical consequences of Sylow's Theorems in a less theoretical manner.

Let : $|G| = p^\alpha m$ - The number of elements in G, where $p \nmid m$.

$Syl_p(G)$ - The set of Sylow p-subgroups of G.

N_p - The number of Sylow p-subgroups in G.

1. N_p has to divide into $|G|/p^\alpha$, combining this with the condition that $N_p \equiv 1(p)$ cuts down the number of candidates for N_p.

   Proof. If we take any $P = Syl_p(G)$, then
   $N_p = [G : N_G(P)] = |G|/|N_G(P)|$. Since $N_G(P)$ contains P, its order contains p^α as a factor. So $|G|/|N_G(P)|$ has no factor of p left in it. □

2. If $Syl_p(G) \trianglelefteq G \iff |Syl_p(G)| = 1$.

   Proof. Sylow's theorem says that we get all theSylow p-subgroups by picking one of them, say P, and then studying all the possible conjugates gPg^{-1}. Now $N_p(G) = 1 \iff gPg^{-1} = P$ for all $g \in G \iff P \trianglelefteq G$ □

3. If G is an abelian group, then any subgroup is normal. So abelian groups have exactly one $Syl_p(G)$ for each p.

4. If $G = p^n$, $(n \geq 1)$, then $Z(G) > 1$, meaning the centre of the group is a non-trivial normal subgroup in G.

5. If $|G| = p$, where p is a prime, then G is a cyclic group.

6. If $|G| = p^2$, then G is an abelian group.

7. Sylow p-subgroups for different primes can only have trivial intersections.

   Proof. If p_1, p_2 are distinct primes and $P_1 \in Syl_{p1}(G), P_2 \in Syl_{p2}(G)$, then $P_1 \cap P_2$ is a subgroup of both P_1 and P_2. So by Lagranges Theorem 2.15, its order has to divide $|P_1|$ as well as $|P_2|$, but since they are both primes, the only common factor they have is 1. So $P_1 \cap P_2 = 1$. □

8. Distinct groups of the same prime order can only have trivial intersections.

Example 5.6. $P_1, P_2 \in Syl_p(G)$ where $|P_1| = |P_2| = p$, then $P_1 \cap P_2$ is a subgroup and has to have $|P_1 \cap P_2| = 1$ or p . If it has order p then $P_1 = P_2$. If P_1 and P_2 are distinct subgroups then $|P_1 \cap P_2| = 1$.

9. The subgroups whose order is the largest power of p dividing into $|G|$, are conjugate to each other.

The list of consequnces is based upon notes from S. Ma'u ([3], p.7-8) and Ryhmäteoria class notes from M. Niemenmaa [5].

5.3 Application of Sylow's Theorems

For this last section we will study the Alternative Group A_4 to illustrate a few of the strengths Sylow's Theorems bring to Group Theory.

Alternating Group A_4			
Cycle Structure	Elements	Element Order	Parity
(a)	(1) - identity element	1	Even
$(ab)(cd)$	$(12)(34), (13)(24), (14)(23)$	2	Even
(abc)	$(123), (124), (142)(132), (134), (143), (234), (243)$	3	Even

Example 5.7. Lagrange's Theorem 2.15 states that the order of a subgroup divides the order of a group. However the corollary of this theorem is not necessarily true. A_4 is an example where the corollary does not hold true. *Claim:* A_4 does not have a subgroup of order 6.

$|A_4| = 12$. Let us assume that there exists a subgroup of H with the order of 6. Then $[G : H] = 2$.

Since the index is 2, then by Proposition 2.19, we have that for every $\alpha \in A_4 \implies \alpha^2 \in H$ for all $\alpha \in H$. If α is a 3-cycle, then α has order 3, so that $\alpha = \alpha^4 = (\alpha^2)^2$. Thus H contains every 3-cycle. This is a contradiction for there are 8 3-cycles in A_4 and $6 = |H| < 8$.

Example 5.8. *What are the Sylow subgroups for A_4?*

$|A_4| = 12 = 2^2 \cdot 3^1$.

Lets first find the **Sylow 3-subgroups** ($Syl_3(A_4)$).

The $Syl_3(A_4)$ have order 3. There are 8 elements of order 3 in A_4. Every group of order 3 is cyclic, so it is easy to write down four such subgroups:

$\{(1), (123), (132)\} = \langle(123)\rangle$,

$\{(1), (124), (142)\} = \langle(124)\rangle$,

$\{(1), (134), (143)\} = \langle(134)\rangle$,

$\{(1), (234), (243)\} = \langle(234)\rangle$.

Next note that the $|Syl_3(A_4)|$ in A_4 is 1 mod 3 and divides 8, and so there are either 1 or 4 such subgroups. But we have already found four such subgroups, so these account for all the Sylow 3-subgroups in S4.

Thus the four $Syl_3(A_4)$ are the four cyclic groups:

$\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$, and $\langle(234)\rangle$.

Now let us see which are the **Sylow 2-subgroups** ($Syl_2(A_4)$) in A_4.

$|Syl_2(A_4)| = 12/3 = 2^2$. If we look at the elements of A_4, we can note that there are three elements of order 2, none of order 4 and one of order 1. These elements whose orders are powers of 2 must be in a single $Syl_2(A_4)$, which is then a normal subgroup of A_4. The only $Syl_2(A_4)$ subgroup is

therefore the following:

$\{(1), (12)(34), (13)(24), (14)(23)\} = \langle (12)(34), (14)(23) \rangle$.

This subgroup is sometimes called the *Klein* subgroup of A_4.

Example 5.9. Assume that a group G has an order of 12. Then either G has a normal $Syl_3(G)$ or it is isomorphic to A_4.

Proof. $12 = 2^2 \cdot 3$. We know $n_3 | 2^2 = 4$ and $n_3 \equiv 1 \mod 3$. So it can be either 1 or 4.

1. If $n_3 = 1$, then $\exists P \trianglelefteq G$ such that $| = 3|P| = 3$.

2. If $n_3 = 4$, then we know that the four $Syl_3(G)$ are acted on by G, by conjugation. Let $S = \{P_1, P_2, P_3, P_4\}$. The action of G gives us a homomorphism $f : G \to S_4$.

   We show that f is injective and $imf = A_4$ which shows that $G \cong imf = A_4$.

   1) *Injective*: To show this is true, we show that $Kerf = 1$.

$$\begin{aligned} Kerf &= \{g \in G : gP_ig^{-1} = P_i, \forall P_i \in S\} \\ &= \bigcap_{i=1}^{4} N_G(P_i) \end{aligned} \tag{2}$$

   We know that for each i: $n_3 = [G : N_G(P_i)] = |G|/|N_G(P_i)|$, so $|N_G(P_i)| = 12/4 = 3$. Since $P_i \leq N_G(P_i)$ and $|P_i| = 3$, we can conclude that $P_i = N_G(P_i)$.

   So $kerf = \bigcap_{i=1}^{4} N_G(P_i)$

Each P_i are distinct groups of prime order, where $|P| = 3$. (See the Practical Consequences of Sylow's, point 8). Showing that $kerf = 1$ and proving that f is indeed injective where $G \cong imf$.

2) $imf = A_4$. G has 4 subgroups,P_1, P_2, P_3, P_4 . Each of these subgroups has two elements of order 3 and the identity element. The two elements of order three have to be different for each P_i.

Therefore G contains $2 \cdot 4 = 8$ distinct elements of order 3. Since $G \cong imf$, these 8 distinct elements of order 3 have to map to 8 distinct elements of order 3 in S_4. Now the only elements of order three in S_4 are the 3-cycles. And 3-cycles are even permutations, so are elements in A_4.

So $(A_4 \cap imf) \leq A_4$ and $(A_4 \cap imf) \leq imf$ with at least 8 elements. However, $|A_4| = |imf| = 12$ $(A_4 \cap imf)|12$. The only factor of 12 that is greater than or equal to 8 is 12. So $A_4 \cap imf$ is a subgroup of both A_4 and imf of size 12, and since both have 12 elements in, it means $A_4 \cap imf = A_4 = imf$. Showing that $G \cong A_4$.

□

References

[1] Paul.E.Bland: *The Basics of Abstract Algebra*. W.H.Freeman and Company, United States of America, 2001.

[2] I.N. Herstein: *Abstract Algebra, 3rd ed.* Prentice Hall, Upper Saddle River, NJ, 1995.

[3] S. Ma'u: *Notes on Sylows Theorems*, Lecture notes. Link: https://math.berkeley.edu/ kpmann/SylowNotes.pdf, Accesed: October 2015.

[4] James McKay: *Another proof of Cauchy's group theorem*, American Math. Monthly, 66, p. 119, 1959.

[5] M. Niemenmaa: *Ryhmäteoria 800660S*. Lecture notes.

[6] M. Niemenmaa:*Algebra II 80043A*. Lecture notes.

[7] Joseph.J. Rotman: *A First Course in Absract Algebra, 2nd ed.* Prentice Hall, Upper Saddle River, NJ, 2000.

[8] Joseph.J.Rotman: *Advanced Modern Algebra*. Prentice Hall, Upper Saddle River, NJ, 2002.

[9] Joseph.J.Rotman: *An Introduction to the Theory of Groups*, Springer-Verlag, New York, 1995.

[10] John S. Rose: *A course on Group Theory*. Dover Publications, Cambridge, England, 2012.

[11] H. Wielandt: *Ein Beweis fur die Existenz der Sylowgruppen.* Archiv der Mathematik, 10:401 - 402, 1959.