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, $x \in A$.

Definitions 1.1. ***Cardinality*** $|A|$ *is the number of elements of the set* A.

Definitions 1.2. *A set* B *is a* ***subset*** *of a set* A, $B \subset A$ *if* $x \in B \implies x \in A$.

Definitions 1.3. *The* ***power set*** $\mathcal{P}(A)$ *of a set* A *is the family of all subsets of* A.

Definitions 1.4. *Two sets* A, B *are* ***equal****,* $A = B$ *if* $A \subset B$ *and* $B \subset A$.

Definitions 1.5. *The* ***union*** *of two sets* A, B *is the set* $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

Definitions 1.6. *The* ***intersection*** *of two sets* A, B *is the set* $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

Definitions 1.7. *The* ***complement*** *of a set* A *with respect to a set* B *is the set* $A - B = \{x \in A : x \notin B\}$.

Definitions 1.8. *The* ***symmetric difference*** *of two sets* A, B *is the set* $A \Delta B = (A - B) \cup (B - A)$.

1.1.1 Relation

Definitions 1.9. *The cartesian* ***product*** *of* A *and* B, $A \times B = \{(a, b) : a \in A,\ b \in B\}$.

Definitions 1.10. *A* ***relation*** *from* A *to* B *is a subset of* $A \times B$. *And* $xRy \implies (x, y) \in R \subset A \times B$. *A relation on* A *is* $R \subset A \times A$.

Definitions 1.11. *A* ***reflexive*** *relation* R *on* A *satisfies* xRx, $\forall x \in A$.

Definitions 1.12. *A* ***symmetric*** *relation* R *on* A *satisfies* $xRy \iff yRx$.

Definitions 1.13. *An* ***antisymmetric*** *relation* R *on* A *satisfies* $(x, y) \in R \implies (y, x) \notin R$.

Definitions 1.14. *A* ***transitive*** *relation* R *on* A *satisfies* $xRy,\ yRz \implies xRz$, $\forall x, y, z \in A$.

Definitions 1.15. *An **equivalence** relation R on A is a reflexive, symmetric, and trasitive relation.*

Definitions 1.16. *Let $x \in A$. An **equivalence class** of a set A containining x is the subset $\hat{x} = \{y \in A : xRy\}$.*

Definitions 1.17. *A **partition** $\{\hat{x}, \hat{y}, \dots\}$ of A is a family of subsets $\hat{x}$ of A which satisfies*

1. $x \in \hat{x}, \ \forall x \in A$.
2. $\hat{x} \cap \hat{y} \iff \hat{x} = \hat{y}$.
3. $A = \cup\{\hat{x} : x \in A\}$.

Definitions 1.18. *A **total** relation R on A satisfies either xRy or yRx, $\forall x, y \in A$, $(x \neq y)$.*

Definitions 1.19. *A **function** from A to B is relation which has a unique element (a, b) for every $a \in A$.*

Definitions 1.20. *An **injection** $f : A \to B$ satisfies $f(x) = f(y) \implies x = y$.*

Definitions 1.21. *A **surjection** $f : A \to B$ satisfies $y = f(x), \ \forall y \in B$.*

Definitions 1.22. *A **bijection** $f : A \to B$ is both injective and surjective.*

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

Definitions 1.23. *A set A is **finite** if there exists a natural number N and a bijection $f : A \to \{1, 2, \dots, N\}$.*

A is finite if and only if there does not exists a bijection from A into any proper subset of A.

Definitions 1.24. *A set A is **countably infinite** if there exists a bijection $f : A \to \mathbb{N}$.*

1. 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 Sequence

Definitions 2.1. *Sequence x_n in a set X is a function $x : \mathbb{N} \to X$ where $x_n = x(n)$.*

Definitions 2.2. *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.*

2.1.1 Convergence

Definitions 2.3 (norm)**.** *A sequence x_n converges to x if there exists $N \in \mathbb{N}$ such that $\forall n > N, \|x_n - x\| < \varepsilon$.*

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n > N,\ \|x_n, x\| < \varepsilon \tag{2.1}$$

Remark (subsequence)**.** *A sequence x_n converges to x if and only if every subsequence has a convergent subsequence.*

2.1.2 Limit Point

Definitions 2.4. *x is a limit point of sequence x_n if x_n converges to x.*

Definitions 2.5. *x is a cluster point of sequence x_n, there exists a subsequence x_{n_k} converging to x.*

2.1.3 Cauchy Criterion

Definitions 2.6 (norm)**.** *A sequence x_n is Cauchy if there exists $N \in \mathbb{N}$ such that $\forall n, m > N,\ \|x_n - x_m\| < \varepsilon$.*

2.1.4 Complete Space

Definitions 2.7 (complete)**.** *A space is complete if every Cauchy sequence in it converges.*

Properties of Convergent Sequences

1. The limit of a convergent real sequence is unique.

2.
$$x_n \to x,\ y_n \to y \implies x_n \pm y_n \to x \pm y$$
$$x_n \to x,\ y_n \to y \implies x_n y_n \to xy$$
$$x_n \to x,\ y_n \to y,\ y_n \neq 0,\ y \neq 0 \implies x_n/y_n \to x/y$$

3.
$$x_n \to x,\ y_n \to y,\ x_n \leq y_n \implies x \leq y$$
$$\text{Squeeze}:\ x_n \leq y_n \leq z_n,\ x_n \to l,\ z_n \to l \implies y_n \to l$$

4.
$$|x_n| \to |x| \not\Longrightarrow x_n \to x$$
$$x_n y_n \to xy,\ x_n \to x \not\Longrightarrow y_n \to y$$

5. Every convergent sequence is absolute convergent.
$$x_n \to x \implies |x_n| \to |x|$$

6. Sequences converging to 0
$$|x_n| \to 0 \iff x_n \to 0$$

7. Continuity of $\surd$.
$$x_n \to x \implies \sqrt{x_n} \to \sqrt{x}, \quad (x_n > 0)$$

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
$$\lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n = e^x$$

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.
$$||a| - |b|| \leq |a - b|$$

2.1.5 Important Notions

1. If space X is T_2, then limit of convergent sequence in X is unique.
2. Derived Set $A' = \{x \in X : \forall N \in \mathcal{N}_x, N - \{x\} \cap A \neq \phi\}$.
$$\bar{A} = A \cup A'$$
3. Every function on $\mathbb{N}$ is continuous.

2.1.6 Techniques

1. Ratio
$$\lim_{n\to\infty} \frac{x_{n+1}}{x_n} = l$$
If $l < 1,\ x_n \to 0$ and $l > 1,\ x_n \to \infty$.
2. Root
$$\lim_{n\to\infty} (x_n)^{\frac{1}{n}} = l$$
If $l < 1,\ x_n \to 0$ and $l > 1,\ x_n \to \infty$.
3. Stolz Theorem
$$\lim_{n\to\infty} \frac{x_1 + x_2 + \cdots + x_n}{y_1 + y_2 + \cdots + y_n} = \lim_{n\to\infty} \frac{x_n - x_{n-1}}{y_n - y_{n-1}} \qquad (y_n \uparrow^{\infty})$$
4. Riemann Sum
$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{\infty} f(k/n) = \int_0^1 f(x)\ dx$$

2.2 Limit Superior/Inferior

Definitions 2.8.
$$\limsup_{n\to\infty} x_n = \inf_{n\geq 0} \sup_{m\geq n} x_n$$

Definitions 2.9.
$$\liminf_{n\to\infty} x_n = \sup_{n\geq 0} \inf_{m\geq n} x_n$$

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,* $x_n = (-1)^n(1 + \frac{1}{n})$.

2.2.1 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 2.10 (Stolz-Cesaro)**.**
$$\liminf_{n\to\infty} \frac{a_{n+1} - a_n}{b_{n+1} - b_n} \leq \liminf_{n\to\infty} \frac{a_n}{b_n} \leq \limsup_{n\to\infty} \frac{a_n}{b_n} \leq \limsup_{n\to\infty} \frac{a_{n+1} - a_n}{b_{n+1} - b_n}$$

2.3 Limit of a function

Definitions 2.11 (limit). *If* $f(x_n) \to L$ *as* $x_n \to a$*, then* $\lim_{x\to a} f(x) = L$.

Definitions 2.12 (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 2.13. *Limit is algebraic.*

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

$$\lim_{x\to a} cf(x) = c \lim_{x\to a} f(x) \tag{2.2}$$

$$\lim_{x\to a} f(x) \pm g(x) = \lim_{x\to a} f(x) \pm \lim_{x\to a} g(x) \tag{2.3}$$

$$\lim_{x\to a} f(x)g(x) = \lim_{x\to a} f(x) \ \lim_{x\to a} g(x) \tag{2.4}$$

$$\lim_{x\to a} \frac{f(x)}{g(x)} = \frac{\lim_{x\to a} f(x)}{\lim_{x\to a} g(x)} \tag{2.5}$$

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

Remark (exceptions).

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

Theorem 2.14 (L'Hospital/Bernouli).

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

Remark (application).

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

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

$$\lim_{x\to a} g(x) = L \tag{2.7}$$

Theorem 2.15 (chain rule). *Suppose* $\lim_{x\to a} g(x) = b$ *and* f *is continuous at* b*, then*

$$\lim_{x\to a} f(g(x)) = f(\lim_{x\to a} g(x)) = f(b) = c \tag{2.8}$$

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*

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

2.4 Limit Inferior/Superior of Functions

Definitions 2.16 (metric).

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

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

2.5 Sequence of Functions

2.5.1 Notions of Convergence

Definitions 2.17 (pointwise). *Sequence of functions are pointwise convergent if for each $x_0 \in X$, the sequence $f_n(x_0)$ converges to $f(x_0)$.*

$$\text{(metric)} \quad \forall x \in X,\ \forall \varepsilon > 0,\ \exists N_{x,\varepsilon} \in \mathbb{N},\ \forall n > N_{x,\varepsilon},\ d(f_n(x), f(x)) < \varepsilon \tag{2.9}$$

$$\text{(norm)} \quad \forall x \in X,\ \forall \varepsilon > 0,\ \exists N_{x,\varepsilon} \in \mathbb{N},\ \forall n > N_{x,\varepsilon},\ \|f_n(x), f(x)\| < \varepsilon \tag{2.10}$$

$$\text{(nbd)} \quad \forall x \in X,\ \forall U \in \mathcal{N}_{f(x)},\ \exists N_{x,U} \in \mathbb{N},\ \forall n > N_{x,U},\ f_n(x) \in U \tag{2.11}$$

Definitions 2.18 (uniform). *Sequence of functions are uniformly convergent if for each $x \in X$, all the sequences $f_n(x)$ converges to $f(x)$ uniformly.*

$$\text{(metric)} \quad \forall \varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall x \in X,\ \forall n > N_\varepsilon,\ d(f_n(x), f(x)) < \varepsilon \tag{2.12}$$

$$\text{(norm)} \quad \forall \varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall x \in X,\ \forall n > N_\varepsilon,\ \|f_n(x), f(x)\| < \varepsilon \tag{2.13}$$

$$\text{(nbd)} \quad ?? \tag{2.14}$$

2.5.2 Notions of Boundedness

Definitions 2.19 (pointwise). *Sequence of functions is pointwise bounded if for each $x_0 \in X$, the sequence $f_n(x_0)$ is bounded.*

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

Definitions 2.20 (uniform). *Sequence of functions if uniformly bounded if the pointwise bounds are uniform.*

$$\exists M \in \mathbb{R},\ \forall x \in X,\ |f_n(x)| < M \tag{2.16}$$

2.6 Limit of a Set

Definitions 2.21.

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

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

2.7 Sequence of Sets

Definitions 2.22.

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

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

Chapter 3

Linear Algebra

3.1 Vector Space

Definitions 3.1 (vector space). *A vector space $V(F)$ or $\langle V, F, +, \cdot \rangle$ satisfies*

1. *F is a field*
2. *$\langle V, + \rangle$ is an abelian group.*
3. *$1\alpha = \alpha, \ \forall v \in V$*
4. *$(c_1c_2)\alpha = c_1(c_2\alpha), \ \forall c_1, c_2 \in F, \alpha \in V$.*
5. *Scalar multiplicaiton $\cdot$ is left as well as right distributive over vectror addition $+$.*

Definitions 3.2 (subspace). *Let $V(F)$ be a vector space with $\langle V, F, +, \cdot \rangle$ and $W \subset V$. Then $W(F)$ is a subspace of $V(F)$ if $\langle W, F, +, \cdot \rangle$ is a vector space. ie, $W \leq V$.*

3.1.1 Important Notions

1. $c0 = 0$, $0\alpha = 0$, $(-1)\alpha = -\alpha$

3.1.2 Basis

Definitions 3.3 (linearly independent). *A set of vectors $W \subset V$ is linearly independent if W has a non-trivial linear combination representation of the zero vector.*

Note. *Linear combinations are of finite length (if not mentioned otherwise).*

Definitions 3.4 (basis). *A basis of a vector space $V(F)$ is a linear independent, spanning subset of the set of vectors V.*

Definitions 3.5 (dimension). *Any two basis of a vector space $V(F)$ are of the same cardinality. The cardinality of basis of $V(F)$ is the dimension of $V(F)$.*

Note. *The linear combinations of a set of vectors $W \subset V$ generates a subspace of $V(F)$. The zero vector always has the trivial linear combination representation for any subset W of V.*

Note. *Even infinite dimensional vector spaces demands an infinite basis with a finite linear combination representation for each of its vectors.*

Definitions 3.6 (change of basis). *Let B_1, B_2 be two bases for $V(F)$. The change of basis matrix $P = [B_1, B_2]$ satisfies $[\alpha]_{B_2} = [B_1, B_2] \cdot [\alpha]_{B_1}$ where $[\alpha]_B$ is the co-ordinate of $\alpha \in V$ with respect to a basis B of $V(F)$ and $[B_1, B_2]$ is the change of basis from B_1 to B_2.*

3.2 System of Equations

3.2.1 Row reduced echelon matrix

Definitions 3.7 (equivalent). *Two system of equations are equivalent if they have the same solution space. And, two matrices are equivalent if the respective systems of equations are equivalent.*

Definitions 3.8 (row operations). *A row operation is a function $f : F^{n\times m} \to F^{n\times m}$ that preserves equivalence. There are three elementary row operations,*

1. *multiplication of a row by a scalar*
2. *addition of a row to another*
3. *interchanging two rows*

Definitions 3.9 (elementary matrix). *Matrix corresponding to an elementary row operation.*

Note. *Any row operation can be performed by the multiplication of a matrix which is a finite product of elementary matrices.*

Note. *Every matrix has a unique row reduced echelon form. A matrix A is invertible if and only if its row reduced echelon form is the identity matrix.*

Note. *Gauss Elimination method with augmented matrix to solve system of equations.*

3.3 Matrices

Definitions 3.10 (matrix). *A matrix $A_{m\times n}$ over the field F is a function $A : \mathbb{Z}_m \times \mathbb{Z}_n \to F$.*

Definitions 3.11 (square). *A square matrix of order n is matrix $A_{n\times n}$. And $M_n(F)$ is the set of all square matrices of order n over the field F. ie, $A_{n\times n} \in M_n(F)$.*

Note. *The entries of $A_{m\times n}$ are represented by a_{ij} where $a_{ij} = A(i, j)$.*

Definitions 3.12 (identity). *The identity matrix of order n, $I_{n\times n}$ is given by $I(i, j) = \delta_{i,j}$.*

Definitions 3.13 (diagonals). *The **diagonal** entries are a_{ij} with $i = j$. The **superdiagonal** entries are a_{ij} with $i = j + 1$. The **subdiagonal** entries are a_{ij} with $i = j - 1$.*

Definitions 3.14 (diagonal). *A diagonal matrix all its entries zero except for the diagonal entries.*

Definitions 3.15 (Jordan normal). *A Jordan normal matrix has all entries zero except for diagonal and superdiagonal entries. All its non-zero superdiagonal entries are* 1.

Definitions 3.16 (submatrix). *$A(i|j)$ is the submatrix obtained from the matrix A by deleting ith row and jth column.*

Definitions 3.17 (normal). *A complex matrix A is normal if it commutes with its conjugate transpose. ie, $AA^* = A^*A$.*

3.3.1 Operations

Definitions 3.18 (trace). *The trace of a square matrix is the sum of its diagonal entries.*

$$tr : M_n(F) \to F,\ tr(A) = \sum_{k=1}^{n} A(k,k) \tag{3.1}$$

Definitions 3.19 (n-linear). *A function $f : M_n(F) \to F$ is n-linear iff is linear function of the ith row when other rows are fixed.*

Definitions 3.20 (alternating). *A function $f : M_n(F) \to F$ is alernating if*

1. *$f(A) = 0$ if two rows are equal.*
2. *$f(A') = -f(A)$*

Definitions 3.21 (determinant). *The determinant of a square matrix $det : M_n(F) \to F$ is an n-linear, alternating function with $D(I) = 1$.*

Note. *Matrix A with $det(A) = 0$ is singular.*

Definitions 3.22 (scalar multiplication). *Let $k \in F$ and $A_{m\times n}$ over the field F. The scalar product $k \cdot A_{m\times n}$ is kA given by $kA(i,j) = k \cdot A(i,j)$.*

Definitions 3.23 (transposition). *The **transpose** of a matrix $A_{m\times n}$ is the matrix $A'_{n\times m}$ given by $A' : n \times m \to F,\ A'(i,j) = A(j,i)$.*

Definitions 3.24 (complex conjugation). *The **complex conjugate** of a matrix $A_{m\times n}$ is the matrix $\bar{A}_{n\times m}$ given by $\bar{A} : n \times m \to F,\ \bar{A}(i,j) = \overline{A(j,i)}$.*

Note. *Conjugates and Complex Conjugate are different notions.*

Definitions 3.25 (addition). *Two matrices A, B are compatible for additon if they are of the same size. The sum of two matrices A, B is the matrix C of the same size with entries $c_{ij} = a_{ij} + b_{ij}$.*

Definitions 3.26 (mulitplication). *Two matrices A, B are compatible for multiplication if the number of columns of the first matrix and the number of rows of the second matrix are the same. The product of two matrices $A_{m\times n}, B_{n\times p}$ is the matrix $C_{m\times p}$ with entries*

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Note. *Matrix multiplication is associative and non-commutative. Every non-singular matrix has a multiplicative inverse.*

3.3.2 Types

Definitions 3.27 (idempotent). *A idempotent matrix A is a square matrix $A_{n\times n}$ which satisfies $A^2 = A$.*

Definitions 3.28 (involutary). *A involutary matrix A is a square matrix $A_{n\times n}$ which satisfies $A^2 = I$.*

Definitions 3.29 (scalar). *A scalar matrix A is a square matrix $A_{n\times n}$ which satisfies $a_{ij} = k \cdot \delta_{i,j}$. ie, $A_{n\times n} = k \cdot I_{n\times n}$*

Definitions 3.30 (nilpotent). *A square matrix is nilpotent of index p if $A^p = 0$ and $A^k \neq 0,\ \forall k < p$.*

Definitions 3.31 (periodic). *A square matrix is nilpotent of period p if $A^p = I$ and $A^k \neq I,\ \forall k < p$.*

Definitions 3.32 (symmetric). *A symmetric matrix $A_{n\times n}$ satisfies $a_{ij} = a_{ji}$. ie, $A' = A$. A skew-symmetric matrix satisfies $a_{ij} = -a_{ji}$. ie, $A' = -A$.*

Definitions 3.33 (hermitian). *A hermitian matrix $A_{n\times n}$ satisfies $\overline{a_{ij}} = a_{ji}$. ie, $A^* = A,\ A^* = \bar{A}'$. A skew-hermitian matrix satisfies $\overline{a_{ij}} = -a_{ji}$. ie, $A^* = -A$.*

Note. *Every matrix A has a decomposition $A = P+Q$ where $P = \frac{A+A'}{2}$ is symmetric and $Q = \frac{A-A'}{2}$ is skew-symmetric. And A has a decomposition $A = P + Q$ where $P = \frac{A+A^*}{2}$ is hermitian and $Q = \frac{A-A^*}{2}$ is skew-hermitian.*

Definitions 3.34 (orthogonal). *An orthogonal matrix A satisfies $A \in M_n(\mathbb{R})$ and $AA' = I$.*

Definitions 3.35 (unitary). *A unitary matrix A satisfies $A \in M_n(\mathbb{C})$ and $AA^* = I$.*

3.3.3 Important Notions

Let $A_{m\times n} \in \mathbb{R}^{m\times n}$.

1. $tr(AA') = 0 \iff A = 0$.

1. Let D be a diagonal matrix. Then $AD = DA \iff A$ is a block diagonal matrix.

3.3.4 Invariants

Definitions 3.36 (conjugation). *Two square matrices A, B are* ***conjugates*** *if there exists an invertible matrix P such that $A = PBP^{-1}$.*

Theorem 3.37. *If $A_{m\times n}$, then $Rank(A) + Nullity(A) = n$*

Theorem 3.38 (Cayley-Hamilton). *Every matrix $A \in M_n(F)$ satisfies its characteristic equation $det(A - xI) \in F[x]$.*

Definitions 3.39 (minimal polynomial). *The minimal polynomial of a square matrix A is the unique, monic polynomial p of least degree satisfied by A. ie, $p(A) = 0$.*

Note. *For every square matrix A has a conjugate matrix of the Jordan normal form which unique upto block permutations.*

Definitions 3.40 (diagonalisable)**.** *A diagonalisable matrix has a diagonal matrix as its Jordan normal form.*

Note. *Jordan normal form determines the minimal polynomial. The set of all polynomials that annihilate A form a principal ideal domain in $\mathbb{C}[x]$ with minimal polynomial as its generator.*

Definitions 3.41 (multiplicity)**.** *Algebraic multiplicity of an eigenvalue α of $A \in M_n(F)$ is the degree of $(\lambda - \alpha)$ in its characteristic equation. Geometric multiplicity of α is the number of blocks in Jordan normal form with diagonal entry α.*

3.3.5 Important Notions

1. If $A \in M_n(F)$ with Jordan normal form $J = P^{-1}AP$, then $A^n = PJ^nP^{-1}$.
2. Eigenvalues, their algebraic and geometric multiplicities, characteristic polynomial, minimal polynomial, trace, determinant, rank and nullity are invaint under conjugation.
3. A matrix is normal if and only if its diagonalisable by a unitary matrix. Thus, real symmetric matrices are diagonalisable over $\mathbb{R}$. And hermitian, skew-hermitian matrices are diagonalisable over $\mathbb{C}$.
4. real skew-symmetric matrices are not diagonalisable over $\mathbb{R}$.
5. Rotation matrices are non-diagonalisable over $\mathbb{R}$ but diagonalisable over $\mathbb{C}$.
6. Non-zero nilpotent matrices are non-diagonalisable over any field F.
7. Sum of diagonalisable matrices need not be diagonalisable.

3.4 Quadratic Forms

Theorem 3.42 (QR decomposition)**.** *Every matrix $A \in M_n(\mathbb{C})$ has a QR-decomposition. ie, $A = QR$ where Q is unitary and R is upper triangular.*

Note. *QR-decomposition unique if R has positive diagonal entries.*

Definitions 3.43 (definite)**.** *Symmetric matrix $A \in M_n(\mathbb{R})$ is positive definite if all its eigenvalues are positive. A is positive semidefinite if if all its eigenvalues are non-negative.*

Definitions 3.44 (definite)**.** *Let $A \in M_n(\mathbb{C})$ be a hermitian matrix. The matrix A is **positive definite** matrix if it satisfies $x'Ax > 0,\ \forall x \in \mathbb{C}^{n\times 1}$. A is **positive semidefinite** matrix if it satisfies $x'Ax \geq 0,\ \forall x \in \mathbb{C}^{n\times 1}$. A is **negative definite** matrix if it satisfies $x'Ax < 0,\ \forall x \in \mathbb{C}^{n\times 1}$.*

Part II

Mathematics 2

Chapter 4

Algebra

4.1 Number Theory

Lemma 4.1 (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 4.2. *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 $\{k \in \mathbb{N} : k \le n,\ \gcd(n,k) = 1\}$.

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 $k \le n$ that are relatively prime to n is $n\phi(n)/2$.

Theorem 4.3 (Fermat)**.** $a^p \cong a \pmod p$

Definitions 4.4. *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 4.5. *A number x is a* ***Carmichael*** *number if $a^x \cong a \pmod x$ whenever $\gcd(a,x) = 1$.*

4.1.1 Arithmetical Functions

Definitions 4.6. *A function $f : \mathbb{N} \to \mathbb{C}$ is an* ***arithmetical*** *(number theoretic) function.*

Definitions 4.7. *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 4.8. *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 4.9. *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 4.10. *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.
Clearly, $\tau = \sigma_0 = \zeta * \zeta$.
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.
Clearly, $\Omega = \zeta * \chi_{\mathcal{P}}$ where $\mathcal{P}$ is the set of all prime powers

Strange Functions

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

4.2 Group Theory

Definitions 4.11. *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 4.12. *A* ***binary relation*** *on a set A is a relation between $A \times A$ and A.*

Definitions 4.13. *An* ***associative*** *binary relation $*$ on A satisfies*

$$(x * y), (y * z) \in A \implies (x * y) * z, x * (y * z) \in A,\ (x * y) * z = x * (y * z) \tag{4.1}$$

Definitions 4.14. *A* ***commutative*** *binary relation $*$ on A satisfies*

$$x * y \in A \implies y * x \in A,\ x * y = y * x \tag{4.2}$$

A commutative algebra is also called abelian.

Definitions 4.15. *A binary* ***operation*** *on A is a function $* : A \times A \to A$.*

Definitions 4.16. *An* ***associative*** *binary operation $*$ on A satisfies*

$$(x * y) * z = x * (y * z) \tag{4.3}$$

Definitions 4.17. *A* ***commutative*** *binary operation $*$ on A satisfies*

$$x * y = y * x \tag{4.4}$$

Definitions 4.18. *A binary* ***algebra*** *$\langle A, * \rangle$ is an algebra with a set A together with a binary operation $*$ on A.*

Definitions 4.19. *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 4.20. *A* ***semigroup*** *is a magma $\langle A, * \rangle$ where $*$ is associative.*

Definitions 4.21. *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 4.22. *A* ***monoid*** *is a semigroup $\langle A, * \rangle$ where $*$ has an identity $e \in A$.*

Definitions 4.23. *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 4.24. *A* ***group*** *is a monoid $\langle A, * \rangle$ where every element $x \in A$ has an inverse x^{-1}.*

Definitions 4.25. *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 4.26. *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 4.27. *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 4.28. *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 $+$.

$$
\begin{tikzcd}
 & Magma \arrow[r, dash, "+totality"] \arrow[d, dash, "+associative"] & Partial\ Algebra \arrow[d, dash] \\
 & Semigroup \arrow[d, dash, "+identity"] & Semigroupoid \arrow[d, dash] \\
 & Monoid \arrow[d, dash, "+inverses"] & Small\ Category \arrow[d, dash] \\
 & Group \arrow[dl, dash, "+generator"'] \arrow[d, dash, "+commutative"] & Groupoid \\
Cyclic\ Group \arrow[r, dash] & Abelian\ Group &
\end{tikzcd}
$$

Figure 4.1: Binary Algebraic Structures

Definitions 4.29. *The* ***sum*** *of two subsets A and B of a magma $\langle X, +\rangle$ is*

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

Definitions 4.30. *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 4.31. *A function $f : R^n \to R'$ is n-**linear** if for $1 \le k \le n$,*

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

Definitions 4.32. *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 4.33. *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[1]

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 4.2: 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 $f : A \to B = \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^m \qquad (n \leq m)$

9. Number of bijections $f : A \to B = n! \qquad (n = m)$

1				
1	2			
2	3	5		
5	7	10	15	
15	20	27	37	52

Figure 4.3: Bell Triangle

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

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

4.2.1 Groups and Subgroups

Definitions 4.34. *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 4.35. *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 4.36. *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.*

Important Notions

Strange Groups

1. Smallest non-abelian group is S_3. Smallest non-cyclic group is the Klein 4-group, $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. 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 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. $\left\langle \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \neq 0 \right\}, \times \right\rangle$ is a group with identity $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$.
5. $\left\langle \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \neq 0 \right\}, \times \right\rangle$ is a group with identity $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.
6. $\left\langle \mathbb{Q}^+, a * b = \frac{ab}{5}, \times \right\rangle$ is a group with idenity 5.
7. $\langle \{5, 15, 20, 25, 30, 35\}, \times_{40} \rangle$ is a group with identity 25.
8. Convergent sequences under addition is a group.
9. Group of rigid motions(rotations) of the cube is a group of order $\binom{8}{1}\binom{3}{1} = 24$ under permutation multiplication.

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 $y = (1,2,\ldots,n)$.

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

   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.

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 : $\phi(x) = 3x - 1,\ \phi(1) = 2,\ x^{-1} = \frac{8-x}{x+1}$)

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 $\phi\left(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\right) = a + ib$.

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, $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}$ is cyclic. However, K_4 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. $\mathbb{Q}^*$ is not cyclic.

    Proof. Suppose $\mathbb{Q}^*$ is cyclic. Then $\mathbb{Q}^* \cong \mathbb{Z}$. But, $o(-1) = 2$ and $\mathbb{Z}$ don't have any element of order two. □

11. $\mathbb{Q}, \mathbb{R}$ are not cyclic.

    Proof. Suppose $\mathbb{Q} \cong \langle p/q \rangle$. Then $p/2q \notin \langle p/q \rangle$. Thus, $\mathbb{Q}$ is not cyclic. Since $\mathbb{Q} \geq \mathbb{R}$, $\mathbb{R}$ is not cyclic. $\square$

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

13. 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 $M_n(F)$. $Z(M_n(F)) = \{aI : a \in F\}$.

2. General Linear Group, $GL(n, F)$ is the multiplicative group of all invertible matrices of order n with entries from field F.
$$|GL(n, F_q)| = \prod_{r=0}^{n-1} (q^n - q^r)$$
   $Z(GL(n, F)) = \{aI : a \in F,\ a \neq 0\}$.

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. $Z(SL(n, F)) = \{aI : a \in F,\ a^n = 1\}$.

4. The determinant, $det : GL(n, F) \to F^*$ is a homomorphism with $\ker(det) = SL(n, F)$.
$$|SL(n, F_q)| = \frac{|GL(n, F_q)|}{q-1} \text{ since } GL(n, F_q)/SL(n, F_q) \cong F_q^*$$

5. The trace, $Tr : M(n, F) \to F$. Then $\ker(Tr)$ is $n^2 - 1$ dimensional over F.

4.2.2 Permutations, Cosets & Direct Products

Definitions 4.37. *The* ***symmetric group*** S_n *is the set of all permutation on a set* $\{1, 2, \ldots, n\}$ *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 4.38 (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 $g \overset{\lambda_x}{\to} xg$ is an homomorphism. □

Definitions 4.39. *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 4.40. *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 4.41. *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 4.42. *The alternating group A_n is the subgroup of all even permutations in the symmetric group S_n.*

Definitions 4.43. *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 4.44 (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 4.45. ***Index*** *of H in G, $(G : H)$ is the number of left cosets of H in G.*

Theorem 4.46. *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. $\square$

Theorem 4.47. *Let $K \leq H \leq G$. Then $(G : K) = (G : H)(H : K)$.*

Definitions 4.48. *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 $(g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2)$.*

Theorem 4.49. *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 4.50. $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{n \times m} \iff \gcd(m, n) = 1$.

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

Theorem 4.51. *Let $(a_1, \ldots, a_n) \in G_1 \times \ldots G_n$ and $o(a_i) = r_i$.*
Then $o((a_1, \ldots, a_n)) = lcm(r_1, \ldots, r_n)$.

Definitions 4.52. *The* ***center*** *of a group G is the set of all elements that commutes with every element in G.*

Theorem 4.53. *Center $Z(G)$ is a subgroup of G.*

Definitions 4.54. *A subgroup H of group G is* ***normal*** *if $gH = Hg$ for every element $g \in G$.*

Definitions 4.55. *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 $g_1 N * g_2 N = (g_1 g_2)N$.*

Definitions 4.56. *An element $g \in G$ is a* ***commutator*** *if $g = aba^{-1}b^{-1}$ for some $a, b \in G$.*

Theorem 4.57. *Let G be a group. Then the set C of all commutators in G is the smallest normal subgroup of G such that G/C is abelian.*

Isomorphism Theorems

Theorem 4.58. *Let $g \in G$. The function $i_g : G \to G$ defined by $i_g(x) = gxg^{-1}$ is an automorphism of the group G.*

Definitions 4.59. *The automorphism $x \to gxg^{-1}$ is the* ***inner automorphism*** *of G by g.*

Definitions 4.60. *The* ***conjugacy class*** *of x, $Cl(x) = \{gxg^{-1} : g \in G\}$.*

Definitions 4.61. *Let G be a group and H, K be subgroups of G. Subgroup H is a* ***conjugate*** *of K if $H = i_g[K]$ for some $g \in G$.*

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

Theorem 4.62. *Let G be group and N be a normal subgroup of G. Then $g \xrightarrow{\phi} gN$ is a group homomorphism.*

Theorem 4.63. *Let $\phi : G \to G'$ be a group homomorphism. Then $\ker(\phi)$ is a normal subgroup of G. And $\phi[G] \cong G/\ker(\phi)$.*

Important Notions

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 $\mathbb{Z}_n / \langle g \rangle \cong \mathbb{Z}_d$ where $d = n/o(g)$.

Order of Elements in a product of Cyclic groups Let $(g_1, g_2, \dots, g_k) \in G_1 \times G_2 \times \cdots \times G_k$. Then $o(g_1, g_2, \dots, g_k) = lcm(o(g_1), o(g_2), \dots, o(g_k))$. And element $k \in \mathbb{Z}_n$ has order $\frac{n}{\gcd(n,k)}$.

For example, an element of (g, h) of $\mathbb{Z}_{12} \times \mathbb{Z}_{10}$ has order 4 only if $o(g) = 4$ and $o(h)$ is either 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 $\mathbb{Z}_{12} \times \mathbb{Z}_{10}$.

To enumerate elements of order 9 in $\mathbb{Z}_{12} \times \mathbb{Z}_{18} \times \mathbb{Z}_{27}$, being cyclic there are $\phi(1), \phi(3), \phi(9)$ elements of order $1, 3, 9$ (if any). There are $3 \times 9 \times 9$ elements out of which precisely $3 \times 3 \times 3$ of them are of order less than 9. Thus 216 elements of order 9.

$\mathbb{Z}_n^\times$ $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$ and $\phi(10) = \phi(2)\phi(5) = 4$. And $\mathbb{Z}_{10}^\times \cong \mathbb{Z}_4$ as $\langle 3 \rangle = \mathbb{Z}_{10}^\times$.

$$\mathbb{Z}_{st}^\times \cong \mathbb{Z}_s^\times \times \mathbb{Z}_t^\times \iff \gcd(st) = 1$$

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

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

Thus, $\mathbb{Z}_4^\times = \mathbb{Z}_2$, $\mathbb{Z}_8^\times = \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_{16}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, ... 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 $\mathbb{Z}_{1000}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{100}$.

Order of an element in a direct product What is the order of $(\mathbb{Z}_{12} \times \mathbb{Z}_{30}) / \langle (g, h) \rangle$ where $o(g) = 6$ and $o(h) = 10$?
$\mathbb{Z}_{12} \times \mathbb{Z}_{30} \cong (\mathbb{Z}_{2^2} \times \mathbb{Z}_3) \times (\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5)$ and $g = (g_1, g_2)$ where $o(g_1) = 2$ and $o(g_2) = 3$. Similarly, $h = (h_1, h_2, h_3)$ where $o(h_1) = 2$, $o(h_2) = 1$ and $o(h_3) = 5$.

$$(\mathbb{Z}_4 \times \mathbb{Z}_3) \times (\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5) / \langle (g_1, g_2, h_1, h_2, h_3) \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_3 \times \mathbb{Z}_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_3$$

since $(\mathbb{Z}_4 \times \mathbb{Z}_2) / \langle (g_1, h_1) \rangle \cong \mathbb{Z}_4$.

Finitely Generated Groups

1. 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 two. The center of the dihedral group $Z(D_n)$ is trivial when n is odd. $Z(D_n) = \{0, R_{180}\} \cong Z_2$ if n is even. The number of subgroup of $D_n = \tau(n) + \sigma(n)$.

2. The center of a symmetric group $Z(S_n)$ is trivial for $n \geq 3$.
3. The center of an alternating group $Z(A_n)$ is trivial for $n \geq 4$.

Definitions 4.64. *The* ***structure*** *of a permuation $\sigma \in S_n$ is $1^{n_1}2^{n_2}\dots r^{n_r}$ where n_j is the number of cycles of length j.*

The number of permutations of the structure $1^{n_1}2^{n_2}\dots r^{n_r}$ 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 $1^3 2^2 3^1$.

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.

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

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

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

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

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

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

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

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

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

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

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

Additional Structures

Definitions 4.65. *The set of all elements of an abelian group G of finite order forms a normal subgroup called* ***torsion*** *subgroup of G.*

Definitions 4.66. *A* ***torsion free*** *group has only one element of finite order in it.*

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 $e^{2\pi ix}$, $x \in \mathbb{R} - \mathbb{Q}$ 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 freee 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. The quotient group $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}_1$ is a torsion group since every rational number $0 \leq p/q < 1$ is of the finite order q. And $\mathbb{Q}_\pi$ is torsion free.

Semidirect Product

Definitions 4.67. *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 $(n_1, h_1) * (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2)$.*

The dihedral group, $D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$.

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

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.

No simple group G can be expressed as a semidirect product as G does not have a normal subgroup.

Definitions 4.68. *The* ***fundamental group*** *of a topological space is the group of equivalent classes under homotopy of the loops contained in the space.*

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.

Theorem 4.69. *If $G/Z(G)$ is cyclic, then 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. □

1. If G is non-abelian, then $G/Z(G)$ is not cyclic.
2. 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.
3. 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. □

For $A_5, S_3, \ldots,$ the group $G/Z(G)$ is non-abelian.
Number of abelian groups of order $n = p_1^{r_1}p_2^{r_2}\ldots p_k^{r_k}$ is $\prod_k B(r_k)$.

1. By Burnside‘s theorem, p-Groups have non-trivial center. And Q_8 is the smallest non-abelian p-group.
2. Every group G of order p is cyclic and $G \cong Z_p$. The number of generators is $\phi(n)$.
3. Every group G of order p^2 is abelian. There are two groups Z_{p^2} and $Z_p \times Z_p$.
4. 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. □

5. No group G of order p^3 is simple.

   Proof. Every group of order p^3 is a semidirect product except $\mathbb{Z}_4$ and Q_8. However, $\mathbb{Z}_4$ is abelian and has normal subgroups isomorphic to $\mathbb{Z}_2$. And Q_8 has normal subgroups isomorphic to $\mathbb{Z}_4$. □

6. Every non-abelian group G of order p^3 has center $Z(G)$ of order p. Since G is a p-group, G has non trivial center. Suppose $|Z(G)| = p^2$, then $G/Z(G)$ is a cyclic group of order p. But G is non-abelian.
7. Every non-abelian group G of order p^3 has $p^2 + p - 1$ distinct conjugacy classes.

8. Every group G of order pq has precisely four subgroups of order $1, p, q, pq$ (by first Sylow theorem). Suppose $p < q$. Then subgroup H of order p is normal. If p does not divide $q-1$, then subgroup K of order q is normal. Clearly, $|H \cap K| = 1$ and $G \cong HK = Z_p \times Z_q$. Thus G is cyclic since $gcd(p,q) = 1$.

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

10. 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 $G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_k \triangleleft G$ such that $|G_1| = p_1$, $|G_2| = p_1p_2$ and $|G_k| = p_1p_2 \dots p_k$. □

11. Every group G of order pqr is

12. Every group G of order p^2q is

13. Every group G of order p^3q is

$$K \triangleleft H \triangleleft G \not\Rightarrow K \triangleleft G \text{ hint } G = D_4$$

Simple Groups

Theorem 4.70. *M is maximal normal subgroup of G iff G/M is simple.*

Theorem 4.71. *Let N be a normal subgroup of G. G/N is abelian iff $C \leq N$.*

Group Action

Definitions 4.72. *An **action** of group G on a set X is a function $* : G \times X \to X$ such that*

1. $\forall x \in X,\ ex = x$
2. $\forall x \in X,\ \forall g_1, g_2 \in G,\ (g_1g_2)x = g_1(g_2x)$

Theorem 4.73. *Let X be a G-set. Then $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ where $x \xrightarrow{\sigma_g} gx$.*

Definitions 4.74. *Let X be a G-set and $x \in X$. The **isotropy** subgroup G_x is the subgroup of G containing all elements that fix x.*

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

Theorem 4.75. *Let X be a G-set and $g \in G$. Then the relation $x_1 \sim_g x_2 \iff gx_1 = x_2$ is an equivalence relation on X.*

Definitions 4.76. *The equivalence class of $\sim_g$ containing x is the **orbit** of x, say Gx.*

Theorem 4.77. $|Gx| = (G : G_x)$

Theorem 4.78 (Burside's Formula)**.** $r|G| = \sum_{g \in G} |X_g|$

4.3 Ring Theory

Lemma 4.79 (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 4.80 (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 4.81 (chinese remainder theorem).

Definitions 4.82 (Bézout Domain). *A Bézout Domain is an integral domain which satisfyies Bézout's identity.*

Every PID is a Bézout Domain.

Definitions 4.83 (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.

4.3.1 Important Notions

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

Definitions 4.84 (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 $\pm 1, \pm w, \pm w^2$.

4.4 Fields

4.4.1 Finite Fields

Definitions 4.85. *For every prime power p^n, there exists a unique Galois field $GF(p^n)$ of order p^n.*

4.4.2 Field Extensions

Theorem 4.86 (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 4.87. *A field E is an extension field of field F if F is containined in E.*

Definitions 4.88. *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 4.89. *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 4.90. *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 4.91. *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 4.92 (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 $\mathbb{C}$.

4.4.3 Important Notions

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

Theorem 4.93. *$\langle \mathbb{Z}_n, +_n, \times_n \rangle$ 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 4.94 (cyclotomic field)**.** *The nth **cyclotomic field** is $\mathbb{Q}(\alpha)$ where α is a primitive nth root of unity.*

Definitions 4.95 (cyclotomic polynomial)**.** *The nth **cyclotomic polynomial** $\Phi_n(x)$ is the monic irreducible polynomial with primitive nth roots of unity as its zeroes.*

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

The nth cyclotomic polynomial has degree $\phi(n)$.

Constructible Numbers

Definitions 4.96. *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).*

The constructible numbers form a field. And 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. The classical problems like trisecting an angle, squaring a circle and doubling a cube are thus impossible.

The constructible numbers fields is an infinite extension of $\mathbb{Q}$.

1. $[E : F]$
2. $\{E : F\}$
3. $(E : F)$

4.4.4 Galois Theory

4.5 Topology

4.5.1 Metric Space

Definitions 4.97 (distance function)**.** *A distance function $d : X \times X \to \mathbb{R}^+$ on a set X is a function which satisfies*

1. $d(x, y) \ge 0, \qquad \forall x, y \in X$
2. $d(x, y) = 0 \iff x = y$
3. $d(x, y) = d(y, x)$
4. $d(x, y) \le d(x, z) + d(z, y), \qquad x, y, z \in X$

4.5.2 Convergence

Definitions 4.98 (metric). *A sequence x_n converges to x if there exists $N \in \mathbb{N}$ such that $\forall n > N,\ d(x_n, x) < \varepsilon$.*

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n > N,\ d(x_n, x) < \varepsilon \tag{4.5}$$

4.5.3 Cauchy Criterion

Definitions 4.99 (metric). *A sequence x_n is Cauchy if there exists $N \in \mathbb{N}$ such that $\forall n, m > N,\ d(x_n, x_m) < \varepsilon$.*

4.5.4 Topological Space

Definitions 4.100 (topological space). *A topological space $\langle X, \mathcal{T} \rangle$ where $\mathcal{T} \subset \mathcal{P}(X)$ satisfies*

1. *$\phi, X \in \mathcal{T}$.*
2. *$\mathcal{T}$ is closed under finite intersections.*
3. *$\mathcal{T}$ is closed under arbitrary unions.*

Let $G \in \mathcal{T}$. Then G is an open set in $\langle X, \mathcal{T} \rangle$. And $X - G$ is a closed set.

Definitions 4.101 (clopen). *A clopen set is both open and closed.*

Definitions 4.102 (dense). *A dense set A intersects every non-trivial open set in $\langle X, \mathcal{T} \rangle$.*

Note. *A dense set has no proper closure. If A is dense in X, then $\bar{A} = X$. If A is dense in X and $x \in X$, then every neighbourhood of x has an element of A.*

Definitions 4.103 (neighbourhood). *A **neighbourhood** N of a point $x \in X$ contains an open set containing x. Then x is an **interior point** of N.*

Definitions 4.104 (neighbourhood system). *The **neighbourhood system** of x, $\mathcal{N}_x$ is the family of all neighbourhoods of x.*

Definitions 4.105 (interior). *The set of all interior points of N is the **interior** of N, N°.*

Definitions 4.106 (exterior). *The interior of $X - N$ is the **exterior** of N.*

Definitions 4.107 (boundary). *The **boundary** of N, ∂N is the set of all points which are neither in its interior or exterior.*

Definitions 4.108 (derived set). *A **limit point** x of a set A has every deleted neighbourhood $N - \{x\}$ intersecting A. The **derived set** A' is the set of all limit points of A.*

Note. *A point x is a limit point of A if and onoy if there exists a non-eventual sequence in A converging to x.*

Definitions 4.109 (closure). *The closure of A, $\bar{A} = A \cup A'$.*

Note. *The closure of A, $\bar{A}$ is the smallest closed set containing A. If A is closed, then $\bar{A} \subset A$. If C is closed and $A \subset C$, then $\bar{A} \subset C$.*

4.5.5 Convergence

Definitions 4.110 (neighbourhood)**.** *A sequence* $\{x_n\}$ ***converges*** *to* x *if any neighbourhood* N *of* x *contains all except finitely many* x_n*'s. Then* x *is a* ***limit*** *of sequence* $\{x_n\}$*.*

Note. *Let* $x_n \to x$ *in* $\langle X, \mathcal{T} \rangle$*. Then* x_n *is eventually in every neighbourhood of* x*.*

$$\forall U \in \mathcal{N}_x,\ \exists N \in \mathbb{N},\ \forall n > N,\ x_n \in U \tag{4.6}$$

Note. *Sequences* $\{\frac{1}{n}\}$*,* $\{\frac{1}{2^n}\}$ *are eventually in every neighbourhood of* 0*.*

4.5.6 Important Notions

Definitions 4.111 (Euler Characteristic)**.** $\chi = V - E + F$

Remark. *Every convex polyhedron has Euler characteristic,* $\chi = 2$*.*