Algebra (BSc Maths Hons, DU - Semester I) – Exam-Focused Notes

1 Sets, Relations, and Functions

This section covers fundamental building blocks of discrete mathematics, essential for understanding more advanced algebraic structures.

1.1 Basic Concepts:

Set Operations:

- **Union ($A \cup B$):** The set of all elements that are in A, or in B, or in both.
- **Intersection ($A \cap B$):** The set of all elements that are common to both A and B.
- **Complement (A^c or A'):** The set of all elements in the universal set that are not in A.
- **Difference ($A - B$ or $A \setminus B$):** The set of all elements that are in A but not in B. This can also be expressed as $A \cap B^c$.
- **Cartesian Product ($A \times B$):** This operation creates a set of all possible ordered pairs where the first element comes from set A and the second from set B. Formally, $A \times B = \{(a, b) | a \in A, b \in B\}$. If A has m elements and B has n elements, then $A \times B$ will have $m \times n$ elements.

1.2 Relations:

A relation R from a set A to a set B is a subset of their Cartesian product, $A \times B$. If A=B, it's a relation on A.

Types of Relations:

- **Reflexive:** A relation R on a set A is reflexive if for every element $a \in A$, $(a, a) \in R$. (Every element is related to itself).
- **Symmetric:** A relation R on a set A is symmetric if whenever $(a, b) \in R$, then $(b, a) \in R$. (If a is related to b, then b is related to a).

- **Transitive:** A relation R on a set A is transitive if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$. (If a is related to b and b is related to c, then a is related to c).
- **Equivalence Relation:** A relation is an equivalence relation if it is reflexive, symmetric, and transitive. Equivalence relations partition a set into disjoint equivalence classes.
- **Partition of a set:** A partition of a set S is a collection of non-empty disjoint subsets of S whose union is S. Each element of S belongs to exactly one subset. An equivalence relation on a set A induces a partition of A, where each part of the partition is an equivalence class.

1.3 Functions:

A function (or mapping) $f : A \to B$ is a special type of relation where each element in the domain A is mapped to exactly one element in the codomain B.

Types of Functions:

- **One-one (Injective):** A function $f : A \to B$ is injective if distinct elements in A map to distinct elements in B. That is, if $f(a_1) = f(a_2)$, then $a_1 = a_2$.
- **Onto (Surjective):** A function $f : A \to B$ is surjective if every element in the codomain B has at least one corresponding element in the domain A. That is, for every $b \in B$, there exists an $a \in A$ such that $f(a) = b$.
- **Bijective:** A function is bijective if it is both one-one (injective) and onto (surjective). Bijective functions establish a perfect pairing between elements of two sets.
- **Inverse Function:** If a function $f : A \to B$ is bijective, then its inverse function $f^{-1} : B \to A$ exists. This means for every $b \in B$, there is a unique $a \in A$ such that $f(a) = b$, and $f^{-1}(b) = a$.
- **Composition of Functions:** If $f : A \to B$ and $g : B \to C$ are functions, then the composite function $g \circ f : A \to C$ is defined by $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

PYQ Focus: Proving a given relation is an equivalence relation and subsequently finding the partition it induces on the set. This often involves demonstrating reflexivity, symmetry, and transitivity, then explicitly listing the equivalence classes.

2 Integers and Division Algorithm

This section lays the groundwork for number theory, a crucial component of abstract algebra.

2.1 Division Algorithm:

For any integers a (dividend) and b (divisor) with $b \neq 0$, there exist unique integers q (quotient) and r (remainder) such that $a = bq + r$, where $0 \leq r < |b|$.

Significance: This theorem guarantees the existence and uniqueness of the quotient and remainder, forming the basis for many number theoretic algorithms, including the Euclidean Algorithm.

2.2 Euclidean Algorithm:

- **Purpose:** The Euclidean Algorithm is an efficient method for computing the greatest common divisor (GCD) of two integers. It is based on the principle that the GCD of two numbers does not change if the larger number is replaced by its difference with the smaller number.

- **Method:** Repeatedly apply the division algorithm:

$$a = bq_1 + r_1 \tag{1}$$
$$b = r_1 q_2 + r_2 \tag{2}$$
$$r_1 = r_2 q_3 + r_3 \tag{3}$$
$$\vdots \tag{4}$$

  The last non-zero remainder is the GCD.

- **Extended Euclidean Algorithm:** This extension allows expressing the GCD of two integers a and b as a linear combination of a and b, i.e., $\gcd(a, b) = ax + by$ for some integers x and y. This is particularly useful in modular arithmetic for finding modular inverses.

2.3 Fundamental Theorem of Arithmetic (Unique Prime Factorization Theorem):

- **Statement:** Every integer greater than 1 can be uniquely expressed as a product of prime numbers, disregarding the order of the factors.

- **Example:** $12 = 2^2 \times 3$, $30 = 2 \times 3 \times 5$.

- **Significance:** This theorem is foundational in number theory, proving that prime numbers are the "atoms" of integers.

PYQ Focus: Applying the Euclidean algorithm to compute the GCD of two integers and expressing the GCD as a linear combination of the given integers (using the Extended Euclidean Algorithm).

3 Modular Arithmetic

Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" when reaching a certain value—the modulus.

3.1 Congruence:

- **Definition:** Two integers a and b are said to be congruent modulo m, written as $a \equiv b \pmod{m}$, if m divides their difference $(a - b)$. This means $a - b = km$ for some integer k. Equivalently, a and b have the same remainder when divided by m.
- **Properties of Congruence:**
  - **Reflexive:** $a \equiv a \pmod{m}$
  - **Symmetric:** If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
  - **Transitive:** If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
  - **Addition:** If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$. More generally, $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$.
  - **Multiplication:** If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. Similar to addition, $(a \times b) \bmod n = ((a \bmod n) \times (b \bmod n)) \bmod n$.
  - **Exponentiation:** If $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ for any positive integer k.

3.2 Inverses (Modular Multiplicative Inverse):

- **Definition:** An integer a^{-1} is the multiplicative inverse of a modulo m if $a \cdot a^{-1} \equiv 1 \pmod{m}$.
- **Existence Condition:** The modular multiplicative inverse $a^{-1} \pmod{m}$ exists if and only if the greatest common divisor of a and m is 1, i.e., $\gcd(a, m) = 1$. This means a and m must be coprime.
- **Finding the Inverse:** The Extended Euclidean Algorithm is commonly used to find modular inverses.

PYQ Focus: Solving linear congruences (e.g., $ax \equiv b \pmod{m}$) and finding modulo inverses.

4 Complex Numbers

Complex numbers extend the real number system by introducing the imaginary unit i, where $i^2 = -1$.

4.1 Forms of Complex Numbers:

- **Cartesian (Rectangular) Form:** $z = x + iy$, where x is the real part ($\text{Re}(z)$) and y is the imaginary part ($\text{Im}(z)$). This form is convenient for addition and subtraction.
- **Polar Form:** $z = r(\cos\theta + i\sin\theta)$, where $r = |z|$ is the modulus (distance from origin) and θ is the argument (angle with the positive x-axis). This form is useful for multiplication, division, and exponentiation.
  - $r = \sqrt{x^2 + y^2}$
  - $\theta = \arctan(y/x)$ (adjusted for the correct quadrant).
- **Exponential Form (Euler's Form):** $z = re^{i\theta}$, derived from Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$. This is the most compact form and is highly efficient for operations.

4.2 Operations and Properties:

- **Conjugate ($\overline{z}$):** The conjugate of $z = x + iy$ is $\overline{z} = x - iy$. Geometrically, it's a reflection across the real axis.
  - Properties: $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 z_2} = \overline{z_1 z_2}$, $z\overline{z} = |z|^2$.
- **Modulus ($|z|$):** The modulus of $z = x + iy$ is $|z| = \sqrt{x^2 + y^2}$. It represents the distance of the complex number from the origin in the complex plane.
- **De Moivre's Theorem:** This fundamental theorem states that for any real number θ and any integer n, $(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$.
  - **Significance:** It provides a direct way to find powers and roots of complex numbers when they are in polar form.
- **Roots of Unity:** The n^{th} roots of unity are the solutions to the equation $z^n = 1$. Using De Moivre's Theorem, these roots are given by $e^{i\frac{2\pi k}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$ for $k = 0, 1, \ldots, n-1$.

PYQ Focus: Proving De Moivre's Theorem (often by induction) and finding the n^{th} roots of unity (or other complex numbers).

5 Theory of Equations

This section deals with polynomial equations and their roots.

5.1 Polynomial Equations:

- A polynomial equation is an equation of the form $a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0 = 0$, where a_i are coefficients and $a_n \neq 0$.
- **Vieta's Formulas:** These formulas establish relationships between the roots of a polynomial and its coefficients. For a polynomial $a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0 = 0$ with roots $r_1, r_2, \ldots, r_n$:
  - Sum of roots: $\sum r_i = -\frac{a_{n-1}}{a_n}$
  - Sum of products of roots taken two at a time: $\sum_{i<j} r_ir_j = \frac{a_{n-2}}{a_n}$
  - $\vdots$
  - Product of roots: $r_1r_2\ldots r_n = (-1)^n\frac{a_0}{a_n}$
- **Symmetric Functions of Roots:** These are expressions involving the roots of a polynomial that remain unchanged when any two roots are swapped. Vieta's formulas provide the elementary symmetric functions. Other symmetric functions can be expressed in terms of these elementary ones.
- **Transformation of Equations:** This involves creating a new polynomial equation whose roots are related to the roots of a given equation by some transformation (e.g., $y = f(x)$). Common transformations include:
  - Roots multiplied by a constant: If roots are α_i, new roots are $k\alpha_i$. Replace x with y/k.
  - Roots are reciprocals: If roots are α_i, new roots are $1/\alpha_i$. Replace x with $1/y$.
  - Roots shifted: If roots are α_i, new roots are $\alpha_i + k$. Replace x with $y - k$.

5.2 Descartes' Rule of Signs:

- **Purpose:** This rule provides information about the maximum number of positive and negative real roots of a polynomial equation.
- **Positive Real Roots:** Count the number of sign changes in the coefficients of $P(x)$ (ignoring zero coefficients). The number of positive real roots is equal to this count, or less than it by an even number.
- **Negative Real Roots:** Count the number of sign changes in the coefficients of $P(-x)$. The number of negative real roots is equal to this count, or less than it by an even number.

PYQ Focus: Applying transformations to equations to find new equations with related roots, and using Vieta's formulas to establish relationships between roots and coefficients.

6 Group Theory Basics

Group theory is a branch of abstract algebra that studies algebraic structures known as groups.

6.1 Binary Operations:

A binary operation $*$ on a set G is a rule that assigns to each ordered pair of elements (a, b) in G a unique element $a * b$ in G.

- **Closure:** For all $a, b \in G$, $a * b \in G$. (The result of the operation stays within the set).
- **Associativity:** For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$. (The order of operations doesn't matter for three or more elements).
- **Identity Element:** There exists an element $e \in G$ (called the identity) such that for all $a \in G$, $a * e = e * a = a$.
- **Inverse Element:** For every $a \in G$, there exists an element $a^{-1} \in G$ (called the inverse of a) such that $a * a^{-1} = a^{-1} * a = e$ (where e is the identity element).

6.2 Definition of a Group:

A set G with a binary operation $*$ is called a **group** if it satisfies the following four axioms:

1. **Closure:** For all $a, b \in G$, $a * b \in G$.
2. **Associativity:** For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
3. **Identity Element:** There exists an element $e \in G$ such that for all $a \in G$, $a * e = e * a = a$.
4. **Inverse Element:** For every $a \in G$, there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

6.3 Types of Groups:

- **Abelian (Commutative) Group:** A group $(G, *)$ is Abelian if, in addition to the four group axioms, it satisfies the commutative property: $a * b = b * a$ for all $a, b \in G$.
- **Finite Group:** A group is finite if the set G has a finite number of elements. The number of elements is called the order of the group, denoted $|G|$.
- **Group Tables (Cayley Tables):** For finite groups, a group table can be constructed to show the result of applying the group operation to every pair of elements. These tables are useful for verifying group properties for small groups.

PYQ Focus: Proving that a given set with a defined operation forms a group. This requires meticulously checking all four (or five, if Abelian) group axioms.

7 Subgroups and Cyclic Groups

7.1 Subgroups:

- **Definition:** A non-empty subset H of a group G is a **subgroup** of G if H itself forms a group under the same binary operation defined on G.

- **Subgroup Test (One-Step Subgroup Test):** A non-empty subset H of a group G is a subgroup if for all $a, b \in H$, $ab^{-1} \in H$. (Here, b^{-1} refers to the inverse of b in G).

- **Two-Step Subgroup Test:** A non-empty subset H of a group G is a subgroup if:

  1. For all $a, b \in H$, $ab \in H$ (Closure under the operation).
  2. For all $a \in H$, $a^{-1} \in H$ (Closure under inverses).

7.2 Cyclic Groups:

- **Definition:** A group G is called a **cyclic group** if there exists an element $a \in G$ (called a generator) such that every element in G can be expressed as a power of a (i.e., a^n for some integer n). We denote this as $G = \langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.

- **Properties of Cyclic Groups:**

  - Every cyclic group is Abelian.
  - Subgroups of a cyclic group are also cyclic.
  - For a finite cyclic group of order n, generated by a, the distinct elements are $e, a, a^2, \ldots, a^{n-1}$.

- **Order of an Element:** The order of an element a in a group G, denoted $|a|$ or $o(a)$, is the smallest positive integer n such that $a^n = e$ (where e is the identity element). If no such positive integer exists, the element has infinite order.

  - In a finite group, the order of an element divides the order of the group (Lagrange's Theorem, though not explicitly in your notes, is highly relevant here).

PYQ Focus: Finding all subgroups of a given cyclic group. This often involves understanding the orders of elements and using properties of cyclic groups.

8 Permutations and Symmetric Groups

This section introduces permutations, which are bijections of a set to itself, forming an important class of groups.

8.1 Permutations:

- **Definition:** A permutation of a set A is a bijection (one-to-one and onto function) from A to itself.
- **Notation:**
  - **Two-line notation:** $\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}$
  - **Cycle notation:** A compact way to represent permutations. For example, (1 2 3) means 1 maps to 2, 2 maps to 3, and 3 maps to 1. An element not listed is mapped to itself. Disjoint cycles commute. Example: (1 2 3)(4 5).
- **Transposition:** A cycle of length 2, e.g., $(a\ b)$. Any permutation can be written as a product of transpositions.

8.2 Symmetric Group S_n:

- **Definition:** The symmetric group S_n is the set of all permutations of a set with n elements (usually $\{1, 2, \ldots, n\}$), under the operation of composition of functions.
- **Order:** The order of the symmetric group S_n is $n!$ (n factorial), which is the total number of distinct permutations of n elements.
- **Non-Abelian:** For $n \geq 3$, S_n is non-Abelian (i.e., permutation composition is not commutative).

8.3 Even and Odd Permutations:

- **Sign of a Permutation:** Every permutation can be expressed as a product of transpositions. While this factorization is not unique, the parity (even or odd number of transpositions) is unique.
  - **Even Permutation:** A permutation is even if it can be written as a product of an even number of transpositions. Its sign is +1.
  - **Odd Permutation:** A permutation is odd if it can be written as a product of an odd number of transpositions. Its sign is -1.
- **Alternating Group A_n:** The set of all even permutations in S_n forms a subgroup called the alternating group A_n. Its order is $n!/2$.

PYQ Focus: Expressing a given permutation as a product of disjoint cycles and then as a product of transpositions, and subsequently classifying it as an even or odd permutation.

9 PYQ Practice Topics (Frequent)

This table summarizes the types of questions frequently asked in exams, correlating with the above topics:

Topic	**Type of Question**
Relations	Equivalence relation & partition
Euclidean Algorithm	GCD and linear combination
Modular Arithmetic	Linear congruence, modulo inverse
Complex Numbers	De Moivre's Theorem and applications
Theory of Equations	Roots & coefficient transformations
Group Theory	Prove set is a group
Subgroups	Identify subgroups, cyclic groups
Permutations	Express and classify permutations