MTS 311 - Groups and Rings

Olusola J. Adeniran
Department of Mathematics
College of Natural Sciences

1 Recommended Texts

1. Elementary Abstract and Linear Algebra by Ilori & Akinyele, University of Ibadan Press
2. Abstract Algebra by Aderemi Kuku, University of Ibadan Press
3. A first course in Abstract Algebra by J.B. Fraleigh
4. A course in Algebra by E.B. Vinberg, American Mathematical Society, 2001

2 Group Theory

1. Groups
2. Examples of groups
3. Some elementary properties of groups
4. Subgroups
5. Cyclic groups
6. Cosets and Langrange's theorem
7. Normal subgroups and Quotient groups
8. Homomorphisms
9. The Isomorphism Theorems
10. Group Actions, orbits and stabilizers
11. Conjugacy
12. Class equation of a finite group
13. Cauchy's Theorem
14. The structure of p-groups
15. The Sylow's theorems
16. Some applications of Sylow's theorems
17. Simple groups
18. Solvable groups

2.1 Groups

A binary operation $\star$ on a set G associates to elements x and y of G a third element $x \star y$ of G. For example addition and multiplication are binary operations of the set of all integers.

Definition 2.1 *A group G consists of a set G together with a binary operation $\star$ for which the following properties are satisfied:*

- $(x \star y) \star z = x \star (y \star z)$ *for all $x, y \& z$ of G (the associative law)*
- *there exist an element e of G (known as the identity element of G) such that $e \star x = x = x \star e$, for all element x of G.*
- *for each element x of G there exists an element x' (known as the inverse of x) such that $x^{\star}x = e = x' \star x$ (where e is the identity element of G).*

2.1.1 Examples of Groups

1. The set of integers, rational numbers, real numbers and complex numbers are Abelian groups together with the binary operation of addition.
2. The set of non-zero rational numbers, non-zero real numbers and non-zero complex numbers are are also Abelian groups with the binary operation of multiplication
3. For each positive integer m $\boldsymbol{Z}_m$ of congruency classes of integers modulo m is a group, where the group operation is addition of congruence classes.
4. For each positive integer n the set of all singular $n \times n$ matrices is a group where the group operation is matrix multiplication. These groups are not Abelian for $n \geq 2$.

2.2 Some elementary properties of groups

In the following the some properties of a group G using multiplicative notation and denoting the identity element e are given.

Lemma 2.1 *A group G has exactly one identity element e such that $xe = ex = e$ for all $x \in G$*

Proof
Suppose that f is an element of G with the property that $fx = x$ foe all elements x of G. Then in particular $f = fe = e$. Similarly one can show that e is the only element of G satisfying $xe = x$ for all element x of G.■

Lemma 2.2 *Every element x of G has exactly one inverse x^{-1}*

Proof
From the axioms of a group, G contains at least one element x^{-1} which satisfies $xx^{-1} = e$ and $x^{-1}x = e$. If z is any element of G which satisfies $xz = e$ then $z = ez = (x^{-1}x)z = x^{-1}(xz) = x^{-1}e = x^{-1}$. Similarly if w is any element of G which satisfies $wx = e$ then $w = x^{-1}$. In particular we conclude that the inverse x^{-1} of x is uniquely determined. This ends the proof. ■

Lemma 2.3 *Let x and y be elements of a group G. Then $(xy)^{-1} = y^{-1}x^{-1}$*

From the axioms of a group $(xy)(y^{-1}x^{-1}) = x(y(y^{-1}x^{-1})) = x((yy^{-1})x^{-1}) = x(ex^{-1}) = xx^{-1} = e$. Similarly $(y^{-1}x^{-1})(xy) = e$, and thus $y^{-1}x^{-1}$ is the inverse of xx^{-1} as required. ■

NOTE In particular that $(x^{-1})^{-1} = x$ for all elements x of a group G, since x has the properties that characterize the inverse of the inverse x^{-1} of x.

Give an element x of a group G, we define x^n for each positive integer n by the requirement that $x^1 = x$. Also, we define $x^0 = e$ where e is the identity element of the group, and we define x^{-n} to be the inverse of x^n for all positive integers n.

Theorem 2.1 *Let x be an element of a group G. then $x^{m+n} = x^m + x^n$ and $x^{mn} = (x^m)^n$ for all integers m and n*

Proof
The identity $x^{m+n} = x^m + x^n$ clearly holds when $m = 0$ and when $n = 0$. The identity $x^{m+n} = x^m + x^n$ can be shown for all positive integers m and n by induction on n. The identity when both m and n are negative then follows from the identity $x^{-m-n} = x^{-m}x^{-n}$ on taking inverses. The result when m and n have opposite signs can easily deduced from that where m and n both have the same sign.
The identity $x^{mn} = (x^m)^n$ follows immediately from the definitions when $n = 0, 1$ or -1. The result when n is positive can be proved by induction on n. The result when n is negative can then be obtained on taking inverses.■

2.3 Subgroups

Definition 2.2 *Let G be a group and let H be a subset of G. We say that H is a subgroup G if the following conditions are satisfied:*

- *the identity element of G is an element of H;*
- *the product of any two elements of H is itself an element of H; the inverse of any element of H is itself an element of H.*

A subgroup H of G is said to be proper if $H \neq G$

Lemma 2.4 *Let x be an element of a group G. Then the set of all elements of G that are of the form x^n for some integer n is a subgroup of G.*

Proof
Let $H = \{x^n : n \in \boldsymbol{Z}\}$. The identity element belongs to H, since it is equal to x^0. The product of two elements of H is itself an element of H since $x^m x^n = x^{m+n}$ for all integers m and n. Also the inverse of an element of H is itself an element of H since $(x^n)^{-1} = x^{-n}$ for all integers n. Thus H is a subgroup of G as required.■

Definition 2.3 *Let x be an element of a group G. The order of x is the smallest positive integer n for which $x^n = e$. The subgroup generated by x is the subgroup consisting of all elements of G that are of the form x^n for some integer n*

Lemma 2.5 *Let H and K be subgroups of G. Then $H \cap K$ is also a subgroup of G.*

Proof
The identity element of G belong to $H \cap K$ since it belong to the two subgroups H and K. If x and y are elements of $H \cap K$ then xy is an element of H, and xy is an element of K, and therefore xy is an element of $H \cap K$. Also the inverse x^{-1} of an element x of $H \cap K$ belongs to H and to K and thus belong to $H \cap K$.■

NOTE that generally the intersection of any collection of subgroups of a given group is itself a subgroup of that group.

2.4 Cyclic Groups

Definition 2.4 *A group G is said to be cyclic with generator x, if every element of G is of the form x^n for some integer n.*

2.4.1 Examples of Cyclic groups

1. The group $\boldsymbol{Z}$ of integers under addition is a cyclic group generated by 1.
2. Let n be a positive integer. The set $\boldsymbol{Z}_n$ of congruence classes of integers modulo n is a cyclic group of order n withe respect to the operation of addition.
3. The group of all rotations of the plane about the origin through an integer multiple of $2\pi/n$ radians is a cyclic group of order n. This group is generated by an anticlockwise rotation through an angle of $2\pi/n$ radian.

2.5 Cosets and Lagranges Theorem

Definition 2.5 *Let H be a subgroup of a group G. A left coset of H in G is a subset of G that is of the form xH, where $x \in G$ and*

$$xH = \{y \in G : y = xh \textit{ for some } h \in H\}$$

Similarly, a right coset of H in G is a subset of G that is of the form Hx, where $x \in G$ and

$$Hx = \{y \in G : y = hx \textit{ for some } h \in H\}.$$

NOTE that a subgroup H of a group G is itself a left coset of H in G.

Lemma 2.6 *Let H be a subgroup of a group G. Then the left coset of H in G have the following properties:*

1. *$x \in xH$ for all $x \in B$*
2. *If x and y are elements of G, and if $y = xa$ for some $a \in H$, then $xH = yH$*
3. *If x and y are elements of G, and if $xH \cap yH$ is non-empty then $xH = yH$.*

Proof
Let $x \in G$. Then $x = xe$, where e is the identity element of G. But $e \in H$. It follows that $x \in xH$ hence *1* is proved.

Let x and y be elements of G where $y = xa$ for some $a \in H$. Then $yh = x(ah)$ and $xh = y(a^{-1}h)$ for all $h \in H$. Moreover, $ah \in H$ and $a^{-1} \in H$ for all $h \in H$, since H is a subgroup of G. It follows that $yH \subset xH$ and $xH \subset yH$ and *2* is proved.

Finally, suppose that $xH \cap yH$ is non-empty for some elements x and y of G. Let z be an element of $xH \cap yH$. Then $z = xa$ for some $a \in H$, and $z = yb$ for some $b \in H$. It follows from 2 that $zH = xH$ and $zH = yH$. Therefore $xH = yH$. This proves *3*.■

Lemma 2.7 *Let H be a finite subgroup of a group G. Then each left coset of H in G has the same number of elements as H.*

Proof
To be provided during Lecture■

Theorem 2.2 *(Lagrange's theorem)*
Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.

Proof
Each element of G belongs to at least one left coset of H in G and no element of can belong to two distinct left cosets of H in G (see Lemma 2.6). Therefore every element of G belongs to exactly one left coset of H. Moreover, each left coset of H contains $|H|$ elements (Lemma 2.7). Therefore,$|G| = n|H|$ where n is the number of left cosets of H in G. Hence the result follows. ■

Definition 2.6 *Let H be a subgroup of a group G. If the number of left cosets of h in G is finite then the number of such cosets is referred to as the index of H in G, denoted by $[H : G]$.*

The proof of Lagrange's Theorem shows that the index $[G : H]$ of a subgroup H of a finite group G given by $[G : H] = |G|/|H|$.

Corollary 2.1 *Let x be an element of a finite group G. Then the order of x divides the order of G.*

Proof
To be provided during Lecture■

Corollary 2.2 *Any finite group of prime order is cyclic.*

Proof
To be provided during Lecture■

2.6 Normal subgroups and quotient groups

Let A and B be subsets of a group G. The product AB of the sets A and B is defined by

$$AB = \{xy : x \in A \text{and} y \in B\}$$

We denote $\{x\}A$ and $A\{x\}$ for all $x \in G$ and subsets $A \subseteq G$. The Associative Law for multiplication of elements of G ensures that $(AB)C = A(BC)$ for all subsets A, B and C of G. We can therefore use the notation ABC to denote $(AB)C$ and $A(BC)$; and we can use analogous notation to denote the product of four or more subsets of G.

If A, B and C are subsets of a group G, and if $A \subset B$ then clearly $AC \subset BC$ and $CA \subset CB$.

Note that if H is a subgroup of the group G and if x is an elements of G then xH is the left coset of H in G that contains the element x. Similarly Hx is the right coset of H in G that contains the element x.

If H is a subgroup of G then $HH = H$. Indeed, $HH \subset H$, since the product of two elements of a subgroup H is itself an element of H. Also, $H \subset HH$ since $h = eh$ for any element $h \in H$, where e, the identity element of G belongs to H.

Definition 2.7 *A subgroup N of a group G is said to be a normal subgroup if G if $xnx^{-1} \in N$ for all $n \in N$ and $x \in G$.*

The notation '$N \lhd G$' signifies 'N is a normal subgroup of G'.

Definition 2.8 *A non-trivial group G is said to be simple if the only normal subgroups of G are the whole of G and the trivial subgroup $\{e\}$ whose only element is the identity element of e of G.*

Lemma 2.8 *Every subgroup of an Abelian group is a nornmal subgroup*

Proof
To be provided during Lecture■

EXAMPLE
Let S_3 be the group of permutations of the set $\{1, 2, 3\}$and let H be the subgroup of S_3 consisting of the identity permutation and the transposition (12). Then H is not normal in G since $(23)^{-1}(12)(23) = (23)(12)(23) = (13)$ and (13) does not belong to the subgroup H.

Proposition 2.1 *A subgroup N of a normal subgroup of G¿ Let x be an element of G. Then $xNx^{-1} = N$ for all element $x \in G$*

Proof
To be provided during Lecture■

Corollary 2.3 *A sugroup N of a group G is a normal subgroup of G if and only if $xN = Nx$ for all element x of G.*

Proof
To be provided during Lecture■

Lemma 2.9 *Let N be a normal subgroup of a group G and let x and y be elements of G. Then $(xN)(yN) = (xy)N$*

Proof
To be provided during Lecture■

Proposition 2.2 *Let G be a group, and let N be a normal subgroup of G. Then the set of all cosets of N in G is group under the operation of multiplication. The identity element of this group is N itself, and the inverse of a coset xN is the coset $x^{-1}N$ for any element $x \in G$.*

Proof
To be provided during Lecture■

Definition 2.9 *Let N be a normal subgroup of a group G. The quotient group G/N is defined to be the group of cosets of N in G under the operation of multiplication.*

Proof
To be provided during Lecture■

EXAMPLE
Consider the dihedral group D_8 of order 8, which we represent as the group of symmetries of a square in the plane with corners at the points whose Cartesian co-ordinates are $(1, 1), (-1, 1), (-1, -1)$ and $(1, -1)$. Then

$$D_8 = \{\mathbf{I}, \mathbf{R}, \mathbf{R^2}, \mathbf{R^3}, \mathbf{T_1}, \mathbf{T_2}, \mathbf{T_3}, \mathbf{T_4}\}$$

where $\mathbf{I}$ denotes the identity transformation, $\mathbf{R}$ denotes an anticlockwise rotation about the origin through a right angle, and $\mathbf{T_1}, \mathbf{T_2}, \mathbf{T_3}$ and T_4 denote the reflections in the lines $y = 0, x = y, x = 0$ and $x = -y$ respectively. let $N = \{\mathbf{I}, \mathbf{R^2}\}$. Then N is a subgroup of D_8. The left cosets of N in D_8 are N, A, B and C, where $A = \{\mathbf{R}, \mathbf{R^3}\}$, $B = \{\mathbf{T_1}, \mathbf{T_3}\}$, $C = \{\mathbf{T_2}, \mathbf{T_4}\}$. Moreover, N, A, B and C are also the right cosets of N in D_8. On multiplying the cosets A, B and C with one another we find that $AB = BA = C$, $CA = AC = B$ and $BC = CB = A$. The quotient group D_8/N consists of the set $\{N, A, B, C\}$ with the group operation just described.

2.7 Homomorphisms

Definition 2.10 *A homomorphism $\theta : G \longrightarrow K$ from a group G to a group K is a function with property that $\theta(g_1 \star g_2) = \theta(g_1) \star \theta(g_2)$ for all $g_1, g_2 \in G$, where $\star$ denotes the group operation on G and on K*

EXAMPLE
Let q be an integer. The function from the group $\boldsymbol{Z}$ of integers to itself that sends integer n to qn is a homomorphism.

EXAMPLE
Let x be an element of a‘group G. The function that sends each integer n to the identity element x^n is a homomorphism from the group $\boldsymbol{Z}$ of integers to G, since $x^{m+n} = x^m x^n$ for all integers m and n.

Lemma 2.10 *Let $\theta : G \longrightarrow K$ be a homomorphism. Then $\theta(e_G) = e_K$, where e_G and e_K denote the identity elements of the groups G and K. Also $\theta(x^{-1}) = \theta(x)^{-1}$ for all elements x of G.*

Proof
To be provided during Lecture■

Definition 2.11 *An isomorphism $\theta : G \longrightarrow K$ between group G and K is a homomorphism that is also a bijective mapping G onto K. Two groups G and K are said to be isomorphic if there exists an isomorphism mapping G onto K.*

EXAMPLE

Let D_6 be the group of symmetries of an equilateral triangle in the plane with vertices X, Y and Z and let S_3 be the group of permutations of the set $\{X, Y, Z\}$. The function which sends a symmetry of the triangle to the corresponding permutation of its vertices is an isomorphism between the dihedral group D_6 of order 6 and the symmetric group S_3

EXAMPLE

Let $\mathbf{R}$ be the group of real numbers with the operation of addition and let $\mathbf{R}^+$ be the group of strictly positive real numbers with the operation of multiplication. The function $exp : \mathbf{R} \longrightarrow \mathbf{R}^+$ that sends each real number x to the positive real number e^x is an isomorphism: it is both homomorphism of groups and a bijection. The inverse of this isomorphism is the function $log : \mathbf{R}^+ \longrightarrow \mathbf{R}$ that sends each strictly positive real number to its natural logarithm

Definition 2.12 *The following are some terminologies regarding homomorphism:*

- *A monomorphism is an injective homomorphism.*
- *An epimorphism is a surjective homomorphism.*
- *An endomorphism is a homomorphism mapping a group into itself.*
- *An automorphism is an isomorphism mapping a group onto itself.*

Definition 2.13 *The kernel $Ker\theta$ of the homomorphism $\theta : G \longrightarrow K$ is the set of all elements of G that are mapped by θ onto the identity element of K.*

EXAMPLE

Let the group operation on the set $\{+1, -1\}$ be multiplication, and let $\theta : \boldsymbol{Z} \longrightarrow \{+1, -1\}$ be the homomorphism that sends each integer n to $(-1)^n$. Then the kernel of the homomorphism θ is the subgroup of $\boldsymbol{Z}$ consisting of all even numbers.

Lemma 2.11 *Let G and K be groups, and let $\theta : G \longrightarrow K$ be a homomorphism from G to K. Then the kernel $ker\theta$ of θ is a normal subgroup of G.*

Proof

To be provided during Lecture■

NOTE

If N is a normal subgroup of some group G then N is the kernel of the quotient homomorphism $\theta : G \longrightarrow G/N$ that sends $g \in G$ to the coset gN. It follows therefore that a subset of a group G is a normal subgroup of G if and only it it is the kernel of some homomorphism.

Proposition 2.3 *Let G and K be groups, let $\theta : G \longrightarrow K$ be a homomorphism from G to K, and let N be a normal subgroup of G. Suppose that $N \subset ker\theta$. Then the homomorphism $\theta : G \longrightarrow K$ induces a homomorphism $\theta : G/N \longrightarrow K$ sending $gN \in G/N$ to $\theta(g)$. Moreover $\hat{\theta} : G/N \longrightarrow K$ is injective if and only if $N = ker\theta$.*

Proof

To be provided during Lecture■

Corollary 2.4 *Let G and K be groups, and let $\theta : G \longrightarrow K$ be a homomorphism. Then $\theta(G) \cong G/ker\theta$.*

Proof
To be provided during Lecture■

2.8 The Isomorphism Theorems

Lemma 2.12 *Let G be a group, let H a subgroup of G, and let N be a normal subgroup of G. Then the set HN is a subgroup of G, where $HN = \{hn : h \in H and n \in N\}$.*

Proof
To be provided during Lecture■

Theorem 2.3 *(First Isomorphism Theorem)*
Let G be a group, and let H be a subgroup of G, and let N be a normal subgroup of G. Then

$$\frac{HN}{N} \cong \frac{H}{N \cap H}$$

Proof
To be provided during Lecture■

Theorem 2.4 *(Second Isomorphism Theorem)*
Let M and N be normal subgroups of a group G, where $M \subset N$. Then

$$\frac{G}{N} \cong \frac{G/M}{N/M}$$

Proof
To be provided during Lecture■

2.9 Group Actions, Orbits and Stabilizers

Definition 2.14 *A left action of a group G on a set X associates to each $g \in G$ and $x \in X$ an element $g \cdot x$ of X in such a way that $g \cdot (h \cdot x) = (gh) \cdot x$ and $1 \cdot x = x$ for all $g.h \in G$ and $x \in X$, and 1 denotes the identity element of G*

Given a left action of a group G on a set X, the orbit of an element x of X is the subset $\{g \cdot x : a \in G\}$ of X and the stabilizer of x is the subgroup $\{g \in G : g \cdot x = x\}$ of G

Lemma 2.13 *Let G be a finite group which acts on a set X on the left. Then the orbit of an element x of X contains $[G : H]$ elements, where $[G : H]$ is the index of stabilizer H of x in G.*

Proof
To be provided during Lecture■

2.10 Conjugacy

Definition 2.15 *Two elements h and k of a group G are said to be conjugate if $k = hhg^{-1}$ for some $g \in G$*

NOTE

- It can readily be verified that the relation of conjugacy is reflexive, symmetric and transitive and therefore an equivalence relation on a group G.

- The equivalence classes determined by this relation are referred to as the conjugacy classes of G.
- A group is a disjoint union of its conjugacy classes. The conjugacy class of the identity element contains no other element of G.
- A group G is Abelian if and only if all its conjugacy classes contain exactly one element of the group G.

Definition 2.16 *Let G be a group. The centralizer $Z(h)$ of an element h of G is the subgroup of G defined by Z(h)=$\{g \in G : gh = hg\}$.*

Lemma 2.14 *Let G be a finite group and let $h \in G$. Then the number of elements in the conjugacy class of h is equal to the index $[G : Z(h)]$ of the centralizer $Z(h)$ of h in G.*

Proof
There is a well-defined function $f : G/Z(h) \longrightarrow G$ defined on the set $G/Z(h)$ of left cosets of $Z(h)$ in G, which sends the coset $gZ(h)$ to ghg^{-1} for all $g \in G$. This function is injective and its image is the conjugacy class of h. The result follows. ■

Let H be a subgroup of a group G. One can easily verify that gHg^{-1} is also a subgroup of G for all $g \in G$, where $gHg^{-1} = \{ghg^{-1} : h \in H\}$

Definition 2.17 *Two subgroups H and k of group G are said to be conjugate if $K = gHg^{-1}$ for some $g \in G$*

The relation of conjugacy is an equivalence relation on the collection of subgroups of a given group G.

2.11 Finitely Generated Abelian groups

Let H be a subgroup of additive group $\boldsymbol{Z}^n$ consisting of all n-tuples of integers with the operation vector addition. A list $b_1, b_2, \ldots, b_r$ of elements of $\boldsymbol{Z}^n$ is said constitute an integral basis (or $\boldsymbol{Z}$-basis) of H if the following conditions are satisfied:

- the element $m_1b_1 + m_2b_2 + \ldots + m_rb_r$ belongs to H for all integers $m_1, m_2, \ldots, m_r$
- given any element $h \in H$, there exist uniquely determined integers $m_1, m_2, \ldots, m_r$ such that $h = m_1b_1 + m_2b_2 + \ldots + m_rb_r$

Note that the elements $b_1, b_2, \ldots, b_n$ of $\boldsymbol{Z}^n$ constitute an integral basis of $\boldsymbol{Z}^n$ if and only if every elements $\boldsymbol{Z}^n$ is uniquely expressible as a linear combination of $b_1, b_2, \ldots, b_n$ with integer coefficients. It follows from basic linear algebra that the rows of an $n \times n$ matrix of integers constitute an integral basis of $\boldsymbol{Z}^n$ if and only if the determinant of that matrix is ± 1.

Theorem 2.5 *Let H be a non-trivial subgroup of $\boldsymbol{Z}^n$. Then there exists an integral basis $b_1, b_2, \ldots, b_n$ of $\boldsymbol{Z}^n$, a positive integer s where $s \leq n$ and positive integers $k_1, k_2, \ldots, k_s$ for which $k_1b_1, k_2b_2, \ldots, k_sb_s$ is an integral basis of H.*

Proof:
To be provided during lecture ■
An Abelian group G is finitely generated by element $g_1, g_2, \ldots, g_n$ if and only if there every element of G is expressible in the form $g_1^{m_1}, g_2^{m_2}, \ldots, g_n^{m_n}$ for some integers $m_1, m_2, \ldots m_n$.

Lemma 2.15 *A non-trivial Abelian group G is finitely generated if and only if there exists a positive integer n and some surjective homomorphism $\theta : \boldsymbol{Z}^n \longrightarrow G$.*

Proof:

Let $e_1, e_2, \ldots, e_n$ be integral basis of $\boldsymbol{Z}^n$ with $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$. If there exists a surjective homomorphism $\theta : \boldsymbol{Z}^n \longrightarrow G$ then G is generated by $g_1, g_2, \ldots, g_n$ where $g_i = \theta(e_i)$ for $i = 1, 2, \ldots, n$. Conversely, if G is generated by $g_1, g_2, \ldots, g_n$ then there is a surjective homomorphism $\theta : \boldsymbol{Z}^n \longrightarrow G$ that sends $(m_1, m_2, \ldots, m_n) \in \boldsymbol{Z}^n$ to $g_1^{m_1}, g_2^{m_2}, \ldots, g_n^{m_n}$ ■

Theorem 2.6 *Let G be a non-trivial finitely generated Abelian group. Then there exist a positive integer n and a non-negative s between 0 and n such that if $s = 0$ then $G \cong \boldsymbol{Z}^n$ and if $s > 0$ then there exist positive integers $k_1, k_2, \ldots k_s$ such that*

$$G \cong C_{k_1} \times C_{k_2} \times \ldots \times C_{k_s} \times \boldsymbol{Z}^{n-s}$$

where C_{k_i} is a cyclic group of order K_i for $i = 1, 2, \ldots, s$.

Proof:

To be provided during lecture ■

Corollary 2.5 *Let G be a non-trivial finite Abelian group. Then there exist positive integers $k_1, k_2, \ldots, k_n$ such that $G \cong C_{k_1} \times C_{k_2} \times \ldots \times C_{k_n}$ where C_{k_i} is a cyclic group of order k_i, for $i = 1, 2, \ldots, n$.*

Remark 2.1 *With some more work it is possible to show that the positive integers $k_1, k_2, \ldots k_s$ in the last theorem may be chosen such that $K_1 > 1$ and K_{i-1} divides K_i for $i = 1, 2, \ldots, n = s$, and that the Abelian group is then determined up to isomorphism by the integer n and the sequence of positive integers $k_1, k_2, \ldots k_s$.*

2.12 The Class Equation of a Finite Group

Definition 2.18 *The center $Z(G)$ of a group G is the subgroup of G defined by*

$$Z(G) = \{g \in G : gh = hg forall h \in G\}.$$

Remark 2.2 *It can be verified that the center of a group G is a normal subgroup of G.*

Let G be a finite group., and let $Z(G)$ be the center of G. Then $G/Z(G)$ is a disjoint union of conjugacy classes contained in $G/Z(G)$, and let $n_1, n_2, \ldots, n_r$ be number of elements of these conjugacy classes. Then $n_i > 1$ for all i, since the center $Z(G$ of G is the subgroup of G consisting of those elements of G whose conjugacy class contains just one element. Now the group G is the disjoint union of its conjugacy classes, and therefore

$$|G| = |Z(G)| + n_1 + n_2 + \ldots + n_r.$$

This equation is referred to as the class equation of the group G.

Definition 2.19 *Let g be an element of a group G. The centralizer $C(g)$ of g is the subgroup of G defined by $C(g) = \{h \in G : hg = gh\}$.*

Proposition 2.4 *Let G be a finite group, and let p be a prime number. Suppose that p^k divides the order of G for some positive integer k. Then either p^k divides the order of some proper subgroup of G, or else p divides the order of the center of G.*

Proof

To be provided during lecture ■

2.13 Cauchy's Theorem

Theorem 2.7 *(Cauchy)*
Let G be a finite group and let p be a prime number that divides the order of G. Then G contians an element of order p

Proof
The result is going to be proved by induction on the order of G. Thus suppose that every finite group whose order is divisible by p and less that $|G|$ contains an element of order p. If p divides the order of some proper subgroup of G then that subgroup contains the required element of order p. If p does not divide the order of any proper subgroup of G then the last proposition ensures that p divides the order of the center $Z(G)$ of G, and thus $Z(G)$ cannot be a proper subgroup of G. But then $G = Z(G)$ of G and the group G is Abelian.

Let G be an Abelian group whose order is divisible by p, and let H be a proper subgroup of G that is not contained in any larger proper subgroup. If $|H|$ is divisible by p then the induction hypothesis ensures that H contains the required element of order p, since $|H| < |G|$. Suppose then that $|H|$ is not divisible by p. Choosing $g \in G/H$, and let C be the cyclic subgroup of G generated by g. Then $HC = G$, since $HC \neq H$ and HC is a subgroup of G containing H. It follows from the first isomorphism theorem that $G/H \cong C/H \cap C$ Now p divides $|G/H|$, since $|G/H| = |G|/|H|$ and p divides $|G|$ but not $|H|$. Therefore p divides $|C|$. Thus if $m = |C|/p$ then g^m is required element of order p. This completes the proof ■

2.14 Structure of p-Groups

Definition 2.20 *Let p be a prime number. a p-group is a finite group whose order is some power p^k of p.*

Lemma 2.16 *Let p be a prime number and let G be a p-group. Then there exists a normal subgroup of G of order p that is contained in the center of G.*

Proof
To be provided during lecture ■

Proposition 2.5 *Let G be a p-group where p is some prime number and let H be a proper subgroup of G. Then there exists some subgroup K of G such that $H \triangleright K$ and K/H is a cyclic group of order p.*

Proof
To be provided during lecture ■

Repeated applications of this proposition yield the following result.

Corollary 2.6 *Let G be a finite group whose order is a power of some prime number p. Then there exist subgroups $G_0, G_1, \ldots, G_n$ of G, where G_0 is the trivial subgroup and $G_n = G$ such that $G_{i-1} \triangleleft G_i$ and G_i/G_{i-1} is a cyclic group of order p for $i = 1, 2, \ldots, n$.*

2.15 Sylow Theorems

Definition 2.21 *Let G be a finite group and let p be a prime number dividing the order $|G|$ of G. A p-subgroup of G is a subgroup whose order is some power of p. A Sylow p-subgroup of G is a subgroup whose order is p^k where k is the largest natural number for which p^k divides $|G|$.*

Theorem 2.8 *(First Sylow Theorem)*
Let G be a finite be finite group, and let p be a prime number dividing the order of G. Then G contains a Sylow p-subgroup.

Proof
To be provided during lecture ■

Theorem 2.9 *(Second Sylow Theorem) Let G be a finite group, and let p be a prime number dividing the order of G. Then all Sylow p-subgroups of G are conjugate, and any p-subgroup of G is contained in some Sylow p-subgroup of G.*

Proof
To be provided during lecture ■

Theorem 2.10 *(Third Sylow Theorem)*
The number of Sylow p-subgroups in finite group G divides the order of G and is congruent to 1 modulo p.

Proof
To be provided during lecture ■

2.16 Some applications of the Sylow Theorems

Theorem 2.11 *Let p and q be prime numbers, where $p < q$ and q is not congruent to 1 modulo p. Then any group of order pq is cyclic.*

Proof
To be provided during lecture ■
Example
Any finite group whose order is 15, 33, 35, 51, 65, 85, 87, 91 or 95 is cyclic.

Theorem 2.12 *Let G be a group of order $2p$ where p is a prime number greater than 2. Then either the group G is cyclic or else the group G is isomorphic to the dihedral group D_{2p} of symmetries of a regular p-sided polygon in the plane.*

Proof
To be provided during lecture ■

Theorem 2.13 *Let p and q be prime numbers with $p < q$ and let d be the smallest positive integer for which $p^d \equiv 1(modq)$. If g is group of order $P^k q$ where $0 < k < d$ then G contains a normal subgroup of order q. If G is a group of order $p^d q$ then either G contains a normal subgroup of order q or else G contains a normal subgroup of order p^d.*

Proof
To be provided during lecture ■

2.17 Simple Groups

Definition 2.22 *A non-trivial group G is said to be simple if the only normal subgroups of G are the whole of G and the trivial subgroup $\{e\}$ whose only element is the identity element e of G.*

Lemma 2.17 *Any nontrivial group Abelian simple group is a cyclic group whose order is a prime number.*

Proof
To be provided during lecture ■

NOTE
Using the Sylow Theorems and related results it is possible to show that any finite simple group whose order is less than 60 is a cyclic group of prime order.

Now the prime numbers less than 60 are the following: 2,3,5,7,11,13,17,23,29,31,37,41,43,47,53 and 59. All groups of these orders are simple groups and are cyclic groups.

If p is a prime number greater than 2 then any group of order $2p$ is either a cyclic group or else is isomorphic to the dihedral group D_{2p} of order $2p$ (the last theorem). In either case such a group contains a normal subgroup of order p and therefore not a simple group. In particular, there are no simple groups of order 6, 14, 22, 26, 34, 38, 46 or 58.

If G is group of order p^k for some prime number p ans for some integer k satisfying $k \leq 2$, then G contains a normal subgroup of order p. It follows therefore that such a group is not simple. In particular, there are no simple groups of order 4, 8, 16, 32, 9,27, 25 and 49.

Let G be a group of order pq where p and q are prime numbers and p, q. Any Sylow q-subgroup of G is of order q, and the number of such Sylow q-subgroups must divide pq and be congruent to 1 modulo q. Now, p cannot be congruent to 1 modulo q since $1 < p < q$. Therefore, G has just one Sylow q-subgroup and this is a normal subgroup of G of order q. It follows that such a goup is not a simple group.

It only remains to verify that there are no simple groups of order 12, 18, 20, 24, 28, 30, 36, 40, 42, 45, 48, 50, 52, 54, or 56.

We can deal with many of these by applying the last theorem. On applying this theorem with $p = 2$, $q = 33$ and $d = 2$, we see that there are no simple groups of orders 6 or 12. On applying the theorem with $p = 2$, $q = 5$ and $d = 4$ we observed that there are no simple groups of orders 10, 20, 40 or 80. on applying the theorem with $p = 2$, $q = 7$ and $d = 3$ we see that there are no simple groups of orders 14, 28 or 56. On applying the theorem with $p = 2$, $q = 11$ we see that there are no simple groups of orders 22, 44 etc. On applying the theorem with $p = 2$, $q = 13$ we see that there are no simple groups of orders 26, 52 etc and on applying the theorem with $p = 3$ and $q = 5$ we see that there are no simple groups of orders 15, 45 etc.

It only remain for us to verify that there are no simple groups of orders 18, 24, 30, 36, 42, 48, 50 or 54.

Using the second Sylow Theorem we see that any group of order 18 has just on Sylow-3 subgroup. This Sylow-3 subgroup is then normal group of order 9 and therefore no group of order 18 is simple. Similarly a group of order 50 has just one Sylow-5 subgroup which is then a normal subgroup of order 25 and therefore no group of order 50 is simple. Also, a group of order 54 has just exactly one Sylow-3 subgroup which is then a normal subgroup of order 27 and therefore no group of order 54 is simple.

On applying the second Sylow it is observed that the number os Sylow-7 subgroups of any subgroup of order 42 must divide 42 and be congruent to 1 modulo 7. This number must then be coprime to 7 and therefore divide 6 since $42 = 7 \times 6$. But no divisor of 6 greater 1 is coprime to 1 modulo 7. It follows that any group of order 42 has just one Sylow-7 subgroup and this subgroup is therefore a normal subgroup of order 7. Thus no group of order 42 is simple.

Lemma 2.18 *Let H and K be subgroups of a finite group G. Then*

$$|H \cap K| \geq \frac{|H||K|}{|G|}.$$

Proof
To be provided during lecture ■

Lemma 2.19 *Let G be a group of order p^2 where p is a prime number and let H be a subgroup of G of order p. Then H is a normal subgroup of G.*

Proof
To be provided during lecture ■

Lemma 2.20 *The alternating group A_5 is simple*

Proof
To be provided during lecture ■