People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research Higher

Normal School of Technological Education

SKIKDA

Department of Mathematics & Computer Sciences

Dissertation

Presented to obtain a degree in mathematics as a teacher of secondary school

Entitled

Classification of Finite Simple Groups

Presented by:

- Benrebiaa Khaoula
- Souillah Amani

Board of Examiners:

President: Bentimama Ouiam	MCA	ENSET SKIKDA
Supervisor: Aiech Messab	MAA	ENSET SKIKDA
Examiner: Ferrag Azouz	MCB	ENSET SKIKDA
Examiner: Ghomrani Sarra	MCA	ENSET SKIKDA

June's session 2024


بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

The Classification of Finite Simple Groups

K.Benrebiaa/A.Souileh

2023/2024

Abstract

In this dissertation, we introduce the classification of the finite simple groups. we start by reviewing Fundamental concept of group then fundamental theorems of finite group, last not least we study the known simple groups in oder to know their characterestics.
Finally we touch classification theorem and its applications.

Résumé

Dans cette mémoire, nous introduisons la classification des groupes simples finis. Nous commençons par revoir le concept fondamental de groupe, puis les théorèmes fondamentaux des groupes finis, enfin nous étudions les groupes simples connus afin de connaître leurs caractéristiques. Enfin, nous abordons le théorème de classification et ses applications.

Key Words: Finite group, Simple group, Classification, Isomorph.

Acknowledgements

We praise Allah Almighty who enabled us to accomplish this work.

Our deepst gratitude to our sepervisor Mr. Aiech Messab, who proposed the topic of this dissertation.

We would like to extend our warmest thanks to the board of examiners for the valuable time they devoted to evaluate this research and for their contribution by their suggestions and remarks to ameliorate the quality of this modest study.

We cannot find words to show our deepest appreciation to ourteachers who brought out the best in us. Without them, this dissertation would not have been possible.

Last but not least, we place on record our sense of thankfulness to one all who directly or indirectly have lent their hand in this venture.

Thanks to all.

Dedication:

بسم الله الرحمان الرحيم

الحمد لله رب العالمين والصلاة والسلام على أشرف المرسلين سيدنا محمد وعلى آله وصحبه اجمعين

First of all, all praise is due to Allah for his guidance to accomplish this work…

I dedicate this work with all my infinite love and gratitude to the inhabitants of my heart…

To the beating heart, a symbol of tenderness, love and sacrifice, to the one who's sincere prayers were the secret of my success, the one who sacrificed for me and was striving for my happiness permanently, to you alone my beloved **Mother**.

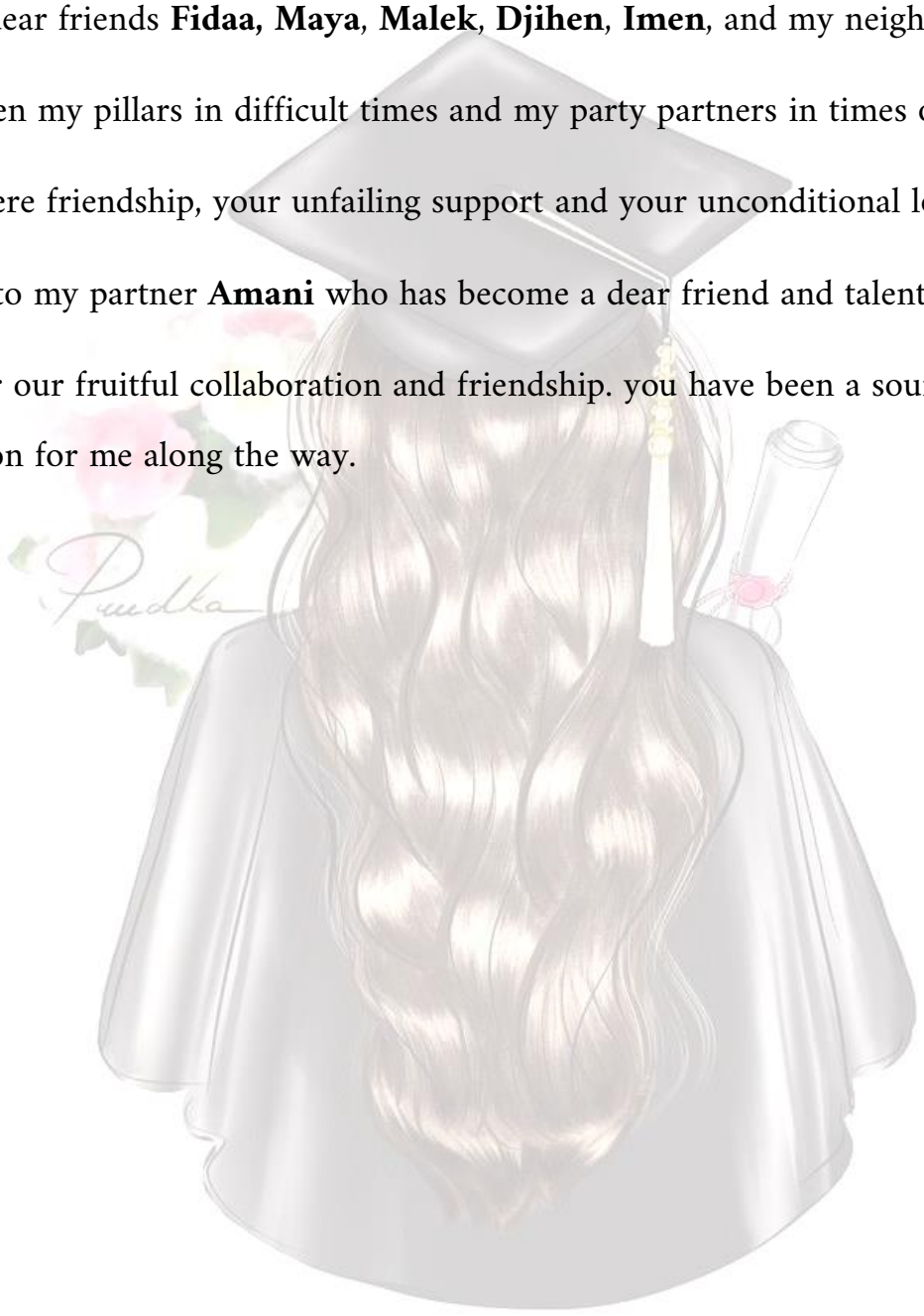
To my first love, to my departed **Father** (رحمه الله), I would like to share with you my first achievements. I hope my feelings reach you and proved that you are the best father, and the best educator.

To those who are our sanctuary and a symbol of our pride, to my brothers **Yacin**, **Nabil**, **Farouk** and my sisters **Bouthaina** and **Meriem** who are also my best friends, thank you for your constant support, your contagious humor and your comforting presence. you are my source of joy and happiness, and I am proud to have you in my life.

To my nephews **Bara**, **Abdeslam**, **Sanad**, **Ahmed** and **Haroun**, who filled my life with so much happiness and joy.

To my dear friends **Fidaa, Maya**, **Malek**, **Djihen**, **Imen**, and my neighbor **Nadjoua**, Who have been my pillars in difficult times and my party partners in times of joy, thank you for your sincere friendship, your unfailing support and your unconditional love.

Finally, to my partner **Amani** who has become a dear friend and talented collaborator, thank you for our fruitful collaboration and friendship. you have been a source of inspiration and motivation for me along the way.



Khaoula Benrebiaa.

Dedication:

First of all, all praise is due to Allah for his guidance to accomplish this work…

“I would like to dedicate this thesis to all the late-night study sessions, the countless cups of coffee, and the moments of self-doubt turned into resilience. To every setback that taught me perseverance and every success that fueled my ambition. This thesis is a tribute to growth, learning, and the endless possibilities that lie ahead.

"I dedicate this thesis to **My Parents**, who have been my pillars of strength, my guiding lights, and the source of my unwavering determination. Their love, sacrifices, and endless support have been the foundation upon which I have built my dreams. This achievement is a reflection of their boundless love and belief in me.

“I dedicate this thesis to my sister **Asma** and my dear brothers **Ali** and **Joud**, who have been my companions in laughter, partners in mischief, and my constant source of inspiration. Their presence in my life has filled my days with joy, my challenges with courage, and my achievements with shared pride. This dedication is a testament to the bond we share and the strength we draw from each other.”

“To my dearest friend **Samah**, your unwavering support and encouragement have been a guiding light throughout my academic journey. This thesis is dedicated to you, with heartfelt thanks for being my rock and source of inspiration. Your friendship means the world to me.”

their unconditional support has been the driving force behind my accomplishments. This dedication is a tribute to the bond we share and the strength they have instilled in me".

"To my dear colleague **khaoula** in this thesis, your collaboration and dedication have made this journey memorable. This thesis is dedicated to you, with sincere appreciation for our teamwork and shared efforts. Thank you for being an exceptional colleague."

Amani souilah.

Contents

Introduction

Finite groups are algebraic objects fundamental to the study of symmetry, and therefore widely applicable to most branches of mathematics concerned with finite objects. Their structures have been studied extensively for the last 200 years, and yet mathematicians are still unable to describe them all; at least not in the way that any natural number may be described as a string of digits, or any finite set a collection of elements. However, in 2004, mathematicians completed the classification of finite simple groups, a major step towards the classification of all finite groups. The Classification Project was a combined effort by nearly a hundred mathematicians over the course of 60 years. Its proof consists of hundreds of articles and thousands of pages, and is considered one of the greatest mathematical achievements of the twentieth century.

The classification of the finite simple group represents one of the milestones in the history of mathematics. Involving the combined efforts of several hundred mathematicians from all around the world, the full proof took thirty years to complete and encampasses some 10,000 journal pages.

This Thesis makes finite simple group theory accessible to a wider audience of professional mathematicians and scientists. It presents an overall picture of the fundamental division of the classification proof into four phases, the grouptheoretic origins, and definitions of each of the known simple groups-including the twenty six sporadic groups- and provides a detailed description of the basic methods that have been developed for studing simple groups.

I Fundamental concepts of group

In mathematics, a group is a fundamental concept. It consists of a set of elements with one operations, addition or multiplication, characterized by specific properties like closure, identity, inverses, and associativity. Groups are used in various branches of mathematics and other sciences to study relationships and structures among elements.

The ultimate goal of group theory is to classify all groups up to isomorphism; that is, given a particular group, we should be able to match it up with a known group via an isomorphism. It is probably not reasonable to expect that we will ever know all groups; however, we can often classify certain types of groups or distinguish between groups in special cases.

In this chapter we will start by giving Fundamental concepts of group then subgroups, then we will touch fondamental theorems of finite groups, then direct products, finlly we will touch simple groups and groups action on sets.

I.1 Group

1.1 Binary operation

Definition I.1.1

A binary operation on a set is a rule for combining two elements of the set. More precisely, if S is nonemty set, a binary operation on S is a function $\alpha : S \times S \to S$.

Thus α associates with each ordered pair (x, y) of elements of S an elemant $\alpha(x, y)$ of S. It is better notation to write $x \circ y$ for $\alpha(x, y)$ refering to "$\circ$ "as the binary operation.

1.2 Semigroup

Definition I.1.2

If $\circ$ *is associative, that is, if* $(x \circ y) \circ z = x \circ (y \circ z)$ *is valid for all* x, y, z *in S,the pair* $(S, \circ)$ *is called a semi group.*

1.3 Group

Definition I.1.3

A group G is said to be 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 $|G|$.

1.4 Group order

Definition I.1.4

The order of a group is defined to be the cardinality of the underlying set G. This is written $|G|$.

1.5 Power of an element

Definition I.1.5

Let x be an element of a multiplicatively written group G and let n be an integer. The nth power x^n of x is defined recursively in the following manner:

(i) $x^0 = 1_G$, $x^1 = x$, *and* x^{-1} *is the inverse of* x,

(ii) $x^{n+1} = x^n x$ *if* $n > 0$,

(iii) $x^n = (x^{-n})^{-1}$ *if* $n < 0$.

Naturally, if G is written additively, we shall write nx instead of x^n and speak of a multipe of x.

1.6 Isomorphism

Definition I.1.6

If G and H are groups, a function $\alpha : G \to H$ is called an isomorphism if it is a bijection (or one-one correspondence) and if $\alpha(xy) = \alpha(x)\alpha(y)$. The symbolism $G \simeq H$ signifes that there is at least one isomorphism from G to H.

Remark

- If $\alpha : G \to H$ is an isomorphism, an application of α to $1_G 1_G = 1_G$ shows that $\alpha(1_G) = 1_H$, and to $xx^{-1} = 1_G$ that $\alpha(x^{-1}) = (\alpha(x))^{-1}$.
- It is easy to prove that isomorphism is an equivalence relation on groups.
- One can see from the definition that isomorphic groups has exactly corresponding underlying sets and groups operations. Thus any property of a group deducible from its cardinality and group operation will be possessed by all groups isomorphic to it. For this reason one is not usually interested in distinguishing between a group and groups that are isomorphic to it.

1.7 Examples of groups

1.7.1 Group of Permutations

If X is a nonempty set, a bijection $\pi : X \to X$ is called a permutations of X. The set of all permutations of X is a group with respect to functional composition called the symmetric group on X, and we write $SymX$.
When $X = \{1, 2, ..., n\}$, it is customary to write S_n for $SymX$, and to call this the symmetric group of degree n.

The signature of a permutation $\pi \in S_n$ is defined to be

$$sign\pi = \prod_{1 \le i < j \le n} \frac{\pi(i) - \pi(j)}{i - j}$$

which equal $+1$ or -1. Recall that π is even if $sign\pi = +1$ and odd if sign $\pi = -1$. From the definition it is easy to check the formulas

$$sign(\pi_1\pi_2) = (sign\pi_1)(sign\pi_2) \text{ and } sign(\pi^{-1}) = sign\pi.$$

Hence the set of all even permutations in S_n is also a group with respect to functional composition; this is alternating group A_n. Obviously $|A_1| = 1$; if $n > 1$, the function $\pi \mapsto \pi(1,2)$ is a bijection from A_n to set of all odd permutations in S_n; hence $|A_n| = \frac{1}{2}(n!)$.

1.7.2 Dihedral group

Definition I.1.7

A dihedral group is a group of symmetries of a regular polygon with n sides, where n is a positive integer. The dihedral group of order $2n$, denoted by D_n, is the group of all possible rotations and reflections of the regular polygon. The group consists of elements, which can be depicted as follows:

- *n rotations, denoted by $R_0, R_{360/n}, R_{(360)(2)/n}, ..., R_{(n-1)360/n}$, represents a rotation of $(360i/n)$ degrees clockwise about the center of the polygon.*
- *n reflections, denoted by $F_0, F_1, F_2, \ldots, F_{(n-1)}$, where F_i represents a reflection across a line passing through the center of the polygon and one of its vertices.*

The group operation in D_n, is the composition of symmetries.
Alternatively, the Dihedral group D_n is defined by $D_n = \langle r, s \mid s^2 = e, r^n = e, srs = r^{-1} \rangle$ and, $|D| = 2n$. All rigid motions on n-gon:

a. *To replace first vertex we have n choices.*

b. *The second vertex can be replaced by kth vertex by $k+1$ or $k-1$.*

For $n \geq 3$, the dihedral group D_n is defined as the rigid motions taking a regular $n-gon$ back to itself, with the operation being composition. These polygons for $n = 3, 4, 5$, and 6 are in Figure 1. The dotted lines are lines of reflection: reflecting the polygon across each line brings the polygon back to itself, so these reflections are in D_3, D_4, D_5, and D_6.

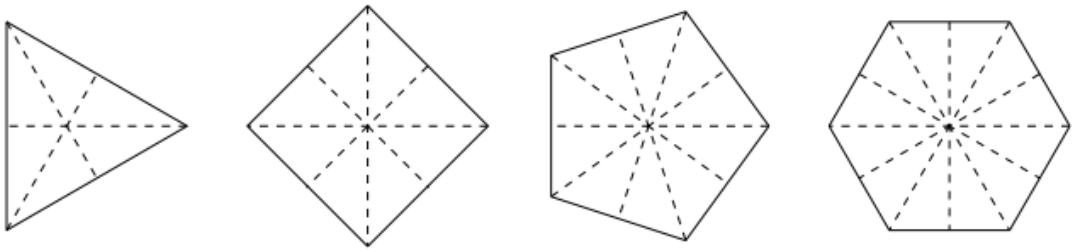


Figure I.1

Theorem I.1.1

Dihedral groups are non-abelian, for integers $n \geq 3$.

Proof I.1.1

Let $a, b \in D_3$.

We will show that $ab \neq ba$, $\forall a, b \in D_n, n \geq 3$.

$D_3 = \{e, (AB), (AC), (BC), (ABC), (ACB)\}$.

Since D_3 is isomorphic to S_3, D_3 is non-abelian.

Since $D_3 \leq D_n, \forall n \geq 3$,$D_n$ is non-abelian for $n \geq 3$.
□

Theorem I.1.2

Let the group $D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle$.

1. *Then $r^k s = sr^{-k}$.*
2. *The order of r^k is: $\dfrac{n}{gcd(k, n)}$.*

Proof I.1.2

1. *Consider $r^k s = er^k s = s^2 r^k s = ssr^k s = sr^{-k}$.*
2. *We will first show that r^k is a generator of D_n if and only if $n \mid k$.*

   Consider $e = r^k$.

   Then by the division algorithm, $k = an + b$ where $0 \leq b \leq n$.

   Thus $e = r^k = r^{na+b} = r^{na} r^b = er^b = r^b$.

   Since the smallest possible integer, m, such that $r^m = e$ is $n, b = 0$.

   Conversely, if $n \mid k$, then $k = ns, s \in Z$.

   Thus $r^k = r^{ns} = (r^n)s = e^s = e$.

   Thus $r^k = e$ iff $n \mid k$.

Let $b = r^k, \in D_4$ since r is a generator of D_n.

We shall show that the smallest integer, m s.t. $r^k = e$ is $\frac{n}{k}$.

Let $d = gcd(n, k)$.

Consider $e = b^m = r^{km}$.

Since this is the smallest integer m such that $n \mid km$. Thus $\frac{n}{d} \mid m(\frac{k}{d})$.

Since d is the greatest common divisor of n and k, $\frac{n}{d}$ and $\frac{k}{d}$ are relatively prime.

Hence $\frac{n}{d} \mid m(\frac{k}{d})$ means that $\frac{n}{d} \mid m$. The smallest such m is $\frac{n}{d}$.

Thus $|r^k| = \frac{n}{gcd(k,n)}$.

□

I.2 Subgroups

Definition I.2.1

Let G be a group and let H be a subset of G. We say that H is a subgroup of G If $(H, *)$ is a group where $*$ is a operation of G restricted to H, we shall write

$$H \leq G \text{ or } G \geq H$$

to signify that H is a subgoup of G.

Theorem I.2.1 *(The Subgroup Criterion)*

Let H be a subset of a group G. Then H is a subgroup of G if and only if H is not empty and $xy^{-1} \in H$ whenever $x \in H$ and $y \in H$.

Proof I.2.1

Necessity being clear, assume that the conditions hold: then there exists an $y \in H$ and $1_G = yy^{-1} \in H$. If $x, y \in H$, then $1_G y^{-1} = y^{-1} \in H$ and hence $x(y^{-1})^{-1} = xy \in H$. Thus H is a subgroup. □

I.2.1 The Subgroup Generated by a Subset

Definition I.2.2

Let X be a nonempty subset of a group G. Define the subgroup generated by X

$$\langle X \rangle$$

to be the intersection of all subgroups of G which contain X, notice that there will always be at least one such subgroup, G itself. That $\langle X \rangle$ is a subgroup . In a real sense $\langle X \rangle$ is the smallest subgroup of G containing X.

Remark I.2.1

Let X be a nonempty subset of a group G and let S a subgroup of G. Then

- *if $X \subseteq S \leq G$, then $\langle X \rangle \subseteq S$,*
- *if X is a subgroup, then $\langle X \rangle = X$.*

Naturally one whishes to have a description of the elements of $\langle X \rangle$.

Definition I.2.3

If n is a positive integer, a group is said to be an n-generator group if it can be generated by a set $\{x_1, x_2, ..., x_n\}$. *A group is finitely generated if it is n-generator for some n.*

I.2.2 Cyclic Group

Definition I.2.4

A cyclic group G is a group can be generated by a single elemant a, so that every element in G has the form a^i *for some integer i. We denote the cyclic group of order n by* $\mathbb{Z}_n$, *since the additive group of* $\mathbb{Z}_n$ *is a cyclic group of order n.*

Theorem I.2.2

Let G be a group and $a \in G$. *If a has infinite order, then*

(i) $a^k = e$ *if and only if* $k = 0$;

(ii) the elements$a^k (k \in Z)$ *are all distinc.*

If a has finite order $m > 0$,*then*

(iii) m is the least positive integer such that $a^m = e$;

(iv) $a^k = e$ *if and only if* $m \nmid k$;

(v) $a^r = a^s$ *if and only if* $r \equiv s(\ mod\ m)$;

(vi) $\langle a \rangle$ *consists of the distict elements* $a, a^2, ..., a^{m-1}, a^m = e$;

(vii) for each k such that $k \mid m$, $|a^k| = m \mid k$.

I.2.3 Normal Subgroup

Definition I.2.5

Let H be a subgroup of a group G, we say that H is a normal subgroup of G if it satisfy one of the following equivalent statements

- $xH = Hx$ *for all* $x \in G$.
- $x^{-1}Hx = H$ *for all* $x \in G$.
- $x^{-1}hx \in H$ *for all* $x \in G$ *and* $h \in H$.

The Notation$H \lhd G$ *sagnifies that H is a normal subgroup of G.*

Remark I.2.2

- 1_G *and G are normal subgroups of G.*
- *The group G is said to be simple if* $G \neq 1$ *and if it hasn't a normal subgroup expect* 1_G *and G.*
- *In an abelian group ,every subgroup is normal.*

Theorem I.2.3 *:*

If G is a finite group and $N \lhd G$, then $|G/N| = |G|/|N|$.

I.2.4 characteristic subgroup

Theorem I.2.4

Let G be a group, and let H be a subgroup of G. We say that H is a characteristic subgroup of G, if for every $\sigma \in Aut(G)$*:*

$$\sigma(H) = H.$$

We shall write $H \sqsubset G$ *to signify that H is a characteristic subgroup in G.*

Theorem I.2.5

- *In any group G, the identity element and G are characteristics subgroups.*
- *In a group* G, $H \sqsubset G \Rightarrow H \lhd G$.

Proof I.2.2

- $\forall \sigma \in Aut(G)$, $\sigma(e_G) = e_G$ *and* $\sigma(G) = G$.
- *Indeed, if H is invariant for every* $\sigma \in Aut(G)$*, then it is also invariant for every internal automorphism of G, which implies that* $H \lhd G$.

□

Theorem I.2.6

In any group G, $Z(G) = \{g \in G, \forall x \in G : gx = xg\}$ is characterestic subgroup.

Proof I.2.3

For all $a \in Z(G)$ and every $x \in G$, we have $xa = ax$, so $\sigma(x)\sigma(a) = \sigma(a)\sigma(x)$, $\forall \sigma \in Aut(G)$; $\forall y \in G$, there exist $x \in G$ such as $y = \sigma(x)$, we deduce that $y\sigma(a) = \sigma(a)y$, for every $y \in G$, as a result $\sigma(Z(G)) \subseteq Z(G)$.
But $\sigma \in Aut(G)$, with applying $\sigma^{-1} \in Aut(G)$ then:

$$\begin{aligned}\sigma^{-1}(Z(G)) \subseteq Z(G) &\Rightarrow \sigma(\sigma^{-1}(Z(G))) \subseteq \sigma Z(G) \\ &\Rightarrow Z(G) \subseteq \sigma(Z(G)).\end{aligned}$$

As a result $\sigma(Z(G)) = Z(G)$. □

Theorem I.2.7

Let G be a group, then:

- $(H \sqsubset G \text{ and } K \sqsubset H) \Rightarrow K \sqsubset G$.
- $(H \lhd G \text{ and } K \sqsubset H) \Rightarrow K \lhd G$.

Proof I.2.4

- *suppose that $H \sqsubset G$ and $K \sqsubset H$ and let $\sigma \in Aut(G)$.*
  We have $\sigma(H) = H$, so the restriction $\sigma_{/H}$ of σ on H is an automorphism of H, as a result $\sigma_H(K) = K = \sigma(K)$, hence $K \sqsubset G$.
- *Let $H \lhd G$ and $K \sqsubset H$. For all $\sigma \in Int(G)$: $\sigma_{/H} \in Aut(H)$, so $\sigma_{/H}(K) = K$, then $xKx^{-1} = K$, for every x in G, Hence $K \lhd G$.*

□

Definition I.2.6

Let G be a group and let $x, y \in G$, then:

$$x^g = g^{-1}xg$$

This element is called the conjugate of x by y.

I.2.5 Product of subgroups

If X and Y are arbitrary non empty subset of a group, define their product to be the subset

$$XY = \{xy | x \in X, y \in Y\}$$

and we define the inverse of X to be the subset

$$X^{-1} = \{x^{-1} | x \in X\}.$$

Theorem I.2.8

If H and K are subgroups of a group G, HK is a subgroup if and only if H and K permute .i.e $HK = KH$. In this event $HK = \langle H, K\rangle = KH$.

Proof I.2.5

Suppose that $HK \leq G$: then $H \leq HK$ and $K \leq HK$, so $KH \subseteq HK$. Taking inverses of each side we get $HK \subseteq KH$, whence HK=KH. Moreover $\langle H, K\rangle \leq HK$ since $HK \leq G$, while $HK \subseteq \langle H, K\rangle$ is always true; thus $\langle H, K\rangle = HK$. Conversly let $HK = KH$: if $h_i \in H$ and $k_i \in K$, then

$$h_1k_1(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1} :$$

now $(k_1k_2^{-1})h_2^{-1} = h_3k_3$ where $h_3 \in H$ and $k_3 \in K$. Hence $h_1k_1(h_2k_2)^{-1} = (h_1h_3)k_3 \in HK$ and $HK \leq G$. □

I.3 Fundamental theorems of finite groups

I.3.1 Lagrange's theorem

Theorem I.3.1

Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G : H]$ is the numbre of distinct left cosets of H in G. In particular, the numbre of elements in H must divide the numbre of elements in G.

Proof I.3.1

The group G is partitioned into $[G : H]$ distinct left cosets. Each left coset has $|H|$ elements; therfore, $|G| = [G : H]|H|$. □

I.3.2 Cayley's Theorem

Theorem I.3.2

Every group G is isomorphic to some subgroup of $Sym(S)$, for an appropriate S.

The appropriate S we used was G it self. But there may be better choisces When G is finite, we can take the set in cayley's theorem to be finite, in which case $Sym(S)$ is S_n and its elements are permutations. In this case, cayley's Theorem is usually stated as: A finite group can be represented as a group of permutations.

This is a good place to discuss the importance of " isomorphic ". Let φ be an isomorphism of G to G'. We can view G' as a relabeling of G, using the label $\varphi(x)$ for the element x. Is this labeling consistent with the structure of G as a group ? That is, if x is labeled $\varphi(x)$, y labeled $\varphi(y)$, what is xy labeled as? Since $\varphi(x)\varphi(y) = \varphi(xy)$, we see that xy is labeled as $\varphi(x)\varphi(y)$, so this renaming of the elements is consistent with the product in G. So two groups that are isomorphic although they need not be equal in a certain sense, as described above, are equal. Often, it is desirable to be able to identify a given group as isomorphic to some concrete group that we know.

I.3.3 Cauchy's theorem

Theorem I.3.3

If G is a finite abelian group of order $|G|$ and p is a prime that divides $|G|$, then G has an element of order p.

Caushy's Theorem has many consequences. we shall present one of these, in which we determine completly the nature of certain groups of order pq, where p and q are distinct primes.

Lemma I.3.1

Let G be a group of order pq, where p, q are primes and $p > q$. If $a \in G$ is of order p and A is a subgroup of G generated by a, then $A \triangleleft G$.

Corollary I.3.1

If G, a are as in I.3.1 and if $x \in G$, then $x^{-1}ax = a^i$, where $0 < i < p$, for some i (dependig on x).

Lemma I.3.2

if $a \in G$ is of order m and $b \in G$ is of order n, where m and n are relativly prime and $ab = ba$, then $c = ab$ is of order mn.

Theorem I.3.4

Let G be a group of order pq, where p, q are primes and $p > q$, if $q \nmid p - 1$, then G must be Cyclic.

I.3.4 The Homomorphism Theorems

Definition I.3.1

Let G, G' be two groups; then the mapping $\varphi : G \to G'$, is a homomorphism if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

Let G be a group and φ a homomorphism of G into G'. If k is the kernal ofφ, then K is a normal subgroup of G , hence we can form G/K. It is fairly natural to expect that there should be a very close relationship between G and G/K.

First Homomorphism Theorem

Let φ be an homomorphism of G into G' with kernal K. Then $G' \simeq G/K$, is isomorphism to $Im(\varphi)$.

$$\psi : G/K \to G'$$

defined by $\psi(Ka) = \varphi(a)$.

Second Homomorphism theorem

Let H be a subgroup of a group G and N a normal subgroup of G. Then $HN = \{hn | h \in H, n \in N\}$is a subgroup of G, $H \cap N$ is a normal subgroup of H, and $H/(H \cap N) \simeq (HN)/N$.

finally, we go on the third Homomorphism Theoremm, which tells us a little more about the relationship between N and N' when $N' \triangleleft G'$.

Third Homomorphism Theorem

If the map $\varphi : G \to G'$ is a homorphism of G into G' with kernal K then, if $N' \triangleleft G'$ and N=$\{a \in G \mid \varphi(a) \in N'\}$, we conclude that $G/N \simeq G'/N'$. Equivalenty $G/N \simeq (G/K)/(N/K)$.

I.3.5 Sylow's Theorem and Prime Power Groups

Theorem I.3.5

Suppose that G is a group of order $p^n m$, where p is a prime and $p \nmid m$, then G has a subgroup of order p^n

Actualy, Sylow's Theorem consists of three parts. The other two are (assuming $p^n m = |G|$, where p don't divide m):

- *Any two subgroups of order p^n in G are conjugate; that is, if $|p| = |Q| = p^n$ for subgroups P, Q of G, then for some $x \in G$,$Q = x^{-1}Px$.*
- *The number of subgroups of order p^n in G is of the form $1 + kp$ and divides $|G|$.*

Since these subgroups of order p^n pop all over the place, they are called p-sylow subgroups of G. An abelian group has one p-sylow subgroup for every prime p dividing its order. This is far from true in general case.

Examples and Applicatins

Example I.3.1

Using the Sylow theorems, we can determine that A_5 has subgroups of order $2, 3, 4$ and 5. The third Sylow theorem tells us exactly how many sylow p-subgroups A_5 has.Since the number of Sylow 5-subgroups must divide 60 and also be congruent to $1(mod 5)$, there are either one or six Sylow 5-subgroups in A_5, all Sylow 5-subgroups are conjugate, if there were only a single Sylow 5-subgroup, it would be conjugate to itself; that is, it would be a normal subgroup of A_5, since A_5 has no normal subgroups, this is impossible; hence,we have determined that there are exactly six distinct Sylow 5-subgroups of A_5.
The sylow theorems allow us to prove many useful results about finite groups.By using them, we can often conclude a great deal about groups of a particular order if certain hypotheses are satified.

Example I.3.2

Every group of order 15 is cyclic, this is true because $15 = 5 \times 3$ and 5 is not equivalent with $1(mod 3)$.

Example I.3.3

Let us classify all of the group of order $99 = 3^2.11$ *up to isomorphism. First we will show that every group G of order* 99 *is abelian. By the sylow Theorem, there are* $1 + 3k$ *Sylow* $3 - subgroup$*, each of order* 9*, for some* $k = 0, 1, 2, ...$ *Also,* $1 + 3k$ *must divide* 11*, hence, there are* $1 + 11k$ *Sylow* $11 - subgroup$ *and* $1 + 11k$ *must divide* 9*. Consequently, there is only one Sylow* $11-$*subgroup K in G.*

Any group of order p^2 *is abelianfor p prime; hence, H is isomorphic either to* $Z_3 \times Z_3$ *or to* Z_9 *.Since K has order* 1*, it must be isomorphic to* Z_{11}*. Therefore, the only possible groups of order* 99 *are* $Z_3 \times Z_3 \times Z_{11}$ *or* $Z_9 \times Z_{11}$ *up to isomorphism.*

Groups Of Prime Power Order

A groups of order p^m*, where p is a prime, m is a positive integer is called a group of prime power order, or briefly a* $p-$*group.*

Example I.3.4 *All Sylow subgroups are* $p-$*groups.*

Remarks I.3.1 *(i)* $p-$*Groups have many properties that of big interest to our aim, and we will see some of them, in particularly, those we needed in the classification process.*

(ii) Subgroups of $p-$*groups are always including an invariant member, that is, a normal subgroup, the one we focused on is that of order p.*

(iii) $p-$*Groups form the " working blocks " when constructing any given (finite) group, thus knowing their structure yields the identifying of almost any kind of finite group. Although, this remark seems promising, the detailed structure of (finite)* $p-$*groups is still challenging tusk, for example the so called power structure is widely unexplored field. one can see the famous Berkovich (and Janko) volumes*

The proof of the Fundamental Theorem of Finite Abelian groups depends on seveal lemm's.

Lemma I.3.3

let G be a finite abelian group of order n, if p is a prime that divides n, then G contains an elemant of order p.

Lemma I.3.4

A finite abelian group is a p-group if and only if its order is a power of p.

Proof I.3.2

If $|G| = p^n$ *then by Lagrange's theorem, then the order of any* $g \in G$ *must divide* p^n*, and therefore must be a power of p.*

Conversly, if $|G|$ *is not a power of p, then it has some other prime divisorq, so by I.3.3 G has an element of order q and thus is not a p-group.* □

Lemma I.3.5

Let G be a finite abelian group of order $n = p_1^{\alpha_1}.....p_k^{\alpha_k}$, where $p_1, .., p_k$ are distinct primers and $\alpha_1, .., \alpha_k$ are positive integers. Then G is the internal direct product of subgroups $G_1, G_2, ..., G_k$, where G_i is the subgroup of G consisting of all elements of order p_i^r for integer r.

Lemma I.3.6

Let G be a finite obelian p-group and suppose that $g \in G$ has maximal order. Then G is isomorphic to $< g > \times H$ for some subgroup H of G.

Proof I.3.3

By lemma I.3.4, we may assume that the order of G is p^n. We shall induct on n, If $n = 1$, then G is cyclic of order p and must be generated by g, suppose now the statement of the lemma holds for all integers k with $1 < k < n$ and let g be of maximal order in G? say $|g| = p^m$. Then $a^{p^m} = e$ for all $a \in G$. Now we choose h in G such that $h \notin < g >$, where h has the smallest possible order, certainly such an h exists, otherwise, $G =< e >$ and we are done. Let $H =< h >$.

We claim that $< g > \cap H = e$. It suffices to show that $|H| = p$, since $|h^p| = |h|/p$, the order of h^p is smaller then the order of h and must be in$< g >$ by the minimality of h; that is, $h^p = g^r$ for some number r, hence:

$$(g^r)^{p^{m-1}} = (h^p)^{p^{m-1}} = h^{p^m} = e$$

and the order of g^h must be less then or equal to p^{m-1} .Therefore, g^r cannot generate $< g >$. Notice that p must occur as a factor of r, say $r = ps$, and $h^p = g^r = g^{ps}$. Define a to be $g^{-s}h$. Then a cannot be on $< g >$; otherwise ,h would also have to be in $< g >$. Also,

$$a^p = g^{-sp}h^p = g^{-r}h^p = h^{-p}h^p = e$$

We have now formed an element a with order p such that $a \notin < g >$ .Since h was chosen to have the smallest order of all of the elements that are not in $< g >$, $|H| = p$.

Now we will show that the order of gH in the factour group G/H must be the same as the order of g in G, if $|gH| < |g| = p^m$, then

$$H = (gH)^{p^{m-1}} = g^{p^{m-1}}H$$

hence, $g^{p^{m-1}}$ must be in $< g > \cap H = e$, which contradicts the fact that the order of g in p^m. Therefore, gH must have maximal order in G/H. By the correspondence theorem and our induction hypothesis,

$$G/H \cong < gH > \times K/H.$$

for some subgroup K of G containing H. We claim that $< g > \cap K = e$. Then $bH \in <$ $gH > \cap K/H = H$ and $b \in < g > \cap H = e$. It follows that $G =< g > K$ implies that $G \cong < g > \times K$. □

I.4 Direct Products

In several of the problems and examples that appeared earlier, we went through the following constructions: if G, G' are two groups, then $G = G_1 \times G_2$ is the set of all ordered pairs (a, b), where $a \in G_1$ and $b \in G_2$ and where the product was defined component-wise via $(a_1, b_2)(a_2 b_2) = (a_1 a_2)(b_1 b_2)$, the products in each component being carried out in the respective groups G_1 and G_2. we should like to formalize this procedure here.

Definition I.4.1

If $G_1, G_2, ..., G_n$ are n groups, then their (external) direct product $G_1 \times G_2 \times ..... \times G_n$. is the set of all ordered n-tuples $(a_1, a_2, ..., a_n)$ where $a_i \in G_i$, for $i = 1, 2, ..., n$, and where the product in $G_1 \times G_2 \times ... \times G_n$ is defined component-wise, that is,

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1 b_1, a_2 b_2, ..., a_n b_n)$$

That $G = G_1 \times G_2 \times ... \times G_n$ is a group is immediate, with $(e_1, e_2, ...e_n)$ as its unit element, where e_i is the unit element of G_i, and where $(a_1, a_2, ..., a_n)^{-1} = (a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$.

G is merely the cartesian product of the groups $G_1, G_2, ..., G_n$ with a product defined in G by component-wise multiplication. We call it external , since the group $G_1, G_2, ..., G_n$ are any groups, with no relation necessarily holding among them.

Consider the subsets $\overline{G}_i \subset G_1 \times G_2 \times ..... \times G_n = G$, where

$$\overline{G}_i = \{(e_1, e_2, .., e_{i-1}, a_i, e_{i+1}, ..., e_n) | a_i \in G_i\}$$

; In other words $\overline{G}_i$ consists of all n-tuples where in the ith component any element of G_i can occur and where other component is the identity element. Clearly , $\overline{G}_i$ is a group and is isomorphic to G_i by the isomorphism

$$\prod_i = \overline{G}_i \to G_i$$

defined by $\prod_i (e_1, e_2, ..., a_i, ..., e_n) = a_i$. Furthermore, not only is $\overline{G}_i$ a subgroup of G but $\overline{G}_i \triangleleft G$.

Definition I.4.2

The group G is said to be the (internal) direct product of its normal subgroups $N_1, N_2, ..., N_n$ if every $a \in G$ has a unique representation in the form $a \approx a_1 a_2 ... a_n$, where each $a_i \in N_i$ for $i = 1, 2, ..., n$.

Lemma I.4.1

If $G = G_1 \times G_2 \times .... \times G_n$ is the external direct product of $G_1, G_2, ..., G_n$ then G is the internal direct product of the normal subgroups $\overline{G}_1, \overline{G}_2, ..., \overline{G}_n$ defined above.

Lemma I.4.2

Let G be a group, M, N normal subgroups of G such that $M \cap N = (e)$. Then, given $m \in M$, $n \in N$, $mn = nm$.

Lemma I.4.3

Let G is the internal direct prouct of its normal subgroups $N_1, N_2, ..., N_n$, then, for $i \neq j$, $N_i \bigcap N_j = (e)$.

Corollary I.4.1

If G is as in lemmaI.4.2, then if $i \neq j$ and $a_i \in N_i$ and $a_j \in N_j$, we have $a_i a_j = a_j a_i$.

Theorem I.4.1

Let G a group with normal subgroups $N_1, N_2, ..., N_n$. Then the mapping

$$\psi(a_1, a_2, .., a_n) = a_1 a_2 ... a_n$$

is an isomorphism from $N_1 \times N_2 \times ... \times N_n$ (external direct product) into G if and only if G is the internal direct product of $N_1, N_2..., N_n$.

Corollary I.4.2

Let G be a group with normal subgroups N_1, N_2, then G is the internal direct product of N_1 and N_2 if and only $G = N_1 N_2$ and $N_1 \bigcap N_2 = (e)$.

I.5 Simple Groups

I.5.1 Simple Group

Definition I.5.1

A group G is simple if its only normal subgroups are the entire group G and the trivial subgroup consisting of the identity element 1 of G. In general, a subgroup X of a group G is normal if $g^{-1}xg \in G$. When this is the case, the set of (right)cosets of X in G form a group, called the factor or quotient group of G by X and denoted by X/G.

Multiplucation in G/X is given by the rule $(Xg).(Xg') = X(gg')$ for $g, g' \in G$, here, for a given $g \in G$, the coset Xg denotes the set of elements xg with x ranging over X. The mapping $\varphi : g \to Xg$ is a homomorphism of G onto G/X. Every homomorphism image of G is easily shown to arise in thhis fashion, thus a group G is simple if and only if its only homomorphic images are it self and the trivial group.

I.5.2 Some Simple Group

The Simplicity of the Alternating Groups

The first nonabelian simple groups to be discovered were the alternating groups A_n, $n \geq 5$. The simplicity of A_5 was known to Galois and is cruel in showing that the general equation of degree 5 is not solvable by radicals.

Theorem I.5.1 *(Jordan)*

The Alternating group A_n is simple if and only if $n \neq 1, 2, or 4$.
To prove this we shall need a simple fact about 3-cycles in A_n.

Theorem I.5.2

A_n is generated by 3-cycles if $n \geq 3$.

Proof I.5.1 *I.5.2*

Every even permutation is the product of an even number of $2-cycle$. Since

$$(a, b)(a, c) = (a, b, c)$$

And

$$(a, b)(c, d) = (a, b, c)(a, d, c)$$

, an even permutation is also a product of $3-cycles$: finally 3-cycles are even and thus belong to A_n. □

Proof I.5.2 *I.5.1*

In the first place A_4 is not simple since the permutations

$$(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)$$

form together with 1 *a normal subgroup. Of course A_1 and A_2 have order* 1*. On the other hand A_3 is obviously simple. It remains therfore only to show that A_n is simple if $n \geq 5$. Suppose this is false and there exists a proper nontrivial normal subgroup N.*

Assume that N contains a $3-cycle(a,b,c)$. If (a',b',c') is another $3-cycle$ and π is a permutation in S_n mapping a to a', b to b', c to c', then clerly $\pi^{-1}(a,b,c)\pi = (a',b',c') : if\, \pi$ is odd, we can replace it by the even permutation $\pi(e,f)$ where e,f differ from a',b',c' without disturbing the conjugacy relation. (Here we use the fact that $n \geq 5$). Hence $(a',b',c') \in N$ and $N = A_n$ which is generated by $3-cycle$ if $n \geq 3$.

Asuume now that N contains a permutation π whose (disjoint) cyclic decomposition involves a cycle of length at least 4*, say*

$$\pi = (a_1, a_2, a_3, a_4....)$$

Then N also contains $\pi' = (a_1)a_2, a_3)^{-1}\pi(a_1,a_2,a_3) = (a_1,a_2,a_3,a_4,...)$ so that Ncontains $\pi^{-1}\pi' = (a_1,a_2,a_4)$: notice that the order cycle decompositions involving cycles of lengths 2 *or* 3*. Moreover such elements cannot involve just one $3-cycle-$ otherwise by squaring we would obtain $3-cycle$ in N.*

Assume that N contains a permutation $\pi = (a,b,c)(a',b',c')$...(with disjoint cycles). Then N contains

$$\pi' = (a',b',c')^{-1}\pi(a',b',c') = (a,b,a')(c,c',b')...$$

and hence$\pi\pi' = (a,a',c,b,c')..$, Which is impossible. Hence each element of N is a product of an even number of disjoint 2-cycles.

If $\pi = (a,b)(a',b') \in N$, Then N contains $\pi' = (a,c,b)^{-1}\pi(a,c,b) = (a,c)(a',b')$ for all c unaffected by π. Hence N contains $\pi\pi' = (a,b,c)$. It follows that if $1 \neq \pi \in N$, then $\pi = (a_1,a_2)(a_1,b_2)(a_3,b_3)(a_4,b_4)$...The number of $2-cycles$ being at least 4. But then N will also contain

$$\pi' = (a_3,b_2)(a_2,b_1)\pi(a_2,b_1)(a_3,b_2) = (a_1,a_2)(a_3,b_1)(b_2,b_3)(a_4,b_4)...$$

And hence $\pi\pi' = (a_1,a_3,b_2)(a_2,b_3,b_1)$, our final contradiction. Using this result it is easy to find all normal subgroups of the symmetric group S_n. □

I.5.3 The Simplicity of The Projective Special Linear Groups

Let R be a commutative ring with identity. Recall that $GL(n,R)$ is the general linear group of degree n over R and $SL(n,R)$ is the special linear group, the subgroup of all A in $GL(n,R)$ such that $\det A = 1$.

The centraliser of $SL(n,R)$ in $GL(n,R)$ is the group of nonzero scalar matrices $a1_n$, $a \in R^*$.

Proof I.5.3

Clearly a scalar matrix will commute with any matrix in $GL(n,R)$. Conversly let $A = (a_{ij})$ belong to the centralizer of $SL(n,R)$ in $GL(n,F)$. Write E_{ij} for the elementary $n \times n$ matrix with 1 in the (i,j)th position and 0 elsewhere. Now $1 + E_{ij} \in SL(n,R)$ if $i \neq j$, so A and $1 + E_{ij}$ commute, where $AE_{ij} = E_{ij}A$. The (k,j)th coefficient of AE_{ij} is a_{ki} while that of $E_{ij}A$ is 0 if $k \neq i$ and is a_{jj} otherwise. Hence $a_{ki} = 0$ if $k \neq i$ and $a_{ii} = a_{jj}$, which shows that A is scalar. □

Lemma I.5.1 *The centar of GL(n,R) is the group of nonzero scalar matrices $a1_n$ .The centre of SL(n,R) is the group of scalar matrices $a1_n$ where $a1_n$=1.*

This follows at once from I.5.1 . The projective general linear group of degree n over the ring R is defined to be

$$PGL(n,R) = GL(n,R)/(GL(n,R))$$

And the projective special linear group is

$$PSL(n,R) = SL(n,R)/(SL(n,R)) = SL(n,R)/SL(n,R) \cap (GL(n,R))$$

In case $R = GF(q)$, the following notation is used :

$$GL(n,q), PGL(n,q), SL(n,q), PSL(n,q)$$

let us compute the orders of these groups .

Lemma I.5.2
(i) $|GL(n,q)| = (q^n - 1)(q^n - q)....(q^n - q^{n-1})$
(ii) $|SL(n,q)| = |GL(n,q)|/(q-1) = |PGL(n,q)|$
(iii) $|PSL(n,q)| = |GL(n,q)|/(q-1)(n,q-1)$.

Proof I.5.4

(i) In forming a matrix in $GL(n,q)$ we may choose the first row in $q^n - 1$ ways, a row of zeros not being allowed, the second row in $q^n - q$ ways, no multiple of the first row being allowed, the third row in $q^n - q^2$ ways, no linear combination of the first two rows being allowed, and so on. Multiplying these numbers together we obtain the order of $GL(n,q)$.

(ii) $A \longmapsto$ det A is an epimorphism from GL(n,q) to $|GF(q)*|$ =q-1, the formula for $|SL(n,q)|$ comes directly from the first isomorphism theorem . The order of $PSL(n,q)$ follows from I.5.1

(iii) follows from I.5.1 and the fact that the number of solutions in $GF(q)$ of $a^n = 1$ is $(n,q-1)$: keep in mind here that $GF(q)^*$ is cyclic of order $q-1$.

□ *Discussion by results. By I.5.2 the groups of PSL(2,2) and PSL(2,3) have orders 6 and 12 , there exist no simple groups of these orders and in fact it is easy to see that $PSL(2,2) \simeq S_3$ and $PSL(2,3) \simeq A_4$.*

PSL(2,4) and PSL(2,5) both have order 60 . Since any sipmle group of order 60 is isomorphic with A_5*, we have* $PSL(2,4) \simeq A_5 \simeq PSL(2,5)$ *. But PSL(2,7) has order 168, not the order of the alternating group : hence this a new simple groups .*

PSL(3,4) is a simple group of order $20,160 = 1/2.(8!)$*. However PSL(3,4) is not isomorphic with*A_8*; for it can demonstrated that PSL(3 , 4) has no elements of order 15, unlike* A_8 *which has* $(1,2,3,4,5)(6,7,8)$ *.Consequently there are two nonisomorphic simple groups of order* $20,160$.

I.5.4 Some more Simple Groups

Apart from the alternating groups and the groups of Lie type , there are twenty six apparently isolated simple groups , two of which have been constructed only very recently . These are the so-called Sporadic groups .The largest of them , the "Monster" has order

$$2^{46}.3^{20}.5^{9}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71$$

or approximately 8.08×10^{53} *. The best known of the sporadic groups are the five groups discovered by Mathieu* over a hundred years ago .*

It is now generally beleived that the alternating groups , the groups of Lie type and the twenty six sporadic groups account for all finite nonabelian simple groups .

I.6 Groups Action on Sets

Definition I.6.1

Let X be a set and G be a group. A (left) action of G on X is a map $G \times X \to X$ given by $(g, x) \mapsto gx$, where;

1. *$ex = x$ for all $x \in X$;*
2. *$(g_1 g_2)x = g_1(g_2 x)$ for all $x \in X$ and all $g, g_2 \in G$.*

Under these considerations X is called a G-set. Notice that we are not requiring X to be relate to G in any way. It is true that every group G acts on every set X by the trivial action $(g, x) \to x$; however, group actions are more interesting if the set X is somehow related to the group G.

Example I.6.1

Let $G = D_4$ be the symmetry group of a square. If $X = 1, 2, 3, 4$ is the set of vertices of the square, then we can consider D_4 to consist of the following permutation:

$$\{(1), (13), (24), (1432), (1234), (12)(34), (14)(23), (13)(24)\}.$$

The elements of D_4 act on X as functions. The permutation (13)(24) acts on vertex 1 by sending in to vertex 3, on vertex 2 by sending it to vertex 4, and so on. It is easy to see that the axioms of a group action are satisfied.

In general, if X is any set and G is a subgroup og S_X, the group of all permutations acting on X, then X is a G-set under the group action:

$$(\sigma, x) \mapsto \sigma(x)$$

for $\sigma \in G$ ans $x \in X$

Example I.6.2

Let G be the permutation group defined by

$$G = (1), (123), (132), (45), (123)(45), (132)(45)$$

and $X = 1, 2, 3, 4, 5$. then X is a G-set. the orbits are $O_1 = O_2 = O_3 = 1, 2, 3$ and $O_4 = O_5 = 4, 5$.

Now suppose that G is a group acting on a set X and let g be an element of G. The fixed point set of g in X. denoted by X_g, is the set of all $x \in X$ such that $gx = x$. We can also study the group elements g that fix a given $x \in X$. This set is more than a subset of G, it is a

subgroup. This subgroup is called the stabilizer subgroup or isotropy subgroup of x. We will denote the stabilizer subgroup of x by G_x.

II The Classification of the Finite Simple Group

Classification theory in general relates to the study of the classification of finite simple groups. It is one of the most important theories in mathematics, concerned with identifying and classifying these groups based on their fundamental properties. The classification of finite simple groups is one of the biggest challenges in mathematics, and great progress has been made in understanding this classification in recent decades.

In this chapter we will provide an introduction to classification. we will start by giving the four phases of the classification, then we touch the classification theory and the classification strategy.

Indroduction To Classification:

A common theme in mathematics is to study a partirular mathematical structure and attempt to classify all instances of it.

Can we classify all finite groups? Since we can combine any two finite groups, for instance via direct product, to create a new finite group, it is natural to begin by considering groups that are "building blocks" for all other finite groups. Similar to the factorization of integers into prime numbers, one can "break down" finite groups into smaller pieces called simple groups, which cannot be decomposed further. A group G is simple if it has no nontrivial proper normal subgroup; i.e., its only normal subgroups are the trivial group and G itself. The JordanHölder Theorem then tells us that for any finite group G, there is an ordered sequence of subgroups,

$$1 = H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_n = G$$

called a composition series, such that each H, is a maximal proper normal subgroup of H_{i+1}/H_i and all H_{i+1}/H_i, called composition factors, are simple. Moreover, any two composition series of a group G are equivalent in the sense that they have the same number of subgroups and the same composition factors, up to permutation and isomorphism.

Nonetheless, the problem of determining all ways to reassemble a set of composition factors into a finite group. is daunting, perhaps infeasible. Although it is very easy to prove that the only abelian simple groups are Z/Z_p, where p is a prime number, the problem of determining all

finite p-groups, Le, groups G all of whose composition factors are isomorphic toZ/Z_p, is of frightening complexity. For example, there are billions of groups of size 2^{10} and many of them are essentially indistinguishable.

Fortunately, in most applications of finite group theory, where the group arises as a group of permutations or symmetries or linear operators on some other structure, the problem can be reduced easily to the case where the group action is "primitive" in some sense.For the remainder of this article, I will discuss the classification of the finite simple groups. In contrast to the abelian case, the classification of nonabelian finite simple groups is quite complex and requires a fullscale classification strategy. The two smallest nonabelian.

simple groups are A_5, the alternating group on five symbols, with 60 elements, and $PSL(2,7)$, a member of one of the families of groups of Lie type (see the next section), with 168 elements. In addition to the simple groups belonging to infinite families, there are also. twenty-six socalled sporadic groups, five discovered by Mathieu in the nineteenth century, and the rest discovered between 1965 and 1975. The sporadic groups range in size from 7920 (the smallest Mathieu group) to approximately 8×10^{53} (the aptly named Monster). In the next section, we discuss our classification strategy to prove the following theorem.

II.0.1 The four phases of the classification

We see that the classification of simple groups divides into the classification of simple groups in each of the following four categories:

- *Nonconnected simple groups .*
- *connected simple groups of component type .*
- *Small simple characterestic 2 type .*
- *Simple group of characterestic 2 type of large odd 2-local rank .*

Specifically , category A refers to the determination of all simple groups having either a proper 2-generated core or sectional 2-rank at most 4 , B to the determination of all connected simple groups of component 2-rank at least 3 ; C to the determination of all thin and quasithin simple groups of characterestic 2 type and of all simple groups of type $GF(2)$; and D to the determination of all simple groups of characterestic 2 type with $e(G) \geq 3$ and not of $GF(2) - type$.

In the sequel to the present volume , we shall give a detailed outline of the principal results within each of these four phases of the classification

II.1 The Classification Theory

Theorem II.1.1

The Classification Theorems for finite Simple Groups (traditionally abbreviated CFSG, conveniently that what is important is not so much the Classification, as the Theorem) states that every finite simple group is isomorphic to one of the following:

1. *a cyclic group C_p of prime order p;*
2. *an alternating group A_n, for $n \geq 5$);*
3. *a classification group:*
   - *linear:*
     $PSL_n(q)$, $n \geq 2$, *excepte* $PSL_2(2)$ *and* $PSL_3(3)$;
   - *unitary:*
     $PSU_n(q)$, $n \geq 3$, *excepte* $PSU_3(2)$;
   - *syplectic:*
     $PSp_{2n}(q)$, $n \geq 2$, *excepte* $PSp_4(2)$;
   - *orthogonal:*
     $P\Omega_{2n+1}(q)$, $n \geq 3$, q *odd;*
     $P\Omega^+_{2n}(q)$, $n \geq 4$;
     $P\Omega^-_{2n}(q)$, $n \geq 4$.

   where q is a power p^a of a prime p;
4. *an exceptional group of Lie type:*

$$G_2(q), q \geq 3; F_4(q); E_6(q);^2 E_6(q);^3 D_4(q); E_7(q); E_8(q)$$

   where q is a prime power, or

$$^2B_2(2^{2n+1}), n \geq 1;^2 G_2(3^{2n+1}), n \geq 1;^2 F_4(2^{2n+1}), n \geq 1$$

   or the Tits group $2^F_4(2)'$;
5. *one of 26 sporadic simple groups;*
   - *the five Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$;*
   - *the seven Leech lattice groups $Co_1, Co_2, McL, HS, Suz, J_2$;*
   - *the three Fischer groups $Fi_{22}, Fi'_{23}, Fi_{24}$;*
   - *the five Monstrous groups M, B, Th, HN, He;*
   - *the six pariahs $J_1, J_3, J_4, O'N, Ly, Ru$.*

Conversely, every group in this list is simple, and the only repetitions in this list are:

$$PSL_2(4) \cong PSL_2(5) \cong A_5;$$
$$PSL_2(7) \cong PSL_3(2);$$
$$PSL_2(9) \cong A_6;$$
$$PSL_4(2) \cong A_8;$$
$$PSU_4(2) \cong PSp_4(3).$$

As far as space allows, the statement of CFSG. Thus we seek to introduce all the finite simple groups, to provide concrete constructions whenever possible, to calculate the orders of the groups, prove simplicity, and study their actions on various natural geometrical or combinatorial objects to the point where much of the subgroup structure is revealed. In so doing, we prove a substantial part (though by no means all) of the converse part of CFSG, that is, we prove the existence of many of the finite simple groups. (In the literature on CFSG the word 'construction' is generally used in this technical sense of 'existence proof", but in this book I shall often use it in the weaker sense of building, possibly without proof, an object which is in fact the group in question.) On the other hand, there is nothing at all here about the proof of the main part of CFSG, that is, the non-existence of any other finite simple groups.

II.2 The classifition Strategy

For about fifty years, the classification strategy has been schematically represented as a box subdivided into four smaller boxes:

small odd	*small even*
large odd	*large even*

Most of the finite simple groups are groups of Lie type defined over some finite field. If you are not familiar with Lie groups, you may consider the example of $PSL(n, F)$, which is the quotient of the group $SL(n, F)$ of $n \times n$ matrices of determinant 1 with entries from the finite field F by the normal subgroup of scalar matrices of determinant 1. In this context, odd and even refer to the parity of $|F|$, while small and large are measured by the size of n. When $n < 3$, the groups are definitely small, though $PSp(4, F)$ is also small. If you know Tits's description of groups of Lie type as BN pairs, then it is more accurate to say that groups of BN rank 1 or 2 are small, while most groups of BN rank at least 3 are large.

Of course, there are also simple alternating groups and sporadic groups which must be fitted into this scheme. Much more serious is the fact that we must provide definitions for terms like "a group G of small odd type" that do not presuppose that G is a group of Lie type or indeed has any known property other than simplicity. However, if p is a prime divisor of $|G|$, then Sylow guarantees the existence of many p-subgroups of G, Le., subgroups of order p^m for some $m \geq 1$. We call the centralizers and normalizers of such subgroups p-local subgroups of G. In his 1954 address, Richard Brauer made the case for attempting to characterize simple groups via their 2-local structures. A crucial validation for this strategy was provided in 1963 when Walter Feit and John G. Thompson [FT] published their proof that all nonabelian finite simple groups have even order. Now, if $G = G(F)$ is a group of Lie type defined over a field F of even order, then the 2-local subgroups of G are contained in parabolic subgroups of G. On the other hand, this is far from true in groups of Lie type when F has odd order, with a small number of interesting exeptions. This gave rise to the initial definitions of "even" and "odd": characteristic 2-type and "non" characteristic 2-type.

Definition II.2.1 *A group H is of 2-parabolic type if H contains a normal 2-subgroup Q such that the centralizer $C_H(Q)$ is just $Z(Q)$.*

Definition II.2.2 *A group G is of characteristics $2 - type$ if every $2_l ocal$ subgroup of G is of $2 - parabolic\ type$.*
A weakness of using this definition to define the line between even and odd is that, in the study of odd type, it forces the consideration of all groups G having a 2-local, no matter how small, which is not of 2-parabolic type. Abetter definition is

Definition II.2.3 *A group G is of even characteristic (or parabolic characteristic 2) if every 2-local subgroup H of odd index in G is of 2-parabolic type.*

II.2.1 Remarks on the proof of the Classification Theorem

There has been much debate about whether CFSG deserves to be called a theorem, and this debate has contributed to the philosophical arguments about what a theorem is, what a proof is, what mathematics is (or are) and how we recognise them when we see them. I believe most mathematicians are pragmatic in their daily professional lives, and do not expect to reach the Platonic ideal of a perfect proof which confers absolute certainty on a result. Certainly some mathematicians who argue most vociferously for the absolute nature of proof are amongst those whose own proofs often fall short of this ideal. Thus my own point of view is that it is ultimately meaningless to argue about whether a written (or spoken) argument 'is' or 'is not' a 'proof'. One can only really argue about the degree of certainty we derive from the argument.
The twentieth century saw announcements of solutions of many long- standing difficult problems in mathematics, including besides the CFSG, also the four-colour problem, Fermat's Last Theorem, the Poincaré conjecture, and others. It is natural, and necessary, to greet these announcements with a healthy degree of scepticism, as not all of them have stood up to the test of time. But in most cases a gradual process of expert scrutiny, tidying up and correcting minor (or major) errors leads eventually to a general acceptance that the problem in question has indeed been solved. On the other hand, it is impossible in practice to satisfy the mathematician's desire for absolute certainty. After all, we are only human and therefore fallible. We make mistakes, which sometimes lie hidden for years.
So what of the CFSG? Has it indeed been proved? Certainly the process of collating the various parts of the proof, filling in the gaps and correcting errors, has taken longer than anyone expected when the imminent completion of the proof was announced around 1980. The project by Gorenstein, Lyons and Solomon to write down the whole proof in one place is still in progress: six of a projected eleven volumes have been published so far. The so-called 'quasithin' case is not included in this series, but has been dealt with in two volumes, totalling some 1200 pages, by Aschbacher and Smith. Nor do they consider the problem of existence and uniqueness of the 26 sporadic simple groups: fortunately this is not in the slightest doubt. So by now most parts of the proof have been gone over by many people, and re-proved in different ways. Thus the likelihood of catastrophic errors is much reduced, though not completely eliminated.

III Concrete Classification

III.1 Process Description: Groups of order at most 15

Here we classified groups of order less than or equal to 15. *We proved that there is only one groupe of order prime up to isomorphism, and that all groups of order prime* (P) *are abelian groups.This covers groups of order*$2, 3, 5, 7, 11, 13$...,*Again we were able to prove that there are up to isomorphism only two groups of order* $2p$, *where* p *is prime and* $p \geq 3$, *and this is* $Z_{2p} \cong Z_2 \times Z_p$.*(where* Z *represents cyclic groups) and* D_p*(the dihedral group of the* $p-gon$*). This covers groups of order* $6, 10, 14$....*And we proved that up to isomorphism there are only two groups of order* p^2. *And these are* Z_{p^2} *and* $Z_p \times Z_p$. *This covers groups of order* $4, 9$...*Groups of order* p^3 *was also dealt with, and we proved that there are up to isomorphism five groups of order* p^3. *Which are* Z_{p^3}, $Z_{p^2} \times Z_p$,$Z_p \times Z_p \times Z_p$, D_{p^3} *and* Q_{p^3}. *This covers of groups of order* 8..*Sylow's theorem was used to classify groups of order pq, where p and q are two distinct primes. And there is only one group of such order up to isomorphism, which is* $Z_{pq} \cong Z_p \times Z_q$. *This covers groups of order* 15 ....*Sylow's theorem was also used to classify groups of order* p^2q *and there are only two Abelian groups of such order which are* Z_{p^2q} *and* $Z_p \times Z_p \times Z_q$. *This covers order 12. Finally groups of order one are the trivial groups. And all groups of order 1 are abelian because the trivial subgroup of any group is a normal subgroup of that group.*

Proposition III.1.1
Let p *and* q *be primes such that* $p > q$. *If* $q \nmid p-1$, *then every group of order* pq *is isomorphic to the cyclic group* Z_{pq}. *If* $q \mid p-1$, *then there are(up to isomorphism) exactly two distinct groups of order* pq: *the cyclic group* Z_{pq} *and a non-abelian group* K *generated by elements* c *and* d *such that:*

$$\mid c \mid = p; \mid d \mid = q; dc = c^R d$$

where $s \neq 1 \pmod p$ *and* $s^q \equiv 1 \pmod p$.

SKETCH OF PROOF
A nonabelian group K of order pq. Given G of order pq, G contains a,b with $\mid a \mid = p$, $\mid b \mid = q$ *by Cauchy's Theorem.*

Furthermore, $S = \langle a \rangle$ is normal in G (or by counting Sylow p-subgroups, as below). The coset bS has order q in the group G/S. Since $\mid G/S \mid = q$, G/S is cyclic with generator bS, $G/S = \langle bS \rangle$.
Therefore every element of G can be written in the form $b^i a^i$ and $G = \langle a, b \rangle$.
The number of Sylow q-subgroups is $kq + 1$ and divides pq. Hence it is 1 or p. If it is 1 (as it must be if $q \nmid \{p - 1\}$), then $\langle b \rangle$ is also normal in G.

Lagrange's Theorem shows that $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$. $G = \langle a \rangle \times \langle b \rangle \cong Z_p \oplus Z_p \cong Z_{pq}$. If the numbre is p, (which can only occur if $p \mid q - 1$), then $bab^{-1} = a^r$ (since $\langle a \rangle \triangleleft G$) and $r \neq 1 (mod p)$ (otherwise G would be abelian and hence have a unique Sylow q-subgroup). Since $bab^{-1} = a^r$, if follows by induction that $b^j ab^{-j} = a^{rj}$.In particular for $j = q, a = a^{rq}$,which implies $r^q \equiv 1$ (mod p).I.2.2

In order to complete the proof we must show that if $q \mid p - 1$ and G is the non-abelian group described in the preceding paragraph, then G is isomorphic to K. We shall need some results from number theory. The congruence $x^q \equiv 1$ (mod p) has exactly q distinct solutions modulo p. If r is a solution and k is the least positive integer such that $r^k \equiv 1$ (mod p), then $k \mid q$. In our case $r \neq 1$ (mod p), whence $k = q$.
It follows that $1, r, r2', ..., r^{q-1}$ are all the distinct solutions modulo p of $x^q \equiv 1$ (mod p).
Consequently, $s \equiv r^t$ (mod p) for some t ($1 \leq t \leq q - 1$). If $b_1 = b^t \in G$, then $\mid b_1 \mid = q$. Our work above (with b_1, in place of b) shows that $G = \langle a, b_1 \rangle$; that every element of G can be written ${b_1}^i a^j$; that $\mid a \mid = p$; and that $b_1 a b_1^{-1} = b^t a b^{-1} = a^{rt} = a$. Therefore, $b_1 a = a b_1$. Verify that the map $G \longrightarrow K$ given by $a \longmapsto c$ and $b_1 \longmapsto d$ is an isomorphism.

Corollary III.1.1
If p,is an odd prime,then every group of order $2p$ is isomorphic either to the cyclic group Z_{2p} or the dihedral group D_p.

PROOF. *Apply Proposition III.1.1 with $q = 2$. If G is not cyclic, the conditions on s imply $s \equiv -1$ (mod p).Hence $G = \langle c, d \rangle$, $\mid d \mid = 2$, $\mid c \mid = p$, and $dc = c^{-1}d$ by the theoremI.2.2.Therfore, $G \cong D_p$ by theorem* **??**

Proposition III.1.2
There are (up to isomorphism) exactly two distinct nonabelian groups of order 8: the quaternion group Q_8 and the dihedral Q_4.

SKETCH OF PROOF OF *III.1.2*
Verify that $D_4 \neq Q_8$. if a group G of order 8 is nonabelian, then it cannot contain an element of order 8or have every nonidentity element of order 2. Hence G contains an element a of order4. the group $\langle a \rangle$ of index 2 is normal. Choose $b \notin \langle a \rangle$. Then $b^2 \in \langle a \rangle$ since $\mid G/\langle a \rangle \mid = 2$. Show that the only possibilities are $b^2 = a^2$ or $b^2 = e$. Since $\langle a \rangle$ is normal in G, $bab^{-1} \varepsilon \langle a \rangle$;the only possibility is $bab^{-1} = a^3 = a^{-1}$.If follows that every elements of G can be written $b^i a^j$. Hence $G = \langle a, b \rangle$. In one case we have $|a| = 4$, $b^2 = a^2, ba = a^{-1}b$, and $G \cong Q_8$; in the order case, $|a| = 4, |b| = 2, ba = a^{-1}$ and $G \cong D_4$.

Proposition III.1.3
There are (up to isomorphism) exactly three distinct nonabelian groups of order 12: the dihedrel

group D_6, the alternating group A_4, and a group T generated by elements a,b such that $|a| = 6, b^2 = a^3$, and $ba = a^{-1}b$.

SKETCH OF PROOF

Verify that there is a group T of order 12 as stated and that no two of D_6, A_4, T are isomorphic. If G is a nonabelian group of order 12, let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. there is a homomorphism $f : G \longrightarrow S$, whose kernel K is contained in P, whence $K = Por\langle e\rangle$. If $K = \langle e\rangle$, f is a monomorphism and G is isomorphic to a subgroup of order 12 of S_4, which must be A_4 , which must be A. Otherwise $K = P$ and P is normal in G. In this case P is the unique Sylow 3-subgroup. Hence G contains only two elements of order 3. If c is one of these, then $[G : C_G(c)]$ = 1 or 2 since [G: Ca(c)] is the number of conjugates of c and every conjugate of c has order 3. Hence $C_G(c)$ is a group of order 12 or 6. In either case there is $d \in C_G(c)$ of order 2 by Cauchy's Theorem. Verify that $|cd| = 6$.
Let $a = cd$; then $\langle a\rangle$ is normal in G and $|G/\langle a\rangle| = 2$. Hence there is an element $b \in G$ such that $b \notin \langle a\rangle$,$b \neq e, b^2\varepsilon\langle a\rangle$,ans $bab^{-1}\varepsilon\langle a\rangle$. Since G is nonabelian and $|a| = 6, bab^{-1} = a^5 = a^{-1}$ is the only possibility; that is, $ba = a^{-1}b$. There are six possibilities for $b^2\varepsilon\langle a\rangle$. $b^2 = a^2 or b^2 = a^4$ lead to contradiction;$b^2 = a$ or $b^2 = a$ imply $|b| = 12$ and G abelian. Therefor, the only possibilities are

1. $|a| = 6; b^2 = e; ba = a^{-1}b$,*whence* $G \cong D_6$.
2. $|a| = 6; b^2 = a^3; ba = a^{-1}b$,*whence* $G \cong T$.

The table below lists(up to isomorphism) all distinct groups of small order. There are 14 distinct groups of order 16 and 51 of order 32; there is no known formula giving the number of distinct groups of order n,for every n.

order	*distinct group*
1	$\langle e\rangle$
2	Z_2
3	Z_3
4	$Z_2 \oplus Z_2, Z_4$
5	Z_5
6	Z_6, D_3
7	Z_7
8	$Z_2 \oplus Z_2 \oplus Z_2, Z_2 \oplus Z_4, Z_8, Q_5, D_4$
9	$Z_3 \oplus Z_3, Z_9$
10	Z_{10}, D_5
11	Z_{11}
12	$Z2 \oplus Z_6, Z_{12}, A_4, D_6, T$
13	Z_{13}
14	Z_{14}, D_7
15	Z_{15}

III.2 Groups Of Order 18

Question: *How many groups of order 18 are there?*

solution: *Let* $|G| = 18 = 2 \times 3^2$ *and* s_p *denote the number of Sylow p-subgroups. Then, by the Sylow Third Theorem,* $s_3|2$ *[and so* $s_3 \in \{1,2\}$ *] and* $s_3 \equiv 1$ *(mod 3). Thus* $s_3 = 1$ *and we have only one subgroup of order 9, say H.*
Since $|H| = 9$, $H \cong C_9$ *or* $H \cong C_3 \times C_3$.
Now, $s_2 \in \{1,3,9\}$ *[since* $s_2|9$*]. We split the problem in cases.*
*Case*1*: Assume that* $s_2 = 1$*. Then, if K is the [only] subgroup of order 2, we have that* $K \triangleleft G$ *[since* $s_2 = 1$*],* $H \cap K = 1$ *[since the groups have relatively prime orders], and* $|H||K| = |G|$*. So, we have that* $G \cong H \times K$*. Therefore,*

$$G = C_3 \times C_3 \times C_2 \cong C_3 \times C_6$$

[if $H \cong C_3 \times C_3$*], or*

$$G \cong C_9 C_2 \cong C_{18}$$

[if $H \cong C_9$*].*
*Case*2*: Assume that* $s_2 = 9$*. This means that there are 9 elements of order 2 [one in each Sylow 2-subgroup]. Since H already has 9 elements, this means that every element not in H has order 2.*
Let $y \in G - H$*. [Hence y has order 2.] Then* $G = H \cup Hy$ *[since* $[G : H] = 2$*. If* $h \in H$*, then hy has order 2 [since it is not in H], i.e.,*

$$\begin{aligned} (hy)^2 = 1 &\Rightarrow hyhy = 1 \\ &\Rightarrow yhy = h^1 \\ &\Rightarrow yh = h^1 \end{aligned}$$

.

1. *If* $H \cong C_9$ *and* $H = \langle x \rangle$ *, then we have that*

$$G = H \cup Hy = \{1, x, x^2, ..., x^8, y, xy, x^2, ..., x^8 y\},$$

the order of x is 9, the order of y is 2 and $yx^i = x^{-i}y$*. Thus,*

$$G \cong D_{18}.$$

[D_{18} *is the dihedral group of order 18, as we've seen in class. It is completely characterized by the properties given above.]*

2. *If* $H \cong C_3 \times C_3$*, we can write*

$$H = \{1, x_1, x_1^2, x_2, x_2^2, x_1x_2, x_1^2x_2, x_1x_2^2, x_1^2x_2^2\}$$

where x_1 and x_2 have order 3 and commute with each other. Hence,

$$G = H \cup Hy = \{1, x_1, x_1^2, x_2, x_2^2, x_1x_2, x_1^2x_2, x_1x_2^2, x_1^2x_2^2,$$
$$y, x_1y, x_1^2y, x_2y, x_2^2y, x_1x_2y, x_1^2x_2y, x_1x_2^2y, x_1^2x_2^2y\},$$

and for any $h \in H, yh = h^{-1}y$. We have not encountered this group before, but we can check that these properties indeed give us a group: the properties allows us to make a multiplication table and check all the requirements. [Note for example that, since x_1 and x_2 commute with each other, we have:

$$(x_1^i x_2^j y)^2 = x_1^i x_2^j y x_1^i x_2^j y = x_1^i x_2^j (x_1^i x_2^j)^{-1} y^2 = x_1^i x_2^j x_1^{-i} x_2^{-j} = 1.$$

So, every element not in H indeed has order 2, as we knew it should be the case. This group is in fact the semi-direct product of $C_3 \times C_3$ with C_2, but we haven't seen those.

Case3: Assume, finally, that $s_2 = 3$. We have in this case only 3 elements of order 2. The elements of H can have order 1 [the identity], 3, or 9 [if any]. Therefore, all the elements left [i.e., not of order 2 and not in H] must have order 6, since their orders has to divide $|G| = 18$, and cannot be equal to 1 [because $1 \in H$], 2 [because we're excluding those], 3 [these must be in H], 9 [these, if exist, must also be in H], or 18 [since if we have an element of order 18, G would be cyclic, and hence all subgroups would be normal, and we would have to have $s_2 = 1$, not 3]. Hence, we have 9 elements [of order 1, 3 or 9] in H, 3 elements of order 2, and 6 elements of order 6. Let y be an element of order 2. So, $y \in G - H$, and as before,$G = H \cup Hy$.

1. *If $H = C_9$, let x be a generator. Let's find what are the other two elements of order 2 [besides y]. If x^iy [which is how every element not in H can be represented] has order 2, then, as before,*

$$(x^iy)^2 = 1 \Rightarrow x^iyx^iy = 1$$
$$\Rightarrow yx^iy = x^{-i}$$
$$\Rightarrow yx^i = x^{-i}y.$$

But then,

$$yx^{ki} = yx^ix^{(k-1)i} = x^{-i}yx^{(k-1)i}$$
$$= x^{-i}yx^ix^{(k-2)i} = x^{-2i}yx^{(k-2)i}$$

$$\vdots$$

$$= x^{-(k-1)i}yx^i = x^{-ki}y,$$

and thus

$$(x^{ki}y)^2 = x^{ki}yx^{ki}y = x^{ki}x^{-ki}yy = 1.$$

Hence, if x^iy has order 2, so does $x^{2i}y$, $x^{3i}y$, etc. Since we have only 3 elements of order 2, they have to be $\{y, x^3y, x^6y\}$.

We can conclude that xy has order 6 [since it's not in H and doesn't have order 2]. But then, $(xy)^2$ has order 3. But the only elements of order 3 [which must be in H] are x^3 and x^6, and so,

$$(xy)^3 = (xy)^2xy = x^3xy = x^4y$$

or

$$(xy)^3 = (xy)^2xy = x^6xy = x^7y.$$

But $(xy)^3$ must have order 2 [since xy has order 6], so $(xy)^3 \in \{y, x^3y, x^6y\}$, giving us a contradiction, which means that if $s_2 = 3$, then $H \cong C_9$.

2. *So, assume that $H = C_3C_3$. Then, there is some element of H_y besides y that also has order 2. [Remember that y has order 2.] Let $x \in H - \{1\}$ be an element such that xy has order 2. Again, this means that $yx = x^{\{} - 1\}y$, and we can easily check that x^2y also has order 2. [Note that since $x \in H - \{1\}$ it must have order 3.] So, the subset*

$$S = \{1, x, x^2, y, xy, xy^2\}$$

satisfy: x has order 3, y has order 2, and $yx = x^2y$. So, S is in fact a subgroup and is isomorphic to S_3.

We will now prove that $S \triangleleft G$: let $g \in G$and $a \in S$. [We need to show that $gag^{-1} \in S$.] If a has order 2 [i.e., $a \in \{y, xy, x^2y\}$], then $gag^{\{} - 1\}$ also has order 2. But since S contain all 3 elements of order 2, we must have that $gag^{-1} \in S$. If a does not have order 2, then $a \in H \cap S$[more precisely $a \in \{1, x, x2\}$]. But since $G = H \cap yH$, we can write $g = y^ih$, where $i \in \{0, 1\}$and $h \in H$. But then, $gag^{-1} = y^ihah^{-1}y^i$ [since $y^i = y^{-1}$]. Since $h, a \in H$and H is commutative, we have that $hah^{-1} = a$. Thus, $gag^{-1} = y^iay^i$. Since $a, y \in S$, we have that $gag^{-1} = y^iay^i \in S$. Therefore, $S \triangleleft G$.

Now, let S be the set of subgroups of order 3 in G. Then $|S| = 4$ [i.e., the 4 subgroups of order 3 of $H \cong C_3C_3$]. Then, $\langle y\rangle = \{1, y\}$ acts on S by conjugation [since conjugation does not change the order]. So, the orbits must have order 1 or 2 [since it must divide $|\langle y\rangle| = 2$]. Also, since $S \triangleleft G$, the orbit of $\{1, x, x^2\}$ has only one element [namely, itself]. So,

$$4 = |S| = 1 + \sum_{O orbit} |O|$$

So, there must be another orbit of order 1. [If not, the right hand side would be odd!] Let K be this subgroup, and so $yKy = K$.

We will now show that $K \triangleleft G$. Let $g \in G$. Then, as before, $g = y^ih$, with $i \in \{0, 1\}$ and $h \in H$. Since $K < H$ and H is Abelian, we have that $hKh^{-1} = K$. And, since $yKy = K$, we have that $gKg^{-1} = y^ihKh^{-1}y^i = y^iKy^i = K$, and hence $K \triangleleft G$.

Thus, $S, K \triangleleft G$ and $|S||K| = |G|$ [remember that $K \in S$, i.e., $|K| = 3$]. Also, $S \cap K = \{1\}$, since $K \neq \{1, x, x^2\}$ [by our choice of K]. we have that $G \cong SK$, i.e.,

$$G \cong S_3C_3.$$

Therefore, there are five groups of order 18 up to isomorphism: C_{18}, C_3C_6, D_{18}, the semi-direct product of C_3C_3 with C_2, and S_3C_3.

III.2.1 The Table Of Finite Simple Groups

This table illustrates the "main" finite simple groups distributed due to their classes of which one can extract useful properties in the contest.

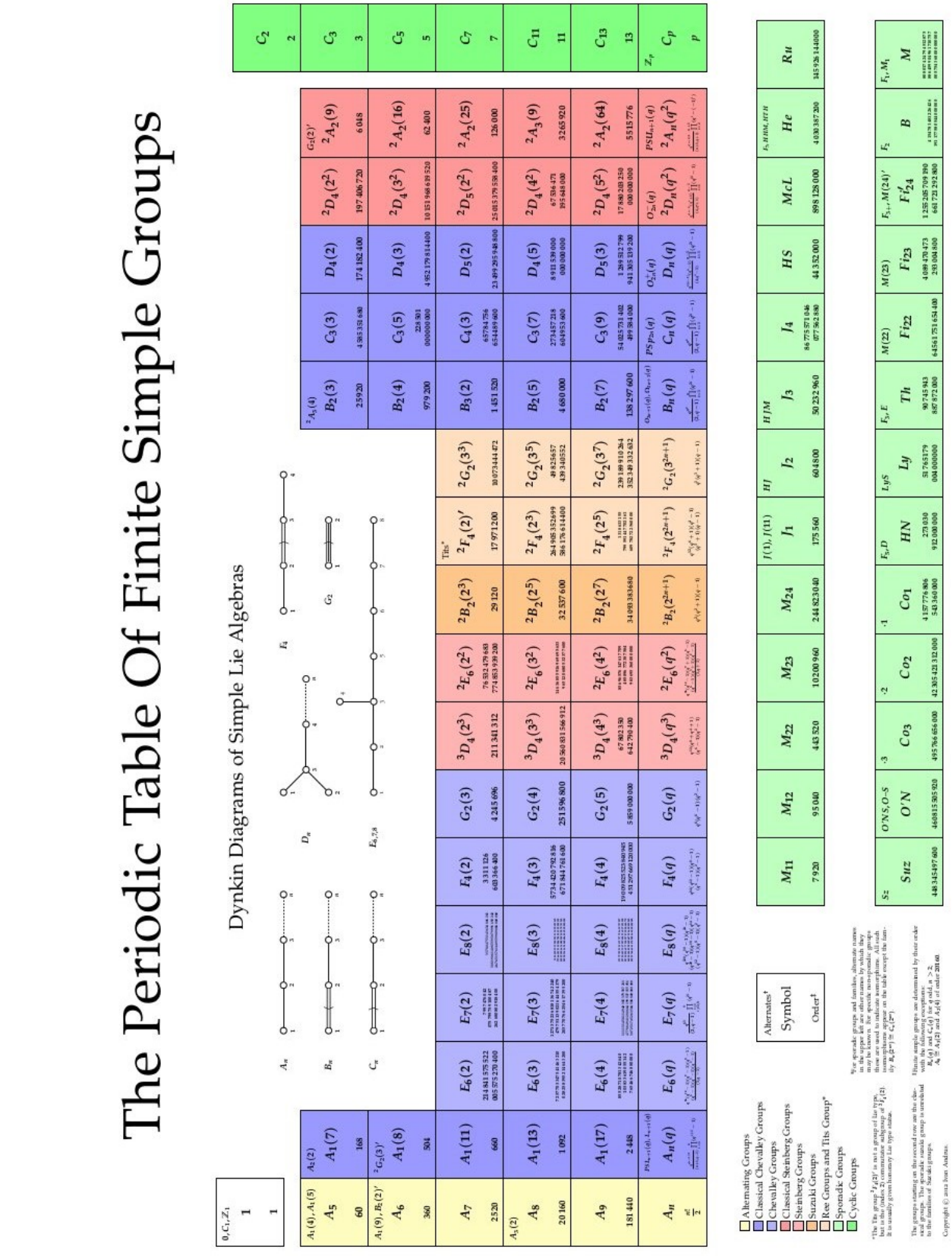

The Periodic Table Of Finite Simple Groups
Dynkin Diagrams of Simple Lie Algebras
Alternating Groups
Classical Chevalley Groups
Chevalley Groups
Classical Steinberg Groups
Steinberg Groups
Suzuki Groups
Ree Groups and Tits Group*
Sporadic Groups
Cyclic Groups
Alternates†
Symbol
Order†
Copyright © 2012 Jess Audras.

Figure III.1

III.3 Computational Approach

Definition III.3.1

The GAP (Groups, Algorithms, and Programming) system is a software package designed for computational discrete algebra. It provides a programming language and a library of algebraic algorithms for working with groups, rings, fields, and other algebraic structures. GAP allows mathematicians and researchers to perform various computations related to group theory, including group presentations, subgroup analysis, and calculations involving permutation groups. It's widely used in research, education, and industry for tasks ranging from basic group theory to advanced algebraic computations.

GAP is used extensively in this area for several purposes:

1.Verification of Results:
The classification involved a tremendous amount of intricate computations. GAP allows mathematicians to perform these computations efficiently and reliably, enabling them to verify the numerous intricate details of the classification.

2.Computational Group Theory:

GAP provides a rich set of algorithms for working with groups, which are essential for investigating the properties of finite simple groups and their subgroups.

3.Exploration and Experimentation:

Researchers can use GAP to explore the properties of finite simple groups, test conjectures, and gain insights into their structures.

4.Implementation of Algorithms:

Many algorithms developed as part of the classification process are implemented in GAP, making them readily accessible to mathematicians and researchers.

In summary, GAP serves as an indispensable tool for both theoretical exploration and computational verification in the classification of finite simple groups, playing a crucial role in advancing our understanding of these fundamental objects in mathematics

Example III.3.1 *let's create a simple GAP program to demonstrate how you can use it to classify finite groups. In this example, we'll classify all groups of order up to 10. We used the following code to view the wanted output:*

```
for n in [1..10] do
    groups := AllSmallGroups(n);;
    Print("Groups of order ", n, ":\n");
    for group in groups do
        Print(GroupToString(group), "\n");
    od;
    Print("\n");
od;
```

Figure III.2

```
for n in [1 .. 10] do
groups:= AllSmallGroups(n);;
Print("Groups of order", n,"\nLeftarrow");
for group i n groups do
Print(GroupToString(group), "\nLeftarrow");
od;
Print("\n");
od;
```

This program iterates over each integer from 1 to 10, representing the order of the groups we want to classify. For each order, it uses the ˜AllSmallGroups˝ function to compute all groups of that order. Then, it prints out the groups and their properties.

IV Conclusion

During the last few years of the classification proof, the idea spread that its completion would somehow coincide with the end of the subject of finite group theory itself. The prevalence of this view was undoubtedly fostered by the unusually wide (for mathematics) press coverage of simple groups and many of the comments (including certainly my own) by finite groups theories.

Mathematicians generally agree that a major new theorem is usually a stimulus to a field rather than a sign of its impending demise. However, because of the unprecedented thirty -year team effort required for the classification theorem; group theory come to be regarded as a notable exception. The explanation for this is easily found: those practitioners concentrating on the classification theorem - and this included a substantial portion of simple group theories - were so fixated on this single objective ,their energies so bound up with it , that they were incapable of seeing beyond the classification itself or considering any other aspect of the subject . There was even a fear that all the marvelous techniques developed in the process of dissecting and analyzing simple groups were about to become obsolete. This feeling was intense enough to push a number of group theorists into other areas of mathematics altogether.

However, the first "post-classification" conference-two-day special session of finite simple groups at the annual meeting of the American Mathematical Society in early 1981- quickly dispelled this gloomy prediction. Indeed, group theory is "alive and well": although the focus has shifted, its vitality continues unimpaired. By the time of the meeting, "revisionism " had begun in earnest: new, simplified approaches were presented to both the analysis of none connected groups and so-called "standard form" problems. Likewise, the geometry of the sporadic groups had been further explored since the classification. In addition, important new paper ties of the known simple groups were described (whose proofs depended upon the full classification theorem); and there also several striking results in the new field of "amalgams", a rich blend of graph and local theory having significance for both finite and infinite groups.

Besides these, there are other major areas of finite group theory not even touched on within the special of the known simple groups, representation of simple group theory in general, determination of the maximal subgroups of the known simple groups, the theory of solvable groups, . . . , etc. each of which abounded with deep unsolved problems.

Thus, the obituary for finite group theory has been totally premature. Nevertheless, the complesion of the classification was accompanied by a sense of loss as well as exhilaration, for there was a clear realization that the "team" would now begin to disperse. Group theory is simply

too broad a field to sustain the degree of cohesiveness inspired by the pursuit of the finite simple groups.

IV.0 Bibliography

[1] *Berkovich, Y.G., & Janko, Z. (2008). Groups of Prime Power Order Volume 1.*

[2] *Berkovich, Y., & Janko, Z. (2008). Groups of Prime Power Order. Volume 2 (Vol. 47). Walter de Gruyter.*

[3] *Conrad, K. E. I. T. H. (2009). Dihedral groups ii. Internet Online Book, 3-6.*

[4] *Judson, T. W. (2020). Abstract algebra: theory and applications.*

[5] *Herstein, I. N. (1996). Abstract algebra. John Wiley & Sons.*

[6] *Hungerford, T. W. (2012). Algebra (Vol. 73). Springer Science & Business Media.*

[7] *Gorenstein, D. (2013). Finite simple groups: an introduction to their classification. Springer Science & Business Media.*

[8] *Robinson, D. J. (2012). A Course in the Theory of Groups (Vol. 80). Springer Science & Business Media.*

[9] *Wilson, R. (2009). The finite simple groups (Vol. 251). London: Springer.*