Contents

Chapter 1

Basics

1.1 Set Theory

Set is a collection of points which satisfies ZFC-axioms. And the points are the elements of A, $x \in A$.

1. **Cardinality** $|A|$ is the number[1] of elements of the set A.

2. Let $n \in \mathbb{N}$, then there exists a finite set of cardinality n given by $\mathbb{N}_n = \{1, 2, \ldots, n\}$.

3. A set B is a **subset** of a set A, $B \subset A$ if $x \in B \implies x \in A$.

4. The **power set** $\mathcal{P}(A)$ of a set A is the family of all subsets of A.

5. Two sets A, B are **equal**, $A = B$ if $A \subset B$ and $B \subset A$.

6. Set Operations

   union of two sets A, B is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

   intersection of two sets A, B is the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

   complement of a set A wrt a set B is the set $A - B = \{x \in A : x \notin B\}$.

   symmetric difference of two sets A, B is the set $A \Delta B = (A - B) \cup (B - A)$.

   cartesian **product** of A and B, $A \times B = \{(a, b) : a \in A,\ b \in B\}$.

7. A **relation** from A to B is a subset of $A \times B$. And $xRy \implies (x, y) \in R \subset A \times B$.

8. A relation on A is $R \subset A \times A$.

   reflexive relation R on A satisfies $xRx,\ \forall x \in A$.

   symmetric relation R on A satisfies $xRy \iff yRx$.

   antisymmetric relation R on A satisfies $(x, y) \in R \implies (y, x) \notin R$.

   transitive relation R on A satisfies $xRy,\ yRz \implies xRz,\ \forall x, y, z \in A$.

   total relation R on A satisfies either xRy or yRx, $\forall x, y \in A,\ (x \neq y)$.

[1] We adopt Cantor's notion of number of elements when the set is infinite.

9. **equivalence** relation R on A is a reflexive, symmetric, and trasitive relation.

   An **equivalence class** of a set A containining x is the subset $\hat{x} = \{y \in A : xRy\}$ where the relation R is an equivalence relation.

10. A **partition** $\{\hat{x}, \hat{y}, \dots\}$ of A is a family of subsets $\hat{x}$ of A which satisfies

    $x \in \hat{x},\ \forall x \in A.$

    $\hat{x} \cap \hat{y} \iff \hat{x} = \hat{y}.$

    $A = \cup\{\hat{x} : x \in A\}.$

11. A **function** from A to B is relation which has a unique element $(a, b),\ \forall a \in A$.

    A function $f : A \to B$ is an **injection** if it satisfies $f(x) = f(y) \implies x = y$.

    A function $f : A \to B$ is a **surjection** if it satisfies $y = f(x),\ \forall y \in B$.

12. A function $f : A \to B$ is a **bijection** if f is both injective and surjective. Then A, B are of the same cardinality $A \sim B$.

    If $f : A \to B$ is an injection, then $\exists C \subset B$ such that $f : A \to C$ is a bijection. Then $A \sim C \subset B \implies |A| \leq |B|$. If A is uncountable, then B is uncountable. If B is countable, then A is countable.

    If $f : A \to B$ is an surjection, then $\exists C \subset A$ such that $f : C \to B$ is a bijection. Then $B \sim C \subset A \implies |B| \leq |A|$. If A is countable, then B is countable, then A is uncountable. If B is uncountable, then A is uncountable.

13. There exists a bijection from the set of all equivalence relations on A to the set of all partitions of A.

14. A set A is **finite** if there exists a natural number n and a bijection $f : A \to \mathbb{N}_n$.

15. A set A is finite if and only if there does not exist a bijection from A into any proper subset of A. A set A is infinite if A has a proper subset B and there exists a bijection $f : A \to B$.

16. A set A is **countably infinite** if there exists a bijection $f : A \to \mathbb{N}$.

    A subset of a countably infinite set is at most countably infinite.

    If A is uncountable and B is countable, then $A - B$ is uncountable.

    Non-degenerate intervals are uncountable.

17. The finite cartesian product of countable sets are countable.
    Proof : cantor diagonalisation process and induction.

18. Countable union of countable sets is countable.
    Let $A_j = \{a_{i,j} : (i, j) \in \mathbb{N} \times \mathbb{N}\}$ and $S = \bigcup_{j \in \mathbb{N}} A_j$. Then $S \sim \mathbb{N} \times \mathbb{N} \implies |S| = \aleph_0$.

19. **Continuum Hypothesis** : Let $\aleph_0, \aleph_1, \dots$ where $2^{\aleph_k} = \aleph_{k+1}$. Then there does not exists a set A such that $\aleph_k < |A| < \aleph_{k+1}$.

    For any set A, there does not exists a bijection from A to power set of $\mathcal{P}(A)$.

20. $\aleph_0^{\aleph_0} = \aleph_1$, $\aleph_0^n = \aleph_0$, and $n\aleph_0 = \aleph_0$.

    Set of all polynomials of degree less than n with rational coefficients is countable. That is, $S \sim \mathbb{Q}^n \implies |S| = \aleph_0$.

    The set of all circles with rational radii and center with rational co-ordinates is countable. That is, $S \sim \mathbb{Q}^3 \implies |S| = \aleph_0$.

    The collection of function, $F = \{f : \mathbb{R} \to \mathbb{R}\}$ is uncountable. $|F| = |\mathbb{R}|^{|\mathbb{R}|} = \aleph_2$.

21. Let $f : X \to Y$, $g : Y \to X$ and $g \circ f = id_X$. Then $f \circ g$ is idempotent.

Part I

Mathematics 1

Chapter 2

Analysis

2.1 Real Set Theory

1. A **neighbourhood** of $x \in S$ is an open interval [1] containing x contained in S.

2. A point $x \in S$ is an **interior point** of S if there exists $\varepsilon > 0$ such that $(x-\varepsilon, x+\varepsilon)$ is contained in S. The set of all interior points of S is the **interior** of S, S^0.

   The interior of a set S is the largest open set contained in it.

   Boundary points of an interval is not its interior points. That is, $[a,b]^0 = (a,b)$.

3. A set G is **open** if and only if $G^0 = G$.

   Open sets are countable union of disjoint open intervals.

4. Arbitrary union of open sets is open. Finite intersection of open sets is open.

5. A set C is closed if $\mathbb{R} - C$ is open.

   Closure of a set S, is the smallest closed set $\bar{S}$ containing S.

   The **exterior** of a set is the interior of its complement. The **boundary** of a set ∂S is the intersection of its closure and closure of its exterior.

6. A point x is a **limit point** of S if every neighbourhood of x has infinitely many points of S.

   A point x is a limit point of S if there exists an eventually nonconstant sequence $\{x_n\}$ in S converging x.

   $S = \{\frac{1}{n} : n \in \mathbb{N}\}$ has limit point 0.

   The set of limit points of a set S is the **derived set** S'.

   $\bar{S} = S \cup S'$.

7. A set S is **rare**(nowhere dense) if its interior is empty. A set S is **meagre**(Baire first category) if it is a countable union of rare sets. A set S is **non-meagre**(second category) if it is not meagre.

   The set of rational numbers is rare.

   The set of irrationals numbers is rare.

[1] N is a neighbourhood of x if there exists an set G containing x which is open in S.

Cantor set is rare.

Notions of smallness : $Countable > Zero\ Measure > Rare$.[2]

8. Cantor function is uniformly continuous, but not absolutely continuous.

   Voltera function is differentiable, but its derivative is not integrable.

   Weierstrass function[3] is continuous everywhere but nowhere differentiable.

9. **Dedekind Cut** : $\mathbb{Q} = [A : B]$ where $A = \{q \in \mathbb{Q} : q < \sqrt{2}\}$ and $B = \{q \in \mathbb{Q} : q > \sqrt{2}\}$. Clearly, $\mathbb{Q} = A \cup B$, A does not have a maximum and B does not have a minimum.

10. A set S is bounded above if there exists $m \in \mathbb{R}$ such that $\forall x \in S,\ x \leq m$. If S is bounded above, there exists infinitely many upperbounds. The least upperbound is the **supremum** of S, say $\sup(S)$. If S is not bounded above, then $\sup(S) = +\infty$.

    $\sup(S) \notin S$

    If $\sup(S) \in S$, then $\sup(S) = \max(S)$.

11. The greatest lowerbound is the **infimum** of S, say $\inf(S)$. If S is not bounded below, then $\inf(S) = -\infty$.

2.2 Properties of Numbers

1. Greatest integer function $\forall x \in \mathbb{R}, \quad x - 1 < \lfloor x \rfloor < x$
2. Arithmetic vs Geometric mean $\forall a, b \in \mathbb{R}, \quad \frac{a+b}{2} \geq \sqrt{ab}$
3. Exponential function $\lim\limits_{n\to\infty} \left(1 + \frac{x}{n}\right)^n = e^x$
4. Archimedian Property $\forall x \in \mathbb{R},\ \exists n \in \mathbb{N} : x < n$
5. Dense Subset $\forall x, y \in \mathbb{R},\ \exists r \in \mathbb{Q} : x < r < y \quad (x < y)$
6. $||a| - |b|| \leq |a - b|$
7. Derived Set $A' = \{x \in X : \forall N \in \mathcal{N}_x, N - \{x\} \cap A \neq \phi\}$.
8. Every function on $\mathbb{N}$ is continuous as the induced topology on $\mathbb{N}$ is discrete.

2.3 Sequence

1. A **sequence** x_n in a set X is a function $x : \mathbb{N} \to X$ where $x_n = x(n)$.
2. A **subsequence** x_{n_k} of a sequence x_n is a function $x \circ n$ where $n : \mathbb{N} \to \mathbb{N},\ n_k = n(k)$ is a strictly increasing sequence.
3. A sequence $\{x_n\}$ is **convergent** if there exists $x \in \mathbb{R},\ \forall \varepsilon > 0,\ \exists N \in \mathbb{N}$ such that $\forall n > N, |x_n - x| < \varepsilon$. Then x is a **limit** of the sequence $\{x_n\}$ and $x_n \to x$.

---

[2] The Smith-Voltera cantor set is a rare set with measure $\frac{1}{2}$, constructed by removing $\frac{1}{4}$th from middle.

[3] Weierstrass' monster function, $f(x) = \sum_{k=1}^{\infty} a^k \cos(b^k \pi x)$

4. If space X is T_2, then limit of convergent sequence in X is unique.

   In $\mathbb{R}$, limit of a convergent sequence is unique.

5. A sequence $\{x_n\}$ converges if and only if every subsequence $\{x_{n_k}\}$ converges.

6. A sequence $\{x_n\}$ is **bounded** if $|x_n| \leq k$.

   Every convergent sequence is bounded.

   Bolzano-Weierstrass Theorem : Every bounded sequence has a convergent subsequence.

7. A point x is a **limit point**(cluster point) of the sequence $\{x_n\}$ if every neighbourhood of x contains infinitely many terms of the sequence.

   x is a limit point of $\{x_n\}$ if and only if it has a subsequence converging to x.

   Every convergent sequence has a unique limit point.

   A bounded sequence with unique limit point is convergent.

8. A sequence x_n is **Cauchy** if $\forall \varepsilon > 0, \ \exists N \in \mathbb{N}$ such that $\forall n, m > N, \ |x_n - x_m| < \varepsilon$.

   Every Cauchy sequence is bounded.

9. A space is **complete** if every Cauchy sequence in it converges.

   In $\mathbb{R}$, sequence is convergent if and only if Cauchy.

   $\mathbb{R}^n, \mathbb{C}^n, l^2, C[a,b]$ are complete.

   Sequence space l^p is complete if and only if $p = 2$.

10. A sequence $\{x_n\}$ is **monotonically increasing** if $\forall n \in \mathbb{N}, \ a_{n+1} \geq a_n$.

    Every sequence has a monotone subsequence.

    Every monotonically increasing(decreasing) sequence which is bounded above(below) is convergent. And the limit is its supremum(infimum).

11. A sequence $\{x_n\}$ is **contractive** if there exists $c \in (0,1)$ such that $|a_{n+2} - a_{n+1}| \leq c|a_{n+1} - a_n|$ for sufficiently large values of n.

    Every contractive sequence is Cauchy.

12. $\forall x \in \mathbb{R}$, there exist a rational sequence and an irrational sequence converging to x. $\left[\frac{10^n x_n}{10^n}\right] \to x$ and $x_n + \frac{\sqrt{2}}{n} \to x$.

13. Logarithm function is continuous. That is, $x_n \to x \implies \ln x_n \to \ln x, \quad (x_n > 0)$.

14. Square root function is continuous. That is, $x_n \to x \implies \sqrt{x_n} \to \sqrt{x}, \quad (x_n > 0)$.

15. Properties of Convergent Sequences,

    $x_n \to x \implies kx_n \to kx.$

    $x_n \to x, \ y_n \to y \implies x_n \pm y_n \to x \pm y.$

    $x_n \to x, \ y_n \to y \implies x_n y_n \to xy$

    $x_n \to x, \ y_n \to y, \ y_n \neq 0, \ y \neq 0 \implies x_n / y_n \to x/y$

16. $x_n \to x,\ y_n \to y,\ x_n \le y_n \implies x \le y$

    $x_n \to x, x_n \le k \implies x \le k.$

17. **Squeeze theorem** : $x_n \le y_n \le z_n,\ x_n \to l,\ z_n \to l \implies y_n \to l.$

18. Every convergent sequence is absolute convergent.

    $|x_n| \to |x| \not\Longrightarrow x_n \to x.$

    $x_n \to 0 \iff |x_n| \to 0.$

19. $x_n y_n \to xy,\ x_n \to x \not\Longrightarrow y_n \to y$

20. $x_n \to \pm\infty \implies x_{n_k} \to \pm\infty.$

21. Tests for non-convergence,

    Unbounded sequences are non-convergent.

    If sequence has two convergent subsequence with distinct limits.

    If it has a non-convergent subsequence.

22. A few popular convergent sequences,

    $x^n \to 0$ where $(|x| < 1)$.

    $\frac{1}{n^p} \to 0$ provided $p > 0$.

    $p^{\frac{1}{n}} \to 1$ provided $p > 0$.

    $n^{\frac{1}{n}} \to 1.$

    $(1 + \frac{1}{n})^n \to e.$

23. $(1 + \frac{2}{n})^n \to e^2$
    Let $x_n = (1 + \frac{2}{n})^n$. Suppose sequence $\{x_n\}$ converges, then subsequence $\{x_{2n}\}$ converges to the same limit and $x_{2n} = \left((1 + \frac{1}{n})^n\right)^2 \to e^2$.

24. A sequence $\{x_n\}$ is **Cesaro summable** if the sequence of arithmetic means is convergent.

25. **Cauchy's First Theorem on Limits** : Every convergent sequence is Cesaro summable and has the same limit. That is, $x_n \to x \implies \frac{x_1+x_2+\cdots+x_n}{n} \to x$.

    Let sequence $\{p_n\}$ be a sequence of positive real numbers with $\frac{1}{p_1+p_2+\cdots+p_n} \to 0$. Then sequence of weighted arithmetic means also converges to the same limit. That is, $x_n \to x \implies \frac{p_1x_1+p_2x_2+\cdots+p_nx_n}{p_1+p_2+\cdots+p_n} \to x$.

    The sequence of geometric means also converges to the same limit. That is, $x_n \to x \implies (x_1x_2\ldots x_n)^{\frac{1}{n}} \to x$ provided $x_n \ge 0$.

26. **Cauchy's Second Theorem** : $\frac{x_{n+1}}{x_n} \to l \implies x_n^{\frac{1}{n}} \to l.$

    D'Alembert's **Ratio Test** : Suppose $x_n > 0$ and let $\frac{x_{n+1}}{x_n} \to l$. If $l < 1,\ x_n \to 0$. If $l > 1,\ x_n \to +\infty$. If $l = 1$, test fails.

    Cauchy's **Root test** : Suppose $x_n \ge 0$ and let $(x_n)^{\frac{1}{n}} \to l$. If $l < 1,\ x_n \to 0$. If $l > 1,\ x_n \to +\infty$. If $l = 1$, test fails.

27. **Cesaro's theorem** : The Cauchy product of two convergent sequences is Cesaro summable. That is, $x_n \to x,\ y_n \to y \implies \frac{x_1y_n+x_2y_{n-1}+\cdots+x_ny_1}{n} \to xy$.

28. **Stolz-Cesaro Theorem** : $\frac{x_n-x_{n-1}}{y_n-y_{n-1}} \to l \implies \frac{x_n}{y_n} \to l$ provided $\{y_n\}$ is strictly monotone and diverges to $\pm\infty$.

    $\frac{x_n-x_{n-1}}{y_n-y_{n-1}} \to l \implies \frac{x_n}{y_n} \to l \implies \frac{x_1+x_2+\cdots+x_n}{y_1+y_2+\cdots+y_n} \to l$ provided $\{y_n\}$ is strictly increasing to $+\infty$.[4]

29. **Riemann Sum**

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=0}^{\infty} f(k/n) = \int_0^1 f(x)\,dx$$

Problems

1. $\frac{(n+1)!}{(n+1)^{n+1}}\frac{n^n}{n!} \to \frac{1}{e} \implies \left(\frac{n!}{n^n}\right)^{\frac{1}{n}} = \frac{\sqrt[n]{n!}}{n} \to \frac{1}{e}$

2.4 Series

1. A **series** $\sum a_n$ is a sequence of the form $\{b_n\}$ where $b_n = \sum_{k=1}^{n} a_n$, the sequence of partial sums. If the sequence of partial sums converges to s, then the **sum** of the series $\sum a_n = s$. If the sequence of partial sums diverges, the series also diverges.

2. nth term test : If $\sum a_n$ converges, then $a_n \to 0$. And if $a_n \not\to 0$ then $\sum a_n$ diverges.

3. Suppose $\sum a_n, \sum b_n$ converges, then $\sum a_n + b_n,\ \sum \alpha a_n$ converges.

    (a) Abel's test : if $\sum a_n$ is monotonic and $\sum a_n, \sum b_n$ converges, then $\sum a_n b_n$ converges

    (b) Dirichlet's test : if $\sum a_n$ is decreasing & converges and sequence of partial sums of $\sum b_n$ is bounded, then $\sum a_n b_n$ converges.

4. Power Series test : $\sum 1/n^p$ converges if $p > 1$ and diverges if $p \leq 1$.

5. Geometric Series test : $\sum a^n$ converges if $|a| < 1$ and diverges if $|a| \geq 1$.

6. Ratio test : Let $a_n > 0$ [5] and $a_{n+1}/a_n \to l$.
   If $l < 1$, $\sum a_n$ converges. If $l > 1$, $\sum a_n$ diverges. If $l = 1$, test fails.

7. Comparison test : Suppose $0 \leq a_n \leq b_n$.
   If $\sum b_n$ converges, then $\sum a_n$ converges. If $\sum a_n$ diverges, then $\sum b_n$ diverges.

8. Limit Comparison Test : Suppose $a_n > 0$ and $b_n > 0$[6] and $a_n/b_n \to l$.
   If $l = 0$ and $\sum b_n$ converges, then $\sum a_n$ converges. If $l \neq 0$, then both behaves alike.

---

[4] Why the corollary of Stolz-Cesaro theorem is not applicable when y_n is strictly monotone and diverges to $\pm\infty$.

[5] The condition $a_n > 0$ can be relaxed a bit, to eventually positive as eventuality is all that matters.

[6] In this case, eventuality is not sufficient.

9. Cauchy's nth root test : If $a_n > 0$ and $a^{\frac{1}{n}} \to l$.
If $l < 1$, then $\sum a_n$ converges. If $l > 1$, then $\sum a_n$ diverges. If $l = 1$, test fails.

10. Condensation test : Suppose sequence a_n is decreasing and positive.
Then $\sum a_n$ and $\sum 2^n a_n$ behaves similar. Tailor-made for logarithmic functions.

11. Rabee's test : Suppose $a_n > 0$ and $n\left(\frac{a_n}{a_{n+1}} - 1\right) \to l$.
If $l < 1$, then $\sum a_n$ converges. If $l > 1$, then $\sum a_n$ diverges. If $l = 1$, test fails.

12. Logarithmic test : Suppose $a_n > 0$ and $n \log(a/a_{n+1}) \to l$.
If $l > 1$, then $\sum a_n$ converges. If $l < 1$, then $\sum a_n$ diverges.

13. Lebinitz test : Suppose sequence a_n is decreasing and converges to zero. $(a_n \downarrow_0)$
Then the **alternating series** $\sum(-1)^n a_n$ converges.

14. A series $\sum a_n$ is **absolutely convergent** if $\sum |a_n|$ converges. In the case of series, absolute convergence implies convergence. A sequence which is convergent, but not absolutely convergent is **conditionally convergent**.

2.5 Limit Superior/Inferior

Definitions 2.1.

$$\limsup_{n\to\infty} x_n = \inf_{n\geq 0} \sup_{m\geq n} x_n$$

Definitions 2.2.

$$\liminf_{n\to\infty} x_n = \sup_{n\geq 0} \inf_{m\geq n} x_n$$

Remark. $\liminf x_n = I, \limsup x_n = S$ *are the bounds for cluster points of* x_n*. Thus, there are at most finitely many terms outside* $(I - \varepsilon, S + \varepsilon)$*. However,* $[I, S]$ *may not contain any term of* x_n*. For example,* $x_n = (-1)^n(1 + \frac{1}{n})$.

2.5.1 Properties of limit superior/inferior

$$\inf x_n \leq \liminf x_n \leq \limsup x_n \leq \sup x_n$$
$$\liminf a_n + \liminf b_n \leq \liminf(a_n + b_n) \leq \limsup(a_n + b_n) \leq \limsup a_n + \limsup b_n$$
$$\liminf a_n \liminf b_n \leq \liminf(a_n b_n) \leq \limsup(a_n b_n) \leq \limsup a_n \limsup b_n$$

Theorem 2.3 (Stolz-Cesaro)**.**

$$\liminf_{n\to\infty} \frac{a_{n+1} - a_n}{b_{n+1} - b_n} \leq \liminf_{n\to\infty} \frac{a_n}{b_n} \leq \limsup_{n\to\infty} \frac{a_n}{b_n} \leq \limsup_{n\to\infty} \frac{a_{n+1} - a_n}{b_{n+1} - b_n}$$

2.6 Limit of a function

Definitions 2.4 (limit)**.** *If* $f(x_n) \to L$ *as* $x_n \to a$*, then* $\lim_{x\to a} f(x) = L$.

Definitions 2.5 (continuity)**.** *A function* $f : X \to Y$ *is continuous at* $a \in X$*, if* $\lim_{x\to a} f(x) = f(\lim_{x\to a} x) = f(a)$.

Theorem 2.6. *Limit is algebraic.*

Suppose $\lim_{x\to a} f(x)$, $\lim_{x\to a} g(x)$ exists, then

$$\lim_{x\to a} cf(x) = c\lim_{x\to a} f(x) \tag{2.1}$$
$$\lim_{x\to a} f(x) \pm g(x) = \lim_{x\to a} f(x) \pm \lim_{x\to a} g(x) \tag{2.2}$$
$$\lim_{x\to a} f(x)g(x) = \lim_{x\to a} f(x) \ \lim_{x\to a} g(x) \tag{2.3}$$
$$\lim_{x\to a} \frac{f(x)}{g(x)} = \frac{\lim_{x\to a} f(x)}{\lim_{x\to a} g(x)} \tag{2.4}$$
$$\lim_{x\to a} f(x)^{g(x)} = \lim_{x\to a} f(x)^{\lim_{x\to a} g(x)} \tag{2.5}$$

Remark (exceptions)**.**

$$\frac{0}{0}, \frac{\pm\infty}{\pm\infty}, \ 0\pm\infty, \ \infty-\infty, \ 0^0, \ \infty^0, \ 1^{\pm\infty}$$

Theorem 2.7 (L'Hospital/Bernouli)**.**

$$\lim_{x\to a} \frac{f(x)}{g(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)}$$

Remark (application)**.**

$$\lim_{x\to 0}(2+x)^{\frac{1}{x}} = \lim_{x\to 0} e^{\frac{1}{x}\log(2+x)} = e^{\lim_{x\to 0} \frac{\log(2+x)}{x}} = e^{\lim_{x\to 0} \frac{1}{2+x}} = \sqrt{e}$$

Squeeze theorem Suppose $f(x) \le g(x) \le h(x)$ for each x in an open interval containing a (except a). If $\lim_{x\to a} f(x) = \lim_{x\to a} h(x) = L$, then

$$\lim_{x\to a} g(x) = L \tag{2.6}$$

Theorem 2.8 (chain rule)**.** *Suppose $\lim_{x\to a} g(x) = b$ and f is continuous at b, then*

$$\lim_{x\to a} f(g(x)) = f(\lim_{x\to a} g(x)) = f(b) = c \tag{2.7}$$

Remark. *The existence of limit $\lim_{y\to b} f(y) = c$ does not imply $f(b) = c$. If g assumes value b in some neighbourhood of a, then*

$$\lim_{x\to a} g(x) = b, \ \lim_{y\to b} f(x) = c \not\Longrightarrow \lim_{x\to a} f\circ g(x) = c$$

2.7 Limit Inferior/Superior of Functions

Definitions 2.9 (metric)**.**

$$\limsup_{x\to a} f = \lim_{\varepsilon\to 0} \sup_{x\in B(a,\varepsilon)^*} \{f(x)\} = \inf_{\varepsilon>0} \sup_{x\in B(a,\varepsilon)^*} \{f(x)\}$$

$$\liminf_{x\to a} f = \lim_{\varepsilon\to 0} \inf_{x\in B(a,\varepsilon)^*} \{f(x)\} = \sup_{\varepsilon>0} \inf_{x\in B(a,\varepsilon)^*} \{f(x)\}$$

2.8 Sequence of Functions

2.8.1 Notions of Convergence

Definitions 2.10 (pointwise)**.** *Sequence of functions are pointwise convergent if for each $x_0 \in X$, the sequence $f_n(x_0)$ converges to $f(x_0)$.*

$$\textit{(metric)} \quad \forall x \in X,\ \forall \varepsilon > 0,\ \exists N_{x,\varepsilon} \in \mathbb{N},\ \forall n > N_{x,\varepsilon},\ d(f_n(x), f(x)) < \varepsilon \tag{2.8}$$
$$\textit{(norm)} \quad \forall x \in X,\ \forall \varepsilon > 0,\ \exists N_{x,\varepsilon} \in \mathbb{N},\ \forall n > N_{x,\varepsilon},\ \|f_n(x), f(x)\| < \varepsilon \tag{2.9}$$
$$\textit{(nbd)} \quad \forall x \in X,\ \forall U \in \mathcal{N}_{f(x)},\ \exists N_{x,U} \in \mathbb{N},\ \forall n > N_{x,U},\ f_n(x) \in U \tag{2.10}$$

Definitions 2.11 (uniform)**.** *Sequence of functions are uniformly convergent if for each $x \in X$, all the sequences $f_n(x)$ converges to $f(x)$ uniformly.*

$$\textit{(metric)} \quad \forall \varepsilon > 0,\ \exists N_{\varepsilon} \in \mathbb{N},\ \forall x \in X,\ \forall n > N_{\varepsilon},\ d(f_n(x), f(x)) < \varepsilon \tag{2.11}$$
$$\textit{(norm)} \quad \forall \varepsilon > 0,\ \exists N_{\varepsilon} \in \mathbb{N},\ \forall x \in X,\ \forall n > N_{\varepsilon},\ \|f_n(x), f(x)\| < \varepsilon \tag{2.12}$$
$$\textit{(nbd)} \quad ?? \tag{2.13}$$

2.8.2 Notions of Boundedness

Definitions 2.12 (pointwise)**.** *Sequence of functions is pointwise bounded if for each $x_0 \in X$, the sequence $f_n(x_0)$ is bounded.*

$$\forall x \in X,\ \exists M_x \in \mathbb{R},\ |f_n(x)| < M_x \tag{2.14}$$

Definitions 2.13 (uniform)**.** *Sequence of functions if uniformly bounded if the pointwise bounds are uniform.*

$$\exists M \in \mathbb{R},\ \forall x \in X,\ |f_n(x)| < M \tag{2.15}$$

2.9 Limit of a Set

Definitions 2.14.

$$\liminf X = \inf\{\textit{limit points}\}$$
$$\limsup X = \sup\{\textit{limit points}\}$$

2.10 Sequence of Sets

Definitions 2.15.

$$\liminf X_n = \bigcup_{n=1}^{\infty} \bigcap_{m=n}^{\infty} X_n$$
$$\limsup X_n = \bigcap_{n=1}^{\infty} \bigcup_{m=n}^{\infty} X_n$$

Part II

Mathematics 2

Chapter 3

Algebra

3.1 Number Theory

Lemma 3.1 (Euclid)**.** *Let p be a prime. If p divides ab, then either p divides a or p divides b.*

Greatest Common Divisor

1. Bézout's Identity : If $\gcd(n, m) = d$, then $\exists s, t \in \mathbb{Z}$ such that $d = sn + tm$.

2. Euclid's Division Algorithm : If $b > 0$, then $\forall a \in \mathbb{Z}$, $\exists q \in \mathbb{Z}$ and $\exists r \in \mathbb{Z}$ such that $a = qb + r$ where $0 \leq r < b$.

3. Euclid's Algorithm : $\gcd(a, b) = \gcd(b, r) = \cdots = \gcd(d, 1)$ where $a = bq + r$.

4. The linear equation $ax + by = c$ has integer solutions if $\gcd(a, b)$ divides c.
   If (x, y) is a solution, then $(x - b/d, y - a/d)$ is also a solution.

5. Chinese Remainder Theorem : Let $x \cong a_j \pmod{n_j}$ be a system of congruences where $\gcd(n_j, n_k) = 1,\ (j \neq k)$. Then there exists a solution.
   If x_1, x_2 is are two solutions, then $x_1 \cong x_2 \pmod{N}$ where $N = \prod n_j$.

$$x \cong \sum a_j M_j N_j \pmod{N} \text{ where } N_j = \frac{N}{n_j} \text{ and } M_j \cong N_j^{-1} \pmod{n_j}$$

Congruences

Definitions 3.2. *The congruence is a relation on $\mathbb{Z}$ defined by*

$$a \cong b \pmod{n} \iff n|(a - b)$$

1. The relation $\cong$ is an equivalence relation.

2. $a \cong b \pmod{n} \implies \forall k,\ a^k \cong b^k \pmod{n}$.

3. If $\gcd(a, n) = 1$, then $a^{-1} \pmod{n}$ exists.

4. Linear congruence equation $ax \cong b \pmod{n}$ has a solution if $\gcd(a, n)$ divides b.

Euler's phi function The function $\phi : \mathbb{N} \to \mathbb{N}$ is defined as $\phi(n) =$ the cardinality of the set $\{k \in \mathbb{N} : k \leq n,\ \gcd(n,k) = 1\}$.

1. ϕ is multiplicative. That is, $\phi(mn) = \phi(m)\phi(n),\ \gcd(m,n) = 1$.
2. $\phi(p^n) = p^n - p^{n-1}$ where p is a prime.
3. $\phi(n)$ is even for $n > 2$.
4. The sum of $\phi(d)$ for all divisors of n is n.
5. The sum of all natural numbers $k \leq n$ that are relatively prime to n is $n\phi(n)/2$.

Theorem 3.3 (Fermat)**.** $a^p \cong a \pmod p$

Definitions 3.4. *A number x such that $a^x \cong a \pmod x$ is a (fermat)* ***pseudoprime*** *for base a where $\gcd(a,x) = 1$.*

Number 341 is the smallest pseudoprime for base 2.

Definitions 3.5. *A number x is a* ***Carmichael*** *number if $a^x \cong a \pmod x$ whenever $\gcd(a,x) = 1$.*

3.1.1 Arithmetical Functions

Definitions 3.6. *A function $f : \mathbb{N} \to \mathbb{C}$ is an* ***arithmetical*** *(number theoretic) function.*

Definitions 3.7. *An arithmetical function f is multiplicative iff $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$. And completely multiplicative iff $f(mn) = f(m)f(n)$ always.*

Definitions 3.8. *The* ***Dirichlet convolution***

$$f * g = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

Clearly, Dirichlet convolution is commutative and associative.
And Dirichlet convolution of multiplicative functions in multiplicative. However, Dirichlet convolution of completely multiplicative functions is not completely multiplicative.

Definitions 3.9. *Every artithmetical function f with $f(1) \neq 0$ has a unique* ***Dirichlet inverse*** *f^{-1}.*

$$f^{-1}(n) = \begin{cases} \frac{1}{f(1)} & n = 1 \\ \frac{-1}{f(1)} \sum\limits_{\substack{d|n \\ d<n}} f(n/d) f^{-1}(d) & n > 1 \end{cases}$$

Clearly, $(f * g)^{-1} = g^{-1} * f^{-1}$ provided f^{-1} and g^{-1} exists.

Theorem 3.10. *Let f be multiplicative. Then f is completely multiplicative iff $f^{-1} = \mu f$.*

Arithmetical Functions and their Dirichlet products

1. **Identity function**, $I(n) = \left[\frac{1}{n}\right]$ vanishes everywhere except at $n = 1$, $I(1) = 1$. Clearly, I is completely multiplicative.

2. **Möbius function**, $\mu(n)$ gives the parity of the number of prime factors of a square free number and vanishes for numbers which are contains a square.
   For example, $\mu(1) = 1,\ \mu(30) = -1,\ \mu(12) = 0$. Clearly, μ is multiplicative.

3. **Riemann Zeta function**, $\zeta(n) = 1$ is completely multiplicative.
   Thus $\zeta^{-1} = \mu\zeta = \mu$.

4. **Power function**, $N^\alpha(n) = n^\alpha$ is completely multiplicative.
   Thus, $(N^\alpha)^{-1} = \mu N^\alpha$. And $N^0 = \zeta$.

5. **Characteristic function**, χ_S is the membership indicator function.

$$\chi_S(n) = \begin{cases} 1 & n \in S \\ 0 & n \notin S \end{cases}$$

   χ_S is not multiplicative.

6. **Euler totient function**, $\phi(n)$ gives the number of positive integers less than n which are relatively prime to n. And $\phi = \mu * N$. Thus, $\phi^{-1} = \zeta * \mu N$.

7. **Liouville function** $\lambda(n)$ gives the parity of sum of prime powers of n.
   For example, $\lambda(1) = 0,\ \lambda(30) = -1,\ \lambda(12) = -1$.
   Clearly, λ is completely multiplicative and $\lambda^{-1} = \mu\lambda$.
   And $\lambda = \mu * \chi_{Sq}$ where Sq is the set of all squares.

8. **Divisor function** $\sigma_\alpha(n)$ is the sum of αth powers of divisors of n.
   Clearly, $\sigma_\alpha = \zeta * N^\alpha$. And $\sigma_\alpha^{-1} = \mu * \mu N^\alpha$.

9. $\tau(n)$ gives the number of divisors of n.And $d(n)$ gives the sum of divisors of n.
   Clearly, $\tau = \sigma_0 = \zeta * \zeta$. And $d = \sigma = \sigma_1 = \zeta * N$.
   We have, $\sigma * \phi = \zeta * N * \mu * N = N * N = N\tau$ since,

$$N * N(n) = \sum_{d|n} N(d)N(n/d) = \sum_{d|n} n = N(n)\tau(n)$$

   and $\tau * \phi = \zeta * \zeta * \mu * N = \zeta * N = \sigma$

10. $\omega(n)$ gives the number of distinct prime factors of n.
    Clearly $\omega = \zeta * \chi_{\mathbb{P}}$ where $\mathbb{P}$ is the set of all primes.

11. $\Omega(n)$ gives the number of prime factors of n counted with multiplicity. Clearly, $\Omega = \zeta * \chi_{\mathcal{P}}$ where $\mathcal{P}$ is the set of all prime powers

12. p-adic valuation $\nu_p(n)$ is the exponent of highest power of prime p that divides n.

$$\omega(2^n 3^m) = 2,\ \Omega(2^n 3^m) = n + m,\ \nu_2(2^n 3^m) = n$$

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots$$

Strange Functions

1. $\sin : \mathbb{N} \to [-1, 1]$ is an injection since $\sin(x) = \sin(y) \implies 2\pi|(x - y)$.

3.2 Group Theory

Definitions 3.11. *An* ***algebra*** *is $\langle \mathcal{S}, \mathcal{F} \rangle$ where $\mathcal{S}$ is a collection of sets and $\mathcal{F}$ is a collection of functions/relations defined on them.*

Definitions 3.12. *A* ***binary relation*** *on a set A is a relation between $A \times A$ and A.*

Definitions 3.13. *An* ***associative*** *binary relation $*$ on A satisfies*

$$(x * y), (y * z) \in A \implies (x * y) * z, x * (y * z) \in A,\ (x * y) * z = x * (y * z) \tag{3.1}$$

Definitions 3.14. *A* ***commutative*** *binary relation $*$ on A satisfies*

$$x * y \in A \implies y * x \in A,\ x * y = y * x \tag{3.2}$$

A commutative algebra is also called abelian.

Definitions 3.15. *A binary* ***operation*** *on A is a function $* : A \times A \to A$.*

Definitions 3.16. *An* ***associative*** *binary operation $*$ on A satisfies*

$$(x * y) * z = x * (y * z) \tag{3.3}$$

Definitions 3.17. *A* ***commutative*** *binary operation $*$ on A satisfies*

$$x * y = y * x \tag{3.4}$$

Definitions 3.18. *A binary* ***algebra*** *$\langle A, * \rangle$ is an algebra with a set A together with a binary operation $*$ on A.*

Definitions 3.19. *A* ***magma*** *is a binary algebra $\langle A, * \rangle$ where $*$ is a binary operation on A. By the definition of binary operation, $*$ is well-defined(closed) on $A \times A$.*

Definitions 3.20. *A* ***semigroup*** *is a magma $\langle A, * \rangle$ where $*$ is associative.*

Definitions 3.21. *A* ***left identity*** *e' of an algebra $\langle A, * \rangle$ satisfies $e' * x = x,\ \forall x \in A$. And* ***right identity*** *e' satisfies $x * e' = x,\ \forall x \in A$. An* ***identity*** *element e of $\langle A, * \rangle$ satisfies both.*

A binary algebra has at most one identity element. Homomorphisms map identity elements into identity elements.

Definitions 3.22. *A* ***monoid*** *is a semigroup $\langle A, * \rangle$ where $*$ has an identity $e \in A$.*

Definitions 3.23. *Let $x \in A$. An* ***inverse*** *x^{-1} of x in an algebra $\langle A, * \rangle$ satisfies $xx^{-1} = x^{-1}x$. Let e be the identity of a monoid $\langle A, * \rangle$. Then, x^{-1} satisfies $xx^{-1} = x^{-1}x = e$.*

Definitions 3.24. *A* ***group*** *is a monoid $\langle A, * \rangle$ where every element $x \in A$ has an inverse x^{-1}.*

Definitions 3.25. *An algebra $\langle R, +, \times \rangle$ is a **ring** if*

1. *$\langle R, + \rangle$ is an abelian group.*
2. *$\langle R, \times \rangle$ is a semigroup.*
3. *$\times$ is distributive over $+$.*

Definitions 3.26. *A commutative ring with unity $\langle D, +, \times \rangle$ is an **integral domain** if*

1. *$\langle D^*, \times \rangle$ has no zero divisors.*
2. *$\times$ is distributive over $+$.*

Definitions 3.27. *An integral domain $\langle F, +, \times \rangle$ is a **field** if*

1. *$\langle F^*, \times \rangle$ is an abelian group.*
2. *$\times$ is distributive over $+$.*

Definitions 3.28. *An algebra $\langle V, F, +, \times \rangle$ is a linear algebra if*

1. *$\langle F \rangle$ is a field.*
2. *$\langle V, + \rangle$ is an abelian group.*
3. *$\langle V, \times \rangle$ is a semigroup.*
4. *$\times$ is distributive over $+$.*

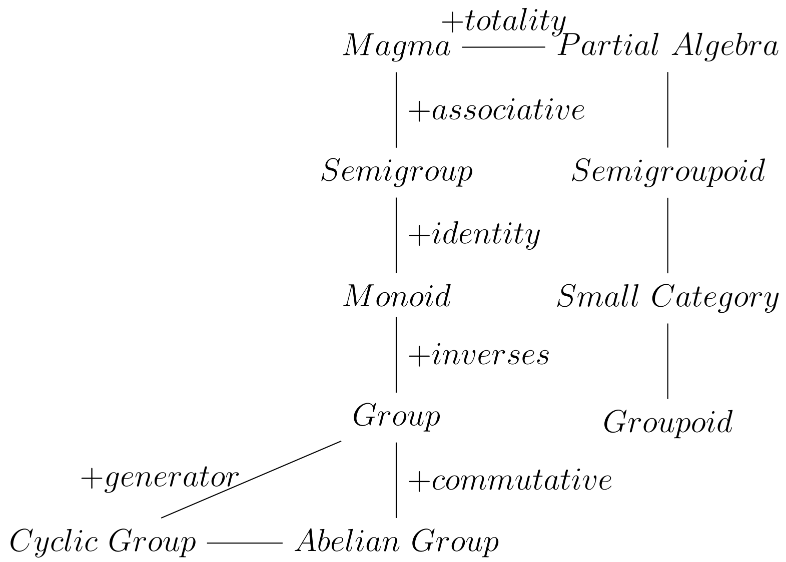

Figure 3.1: Binary Algebraic Structures

Definitions 3.29. *The **sum** of two subsets A and B of a magma*[1] *$\langle X, + \rangle$ is*

$$A + B = \{a + b : a \in A, b \in B\}$$

[1] Instead of magma, the name groupoid is used in many texts that don't study groupoid in detail

Definitions 3.30. *Let $\langle R, +, \cdot \rangle, \langle R', +', \cdot' \rangle$ be two commutative rings with identity. A function $f : R \to R'$ is **linear** if $f(k \cdot x + y) = k \cdot' f(x) +' f(y)$.*

Definitions 3.31. *A function $f : R^n \to R'$ is n-**linear** if for $1 \leq k \leq n$,*

$$f(a_1, a_2, \ldots, ka_i + a_i', \ldots, a_n) = kf(a_1, a_2, \ldots, a_i, \ldots, a_n) + f(a_1, a_2, \ldots, a_i', \ldots, a_n)$$

Definitions 3.32. *Let $\langle G, *_1, *_2, \ldots, *_r \rangle$ and $\langle H, \star_1, \star_2, \ldots, \star_r \rangle$ be two algebraic structures. A function $f : G \to H$ is a **homomorphism** if $\forall *_k,\ f(x *_k y) = f(x) \star_k f(y)$.*

Definitions 3.33. *An **isomorphism** is a bijective, homomorphism.*

1. Number of relations on $A = 2^{n^2}$.
2. Number of reflexive relations on $A = 2^{n^2 - n}$.
3. Number of symmetric relatons on $A = 2^{\frac{n(n+1)}{2}}$.
4. Number of equivalence relations on $A = B(n)$, n^{th} Bell number[2]
5. Number of total relations on $A = 2^n 3^{\frac{n(n-1)}{2}}$.

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 4 & 0 & 5 & 6 \\ 7 & 8 & 0 & 9 \\ 10 & 11 & 12 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 4 & 7 \\ \bar{2} & 3 & 5 & 8 \\ \bar{4} & \bar{5} & 6 & 9 \\ \bar{7} & \bar{8} & \bar{9} & 10 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & 2 & 3 \\ \bar{1} & 2 & 4 & 5 \\ \bar{2} & \bar{4} & 3 & 6 \\ \bar{3} & \bar{4} & \bar{6} & 4 \end{bmatrix}$$

Figure 3.2: Enumerating Relations - Reflexive, Symmetric, and Total

6. Let $|A| = m$, $|B| = n$. Number of functions $f : A \to B = n^m$.
7. Number of injections $f : A \to B = {}^nP_m \qquad (n \geq m)$.
8. Number of surjections $f : A \to B = \displaystyle\sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^m \qquad (n \leq m)$
9. Number of bijections $f : A \to B = n! \qquad (n = m)$

$$\begin{array}{lllll} 1 \\ 1 & 2 \\ 2 & 3 & 5 \\ 5 & 7 & 10 & 15 \\ 15 & 20 & 27 & 37 & 52 \end{array}$$

Figure 3.3: Bell Triangle

10. Number of binary operations on $A = n^{n^2}$ where $|A| = n$.

[2] $B(n) = \sum S(n, k)$ where $S(n, k)$ are Stirling numbers of second kind.

3.2.1 Groups and Subgroups

Definitions 3.34. *A* ***group*** *is a binary algebraic structure* $\langle G, * \rangle$ *which satisfies*

1. $*$ *is closed,* $\forall x, y \in G,\ x * y \in G$
2. $*$ *is associative,* $\forall x, y, z \in G,\ (x * y) * z = x * (y * z)$.
3. $*$ *has an identity element,* $\exists e \in G,\ \forall x \in G,\ e * x = x = x * e$.
4. $*$ *has inverses for every element of* G*,* $\forall x \in G,\ \exists x^{-1} \in G,\ x * x^{-1} = e = x^{-1} * x$

Definitions 3.35. *The* ***order*** *of a group is the number of elements in it. The* ***order*** *of an element* $g \in G$ *is the order of the smallest subgroup of* G *containing* g.

Definitions 3.36. *An element* $g \in G$ *is a* ***generator*** *if the smallest subgroup of* G *containing* g *is* G *itself. A group* G *is* ***cyclic*** *if it has a generator.*

Definitions 3.37. *The* ***center*** *of a group,* $Z(G)$ *is the set of all elements that commutes with every element in* G.

Definitions 3.38. *The* ***centralizer*** *of an element* g*,* $C(g)$ *is the set of all elements that commute with* g.

Properties of Center

1. The center $Z(G)$ of a group G is a normal subgroup of G. The centralizer of g, $C(g)$ is a subgroup of G.
2. $Z(G) \leq C(g) \leq C(g^k)$.
3. $C(g) = C(g^k) \iff \gcd(k, n) = 1$ where $o(g) = n$.
4. $Z(S_n)$ is trivial for $n \geq 3$.
5. $Z(D_n)$ is trivial when n is odd.
6. $Z(A_n)$ is trivial for $n \geq 4$.
7. $Z(M_n(F)) = \{aI : a \in F\}$.
8. $Z(GL(n, F)) = \{aI : a \in F,\ a \neq 0\}$.
9. $Z(SL(n, F)) = \{aI : a \in F,\ a^n = 1\}$.
10. $Z(Q_8) = \{1, -1\} \cong \mathbb{Z}_2$.
11. Center of a direct product is the direct product of centers.
12. Center of a simple group is either trivial(nonabelian) or the whole group(abelian).
13. Grün‘s Lemma : If G is perfect, then $Z(G/Z(G))$ is trivial.

Important Notions

Properties of Groups

1. $o(a) = o(a^{-1})$

   Proof. $a^n = e \iff (a^{-1})^n a^n = (a^{-1})^n \iff e = (a^{-1})^n$ □

2. $o(xax^{-1}) = o(a) = o(x^{-1}ax)$

   Proof. $(xax^{-1})^n = e \iff xa^nx^{-1} = e \iff a^n = x^{-1}x \iff a^n = e$ □

3. $o(ab) = o(ba)$

   Proof. $(ab)^n = e \iff b(ab)^n b^{-1} = e \iff (ba)^n = e$ □

4. $\forall a \in G,\ a^{-1} = a \implies G$ is abelian.

   Proof. $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$ □

5. $\forall a, b \in G,\ (ab)^2 = a^2b^2 \iff G$ is abelian.

   Proof. $abab = aabb \iff bab = abb \iff ba = ab$ □

6. $\forall a, b \in G,\ (ab)^{-1} = a^{-1}b^{-1} \iff G$ is abelian

   Proof. $(ab)^{-1} = a^{-1}b^{-1} \iff (ab)^{-1} = (ba)^{-1} \iff ab = ba$ □

7. If $\forall a, b \in G,\ a^3b^3 = (ab)^3$, then every commutator is of order 3.

   Proof. $a^3b^3 = (ab)^3 \implies a^2b^2 = (ba)^2$.
   $$(aba^{-1}b^{-1})^2 = (a^{-1}b^{-1})^2(ab)^2 = b^{-2}(a^{-2}b^2)a^2 = b^{-2}(ba^{-1})^2a^2 = b^{-1}a^{-1}ba$$
   $(aba^{-1}b^{-1})^4 = (b^{-1}a^{-1}ba)^2 = aba^{-1}b^{-1} \implies (aba^{-1}b^{-1})^3 = e$ □

8. $a^n = 1,\ aba^{-1} = b^2 \implies b^{2^n-1} = e$.

   Proof. $(aba^{-1})^2 = ab^2a^{-1} = b^4 \implies a^2ba^{-2} = b^4 \implies a^nba^{-n} = b^{2^n}$. □

9. Let a, b be elements of fintie order, then ab is not necessarily of finite order.

10. If x commutes with y, then

    x commutes with y^{-1}, since $y^{-1}(xy)y^{-1} = y^{-1}(yx)y^{-1}$
    x^{-1} commutes with y, since $x^{-1}(xy)x^{-1} = x^{-1}(yx)x^{-1}$.
    x^{-1} commutes with y^{-1}, since $(xy)^{-1} = (yx)^{-1}$.

11. Group G has precisely one element g of order two, then g commutes with every element of G.

    Proof. Let $g \in G$ such that $o(g) = 2$.
    $\forall x \in G,\ o(xgx^{-1}) = o(g) = 2 \implies xgx^{-1} = g \implies xg = gx$ □

Subgroups

1. Subgroup Test : $a^{-1}b \in H,\ \forall a, b \in H \implies H \leq G$.
2. Finite Subgroup Test : H is a subgroup of a finite group if $*$ is closed in H.
3. Group G has a element of order n iff G has a `cyclic` subgroup of order n.
4. Let G be an `abelian` group. The set $\{g \in G : g^p = e\}$ is a subgroup of G. However, it is not true for nonabelian groups. $\{g \in D_4 : g^2 = e\}$ is not a subgroup of D_4.
5. Let G be an `abelian` group of order n. If $d|n$, then G has a subgroup of order d. If d is square-free, then G has an element of order d.
6. Every cyclic group of order n has $\phi(n)$ elements of order n. Suppose G has n_m elements of order m, then G has $n_m/\phi(m)$ cyclic subgroups of order m.

   If a finite abelian group G has 24 elements of order 6, then G has $24/\phi(6) = 12$ subgroups of order 6 as abelian group of order 6 are cyclic.
7. The dihedral group D_n has $\phi(d)$ elements of order d for every divisor d of n, except $d = 2$. There are either n or $n + 1$ elements of order 2 depending on the parity of n. The number of subgroup of $D_n = \tau(n) + \sigma(n)$.
8. $H, K \leq G \implies H \cap K \leq G$. And $H \cup K \subset HK \leq G$.

   $|HK| = |H||K|/|H \cap K|$.

   $m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$ where $k = lcm(m, n)$.

   $m\mathbb{Z} + n\mathbb{Z} = k\mathbb{Z}$ where $k = \gcd(m, n)$.

Strange Groups

1. Smallest non-abelian group is S_3. Smallest non-cyclic group is the Klein 4-group, $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Smallest non-abelian simple group is A_5. Thus, A_5 is the smallest perfect group.
2. $D_p, D_4, Q_8, A_4, \ldots$ are non-abelian groups with every proper subgroup abelian.
3. $\mathbb{C}^*$ is a multiplicative group with identity 1. Unit circle is a subgroup of $\mathbb{C}^*$. Unit circle has a unique cyclic subgroup for any order. The nth roots of unity is the cyclic subgroup of unit circle with order n.
4. $\mathbb{Q}/\mathbb{Z}$ is torsion group which has a unique cyclic subgroup of any finite order. And every proper subgroup of $\mathbb{Q}/\mathbb{Z}$ is finite and cyclic.
5. $\left\langle \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \neq 0 \right\}, \times \right\rangle$ is a group with identity $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$.
6. $\left\langle \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \neq 0 \right\}, \times \right\rangle$ is a group with identity $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.
7. $\langle \mathbb{Q}^+, a * b = \frac{ab}{5}, \times \rangle$ is a group with idenity 5.
8. $\langle \{5, 15, 20, 25, 30, 35\}, \times_{40} \rangle$ is a group with identity 25.

9. The multiplicative group $\mathbb{Z}_n^\times = \{m \in \mathbb{Z}_n : \gcd(m,n) = 1\}$.
   If it is cyclic, then it has $\phi(\phi(n))$ generators.

10. Convergent sequences under addition is a group.

11. Group of rigid motions(rotations) of the cube is a group of order $\binom{8}{1}\binom{3}{1} = 24$ under permutation multiplication. This group is isomorphic to S_4.

Group Representations

1. The function $\phi : G \to S_G,\ \phi(x) = \lambda_x,\ \lambda_x(g) = xg$ is the **left regular representation** of G.

2. Let G be a finite group with a generating set S. The **Cayley digraph** of G has elements of G as its vertices and generators from S as its arcs.
   The Cayley digraph for an abelian graph is symmetric.

3. A **permutation matrix** is obtained by reordering rows of an identity matrix.
   The permutation matrices $P_{n\times n}$ under matrix multiplication forms a group which is isomorphic to S_n. By Cayley's theorem, every group G is isomorphic to a group of permutation matrices where left regular representation corresponds to left multiplication.

4. The **set theoretic group representation** using generators and their relations.
   The dihedral group with generators $y = R_{2\pi/n}$, rotation by $2\pi/n$ radians and $x = \mu$, reflection (about the line through the center and a fixed vertex) of a regular n-gon.

$$D_n = \{x^i y^j : x^2 = y^n = 1, (xy)^2 = 1\}$$

   The symmetric group with generators $x = (1,2)$ and $y = (1,2,\dots,n)$.

$$S_n = \{x^i y^j : x^2 = y^n = 1, (yx)^{n-1} = 1\}$$

   The alternating group with the set of all three cycles of the form $x_j = (1,2,j)$ as generating set S.

$$A_n = \left\{\prod_{j=3}^{n} x_j^{n_j} : x_j^3 = 1,\ (x_i x_j)^2 = 1\right\}$$

Counter Examples

1. $\langle \mathbb{R}^*, *\rangle$ where $a * b = a/b$ is not associative.

2. $\langle \mathbb{C}, *\rangle$ where $a * b = |ab|$ has no identity element.

3. $\langle C[0,1] - \{0\}, \times\rangle$ is a not closed. There exists a pair of functions with product 0.

4. Let G be a group and $\mathscr{P}(G)$ be the power set of G. Define $A * B = \{ab : a \in A,\ b \in B\}$. Then $\langle \mathscr{P}(G), *\rangle$ is a monoid with identity $\{e\}$. The units are the left cosets of the trivial subgroup.

5. $\langle GL(n,F), +\rangle$ is not closed as $I_n + (-I_n) \notin GL(n,F)$.

Group Homomorphisms

1. $\phi : \mathbb{Z} \to \mathbb{Z}$ where $\phi(n) = 2n$ with $\ker(\phi) = 0$ and $\phi[\mathbb{Z}] = 2\mathbb{Z}$.

2. $\phi : \mathbb{Q} \to \mathbb{Q}$ where $\phi(x) = 2x$ with $\ker(\phi) = 0$ and $\phi[\mathbb{Q}] = \mathbb{Q}$.

3. $\phi : \mathbb{R} \to \langle \mathbb{R}^+, \times \rangle$ where $\phi(x) = 0.5^x$ with $\ker(\phi) = 0$ and $\phi[\mathbb{R}] = \mathbb{R}^+$.

4. $\phi : \mathbb{Z} \to \langle \mathbb{Z}, * \rangle$ where $m * n = m + n - 1$ is a group with $\ker(\phi) = 0$ and $\phi[\mathbb{Z}] = \mathbb{Z}$. (hint : $\phi(n) = n + 1,\ \phi(0) = 1,\ x^{-1} = -x - 2$)

5. $\phi : \mathbb{Q} \to \langle \mathbb{Q}, * \rangle$ where $x * y = x + y + 1$ is a group with $\ker(\phi) = 0$ and $\phi[\mathbb{Q}] = \mathbb{Q}$. (hint : $\phi(x) = 3x - 1,\ \phi(0) = -1,\ x^{-1} = -x - 2$)

6. $\phi : \mathbb{Q}^* \to \langle \mathbb{Q} - \{-1\}, * \rangle$ where $x * y = \frac{(x+1)(y+1)}{3} - 1$ is a group with $\ker(\phi) = 1$ and $\phi[\mathbb{Q}^*] = \mathbb{Q} - \{-1\}$. (hint : $\phi(x) = 3x - 1,\ \phi(1) = 2,\ x^{-1} = \frac{8-x}{x+1}$)

Cyclic Groups

1. Every cyclic group is abelian.

   Proof. $G = \langle g \rangle \implies \forall a, b \in G,\ ab = g^n g^m = g^m g^n = ba.$ □

2. Subgroup of cyclic group is cyclic. Let G be a cyclic group of order n. The order of the subgroup generated by g^m is $n/\gcd(n,m)$. For each divisor d of n, there exists unique cyclic subgroup of order n/d.

   The multiplicative group $\mathbb{Z}_{25}^{\times} \cong \mathbb{Z}_{20}$ has generator 3. We have $\gcd(20,5) = \gcd(20,15)$. Clearly, $3^5 \cong 18 \pmod{25}$ and $3^{15} \cong 7 \pmod{25}$. Thus, $\langle 7 \rangle \cong \langle 18 \rangle \cong \mathbb{Z}_4$.

3. Every proper subgroup of the Klein 4-group, $V \cong \mathbb{Z}_2 \times \mathbb{Z}$ is cyclic. However, V is not cyclic.

4. For any natural number n, there exists a cyclic group of order n. Two cyclic group of same order are isomorphic.

   Proof. The finite group $\langle \mathbb{Z}_n, +_n \rangle$ is cyclic with order $n \in \mathbb{N}$ and the infinite group $\mathbb{Z}$ is cyclic. Let G, H be cyclic groups of the same order with generators g, h respectively. Then $\phi : G \to H,\ g \xrightarrow{\phi} h$ is an isomorphism. □

5. An automorphism of a cyclic group is well defined by the image of a generator. Clearly, $\mathbb{Z}_{12}$ has $\phi(12) = 4$ generators and there are four distinct automorphisms.

6. For finite cyclic group $\mathbb{Z}_n$, a generator is an element with the same order as the group. However, this is not the case for inifinite cyclic group $\mathbb{Z}$.

$$o(g) = o(G) \not\Rightarrow \langle g \rangle \cong G$$

7. Every finite cyclic group, $\mathbb{Z}_n$ has $\phi(n)$ generators which are relatively prime to n. Clearly, $\mathbb{Z}_{20}$ has a non-prime generator, say 9.

8. The equation $x^m = e$ has m solutions in any finite cyclic group $\mathbb{Z}_n$ where $m|n$.

9. Let G be an abelian group and H, K are cyclic subgroups of G with generators h, k respectively. Then $\langle hk \rangle$ is a cyclic subgroup of order $lcm(r, s)$.

10. $\mathbb{Q}/\mathbb{Z}$ is not cyclic.
proof : $o(\frac{1}{2} + \mathbb{Z}) = 2$, where the infinite cyclic group $\mathbb{Z}$ has no such element.

11. $\mathbb{Q}^*$ is not cyclic.
proof : $o(-1) = 2$, where $\mathbb{Z}$ don't have any element of order two.

12. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are not cyclic.
proof : If $\mathbb{Q}$ is cyclic, then $\mathbb{Q}/\mathbb{Z}$ is a cyclic quotient group. But $\mathbb{Q}/\mathbb{Z}$ is not.

13. The subgroup generated by nth primite root of unity is a cyclic subgroup of $\mathbb{C}^*$ isomorphic to $\mathbb{Z}_n$. Clearly, $\left\langle (1+i)/\sqrt{2} \right\rangle \cong \mathbb{Z}_8$.

14. The subgroup generated by any complex number which is a non-root of unity is a cyclic subgroup of $\mathbb{C}^*$ isomorphic to $\mathbb{Z}$. Clearly $\langle 1+i \rangle \cong \mathbb{Z}$.

Number Groups

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, n\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}_c, \mathbb{R}_c, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{Z}_n^\times$ are groups with a suitable arithmetic operators from $\{+, \times, +_c, \times_c, +_n, \times_n\}$.

2. Any nontrivial subgroup of $\mathbb{Q}$ is an infinite cyclic group.

3. $\langle \mathbb{R} - \{-1\}, * \rangle$ where $a * b = a + b + ab$ is a group with identity 0 and $o(-2) = 2$.

4. The cyclic group, $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} = \{g^n : n \in \mathbb{N}\}$. $\mathbb{Z}_n$ has $\phi(d)$ elements of order d for every divisor d of n.
$$a^{-1}b \in Z_n \iff \gcd(a, n)|b$$

5. Group $\mathbb{Z}_n^\times$ is the multiplicative group of natural numbers less than n that are relatively prime to n. Thus $|\mathbb{Z}_n^\times| = \phi(n)$. Clearly, $\mathbb{Z}_n^\times$ are abelian.

Linear Groups

1. $M_{m\times n}(F)$ is the additive group of all matrices of order $m \times n$ with entries from the field F. When $m = n$, we may write $M_n(F)$.

2. General Linear Group, $GL(n, F)$ is the multiplicative group of all invertible matrices of order n with entries from field F.

3. Special Linear Group, $SL(n, F)$ is the multiplicative group of all matrices of order n and determinant 1 with entries from field F.

3.2.2 Permutations, Cosets & Direct Products

Definitions 3.39. *The **symmetric group** S_n is the set of all permutation on a set $\{1, 2, \dots, n\}$ together with the function composition operation.*

The cycle $f : (1, 2, 3) \in S_5$ maps $1 \to 2 \to 3 \to 1$ and fixes $4, 5$. And cycle $g : (1, 2, 5) \in S_5$ maps $1 \to 2 \to 5 \to 1$ and fixes $3, 4$. For example $f(g(1)) = f(2) = 3$, and $f(g(3)) = f(3) = 5$.. Thus by function composition $f \circ g : (1, 2, 3)(1, 2, 5) = (1, 3)(2, 5)$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$$

Theorem 3.40 (Cayley)**.** *Every group is isomorphic to a subgroup of a symmetric group.*

Proof. The function $\phi : G \to S_G$ defined by $\phi(x) = \lambda_x$ where $g \stackrel{\lambda_x}{\to} xg$ is an homomorphism. □

Definitions 3.41. *Let σ be a bijection/permutation on a set A. The **orbits** of the permutation σ are the equivalent classes of the relation*

$$a \sim_\sigma b \iff \exists n \in \mathbb{N},\ a = \sigma^n(b)$$

Definitions 3.42. *A permutation σ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle σ is the number of elements in its largest orbit.*

The multiplication of disjoint cycles is commutative.

Theorem 3.43. *Every permutation of a finite set has a unique cycle decomposition.*

Proof. construct cycles corresponding to each orbit under the permutation □

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 2 & 4 & 1 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 5 \\ 3 & 5 & 2 & 1 \end{pmatrix} \begin{pmatrix} 4 \\ 4 \end{pmatrix} \begin{pmatrix} 6 & 7 \\ 7 & 6 \end{pmatrix}$$

In short, we may write $(1, 3, 2, 5)(6, 7)$ ignoring those which are left fixed by the permutation. And $(1, 3, 2, 5)(6, 7) = (1, 5)(1, 2)(1, 3)(6, 7)$ is an even permutation.

Definitions 3.44. *The alternating group A_n is the subgroup of all even permutations in the symmetric group S_n.*

Definitions 3.45. *Let H be a subgroup of group G. The **left coset**, gH of H containing $g \in G$ is the set of all element of the form gh where $h \in H$. The **right coset** Hg of H containing $g \in G$ is the set of all element of the form hg where $h \in H$.*

Theorem 3.46 (Lagrange)**.** *The order of a subgroup H of a finite group G divides the order of G.*

Proof. The left cosets of H in G are disjoint and covers G. Thus $|H|$ must divide $|G|$. □

Definitions 3.47. ***Index** of H in G, $(G : H)$ is the number of left cosets of H in G.*

Theorem 3.48. *The number right cosets of H in G is same as the number of left cosets of H in G.*

Proof. $aH = bH \iff ah_1 = bh_2 \iff (ah_1)^{-1} = (bh_2)^{-1} \iff h_1^{-1}a^{-1} = h_2^{-1}b^{-1} \iff Ha^{-1} = Hb^{-1}$. Thus, $aH \xrightarrow{\phi} Ha^{-1}$ is bijective. □

Theorem 3.49. *Let $K \leq H \leq G$. Then $(G : K) = (G : H)(H : K)$.*

Definitions 3.50. *Let G, H be two groups. The* ***direct product*** *$G \times H$ is defined as the group $\langle G \times H, *\rangle$ where $* : (G \times H) \times (G \times H) \to (G \times H)$ such that $(g_1, h_1) * (g_2, h_2) = (g_1g_2, h_1h_2)$.*

Theorem 3.51. $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{n\times m} \iff \gcd(m, n) = 1$.

Proof. $(1, 1) \in Z_n \times Z_m$ has order mn. Thus, $Z_n \times Z_m$ is cyclic. □

Suppose $\gcd(m, n) = 1$. The canonical isomorphism $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ is given by

$$a \pmod{mn} \xrightarrow{\phi} (a \pmod{m}, a \pmod{n})$$

Theorem 3.52. *Let $(a_1, \ldots, a_n) \in G_1 \times \ldots G_n$ and $o(a_i) = r_i$.*
Then $o((a_1, \ldots, a_n)) = lcm(r_1, \ldots, r_n)$.

Theorem 3.53. *Let G be a finitely generated group. Then $G \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ where the number of $\mathbb{Z}$ is its Betti number.*

Theorem 3.54. *Let G be a finite abelian group with order n. If $m|n$, then G has a subgroup H of order m.*

Proof. We have, $n = \prod P_j^{r_j}$ and $m = \prod P_j^{s_j}$ where $0 \leq s_j \leq r_j$. From the structure of finitely generated abelian group G, we may derive the structure of its subgroup H of order m by diminishing the powers of primes as required. □

Important Notions

Definitions 3.55. *Let $H, K \leq G$. The equivalent classes of the equivalence relation $aRb \iff a = hbk,\ h \in H,\ k \in K$ are the* ***double cosets*** *of G.*

Definitions 3.56. *A group G is* ***decomposable*** *if $G \cong H \times K$ where H, K are proper, nontrivial subgroups of G. Otherwise, G is indecomposable.*

Finite indecomposable groups are $\mathbb{Z}_p$.

Consequences of Lagrange‘s theorem

1. By Lagrange‘s theorem, every group of prime order is cyclic.

2. If $|G| = pq$, then every proper subgroup of G is cyclic.

3. The quotient group $\mathbb{Z}_n / \langle g\rangle \cong \mathbb{Z}_{\frac{n}{m}}$ where $o(g) = m$.

Finite Abelian Groups

1. Finite abelian groups are finitely generated.
2. Number of abelian groups of order $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ is $\prod_k B(r_k)$.
3. Order of an abelian group G is square free, then G is cyclic.
4. Order of an element in a cyclic group
   Let $m \in \mathbb{Z}_n$. Then it has order
   $$o(m) = \frac{n}{\gcd(n,m)}$$
5. Order of an element in a product of Cyclic groups
   Let $(g_1, g_2, \dots, g_k) \in G_1 \times G_2 \times \dots \times G_k$. Then
   $$o(g_1, g_2, \dots, g_k) = lcm(o(g_1), o(g_2), \dots, o(g_k))$$
6. Enumerating the elements of same order in a finite abelian group.

   Enumerate elements of order 4 in $\mathbb{Z}_{12} \times \mathbb{Z}_{10}$?

   Let $(g,h) \in \mathbb{Z}_{12} \times \mathbb{Z}_{10}$ has order $o(g,h) = 4 \iff o(g) = 4,\ o(h) = 1$ or 2. Clearly, an element $k \in \mathbb{Z}_{12}$ is of order 4 iff $\frac{12}{\gcd(12,k)} = 4$. For $\gcd(12,k) = 3$, we have $k = 3$ or 9. For $\gcd(10,k) = 5$, we have $k = 5$. For $\gcd(10,k) = 10$, we have $k = 0$. Thus, the elements are $(3,0), (3,5), (9,0)$ and $(9,5)$. In other words, $\phi(4)\phi(2) + \phi(4)\phi(1) = 4$ elements of order four in $\mathbb{Z}_{12} \times \mathbb{Z}_{10}$.

   Enumerate elements of order 9 in $\mathbb{Z}_{12} \times \mathbb{Z}_{18} \times \mathbb{Z}_{27}$?

   There are $\phi(1), \phi(3), \phi(9)$ elements of order $1, 3, 9$ respectively(if any[3]). There are $1+2+6$ elements of order either $1, 3$ or 9 in both $\mathbb{Z}_{18}$ and $\mathbb{Z}_{27}$. There are $3 \times 9 \times 9$ elements out of which precisely $3 \times 3 \times 3$ of them are of order either 1 or 3. Thus, there are 216 elements of order 9.
7. Let $g \in \mathbb{Z}_n$ with $o(g) = m$ where $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ and $m = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ such that $0 \le s_j \le r_j$. Then $g = (g_1, g_2, \dots, g_k) \in \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \dots \mathbb{Z}_{p_k^{r_k}}$ with $o(g_j) = s_j$. For example, $o(15) = 12$ in $\mathbb{Z}_{36}$. The isomorphism $\phi : \mathbb{Z}_{36} \to \mathbb{Z}_4 \times \mathbb{Z}_9$ where $\phi(a) = (a \pmod 4, a \pmod 9)$. Clearly $15 \to (3,6)$. And $o(3) = 4$ and $o(6) = 3$.
8. Let $(g,h) \in \mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}}$ with $o(g,h) = p^{r_3}$ where $r_1 \ge r_2$. Then, $(\mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}}) / \langle (g,h) \rangle \cong$

   $\mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2 - r_3}}$ when $o(h) = o(g,h)$.

   $\mathbb{Z}_{p^{r_1 - r_3}} \times \mathbb{Z}_{p^{r_2}}$ when $o(h) < o(g,h)$.

   For example, $(\mathbb{Z}_8 \times \mathbb{Z}_4) / \langle (2,1) \rangle \cong \mathbb{Z}_8$ and $(\mathbb{Z}_8 \times \mathbb{Z}_4) / \langle (2,2) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.
9. Order of an element in S_n Let $\sigma \in S_n$ be a permutation with structure $1^{n_1} 2^{n_2} \dots r^{n_r}$. Then $o(\sigma) = lcm(\{k : n_k \ge 1\})$. Order of an element in A_n can be found using the same rule as above. Parity of permutation is the parity of $\sum (j-1) n_j$.
   Maximum order of an element in A_{10} is $3 \times 7 = 21$. And maximum order of an element in S_{10} is $2 \times 3 \times 5 = 30$ where $2^1 3^1 5^1$ is an odd permutation, $\because (1+2+4)$.

   A_7 has a element of order 6 with structure $2^2 3^1$, since $2+2=4$ is even parity.

[3] We know that, $\mathbb{Z}_{12}$ don't have any element of order 9.

10. Maximal abelian subgroup of S_n
S_{10} has maximal abelian subgroup of order 36 which is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_6$ and is generated by $\{(1,2),(3,4,5),(6,7),(8,9,10)\}$. It is abelian as the cycles are disjoint.

11. Direct product form of the multiplicative group of units, $\mathbb{Z}_n^\times$
$\mathbb{Z}_{10}^\times = \{1,3,7,9\}$ and $\phi(10) = \phi(2)\phi(5) = 4$. And $\mathbb{Z}_{10}^\times \cong \mathbb{Z}_4$ as $\langle 3 \rangle = \mathbb{Z}_{10}^\times$.

$$\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times \iff \gcd(m,n) = 1$$

$$\forall n \in \mathbb{N},\ \mathbb{Z}_{2^{n+2}}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$$

$$\forall p > 2,\ \forall n \in \mathbb{N},\ \mathbb{Z}_{p^n}^\times \cong \mathbb{Z}_{p^n - p^{n-1}}$$

Thus, $\mathbb{Z}_4^\times = \mathbb{Z}_2,\ \mathbb{Z}_8^\times = \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbb{Z}_{16}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_4,\ \ldots$ Clearly, $\phi(40) = \phi(8)\phi(5)$ and $\mathbb{Z}_{40}^\times \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_4$. And $\mathbb{Z}_{1000}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{100}$.

Structure of a Permutation

Definitions 3.57. *The **structure** of a permuation $\sigma \in S_n$ is $1^{n_1}2^{n_2}\ldots r^{n_r}$ where n_j is the number of cycles of length j.*

The number of permutations of the structure $1^{n_1}2^{n_2}\ldots r^{n_r}$ in S_n is

$$\frac{n!}{\prod_{k=1}^{r} n_k!\ k^{n_k}}$$

There are $\frac{10!}{3!\ 2!\ 1!\ 2^2\ 3}$ elements of the structure $1^3 2^2 3^1$.

Definitions 3.58. *The set of all elements of an abelian group G of finite order forms a normal subgroup called **torsion** subgroup of G.*

Definitions 3.59. *A **torsion free** group has only one element of finite order in it.*

Torsion and Torsion Free Groups

1. The torsion subgroup of $\mathbb{C}^*$ is the set of all roots of unity. The cyclic group generated by z where $|z| \neq 1$ is a torsion free subgroup of $\mathbb{C}^*$. The cyclic group generated by $e^{2\pi i x},\ x \in \mathbb{R} - \mathbb{Q}$ is a torsion free subgroup of the unit circle.

2. Any finite group is a torsion group. The subgroups and quotient groups of any torsion group is also a torsion group.

3. Every infinite group has a nontrivial torsion free subgroup. The subgroups of a torsion free group is always torsion free.

4. Let T be the torsion subgroup of an abelian group G. Then the quotient group G/T is torsion free.

The group $\mathbb{Q}^*$ has only two elements of finite order, say 1 and -1. The torsion subgroup of $\mathbb{Q}^* \cong \mathbb{Z}_2$. Thus $\mathbb{Q}^+ \cong \mathbb{Q}^*/\{1,-1\}$ is torsion free. Similarly, $\mathbb{R}^+$ is torsion free.

5. Suppose normal subgroup H contains the torsion subgroup of a group G. Then G/H is torsion free. Thus $\mathbb{C}^*/U \cong \mathbb{R}^+$ is torsion free.

6. There is no bound for the order of elements in this torsion group.

   $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}_1$ is a torsion group and $o(p/q + \mathbb{Z}) = q$.

   $\mathbb{Q}_\pi$ is torsion free.

3.2.3 Homomorphisms & Factor Groups

Definitions 3.60. *Let $\phi : G \to G'$ be a homomorphism. Then $\phi[G]$ is the range of ϕ.*

Compositions of group homomorphisms is again a group homomorphism.

Definitions 3.61. *Let $\phi : G \to G'$ be a group homomorphism. Then, the **kernel** of ϕ,*

$$\ker(\phi) = \phi^{-1}[e'] = \{g \in G : \phi(g) = e'\}$$

Properties of Homomorphisms Let $\phi : G \to G'$.

1. $\phi(e) = e'$.

2. $\phi(a^{-1}) = \phi(a)^{-1}$.

3. $H \leq G \implies \phi[H] \leq \phi[G] \leq G'$.

4. $K' \leq \phi[G] \implies \phi^{-1}[K'] \leq G$.

5. Let $N = \ker(\phi)$. Then $\phi^{-1}(\phi(a)) = aN$. And ϕ is injective iff N is trivial.

6. Let $\phi : G \to G'$ with $\ker(\phi) = N$.

   Rule for Kernel : $G/N \cong \phi[G] \implies o(G)/o(N) = o(\phi[G]) \implies o(G)|o(N)o(G')$

   Rule for Generators : $(gh)^n = e \implies \phi(gh^n) = e' \implies o(\phi(g)\phi(h))|o(G)$,

7. $T : \mathbb{Z}_8 \to \mathbb{Z}_{12}$ where $T(x) = 4x$ is not a homomorphism (by Rule of generators).

   Number of surjection homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ is $\phi(m)$ where $m|n$.

8. Given G, G' and normal subgroup N. The homomorphism $\phi : G \to G'$ with $\ker(\phi) = N$ exists only if $o(G)/o(N) < o(G')$. (Rule of Kernel)
   proof : $\nexists \phi : S_4 \to S_3$ with $\ker(\phi) = \mathbb{Z}_2$ as $S_4/\mathbb{Z}_2$ is too big to be a subgroup of S_3.

9. If $\phi : G \to G'$ is surjective and G is cyclic(abelian), then G' is cyclic(abelian).

10. If $\phi : G \to G'$ is injective, then $G \cong \phi[G] \leq G'$.

    There does not exists an injective homomorphism, $\phi : S_n \to \mathbb{C}^*$ as $\phi : S_n \to \phi[S_n]$ where $\phi[S_n] \leq \mathbb{C}^a st$ is an isomorphism. However, subgroups of $\mathbb{C}^*$ is abelian.

11. $\phi : G \to G$ where $\phi(x) = x^m$ is an automorphism iff $\gcd(m, n) = 1$.

Definitions 3.62. *Let $H \leq G$. H is **normal** in G if $gH = Hg$ for every element $g \in G$.*

Definitions 3.63. *Let $H \leq G$. H is a **characteristic subgroup** if $\phi[H] \subset H$ for every automorphism ϕ on G.*

1. Intersection of normal subgroups are again normal.
2. For every subset S of a group G, there exists a minimal normal subgroup of G containing S.
3. Subgroup of index two is normal (if exists).
4. Subgroups of the center $Z(G)$ are normal.
   $H = \{I_3, 2I_3, 4I_3\} \trianglelefteq GL(3, F_{11})$ as $H \leq Z(GL(3, F_{11})) = \{aI_3 : a \in F_{11}^*\}$
5. $\forall k|n, \ \{m \in \mathbb{Z}_n^\times : m \cong 1 \pmod{k}\} \trianglelefteq \mathbb{Z}_n^\times$
   $\{1, 7, 13, 19\} \trianglelefteq \mathbb{Z}_{30}^\times$ where $k = 6$.
6. Characteristic subgroups are normal.
7. Let $\phi : G \to G'$ be a homomorphism. Then $\ker(\phi) = N$ is normal subgroup of G.
8. Let $\phi : G \to G'$. If $N \trianglelefteq G$, then $\phi[N] \trianglelefteq \phi[G]$. If $N' \trianglelefteq G'$, then $\phi^{-1}(N') \trianglelefteq G$.
9. Intermediate subgroup condition : Let $K \leq H \leq G$ and $K \trianglelefteq G$ then $K \trianglelefteq H$.
10. Let $K \leq H \leq G$. If H, K are normal subgroups of G, then $G/H \trianglelefteq G/K$.
11. $K \trianglelefteq H \trianglelefteq G \not\Rightarrow \ K \trianglelefteq G$

    Proof. $D_5 \trianglelefteq D_{10} \trianglelefteq D_{20}$. But $D_5 \ntrianglelefteq D_{20}$. □

12. Let $H \leq G$ and $N \trianglelefteq G$. Then $HN = \{hn : h \in H, n \in N\}$ is the smallest subgroup of G containing both N and H.
13. Let H, K be normal subgroups of G, then HK is normal in G.
14. Let H, K be normal subgroups of G such that $H \cap K = \{e\}$. Then $hk = kh$.
15. $Z(G) \trianglelefteq G$ and $Z(G/Z(G)) \trianglelefteq G/Z(G)$.
16. Let $\gamma : G \to G/Z(G), \ \gamma(g) = gZ(G)$. Then $\gamma^{-1}(Z(G/Z(G))) \trianglelefteq G$.

Definitions 3.64. *Let N be a normal subgroup of G. The* ***quotient group*** *G/N is the set of all left cosets of N with binary operation $g_1N * g_2N = (g_1g_2)N$.*

Theorem 3.65. *Let $N \trianglelefteq G$. $\gamma : G \to G/N$ where $\gamma(g) = gN$ is canonical homomorphism with $\ker(\gamma) = N$.*

Theorem 3.66. *Let $\phi : G \to G'$ be a homomorphism with $\ker(\phi) = N$. Then there exists a canonical homomorphism $\gamma : G \to G/N$ where $\gamma(g) = gN$ such that $G/N \cong \phi[G]$.*

Theorem 3.67. *Let G, G' be groups with normal subgroups H, H'. Let $\phi : G \to G'$ be a homomorphism with $\phi[H] \leq H'$. Then there exists an induced canonical homomorphism $\phi_* : G/H \to G'/H'$ where $\phi_*(gH) = \phi(g)H'$.*

Definitions 3.68. *The map $x \to gxg^{-1}$ is the* ***inner automorphism*** *of G by g.*

1. The set of all inner automorphisms on G is a group, say $Inn(G)$.

2. $Inn(G) \cong G/Z(G)$.

3. $Inn(G) \trianglelefteq Aut(G)$.

4. Let G be a finite cyclic group of order n. Then $Aut(G) \cong \mathbb{Z}_n^{\times}$.

   $Aut(V) \cong S_3$.

   $Aut(Q_8) \cong S_4$.

   $Aut(F \times F \times \ldots F) \cong GL(n, F)$.

   $Aut(A_n) \cong Aut(S_n) \cong S_n,\ n \neq 6,\ n > 2$

   $Aut(A_6) \cong Aut(S_6) \cong S_6 \rtimes Z_2$

5. Outer automorphism group is the quotient group, $Out(G) \cong Aut(G)/Inn(G)$.

6. A group G is complete if both center $Z(G)$ and outer automorphism group $Out(G)$ are trivial.

   S_n is complete, $n \geq 3,\ n \neq 6$.

   If G is a nonabelian simple group, then $Aut(G)$ is complete.

7. $G \cong Aut(G) \not\Rightarrow G$ is complete.

   Proof. $D_4 \cong Aut(D_4)$, D_4 is not complete. □

Definitions 3.69. *The* ***conjugacy class*** *of x, $Cl(x) = \{gxg^{-1} : g \in G\}$.*

Definitions 3.70. *Let $H, K \leq G$. The subgroups are conjugates if $\exists g \in G,\ K = i_g[H]$.*

1. Conjugacy is an equivalence relation on the set of all subgroups of G.

2. Normal subgroups are alone in their conjugacy equivalence class.

Definitions 3.71. *A group G is simple if it does not have a proper, nontrivial, normal subgroup.*

1. M is a maximal normal subgroup of G iff G/M is simple.

2. Abelian simple groups are cyclic groups of prime order, say $\mathbb{Z}_p$.

3. $G/Z(G)$ is cyclic iff G is abelian.

   Proof. Let $gZ(G)$ be a generator of $G/Z(G)$. Let $g_1, g_2 \in G$. Then $g_1 = g^{n_1}z_1$ and $g_2 = g^{n_2}z_2$ where $z_1, z_2 \in Z(G)$. Thus, $g_1g_2 = g_2g_1$. Therefore, G is abelian. If G is abelian, then $Z(G) \cong G$ and $G/Z(G)$ is trivial, thus cyclic. □

Definitions 3.72. *An element $g \in G$ is a* ***commutator*** *if $g = aba^{-1}b^{-1}$ for some $a, b \in G$.*

1. The set of all commutators in a group G is a subgroup of G, say **commutator subgroup** C.

2. Commutator subgroup C is the smallest normal subgroup of G such that G/C is abelian.

3. Let $N \trianglelefteq G$. G/N is abelian iff $C \leq N$.

4. Commutator subgroup of a simple group is either trivial(abelian) or the whole group(nonabelian).

5. Commutator subgroup of S_n is A_n.

Definitions 3.73. *A group is* ***perfect*** *if the commutator subgroup is the whole group.*

1. Any nonabelian, simple group is perfect.

2. Direct product of nonabelian simple groups in perfect but not simple.

3. $SL(2, F_5)$ is a perfect group which is not simple.

Definitions 3.74. *An* ***action*** *of group G on a set X is a function $* : G \times X \to X$ where*

1. $\forall x \in X,\ ex = x$

2. $\forall x \in X,\ \forall g_1, g_2 \in G,\ (g_1 g_2)x = g_1(g_2 x)$

The set X is G-set if G acts on X. Let $S \subset G$ such that $\forall s \in S,\ Gs \subset S$. Then S is a sub G-set.

Theorem 3.75. *Let X be a G-set. Then $\phi : G \to S_X$ where $\phi(g) = \sigma_g,\ \sigma_g(x) = gx$ is the group action induced homomorphism.*

1. ϕ is the permutation representation of G induced by the group action of G on X.

2. Group action is **faithful** if $e \in G$ is the only element that fixes every $x \in X$.

   For a faithful group action, the kernel of the induced homomorphism is trivial.

3. Group action is **transitive** if $\forall x_1, x_2 \in X,\ \exists g \in G,\ gx_1 = x_2$.

4. Every group G is a G-set where the action is both faithful and transitive.

5. Let $H \leq G$.

   Conjugation is an action of G on H, say $(g, h) \to ghg^{-1}$.

   Left multiplication is an action of G on H, say $(g, h) \to gh$.

6. Let $H \leq G$ and L_H be the set of left cosets of H.

   L_H is a G-set under conjugation, say $(g, aH) \to g(aH)g^{-1}$.

7. Let $V(F)$ be a vector space. Then V is an F^*-set.

8. Disjoint union of G-sets is also a G-set.

9. G_x is the **isotropy subgroup** of G containing all elements that fix x.

10. X_g is the subset of X fixed by $g \in G$.

11. The relation $x_1 \sim_g x_2 \iff gx_1 = x_2$ is an equivalence relation on X.
12. The equivalence classes of the above relation, Gx is the **orbit** of x in a G-set X,
13. Orbit Stabiliser theorem : $|Gx| = (G : G_x)$
14. Burnside's Formula, $r|G| = \sum_{g \in G} |X_g|$

Important Notions

Group Homomorphisms

1. $\phi : S_n \to \mathbb{Z}_2$ where $\phi(\sigma) = 1$ if the σ is an odd permutation and $\phi(\sigma) = 2$ otherwise. Then $\ker(\phi) = A_n$.
2. Evaluation Homomorphism, $\phi_c : F \to \mathbb{R}$ where $\phi_c(f) = f(c)$ where F is the additive group of all functions $f : \mathbb{R} \to \mathbb{R}$.
3. $\phi : \mathbb{R}^n \to \mathbb{R}^m$ where $\phi(v) = Av,\ A \in M_{m\times n}(\mathbb{R})$.
4. The trace, $tr : M_n(\mathbb{R}) \to \mathbb{R}$.
5. The trace, $tr : M(n, F) \to F$. Then $\ker(tr)$ is $n^2 - 1$ dimensional over F.
6. Determinant $\det : GL(n, \mathbb{R}) \to \mathbb{R}^*$ where $\det(A) = |A|$ with $\ker(\det) = SL(n, \mathbb{R})$ and $\det[GL(n, \mathbb{R})] \cong \mathbb{R}^*$.
7. Determinant $\det : GL(n, F_q) \to F_q^*$ where $\det(A) = |A|$ with $\ker(\det) = SL(n, F_q)$ and $\det[GL(n, F_q)] \cong F_q^*$.

$$|GL(n, F_q)| = \prod_{r=0}^{n-1} (q^n - q^r)$$

$$|SL(n, F_q)| = \frac{|GL(n, F_q)|}{q - 1} \text{ since } GL(n, F_q)/SL(n, F_q) \cong F_q^*$$

8. $\phi : \mathbb{Z}_n^\times \to \mathbb{Z}_k^\times$ with $\ker(\phi) = \{m \in \mathbb{Z}_n^\times : m \cong 1 \pmod{k}\}$.
9. $\phi_r : \mathbb{Z} \to \mathbb{Z}$ where $\phi_r(n) = rn$. ϕ_0 is trivial, ϕ_1 is identity, ϕ_{-1} is surjective.
10. Projection map $\pi_i : \prod G_j \to G_i$ where $\pi_i(g_1, g_2, \ldots, g_n) = g_i$.
11. $\sigma : F \to \mathbb{R}$ where $\sigma(f) = \int_0^1 f(x)\, dx$ and F is the additive group of all continuous functions $f : [0, 1] \to \mathbb{R}$.
12. $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ where $\gamma(m) = r,\ m = qn + r,\ 0 \leq r < n$.
13. $\phi : \mathbb{C}^* \to \mathbb{R}^*$ where $\phi(z) = |z|$. Left cosets aN are circles of radius a about origin.
14. Let D be the set of all differentiable function. Define $\phi : D \to F$ where $\phi(f) = f'$. Left cosets fN are $f(x) + C$.
15. $\phi : \mathbb{Z} \to \mathbb{R}$ where $\phi(n) = n$.

16. $\phi : \mathbb{R} \to \mathbb{Z}$ where $\phi(x) = [x]$ with $\ker(\phi) = [0, 1)$.

17. $\phi : \mathbb{R}^* \to \mathbb{R}^*$ where $\phi(x) = |x|$ with $\ker(\phi) = \{1, -1\} \cong \mathbb{Z}_2$.

18. $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2$ where $\phi(n) \cong n \pmod 2$ with $\ker(\phi) = \{0, 2, 4\} \cong \mathbb{Z}_3$.

19. $\phi : \mathbb{R} \to \mathbb{R}^*$ where $\phi(x) = 2^x$ with $\ker(\phi) = \{0\}$.

20. Injection map, $\phi_i : G_i \to \prod G_j$ where $\phi_i(g) = (e_1, e_2, \ldots, ge_i, \ldots, e_n)$ with $\ker(\phi) = \{e_i\}$.

21. $\phi : G \to G$ where $\phi(g) = g^{-1}$ with $\ker(\phi) = \{e\}$.

22. $\phi : F \to F$ where $\phi(f) = f''$ where F is the set of all functions f having derivatives of all orders with $\ker(\phi) = \{ax + b : a, b \in \mathbb{R}\}$.

23. $\phi : F \to F$ where $\phi(f) = \int_0^4 f(x)\, dx$ where F is the set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$.

24. $\phi : F \to F$ where $\phi(f) = 3f$ with $\ker(\phi) = \{0\}$.

25. $\phi : F \to \mathbb{R}^*$ wherer $\phi(f) = \int_0^1 f(x)\, dx$ where F is the multiplicative group of continuous functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) \neq 0$.

26. $\phi : \mathbb{Z} \to \mathbb{Z}_7$ where $\phi(1) = 4$ with $\ker(\phi) = 7\mathbb{Z}$.

27. $\phi : \mathbb{Z} \to \mathbb{Z}_{10}$ where $\phi(1) = 6$ with $\ker(\phi) = 5\mathbb{Z}$.

28. $\phi : \mathbb{Z} \to S_8$ where $\phi(1) = (1, 4, 2, 6)(2, 5, 7)$ with $\ker(\phi) = 12\mathbb{Z}$.

29. $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20}$ where $\phi(1) = 8$ with $\ker(\phi) = \{0, 5\} \cong \mathbb{Z}_2$.

30. $\phi : \mathbb{Z}_{24} \to S_8$ where $\phi(1) = (1, 4, 6, 7)(2, 5)$ with $\ker(\phi) = \{0, 4, 8, 12, 16, 20\} \cong \mathbb{Z}_6$.

31. $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi(1, 0) = 3$, $\phi(0, 1) = -5$ with $\ker(\phi) = \langle(5, 3)\rangle \cong \mathbb{Z}$.

32. $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ where $\phi(1, 0) = (2, -3)$ and $\phi(0, 1) = (-1, 5)$ with $\ker(\phi) = \{(0, 0)\}$.

33. $\phi : \mathbb{Z} \times \mathbb{Z} \to S_{10}$ where $\phi(1, 0) = (3, 5)(2, 4)$ and $\phi(0, 1) = (1, 7)(6, 10, 8, 9)$ with $\ker(\phi) = \langle(2, 4)\rangle \cong \mathbb{Z}$.

34. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_5$ where $\phi(1) = 0$ with $\ker \phi = \mathbb{Z}_{12}$.

35. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_4$ where

    $\phi(1) = 0$ with $\ker(\phi) = \mathbb{Z}_{12}$

    $\phi(1) = 1$ with $\ker(\phi) = \{0, 4, 8\} \cong \mathbb{Z}_3$

    $\phi(1) = 2$ with $\ker(\phi) = \{0, 6\} \cong \mathbb{Z}_2$

    $\phi(1) = 3$ with $\ker(\phi) = \{0, 4, 8\} \cong \mathbb{Z}_3$

36. $\phi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_5$ where

    $\phi(1,0) = (0,0),\ \phi(0,1) = (0,0)$ with $\ker(\phi) = \mathbb{Z}_2 \times \mathbb{Z}_4$

    $\phi(1,0) = (1,0),\ \phi(0,1) = (0,0)$ with $\ker(\phi) = \{0\} \times \mathbb{Z}_4$

    $\phi(1,0) = (0,0),\ \phi(0,1) = (1,0)$ with $\ker(\phi) = \mathbb{Z}_2 \times \{0,2\} \cong V$

    $\phi(1,0) = (1,0),\ \phi(0,1) = (1,0)$ with $\ker(\phi) = \{0\} \times \{0,2\}$

37. $\phi : \mathbb{Z}_3 \to \mathbb{Z}$ where $\phi(1) = 0$

38. $\phi : \mathbb{Z}_3 \to S_3$ where

    $\phi(1) = ()$ with $\ker(\phi) = \mathbb{Z}_3$

    $\phi(1) = (1,2,3)$ with $\ker(\phi) = \{0\}$

    $\phi(1) = (1,3,2)$ with $\ker(\phi) = \{0\}$

39. $\phi : \mathbb{Z} \to S_3$ where $\phi(1) = ()$ with $\ker(\phi) = \mathbb{Z}$.

40. $\phi : \mathbb{Z} \times \mathbb{Z} \to 2\mathbb{Z}$ where $\phi(1,0) = 2s,\ \phi(0,1) = 2t$ with $\ker(\phi) = \{0\},\ s,t \neq 0$.

41. $\phi : 2\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ where $\phi(2) = (s,t)$ with $\ker(\phi) = \{0\},\ s,t \neq 0$.

42. $\phi : D_4 \to S_3$ where

    $\phi(R_{90}) = (),\ \phi(\mu) = ()$ with $\ker(\phi) = D_4$.

    $\phi(R_{90}) = (i,j),\ \phi(\mu) = ()$ with $\ker(\phi) = \{0, R_{180}, \mu, R_{180}\mu\}$.

    $\phi(R_{90}) = ()$ or $\phi(\mu) = (i,j)$ with $\ker(\phi) = \{0, R_{90}, R_{180}, R_{270}\}$.

    $\phi(R_{90}) = (i,j)$ or $\phi(\mu) = (i,j)$ with $\ker(\phi) = \{0, R_{90}\mu, R_{180}, R_{270}\mu\}$.

    $\phi : D_4 \to S_3,\ \ker(\phi) \ncong \mathbb{Z}_2$ since S_3 don't have a subgroup isomorphic to $D_4/\mathbb{Z}_2$

43. $\phi : S_3 \to S_4$ where

    $\phi(1,2) = (),\ \phi(1,2,3) = ()$ with $\ker(\phi) = S_3$.

    $\phi(1,2) = (i,j),\ \phi(1,2,3) = ()$ with $\ker(\phi) = \{(), (1,2,3), (1,3,2)\}$.

    $\phi(1,2) = (),\ \phi(1,2,3) = (i,j,k)$ with $\ker(\phi) = k\{(), (1,2)\}$.

    $\phi(1,2) = (i,j),\ \phi(1,2,3) = (i,j,k)$ with $\ker(\phi) = \{()\}$.

    $\phi(1,2) = (i,j)(k,l),\ \phi(1,2,3) = ()$ with $\ker(\phi) = \{(), (1,2,3), (1,3,2)\}$.

44. $\phi : S_4 \to S_3$ where

    $\phi(1,2) = (),\ \phi(1,2,3,4) = ()$ with $\ker(\phi) = S_4$.

    $\phi(1,2) = (i,j),\ \phi(1,2,3,4) = (i,j)$ with $\ker(\phi) = A_4$.

    $\phi(1,2) = (i,j),\ \phi(1,2,3,4) = (i,k)$ is surjective with
    $\ker(\phi) = \{(), (1,3)(2,4), (1,2)(3,4), (1,4)(2,3)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$.

Counter Examples

1. $\phi : \mathbb{Z}_9 \to \mathbb{Z}_2$ where $\phi(n) \cong n \pmod 2$. But, $\phi(2+8) \neq \phi(2) + \phi(8)$.
2. $\phi : M_n(\mathbb{R}) \to \mathbb{R}$ where $\phi(A) = \det(A)$. However, $\det(A+B) \neq \det(A) + \det(B)$.
3. $\phi : GL(n, \mathbb{R}) \to \mathbb{R}^*$ where $\phi(A) = tr(A)$. However, $tr(AB) \neq tr(A)tr(B)$.
4. $\phi : S_3 \to S_4$ where $\phi(1,2) = (1,2)$, $\phi(1,2,3) = (1,3,4)$ is not a homomorphism. Let $\sigma = (1,2)(1,2,3) = (2,3)$, $\phi(\sigma) = \phi(1,2)\phi(1,2,3) = (1,3,4,2)$ and $\phi(\sigma^2) \neq ()$.
5. $\phi : S_3 \to S_4$ where $\phi(1,2) = (1,2)(3,4)$, $\phi(1,2,3) = (1,2,3)$ is not as well. Let $\sigma = (1,2)(1,2,3) = (2,3)$, $\phi(\sigma) = \phi(1,2)\phi(1,2,3) = (2,4,3)$ and $\phi(\sigma^2) \neq ()$.
6. $\phi(1,2) = (i,j)$, $\phi(1,2,3,4) = ()$. Let $\sigma = (2,3,4) = (1,2)(1,2,3,4)$. Then $\phi(\sigma) = (i,j)$ and $\phi(\sigma^3) \neq ()$.
7. $\phi(1,2) = ()$, $\phi(1,2,3,4) = (1,2)$. Let $\sigma = (1,2)(1,2,3,4) = (2,3,4)$. $\phi(\sigma) = (1,2)$ and $\phi(\sigma^3) \neq ()$.

Special Homomorphisms

1. There are two homomorphisms of $\mathbb{Z}$ onto $\mathbb{Z}$. $\phi_1(n) = n$ and $\phi_2(n) = -n$.
2. There are countably many homomorphisms of $\mathbb{Z}$ into $\mathbb{Z}$. $\phi_r(n) = rn$, $r \in \mathbb{Z}$.
3. There is a unique homomorphisms of $\mathbb{Z}$ into $\mathbb{Z}_2$. $\phi(n) \cong n \pmod 2$.
4. $\phi_g : G \to G$ where $\phi_g(x) = gx$ is a homomorphism only when $g = e$.
5. $\phi_g : G \to G$ where $\phi_g(x) = gxg^{-1}$ is a homomorphism with $\ker(\phi_g) = \{e\}$.
6. There exists exactly 24 surjective homomorphisms from S_4 onto S_3. However, the $\ker(\phi) = \mathbb{Z}_2 \times \mathbb{Z}_2$ as it is the only normal subgroup of S_4 with order 4.
7. The field $\left\langle \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}, +, \times \right\rangle \cong \mathbb{C}$ where $\phi\left(\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \right) = a + ib$.

Quotient Groups

1. $\mathbb{R}/n\mathbb{R} \cong \{e\}$ where $n\mathbb{R} = \{nr : r \in \mathbb{R}\}$.
2. $S_n/A_n \cong \mathbb{Z}_2$, $n > 1$.
3. $A_4/V = \{[V],\ (1,2)[V],\ (1,2,3,4)[V]\} \cong \mathbb{Z}_3$.
4. $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,1)\rangle \cong \mathbb{Z}_4$.
5. $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,2)\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.
6. $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(2,3)\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_3$.
7. $D_n/\mathbb{Z}_n \cong \mathbb{Z}_2$, $n > 2$. And $D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$.
8. $\mathbb{Z}_n^\times/N \cong \mathbb{Z}_k^\times$ where $N = \{m \in \mathbb{Z}_n^\times : m \cong 1 \pmod k\}$.

9. Factor groups of cyclic groups are cyclic. $\mathbb{Z}_n/\mathbb{Z}_d \cong \mathbb{Z}_{n/d}$, $d|n$.

10. $F/K \leq F$ where F is the additive group of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ and K is the subgroup of all constant functions.

11. $F^*/K^* \leq F^*$ where F^* is the multiplicative group of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) \neq 0$ and K^* is the subgroup of all nonzero constant functions.

Maximal Normal Subgroups

1. S_n : A_n, $n > 5$

   S_4 : A_4, $\mathbb{Z}_2 \times \mathbb{Z}_2$

2. A_4 : $\mathbb{Z}_2 \times \mathbb{Z}_2$

   A_n is simple, $n > 4$.

3. D_n : $D_{n/2}$, $\mathbb{Z}_n$, D_d where $d|n$, $n > 2$.

   D_4 is the only dihedral group in which $\mathbb{Z}_2 \times \mathbb{Z}_2$ is normal. (index 2)

Order of Quotient Groups

1. $\mathbb{Z}_6/\langle 3\rangle$. We have $|H| = o(3) = 6/\gcd(6,3) = 2$ and $|G/H| = |G|/|H| = 6/2 = 3$

2. $(\mathbb{Z}_4\times\mathbb{Z}_{12})/(\langle 2\rangle\times\langle 2\rangle)$. We have, $o(2) = 4/\gcd(4,2) = 2$ and $o(2) = 12/\gcd(12,2) = 6$. And $|G|/|H| = 48/12 = 4$.

3. $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(2,1)\rangle$. We have, $o(2,1) = lcm(o(2), o(1)) = lcm(2,2) = 2$. And $|G/H| = 8/2 = 4$.

4. $(\mathbb{Z}_3 \times \mathbb{Z}_5)/\{0\} \times \mathbb{Z}_5$. Clearly, $|G/H| = 15/5 = 3$.

5. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1,1)\rangle$. We have, $o(1,1) = lcm(o(1), o(1)) = lcm(2,4) = 4$. And $|G/H| = 8/4 = 2$.

6. $(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle(4,3)\rangle$. We have $o(4,3) = lcm(o(4), o(3)) = lcm(3,6) = 6$. And $|G/H| = 12 \times 18/6 = 36$.

7. $(\mathbb{Z}_2 \times S_3)/\langle(1,\rho_1)\rangle$ where $\rho_1 = (1,2,3)$. We have $o(1,\rho_1) = lcm(o(1), o(\rho_1)) = lcm(2,3) = 6$. And $|G/H| = 12/6 = 2$.

8. $(\mathbb{Z}_{11} \times \mathbb{Z}_{15})/\langle(1,1)\rangle$. Clearly $o(1,1) = 11 \times 15$. And $|G/G| = 1$.

Order of an element in the quotient group

1. $5 + \langle 4\rangle \in \mathbb{Z}_{12}/\langle 4\rangle$. $4 \times 5 + \langle 4\rangle = 0 + \langle 4\rangle$.

2. $26 + \langle 12\rangle \in \mathbb{Z}_{60}/\langle 12\rangle$. $6 \times (2 + 24) + \langle 12\rangle = 0 + \langle 12\rangle$.

3. $(2,1) + \langle(1,1)\rangle \in (\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1,1)\rangle$. $3 \times [(1,0) + (1,1) + \langle(1,1)\rangle] = (0,0) + \langle(1,1)\rangle$.

4. $(3,1) + \langle(1,1)\rangle \in (\mathbb{Z}_4 \times \mathbb{Z}_4)/\langle(1,1)\rangle$. $2 \times [(2,0) + (1,1) + \langle(1,1)\rangle = (0,0) + \langle(1,1)\rangle$.

5. $(3,3) + \langle(1,2)\rangle \in (\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle$. $8 \times [(2,1) + (1,2) + \langle(1,2)\rangle] = (0,0) + \langle(1,2)\rangle$.

6. $(2,0) + \langle(4,4)\rangle \in (\mathbb{Z}_6 \times \mathbb{Z}_8)/\langle(4,4)\rangle$. $3 \times [(2,0) + \langle(4,4)\rangle] = (0,0) + \langle(4,4)\rangle$.

Conjugate Subgroups

1. $i_{\rho_1}[H]$ where $H = \{\rho_0, \mu_1\}$ and $\mu_1 = (2, 3)$.
   We have, $i_{\rho_1}(\mu) = (1, 2, 3)(2, 3)(1, 3, 2) = (1, 3) = \mu_2$. Thus, $i_{\rho_1}[H] = \{\rho_0, \mu_u\}$.

Group G characterised by $G/Z(G)$

1. If G is non-abelian, finite group then $|Z(G)| \leq \frac{1}{4}|G|$. Otherwise $G/Z(G)$ is a group of order $1, 2$ or 3. And groups of order $1, 2, 3$ are cyclic.

2. If G is non-abelian, then $Z(G)$ is not a maximal subgroup of G.

   Proof. Suppose $Z(G)$ is a maximal subgroup of G. Then $G/Z(G)$ has no nontrivial subgroups. That is, $G/Z(G)$ is of prime order and thus cyclic which is not possible as G is non-abelian. □

3. For $A_5, S_3, \ldots$, the group $G/Z(G)$ is non-abelian.

Group Actions

1.

Definitions 3.76. *Let G be a group. The dual group of G, $\hat{G}$ is the abelian group of all homomorphisms $\phi : G \to \mathbb{C}^*$.*

$\widehat{A \times B} \cong \hat{A} \times \hat{B}$

3.2.4 Advanced Group Theory

Isomorphism Theorems

1. $\forall \phi : G \to G',\ \exists \gamma_N : G \to G/N,\ \phi = \mu\gamma$ where $N = \ker(\phi)$ and $\phi[G] \xrightarrow{\mu} G/N$.

2. Let $H \leq G$ and $N \trianglelefteq G$. Then $(HN)/N \cong H/(H \cap N)$.

   $|HN| = |H||N|/|H \cap N|$.

   If $H \cap N = \{e\}$, then $|HN| = |H||N|$.

3. Let $K \leq H \leq G$ and H, K are normal subgroups of G. Then $G/H \cong (G/K)/(H/K)$.

Definitions 3.77. *A **subnormal series** of a group G is a finite sequence $\{H_i\}_{i=0}^n$ such that $H_i \trianglelefteq H_{i+1},\ H_0 = \{e\}$ and $H_n = G$.*

Definitions 3.78. *A **normal series** of a group G is a finite sequence $\{H_i\}_{i=0}^n$ such that $H_i \trianglelefteq G,\ H_0 = \{e\}$ and $H_n = G$.*

Definitions 3.79. *A subnormal(normal) series of a group G is a **composition(principal) series** of group G if every quotient group H_{i+1}/H_i is simple.*

Definitions 3.80. *A composition series of a group G is **solvable** if every quotient group H_{i+1}/H_i is abelian.*

Definitions 3.81. *The ascending central series of the group G is $\{e\} \leq Z(G) \leq Z_1(G) \leq Z_2(G) \ldots$ where $Z_1(G) = \gamma^{-1}(Z(G/Z(G)))$, $Z_i(G) = \gamma_1^{-1}(Z(G/Z_1(G))) \ldots$ and $\gamma : G \to G/Z(G)$, $\gamma(g) = gZ(G)$ and $\gamma_1 : G \to G/Z_1(G)$, $\gamma_1(g) = gZ_1(G), \ldots$.*

1. Zassenhaus Lemma (Butterfly Lemma) : Let $H^* \trianglelefteq H$ and $K^* \trianglelefteq K$. Then

   $H^*(H \cap K^*) \trianglelefteq H^*(H \cap K)$,

   $K^*(H^* \cap K) \trianglelefteq K^*(H \cap K)$,

   $(H^* \cap K)(H \cap K^*) \trianglelefteq (H \cap K)$, and

   $$H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K) \cong (H \cap K)/(H^* \cap K)(H \cap K^*)$$

2. Schreier Theorem : Any two subnormal series of a group G have isomorphic refinements.

3. Jordan-Hölder Theorem : Any two composition(principal) series of a group G are isomorphic.

4. Every normal subgroup N of G belongs to some composition series of the group G.

5. Finite product of solvable groups is solvable.

Definitions 3.82. *If every element of G has order a power of prime p, then G is a **p-group**. Let $H \leq G$ and H is a p-group, then H is a **p-subgroup** of G.*

Definitions 3.83. *Let G be a group and $H \leq G$. The **normaliser** $N[H]$ of H is the largest subgroup of G such that $H \trianglelefteq N[H]$.*

Definitions 3.84. *Maximal p-subgroup is a **Sylow p-subgroup** of G.*

Definitions 3.85. *The **class equation** of G is $|G| = c + n_{c+1} + \cdots + n_r$ where n_j is the length of jth orbit in the partition of G under conjugation and $c = |Z(G)|$ is the number of element that are alone in their conjugacy class.*

1. The set of all Sylow p-subgroups of G, $Syl_p(G)$ is a G-set with conjugation action.

2. Let X be a finite G-set and $|G| = p^n$. Then $|X| \cong |X_G| \pmod{p}$.

3. Cauchy's theorem : Let G be a finite group and p divides the order of G, then G has element g of order p.

4. Let H be a p-subgroup of a finite group G. Then $(N[H] : H) \cong (G : H) \pmod{p}$.

   If p divides the index of H in G, $(G : H)$, then $N[H] \neq H$.

   $N[H]$ is isomorphic to the group of all inner automorphisms G that map H onto itself.

5. The class equation of various groups,

   $G : n = n$, if G is abelian.

   $G : p^3 = p + p + \cdots + p$, if G non-abelian.

   $S_3 : 6 = 1 + 2 + 3$.

$S_4 : 24 = 1 + 3 + 8 + 6 + 6.$

$S_5 : 120 = 1 + 10 + 15 + 20 + 20 + 24 + 30.$

$A_4 : 12 = 1 + 3 + 4 + 4.$

$A_5 : 60 = 1 + 20 + 12 + 12 + 15.$

$D_4 : 8 = 2 + 2 + 2 + 2.$

$D_5 : 10 = 1 + 2 + 2 + 5.$

$D_6 : 12 = 2 + 2 + 2 + 3 + 3.$

$Q_8 : 8 = 2 + 2 + 2 + 2.$

6. Distinct groups can have the same class equation.

Sylow Theorems

1. If $|G| = p^n m$, then $\{H_i\}_{i=0}^n$ is a subnormal series such that $|H_i| = p^i$ and $H_i \leq G$.
2. Let P_1, P_2 be Sylow p-subgroups of a finite group G. Then P_1, P_2 are conjugate subgroups of G.
3. Let G be a finite group and p divides the order of G. Then the number of Sylow p-subgroups, $n_p \cong 1 \pmod p$ and $n_p | o(G)$.

Applications of Sylow theorems

1. Wilson‘s theorem : $(p-1)! \cong -1 \pmod p$.
   S_p has $(p-2)!$ Sylow p-subgroups. Clearly, $(p-2)! \cong 1 \pmod p$ and theorem holds.
2. Nonabelian group of order pq is isomorphic to $\mathbb{Z}_q \rtimes \mathbb{Z}_p$. It has q Sylow-p subgroups.
3. Sylow p-subgroups are conjugates. Suppose $|G| = 36$ with four Sylow 3-subgroups (of order 9). Then either they are isomorphic to $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Important Notions

HN subgroups

1. $G = \mathbb{Z}_{24},\ H = \langle 4 \rangle,\ N = \langle 6 \rangle.\ HN = \langle 2 \rangle.$
2. $G = \mathbb{Z}_{36},\ H = \langle 6 \rangle,\ N = \langle 9 \rangle.\ HN = \langle 3 \rangle.$

Third Isomorphism Theorem

1. $G = \mathbb{Z}_{24},\ H = \langle 4 \rangle,\ N = \langle 8 \rangle.\ G/K = \{\langle 8 \rangle, 1 + \langle 8 \rangle, \ldots, 7 + \langle 8 \rangle\}.$
   $H/K = \{\langle 8 \rangle, 4 + \langle 8 \rangle\}.\ G/H = \{\langle 4 \rangle, 1 + \langle 4 \rangle, 2 + \langle 4 \rangle, 3 + \langle 4 \rangle\}.$

Non-abelian Groups There are a few classes of non-abelian groups which has every proper subgroup abelian : 1) every nonabelian group of order pq where $p|q$, and 2) two non-abelian groups of order p^3.

Important Notions

Semidirect Product

Definitions 3.86. *Let $\phi : H \to Aut(N)$ be a group homomorphism where N, H are two group. Then the* ***semidirect product*** *$N \rtimes H$ is defined as the group $\langle N \rtimes H, *\rangle$ where $* : (N \times H) \times (N \times H) \to (N \times H)$ such that $(n_1, h_1) * (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2)$.*

Let G be a group with nontrivial normal subgroups $N, H \leq G$ such that $N \cap H = \{1\}$ and $N \vee H = G$. Then $G/N \cong H$ and $G/H \cong N$. Thus $G \cong N \times H$.

We can extend the notion direct product as follows. Let G be a group with nontrivial subgroups N, H such that N is normal and $N \cap H = \{1\}$. Then $G \cong N \rtimes H$ except for $G \cong \mathbb{Z}_4$ and Q_8.

Definitions 3.87. *The* ***fundamental group*** *of a topological space is the group of equivalent classes under homotopy of the loops contained in the space.*

Semidirect Products

1. The dihedral group, $D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$.
2. No simple group G can be expressed as a semidirect/direct product.

   Simple groups are indecomposable.
3. The fundamental group of the Klein bottle is $\mathbb{Z} \rtimes \mathbb{Z}$.

The converse of Lagrange‘s theorem Finite group G not necessarity have subgroups for each divisor of its order. For example, the alternating group A_5 of order 12 does not have a subgroup of order 6.

Classification of Finite Groups

1. By Burnside‘s theorem, p-Groups have non-trivial center. And Q_8 is the smallest non-abelian p-group.
2. By Sylow first theorem, no group of prime power order is simple.
3. Every group of prime power order is solvable.
4. Every group G of order p is cyclic and $G \cong Z_p$. The number of generators is $\phi(n)$.
5. Every group G of order p^2 is abelian. There are two groups Z_{p^2} and $Z_p \times Z_p$.
6. There are exactly five groups of order p^3.

   Proof. Three abelian groups – $Z_{p^3}, Z_{p^2} \times Z_p,$ and $Z_p \times Z_p \times Z_p$ and two non-abelian groups – $(Z_p \times Z_p) \rtimes Z_p,$ and $Z_{p^2} \rtimes Z_p$ except for $p = 2$. For $p = 2$, $Z_4 \rtimes Z_2 \cong (Z_2 \times Z_2) \rtimes Z_2 \cong D_4$. However we have Q_8, which is another nonabelian group of order 8. □

7. Every non-abelian group G of order p^3 has center $Z(G)$ of order p.

   Proof. Since G is a p-group, G has nontrivial center. Suppose $|Z(G)| = p^2$, then $G/Z(G)$ is a cyclic group of order p. But G is non-abelian. □

8. Every non-abelian group G of order p^3 has $p^2 + p - 1$ distinct conjugacy classes.

9. Abelian group of order pq is cyclic. Non-abelian group of order pq exists and is isomorphic to $\mathbb{Z}_q \rtimes \mathbb{Z}_p$ provided $q \cong 1 \pmod p$.

10. Every non-abelian group G of order pq has trivial center.

    Proof. Suppose nonabelian group G has a nontrivial center of order p (wlog), then $G/Z(G)$ is a cyclic group of order q. But G is non-abelian. Thus $Z(G)$ is trivial. □

11. Every group of square free order is supersolvable. And thus solvable.

    Proof. Suppose $|G| = p_1p_2 \dots p_k$ where $p_1 > p_2 > \dots p_k$. Then there exists a normal series $G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_k \trianglelefteq G$ such that $|G_1| = p_1$, $|G_2| = p_1p_2$ and $|G_k| = p_1p_2 \dots p_k$. □

3.3 Ring Theory

3.3.1 Rings & Fields

1. Every finite PID is field.

3.3.2 Ideals & Factor Rings

3.3.3 Factorisation

Lemma 3.88 (Bézout). *Let $gcd(a, b) = d$. Then there exists integers x, y such that $ax + by = d$. And integers of the form $as + bt$ are exactly the multiples of d.*

The integers x, y are the Bézout coefficients for (a, b). Bézout coefficients are not unique. Bézout identity implies Euclid's lemma, and chinese remainder theorem.

Lemma 3.89 (Euclid). *Let p be a prime. If p divides ab, then p divides either a or b.*

Proof. By Bézout's identity or By induction using Euclidean algorithm. □

Theorem 3.90 (chinese remainder theorem).

Definitions 3.91 (Bézout Domain). *A Bézout Domain is an integral domain which satisfyies Bézout's identity.*

Definitions 3.92 (Gaussian Integers). *Gaussian integers, $\mathbb{Z}[i]$ are complex numbers of the form $a + ib$, $a, b \in \mathbb{Z}$.*

Let x, y are Gaussian integers. x divides y if there exists a Gaussian integer z such that $y = xz$. The Gaussian integers not divisible by any non-unit Gaussian integer is a Gaussian prime.

Properties

1. $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$
2. $\mathbb{Z}[i]$ is an integral domain.
3. $\mathbb{Z}[i]$ is a principal ideal domain (PID).
4. $\mathbb{Z}[i]$ i s a Unique factorisation domain (UFD).
5. $\mathbb{Z}[i]$ with norm $N(a+ib) = a^2 + b^2$ is a Euclidean Domain.
6. $\mathbb{Z}[i]$ is a Bézout Domain.
7. Every PID is a Bézout Domain.

Important Notions

1. Every PID is a UFD.
2. If D is a UFD, then $D[x]$ is a UFD.

Definitions 3.93 (Eisenstein Integers)**.** *Eisenstein Integers, $\mathbb{Z}[w]$ are complex numbers of the form $a + wb$, $a, b \in \mathbb{Z}$ and $w = e^{i2\pi/3}$.*

The units in $\mathbb{Z}[w]$ are $\pm 1, \pm w, \pm w^2$.

3.4 Fields

3.4.1 Extension Fields

Definitions 3.94. *There exists a unique* ***Galois field*** *$GF(p^n)$ of order p^n.*

Theorem 3.95 (Kronecker)**.** *Let F be a field and $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.*

Definitions 3.96. *A field E is an* ***extension field*** *of field F if F is containined in E.*

Definitions 3.97. *A field E is a* ***simple extension*** *of field F if there exists some $\alpha \in E$ such that E is the minimal extension field of F containing α.*

Definitions 3.98. *Let field E be an extension of field F. A number $\alpha \in E$ is* ***algebraic over*** *F if there exists $f(x) \in F[x]$ such that $f(\alpha) = 0$.*

Then α is **algebraic over the field** F**.** Otherwise α is **transcendental over the field** F. If $F = \mathbb{Q}$, then α is an **algebraic number**.

Definitions 3.99. *An extension E of a field F is* ***algebraic*** *if $E \cong F(\alpha)$ for some α algebraic over F.*

The field $\mathbb{Q}(\pi)$ is a simple, transcendental extension of $\mathbb{Q}$. And $\mathbb{Q}(i)$ is a simple, algebraic extension of $\mathbb{Q}$ as $f(x):\ x^2 + 1 \in \mathbb{Q}[x]$ and $f(i) = 0$.

Definitions 3.100. *Let field E be an n-dimensional vector space over field F. Then E is a* ***finite extension*** *of F. And $[E : F] = n$.*

Theorem 3.101 (Fundamental Theorem of Algebra)**.** *The field $\mathbb{C}$ is algebraically closed.*

Proof. Every non-constant polynomial has a linear factorisation. Let $f(z)$ be a non-constant polynomial which has no zero in $\mathbb{C}$. Then $1/f(z)$ is entire. Clearly $f(z) \to \infty$ as $z \to \infty$. Thus, $1/f(z) \to 0$ as $z \to \infty$. Therefore, f is bounded. However, by Liouville's theorem, the bounded, entire function $1/f(z)$ is constant. □

Field $\mathbb{C}$ does not have any algebraic extensions. However, the field of all rational functions $\mathbb{C}(x)$ is a transcendental extension of $\mathbb{C}$.

Important Notions

The binary algebra, $\langle \mathbb{Z}_n, +_n, \times_n \rangle$ is a commutative ring with unity.

Theorem 3.102. *$\langle \mathbb{Z}_n, +_n, \times_n \rangle$ is a field iff n is a prime.*

Proof. A number $a \in \mathbb{Z}_n$ is not a zero divisor(and has an inverse) iff $\gcd(a, n) = 1$. □

Simple Extensions of $\mathbb{Q}$ Let α be an algebraic number. Then there exists a polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. From $f(x)$, we may obtain a monic polynomial $p(x) \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$. By division algorithm, such monic irreducible polynomials are unique. Thus, we may refer $p(x) = irr(\alpha, \mathbb{Q})$. By Kronecker's theorem, field $\mathbb{Q}$ has an algebraic extension $\mathbb{Q}(\alpha)$.

Definitions 3.103 (cyclotomic field)**.** *The nth **cyclotomic field** is $\mathbb{Q}(\alpha)$ where α is a primitive nth root of unity.*

Definitions 3.104 (cyclotomic polynomial)**.** *The nth **cyclotomic polynomial** $\Phi_n(x)$ is the monic irreducible polynomial with primitive nth roots of unity as its zeroes.*

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - \zeta_k)$$

Definitions 3.105. *A number α is **constructible** if you can draw a line of α length in a finite number of steps using a straightedge and a compass (given a line of unit length).*

1. The nth cyclotomic polynomial has degree $\phi(n)$.
2. The constructible numbers form a field.
3. A number α is constructible iff the degree of the monic, irreducible polynomial of α over $\mathbb{Q}$ is a power of the prime 2.
4. The constructible numbers field is an infinite extension of $\mathbb{Q}$.

The classical problems like trisecting an angle, squaring a circle and doubling a cube are thus impossible.

3.4.2 Automorphisms & Galois Theory

Part III

Calculus

Chapter 4

Ordinary Differential Equations

4.1 Basic Calculus

4.1.1 Differentiation

1. Linearity : $[f(x)+g(x)]' = f'(x) \pm g'(x)$ and $[cf(x)]' = cf'(x)$.
2. Product rule : $[f(x)g(x)]' = f(x)g'(x) + f'(x)g(x)$.
3. Quotient rule : $[f(x)/g(x)]' = [f'(x)g(x) - f(x)g'(x)]/g^2(x)$.
4. Chain rule : $[f(g(x)]' = f'(g(x))g'(x)$.
5. $[x^r]' = rx^{r-1}$ where $r \in \mathbb{R}$.
6. $[a^x]' = a^x \ln a$ where $a \in \mathbb{R}^+$.
7. $[\sin x]' = \cos x$, $[\cos x]' = -\sin x$, $[\tan x]' = \sec^2 x$, $[\csc x]' = -\csc x \cot x$, $[\sec x]' = \sec x \tan x$ and $[\cot x]' = -\csc^2 x$.
8. $[\sin^{-1} x]' = \frac{1}{\sqrt{1-x^2}}$, $[\tan^{-1} x]' = \frac{1}{1+x^2}$, and $[\sec^{-1} x]' = \frac{1}{x\sqrt{x^2-1}}$.
   Hint : $y = f^{-1}(x) \implies f(y) = x \implies f'(y) = 1$.

4.1.2 Integration

1. Linearity : $\int [f(x) \pm g(x)]\,dx = \int f(x)\,dx \pm \int g(x)\,dx$ and $\int cf(x)\,dx = c\int f(x)\,dx$.
2. Product rule : $\int [f(x)g(x)]\,dx = f(x)\int g(x)\,dx - \int f'(x)\left[\int g(x)\,dx\right]\,dx$.

$$\int fg\,dx = f\int g - f'\iint g + f''\iiint g + \cdots$$

3. $\int \tan x\,dx = -\log\cos x$ and $\int \cot x\,dx = \log\sin x$.
4. $\int \csc x\,dx = \log(\csc x - \cot x)$ and $\int \sec x\,dx = \log(\sec x + \tan x)$.

4.2 Ordinary Differential Equation

1. An equation involving derivatives with respect to an independent variable and involving dependent variable is called an **ordinary differential equation**(ODE).

2. The **order** and **degree** of an ODE is the order and degree of its highest derivative.

3. An ODE is **linear** if it does not contain product of dependent variable and its derivatives.

4. A **solution** of a differential equationis a relation between the dependent variable and the independent variable. Solution has the general form : $f(x, y) = 0$.

   A **general solution** is of the form $\sum c_j y_j(x)$ where c_js are arbitrary constants and the number of arbitrary constants is equal to the order of the differential equation.

   A **particular solution** is obtained from general solution by giving particular values to its arbitrary constants.

   A **singular solution** is a solution which cannot be obtained from a general solution by a choice of arbitrary constants.

5. There are two major type of problems :

   An **initial value problem** is a differential equation together with values of dependent variable and its derivatives for a particular value of independent variable.

   A **boundary value problem** is a differential equation together with functions of dependent variable and its derivatives at different values of independent variable.

4.2.1 Solving first order ordinary differential equations

1. Variable Separable : $f(x)dx = g(y)dy$
   $\int f(x)dx = \int g(y)dy$.

2. Homogeneous : $x^k f(y/x, y')$
   $y = vx \implies dy = vdx + xdv$. Then $g(x)dx = h(v)dv$.

3. Exact : $Mdx + Ndy = 0$ where $M_y = N_x$ and M, N, M_y, N_x are continuous.
   $\int M\ dx + \int N^\star\ dy = C$ where $N^\star$ is the part of $N(x, y)$ not containing x.

4. Almost Exact : $Mdx + Ndy = 0$ but $M_y \neq N_x$.
   Case 1 : $(M_y - N_x)/N = f(x)$, Case 2 : $(M_y - N_x)/-M = g(y)$ and
   Case 3 : $(M_y - N_x)/(N_y - M_x) = h(z)$ where $z = xy$. Suppose Case 1 is true,
   then $IF = e^{\int f(x)\ dx}$ and $\int M\ IF\ dx + \int (N\ IF)^\star\ dy = C$.

5. Inspection Method - Use known results to simply the ODE.

   $[y/x]' = (xdy - ydx)/x^2$.

   $[x/y]' = (ydx - y^2dx)/y^2$.

   $[y^2/x]' = (2xydy - y^2dx)/x^2$.

   $[\ln(xy)]' = (xdy + ydx)/xy$.

   $[xy]' = xdy + ydx$.

$[x^2 + y^2]' = 2(xdx + ydy).$
$[\tan^{-1}(x/y)]' = (ydx - xdy)/(x^2 + y^2).$
$[\sin^{-1}(x/y)]' = (ydx - xdy)/y\sqrt{y^2 - x^2}.$
$[\sec^{-1}(x/y)]' = (ydx - xdy)/\sqrt{x^2 - y^2}.$
$[\ln(x/y)]' = (ydx - xdy)/xy.$

6. Leibnitz's Method : $y' + P(x)y = Q(x)$.
   The solution is : $y\ IF = \int IF\ Q(x)\ dx$ where $IF = e^{\int P(x)\ dx}$.

7. Bernouli's Method : $y' + P(x)y = Q(x)y^n$ where $n \neq 0, 1$.
   The solution is : $y^{1-n}\ IF = \int IF\ Q(x)(1-n)\ dx$ where $IF = e^{\int P(x)(1-n)\ dx}$.[1]

Problems

1. Computing M from N in an exact differential equation
   Suppose $g(x, y)dx + (x + y)dy = 0$ is exact and $g(x, 0) = x^2$.
   Exact $\implies g_y = N_x = 1 \implies g(x, y) = y + f(x)$
   And $g(x, 0) = f(x) = x^2 \implies g(x, y) = x^2 + y$.

2. Set $S = \{\frac{2}{x+1} : x \in (-1, 1)\}$.
   $-1 < x < 1 \implies 0 < x + 1 < 2 \implies \infty > 1/(x + 1) > 1/2$
   $\implies \infty > 2/(x + 1) > 1 \implies S = (1, \infty) \implies S' = [1, \infty)$.

3. S is union of disjoint bounded intervals.
   S is compact only if each interval is closed. $\sup S \in S$ if right most interval is right closed and $\inf S \in S$ if left most interval is left closed. If S has more than one interval in it, then S being compact is a different story.

4. Let $A \subset \mathbb{R}$. Then $I(A)$ is an open set. Thus, either $I(A)$ is empty or uncountable.

4.2.2 Existence & Uniqueness

1. A function $f(x, y)$ such that $|f(x, y_1) - f(x, y_2)| \leq k|y_1 - y_2|$ is a **Lipschitz** function with Lipschitz constant k. If the function is differentiable, then condition reduces to the form $|\partial f/\partial y| \leq k$.

2. Peano's Theorem : Consider an initial value problem $y' = f(x, y),\ y(x_0) = y_0$. If $f(x, y)$ is continuous and is bounded, say $|f(x, y)| \leq M$, in the rectangle $|x - x_0| \leq h$ and $|y - y_0| \leq k$. Then there exists at least one solution ϕ such that $\frac{d\phi}{dx} = f(x, y)$ on the interval $|x - x_0| \leq \min\{h, k/M\}$.

3. Picard's Theorem : Consider an initial value problem $y' = f(x, y),\ y(x_0) = y_0$. If $f(x, y)$ is continous and is bounded in the rectangle $|x - x_0| \leq h$ and $|y - y_0| \leq k$ and $f(x, y)$ satisfies Lipschitz condition, then the there exists a unique solution.

4. Types of IVP,

   (a) No Solution. The general solution reduces to an contradictory statement with given initial values. Or Peano's theorem hypotheses donot hold.

[1] In an intermediate step, we replace y^{1-n} with u and solve using Leibnitz's method.

(b) Unique Solution. Unique particular solution is obtained. Or Picard's theorem hypotheses hold.

(c) Uncountably many solutions. Particular solutions together with zero function and other variants.

4.2.3 Solving First Order ODEs of Degree $n > 1$

1. Solutions are of the form (a) Cartesian Form (Equation containing x, y and constants.) (b) Parametric Form, $x = f_1(P, c)$ and $y = f_2(P, c)$. (c) $x = g(x, P)G(x, P, c)$ and $y = f(x, P)F(x, P, c)$.

2. General Form : $p_0P^n + p_1P^{n-1} + \cdots + p_{n-1}P + p_n = 0$ where $P = y'$ and p_k's are functions of x and y. If we can factorise it into linear factors, say $(P - f_1)(P - f_2)\cdots(P - f_n) = 0$. Then we can solve each one of those factor $P - f_k = 0$ into some $F_k(x, y, c_k) = 0$. And the general solution is $F_1(x, y, c)F_2(x, y, c)\cdots F_n(x, y, c) = 0$.

3. Solvable for x. That is, $x = f(y, P)$ where $P = dy/dx$.
   $x = f(y, P) \implies 1/P = F(y, P, dP/dy) \implies \psi(y, P, c) = 0 \implies y = g(P, c)$.

   (a) Case 1: $x = f(P) \implies 1/P = F(P, dP/dy) \implies y = g(P, c)$.

4. Solvable for y.
   $y = f(x, P) \implies P = F(x, P, dP/dx) \implies \psi(x, P, c) = 0 \implies x = g(P, c)$.

   (a) Case 1: $y = f(P) \implies P = F(P, dP/dx) \implies x = g(P, c)$.

   (b) Case 2: Lagrange's Equation : $y = xF(P) + f(P)$.
   $y = xF(P) + f(P) \implies P = \psi(x, y, P, dP/dx) \implies dx/dP + g(P)x = h(p)$.
   Solve Leibnitz Equation.

   (c) Case 3 : Clairut's Equation : $y = xP + f(P)$.
   $y = xc + f(c)$.

4.2.4 Orthogonal Trajectory

1. If a family of curves $f(x, y, c) = 0$ satisfies differential equation $F(x, y, P) = 0$. Then the differential equation of their orthogonal trajectory is $F(x, y, -1/P) = 0$.

4.2.5 Solving ordinary differential equations for a singular solution

Definitions 4.1. *If a family of curves $f(x, y, c) = 0$ represented by $F(x, y, P) = 0$ and it has an envelope. Then the envelope is the[2] singular solution of $F(x, y, P) = 0$.*

1. Method 1 : P discriminant.
   Let $f(x, y, P) = 0$. From $\frac{\partial f}{\partial P} = 0$ obtain a P-discriminant[3] relation, $F(x, y) = 0$. Then $F(x, y)$ or its factors satisfying $f(x, y, P) = 0$ are the singular solutions.

[2] It is possible to have multiple singular solutions ?

[3] relation not containing P

2. Method 2 : c-discriminant.
   Let $\phi(x, y, c) = 0$ be a solution for $f(x, y, P) = 0$. From $\frac{\partial\phi}{\partial c}$ obtain a c-discriminant relation $F(x, y) = 0$. Then $F(x, y)$ or its factors satisfying $f(x, y, P) = 0$ are the singular solutions.

3. Method 3 : Quadratic Relation in P.
   Let $AP^2 + BP + C = 0$. Then $F(x, y) = B^2 - 4AC$ is the respective P-discriminant relation. And $F(x, y)$ or its factors satisfying $f(x, y, P) = 0$ are the singular solutions.

4.2.6 Solving second order ordinary differential equaitons

1. Linear Differential Equations with Constant Coefficients

$$D^n y + a_1 D^{n-1} y + \cdots + a_n y = R(x) \tag{4.1}$$

   Solution is of the form : Complementary function + Particular Integral where Complementary function is the solution of the respective homogenous equation.

2. We may write $f(D)y = R(x)$ where $f(D) = D^n + a_1 D^{n-1} + \cdots + a_n$ is the respective auxiliary equation. Let $m_1, m_2, \ldots$ be solutions of the auxiliary equation. Then $e^{m_i x}$ is solution of the homogenous equation. If m_i is a root of multiplicity n then $x^k e^{m_i}$, $k = 0, 1, 2, \ldots, n-1$ are the respective solutions.

   (a) Case 1 : Real Distinct Roots.
   Let $m = m_1, m_2$. Then $y = c_1 e^{m_1} x + c_2 e^{m_2 x}$ is the complementary function.

   (b) Case 2 : Real, Multiple Roots.
   Let m be a real root of multiplicity 4. Then $y = (c_1 + c_2 x + c_3 x^2 + c_4 x^3)e^{mx}$ is the complementary function.

   (c) Case 3 : Complex, Conjugate Roots.
   Let $m = \alpha \pm i\beta$. Then $y = e^{\alpha x}(c_1 \cos\beta x + c_2 \sin\beta x)$ is the complementary function.

   (d) Case 4 : Complex, Conjugate, Multiple Roots.
   Let $\alpha \pm i\beta$ be conjugate roots of multiplicity 4. Then $y = e^{\alpha x}((c_1 + c_2 x + c_3 x^2 + c_4 x^3)\cos\beta x + (c_5 + c_6 x + c_7 x^2 + c_8 x^3)\sin\beta x)$ is the complementary function.

   (e) Case 5 : Conjugate Surds.
   Let $m = \alpha \pm \sqrt{\beta}$. Then $y = e^{\alpha x}(c_1 \cosh\beta x + c_2 \sinh\beta x)$ is the complementary function. [4]

3. Particular Integral y_p

   (a) Case 1 : $R(x) = e^{\alpha x}$.

$$y_p = \begin{cases} \frac{e^{\alpha x}}{f(\alpha)} & f(\alpha) \neq 0 \\ \frac{1}{\phi(\alpha)} \frac{x^r}{r!} e^{\alpha x} & f(\alpha) = 0 \end{cases}$$

[4] Why ?

(b) Case 2 : $R(x) = \sin x$.

$$y_p = \begin{cases} \frac{1}{f(D)} \sin \alpha x & f(D) \neq 0, D^2 = -\alpha^2 \\ \frac{x}{2} \int \sin \alpha x & f(D) = 0 \end{cases}$$

(c) Case 3 : $R(x) = x^m$.

$$y_p = \frac{1}{f(D)} x^m \text{ where } (1 - D)^{-n} = \sum_{r=0}^{\infty} \binom{-n}{r} D^r$$

(d) Case 4 : $R(x) = e^{\alpha x} v(x)$.

$$y_p = e^{\alpha x} \frac{1}{f(D + \alpha)} v(x)$$

4. Cauchy-Euler Equations

$$a_n x^n D^n y + a_{n-1} x^{n-1} D^{n-1} y + \cdots + a_1 x D y + a_0 y = R(x) \tag{4.2}$$

Put $x = e^t$. Then $t = \log x$, $xDy = Dy$, $x^2 D^2 y = D(D - 1)y, \ldots$. The Cauchy-Euler equation reduces to a linear differential equation with constant coefficient.

5. Legendre‘s Linear Differential Equation

$$a_n(\alpha x+\beta)^n D^n y + a_{n-1}(\alpha x+\beta)^{n-1} D^{n-1} y + \cdots + a_1(\alpha x+\beta) D y + a_0 y = R(x) \tag{4.3}$$

Put $\alpha x + \beta = e^t$. Then $t = \log(\alpha x + \beta)$, $(\alpha x + \beta)Dy = \alpha Dy$, $(\alpha x + \beta)^2 D^2 y = \alpha^2 D(D - 1)y, \ldots$. The Legendre‘s linear differential equation reduces to a linear differential equation with constant coefficient.

6. Finding general solution from a fundamental solution.