MATH 403 Notes

Contents

1 Groups

1.1 Groups

A group $(G, *)$ is a nonempty set G that can undergo binary operations $*$

- Binary operations satisfy the following axioms
  1. Closed: if $a \in G$ and $b \in G$, then $a * b \in G$
  2. Associative: $a * (b * c) = (a * b) * c$
  3. Identity element: there exists an element $e \in G$ such that $a * e = e * a = a$
  4. Inverse element: for each a, there exists an element $x \in G$ such that $a * x = x * a = e$

1.2 Abelian Groups

An abelian group is a group $(G, *)$ in which binary operations $*$ are commutative, i.e. $a * b = b * a$

- Let R be a ring. Then $(R, +)$ is an abelian group under addition operation $+$
- Let $\mathbb{F}$ be a field and $\mathbb{F}^\times$ be the set of non-zero elements in $\mathbb{F}$. Then $(\mathbb{F}^\times, \cdot)$ is an abelian group under multiplication operation $\cdot$
- Let $\mathbb{U}_n$ be the set of units in $\mathbb{Z}_n$. Then $(\mathbb{U}_n, \cdot)$ is an abelian group under multiplication operation $\cdot$

1.3 Subgroups

A subgroup is a nonempty subset S of a group G that can undergo operations inherited from G

- A subgroup must satisfy all the axioms of a group
- The notation $H < G$ indicates that H is a subgroup of G

1.4 Subgroup Theorem

Given S is a subset of G, S is a subgroup of G if and only if it satisfies the following axioms

- Closed under binary operation: if $a \in S$ and $b \in S$, then $a * b \in S$
- Inverse element: for each $a \in S$, there exists an element $x \in S$ such that $a * x = x * a = e$

If S is a finite subset of G closed under the operation in G, then S is a subgroup of G

1.5 Cartesian Product Groups $G \times H$

Let G and H be groups under operation $*$ and $\circ$ respectively. Then $(G \times H, \bullet)$ is a group under operation $\bullet$ defined as $(g_1, h_1) \bullet (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$

- If G and H are abelian groups, then $G \times H$ is an abelian group
- If G and H are finite, then $G \times H$ is finite with $|G \times H| = |G||H|$

1.6 Unit Groups $\mathbb{U}_n$

Let $\mathbb{U}_n$ be the set of units in $\mathbb{Z}_n$. Then $(\mathbb{U}_n, \times)$ is an abelian group under multiplication operation

- If n is a prime integer, then
  - $\mathbb{U}_n$ is a cyclic group with cyclic generator a
  - $(\mathbb{U}_n, \times)$ is isomorphic to $(\mathbb{Z}_{n-1}, +)$ via the function $\phi : \mathbb{Z}_{n-1} \to \mathbb{U}_n$ defined as $\phi(k) = a^k$
- If n is a composite integer and $\mathbb{U}_n$ is cyclic group with generator a, then
  - Let $\sigma = |\mathbb{U}_n| = |a|$
  - $(\mathbb{U}_n, \times)$ is isomorphic to $(\mathbb{Z}_\sigma, +)$ via the function $\phi : \mathbb{Z}_\sigma \to \mathbb{U}_n$ defined as $\phi(k) = a^k$
- If n is a composite integer, but $\mathbb{U}_n$ is not a cyclic group
  - $(\mathbb{U}_n, \times)$ is isomorphic to $(\langle A \rangle \times \langle B \rangle, *)$ for some $A, B \in \mathbb{U}_n$ via the function $\phi : \langle A \rangle \times \langle B \rangle \to \mathbb{U}_n$ defined as $\phi(a, b) = ab$
  - The operation $*$ is defined as $(a_1, b_1) * (a_2, b_2) = (a_1 a_2,\ b_1 b_2)$
  - $\langle A \rangle$ and $\langle B \rangle$ are isomorphic to $\mathbb{Z}_k$ and $\mathbb{Z}_j$ for some integers k, j
    - $\mathbb{U}_n$ is isomorphic to $\mathbb{Z}_k \times \mathbb{Z}_j$ for some integer k, j

1.7 Center Groups $Z(G)$

The center $Z(G)$ of a group G is the set of all elements that commute with every element of G

- $Z(G) = \{a \in G \mid ag = ga \text{ for every } g \in G\}$
- $Z(G)$ is a normal subgroup of G

1.8 Group Homomorphism

Groups G and H are homomorphic if there exists a well-defined function $\lambda : G \to H$ such that

- $\lambda(a *_G b) = \lambda(a) *_H \lambda(b)$

where $*_G$ is the binary operation defined in G and $*_H$ is the binary operation defined in H

- As a consequence of the condition
  - Identity element preserving: $\lambda(e_G) = e_H$
  - Inverse element preserving: $\lambda(x_G) = x_H$

1.9 Group Isomorphism

Groups G and H are isomorphic, denoted $G \cong H$, if there exists a well-defined bijective function $\phi : G \to H$ such that

- $\phi(a *_G b) = \phi(a) *_H \phi(b)$

where $*_G$ is the binary operation defined in G and $*_H$ is the binary operation defined in H

- The operation tables of G and H match when translated via ϕ
- Isomorphic groups have the same size/cardinality
- Isomorphic rings have the same number of elements of the same order

1.10 Generating Sets

A subset X of a group $(G, *)$ is a generating set, denoted $G = \langle X \rangle$, if every element of G has form ${x_1}^{a_1} * {x_2}^{a_2} * ... * {x_r}^{a_r}$ for some $x_i \in X$ and $a_i \in \mathbb{Z}$

- Every element of a group $(G, *)$ can be expressed as a product of the elements of its generating set X
- i.e. $\mathbb{Z} = \langle 1 \rangle$
- i.e. $S_n = \langle \{(12), (23), ..., (n-1\ n)\} \rangle = \langle \{(12), (123...n)\} \rangle$

1.11 Cyclic Groups

A group G is cyclic if and only if there exists $a \in G$ such that $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} = G$

- G is a cyclic group with cyclic generator a

1.12 Cyclic Groups Theorems

- Every cyclic group is abelian
- Every subgroup of a cyclic group is cyclic
- If $\gcd(n, k) = 1$, then the product $\mathbb{Z}_n \times \mathbb{Z}_k$ is a cyclic group
- Given finite cyclic group G with $|G| = n$ and cyclic generator $\langle a \rangle$, $\left\langle a^k \right\rangle = G$ if and only if $\gcd(k, n) = 1$

1.13 Primitive Root Theorem

Let $\mathbb{F}_n$ be a finite field. Then the multiplicative group ${\mathbb{F}_n}^{\times}$ is a cyclic group of order $n - 1$

1.14 Cyclic Subgroups

Let G be a group and a be an element of G. Then the cyclic subgroup generated by a is the set $\langle a \rangle = \left\{a^k \mid k \in \mathbb{Z}\right\}$

- If $\langle a \rangle$ is an infinite set, then $\langle a \rangle$ is isomorphic to $(\mathbb{Z}, +)$
- If $\langle a \rangle$ is a finite set, then a is said to have a finite order k where $k = |\langle a \rangle|$
  - $|\langle a \rangle| = k$ where k is the smallest positive integer such that $a^k = e$

1.15 Cyclic Subgroups Theorems

Let G be an abelian group and a be an element of G. If $|a| = n$, then

- $a^k = e$ if and only if $n \mid k$
- $a^i = a^j$ if and only if $i \equiv j \bmod n$
- If $n = td$ with $d \geq 1$, then $\left|a^t\right| = d$

Given an abelian group G, let a, b be elements of G. If $|a| = s$ and $|b| = t$ such that $\gcd(s, t) = 1$, then $|ab| = st$

- If $(ab)^k = a^k b^k = e$, then $st \mid k$

Given a finite abelian group G, let N be the maximal order of elements of G. If $a \in G$, then $|a| \mid N$

1.16 Fundamental Theorem of Infinite Cyclic Groups

Let G be an infinite cyclic group with cyclic generator a. Then

- G is isomorphic to $(\mathbb{Z}, +)$
- If H is a subgroup of $\mathbb{Z}$, then $H = n\mathbb{Z}$ for some unique $n \geq 0$
- Every non-zero subgroup of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$
- If $s, t \geq 1$, then $s\mathbb{Z} \subset t\mathbb{Z}$ if and only if $t \mid s$

1.17 Fundamental Theorem of Finite Cyclic Groups

Let G be a finite cyclic group with cyclic generator a and $n = |\langle a \rangle|$. Then

- G is isomorphic to $(\mathbb{Z}_n, +)$
- If H is a subgroup of G, then $H = \left\langle a^k \right\rangle$ for some $k \mid n$. In particular, $|H|$ divides n
- If $k \mid n$, then $\left\langle a^{\frac{n}{k}} \right\rangle$ is the unique subgroup of G of order k
- There is a one-to-one correspondence between the set of subgroups of G and the set of positive divisors of n
- If s, t are both divisors of n, then $\left\langle g^{\frac{n}{s}} \right\rangle \subset \left\langle g^{\frac{n}{t}} \right\rangle$ if and only if $\frac{n}{t} \mid \frac{n}{s}$

1.18 Symmetry

A symmetry is a rigid motion in $\mathbb{R}^3$ that maps an object onto itself.

- A rigid motion is a bijective function $f : \mathbb{R}^3 \to \mathbb{R}^3$ that preserves length such that $||v - w|| = ||f(v) - f(w)||$

1.19 Rotational Symmetry

Let G_{object} denote the set of rotational symmetries of the object

- $|G_{\text{tetrahedron}}| = |G_{\text{hexagon}}| = |G_{\text{dodecagon cone}}| = 12$
- If $s \in G_{\text{object}}$ and $r \in G_{\text{object}}$, then $s \circ r \in G_{\text{object}}$
- Every rotational symmetry δ has an inverse τ such that $\delta \circ \tau$ is an idempotent transformation

1.20 Finite Symmetric Groups S_n

The finite symmetric group S_n of a set $X_n = \{1, 2, ..., n\}$ is the set of bijective functions $f : X_n \to X_n$

- A bijective function f may be expressed by an array in which the image under f of an element in the first row is listed immediately below it in the second row
  - i.e. a bijective function whose rule is $f(1) = 2,\ f(2) = 3,\ f(3) = 1$ may be represented by the array $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
- The binary operation of the group is the composition of bijective functions
  - Composition of bijective function yields a bijective function
  - Composition of bijective functions is associative
  - Every bijective function has an inverse function

1.21 Dihedral Groups D_n

The dihedral group D_n is the group of symmetries of a regular n-sided polygon, which includes rotations and reflections

- r represents a $\frac{2\pi}{n}$ rad counter-clockwise rotation and d represents a reflection in the x-axis
- $D_n = \{e, r, r^2, ..., r^{n-1}, d, rd, ..., r^{n-1}d\}$
- $|D_n| = 2n$
- $dr^k = r^{n-k}d$

1.22 Cayley's Theorem

Let $S(G)$ be the set of all bijections from G to G. Then every group G is isomorphic to a subgroup of $S(G)$

- Since $S(G) \cong S_n$ where $n = |G|$, every group G is isomorphic to a subgroup of S_n

1.23 Cycle Decomposition

Let $a_1, a_2, ..., a_k$ be distinct elements in the set $X_n = \{1, 2, ..., k\}$. Then the k-cycle $(a_1, a_2, ..., a_k)$ represents a permutation in S_n that sends $a_1 \to a_2$, $a_2 \to a_3$,...,$a_{k-1} \to a_k$, $a_k \to a_1$

- i.e. the permutation array $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 7 & 5 & 9 & 1 & 8 & 2 \end{pmatrix}$ in S_9 is represented as $(1347)(269)(5)(8)$, which can be further simplified as $(1347)(269)$
- If τ is the k-cycle $(a_1\ a_2\ ...\ a_k)$ and $\sigma \in S_n$, then $\sigma\tau\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ ...\ \sigma(a_k))$

1.24 Disjoint Cycles

A k-cycle $\sigma = (a_1, a_2, ..., a_k)$ and an ℓ-cycle $\tau = (b_1, b_2, ..., b_\ell)$ in S_n are said to be disjoint if $\{a_1, a_2, ..., a_k\} \cap \{b_1, b_2, ..., b_\ell\} = \varnothing$

- If a k-cycle σ and an ℓ-cycle τ are disjoint cycles in S_n, then $\sigma\tau = \tau\sigma$
- If a k-cycle σ and an ℓ-cycle τ are disjoint cycles in S_n, then $|\sigma\tau| = \mathrm{lcm}(k, \ell)$

1.25 Cycle Decomposition Theorems

Let σ be a permutation in S_n. Then we can express its cycle decomposition as $\sigma = \lambda_1\lambda_2...\lambda_t$ where

- Each cycle λ_i is a k_i-cycle
- Each k_i-cycle has order k_i
- σ has order $\mathrm{lcm}(k_1, k_2, ..., k_t)$
- The set $\{\lambda_1, \lambda_2, ..., \lambda_t\}$ consists of disjoint cycles
- $k_1 \geq k_2 \geq ... \geq k_t$
- $k_1 + k_2 + ... + k_t = n$ such that $\mathrm{par}(\sigma) = [k_1, k_2, ..., k_t]$ is a partition of n

1.26 Partitions

A partition of n is a sequence of positive integers $[k_1, k_2, ..., k_s]$ such that $n = k_1 + k_2 + ... + k_s$ where $k_1 \geq k_2 \geq ... \geq k_s$

- i.e. the partitions of $n = 3$ are $[3], [2, 1], [1, 1, 1]$
- There is a one-to-one correspondence between the disjoint cycle decompositions in S_n and the partitions of n

1.27 Transpositions

A transposition is a 2-cycle (ab) in S_n

- If σ is a transposition, then $\sigma = \sigma^{-1}$ and $|\sigma| = 2$
- Every permutation in S_n can be written as the product of transpositions
  - $(a_1, a_2, ..., a_k) = (a_1a_2)(a_2a_3)...(a_{k-1}a_k)$

1.28 Odd/Even Permutations

A permutation σ in S_n is odd if it can be written as the product of an odd number of transpositions, and even if it can be written as the product of an even number of transpositions

- It is possible that a permutation σ is both odd and even
- The identity permutation $e = (12)(21)$ is even but not odd
- No permutation in S_n is both even and odd
  - A k-cycle of even length in S_n is an odd permutation
  - A k-cycle of odd length in S_n is an even permutation

1.29 Alternating Groups A_n

An alternating group A_n is a subgroup of S_n consisting of the set of even permutations in S_n

- Half of the permutations in S_n are even such that $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$

1.30 Orthogonal Groups $O_n(\mathbb{R})$

Let $O_n(\mathbb{R})$ is the set of orthogonal matrices in $M_n(\mathbb{R})$. Then $(O_n(\mathbb{R}), \cdot)$ is a group under matrix multiplication

- $O(n, \mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$
- $O_n(\mathbb{R})$ is the union of $SO_n(\mathbb{R})$ and the set $\{A \mid \det(A) = -1\}$
- An $n \times n$ matrix A in $M_n(\mathbb{R})$ is orthogonal if $A^T = A^{-1}$

1.31 Examining $O_2(\mathbb{R})$

If a 2×2 matrix $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is orthogonal, then $a^2 + b^2 = 1$ and $ac + bd = 0$. If we set $a = \cos(\theta)$ and $b = \sin(\theta)$, then

- If $c = -\sin(\theta)$ and $d = \cos(\theta)$
  - $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ corresponds to a θ radian counter-clockwise rotation transformation
- If $c = \sin(\theta)$ and $d = -\cos(\theta)$
  - $\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$ corresponds to a reflection along the x-ax

This means that elements of $O_2(\mathbb{R})$ are either rotations or reflections

1.32 Special Orthogonal Groups $SO_n(\mathbb{R})$

Let $SO_n(\mathbb{R})$ be the set $\{A \in O_n(\mathbb{R}) \mid \det A = 1\}$. Then $(SO_n(\mathbb{R}), \cdot)$ is a normal subgroup of $O_n(\mathbb{R})$ under matrix multiplication

1.33 Isometry

An isometry of $\mathbb{R}^n$ is a map $f : \mathbb{R}^n \to \mathbb{R}^n$ such that $||a - b|| = ||F(a) - F(b)||$

- An isometry is a map that preserves length

1.34 Linear Maps

Given a linear map $\tau : \mathbb{R}^n \to \mathbb{R}^n$, there exists an $n \times n$ transformation matrix A_τ such that $\tau(v) = A_\tau \cdot v$

- The set of linear maps from $\mathbb{R}^n$ to $\mathbb{R}^n$ is isomorphic to the set of $n \times n$ matrices $M_n(\mathbb{R})$
- The i^{th} column of A_τ is given by $\tau(e_i)$, where $e_i = (0_1 \ldots 1_i \ldots 0_n)$

1.35 Linear Maps Theorems

The following are equivalent

- $\tau : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry fixing the origin
- $\tau : \mathbb{R}^n \to \mathbb{R}^n$ is a linear map and the corresponding matrix A_τ is in $O_n(\mathbb{R})$

2 Normal Subgroups and Quotient Groups

2.1 Group Equivalence Relations

Let H be a subgroup of G. Given $a, b \in G$

- $a \equiv_R b \bmod H$ if and only if $ab^{-1} \in H$
- $a \equiv_L b \bmod H$ if and only if $b^{-1}a \in H$

$\equiv_R$ and $\equiv_L$ are equivalence relations on G

- Reflexive: $a \equiv_* a \bmod H$
- Symmetric: $a \equiv_* b \bmod H$ if and only if $b \equiv_* a \bmod H$
- Transitive: if $a \equiv_* b \bmod H$ and $b \equiv_* c \bmod H$, then $a \equiv_* c \bmod H$

2.2 Cosets

Let H be a subgroup of G

- The right coset Hg of the element $g \in G$ is given by $\{p \mid p \equiv_R g \bmod H\} = \{hg \mid h \in H\}$
  - $a \equiv_R b \bmod H$ if and only if $Ha = Hb$
- The left coset gH of the element $g \in G$ is given by $\{p \mid p \equiv_L g \bmod H\} = \{gh \mid h \in H\}$
  - $a \equiv_L b \bmod H$ if and only if $aH = bH$

2.3 Cosets Theorems

Let H be a subgroup of G

- There exists a bijection between the right and left cosets in G, given by $\phi(Ha) = a^{-1}H$
  - There is an equal number of right and left cosets in G
- All cosets in G have the same cardinality
- If G is abelian, then the right and left cosets in G are identical

2.4 Grand Theory of Equivalence Relations

- Cosets are either equal or disjoint
- The group G is the disjoint union of $\displaystyle\bigcup_{g \in \Lambda} Hg$, where Λ is a non-unique subset of G
  - Λ is the set of right coset representatives
- The group G is the disjoint union of $\displaystyle\bigcup_{g \in \Gamma} gH$, where Γ is a non-unique subset of G
  - Γ is the set of left coset representatives

2.5 Lagrange's Theorem

If G is a finite group and H is a subgroup, then $|H| \bigm| |G|$

- The order of an element $g \in G$ must divide the order of the finite group G
- If G is a finite group of order n, then the only possible orders of the subgroups of G are the factors of n
- If G is a finite group of order p, then G is cyclic
  - Every non-identity element in G is a cyclic generator of G

2.6 Converse of Lagrange's Theorem

- If G is a finite abelian group and $k \mid |G|$, then G contains a subgroup of order k
- If G is a finite group and $p \mid |G|$ for some prime p, then G contains a subgroup of order p

2.7 Subgroup Index

Let H be a subgroup of a group G where H has a finite number of right cosets. Then the index of H is the number of right cosets, denoted $[G : H]$

- $[G : H] = \frac{|G|}{|H|}$
- H is also the number of left cosets since there exists a bijection between the right and left cosets

2.8 Normal Subgroups

A subgroup N of a group G is normal if $aN = Na$ for all $a \in G$, denoted $N \triangleleft G$

- $aN = Na$ if and only if $aNa^{-1} = N$ or $a^{-1}Na = N$
- Every subgroup of an abelian group is normal
- An abelian subgroup may not be normal
- A normal subgroup may not be abelian
- If H is a subgroup of G with index 2, then H is normal

2.9 Conjugate Subgroups

The conjugate subgroups of a group G are the sets $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ and $a^{-1}Ha = \{a^{-1}ha \mid h \in H\}$ where H is a subgroup of G and $a \in G$

- If N is a normal subgroup of G, the following are equivalent
  - $a^{-1}Na \subseteq N$ for all $a \in G$ if and only if $a^{-1}Na = N$ for all $a \in G$
  - $aNa^{-1} \subseteq N$ for all $a \in G$ if and only if $aNa^{-1} = N$ for all $a \in G$

2.10 Quotient Groups

Let N be a normal subgroup of a group G. Then the set of all right cosets of N in G, denoted G/N, is a group under operation $*$ where $(Na) *_{G/N} (Nb) = N(a *_G b)$

- If $Na = Nb$ and $Nc = Nd$ for $a, b, c, d \in G$, then $Nac = Nbd$
- If $|G|$ is finite, then $|G/N| = \frac{|G|}{|N|}$
- If G is abelian, then G/N is also abelian
- If T is a subgroup of G/N, then $T = H/N$ where H is a subgroup of G that contains N

2.11 Finite Group Classification

Let G be a finite group

- If $|G| = p$ for some prime p, then $G \cong \mathbb{Z}_p$
- If $|G| = 4$, then $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
  - $\mathbb{Z}_4$ is cyclic
  - $\mathbb{Z}_2 \times \mathbb{Z}_2$ is non-cyclic
- If $|G| = 6$, then $G \cong \mathbb{Z}_6$ or $G \cong S_3$
  - $\mathbb{Z}_6$ is abelian
  - S_3 is non-abelian
- If $|G| = p^2$ for some prime p, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$

2.12 Abelian Group Identification

- If $G/Z(G)$ is cyclic, then G is abelian
  - $Z(G) = \{a \in G \mid ag = ga,\ \forall g \in G\}$ denotes the center G
  - $Z(G)$ is a normal subgroup

2.13 Kernel

The kernel of a homomorphism $f : G \to H$ is $\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\}$

- $\mathrm{Ker}(f)$ is the set of all elements in G that maps to the identity in H
- $\mathrm{Ker}(f)$ is a normal subgroup of G

2.14 Additional Theorems

- If $f : G \to H$ is a homomorphism, f is injective if and only if $\mathrm{Ker}(f) = \{e_G\}$
- If $f : G \to H$ is a homomorphism and $K = \mathrm{Ker}(f)$, then $f(a) = f(b)$ if and only if $Ka = Kb$
- If N is a normal subgroup of G, then the map $\pi : G \to G/N$ given by $\pi(g) = Ng$ is a surjective homomorphism with $\mathrm{Ker}(\pi) = N$

2.15 First Isomorphism Theorem

Let $f : G \to H$ be a surjective homomorphism with $K = \mathrm{Ker}(f)$. Then there exists an isomorphic function $\bar{f}$ between G/K and H

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\
G/K \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

2.16 Second Isomorphism Theorem

Let K be a subgroup of G and N be a normal subgroup of G. Then

- $NK = \{nk \mid n \in N,\ k \in K\}$ is a subgroup of G
- N is a normal subgroup of NK
- K is a subgroup of NK
- $N \cap K$ is a normal subgroup of K

such that NK/N is isomorphic to $K/N \cap K$

$$\begin{tikzcd}
 & NK \arrow[dl, dash] \arrow[dr, equal] & \\
K \arrow[dr, equal] & & N \arrow[dl, dash] \\
 & N \cap K &
\end{tikzcd}$$

2.17 Third Isomorphism Theorem

Let N and K be normal subgroups of G with $N \subseteq K \subseteq G$. Then

- K/N is a normal subgroup of G/N
- ${}^{G/N}/_{K/N}$ is isomorphic to G/K

Corollaries of the Third Isomorphism Theorem

- Let N be a normal subgroup of G and let K be any subgroup of G that contains N. Then K is normal in G if and only if K/N is normal in G/N

2.18 Fourth Isomorphism Theorem

Let N be a normal subgroup of G. Then there exists a one-to-one correspondence

$$\{\text{subgroups } H \text{ of } G \text{ that contain } N\} \xleftrightarrow{\phi} \{\text{subgroups of } G/N\}$$

- Given a subgroup H in G that contains a normal subgroup N, there exists a bijective function $\phi : H \to H/N$
- The lattice structure for H and H/N are similar

2.19 Simple Groups

A group G is simple if its only normal subgroups are $\{e\}$ and G

- Simple groups have no non-trivial normal subgroups
- If p is prime, then $\mathbb{Z}_p$ is simple
- The alternating group A_n is simple for $n \neq 4$

2.20 Composition Series

Suppose G is a finite group and let $G_0 = G$

- If G_i is simple, then let G_{i+1} be the trivial group $\{e\}$. We stop here
- If G_i is non-simple, then let G_{i+1} be a normal subgroup of G_i of largest order
  - The quotient group G_{i+1}/G_i is simple

This procedure gives us the subgroup chain

$$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_{n-1} \supset G_n = \{e\}$$

where $G_{i+1} \triangleleft G_i$ and the quotient group G_{i-1}/G_i is simple

- The simple groups G_0/G_1, $G_1/G_2, ..., G_{n-1}/G_n$ are the composition factors of G
- Given a finite group G, it has a finite composition series
- The simple successive quotient groups in the composition series are unique up to ordering
  - All possible choices for G_i are isomorphic to one another

2.21 Finite Simple Abelian Groups Theorem

Every finite simple abelian group is isomorphic to $\mathbb{Z}_p$ for some prime p

- Every simple abelian group is finite

2.22 Finite Simple Non-Abelian Groups Theorem

Every finite simple non-abelian group is isomorphic to one of the following

- An alternating group A_n for some $n \geq 5$
- A simple group of Lie type
- One of the 26 sporadic simple groups

This information is beyond the scope of this class and may be ignored

3 Topics in Group Theory

3.1 Direct Products

Given groups $G_1, G_2, ..., G_k$, the direct product $G = G_1 \times G_2 \times ... \times G_k$ is a group under operation $*$ defined as $(a_1, a_2, ..., a_k) * (b_1, b_2, ..., b_k) = (a_1 b_1, a_2 b_2, ..., a_k b_k)$

- Let M and N be normal subgroups of G such that $M \cap N = \langle e \rangle$. If $a \in M$ and $b \in N$, then $ab = ba$
- Let $N_1, N_2, ..., N_k$ be normal subgroups of G such that every element in G can be written uniquely in the form $a_1 * a_2 * ... * a_k$ with $a_i \in N_i$. Then G is isomorphic to $N_1 \times N_2 \times ... \times N_k$
- Let M and N be normal subgroups of G such that $G = MN = \{mn \mid m \in M,\ n \in N\}$ and $M \cap N = \langle e \rangle$. Then $G = M \times N$

3.2 External and Internal Direct Products

- If the factors $G_1, G_2, ..., G_k$ are not subgroups G, then G is an external direct product of $G_1, G_2, ..., G_k$
- If the factors $G_1, G_2, ..., G_k$ are subgroups G, then G is an internal direct product of $G_1, G_2, ..., G_k$

3.3 p-Groups

Let G be an additive abelian group and p be a prime integer. Then G is a p-group if the order of every element in G is a prime power, that is some multiplicative power of p

- $G(p)$ is the set of all elements in G whose order is some multiplicative power of p
  - $G(p)$ is a subgroup of G
  - Any subgroup of $G(p)$ is a p-group
- A finite group G is a p-group if and only $|G| = p^k$ for some $k \in \mathbb{Z}$
- Let G be a finite abelian p-group and a be an element of maximal order in G. Then there exists a p-group $K < G$ such that $G = \langle a \rangle + K$

3.4 Direct Sums

Given additive groups $G_1, G_2, ..., G_k$, the direct sum $G = G_1 + G_2 + ... + G_k$ is a group under operation $+$ defined as $(a_1, a_2, ..., a_k) + (b_1, b_2, ..., b_k) = (a_1 + b_1, a_2 + b_2, ..., a_k + b_k)$

- Let G be an abelian group and $a \in G$ be an element of finite order. Then $a = a_1 + a_2 + ... + a_t$ with $a_i \in G(p_i)$, where $p_1, p_2, ..., p_t$ are distinct primes that divide the order of a
  - $|a| = {p_1}^{k_1} {p_2}^{k_2} ... {p_t}^{k_t}$ for some $k_1, k_2, ..., k_t \in \mathbb{Z}$
- Let G be a finite abelian group. Then $G = G(p_1) + G(p_2) + ... + G(p_t)$ where $p_1, p_2, ..., p_t$ are distinct primes that divide the order of G
  - $|G| = {p_1}^{k_1} {p_2}^{k_2} ... {p_t}^{k_t}$ for some $k_1, k_2, ...k_t \in \mathbb{Z}$
- If $\gcd(m, k) = 1$, then $\mathbb{Z}_{mk} = \mathbb{Z}_m + \mathbb{Z}_k$
- If $n = {p_1}^{k_1} {p_2}^{k_2} ... {p_t}^{k_t}$ where $p_1, p_2, ..., p_t$ are distinct primes, then $\mathbb{Z}_n = \mathbb{Z}_{{p_1}^{k_1}} + \mathbb{Z}_{{p_2}^{k_2}} + ... + \mathbb{Z}_{{p_t}^{k_t}}$

3.5 Fundamental Theorem of Finite Abelian Groups

Every finite abelian group G is a direct sum of cyclic groups, each of prime power order

- Every finite abelian group G is a direct sum of cyclic groups of orders $m_1, m_2, ..., m_t$, where $m_1 \mid m_2$, $m_2 \mid m_3$, ..., $m_{t-1} \mid m_t$

3.6 Elementary Divisors

When a group G is written as a direct sum of cyclic groups of prime power orders, the prime powers are called the elementary divisors of G

- The prime powers may not be distinct
- The elementary divisors of a group G is not unique
- i.e. If we can write a group G as $\mathbb{Z}_2 + \mathbb{Z}_2 + \mathbb{Z}_3 + \mathbb{Z}_{125}$, then the elementary divisors of G are $2, 2, 3, 5^3$

3.7 Invariant Factors

When a group G is written as a direct sum of cyclic groups of orders $m_1, m_2, ..., m_t$, where $m_1 \mid m_2$, $m_2 \mid m_3$, ..., $m_{t-1} \mid m_t$, then $m_1, m_2, ..., m_t$ are called the invariant factors of G

- The invariant factors of a group G is not unique
- i.e. If we can write a group G as $\mathbb{Z}_2 + \mathbb{Z}_{750}$, then the invariant factors of G are $2, 750$

3.8 Elementary Divisor Isomorphism Theorem

Let G and H be finite abelian groups. Then G is isomorphic to H if and only if G and H have the same set of elementary divisors

- We can use this theorem to find all possible finite abelian groups of order n
  1. Use the prime factorization of n to determine all possible elementary divisors
  2. Use the elementary divisors to generate all possible groups of order n

4 Supplementary Material

4.1 Euler Phi Function

Let the function $\phi : \mathbb{Z} \to \mathbb{Z}$ be defined as $\phi(n) = \big|\{x \mid 1 \leq x \leq n,\ \gcd(x, n) = 1\}\big|$

- If p is prime, then $\phi(p^k) = p^k - p^{k-1}$
- If $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$
- $|\mathbb{U}_n| = \phi(n)$

4.2 Factorization of $\mathbb{U}_n$

If $n = {p_1}^{k_1}{p_2}^{k_2}...{p_r}^{k_r}$ is a factorization of n into distinct prime powers, then $\mathbb{U}_n$ is isomorphic to $\mathbb{U}_{{p_1}^{k_1}} \times \mathbb{U}_{{p_2}^{k_2}} \times ... \times \mathbb{U}_{{p_r}^{k_r}}$

4.3 Lemmas for $\mathbb{U}_n$ for Even n

- If $k \geq 3$, then $3^{(2^{k-2})} \equiv 1 \bmod 2^k$
- If $k \geq 3$, then $3^{(2^{k-3})} \not\equiv 1 \bmod 2^k$
- If $k \geq 3$, then $|\langle 3 \rangle| = 2^{k-2}$ in $\mathbb{U}_{2^k}$
- If $k \geq 3$, then $\mathbb{U}_{2^k}$ contains three distinct elements of order 2
  - $\big|\big\langle 2^k - 1 \big\rangle\big| = \big|\big\langle 2^{k-1} - 1 \big\rangle\big| = \big|\big\langle 2^{k-1} + 1 \big\rangle\big| = 2$
- If $k \geq 3$, then $\mathbb{U}_{2^k}$ is not cyclic

4.4 Structure of $\mathbb{U}_n$ for Even n

- $\mathbb{U}_2$ is a cyclic group of order 1
- $\mathbb{U}_{2^2}$ is a cyclic group of order 2
- $\mathbb{U}_{2^k} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ for all $k \geq 3$

4.5 Lemmas for $\mathbb{U}_n$ for Odd n

- If $k \geq 2$ and p is an odd prime, then $(1+p)^{(p^{k-1})} \equiv 1 \bmod p^k$
- If $k \geq 2$ and p is an odd prime, then $(1+p)^{(p^{k-2})} \equiv 1 + p^{k+1} \bmod p^k$
- If $k \geq 2$ and p is an odd prime, then $(1+p)^{(p^{k-2})} \not\equiv 1 \bmod p^k$
- If $k \geq 2$ and p is an odd prime, then $|\langle 1 + p \rangle| = p^{k-1}$ in $\mathbb{U}_{p^k}$

4.6 Structure of $\mathbb{U}_n$ for Odd n

- $\mathbb{U}_p \cong \mathbb{Z}_{p-1}$ for all odd primes p
- $\mathbb{U}_{p^k} \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{k-1}}$ for all $k \geq 2$ and all odd primes p

4.7 Group Action

An action of a group G on a set X is a homomorphism $\varphi : G \to S(X)$, where $S(X)$ is the set of all bijections from X to X

- Given $g \in G$, then the function $\varphi(g) : X \to X$ is a bijection
- Given $g, h \in G$ and $x \in X$, then φ is homomorphic such that $\varphi(g *_G h)(x) = \varphi(g)(x) *_{S(X)} \varphi(h)(x)$

4.8 Group Action Equivalence Relation

Let G act on X and $x, y \in X$. Then $x \sim y$ if and only if there exists $g \in G$ such that $\varphi(g)(x) = y$

4.9 Orbit

Let G act on X and $x \in X$. Then the orbit of x under the action of G, denoted $O(x)$, is the equivalence class of x defined as

$$\begin{aligned} O(x) &= \{y \mid x \sim y\} \\ &= \{\varphi(g)(x) = y \mid g \in G\} \end{aligned}$$

- The orbits partition X
- If there is just one orbit, then the group action is said to be transitive

4.10 Stabilizer

Let G act on X and $x \in X$. The stabilizer of x, denoted $\mathrm{Stab}(x)$, is the set of all $g \in G$ such that $\varphi(g)(x) = x$

- The stabilizer of x is a subgroup of G

4.11 Orbit-Stabilizer Theorem

Let G act on X and let $x \in X$. Then $\psi : a\mathrm{Stab}(x) \to ax$ defines a bijection from $G/\mathrm{Stab}(x)$ onto $O(x)$ which satisfies

$$\psi(g(\underbrace{a\mathrm{Stab}(x)}_{\text{left coset}})) = g\psi(a\mathrm{Stab}(x))$$

for $g, a \in G$

- If G is finite, then $|O(x)| = [G : \mathrm{Stab}(x)] = \frac{|G|}{|\mathrm{Stab}(x)|}$
- If G is finite, then $|O(x)| \,\big|\, |G|$

4.12 Left Regular Action

The left regular action is a group action $\varphi : G \to S(G)$ defined as $\varphi(g)(x) = gx$

4.13 Conjugation Action

The conjugation action is a group action $\varphi : G \to S(G)$ defined as $\varphi(g)(x) = gxg^{-1}$

- In the context of conjugation action, orbits are called conjugacy classes, denoted $C(x)$, and stabilizers are called centralizers, denoted $\mathrm{Cent}(x)$
- If $|\mathrm{Cent}(x)| = 1$, then $x \in Z(G)$
- If G is a finite group, then $|G| = |Z(G)| + \sum\limits_{g \notin Z(G)} \frac{|G|}{|\mathrm{Cent}(g)|}$
- If $|G|$ is a power of a prime integer p, then $|Z(G)| > 1$