1 Preliminaries

Abstract algebra is the study of the structures, also known as **Algebraic Structures**, provided by operations (mappings between elements) on sets. Of these structures, a traditional first course in Abstract Algebra covers the theoretical aspects of groups, rings, and fields.

Contents of MATH 4323

These notes cover the contents of my Abstract Algebra I course (MATH 4323). This includes: proofs, induction, the division algorithm, congruences and symmetries, groups, subgroups, cyclic groups, repeated squaring, complex numbers, permutations, dihedral groups, cosets, Lagrange's Theorem, Fermat's and Euler's Theorems, private key cryptography, public key cryptography, isomorphisms, direct products, normal subgroups, simplicity of A_n, homomorphisms, isomorphism theorems, matrix groups, finite Abelian groups, solvable groups, group actions, the Class Equations, Bursinde's Counting Theorem, the Sylow Theorems, applications of the Sylow Theorems.

1.1 Set Theory

A basic knowledge of set theory, mathematical induction, equivalence relations, and matrices is a must. Even more important is the ability to read and understand mathematical proofs.

A Short note on Proofs

Although mathematics is often motivated by physical experimentation or by computer simulations, **mathematics is made rigorous through the use of logical arguments**.

Definition: Axiomatic Approach to Abstract Mathematics

In studying abstract mathematics, we take what is called an **axiomatic approach**; that is, we:

- take a collection of objects $\mathcal{S}$, and
- assume some rules about their structure.

Rules about the structure of elements in a set are called **axioms**. With a **set** and a **system of axioms**, we can achieve the following:

- derive other information about S by using logical arguments
- derive other information that does not contradict one another
- not include redundant axioms
- provide enough flexibility to investigate many kinds of mathematical objects

A **proposition** in logic or mathematics is an assertion that is either true or false. A **mathematical proof** is nothing more than a convincing argument about the accuracy of a proposition. Mathemeticians are interested in statements like "if p, then q." Here p is called the **hypothesis** and q is known as the **conclusion**. Many mathematical conclusions are derived from a chain of hypotheses and conclusions.

The following are useful facts about proofs. Never assume any hypothesis that is not explicitly stated in the theorem; you cannot take things for granted. To show that an object is unique, assume that there are two such objects, say r and s, and then show that r = s. Sometimes it is easier to prove the contrapositive of a statement. Although it is better to find a direct proof of a theorem, this task can sometimes be difficult. Use contradiction: assume the theorem is false and show that the assumption makes some statement that cannot possibly be true.

Definition: Set

A **set** is a well-defined collection of objects; that is, it is defined in such a manner that we can determine for any given object x whether or not x belongs to the set.

We can find various relations between sets as well as perform operations on sets.

Example: Subsets

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

When two sets have no elements in common, they are said to be **disjoint**; for example, if E is the set of even integers and O is the set of odd integers, then E and O are disjoint.

Definition: Difference of Sets

We define the difference of two sets A and B to be:

$$A \setminus B = A \cap B' = \{x : x \in A, x \notin B\}$$

Theorem: De Morgan's Laws

Let A and B be sets. Then

- $(A \cup B)' = A' \cap B'$
- $(A \cap B)' = A' \cup B'$

Proof: □

1.2 Cartesian Products and Mappings

Given sets A and B, we can define a new set $A \times B$, called the **Cartesian product** of A and B, as a set of ordered pairs.

Definition: Cartesian Product

Let A and B be sets. Then the **Cartesian product** of A and B,

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

We define a **Cartesian Product of n sets** to be

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i \text{ for all } i \in \{1, \ldots, n\}\}$$

In general, if $A_1 = \cdots = A_n$, we often write A^n to denote $A \times \cdots \times A$ where A would be written n times. A mathematical **relation** encodes the common concept of relation: an element x is related to an element y, if and only if the pair (x, y) belongs to the set of ordered pairs that defines the binary relation. Subsets of $A \times B$ are called **binary relations**. Subsets of $A_n \times \cdots \times A_n$ are called **n-ary relations.**

Example: $\mathbb{R}^3$

The set $\mathbb{R}^3$ consists of all 3-tuples of real numbers.

Mappings

Definition: mappings, functions

We will define a **mapping** or **function** from $f \subset A \times B$ from a set A to B to be the special type of binary relation where the relation f is

- **functional** (also called right-unique) if:

$$\forall x \in A, \forall y \in B, \forall z \in B, \quad ((x, y) \in f \wedge (x, z) \in f) \implies y = z;$$

- **serial** (also called left-total) if:

$$\forall x \in A, \exists y \in B, \quad (x, y) \in f.$$

Instead of writing down ordered pairs $(a, b) \in f \subset A \times B$, mathematicians will usually denote that f is a function from set A to set B by optionally writing $f : A \to B$ or $A \overset{f}{\mapsto} B$ followed by an expression that f satisfies for all $a \in A$. When the domain is obvious, mathematicians will usually forego meantioning the sets under the relation f.

Definition: Domain

The **domain** or set of departure of a function is the set into which all of the input of the function is constrained to fall.

Definition: Range, Image

The **range** or **image** or set of destination of a function $f : A \to B$ of all output values it may produce. The range of f is denoted by,

$$f(A) = \{b \in B : \exists a \in A, \text{ with } g(a) = b\}$$

Definition: Composition

Let $f : A \to B$ and $g : B \to C$ be mappings between sets. Define a new map, the **composition** of f and g from A to C, by

$$g \circ f = g(f(a))$$

for all $a \in A$.

The domain and codomain are not always explicitly given when a function is defined, and one might only know that the domain is contained in a larger set. Typically, this occurs in mathematical analysis, where "a function from X to Y " often refers to a function that may have a proper subset of X as domain. For example, a "function from the reals to the reals" may refer to a real-valued function of a real variable. However, a "function from the reals to the reals" does not mean that the domain of the function is the whole set of the real numbers, but only that the domain is a set of real numbers that contains a non-empty open interval. Such a function is then called a partial function.

Theorem: Invertable iff one-to-one

A mapping is invertable if and only if it is both one-to-one and onto.

Proof: □

Equivalence Relations

A fundamental notion in mathematics is that of equality. We can generalize equality with equivalence realtions and equivalence classes.

Definition: Equivalence Relation

An **equivalence relation** on a set X is a relation $R \subset X \times X$ such that

- $(x, x) \in R$ for all $x \in X$ (**reflexive property**)
- $(x, y) \in R$ implies $(y, x) \in R$ (**symmetric property**)
- $(x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R$ (**transitive property**)

Notation:

We usually write $x \sim y$ instead of $(x, y) \in R$. If the equivalence relation already has an associated notion such as $=$, $\equiv$, or $\cong$.

Example:

Let p, q, r, and $s \in \mathbb{Z}$ where $q \neq 0 \neq s$. Define $p/q \sim r/s$ if $ps = qr$.

Theorem: Partition for every equivalence relation

Given an equivalence relation $\sim$ on a set X, the equivalence classes of X form a partition of X. Conversely, if $\mathcal{P} = \{X_i\}$ is a partition of a set X, then there is an equivalence relation on X with equivalence classes X_i.

Proof:

□