Foundations of Abstract Mathematics

Part1: Groups, Rings, Fields and Modules

Raoof Mirzaei

(Last revised: September 23, 2015)

Dedicated to Neda

Contents

Preface

This book is intended for mathematicians who are not satisfied with ambiguity of definitions and consideration in Abstract Mathematics, in particular Abstract Algebra. As it is know Logic and set theory is the backbone of pure mathematics and every branch of study is build upon it, So The Part I, incuding chapter 1 to 4 is the foundation of set theory from the begining, without almost any harm!

As we proceed in following chapters I try to take back every modern consept and definition into our base language we defined in set theory.

In Part II We strat to giving an structure to a set which we will call Groups, with the consept of an n-ary operation which is a generalisation of a function that we defined before and some other axioms.

In Part III We will continue with structures, with two n-ary operation, and introduce Fields, Ring and their Modules.

In Part IV We will discuss the famous "told story" of Galois theory in complete detail.

In Part V We will talk enough about what we have established Using Category theory.

In Part VI We will eventually get to the main goal of this book: thinking over new stories about Galois theory.

Chapter 0

What is Abstract Algebra

> *It was a shocking discovery of course that Newton's laws are wrong ... we now have a much more humble point of view of our physical laws : EVERYTHING CAN BE WRONG.*
>
> Richard Feynman,

We all are familiar with the notion of algebra from high school. The word abstract might seems weird at the first look. Iranian Mathematiton Mohammad Khawarizmi first used the word al-jabr meaning balencing or reduction. Although the modern algebra is completly different from the ancient algebra,but it has something to do with it. If you ask someone randomly about algebra you will probably get : An unknown stupid game with the unknown variable x. Then, what if you ask about abstract algebra ? Probably if you ask this question they dont notice the change. If someone asks me what is abstract algebra ? I simply answer : It is an abstract approach to algebra. What does this mean? Is it just a nice fancy statement ? I claim no. Abstract Algebra is the formal structure of our mathematical intuition. At the beggining we simply used mathematics to satisfy our intentions. At first we would like to have measurement , well that is not abstract at all, on the contrary it is very intutive. That is why we first start to introduce numbers, to count our sheep for example. I call this event The birth of Mathematics. That is what we call today a natural number. The set of natural numbers is called N. Then we generalise this idea to get an integer number system, the one including

the natural numbers, and their negatives, together with zero. We do not stop, we keep on going to generalise this to the rational number system, the set consisting of all fractions except when the denominator is zero. Then we construct other number systems for our perposes, the real numbers, consisting of all points in a continuous geometric line. We did it because the rational numbers were not enough. I used the word enough. Enough for what? Enough for who? In Mathematics everything must be defined precisely. If someone uses the number of his sheep, the integers are more than enough. the number of sheeps can not be 2.576 . If he owes someone we can say he has -4 sheep for example. In Mathematics we would like to solve equations and real numbers are not enough to contain the solution of every algebraic equation. So again we extend real numbers to get a another space for which every algebraic equation has a solution in that number system which is called the complex numbers. The first number system which is in 2 Dimensions. Before this we worked with 1 Dimensional world. Now, is this enough ? Enough for what? Enough for who? If we want to solve an algebraic polynomial equation it turns out that the fundamental theorem of algebra guarantees every such equation has all of its solutions in complex numbers.

But we can go on and generalise again to get number systems in higher dimensions. One such generalisation is Cayley Dickson Construction which from we get hypercomplex systems in in 4 (Quaternions); 8 (Octonions); 16 (sedenions); and in general $2n$ dimensions (an algebra is merely a vector space, A, equipped with a bilinear map which prescribes the multiplication of vectors. The Cayley-Dickson Process affords a means of building a larger algebra, B, which contains A as a subalgebra)

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O} \subset \mathbb{S}$$

$$\begin{aligned} \mathbb{N} &= \{1, 2, 3, \dots\} \\ \mathbb{Z} &= \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} \\ \mathbb{Q} &= \{\frac{n}{m} : n, m \in \mathbb{Z} \text{ and } m \neq 0\} \end{aligned}$$

Every highschool student obviusly knows on this number system we have $a + b = b + a \ \ \forall a, b \in R$

$(a \times b) \times c = a \times (b \times c)$

They think that is always so , but it is not.

For quaternions, a number system in 4 dimensions, the multiplication commutativity fails i.e. $a \times b \neq b \times a$

But associativity still holds i.e.

$(a \times b) \times c = a \times (b \times c)$

But interestingly for octionions associativity fails too. $(a \times b) \times c \neq a \times (b \times c)$

Abstract algebra is about generalizing these number systems and studying the properties of these number systems and classifiying them up to their structure. We do so by considering sets toghter with operation(s) defined on that set and cheking axioms they satisfy. For example

$(\mathbb{Z}, +) \Rightarrow$ Group

$(\mathbb{Z}, +, \times) \Rightarrow$ Ring

$(Q, +, \times) \Rightarrow$ Field

$(\mathbb{R}^n, +) \Rightarrow$ Vector spaces over $\mathbb{R}$

Part I

Sets and First-Order Logic

Chapter 1

Set Theory

> *Zeno was concerned with three problems . . . These are the problem of the infinitesimal, the infinite, and continuity . . .*
>
> Bertrand Russell,

Set theory is the foundation of mathematics. Almost all branches of study are built up from the concepts somehow derived from it. So as a backbone of all mathematics it needs to be well established. The beginning of mathematics is concerned with counting and measurement, and these are described in terms of numbers and arithmetic. Even arithmetic can be derived from sets, Namely those finite sets whose elements are also finite sets, the elements of which are also finite, and so on, which is called pure sets is formally equivalent to arithmetic. Since set theory plays the role of forerunner to arithmetic, it seems to be a good candidate for the foundation of almost all mathematics.

In fact, set theory can be studied as:

- Set Theory as a foundation for mathematics
- Set Theory as a subject

Set Theory as Foundation

At the end of the 19th century, mathematicians became concerned that the did not fully understand the nature of the basic mathematical notions. For example:

> What is a number? We understand the set $\mathbb{N}$ of natural numbers intuitively, but what is the real foundation for that? Even if we accept naturals and

rationals, we have so much difficulties with real numbers ? What is the meaning of a function $f : \mathbb{R}^2 \to \mathbb{R}^2$?

The reason that mathematicians become so concern was because of rising some paradoxes in set theory.

So the most logical way seems to be : seeking for a strong foundations. What better than set theory, since it starts with a limited number of *axioms* from logic that is based on humans pure mind atleast apparently.

Once we stablished a good foundations, it is turn for the other subjects, such as: Number theory, Analysis, Probability , etc to build on it.

Or—we can do something simpler: show that all of mathematics can be reduced to (encoded in) set theory. We must show that the notions of real number, function, and so on can be *defined* inside set theory in such a way that these notions have the correct properties. For the reals, this includes:

- Laws of arithmetic in ;
- Completeness of the ordering (least upper bound principle)

Calculus can be developed rigorously in terms of the theory of limits, if the reals have these fundamental properties.

Set Theory as a subject

This involves understanding the sizes of infinite sets in two ways:

- Comparison of size: cardinality
- Counting: ordinals

It leads to the study of *well ordering* and *the axiom of choice* and eventually to a picture of the universe of all sets called *the Cumulative Hierarchy*.

1.1 Origin

Set theory had some revolutions from the word go. Set theory, began with the work of Georg Cantor[1] and Richard Dedekind in the 1870's.it came to born by a single paper in 1874 by Georg Cantor: "On a Characteristic Property of All Real Algebraic Numbers".[1]

[1]Georg Cantor is a great German mathematician who opend the door of thinking about different kinds of infinity..

Cantor himself gave in a publication in 1895 a description of the term set.

A set is a gathering together into a whole of definite, distinct objects of our perception or of our thought. These objects are called elements of the set. The question about what actually the word set means is a fundamental question and fundamental problem in the subject. One of the difficulties is that the word set is common word in any informal language, and some of the definitions of set are as following:

1. A number of things of the same kind that belong or are used together (Webster)

2. A group of things that belong together (Cambridge)

3. A group or collection of things that belong together or resemble one another or are usually found together (Oxford)

In these definition the notion of a set is very general, because there is no restriction on the nature of the things which may be elements of a set. If we want to take this word and apply it to mathematics, we need to be much more precise to define what it means in a mathematical sense. In the naive set theory we consider every well-defined collection of objects to be a set. The problem with this definition is that the terms ‘collection’ , ‘object’ and ‘well-defined’ are themselves undefined. there is a problem of circularity for defining the primitive concepts like set,point,line,etc. for example you can start by: a set is a collection, then it comes to ask what is a collection, then you say a collection is a family, a family is a group , a group is a class and eventually we get back to where we started. So we consider set as a primitive concept and defining everything else in terms of sets. I don’t know whether it is possible or not, but most of the community of mathematicians agree with that.

1.2 Classification

Set theory is classified in several different ways, but in general there are two approaches to set theory:

1. Naive Set Theory

2. Axiomatic Set Theory

Naive Set Theory

Set theory was introduced to clarify paradoxes of infinite size.

For example, The paradox of the Even Numbers (Bolzano Paradox) : There are as many even natural numbers as natural numbers?

- The answer is yes, because for every natural number n there is a even natural number $2n$, and Vice versa.
- The answer is no, because the evens are a proper subset of the naturals: every even number is a natural number but there are natural numbers, which are even.

To solve this paradox and in general whenever it comes to infinity we need to be precise about what is meant by size.

Cantor's notion of sets makes this clear. The first development of set theory is called *naive set theory* . It was created at the end of the 19th century by Georg Cantor as part of his study of infinite sets.

He established the notion of a one-to-one correspondence and proved a theorem now called the Cantor-Schroeder-Bernstein Theorem which is used for proving equivalence of two sets. the theorem states that if there exists a one-to-one function from $A \longmapsto B$ (not necessarily onto) and a one-to-one function from $B \longmapsto A$ (not necessarily onto), then there exists a bijection from one set to the other; i.e. the two sets are equivalent. Using this theorem paradoxes like the former are solved. Cantor showed there was no one-to-one correspondence from N to R , and hence the natural numbers have a smaller cardinality than the real numbers.

Cantor thought if we can add numbers with each other then we can be able to add infinity and infinity. He realized that it was actually possible to add and subtract infinities, and that beyond what was normally thought of as infinity existed another, larger infinity, and then other infinities beyond that.

Cantor showed that there is more than one kind of infinity. Before him it was assumed that all kinds of infinity having the same number of elements as it seems even today with our intuition. Cantor proved using his well known diagonal argument, that the collection of real numbers has more elements than integers, but surprisingly the integers and rationals have the same number of elements. In other words,Unlike integers and rational numbers, the real numbers are not countable. So, however infinite the infinity is, there are infinite kinds of infinity, so he divided numbers into two classes, countable and uncountable. A set that has a larger cardinality than the natural numbers is called uncountable.

In set theory all existing objects are sets. If an object exists it is a set otherwise it does not exist. To remind us of the fact that sets include elements we sometimes refer to sets as a collection of sets, or as a families of sets. This is just a "human factors" trick since the theory makes no distinction between sets, families, collections or elements. In axiomatic set theory elements, collections, and families are just sets.

So Cantor's set theory solved these kinds of paradoxes,but nothing is over in the world of mathematics. Yes, it solved some paradoxes, but created others So after Cantor another mathematician came along and tried to rebuild set theory in a way that got free of these new paradoxes.

In naive set theory (NST) we define concepts informally based on natural language.

The words and, or, if ... then, not, for some, for every are not here subject to rigorous definition, it is an approach to set theory which assumes the existence of a universal set, despite the fact that such an assumption leads to paradoxes. Frege constructed a formal theory which is the axiomatization of naive set theory.

Axiomatic Set Theory

Axiomatic set theory was developed with the purpose of eliminating paradoxes which occured, with the goal of determining precisely what operations were allowed and when.

Structure of set theory and other fields constructed upon it has the three following following elements:

1. Variables (e.g., $a, b, ..., x, y, z$) which stand for sets.
2. The predicate $\in$, which stands for element inclusion
3. Logical operators and symbols include
   (a) $\neg P$, where $\neg$ is the logical "negation" operator.(not)
   (b) $\wedge P$, where $\wedge$ is the logical "and" operator.(and)
   (c) $\vee P$, where $\vee$ is the logical "or" operator.(or)
   (d) $P \implies P$, where $\implies$ is the logical "implication" operator.(implies)
   (e) $P \iff P$, where $\iff$ is the logical "bijection" operator.(if and only if)
   (f) $\forall\, x\ P$ is the logical "for-all" quantifier.(for all)

(g) $\exists\ x\ P$ is the logical "exists" quantifier.(there exists)

(h) $\exists!\ x\ P$ is the logical "exists" quantifier.(there exists exactly one,unique)

In set theory all propositions are constructed from the non-logical predicate $\in$ and connected to each other using these logical operators. propositions.

Tautology table of propositions is here:

P	Q	$P \vee Q$	$P \wedge Q$	$\sim (P \wedge Q)$	$(P \vee Q) \wedge \sim (P \wedge Q)$
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

P	Q	$P \implies Q$	$Q \implies P$	$P \iff Q$	$\sim (P \iff Q)$
T	T	T	T	T	F
T	F	F	T	F	T
F	T	T	F	F	T
F	F	T	T	T	F

In Zermelo-Fraenkel set theory this notion of equality is taken as an axiom. In fact, all of the definition and axiom in naive set theory with the pioneer work of Cantor is axiomatized as 3 axiom in ZFC (Zermelo-Fraenkel with the axiom of choice)

has two axioms: The Axiom of Extensionality.

First, I use the approach of naive set theory, That is defining concepts intuitively but for avoiding duplication I try to make it similar to axiomatic approach as much as possible. I call this axiomatic approach to naive set theory or Frege axomatization of NFS.

Then we see some paradoxes will occur, and naive set theory falls. Then we proceed in a way to rescue set theory from these paradoxes. After that I briefly talk about ZFC.

1.3 Basic Definitions and Axioms

A set is an unordered collection of distinct elements or objects .[2] These elements can be anything like numbers, letters, logical proposition, points in arbitrary

[2]In this definition we assume these elements or objects are distinct.

space ,etc. Sets even may include sets as their elements. You are familiar with sets of numbers, that is a set consisting of numbers. We have several kind of number system. We can generalize this notion of a set to consists things other than numbers. These kind of generalization is called abstraction. Number themselves are abstraction of things. We could simply count our sheep without having a formal theory of natural numbers.

If A is a set, then the objects in the collection A are called either the members of A or the elements of A.

When we talk about a set as a collection of objects it is natural to ask "what does it consist of ?".

This motivates the notion of membership. Membership is a binary relation [3] $\in$ between an object o and a set A.

We write $o \in A$ to indicate that the object o is an element, or a member, of the set A . We also say that o belongs to A , that o is contained in A , or simply that o is in A .The negation of $o \in A$ is $\neg($ o $\in A)$ which is denoted by o $\notin A$.

We use capital letters to display a set and small letters to denote its element and put the elements of a set between brackets , For example $S = \{a, b, c\}$ and $T = \{\{a, b, c\}, \{a, c\}, b, c\}$.

A set can consists of only one element, so given an object x we can form the set that has x as its only element which is denoted by $\{x\}$.

Likewise, for any two objects x and y, we can form the pair set $\{x, y\}$ consisting of just the elements x and y.

More generally, for any objects $x, y, z, \ldots$ we can form the set having $x, y, z, \ldots$ as its elements, which we denote by $\{x, y, z, \ldots\}$

A set containing only one element is called a singleton. This set $\{x\}$ is not the same as x, because, x is an element while the singleton $\{x\}$ is like a basket that has x as its element. That is, $x \in \{x\}$, but not that $x \in x$.

Even worse, a set that has no element at all is called an ***empty set*** or ***null set*** denoted by $\{\ \}$ or $\emptyset$. The existence of empty set is stated as an axiom in *Axiomatic set theory* called *axiom of empty set*[4] and the uniqness of empty set is obtained from the axiom of extensionality which we will discuss below.

[3] Consider it as just a relation for now, we will define binary relation in terms of sets later.

[4] This axiom is stronger condition from the axiom of specification.

Definition 1.3.1 *(Cardinality)* The number of elements in a set A is called its cardinality or order, and denoted by $\mid A \mid$ *or* $n(A)$.

For example, if $T = \{\{a, b, c\}, \{a, c\}, b, c\}$, then $\mid T \mid = 4$

A set which has only a finite number of elements is called a finite set .i.e. A set is said to be a finite set if all of its elements can be listed, this include the condition that set has no elements.

otherwise A is an infinite set.

Definition 1.3.2 *(Equivalent Sets)*

Two sets A and B are said to be equivalent if their cardinal number is same, $i.e.$, $n(A) = n(B)$. The symbol for denoting an equivalent set is ‘’.

For example:

$A = \{a, b, c\}$; n(A) = 3

$B = \{1, 2, 3\}$; n(B) = 3

Therefore, A $\longleftrightarrow$ B

Since sets are objects themselves, the membership relation can be defined on two set. A binary relation between two sets is the subset relation $\subseteq$.

Definition 1.3.3 *(Subset)* Suppose A and B are sets. the expression $A \subseteq B$, $i.e.$ B contains all the elements of A is defined in terms of membership by

$$\forall x(x \in A \Rightarrow x \in B) \tag{1.1}$$

Then A is said to be a subset of B .

Furthermore, $A \subset B$ if

$$\forall x(x \in A \Rightarrow x \in B) \wedge \exists x \in B s.t.\ x \notin A$$

(1.2)

, i.e. there is an element of B which is not in A . In this case we call A a proper subset of B (or that A is strictly contained in B) . In other word, a subset of A is proper if it is neither A itself nor $\emptyset$.

The set B is also called a superset of A .

Remark According to this definition, for every set A , $A \subseteq A$, $\emptyset \subseteq A$

Clearly, two sets A and B are equal if they contain the same elements , i.e.

$$A = B \text{ if and only if } \forall x(x \in A \Rightarrow x \in B) \wedge \forall x(x \in B \Rightarrow x \in A) \tag{1.3}$$

where $\wedge$ denotes logical AND.

Equivalently

$$A = B \text{ if and only if } (A \subseteq B \wedge B \subseteq A) \tag{1.4}$$

This is called the axiom of extentionality.

Axiom of Extensionality The axiom of extensionality says that a set is defned by its members, so sets formed by the same elements are equal,

$$\forall A \forall B[\forall x(x \in A \iff x \in B) \Rightarrow A = B]. \tag{1.5}$$

This implies, for example, that empty set (if it exists) is unique. Since $\emptyset$ has no elements at all and it is the only set with no elements, so by extensionality any two such sets must be equal.

This axiom and definition has the direct consequence that within sets, there is no order. For example if $A = \{a, b\}$ and $B = \{b, a\}$ then $A = B$

What about repetition? Does it matter?

Are $A = \{a, b\}$, $B = \{a, a, b, b, b, c\}$ and $C = \{a, b, c, b, b\}$ equal?

According to equality definition

$$\forall x \in A \Rightarrow x \in B, C \ \wedge \forall x \in B, C \Rightarrow x \in A.$$

But according to cardinality definition of a set the number of elements in A, B and C are 3 , 6 and 5 respectivly.

Counting the number of elements in a set is like you have a basket and you close your eyes and take element one by one so you wont notice if you pick an element

more than once. Against all of the elementry set theory books, unlike ordering repetiton in a set matters. So non of the A, B and C are equal.

Note that, we dont consider collections that have multiple copies of the same element in the set. In other word a set is a collection that has distinct elements. So by this contract B and C are not sets, they are called ***multisets***.

Multisets are extension of the idea of a set that unlike a set can have multiples of the elements.

The number of repetition of an element in amultiset is called ***multiplicity***. The elements of multisets usually represented in square brackets [ ]. for example $C = [a, b, c, b, b]$ is not a set but a multiset.

The idea of multisets arise from the work of Dedekind, and is a quite rich subject. We dont want to get into this but here I give a formal definition of multiset and its relation with our familiar sets.

Multiset is a pair (A, m) where A is a set and $m\colon A \to \mathbb{N}$ is a function from A to the set N = $\{1, 2, 3, \dots\}$

For each $a \in A$ the multiplicity of a is the number $m(a)$.

If

$$\forall a\ m(a) = 1$$

then we have a simple set. In other word a set is a mutiset $(A, 1)$, i.e. each element in the multiset occurs just once.

In A the multiplicity of elements are : $a = 1$, $b = 1$ and $c = 1$

In B the multiplicity of elements are : $a = 2$, $b = 3$ and $c = 1$

In C the multiplicity of elements are : $a = 1$, $b = 3$ and $c = 1$

1.4 Operations on Sets

There are various natural operations we can perform on sets. (They are analogue of addition, multiplication, and subtraction for numbers.) There are a number of simple operations that can be performed on sets, forming new sets from given sets.(They are analogue of addition, multiplication, and subtraction for numbers.)

Definition 1.4.1 (Union and Intersection) Given any two sets A and B;

(i) The Union $A \cup B$ of A and B is the set which consists of all the elements of A and all the elements of B such that no element is repeated. The union of two given sets is the smallest set which contains all the elements of both the sets.

$$A \cup B = \{x | (x \in A) \vee (x \in B)\}$$

(ii) The Intersection $A \cap B$ of A and B is the set which consists of all elements that belong to both A and B. That is, the largest set which contains all the elements that are common to both the sets And has the formal definition

$$A \cap B = \{x | (x \in A) \wedge (x \in B)\}$$

Furthermore, the operations are commutative. That is,

$$A \cup B = B \cup A, \;\; A \cap B = B \cap A$$

And associative. That is,

$$A \cup (B \cup C) = (A \cup B) \cup C, \;\; A \cap (B \cap C) = (A \cap B) \cap C$$

This is an analogy between sets and numbers[5] , in numbers addition $+$ and multiplication $\times$ is commutative.

We have commutative laws $x + y = y + x$ and $x \times y = y \times x$, and also associative laws $x + (y + z) = (x + y) + z$ and $x \times (y \times z) = (x \times y) \times z$.

The set theoretic distributive laws are

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \;\; A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Which are called Demorgan law and corresponds to number distributive law. $x \times (y + z) = x \times y + x \times z$.

But this analogy is not always true. For example, $A \cap A = A$ is an identity for sets but in algebra $a \times a = a$ is not an identity.

Example 1.4.2 (i) Let $A = \{-3, 7, 0, 8, 10\}$ and $B = \{1, 8, 3, 7, 0, 6\}$.

Then $A \cup B = \{-3, 7, 7, 0, 8, 10, 1, 3, 6\}$ and $A \cap B = \{0, 8\}$.

[5]Numbers that are subsets of complex number, because for example Quaternion are not commutative. Octonion are not even associative.

(ii) Let $X = \{a, b, c\}$ and $Y = \{\emptyset\}$.

Then $A \cup B = \{a, b, c, \{\emptyset\}\}$ and $A \cap B = \emptyset$.

Two set A and B are called disjoint or not connected if and only if $A \cap B = \emptyset, i.e.$ they have no elements in common. For example, the set of even numbers and the set of odd numbers are disjoint.

Definition 1.4.3 (Universal Set)

A Universal Set is a fixed set under consideration and consisting of all objects considered in the theory.

It is not necessary the set of everything in the world. for example, when we talk about ordinals, natural numbers can be considered as a universal set. It is usualy denoted by U.

The complement of the universal set is the empty set

Definition 1.4.4 (Complement)

Suppose U is the universal set and A is a subset, then the complement of A denoted by $\overline{A}$ or A^c is the set consisting of all the elements of U which are not the elements of A.

$\overline{A} = \{x \in U : x \notin A\}$

Definition 1.4.5 (Relative Complement)

If A and B are sets, then the set theoretic difference of A and B, also known as relative complement of B relative to A is the set of all those elements of A which do not belong to B, denoted by $A \setminus B$ or $A - B$

$$A \setminus B = A - B = \{x | x \in A \wedge x \notin B\}$$

This is analoge of subtraction in numbers but not exactly, so we call it set theoretic difference.

Definition 1.4.6 *(Symmetric differences)*

The symmetric difference of two sets A and B is the set of all objects that are in one and only one of the sets. The symmetric difference is written $A \Delta B$.

$$A \Delta B = \{(A \setminus B) \cup (B \setminus A)$$

1. Commutative Laws

$$(a) A \cup B = B \cup A$$

$$(b) A \cup B = B \cup A$$

2. Associative Laws

$$(a) A \cup (B \cup C) = (A \cup B) \cup C$$

$$(b) A \cap (B \cap C) = (A \cap B) \cap C$$

3. Distributive Laws

$$(a) A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$(b) A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

4. Identity Laws

$$(a) A \cup \emptyset = A$$

$$(b) A \cap U = A$$

5. Inverse Laws

$$(a) A \cup \overline{A} = U$$

$$(b) A \cap \overline{A} = \emptyset$$

6. Double Negation Law

$$\overline{\overline{A}} = A$$

7. Idempotent Laws

$$(a) A \cup A = A$$

$$(b) A \cap A = A$$

8. DeMorgan's Laws

$$(a) \overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$(b) \overline{A \cap B} = \overline{A} \cup \overline{B}$$

9. Domination Laws

$$(a) A \cup U = U$$

$$(b) A \cap \emptyset = \emptyset$$

10. Absorption Laws

$$(a) A \cup (A \cap B) = A$$

$$(b) A \cap (A \cup B) = A$$

11. Complements of U and $\emptyset$

$$(a)\overline{U} = \emptyset$$
$$(b)\overline{\emptyset} = U$$

12. Consistency Principle

$$(a)A \subseteq B \iff A \cup B = B$$
$$(b)A \subseteq B \iff A \cap B = A$$

Proof We shall proof (2.a), (3.a), (5.a), (5.b), 6 and (8.a). The others left to readers.

2.(a) $A \cup (B \cup C) = (A \cup B) \cup C$

$$\begin{aligned} x \in A \cup (B \cup C) &\iff x \in A \vee (x \in B \vee x \in C) \\ &\iff (x \in A \vee x \in B) \vee x \in C \\ &\iff x \in (A \cup B) \cup C \end{aligned}$$

Therefore, x $\in A \cup (B \cup C)$ if and only if $x \in (A \cup B) \cup C$.

3.(a) We shall prove two cases :

I. $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$

II. $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$

I. $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$

Let $x \in A \cap (B \cup C) \implies x \in A \wedge x \in (B \cup C)$

$\implies x \in A \wedge \{x \in B \vee x \in C\}$

$\implies \{x \in A \wedge x \in B\} \vee \{x \in A \wedge x \in C\}$

$\implies x \in (A \cap B) \vee x \in (A \cap C)$

$\implies x \in (A \cap B) \cup (A \cap C)$

$\therefore x \in A \cap (B \cup C) \implies x \in (A \cap B) \cup (A \cap C)$

$\therefore A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$

II. $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$

Let $x \in (A \cap B) \cup (A \cap C) \implies x \in (A \cap B) \vee x \in (A \cap C)$

$\implies \{x \in A \wedge x \in B\} \vee \{x \in A \wedge x \in C\}$

$\implies x \in A \wedge \{x \in B \vee x \in C\}$

$\implies x \in A \wedge \{B \cup C\}$

$\implies x \in A \cap (B \cup C)$

$\therefore x \in (A \cap B) \cup (A \cap C) \implies x \in A \cap (B \cup C)$

$\therefore (A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$

$\therefore A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

5.(a)

$$\begin{aligned} x \in A \cup \overline{A} &\iff x \in A \vee x \in \overline{A} \\ &\iff x \in A \vee x \in U \setminus A \\ &\iff x \in A \vee (x \in U \wedge x \notin A) \\ &\iff x \in U \end{aligned}$$

We have shown, A $\cup \overline{A} = U$

5.(b) $A \cap \overline{A} = \emptyset$

$$\begin{aligned} x \in A \cap \overline{A} &\iff x \in A \wedge x \in \overline{A} \\ &\iff x \in A \wedge x \in U \setminus A \\ &\iff x \in A \wedge (x \in U \wedge x \notin A) \end{aligned}$$

that is a contradiction. So, there is no x , such that $x \in A \cap \overline{A}$, hence $A \cap \overline{A} = \emptyset$

6. $\overline{\overline{A}} = A$

$$\begin{aligned} x \in \overline{\overline{A}} &\iff x \in U \setminus \overline{A} \\ &\iff x \in U \wedge x \notin \overline{A} \\ &\iff x \in U \wedge x \in A \\ &\iff x \in A \end{aligned}$$

8.(a) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

$$\begin{aligned} x \in \overline{A \cup B} &\iff x \in U \setminus A \cup B \\ &\iff x \in U \wedge x \notin A \cup B \\ &\iff x \in U \wedge x \notin A \wedge x \notin B \\ &\iff x \in U \wedge x \in \overline{A} \wedge x \in \overline{B} \\ &\iff x \in U \wedge x \in \overline{A} \cap \overline{B} \\ &\iff x \in \overline{A} \cap \overline{B} \end{aligned}$$

1.5 Families of Sets

Sets can be elements of other sets. Instead of calling them set of sets we refer to them as collection or families of sets .

A family of sets is not a set necessarily, because we allow repeated elements, so a family is a multiset.

Definition 1.5.1 (Power set) Let A be a set. The set consisting of all subsets of A is called the power set of A and denoted by $\mathcal{P}(A)$.

$\mathcal{P}(A) = \{X : X \subseteq A\}$

Remark 1. $\emptyset \subseteq A$ for any set A, So $\mathcal{P}(A) \neq \emptyset$

In particular, $\mathcal{P}(\emptyset) = \emptyset$

2. According to definition, $A \subseteq A$, therefore $A \in \mathcal{P}(A)$ but an element $a \in A$ could not be an element of $\mathcal{P}(A)$,i.e. $a \notin \mathcal{P}(A)$

Example 1.5.2 If $A = \{a, b, 1\}$, then

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{1\}, \{a, b\}\, \{a, 1\}, \{b, 1\}, \{a, b, 1\}\}.$$

Note that:

$$a \in A; \qquad \{a\} \subseteq A; \qquad \{a\} \in \mathcal{P}(A); \qquad a \notin \mathcal{P}(A)$$

$$\emptyset \subseteq A; \qquad \emptyset \notin A; \qquad \emptyset \in \mathcal{P}(A); \qquad \emptyset \subseteq \mathcal{P}(A)$$

Arbitrary Unions and Intersections

The union operation $\cup$ allows us to form the union $A \cup B$ of two sets. As a result of associativity laws we can form the union and intersection of finitely many arbitrarily collections of sets.

$$A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_{n-1} \cup A_n = A_1 \cup (A_2 \cup A_3) \cup \ldots (A_{n-2} \cup A_{n-1}) \cup A_n$$

But what about infinite collections of sets ? The above approach does't work for the infinite case.

Definition 1.5.3 Suppose I is a set, called the index set, and with each $i \in I$ we associate a set A_i . We call $\{A_i : i \in I\}$ an indexed family of sets. Sometimes this is denoted by $\{A_i\}_{i \in I}$.

The size of the collection of sets being "unioned over" is whatever the size of I is. This notion makes perfect sense even if I is an infinite set (countable or uncountable).

For example, if $I = \mathbb{N}$, the set of natural numbers, we could write $\{A_i\}_{i \in \mathbb{N}}$, meaning that we have a countable number of sets which are being considered. (Note, in general, it is not necessary that be even countable. The set of all real numbers denoted by R is an example of an uncountable set as compared to N, which is a countable set.)

Example 1.5.4 $I = \{A_1, A_2, A_3\}$ with $A_1 = \{a, b, 2\}, A_2 = \{a, b\}, A_3 = \{a, d\}$ and is a family of sets.

Given an indexed family $\{A_i\}_{i \in I}$ we can define the intersection and union of the sets A_i

Definition 1.5.5 (Extended Union and Intersection) Let I be a family of sets. Then we define:

The union over I by:

$$\bigcup_{i\in I} A_i = \{x \mid \exists i \in I : x \in A_i\}$$

and the intersection over I by:

$$\bigcap_{i\in I} A_i = \{x \mid \forall i \in I : x \in A_i\}$$

That is, $\bigcup_{i\in I} A_i$ is the set of all those elements which belongs to one or more of the sets A_i in the family, and $\bigcap_{i\in I} A_i$ is the set of those elements which belongs to every A_i .

Note that if I has two elements, like $I = \{1, 2\}$, then we have only two sets A_1 and A_2.

So the union of the collection $\{A_i : i \in I\} = \{A_1, A_2\}$ is just

$$\bigcup_{i\in I} A_i = A_1 \cup A_2$$

And the intersection

$$\bigcap_{i\in I} A_i = A_1 \cap A_2$$

So the definition of arbitrary union and intersection over indexed families reduses to the former notions of union and intersection of pairs of sets.

If $I = \mathbb{N}$, is the set of natural numbers we can form the union of the collection over an infinite countable sequence of sets $A_1, A_2, A_3, \ldots$ then $\{A_i : i \in I\}$ is $A_1 \cup A_2 \cup A_3 \cup \ldots$.

We can go further and take the union of the collection over an infinite uncountable sequence. Let $I = \mathbb{R}$ the set of real numbers. [6]

Example 1.5.6 let $I = \{1, 2, 3, ..., n\}$.

$$\bigcup_{i\in I}^{\infty} A_i = \mathbb{N}$$

$$\bigcap_{i=1}^{\infty} A_i = \{1\}$$

[6] (Although the sets I used in indexing collections of sets are often sets of numbers, they don't have to be; this notion makes perfect sense for any set I whatsoever.)

$$\bigcap_{i=5}^{8} A_i = \{1, 2, 3, 4, 5\}$$

Example 1.5.7 Let $I = \{A_1, A_2, A_3\}$ where $A_1 = \{a, b, 2\}, A_2 = \{a, b\}, A_3 = \{a, d\}$:

$$\bigcup_{i \in I} A_i = \{a, b, 2, d\} \qquad \bigcap_{i \in I} A_i = \{a\}$$

Note that

$I \subseteq \mathcal{P}\left(\bigcup_{i \in I} A_i\right) = \mathcal{P}\left(\{a, b, 2, d\}\right)$

Example 1.5.8 Let R denote the set of real numbers, N denote the set of natural numbers and S denote the set of all finite subsets of R.

For each $n \in \mathbb{N}$ consider the subset $A_n = \{n\}$ of R.

For all $n \in \mathbb{N}$, $A_n \in T$.

But

$$\bigcup \{A_n : n \in N\} = \bigcup \{n : n \in N\} = N \notin T$$

Because it is neither finite, nor equal to the entire set of real numbers.

A family with index set $\mathbb{N}$ is called a sequence.

1.6 Representation of sets and subsets

There are some way of describing a set. The elements of a finite sets can be described by listing them all, but for the sets with large number of elements or infinite sets the best way to describing them is giving the property which defines the set.

Intuitively, a set is a collection of all elements that satisfy a certain given property, so If $P(x)$ is some property we write $\{x \ : P(x)\}$, or $x \in A$ to mean the set of all those x that satisfy $P(x)$, so that for all x,

$$x \in A \iff P(x)$$

Formally,

$$\{x \in A \,|P(x)\} := \{x | x \in A \ \wedge P(x)\},$$

For example,

$$A = \{x | x \text{ is a prime number}\}$$

, the closed form of {2, 3, 5,7, 11, . . . }, is the set of all prime number which is an infinite set.

The set of natural numbers can be described :

$$\mathbb{N} = \{x \in \mathbb{Z} \ | x > 0\}$$

i.e. the set of all x belonging to integer numbers with this restriction that x is positive integer.

The empty set

$$\emptyset = \{x \in \mathbb{R} \ | x^2 < 0\}$$

Suppose A and B are sets and $A \subseteq B$. Another way of Specifying a subset of a set B is of the form:

$$\{F(x) : x \in A\}$$

where $F(x)$ is some formula depends on x. It consists of all objects obtained by putting members of the set A into the formula F. For example,

$$\{x^2 : x \in \mathbb{N}\} = \{1, 4, 9, 16, 25, \dots\} = B$$

and if $A = \{-3, 0, 1, 2, 5\}, then$

$$C = \{F(x) : x \in A\} = \{x^2 : x \in A\} = \{9, 0, 1, 4, 25\} \subseteq B$$

In formal,

$$\{F(x) : x \in A\}$$

can be defined as

$$\{y \in B : \exists x \in A \ s.t. \ y = F(x)\}$$

The empty set can be specified in many ways, e.g.,

$$\emptyset = \{x \in \mathbb{R} \ | x^2 = -1\}$$

$$\emptyset = \{x \ | x \neq x\}$$

This is an axiom called The Axiom of Unrestricted Comprehension.

1. **Axiom Schema of Unrestricted Comprehension** This says that, for any property, there exists a set of all and only those things that have that property, $Y = \{x \ : P(x)\}$. More precisely, we restrict to properties that can be defined by formulae in the language of set theory with parameters:

$$\exists A \, \forall x \, (x \in A \iff P(x)) \tag{1.6}$$

This axiom guarantee for any proposition there exists a set with some elements corresponding to that property.

Now consider following sets:

$$A = \{x \, | x \text{ is a number}\}$$

$A = \{0, 9, 1, -15, \dots\} =$ the set of all real numbers $\mathbb{R}$

$$B = \{x \, | x \text{ is not a number}\}$$

$B = \{\{0\}, \{9\},$ Grothendick, Stars, Sky, logical proposition, lines, $\dots \ B \}$
$=$ The set of every thing except numbers

Notice that $A \notin A$ and $B \in B$.

$A \notin A$, because A is not a number.

$B \in B$, because the set B is not a number so it contains even itself!

So there are sets that **Do** belong to themselves and there are sets that **Do not** belong to themselves

Now consider the collection of all sets $U = \{\text{all sets}\}$.

Since U is a set it contains itself as a set, $i.e.$ $U \in U$.

Lemma 1.6.1 *For every A, there is a unique set B such that $x \in B$ if and only if $x \in A$ and $P(x)$.*

Proof Suppose B' is another set such that $x \in B'$ if and only if $x \in A$ and $P(x)$.

If $x \in B$ implies $x \in A$ and $P(x)$, then $x \in B'$.

If $x \in B'$ implies $x \in A$ and $P(x)$, then $x \in B$.

Thus we have $x \in B$ and only if $x \in B'$.

Therefore $B = B'$.

Although this axiom seems quite obvious but it leads to several paradoxes.

Before I get to these paradoxes I introduce some basic operation on sets.

1.7 Paradoxes

The Axiom Schema of Unrestricted Comprehension allows us to generate collection of sets.

We can form, "the collection of all sets x that satisfy a condition $P(x)$. In set builder notation, this is written $Y = \{x \ : P(x)\}$. The question is can we assume this new collection of sets is a set itself? It turns out NO.

The set of all sets which have the property of:

- Not being members of themselves $\Longrightarrow$ Russell's Paradox
- Being a set $\Longrightarrow$ Cantor's Paradox
- Being an ordinal $\Longrightarrow$ Burali-Forti's Paradox

Therefore, we don't consider the set of all sets to be a set, but a *proper class*.

Russell's Paradox

Bertrand Russell considered the following set:

$$R = \{x : x \notin x\}$$

That is, the collection of all sets x that are not members of themselves.

So, the set x is a member of R if and only if x is not a member of x ,i.e.

$$\forall x(x \in R \iff x \notin x)$$

And asked a question: Is R a member of itself or not ?

- If $R \in R$, then according to the definition of R we have $R \notin R$.
- If $R \notin R$, then according to the definition of R we have $R \notin R$.

If we accept either of them we get contradiction.

$$R \in R \iff R \notin R$$

It is always both true and false or it is neither true nor false! must satisfy the defining condition, so $R \notin R$, and that is also a contradiction.

Thus we must confess that $\{x : x \notin x\}$ is not a set.

Cantor's Paradox

Cantor prooved for every set A the power set of A; that is, the set of all subsets of A denoted by $\mathcal{P}(A)$, has a larger cardinality than A itself.[7]

$\mathcal{P}(A)$ has $|2^A|$ elements. So $|A| < |2^A|$

Now let A be the set of all sets,

$$|A| < |2^A|$$

but 2^A is a subset of A, because every set in 2^A is in A. Therefore

$$|2^A| \leq |A|$$

A contradiction. Therefore the set of all sets doesn't exist.

So we must give set theory an axiomatic foundation which does not lead to contradictions.

Exercise (Curry's Paradox) P be the statement "The earth is flat." Let S be the set

$$\{x | x \in x \implies P\}$$

(a) Prove that $S \in S \implies P$.

(b) Prove that $S \in S$

(c) Prove P!

Naive Set Theory failed because it allowed us to form sets that comprehend arbitrary properties. One way to solve paradoxes of this type is to abandon the Axiom Schema of Unrestricted Comprehension and restrict it to, the Axiom Schema of Restricted Comprehension (also called the Schema of Separation). In ZFC, we are allowed to form subsets that comprehend any property definable by a formulae with parameters.

Now this axiom says, for each such property of sets $P(x)$ and given any set A the set $Y = \{x \in A : P(x)\}$ exists.

Let's consider the Russele's Paradox again:

$$R = \{x : x \in A \wedge x \notin x\}$$

[7] In the next section we will proof it.

- If $R \in R$, then $R \in A$ & $R \notin R$ (Contradiction).
- Therefore, $R \notin R$, and either $R \notin A$ or $R \in R$.

  We conclude that $R \notin R$ & $R \notin A$.

  So $R \in R$ is false, and $R \notin R$ is true.

  In other word in :

$$R \in R \iff R \notin R$$

  we can only prove $R \in R \implies R \notin R$ not $R \notin R \implies R \in R$.

As we see Russele's Paradox is not a Paradox anymore. Since the existence of the set $\{x : x \notin x\}$ is not valid in ZFC becuase of Axiom Schema of Restricted Comprehension.

This axiom only allows us to create such sets as $\{x : x \in A \wedge P(x)\}$. By another axiom called the axiom of foundation this set is just the empty set.

As a matter of fact, it is the concept of the set of all sets that is paradoxical, not the idea of comprehension itself.

Axiom Schema of Restricted Comprehension [8]

If P is a property (with parameter p), then for any X and p there exists a set $Y = \{x \in X : P(x, p)\}$ that contains all those $x \in X$ that have property P.

In other word, for a given set X and proposition $P(x)$, there exists a subset A of X such that:

$$\forall X \, \exists A \, \forall x (x \in A \iff x \in X \wedge P(x))$$

Restricted Comprehension allows us to define some other set-theoretical constructions.

- Intersection

  If we apply the axiom to the set A and the property $P(x) : x \in B$ we get the definition for intersection of two sets.

$$Y = \{x \,|x \in A \wedge x \in B\}$$

$$Y = A \cap B$$

[8] Also called axiom schema of specification or separation

- Relative complement

  If we make the restriction that $P(x) : x \notin B$, we get definition of relative complement.

$$Y = \{x \,|x \in A \wedge x \notin B\}$$

$$Y = A \setminus B$$

- Empty set

  Taking $P(x) : x \neq x$ we get :

$$Y = \{x \,|x \in A \wedge x \neq x\}$$

$$Y = \emptyset$$

Empty set can be derived from some other axioms and sometimes the existence of empty set is taken as an axiom in ZFC.

Not to mention that the Cantor paradox fails if we do not assume the power set axiom, namely it might be that not all sets have a power set. So if the universal set does not have a power set, there is no problem in terms of cardinality.

This seems quite coherent so naive set theory takes it as an axiom, precisly:

As we mentioned before, for any two objects x and y, we can form the pair set $\{x, y\}$ consisting of just the elements x and y.

In ZFC we take the existence of this new set as axiomatic, called Pairing axiom.

Axiom of pairing The axiom of pairing says that if x and y exist (i.e., if they are sets) there also exists a set whose only elements are x and y.

$$\forall A \, \forall B \, \exists C \, [\forall x(x \in C \Leftrightarrow x = A \text{ or } x = B]. \tag{1.7}$$

Again, by Extensionality, there is a unique such set. We will represent such set as $\{x, y\}$. The set consists of the sets a is $\{a\}$ and is called the singleton whose only element is a . So again having $\{a\}$ it follows that the set $\{\{a\}\}$ exists applying pairing axiom again the set $\{\{\{a\}\}\}$ exists.

This axiom will allow us to set up the definition of union between two sets.

Axiom of union For every set A, there exists a set, denoted by , whose elements are all the elements of the elements of A.

$$\forall A\, \exists B\, [\forall x(x \in B \iff \exists y(y \in A \wedge x \in y)] \tag{1.8}$$

For example, if $x = \{\{1, 2, a, b\}, \{2, 3, b, d\}\}$ then $\bigcup x = \{1, 2, 3, a, b, d\}$ Using the axiom of equality $\bigcup x$ is unique. This axiom together with the pair set axiom, allows us to take the union of finite sequence $x_1, \ldots, x_n$. From the pairing axiom, we have:

$$\{A, B\}$$

From the union axiom, we have the union of $\{A, B\}$:

$$\bigcup\{A, B\}$$

There are only two members in $\{A, B\}$. Therefore:

$$x \in \bigcup\{A, B\} \iff x \in A \vee x \in B \iff x \in (A \cup B)$$

So as a special Case we define the union of the two sets as follows : $\bigcup\{A, B\} = A \cup B$

Just as we defined the union of only one set we can also define the intersection of one set. But we don't need an axiom for that becuase it can be derived from the axiom of separation and Axiom of pairing.

The axiom of separation guarantee if A exists then $\bigcap A$ also exists.

$$\bigcap A = \{x : \forall y((y \in A) \Longrightarrow (x \in y))\}$$

As a special Case we define the intersection of the two sets as follows :

$\bigcap\{A, B\} = A \cap B$ Beacuse :

$$x \in \bigcap\{A, B\} \iff x \in A \wedge x \in B \iff x \in (A \cap B)$$

For example, if $x = \{\{1, 2, a, b\}, \{2, 3, b, d\}\}$ then $\bigcap x = \{2\}$

Remark

$\bigcup \emptyset = \emptyset$

$\bigcap \emptyset = U$

Beacuse

$$\bigcap \emptyset = \{x : x \in \emptyset\} = \{x : x \in \mathbb{U}\}$$

is a paradox since the set of all set dosen't exist.

But this paradox will not occur anymore since ZFC axioms doesn't allow us to make that set. In ZFC that is :

$$\left\{x \in X : x \in \bigcap \varnothing\right\} = X$$

Which dosen't come up with a paradox.

1.8 ZFC Axioms

1. *Axiom of extensionality:*

$$\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow \forall w (x \in w \Leftrightarrow y \in w)]$$

2. *Axiom Schema of Restricted Comprehension (specification):*

$$\forall X \; \exists A \; \forall x (x \in A \iff x \in X \wedge P(x))$$

3. *Axiom of pairing:*

$$\forall A \; \forall B \; \exists C \; [\forall x (x \in C \Leftrightarrow x = A \text{ or } x = B]$$

4. *Axiom of union:*

$$\forall A \; \exists B \; [\forall x (x \in B \iff \exists y (y \in A \wedge x \in y)]$$

5. *Axiom of foundation:*

$$\forall x [\exists a (a \in x) \Rightarrow \exists y (y \in x \wedge \neg \exists z (z \in y \wedge z \in x))]$$

6. *Axiom schema of replacement:*

$$\forall x \in X \; \exists! y \, P(x, y) \Rightarrow [\, \exists Y \; \forall y \, (y \in Y \iff \exists x \in X \, (P(x, y)))\,]$$

7. *Axiom of power set :*

$$\forall X \; \exists Y \; \forall Z \, [\, Z \in Y \Leftrightarrow \forall z (z \in Z \implies z \in X)\,]$$

8. *Axiom of infinity:*

$$\exists X \, [\, \emptyset \in X \text{ and } \forall x (x \in X \Rightarrow x \cup \{x\} \in X)\,]$$

9. *Axiom of choice:*

$$\forall X \, [\, \emptyset \notin X \text{ and } \forall Y, Z \in X (Y \neq Z \implies Y \cap Z = \emptyset) \Rightarrow \exists Y \; \forall Z \in X \; \exists! z \in Z \, (z \in Y)\,]$$

Exercise

1. uppose that $A \subseteq B$ with $|B| = n$ and $|A| = m$. Compute the number of subsets of B that contain A.
2. Proof that following conditions are equivalent.
   (a) $A \subseteq B$
   (b) $A \cup B = B$
   (c) $A \setminus B = \emptyset$
   (d) $A \cap B = A$
3. Show that
   (a) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$
   (b) $A \Delta (B \Delta C) = (A \Delta B) \Delta C$
4. Proof for two sets A, B for which $A \cap B$ is non-empty
$$\bigcap A \cap \bigcap B \neq \bigcap (A \cap B)$$
5. Let F be a family of sets. Prove that
   F is the smallest set B such that $A \subseteq B$ for all $A \in F$.
6. Show that for any set A, $\bigcup \mathcal{P}(A) = A$
7. Show that for any set A, $A \subseteq \mathcal{P} \bigcup A$
8. Show that for any set A, $\{\emptyset, \{\emptyset\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(A)))$
9. Proof $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$

Georg Ferdinand Ludwig Philipp Cantor (1845 – 1918)

He was born in Saint Petersburg. Cantor, father was German and his mother was Russian and Roman catholic. When CANTOR was eleven years old ,his family moved to Germany, although cantor was never at ease in this country. Canton studied at the Gymnasium here and graduated with an outstanding report In 1860, He entered the Polytechnique of Zurich in 1862, where he studied mathematics with his parents approval, he studied there for a couple of years. In 1863, after the death of his father, Cantor moved to the university of Berlin. He studied at the University of Gottingen over summer and completed His first dissertation on the number theory named 'De aequationibus secondi gradus indeterminatis'. He received his doctorate in mathematics in 1867. He continued working an separate dissertations on the number theory and analysis. Cantor solved the problem proving the uniqueness of the representation. Cantor proved that rational numbers were countable and could be placed in correspondence to the natural numbers .Cantor had proved that real algebric numbers, were also countable. He loved to play The violin. He was awarded with the Sylvester medal for his work in mathematics in 1913. Some of his Major Works in mathematics are: Infinite sets, Uncountable sets, Cantor set, Cardinals and Ordinals, The Continuum hypothesis. Georg Cantor died on 1918 in Halle, after a prolonged mental illness. There were many publications on Cantor such as 'Men of Mathematics' and the 'history of mathematics'. He laid the foundation for Modern Mathematics and most of his works have survived to date.

Chapter 2

Enough Number Theory

> *No two persons ever read the same book.*
>
> Edmund Wilson,

This is not a book in number theory, but we need some basic definiton and theorm that will be used in following chapters. So I try to talk briefly as much as possible.

Well Ordering Principle

A nonempty set S of nonnegative integers always contains a smallest element m. That is, m satisfies the following two conditions: $(i) m \in S$ and $(ii) m < n$ for every number n in S.

Assume $a \neq 0$ and b are integers. if the remainder of division of b by a is zero then $b = ka$. This motivates following definition.

2.1 Divisibility

In number theory divisibility is the key idea and every ideas based on its notion.

Definition 2.1.1 For $a, b \in \mathbb{Z}$ such that $a \neq 0$, we say "a divides b" if there exists an integer q such that $b = qa$.

$$a \mid b \iff \exists q : b = qa$$

If a divides $b, i.e.\ a \mid b$ we say b is divisible by a or a is a factor of b. If a doesn't divide b, then we write $a \nmid b$. For example $4 \mid 12$ and $3 \mid 21$, while $2 \nmid 3$.

As an example take $a, b \in \mathbb{Q}$ such that $a \neq 0$, then a always divides $b, i.e.\ a \mid b$ because $\exists q : q = b/a \in \mathbb{Q}$,i.e. there always exists such q in the rationals. Even $b \mid a$ since $\exists q : q = a/b \in \mathbb{Q}$, That is I call this trivial divisibility because every non-zero element always divides any other one.

Definition 2.1.2 Any even integer has the form $2k$ for some integer k, while any odd integer has the form $2k + 1$ for some integer k.

Example 2.1.3 $2|n$ if n is even, while $2 \nmid n$ if n is odd.

Here we state some Basic Properties of Divisibility.

Theorem 2.1.4 For all $a, b, c \in \mathbb{Z}$, we have

(1) $a \mid a,\ 1 \mid a,$ and $a \mid 0$

(2) $0 \mid a \iff a = 0$

(3) $a \mid b \iff -a \mid b \iff a \mid -b$

(4) $a \mid b \,\&\, a \mid c \Longrightarrow a \mid (b \pm c)$

(5) $a \mid b \,\&\, b \mid c \Longrightarrow a \mid c$

(6) $a \mid b \,\&\, b \mid a \iff a = \pm b$

Proof These can be directy concluded from the definition, and the proof is left for readers.

The product of any two non-zero integers is non-zero. This implies the usual cancellation law: if a, b, and c are integers such that $a \neq 0$ and $ab = ac$, then we must have$b = c$; indeed, $ab = ac$ implies $a(b - c) = 0$, and so $a \neq 0$ implies $b - c = 0$, and hence $b = c$.

More generally, we have the following fundamental theorem, called The Division Algorithm.

Theorem 2.1.5 [The Division Algorithm]

Given any $a, b \in \mathbb{Z}$, $b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$.

$$\forall a, b \in \mathbb{Z}, b \neq 0 : \exists! q, r \in \mathbb{Z} : a = qb + r, 0 \leq r < b$$

Here q is called quotient of the integer division of a by b, and r is called remainder.

The number r will be denoted by $a \mod b$.

Existence

Consider the set $S = \{a - bq | q \in \mathbb{Z} \text{ and } a - bq \geq 0\}$. If $0 \in S$, then b divides a and we get $q = a/b$ and $r = 0$.

Now assume $0 \notin S$. According to Well Ordering Principle Since S is a nonempty set, we know that S has a smallest member $r = a - bq$ Then $a = bq + r$ and $r \geq 0$.

Moreover, if $r \geq b$, then $r - b \geq 0$, so $a - bq - b \geq 0$, or $a - b(q + 1) \geq 0$ So $a - b(q + 1) \in T$, but $r = a - bq > a - b(q + 1)$. This contradicts the assumption that r was the smallest element of S

Uniqueness

Suppose we have another pair q' and r' such that $a = bq' + r', \ \ 0 \leq r' < b$.

Then $bq + r = bq' + r'$.

So $r - r' = b(q' - q)$, so $b \mid (r - r')$.

Since $0 \leq r < b$ and $0 \leq r' < b$, we have $r - r' = 0$, and therefore $r = r'$ and $q = q'$

Example 2.1.6 For $a = 23$ and $b = 3$, then $23 = 3 \cdot 6 + 5$. Here $q = 6$ and $r = 5$. For $a = -23$ and $b = 3$, then $-23 = 3 \cdot (-8) + 1$. Here $q = -8$ and $r = 1$.

Remark The Division Algorithm is a consequence of the Well-Ordering Axiom for the positive integers.

Definition 2.1.7 Let $a, b \in \mathbb{Z}$, and write $a = qn + r$. We denote the remainder r by $\bar{a}$, or $[a]_n$, and call it the remainder of a mod n.

Example 2.1.8 Let $a = 31$ and $n = 7$. Then $a = 31 = 4.7 + 3$ so the remainder is $[a]_n = [37]_7 = 3$

We consider cases that two integers have the same remainder divided by n . This leads us to define the notion of congruence mod n.

2.2 Congruence

Definition 2.2.1 Given integers a and n, with $n > 0$, a mod n is defined to be the remainder when a is divided by n.

The most important application of the division algorithm that we use in everyday life is modular arithmetic. For example, if you measure time with a 12-hour clock, then you are calculating the hour modulo 12. Now that I'm writing this paper, the time is 11 o'clock. If someone asks me to call him 4 hours later,it means 3 o'clock. What we do without thinking is in fact this : $11 + 4 = 15 \equiv 3 \pmod{12}$.

Today is Saturday, they say the university start then 20 days from today. $20 \equiv 6 \pmod{7}$ will be Friday.

Today is Saturday August 29 2015. To say what day of the week it will be in 2017, we can calculate $730 \equiv 2 \pmod{7}$ $2 \cdot 365 = 730 \equiv 2 \pmod{7}$

Definition 2.2.2 (Gauss) Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then a is congruent to b modulo (or mod) n, if $n \mid (b - a)$. That is, a and b have the same remainder when divided by $n, i.e.$ $[a]_n = [b]_n$ And we write

$$a \equiv b \pmod{n}.$$

or $a \equiv_n b$

For example, $26 \equiv 4 \pmod{11}$. since 26 - 4 = 22 is divisible by 11.
We say 26 and 4 are congruent mod 11.

Example 2.2.3

$23 \mod 4 \equiv 3$ since $23 = (5)4 + 3$ and $0 \leqslant 2 \leqslant 3$

$-23 \mod 4 \equiv 1$ since $-23 = (-4)4 + 1$ and $0 \leqslant 1 \leqslant 4$

Lemma 2.2.4 *Let $a, b, n \in \mathbb{Z}$.Then the following statements are equivalent .*

(a) $a \equiv b \pmod{n}$.

(b) $a - b = kn$ for some integer k.

(c) $a = kn + b$ for some integer k.

(d) $a \pmod n = b \pmod n$.

Proof The proof is obtained from the definition, and is left to readers.

Remark

If $n = 0$ then $a \equiv b \pmod n \iff a = b$. So equality is a special kind of congruency.

If $n = 1$ then $a \equiv b \pmod n \iff a - b = k$ is always true.

So congruence mod $n = 0, 1$ is not interesting.

We proof a theorem which states congruence modulo n is an equivalence relation.

According to division algorithm, if $a, b \in \mathbb{Z}$ we can talk about quotient and remainder of division a by b.Take b as a fixed integer, then the remainder of division a by b is a cyclic set.

Since the remainder is between zero and b, $i.e.$ $0 \leq r < b$ the set $\{a \pmod n : n \in \mathbb{Z}\}$ is exactly the same as $\{0, 1, \ldots, n-1\}$ these are all possible remainders when n is divided by m.

Taking $n = 2$, every integer is congruent mod 2 to exactly one of 0 and 1.

Saying $a \equiv 0 \pmod 2$ means $n = 2k$ for some integer k, so n is even.
$Andsaying\ a \equiv 1 \pmod 2$means $n = 2k + 1$ for some integer k, so n is odd.

We have $a \equiv b \pmod 2$ precisely when a and b have the same parity, $i.e.$ both are even or both are odd.

Take $b = 2$. the remainder of division $0, 1, 2, 3, 4, \ldots$ by 2 is $0, 1, 0, 1, 0, \ldots$

Take $b = 3$. the remainder of division $a \in \mathbb{Z}$ by 3 is one of $\{0, 1, 2\}$.

Take $b = 4$. the remainder of division $a \in \mathbb{Z}$ by 3 is one of $\{0, 1, 2, 3\}$.

Take $b = n$. the remainder of division $a \in \mathbb{Z}$ by n is one of $\{0, 1, \ldots, n-1\}$.

Theorem 2.2.5 Let n be a positive integer. Every integer is congruent modulo n to exactly one integer between 0 and $n - 1$.

Proof Let n be a positive integer. If a is an integer, then the Division Algorithm gives us integers q and r with $a = qn + r$ and $0 \leqslant r < n$. Thus, $a - r = qn$ is divisible by n, so $a \equiv r \pmod{n}$.

If s is between 0 and $n-1$ and $a \equiv s \pmod{n}$, according to Division Algorithm a and s have the same remainders after division by n. But, since $s = 0.n + s$ and $a = qn + r$, the lemma tells us that $s = r$. Thus, a is congruent modulo n to exactly one integer between 0 and $n - 1$.

All the other numbers can be found congruent to one of the n numbers.

Remark The mod operation is derived from the Division Algorithm: If we divide the integer a by the positive integer b, we get a unique quotient q and remainder r satisfying $a = bq + r$ and $0 \leqslant r < b$. The remainder r is defined to be the value of $a \mod m$.

Definition 2.2.6 Let $n \in \mathbb{N}$ *and* a $\in \mathbb{Z}$. The unique integer between 0 and $n - 1$ to which a is congruent modulo n is called the least residue of a modulo n.

Definition 2.2.7 The set of remainders of integer division by n is denoted by $\mathbb{Z}_n$. For any integer a , its remainder after division by n,i.e. $[a]_n \in \mathbb{Z}$

For example, let $n = 4$. Then $[7]_4 = [11]_4 = [3]_4 = [-1]_4 = 3$

Corollary 2.2.8

The set of all elements congruent to x modulo n is called the *congruence class containing* x and is denoted $\bar{x}$ or $[x]_n$. The set of all congruences class modulo n is denoted $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

Since size of the set $\mathbb{Z}_n$ is equal to n and every integer must be in one of the n congruences classes.

The additive identity, additive inverse, and multiplicative identity always exist. In particular, if we want to solve $x + a \equiv b \pmod{n}$, then we are guaranteed that the additive inverse of a, called $-a$ (or $n - a$), exists and we are allowed to write $x \equiv b - a \pmod{n}$.

2.3 Modular Arithmetic

We can add, subtract or multiply congruences. That is, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n} \quad \text{and} \quad ac \equiv bd \pmod{n}.$$

Definition 2.3.1 Let $a, b \in \mathbb{Z}_n$. Take $x, y \in \mathbb{Z}$ such that $a = [x], b = [y]$. The addition of two elements is defined as

$$a + b = [x] + [y] := [x + y]$$

or sometimes

$$a +_n b = [x] +_n [y] := [x + y]_n$$

Also The multiplication of two elements is defined as

$$a.b = [x].[y] := [x.y]$$

or

$$a._n b = [x]._n [y] := [x.y]_n$$

Example 2.3.2 The set $\mathbb{Z}_4$ consists of $[0], [1], [2], [3]$. Addition and multiplication rule can be given by a table.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	4
2	2	3	0	1
3	3	4	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Table 2.1: Addition and multiplication mod 4

Theorem 2.3.3 Addition and multiplication defined above is well-defined.

Theorem 2.3.4 Let a, b, c and d denote integers. Let m be a positive integers. Then:

1. If $a \equiv b(mod\ m)$, then $b \equiv a(mod\ m)$.
2. If $a \equiv b(mod\ m)$ and $b \equiv c(mod\ m)$, then $a \equiv c(mod\ m)$.
3. If $a \equiv b(mod\ m)$, then $a + c \equiv b + c(mod\ m)$.
4. If $a \equiv b(mod\ m)$, then $a - c \equiv b - c(mod\ m)$.
5. If $a \equiv b(mod\ m)$, then $ac \equiv bc(mod\ m)$.
6. If $a \equiv b(mod\ m)$, then $ac \equiv bc(mod\ mc)$, for $c > 0$.
7. If $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$ then $a + c \equiv (b + d)(mod\ m)$.
8. If $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$ then $a - c \equiv (b - d)(mod\ m)$.
9. If $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$ then $ac \equiv bd(mod\ m)$.

Proof If $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Thus there exists integer k such that $a - b = mk$, this implies $b - a = m(-k)$ and thus $m \mid (b-a)$. Consequently $b \equiv a(mod\ m)$.

2. Since $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Also, $b \equiv c(mod\ m)$, then $m \mid (b-c)$. As a result, there exit two integers k and l such that $a = b + mk$ and $b = c + ml$, which imply that $a = c + m(k+l)$ giving that $a = c(mod\ m)$.

3. Since $a \equiv b(mod\ m)$, then $m \mid (a-b)$. So if we add and subtract c we get

$$m \mid ((a+c) - (b+c))$$

and as a result

$$a + c \equiv b + c(mod\ m).$$

4. Since $a \equiv b(mod\ m)$, then $m \mid (a-b)$ so we can subtract and add c and we get

$$m \mid ((a-c) - (b-c))$$

and as a result

$$a - c \equiv b - c(mod\ m).$$

5. If $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Thus there exists integer k such that $a-b = mk$ and as a result $ac - bc = m(kc)$. Thus

$$m \mid (ac - bc)$$

and hence

$$ac \equiv bc(mod\ m).$$

6. If $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Thus there exists integer k such that $a-b = mk$ and as a result

$$ac - bc = mc(k).$$

Thus

$$mc \mid (ac - bc)$$

and hence

$$ac \equiv bc(mod\ mc).$$

7. Since $a \equiv b(mod\ m)$, then $m \mid (a-b)$. Also, $c \equiv d(mod\ m)$, then $m \mid (c-d)$. As a result, there exits two integers k and l such that $a - b = mk$ and $c - d = ml$. Note that

$$(a-b) + (c-d) = (a+c) - (b+d) = m(k+l).$$

As a result,

$$m \mid ((a+c)-(b+d)),$$

hence

$$a + c \equiv b + d (mod\ m).$$

8. If $a = b + mk$ and $c = d + ml$ where k and l are integers, then

$$(a-b)-(c-d) = (a-c)-(b-d) = m(k-l).$$

As a result,

$$m \mid ((a-c)-(b-d)),$$

hence

$$a - c \equiv b - d (mod\ m).$$

9. There exit two integers k and l such that $a - b = mk$ and $c - d = ml$ and thus $ca - cb = m(ck)$ and $bc - bd = m(bl)$. Note that

$$(ca - cb) + (bc - bd) = ac - bd = m(kc - lb).$$

As a result,

$$m \mid (ac - bd),$$

hence

$$ac \equiv bd (mod\ m).$$

Properties of arithmetic modulo n

Because of the simple formula for addition and multiplication in $\mathbb{Z}_n$, there are some we analogues of the common properties of integer arithmetic. In particular, the following properties hold for all elements $a, b, c \in \mathbb{Z}_n$.

Commutativity of Addition: $[a + b] = [b + a]$

Associativity of Addition: $([a] + [b]) + [c] = [a] + ([b] + [c])$

Existence of an Additive Identity:$[a] + [0] = [a]$

Existence of Additive Inverses:$[a] + ([-a]) = 0$

Commutativity of Multiplication:$[a] \cdot b = b \cdot a$

Associativity of Multiplication:$([a] \cdot [b]) \cdot [c] = [a](\cdot[b] \cdot [c])$

Existence of a Multiplicative Identity: $[a] \cdot 1 = [a]$

Distributivity:$[a] \cdot ([b] + [c]) = ([a] \cdot [b]) + [c]$

Chapter 3

Relations and Functions

> *"Whoever loves to meet God, God loves to meet him*[1]*."*
>
> Prophet Muhammad,

In this chapter we continue our program to build up useful notion and concepts from set theory, with some basic set-theoretic definitions of ordered pairs, relations, and functions.

3.1 Ordered pairs and Cartesian products

In euclidean geometry a point is described by two co-ordinates x, y , that is, the point is described by a pair (x, y) and (x, y, z) in plane and space respectively. the pair (x, y) is called an ordered pair because In a pair, the order of the terms are important . (x, y) and (y, x) represent different points in the plane. But as we mentined in the first chapter because of axiom of extensionality the sets $\{x, y\}$ and $\{y, x\}$ are the same, since they have the same elements. Therefore, the ordered pair (x, y) is not the same as the set $\{x, y\}$ which is defined to be unordered. So we come up with following definition :

Definition 3.1.1 (Equality of ordered sets) The ordered pair construct (a, b) with first component a and second component b have the property that

$$(a, b) = (c, d) \iff a = c \ \wedge \ b = d$$

[1]This is a symmetric relation

We would like to define ordered pairs in terms of sets but how ? Because sets don't respect order.

Consider a set $\{a, b, c, d\}$. Suppose we want to propose an order in a set-theoretic manner for the elements of the set as follows : d first, a second, b third, c forth Take the first element and build a set out of it, that is $\{d\}$.Then take a set and put the next element and everything that is before it, that is , $\{d, a\}$. Doing so again we have $\{d, a, b\}$ and the last one is $\{d, a, b, c\}$. Now collect them all in a new set $O = \{\{d\}, \{d, a\}, \{d, a, b\}, \{d, a, b, c\}\}$ In this way we have a notion of order because d, a, b, c are repeated $4, 3, 2, 1$ respectively. Changing the order of members of O is irrelevant. For example if you write this, $O = \{\{d\}, \{a, d\}, \{a, b, d\}, \{a, b, c, d\}\}$ or even $O = \{\{d\}, \{a, d\}, \{d, a, b\}, \{d, c, b, a\}\}$ nothing is wrong and we can find out what the order of elements are.

This motivates Kuratowski definition of Ordered Pair.

Definition 3.1.2 The ordered pair (a, b) is defined as follows:

$$(a, b) = \{\{a\}, \{a, b\}\}$$

Notice that its existence follows from the Axiom of Pair Set alone.

We have to prove that Kuratowski definition obeys the definition of Equality of ordered sets. That is,

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} \iff a = c \wedge b = d$$

Proof $\Longleftarrow$

This follows from our definition.

If $a = c \wedge b = d$ then (a,b) = $\Big\{\{a\}, \{a, b\}\Big\} = \Big\{\{c\}, \{c, d\}\Big\} = (c, d)$.

$\Longleftarrow\Longrightarrow$

(i) If $a = b$, then $\{a, b\} = \{a, a\} = \{a\}$, so the set $(a, b) = \{\{a\}, \{a\}\} = a$ is a singleton, so the set (c, d) is also a singleton, so that $c = d$ and $(c, d) = \{\{c\}\}$, and since this last singleton is equal to $\{\{a\}\}$, we have $a = c$ and, hence, also $a = b = c = d$.

(ii) If $a \neq b$ ...

Take it as an exersice.

Remark (i) $\Big\{\{a\}, \{a, b\}\Big\} = \Big\{\{a, b\}, \{a\}\Big\}$ because two sets are equal if and only if they have the same elements and the order dosen't matter.

(ii)

We can further define ordered triples

$$(a, b, c) = ((a, b), c) = \{\{\{a\}, \{a, b\}\}, \{\{\{a\}, \{a, b\}\}, c\}\}$$

or simply

$$(a, b, c) = \{\{a\}, \{a, b\}, \{a, b, c\}$$

Generally, the ordered n-tuples

$$(a_1, \ldots, a_n) = \{\{a_1\}, \{a_1, a_2\}, \ldots, \{a_1, \ldots a_{n-1}\}, \{a_1, \ldots a_n\}\}$$

Cartesian product

Suppose we have two sets A and B and we form ordered pairs by taking an element of A as the first member of the pair and an element of B as the second member.

Definition 3.1.3 The Cartesian product of two sets A and B, denoted $A \times B$ is the set of all ordered pairs (a, b) with $a \in A$, $b \in B$. and defined as follows

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

Theorem 3.1.4 The Cartesian product of two sets A and B exists

Proof We can use the axioms to show that the set $A \times B$ exists. By Axiom of Pair, $A \cup B$ exists as a unique set. Thus $\mathcal{P}(A \cup B)$ exists. Using Axiom of Power Set again guarantee $\mathcal{P}(\mathcal{P}(A \cup B))$ exists.

If $a \in A$ and $b \in B$ then $\{a\} \subset A$ and $\{b\} \subset B$, therefore $\{a, b\} \subset A \cup B$ so we can conclude $\{a, b\} \in \mathcal{P}(A \cup B)$ since also $\{a\} \subset A \cup B$ we can say $\{a\} \in \mathcal{P}(A \cup B)$. We can conclude again, $\{\{a\}, \{a, b\}\} \subset \mathcal{P}(A \cup B)$ and hence $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$.

So we proved $\{\{a\}, \{a, b\}\} = (a, b)$ is an element of $\mathcal{P}(\mathcal{P}(A \cup B))$. Now apply the Axiom of Seperation with the properties $P(a) : a \in A$ and $P(b) : b \in B$ to construct $A \times B$.

In general, we can extend the definition to n arbitrary sets $A_1, A_2, \ldots, A_n$.

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1 \ \wedge \ a_2 \in A_2 \ \ldots \ \wedge \ a_n \in A_n\}$$

If $A_1 = A_2 = \cdots = A_n$ we write A^n istead of $A_1 \times A_2 \times \cdots \times A_n$.

For example $\{(x, y) : x \in \mathbb{R} \ \wedge \ y \in \mathbb{R}\}$ is the set of coordinates of points in the plane . We often write it as $(x, y) \in \mathbb{R} \times \mathbb{R}$ or $(x, y) \in \mathbb{R}^2$.

Example 3.1.5 Let $A = \{a, 1, 2\}$ and $B = \{b, c\}$. Then

$$A \times B = \{(a, b), (a, c), (1, b), (1, c), (2, b), (2, c)\}$$

But

$$B \times A = \{(b, a), (c, a), (b, 1), (c, 1), (b, 2), (c, 2)\}$$

The Cartesian product $A \times B$ is not commutative,

$A \times B \neq B \times A$, Unless $A = B$ or one of them is the empty set.

It is not even associative.

$(A \times B) \times C \neq A \times (B \times C) \neq A \times B \times C$

If A, B are any finite sets, then $|A \times B|$ = $|A||B|$, because there are $|A|$ ways of choosing to first component of an element (x, y) of $|A \times B|$, and for each choice $|B|$ ways of choosing the second component.

That is why we use $\times$ to denote Cartesian product of sets.

3.2 Relation

As it comes from its name a **relation** is a relation; that is it considers two objects. Even when we have only an element x and a relation R we are comparing x with itself and generalizing the idea of relation between two objects to one object with itself. So it is pointless to define a relation on a singleton. It is convinent to define a relation as a subset of cartesian product since it deals with the set of two things related toghter, If we want to define a relation on a set X we may define it in the product of a set with itself, $i.e.$ $X \times X$.

Because a relation might be consists of some pairs or include entire set it is a subset of $X \times X$.

If a point $(a, b) \in X \times X$ is in R we write aRb. for example a relation $>$ is a subset of $\mathbb{R}^2$ if $(a, b) \in >$ then we write $a > b$.

Examples of relations on the set of real numbers include $<, =, and \geq$. And of relations on $\mathcal{P}(X)$, the power set of X, include $=$ and $\subseteq$.

In fact, given sets A and B, a relation between A and B makes a special link between elements of A with elements of B.

Definition 3.2.1 Let A and B be two sets. A (binery) relation from A to B, denoted by $A \to B$ is a triple, (A, R, B) where $R \subseteq A \times B$ is any subset of $A \times B$

. If $A = B$ then we call such a relation a relation on A. If $(a, b) \in R$ then we say a and b are related and we write aRb .

Note that by this definition a relation is just any subset of $A \times B$. If R is a relation on $A \times B$, we call the set A the domain of R and B the codomain of R.

The relation of equality in a nonempty set A. $R = \{(a, a) : a \in A\}$ thus $(a, b) \in R \subseteq A \times B \iff a = b$

Like ordered pairs, two relations, (A, R, B) and (A', R', B'), are equal $\iff$ $A = k'$, B = B′ and $R = R'$

Definition 3.2.2 (Domain and range of relations.) Let A and B be two sets and R be a relation from $A \to B, i.e.\ R \subseteq A \times B$.

(i) Domain of the relation R: The domain of R is defined by

$$Dom(R) := \{a \in A : \exists b \in B\ ,\ (a, b) \in R\}$$

(ii) Range of the relation R: The range of R is defined by

$$Rng(R) := \{b \in B : \exists a \in A\ ,\ (a, b) \in R\}$$

Here for some reasons we would like to compare objects from the same set, $i.e.$ we consider relation on one set $A \times A$.

In the case where R is a relation for which the domain and codomain are the same set A, that set A is called the underlying set for R.

Definition 3.2.3 (Inverse relation.) Let A and B be two sets and R be a relation from $A \to B, i.e.\ R \subseteq A \times B$. The inverse of R (denoted by R^{-1}) is defined by

$$R^{-1} := \{(b, a) \in B \times A\ \ (a, b) \in R\}$$

What we have defined is abinary relations, $i.e.$, sets of ordered pairs. We can also define ternary, quaternary or just n-place relations consisting respectively of ordered triples, quadruples or n-tuples.

Example 3.2.4 Let $A = \{1, 2, 3, 4\}$ then each of the following is a relation on A.

$R_1 = \{(1, 3), (2, 4)\}$

$R_2 = \{(1, 1), (2, 2), (3, 3), (4, 4)\} = \{(a, b) \in A \times A : a = b\}$

In relation $R_1 : 1$ is related to 3 and 2 is related to 4 ,i.e. $(1, 3) \in R_1$ and $(2, 4) \in R_1$ respectivly. But 4 is not related to 1 $(4, 1) \notin R_1$. We say relation R_1 is not symmetric. $(a, b) \in R_1$ but $(b, a) \notin R_1$ or $a\ R_1\ b$ but $b \not R_1\ a$.

In relation R_2 : 1 is related to 1 , 2 is related to 2,etc. That is, every element is related to itself. $(a, a) \in R_2$ or $a\ R_2\ a$.

There are some differences between relations. Consider the "sisterhood" relation. Neda could be a sister of Ali, but Ali is not a sister of Neda. We say that sisterhood relation is not symmetric.

However, the "neighborhood" relation is symmetric: if A is the neighbor of B then B is the neighbor of A.

In this case, the relation has a further property. If A is a neighbor of B and B is a neighbor of C then A is a neighbor of C. We call this property transitivity. An important, and very useful, class of relations are the relations that are reflexive, symmetric and transitive. We call this kind of relation, equivalence relations. For equivalence relations instead of $a\ R\ b$ we use the special notation a $\sim b$.

3.3 Partitions of a Set

Consider the set of integers $\mathbb{Z}$.
We can divide it into two parts in different ways:

- The set of negative and non-negative integers.

$$\mathbb{Z} = \{\dots, -5, -3, -1\} \cup \{0, 2, 4, \dots\}$$

- The set of even integers and the set of odd integers.

$$\mathbb{Z} = \{\dots, -5, -3, -1, 1, 3, 5, \dots\} \cup \{\dots, -4, -2, 0, 2, 4, 5, \dots\}$$

In both cases every integer is a member of one of these subsets, and no integer is a member of both, so this gives a partition of $\mathbb{Z}$:

Definition 3.3.1 A partition of a set A is a collection $\mathcal{P}$ of non-empty subsets $A_1, A_2, \dots, A_n$ satisfying the following properties.

(a) A is the union of all the A_i' : $A =$$\mathrm{A}_1 \cup A_2 \cup \dots A_n$

(b) the A_i are disjoint: $A_i \cap A_j = \emptyset$; for all $i \neq j$, $1 \leq i, j \leq n$.

The elements of $\mathcal{P}$ are called the blocks of the partition.

The sequence of sets $A_1, A_2, \dots$ could be finite or infinite, so we had better defined partition of A to be collection of subsets $\{A_i\}_{i \in I}$ of A such that $\bigcup_{i \in I} A_i$.

Remark

(a) For any set A, $\mathcal{P} = \{A\}$ is a partition of A, called the trivial partition.

(b) For any $A \subset U$, the set A with its complement $\overline{A}$ form a partition of U.

Example 3.3.2

(a) The empty set $\{\}$ and singleton $\{x\}$ have only one partition, $\{\{\}\}$ and $\{\{x\}\}$ respectivly

(b) A set with 2 elements, say , $\{1, 2\}$ has 2 different partition:

$$\{1, 2\}$$

$$\{\{1\}, \{2\}\}$$

(c) A set with 3 elements, say , $\{1, 2, 3\}$ has 5 different partition:

$$\{1, 2, 3\}$$

$$\{\{1\}, \{2\}, \{3\}\}$$

$$\{\{1, 2\}, \{3\}\}$$

$$\{\{1, 3\}, \{2\}\}$$

$$\{\{1\}, \{2, 3\}\}$$

The number of different partition of a set with n element is called the Bell number B_n.

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

The number of partition is exponentialy increasing as the cardinal goes higher, for example the set $\mid A \mid = 7$ has 877 partition.

3.4 Equivalence relations, equivalence classes

The equality relation $=$ between two or more objects is associate with the concept of being the same or being identical but sometimes we classify non-identical object into a collecton. This abstraction of equality is called Equivalence relation.

Equivalence relation is generalization of the notion of equality. Indeed, the usual notion of equality among the set of integers is an example of an equivalence relation. This is the " equivalence The more interesting concepts arose from trying to abstract some of the most useful properties of equality.

Definition 3.4.1 Let $\sim$ be a relation on a set A. We call $\sim$ an equivalence relation on A if it satisfies the following properties:

- (i) Reflexivity: $a \sim a \quad (\forall a \in A)$
- (ii) Symmetry: $a \sim b \Longrightarrow b \sim a \quad (\forall a, b \in A)$
- (iii) Transitivity: $a \sim b \ \wedge \ b \sim c \Longrightarrow a \sim c \quad (\forall a, b, c \in A)$

Remark Since an equivalence relation is reflexive, it implise that the set A is not empty. That is why we didn't note being nonempty in the definition.

In the language of sets, we can rewrite these properties as follows:

- (i) Reflexivity: $(a, a) \in\sim \quad (\forall a \in A)$
- (ii) Symmetry: $(a, b) \in\sim \Longrightarrow (b, a) \in\sim \quad (\forall a, b \in A)$
- (iii) Transitivity: $(a, b) \in\sim \ \wedge (b, c) \in\sim \Longrightarrow (a, c) \in\sim \quad (\forall a, b, c \in A)$

Example 3.4.2

(a) Let A be a set and consider equality $=$ relation. Then $=$ is obviously an equivalence relation on A since

- (i) Reflexivity: $a = a \quad (\forall a \in A)$
- (ii) Symmetry: if $a = b \Longrightarrow b = a \quad (\forall a, b \in A)$
- (iii) Transitivity: if $a = b \ \wedge \ b = c \Longrightarrow a = c \quad (\forall a, b, c \in A)$

(b) The relation $<$ on $\mathbb{Z}$ is transitive, but not reflexive or symmetric. The relation $\leq$ is transitive and reflexive, but not symmetric.

(c) The relation $\sim$ on $\mathbb{R}$ defined by $a \sim b \iff a - b \in \mathbb{Z}$ is an equivalence relation, but the same relation defined by $a \sim b \iff a - b \in \mathbb{N}$ is not, since it

dosen't satisfy symmetry property.

As we mentioned equality is a special case of equivalence relation. Any kind of equality, such as congruence of triangles, is generally an equivalence relation.

If $\sim$ is an equivalence relation on a set A , then $x \sim y$ is more than just being related, they are equivalent.

Recall, the next definition which is another example of an equivalence relation.

Definition 3.4.3 (Gauss) Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then a is congruent to b modulo (or mod) n, if $n \mid (b - a)$. That is, a and b have the same remainder when divided by $n, i.e.$ $[a]_n = [b]_n$ And we write

$$a \equiv b \pmod{n}.$$

we define the modular relation $\equiv_n$, *by* a $\equiv_n b$ if $n \mid a - b$, i.e.

$$\equiv_n := \{(a, b) : n \mid a - b\}.$$

Theorem 3.4.4 Congruence modulo n is an equivalence relation on $\mathbb{Z}$. That is: $\forall a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$

- (i) Reflexivity: $a \equiv a \pmod{n}$

  (ii) Symmetry: $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$

  (iii) Transitivity: $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.

  Proof

  (i) $a - a = 0$ and $n \mid 0 \implies a \equiv a \pmod{n}$

  (ii) $a \equiv b \pmod{n}$ means $a - b = nk$ for some $k \in \mathbb{Z}$. Therefore, $b - a = -nk = n(-k)$ so $b \equiv a \pmod{n}$

  (iii) $a \equiv b \pmod{n}$ means $a - b = nk$ and $b \equiv c \pmod{n}$ means $b - c = nk'$

  Therefore, $a - c = n(k - k')$, so $a \equiv c \pmod{n}$

Equivalence relation partitions a set into disjoint subsets, each of them consists of equivalent elements. These subsets are called equivalence classes.

Definition 3.4.5 Let $\sim$ be an equivalence relation on a set A. For each $a \in A$ the equivalence class of a is defined to be the set of all elements of A that are equivalent to a. The equivalence class of a will be denoted by $[a]$ or $[a]_\sim$ or $\overline{a}$.

$$[a] = \{x \in A \mid x \sim a\}$$

$[a]$ is not just an element, it is a set of elements. An element of an equivalence class $X \subseteq A$ is called a representative of X. Here a is a representative of the equivalence class $[a]$.

Beacuse of reflexivity we have $a \in [a]$. So any $a \in A$ is a representative of its own equivalence class.

Every equivalence relation makes equivalence classes.

The equivalence classes $[a]$ are subsets of A. The set of all equivalence classes is called the quotient space, denoted by $A/\sim$.

Equivalence classes for congruence mod n are also called congruence classes. Let a be an integer. By the definition of an equivalence class we have $[a] = \{x \in \mathbb{Z} \mid x \equiv_n a\} = \{x \in \mathbb{Z} \mid x = a + kn$;k $\in \mathbb{Z}$ $\}$.

Consider the relation $\equiv_2$ on Z.Then

$[0] = \{n \in \mathbb{Z} \mid 0 \equiv_2 n\} = \{n \in \mathbb{Z} \mid 2 \mid n\} = \{n \in \mathbb{Z} \mid n = 2k, k \in \mathbb{Z}\} = \{2k | k \in \mathbb{Z}\}$

$[1] = \{n \in \mathbb{Z} \mid 1 \equiv_2 n\} = \{n \in \mathbb{Z} \mid 2 \mid (n-1)\} = \{n \in \mathbb{Z} \mid n-1 = 2k, k \in \mathbb{Z}\} = \{2k+1 | k \in \mathbb{Z}\}$

$[2] = \{n \in \mathbb{Z} \mid 2 \equiv_2 n\} = \{n \in \mathbb{Z} \mid 2 \mid (n-2)\} = \{n \in \mathbb{Z} \mid n - 2 = 2k', k' \in \mathbb{Z}\}$

$= \{2k | k \in \mathbb{Z}\} = [0]$

$[3] = \{a \in \mathbb{Z} \mid 3 \equiv_2 a\} = \{a \in \mathbb{Z} \mid 2 \mid (n-3)\} = \{a \in \mathbb{Z} \mid n - 3 = 2k', k' \in \mathbb{Z}\}$

$= \{2k + 1 | k \in \mathbb{Z}\} = [1]$

We have :

Let $R = \{(x, y) |$ x and y have the same parity$\}$ be a relation on $\mathbb{Z}$

$$[0] = [2] = ... = [2k] = \{0, \pm 2, \pm 4, \pm 6, \ldots, \pm 2k, \ldots\}$$

$$[-1] = [1] = ... = [2k + 1] = \{\pm 1, \pm 3, \pm 5, \ldots, \pm(2k + 1), \ldots\}$$

This shows when $n = 2$, the equivalence classes under congruence mod 2 partition $\mathbb{Z}$ into two class, the even integers and the odd integers.

Therefore, the quotient space (the set of all equivalence classes) has only 2 elements.

$$\mathbb{Z}/\equiv_2 = \{[0],[1]\} = \{[2k],[2k+1]\}$$

Now consider the relation $\equiv_3$ on $\mathbb{Z}$. The equivalence relation $\sim$ on $\mathbb{Z}$ has three equivalence (congruence) classes:

$$[0] = \{n \in \mathbb{Z} \,|\, 0 \equiv_3 n\} = \{n \in \mathbb{Z} \,|\, 3 \mid n\} = \{n \in \mathbb{Z} \,|n = 3k, k \in \mathbb{Z}\} = \{3k | k \in \mathbb{Z}\}$$

$$[1] = \{n \in \mathbb{Z} \,|\, 1 \equiv_3 n\} = \{n \in \mathbb{Z} \,|\, 3 \mid (n-1)\} = \{n \in \mathbb{Z} \,|n-1 = 3k, k \in \mathbb{Z}\} = \{3k+1 | k \in \mathbb{Z}\}$$

$$[2] = \{n \in \mathbb{Z} \,|\, 1 \equiv_3 n\} = \{n \in \mathbb{Z} \,|\, 3 \mid (n-2)\} = \{n \in \mathbb{Z} \,|n-2 = 3k, k \in \mathbb{Z}\} = \{3k+2 | k \in \mathbb{Z}\}$$

$$\mathbb{Z}/\equiv_3 = \{[0],[1],[2]\} = \{[3k],[3k+1],[3k+2]\}$$

In general, for any $a \in \mathbb{Z}$, the equivalence class of a is

$$[a] = \{a + kn \,|k \ \in \mathbb{Z}\}$$

Therefore, the quotient space (the set of all equivalence classes also called congruence class representatives modulo n) has only n elements.

$$\mathbb{Z}/\equiv_n = \{[0],[1],[2],\ldots,[n-1]\} = \{[nk],[nk+1],[nk+2],\ldots,[nk+(n-1)]\}$$

The quotient space $\mathbb{Z}/\equiv_n$ is also denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$. This is one of the most important and useful example of equivalence classes so I make a definition out of it.

Definition 3.4.6

The set of all elements congruent to a modulo n is called the *congruence class containing* a and is denoted $[a]$ or $\overline{a}$. The set of all congruences class modulo n is denoted $\mathbb{Z}/\equiv_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{[0],[1],[2],\ldots,[n-1]\}$.

Operations on equivalence classes

An operation like addition or multiplication defined on the original set A can also be defined on the equivalence classes. For example, in $\mathbb{Z}_3$ we have three equivalence classes, namely

$$[0] = \{3k | k \in \mathbb{Z}\} = \{\ldots,-3,0,3,\ldots\}$$

$$[1] = \{3k+1 | k \in \mathbb{Z}\} = \{\dots, -2, 1, 4, \dots\}$$
$$[2] = \{3k+2 | k \in \mathbb{Z}\} = \{\dots, -1, 2, 5, \dots\}$$

Every integer is in one and only one of these classes.

we can say for example, $-3+4=1$ but since $-3 \in [0]$ and $4 \in [1]$ and every element of [0] and [1] is of the form $3k$ and $3k+1$ respectivly, $3n+3m+1 = 3(n+m)+1 = 3k'+1 = [1]$ so the addition we defined in perivious chapter makes sence here. $-3+4 = [0]+[1] = [0+1] = [1]$

Example 3.4.7 Let A be the set of fractions: $A = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ Define a relation $\sim$ on A by:

$$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$$

This relation is an equivalence relation. Beacuse

1) For any fraction $\frac{a}{b} \sim \frac{a}{b}$ since $ab = ba$. (Reflexitivity)

2) If $\frac{a}{b} \sim \frac{c}{d}$, then $ad = bc$, so $cb = da$ and $\frac{c}{d} \sim \frac{a}{b}$. (Symmetry)

3) If $\frac{a}{b} \sim \frac{c}{d}$, and $\frac{c}{d} \sim \frac{e}{f}$, then $ad = bc$ and $cf = de$. Multiply the first equation by f and divide by d to get $af = be$, so $\frac{a}{b} \sim \frac{e}{f}$. (Transitivity)

The equivalence classes of this equivalence relation, for example:

$$[\frac{1}{1}] = \{\frac{1}{1}, \frac{2}{2}, \frac{3}{3}, \dots, \frac{n}{n}, \dots\}$$
$$[\frac{1}{2}] = \{\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \dots, \frac{n}{2n}, \dots\}$$
$$[\frac{3}{7}] = \{\frac{3}{7}, \frac{6}{14}, \frac{9}{21}, \dots, \frac{3n}{7n}, \dots\}$$

The set of all the equivalence classes are called rational numbers denoted by $\mathbb{Q}$.

$$A/\sim = \mathbb{Q}$$

Since $\sim$ is reflexive $x \sim x$, therefore $x \in [x]$.

Theorem 3.4.8 Let $\sim$ be an equivalence relation on a set A. Then the following are equivalent:

$(i) a \sim b$

$(ii) [a] = [b]$

$(iii) [a] \cap [b] \neq \emptyset$

Proof $(i) \Rightarrow (ii)$. Suppose $a, b \in A$ and $a \sim b$. We must show that [a] = [b]. Suppose $x \in [a]$. Then, by definition of $[a]$, $x \sim a$. Since $\sim$ is symmetric and $a \sim b$,then $x \sim b$. Therefore, $x \in [b]$.
Suppose $x \in [b]$. Then $b \sim x$. Since $a \sim b$ and $\sim$ is transitive, $a \sim b$. Thus, $x \in [a]$.
We have shown that $x \in [a] \iff$ x $\in [b]$. Thus, $[a] = [b]$.
$(ii) \Rightarrow (iii)$. Suppose $a, b \in A$ and $[a] = [b]$. Then $[a] \cap [b] = [a]$. Since $\sim$ is reflexive, $a \sim a$; that is $a \in [a]$. Thus $[a] \cap [b] = [a]$
$(iii) \Rightarrow (i)$. Suppose $[a] \cap [b] \neq \emptyset$. Then there is an $x \in [a] \cap [b]$. By definition, $a \sim x$ and $b \sim x$. Since $\sim$ is symmetric, $x \sim b$. By transitive $a \sim x$ and $x \sim b$, hence $a \sim b$.

Equivalence relations and partitions

Equivalence relations and artitions are related closely together. The following theorem connects the concepts of an equivalence relation on a set A (which, is a subset of $A \times A$ with certain properties) and a partition on A (which is a collection of subsets of A with certain properties).

Theorem 3.4.9 There is a one to one correspondence between equivalence relations defined on a set A and the set of partitiona of A.

- Equivalence relations $\Rightarrow$ partitions:
If $\sim$ is any equivalence relation on the set A then the collection of all distinct equivalence classes (i.e. $A/\sim$) is a partition of A.

According to the previous theorem, we have:
(a) For any $x \in A$ there exists an equivalence class that contains x (namely, the class $[x]$).

(b) For any $a, b \in A$, the associated equivalence classes $[x]$ and $[y]$ are either equal $[a] = [b]$

or disjoint $[a] \cap [b] = \emptyset$

- Partitions $\Rightarrow$ equivalence relations:
Given any partition $\mathcal{P}$ of the set A into sets $A_1, A_2, \ldots, A_n$, the relation defined by

$$a \sim b \Longleftrightarrow a, b \in A_i \text{ for some block } A_i \in \mathcal{P}$$

is an equivalence relation on A. in which case the equivalence classes of $\sim$ are the blocks of the partition

According to the definition of a partition, each element of A is in exactly one block.

(i) Since x is in the same block as itself, $x \sim x$, so $\sim$ is reflexive.

(ii) If $a \sim b$, then a and b are in the same block, which is the same thing as $b \sim a$, so . So $\sim$ is symmetric.

(iii) If $a \sim b$ and $b \sim c$ then a and b are in the same block also as b and c. again with the definition of a partition a and c must be in the same block, so $a \sim c$ Hence $\sim$ is transitive.

3.5 Functions

function is generally represented in set-theoretic terms as a special kind of relation.

A function is a special type of relation. It is a relation with a special restriction on the first coordinate. For a relation to be a function, it must be the case that every element in its domain is associated to one and only one element in its range.

Definition 3.5.1 A function (mapping or transformation) f from A to B, denoted $f : A \to B$, is a relation$f \subseteq A \times B$ such that every element $a \in A$ is related to exactly one element $b \in B$.

In formal notation :

1. $\forall a \in A \; \exists! \; b \in B : (a, b) \in f$

2. $(a, b_1) \in f \; \wedge \; (a, b_2) \in f \Rightarrow b_1 = b_2$

By condition 1 we have for any $a \in A$ there exists a unique $b \in B$ such that $(a, b) \in f$. We usually write $f(a) = b$ or $a \longmapsto f(a)$ instead of $(a, b) \in f$.

If $f : A \to B$, we refer to the set A as the domain of f and the set B as the codomain. and if $b = f(a)$, then b is called the image of a and a is a pre-image of b under f.

Definition 3.5.2 Let $f : A \to B$ be a function. Suppose X is a subset of A, $X \subseteq A$. The image set $f[X]$ is defined by

$$\text{Img}f = f[X] = \{b \in B | (\exists a \in A)(b = f(a))\} = \{f(x) \in B \mid x \in X\}$$

If $Y \subseteq B$ then the pre-image $f^{-1}[f]$ is defined by

$$f^{-1}[Y] = \{x \in A \mid f(x) \in Y\}$$

A Function Must be Defined

Let $f : A \to B$ be a function. Note that by definition, f assgns to each element $a \in A$ a unique element $b \in B$. Thus, for f to be a function f must be defined on its entire domain.

Example 3.5.3 Let $A = \{a, b, c\}$ and $B = \{1, 2\}$. The relation $\varphi : A \to B$ defined by $\varphi(a) = 2$, $\varphi(b) = 1$ is not a function unless we also define $\varphi(3) =?$

This motivates the following definition which is a generalization of the concept of a function by defining f to just some elements of the domain not all of it.

Definition 3.5.4 A partial function$f$ from A to B, denoted $f : A \rightharpoonup B$, is a relation$f \subseteq A \times B$ such that some element $a \in A$ is related to exactly one element $b \in B$.

In formal notation :

1. $\exists! b \in B \; \forall a \in A : (a, b) \in f$

2. $(a, b_1) \in f \; \wedge \; (a, b_2) \in f \Rightarrow b_1 = b_2$

Be careful about the difference between definition of a function and a partial function. The only difference is that in condition 1, I swap $\forall$ and $\exists!$

A partial function from A to B denoted $f : A \rightharpoonup B$ is a function $f : X \to B$, for some subset $X \subset A$.

A Function Must be Well-Defined

Note that by definition, f assgns to each element $a \in A$ a unique element $b \in B$. That is, $f : A \to B$ is well-defined $\iff$ $\forall a_1, a_2 \in A$, if $a_1 = a_2$ then $f(a_1) = f(a_2)$.

By condition 2, a function must be well-defined.

Definition 3.5.5 (Equality of functions) Let $f : A \to B$ and $g : C \to D$ be functions.
$f = g \iff A = C, B = D$ and $f(a) = g(a)$ $\forall$a $\in A$

Definition 3.5.6 (Injective, surjective, bijective functions.) Let $f : A \to B$ be a function.

(1) **Injective function**
$f : A \rightarrowtail B$ is injective if and only if for each $b \in B$ there is at most one $a \in A$ with $f(a) = b$

$$(\forall a, a' \in A) \ [f(a) = f(a') \Rightarrow a = a']$$

Equivalently

$$(\forall a, a' \in A) \ [a \neq a' \Rightarrow f(a) \neq f(a')]$$

We also say that f is an injection, or a one-to-one correspondence.

(2) **Surjective function**
$f : A \twoheadrightarrow B$ is surjective if and only if every element of B is in the image of f:

$$(\forall b \in B) \ (\exists a \in A) \ [b = f(a)]$$

That is Img$f = B$.
We also say that f is a surjection, or f is a map onto B

(3) **Bijective function**
f is bijective if and only if it is both injective and surjective.

The notation $\rightarrowtail$ is used to denote that f is an injective map from A to B. Similarly $\twoheadrightarrow$ means that f is a surjective map.

Remark 1.Any function, $f : \emptyset \to B$ is trivially injective.

2. $f : \emptyset \to \emptyset$ is trivially surjective.

3. Since Img$f = \{b \in B | (\exists a \in A)(b = f(a))\}$, a function $f : A \twoheadrightarrow B$ is always surjective onto its image.

Example 3.5.7 Let $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$. The Cartesian product is

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}$$

A relation is just any subset of $A \times B$. It could be the entire set. Let $f_i \subseteq A \times B$ be defined by

1. $f_1 = \{(a, 1), (b, 3), (c, 2)\}$ is a function

$$\text{Img} f_1 = \{1, 3, 2\}$$

$$f^{-1}[B] = \{a, b, c\}$$

Also f_1 is injective and surjective.

2. $f_2 = \{(a, 1), (b, 3), (c, 1)\}$ is a function

$$\text{Img} f_2 = \{1, 3\}$$

$$f^{-1}[B] = \{a, b\}$$

Also f_3 is not injective and not surjective.

4. $f_4 = \{(a, 1), (b, 3)\}$ is **not** a function but a partial function.

$$\text{Img} f_4 = \{1, 3\}$$

$$f^{-1}[B] = \{a, b\}$$

Also f_4 is not injective and not surjective.

5. $f_5 = \{(a, 1), (b, 3), (c, 1)\}$ is **not** a function **nor** a partial function but a relation.

$$\text{Img} f_5 = \{1, 3\}$$

$$f^{-1}[B] = \{a, b, c\}$$

Also f_5 is injective but and not surjective.

Note that it is not possible in this example to define a function that is injective but not surjective or converse, because of the condition 2 in the definition of a function.

Example 3.5.8 Let $A = \{a, b, c\}$ and $B = \{1, 2\}$. It is not possible to define a function $f : A \to B$ that is injective, since $|A| > |B|$.

Think how can you prove it in terms of set theory, although it turns out not be possible to prove, so we make it as an axiom or principle.

Pigeonhole Principle

Let $f : A \to B$ be a function, where A and B are finite. If $|A| > |B|$, then f cannot be an injective function.

Use Pigeonhole Principle to following theorem

Theorem 3.5.9 Let A and B be finite sets, and let $f : A \to B$.

1. If f is one-to-one, then $|A| \leq |B|$.

2. If f is onto, then $|A| \geq |B|$.

3. If f is a bijection, then $|A| = |B|$.

Definition 3.5.10 Let A be a set. We define the function $id_A : A \to A$ by the rule

$$id_A(x) = x \ \ \forall \text{x} \in A.$$

ι_A is called the identity function.

Sometimes 1_A or ι_A are also used instead of id_A to indicate the identity function on A.

Definition 3.5.11 If $f : A \to B$ and $g : C \to A$ then the rule defined by

$$f \circ g(a) = f(g(a)) \quad \forall a \in A$$

defines a function $f \circ g$: C $\to B$. This function is called the **composition of** f **and** g**.**

Theorem 3.5.12 (Associativity) Let $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions.

Then

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

Proof Let $a \in A$. Then

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

The associativity rule can be extended to any finite arbitrary function. We can calculate

$$f_1 \circ (f_2 \circ (\ldots (f_{n-1} \circ f_n)))$$

in any oreder for example,

$$f_3 \circ f_1 \circ f_2 \circ \ldots f_n \circ f_{n-1}$$

Definition 3.5.13 A left inverse g (if it exists) to a function $f : A \to B$ is a function $f : B \to A$ such that $g \circ f = \mathrm{id}_A$.
A right inverse g (if it exists) to a function $f : A \to B$ is a function $g : B \to A$ such that $f \circ g = \mathrm{id}_B$,

Theorem 3.5.14 A function $f : A \to B$ has

(i) a left inverse $g : B \to A \iff$ it is injective .

(ii) a right inverse $g : B \to A \iff$ it is surjective.

(iii) an inverse $\iff$ it is bijective.

Proof $(i) \Rightarrow$ First, assume that there is such a g. To proof f is injective, suppose $f(x) = f(y)$. Then

$g(f(x)) = g(f(y)) \Rightarrow x = y$ Therefore, f is injective.

$\Leftarrow$ Assume that f is injective. $\forall y \in \mathrm{Im}\, f \; \exists! x \; s.t. \; f(x) = y$

Define $g : B \to A$ as follows:

$$\mathrm{g}\,(y) = \begin{cases} f^{-1}\,(y) & y \in \mathrm{Im}\,(f) \\ a & y \notin \mathrm{Im}\,(f) \end{cases}$$

$g \circ f = x = \mathrm{id}_A$.

Proof (ii) & (iii) as an exsersice.

Hint: Use the seconed form of the *Axiom of choice*, That is

For any relation R there is a function $H \subseteq R$ with Dom $H =$ Dom R

Corollary 3.5.15 From previous definition and theorem it turns out that left and right inverses dosen't have to be unique, but if $f : A \to B$ has an inverse, it is unique. In this case f is called an invertible function and it's inverse denoted by f^{-1}.

Theorem 3.5.16 If $f : A \to B$ is a bijection then the rule

$$\forall b \in B \; f^{-1}(b) = a \iff f(a) = b$$

defines a function $f^{-1} : B \to A$. The function f^{-1} is a bijection itself and satisfies

$f \circ f^{-1}$ = id$_B$ and $f^{-1} \circ f$ =id$_A$

The function f^{-1} defined in the above theorem is called the **inverse of** f.

Proof It is straightforward.

Theorem 3.5.17 Let $f : A \to B$ and $g : B \to C$.

(i) If f and g are injective then $g \circ f$: A $\to C$ is injective.

(ii) If f and g are serjective then $g \circ f$: A $\to C$ is serjective.

(iii) If f and g are bijective then $g \circ f$: A $\to C$ is also bijective. bijective.

Proof 1. Let $f : A \to B$ and $g : B \to C$ be injections. Let $a_1, a_2 \in A$ such that $g \circ f(\text{a}_1) = g \circ f(\text{a}_2)$.
Then $g(f(a_1)) = g(f(a_2)) \xrightarrow{g \text{ is injective}} f(a_1) = f(a_2) \xrightarrow{f \text{ is injective}} a_1 = a_2$

2. Let $f : A \to B$ and $g : B \to C$ be surjections. Let $c \in C$.
Since g is serjective, there exists $b \in B$ such that $g(b) = c$.
Since f is serjective, there exists $a \in A$ such that $f(a) = b$. By definition of a composition of function

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

3. It is a consequence of 1 & 2.

3.6 Set of all functions

Let $A = \{a, b, c\}$ and $B = \{1, 2\}$.

$$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

List the set of all functions from A to B.

$f_1 = \{(a,1),(b,1),(c,1)\}$ is a function.
$f_2 = \{(a,2),(b,1),(c,1)\}$ is a function.
$f_3 = \{(a,1),(b,1),(c,2)\}$ is a function.
$f_4 = \{(a,1),(b,2),(c,2)\}$ is a function.
$f_5 = \{(a,2),(b,1),(c,2)\}$ is a function.
$f_6 = \{(a,1),(b,2),(c,1)\}$ is a function.
$f_7 = \{(a,2),(b,2),(c,1)\}$ is a function.
$f_8 = \{(a,2),(b,2),(c,2)\}$ is a function.

The set of all functions $f : A \to B$ has $2^3 = 8$ elements.

Now list the set of all functions from B to A. The set of all functions $f : B \to A$ has $3^2 = 9$ elements.

An ordered pair $x = (x_1, x_2) \in R^2$, is a function $x : \{1,2\} \to R$.
An n-tuple $x = (x_1, x_2, \ldots, x_n) \in R^n$ is a function $x : \{1,2,\ldots,n\} \to R$.

Theorem 3.6.1 Let A and B be two set. The set of all functions $f : A \to B$ is denoted B^A or $\mathrm{Hom}(A,B)$ or $Fun(A,B)$ has $|B^A|$ elements.

Proof Suppose $|A| = m$ and $|B| = n$. Each element of A has n choice to be mapped to. since each element has n choice the number of all functions from A to B is $n \times n \times \cdots \times n = n^m = |B|^{|A|}$.

Exercise

1. Let $n \geq 2$ be an integer. Define a relation R on by $a \; R \; b$ if and only if $a^2 \equiv b^2 \pmod{n}$.

   (a) Prove that R is an equivalence relation when $n = 4$ and determine the distinct equivalence classes.

   (b) In general, under what conditions on n is R an equivalence relation?

   (c) When R is an equivalence relation, what are the equivalence classes?

2. Let R be a relation from a set A to a set B.

   (a) Prove that a relation R on a set A is symmetric if and only if $R = R^{-1}$.

   (b) Prove that a relation R on a set A is antisymmetric if and only if $R \cap R^{-1}$ is a subset of the diagonal relation $\Delta = \{(a, a) \mid a \in A\}$.

3. Let A, B, C, D be sets. Then:

   (a) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

   (b) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

   Consider the case (b) when the sets are empty.

4. Let $A = \{1, 2, 3\}$. Define a relation on A that is:

   (a) reflexive, not symmetric, not transitive

   (b) not reflexive, symmetric, not transitive

   (c) not reflexive, not symmetric, transitive

   (d) not reflexive, symmetric, transitive

   (e) reflexive, not symmetric, transitive

   (f) reflexive, symmetric, not transitive

   (g) not reflexive, not symmetric, not transitive

(h) reflexive, symmetric, transitive.

5. Define R on $\mathbb{N}$ by $mRn \iff 3|m+n$. Prove that R is not an equivalence relation on $\mathbb{N}$.

6. Let F be the collection of all finite sets. Define $\simeq$ on F by: $X \simeq Y$ if and only if there is a bijection $f : X \to Y$

   (a) Prove that $\simeq$ is an equivalence relation on F.

   (b) What are the equivalence classes of the sets , $\{\}, \{1, 2, 3\}$?

   (c) What is the equivalence class of the set $\{a_1, \ldots, a_n\}$ for any distinct objects $a_1, , a_n$?

7. Let f, g be functions.

   (a) Show that $f \cap g$ is a function.

   (b) Show that $f \cup g$ is a function if and only if

$$f(x) = g(x) \ \ \forall x \in (Domf) \cap (Domg)$$

Part II

Group Theory

Evariste Galois (1811–1832)

Galois was a tragic and romantic figure who died in a duel at age twenty. He was also one of the foremost mathematicians of all time. In his very brief life he created one of the great edifices of mathematics—Galois Theory—of fundamental importance to this day. He was born October 25, 1811, in Bourg-la-Reine, a village near Paris. His father was a progressive thinker who headed the liberal party in the town. He was elected mayor in 1815, the year in which Napoleon returned from exile on the island of Elba and took control for the period known as the Hundred Days. (Later in the year Napolean was exiled by the British to St. Helena.) This was the year the monarchy was restored, and, unlike in the eighteenth century, came to accept a Charter confirming most of the gains of the French Revolution. Galois' mother came from a family of jurists and received an education in the classics. She was his sole teacher for the first 12 years of his life, stressing the study of Greek and Latin. There is no evidence she taught him any mathematics beyond rudimentary arithmetic. But these were happy years for Galois, with no hint of the troubled times to come. His formal education began in 1823, when he enrolled in the Collège Royal de Louis-le-Grand, a Paris preparatory school (the alma mater of Robespierre and Hugo). It was at this time that he acquired his political consciousness. During the first term the students rebelled and refused to take part in the required religious observances. Scores were expelled for their disobedience. Galois was not among them, but the severity and apparent arbitrariness of the action made a deep impression on him. Galois' first two years at Louis-le-Grand were academically successful. He won several prizes in Greek and Latin and a number of honorable mentions. During his third year his work in rhetoric was poor and he had to repeat the year. Following this reversal he enrolled, at age fifteen, in his first mathematics course. This awakened his mathematical talent. The standard

mathematics texts were no challenge. He soon came across Legendre's Elements of Geometry and Lagrange's "The resolution of algebraic equations" and Theory of Analytic Functions. These fired the young Galois' imagination. Undoubtedly he was influenced in his subsequent work on Galois Theory by Lagrange's important paper "The resolution of algebraic equations". He later also read Abel's work on the subject. After these encounters with masterful mathematical works he seems to have lost all interest in his normal classes at the school. There soon followed a series of events which proved to be traumatic for the young Galois and soured him on authority. In 1828, at age sixteen, he applied, a year earlier than normal, to the very prestigious Ecole Polytechnique. But he failed the competitive entry exams. He blamed the failure on the ignorance of the examiners, but the most likely reason was his lack of preparation and communication skills. That year his father, whom he loved dearly, committed suicide as a result of persecution by authorities for his liberal views.

Galois began to make fundamental breakthroughs in the study of solvability of equations, and in early 1829 submitted a paper on the topic to the French Academy of Sciences. The referee was Cauchy, who did not present the paper to the Academy. Many sources have claimed that he lost the paper, but recent research has found otherwise. Here is Cauchy: I was supposed to present to the Academy . . . a report on the work of the young Galois . . .. Am indisposed at home. I regret not to be able to attend today's session and I would like you to schedule me for the following session.

Chapter 4

Algebraic Structure *

> *I think there is some change. If you went back to the 19th century or earlier, mathematicians and physicists tended to be the same people. But in the 20th century, mathematics became much broader and in many ways much more abstract. What has happened in the last 20 years or so is that some areas of mathematics that seemed to be so abstract that they were no longer connected with physics instead turn out to be related to the new quantum physics, the quantum gauge theories, and especially the supersymmetric theories and string theories that physicists are developing now.*
>
> Edward Witten, *Frontline*, 2001

A non-empty set together with one or more binary operation $+, \times, \ldots$ that satisfies certain property is called an algebraic structure. The set is called underlying set and the properties are called axioms.

Simple structures: no binary operation

Set A : A single set without having any operation.

Group-like structures: one binary operation

- Magma or groupoid $(M, \cdot)$:
  M and a single binary operation over M.

- Semigroup:
  1. $(M, \cdot)$ is a magma.
  2. $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \quad \forall g_1, g_2, g_3 \in M$

- Monoid $(M, \cdot)$:
  1. $g_1 \cdot g_2 \in M \quad \forall g_1, g_2 \in M$
  2. $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \quad \forall g_1, g_2, g_3 \in M$
  3. $e \cdot g = g \cdot e = g \quad \forall g, e \in M$,

- Group $(G, \cdot)$:
  1. $(G, \cdot)$ is a monoid
  2. $g \cdot g^{-1} = g^{-1} \cdot g = e \quad \forall g, g^{-1} \in G$

- Abelian (commutative) group $(G, +)$:
  $g_1 + g_2 = g_2 + g_1$

Ring-like structures or Ringoids: two binary operations

- Ring $(R, +, \cdot)$:
  1. $(R, +)$ is an Abelian group
  2. $(R, \cdot)$ is a monoid
  3. $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3, (r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$
- Division ring:
  1. $1 \neq 0$
  2. $(R \setminus \{0\}, \cdot)$ is a group
- Field:
  R is a division ring with commutative multiplication.

Module-like structures: Systems involving two sets and with at least two binary operations.

- Module$(M, R, +)$ or M over the ring R (R-module):

  1. (M, +) is an Abelian group
  2. $\forall n, m \in R \,\&\, \forall a, b \in M, na \in M$
     $(i)\ n(a+b) = na + nb$
     $(ii)\ (n+m)a = na + ma$
     $(iii)\ n(ma) = (nm)a$

     R itself is a special (one-dimensional) module over R.

- Vector space over R (R-vector space):

  R is a field. R itself is a special (one-dimensional) vector space over R.

- Algebra $(A, R, +, \cdot)$ or A (R-algebra):

  1. R is a commutative ring (with unity),
  2. $(A, R, +)$ is a module
  3. $(A, \cdot)$ is a monoid, and $\forall a, b, c \in A$ and $\forall n \in R$
     $(i)\ a \cdot (b+c) = a \cdot b + a \cdot c \qquad (a+b) \cdot c = ac + b \cdot c$
     $(ii)\ n(a \cdot b) = (na) \cdot b = a \cdot (nb)$

  R itself is a special (one-dimensional) algebra over R.

Chapter 5

Introduction to groups

> *Mathematicians do not study objects, but relations between objects. Thus, they are free to replace some objects by others so long as the relations remain unchanged. Content to them is irrelevant: they are interested in form only.*
>
> Henri Poincar,

In this chapter, along the way of our journey in mathematical structures we come up with one of the first and maybe for most important algebraic structure called **Group**.

It is hard to say when groups first appeared in mathematics since its application were used long before we even give an abstract definition of a group.

Euler (1761) and Gauss (1801) studied modular arithmetic, and Lagrange (1770) and Cauchy (1815) studied groups of permutations. Important moves towards a more formal, abstract theory were taken by Cauchy (1845), von Dyck (1882) and Burnside (1897). But it came to work magicaly as we shall see.

The story all begins with the pioneer work of young French mathematician **Evariste Galois**, who was working on insolvability of quintic equations. He died in May 31, 1832 at the young age of 20 in a duel over a whore girl. Before he dies he invented a language called **Group Theory** which is seems to be a good candidate to describe symmetry in mathematical structures. The notion of symmetry is universal ,all mankind have a universal understanding of the notion of symmetry. Moreover, every living creature knows what symmetry is. Even subatomic particles treatment correspond with symmetries of mathematical structures.

Groups are seems to be a good candidate to measuring the symmetry.

Symmetry appears everywhere in the world, from atomic scale (the quantum mechanics world) to galaxy (the relativistic world), So its mathematical co-exist ought to be very important .

Abstract Algebra is abstraction of our thought , it translate informal notions into its own magical language (which is build up from basic logic and set theory) and gives us new results which does not come up to our mind without it. As I mentioned language of Abstract Algebra is completely based on logic and set theory, so everything must be converted to its language.

The nature of symmetry is different from numbers or even object itself, yes we can associate a scale to a object for its number of symmetries, but in nature symmetry is not a number. Symmetry is more like a kind of transformation which can be applied to an object. If after the transformation the object looks the same as before that transformation is considered as a symmetry of the object. For example, one symmetry of a square is rotation by $\frac{\pi}{2}$. After rotating by $\frac{\pi}{2}$ the square looks the same as before. In set theoretic language this is a one-to-one and onto function (a bijection) from the set of vertices of square to itself. Another symmetry is rotation by π, it is a bijective function again. The set of all bijections from a set to itself, $i.e.$

$$Hom(A) = \{f \mid f : A \to A\}$$

has some properties :

1. The composition of functions is closed. $\circ : A \times A \to A$.
2. The composition of functions is associative.
3. The composition of functions contains an identity element which does noting.
4. The composition of functions contains an inverse for each transformation which gets back to the identity.

This Motivates the formal definition of a Group, but first we need some preliminaries.

5.1 Binery operation

Binery operation is a rule which takes two elements in the set A, combine them and give another element from the same set A.

Definition 5.1.1 A **binary operation** $*$ on a set A is a mapping or function $* : A \times A \to A$. That is, it sends elements of the Cartesian product $A \times A$ to A to A If $a, b, c \in A$ according to Axiom of Pairing $(a, b) \in A \times A$ exists. Instead of using the functional notation $*(a, b) = c$, we write $a * b = c$

Binary operations are usually denoted by special symbols such as

$$+, -, ., \times, \circ, \cup, \cap, \vee, \wedge$$

By the definition of function a binary operation is a triple $(A \times A, A, *)$ but as is usual in mathematics we write the binary operation $*$ instead of the binary operation $(A \times A, A, *)$

Remark In the definition of binary operation it is not necessary to point out the set must be non-empty. Beacuse a binary operation on A is a function $* : A \times A \to A$. If $A = \emptyset$ we have $\emptyset \times \emptyset = \emptyset$. so a binary operation on $\emptyset$ is a function $f : \emptyset \to \emptyset$. There is exactly one such function, the empty function.

The notion of operation is a generalization of function. In general, a function $f^A : \underbrace{A \times A \times \cdots \times A}_{n \text{ times}} \to A$ or $f^A : A^n \to A$ is called an n-ary operation and n is called the order of the nullary or its its **arity**. It is called nullary if $n = 0$, unary if $n = 1$ (it is a function), binary if $n = 2$, ternary if $n = 3$.

In the case of nullary $n = 0$, since A^0 is a singleton like $\{\emptyset\}$.

$$A^0 = \{\emptyset : \emptyset \to A\}$$

Since a binary operation is a function, it has to obey it's definition. The following lemma explains

Lemma 5.1.2 *Let $*$ be a binary operation on a set A. This must satisfy the following conditions:*

(a) $a \in A$ *and* $b \in A \Longrightarrow a * b \in A$. [$A$ is closed under $*$.]

(b) *For all* a, b, c, d *in* A
$a = c$ *and* $b = d \Longrightarrow a * b = c * d$. [Substitution is permissible.]

(c) *For all* a, b, c, d *in* A
$a = b \Longrightarrow a * c = b * c$. [Multiplication both side on the right.]

(d) *For all* a, b, c, d *in* A
$c = d \Longrightarrow a * c = a * d$. [Multiplication both side on the left.]

Proof multiply both sides of an equation on the right by the the same element

As we mentined if $a, b \in A$ according to Axiom of Pairing $(a, b) \in A \times A$ exists. Since $*$ is a function $* : A \times A \to A$ it assgns to (a, b) an element $a * b \in A$

$$*(a, b) = a * b \in A$$

This proofs (a).

For $*$ to be a function, it must satisfy well-defined condition

$$x = y \Longrightarrow *(x) = *(y)$$

and a function acts on ordered pairs, (a, b) where $a, b \in A$ which are a subset of the Cartesian product $A \times A$. Equality of ordered pairs is defined by the rule

$$a = c \ \wedge \ b = d \Longleftrightarrow (a, b) = (c, d)$$

To satisfy well-defined condition we must have

$$(a, b) = (c, d) \Longrightarrow a * b = c * d$$

According to equality of ordered pairs we have

$$a = c \text{ and } b = d \Longrightarrow a * b = c * d.$$

This Proofs **(b)**.

To prove **(c)** Take $a = b$ and by reflexivity of equality we have $c = c$. Substitution in part **(b)** we get $a * c = b * c$.

To prove **(d)** Take $c = d$ and by reflexivity of equality we have $a = a$. Substitution in part **(b)** we get $a * c = a * d$.

Binary operations are usually denoted by symbols such as

$$+, +_n, -, ., ._n, \times, \circ, \cdot, \cup, \cap, \vee, \wedge, \uplus$$

When we say A is closed under operation $*$ we mean $*(a, b) = a * b$ is on the same set A.

Let A be a set and f be a function

Definition 5.1.3 Let $*$ be a binary operation on a set A.

1. $*$ is **Commutative** if
$$a * b = b * a \quad \forall a, b \in A$$

2. $*$ is **Anti-commutative** if
$$a * b = -b * a \quad \forall a, b \in A$$

3. $*$ is **Associative** if
$$a * (b * c) = (a * b) * c \quad \forall a, b, c \in A.$$

4. $*$ satisfies **Jacobi identity**
$$a * (b * c) + c * (a * b) + b * (c * a) = 0 \quad \forall a, b, c \in A.$$

As we mentioned a binery operation is a function that is defined on a set, so it does not make sense to call a single operation $*$ is a binary operation without specifying underling set.

The most familiar example of binary operations are ordinary addition and multiplication.

Example 5.1.4 Addition is a binary operation on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Let $+$ be the addition operation on $\mathbb{Z}$.
$+ : \mathbb{Z} \times \mathbb{Z} \longmapsto \mathbb{Z}$ defined by $+(a, b) = a + b$

2. Multiplication is a binary operation on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

   $\times : \mathbb{Q} \times \mathbb{Q} \longmapsto \mathbb{Q}$ defined by $\times(a, b) = a + b$

3. Subtraction is a binary operation on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. But subtraction is not a binary operation on $\mathbb{N}$ since, for example, $7 - 5 \in \mathbb{N}$ but $5 - 7 \notin \mathbb{N}$.

4. Addition and multiplication are both associative and commutative operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ but Subtraction is niether associative nor commutative .

5. Division is not a binary operation on $\mathbb{R}$ because $1, 0 \in \mathbb{R}$ but $\frac{1}{0} \notin \mathbb{R}$. Thus $\mathbb{R}$ is not closed under division. If $*$ is not a function, but is a partial function instead, it is called a **partial binary operation**. Here division is a partial binary operation. In other word division is a binary operation on $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

   But addition is no longer a binary operation on $\mathbb{R}^*$; because $a, (-a) \in \mathbb{R}^*$ but $a + (-a) = 0 \notin \mathbb{R}^*$. So it does not worth to count division as a binary operation.

6. Let $M_n(K)$ be the set of all $n \times n$ matrices with entries from K. And let K denote each one of the following: $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

   We denote (i, j) entry of an $n \times n$ matrix A by a_{ij} ,

   Matrix addition and multiplication are defined by the following rules

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nm} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1m}+b_{1m} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2m}+b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \cdots & a_{nm}+b_{nm} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix} \times \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nm} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{12}b_{12} & \cdots & a_{1m}b_{1m} \\ a_{21}b_{21} & a_{22}b_{22} & \cdots & a_{2m}b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}b_{n1} & a_{n2}b_{n2} & \cdots & a_{nm}b_{nm} \end{pmatrix}$$

   where $a_i, b_j \in K$. Matrix addition and multiplication is a binary operation on $M_n(K)$.

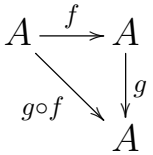
7. Recall the power set of the set A; that is, the set of all subsets of A denoted by $\mathcal{P}(A)$. If A_1, A_2 are subsets of A, then $A_1A_2, A_1 \cap A_2$ and $A_1 \setminus A_2$ are also subsets of A. Therefore, union, intersection and set theoretic difference are binary operations on the set $\mathcal{P}(A)$. Moreover, $\cup, \cap$ are both commutative and associative.

8. Let P be the set of all logical propositions. Then $\bigwedge$ and $\bigvee$ are binary operation on P.

9. Recall the set of all functions $f : A \to A$ denoted by A^A or $\mathrm{Hom}(A, A)$ or $Fun(A, A)$ or simply $Fun(A)$.

$$Fun(A) = \{f \mid f : A \to A\}$$

   Define a operations on $Fun(A)$ by composition of functions $\circ$. This is a binary operation because given functions $f : A \to A$ and $g : A \to A, i.e.\ f, g \in Fun(A)$ their composition $f \circ g$ is also a function $f \circ g : A \to A$.



Moreover, composition of functions $\circ$ is associative but not commutative .

10. The usual addition of vectors in Euclidean n-space as $\mathbb{R}^n$, $n \in \mathbb{N}$.

$$\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{R} \quad \forall i\}.$$

Thus $\mathbb{R}^2$ is the set of vectors in the plane, and $\mathbb{R}^3$ is the set of vectors in the space.

Componentwise addition is defined by the rule

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

is a binary operation since $(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \in \mathbb{R}^n$.

But scalar multiplication is not a binary operation, because if $\lambda \in \mathbb{R}$ and $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ scalar multiplication is defined as

$$\lambda x = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$$

Despite of the fact that $\lambda x \in \mathbb{R}^n$ but here we do not combine two elements of $\mathbb{R}^n$ so it is not a binary operation.

11. The dot product $X \cdot Y$ of vectors X and Y in $\mathbb{R}^n$ is not a binary operation. If

$$\begin{aligned} \mathbf{X} &= (x_1, x_2, \ldots, x_n) \\ \mathbf{Y} &= (y_1, y_2, \ldots, y_n) \end{aligned}$$

their dot product is defined to be

$$\mathbf{X} \cdot \mathbf{Y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$$

Notice that the result is not in $\mathbb{R}^n$, so the dot product is not a binary operation.

12. The cross product $\mathbf{A} \times \mathbf{B}$ of vectors $\mathbf{A}$ and $\mathbf{B}$ in $\mathbb{R}^3$ is a binary operation since it takes two vectors in $\mathbb{R}^3$ and produce another vector in $\mathbb{R}^3$. Recall that if

$$\begin{aligned} \mathbf{A} &= (a_1, a_2, a_3) \\ \mathbf{B} &= (b_1, b_2, b_3) \end{aligned}$$

then $\mathbf{A} \times \mathbf{B}$ is defined by the formula

$$\mathbf{A} \times \mathbf{B} = \left(\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, - \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}, \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \right)$$

However, the cross product of two vectors is not commutative $\mathbf{a} \times \mathbf{b} \neq \mathbf{b} \times \mathbf{a}$, but anti-commutative $\mathbf{A} \times \mathbf{B} = -\mathbf{B} \times \mathbf{A}$ or $[A, B] = [B, A]$

it is not even associative $A \times (B \times C) \neq (A \times B) \times C$, but it satisfies Jacobi identity

$$A \times (B \times C) + B \times (C \times A) + C \times (A \times B) = 0$$

or in closed form

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$$

The set $\mathbb{R}^3 = \{(a_i, b_i, c_i) \quad a, b, c \in R\}$ equipped with the cross product(**Lie bracket**) defined is a **Lie algebra**

Lie algebras are algebras satisfying anticommutativity and the Jacobi identity and two additional property, called **Bilinearity** and **Alternativity**.

Definition 5.1.5 If A is a non-empty set with binary operation $*$, then an element $e \in A$ is called a

(a) right identity if $a * e = a \quad \forall a \in A$

(b) left identity if $e * a = a \quad \forall a \in A$

If $e \in A$ is the right and left identity, e is called an identity element with respect to $*$. That is,

$$a * e = a = e * a \quad \forall a \in A$$

Example 5.1.6

1. $a \diamond b$ = max(a, b).
$e = 1$ is an identity element: $1 \diamond a = a \diamond 1 = a \quad \forall a \in$N

2. The identity element for addition and multiplication of $M_n(K)$ is e = O_n (the zero matrix) and $e = I_n$ (the identity matrix) respectivly.

3. $\circ$ on $Fun(A) = id$ (the identity map defined by $id(x) = x \forall x \in A$). Since, for any function $f : A \to A$ we have $f \circ id = id \circ f = f$.

Definition 5.1.7 If A is a non-empty set with binary operation $*$ and identity element e and $a \in A$. Then an element $a^{-1} \in A$ is called a

1. right inverse if $a * a^{-1} = e \quad \forall a \in A$
2. left inverse if $a^{-1} * a = e \quad \forall a \in A$

If $a^{-1} \in A$ is the right and left inverse, a^{-1} is called an (two-side)inverse with respect to $*$. That is,

$$a * a^{-1} = e = a^{-1} * a \quad \forall a \in A$$

a^{-1} is called an invertible element of a

In additive notation the inverse of an element is shown by $-a$ and in multiplicative notation by a^{-1}

Example 5.1.8

1. The identity element for addition of $\mathbb{Z}$ is $e = 0$, since
$0 + a = a = a + 0$ and for multiplication in $\mathbb{Z}$ is $e = 1$, since
$1.a = a = a.1$ But the identity element for subtracttion on $\mathbb{Z}$ does not exist. Beacuse we should have $e - a = a = a - e$ but $e - a = a \Rightarrow e = 2a$ and $a - e = a \Rightarrow e = 0$ Therefore, the inverse is not unique, so it does not exists.

2. 0 is a right identity for subtraction, but subtraction has no left identity.

Theorem 5.1.9 The identity element on a set A with respect to binary operation $*$ (if it exists) is unique.

Proof Suppose e_1, e_2 be identity elements with respect to $*$.

Definition 5.1.10 Let G be a set and $*$ a binary operation on G. A non-empty subset H of G is said to be closed respect to $*$ if, for every pair (x, y) of elements of H, also $x * y$ belongs to H. That is,

$$\forall a, b \in H \Rightarrow a * b \in H$$

Example 5.1.11 Recall $\mathbb{Z}_n$ for the set of all congruences classes modulo n.

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\} = \{[0], [1], \ldots, [n-1]\}$$

In previous chapters we introduced operations of addition and multiplication for congruence classes.

Definition 5.1.12 Let $a, b \in \mathbb{Z}_n$. Take $x, y \in \mathbb{Z}$ such that $a = [x], b = [y]$. The addition of two elements is defined as

$$a + b = [x] + [y] := [x + y]$$

or sometimes

$$a +_n b = [x] +_n [y] := [x + y]_n$$

Also The multiplication of two elements is defined as

$$a.b = [x].[y] := [x.y]$$

or

$$a._n b = [x]._n [y] := [x.y]_n$$

Every congruence class can be represented by any one of its elements, we have to show the operations defined does not depend on representative of the class (It is well-defined) .

Theorem 5.1.13 The addition and multiplication defined for congruence classes is a binary operation .

$+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ where $+_n([a],[b]) \longmapsto [a +_n b]$ and

$._n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ where $._n([a],[b]) \longmapsto [a._n b]$

Proof Let $x' \in [x]$ and Let $y' \in [y]$. We show $[x+y] = [x'+y']$ and $[x.y] = [x'.y']$. $x' = x + mk$ and $y' = y + mt$ forsome $k, t \in \mathbb{Z}$. Therefore, $x' + y' = (x + y) + m(k + t)$ and $x'.y' = (x.y) + m(xt + yk + mkt)$.

So $x' + y' = x + y \pmod m$ and $x'.y' = x.y \pmod m$.

Thus, $[x' + y'] = [x + y]$ and $[x'.y'] = [x.y]$.

The operaton $+_n$ and $._n$ are commutative and associative. 0 is additive identity and 1 is multiplicative identity.

Every element of $\mathbb{Z}_n$ is invertible with respect to $+_n$

$$-a = \begin{cases} n - a & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}$$

5.2 Cayley Table

Recall the definition of a binary operation on a set A, it is a rule which $\forall a, b \in A$ produces a third element back in A again. So if the set A is finite, this is possible to determine by means of a composition table, for any pair of elements of A what the third element is.

Let $A = \{a_1, a_2, ..., a_n\}$ be a finite set, and let $*$ be a binary operation on A. The multiplication table of $*$ is a square table of size $|A| \times |A|$.

$\circ$	a_1	a_2	a_3	$\dots$	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	$a_1 \circ a_3$	$\dots$	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	$a_2 \circ a_3$	$\dots$	$a_2 \circ a_n$
a_3	$a_3 \circ a_1$	$a_3 \circ a_2$	$a_3 \circ a_3$	$\dots$	$a_3 \circ a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	$a_n \circ a_1$	$a_3 \circ a_2$	$a_3 \circ a_3$	$\dots$	$a_3 \circ a_n$

This multiplication table usually called a **Cayley table**[1].

Remark A binary operation is commutative if and only if its multiplication table is symmetric with respect to the main diagonal.

Example 5.2.1 The set $\mathbb{Z}_8$ consists of $[0], [1], [2], [3], [4], [5], [6], [7]$. Addition and multiplication rule can be given by a table.

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\cdot_8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Number of binary operation on a set

Since a binary operation is a function $f : A \times A \to A$ we can apply the rules of counting to determine how many binary operations can be defined on a given set with n element.

The number of binary operation on a set $|A| = n$ $f : A \times A \to A$ is $|A|^{|A\times A|} = n^{n^2}$. Furthermore, we can also determine the number of commutative binary operation on a given set.

Let $A = \{a_1, a_2, \dots, a_n\}$ then recall the operation $*$ is said to be commutative if

$$a_i * a_j = a_j * a_i \quad \forall a_i, a_j \in A$$

[1] In the honors of British mathematician Arthur Cayley 1821 - 1895.

In $A \times A$ there are n ordered pairs (a_i, a_j) and $\binom{n}{2}(a_i, a_j)$ and $\binom{n}{2}(a_j, a_i)$, so the number of all elements (ordered pairs) are

$$n + \binom{n}{2} + \binom{n}{2} = n^2$$

Because we want commutative binary operations, that is $*(a_i, a_j)$ and $*(a_j, a_i)$ must map to the same value in the set. So we should throw away one of $\binom{n}{2}$ of ordered pairs. Now the restricted set $A \times A$ has caedinality $n + \binom{n}{2}$

Therefore, commutative binary operations from restricted set $A \times A \to A$ has cardinality

$$n^{n+\binom{n}{2}} = n^{\frac{n^2+n}{2}}$$

Corollary 5.2.2 More than half binary operations on a finite set are commutative.

Lemma 5.2.3 *For a given set* $|A| = n$

(a) The number of operations containing an identity is $n^{(n-1)^2+1}$

Proof Exersice

Unfortunetly, it appears that there is no closed formula for counting the number of associative binary operations on a set.

Example 5.2.4 Let $A = \{a, b\}$ be a with two elements. The number of different binary operations on this set is $2^{2^2} = 16$. Those operations are:

1)
$*$		
	a	a
	a	a

2)
$*$		
	a	a
	a	b

3)
$*$		
	a	a
	b	a

4)
$*$		
	a	b
	a	a

5)
$*$		
	b	a
	a	a

6)
$*$		
	a	a
	b	b

7)
$*$		
	a	b
	a	b

8)
$*$		
	b	a
	a	b

9)
$*$		
	a	b
	b	a

10)
$*$		
	b	a
	b	a

11)
$*$		
	b	b
	a	a

12)
$*$		
	a	b
	b	b

13)
$*$		
	b	a
	b	b

14)
$*$		
	b	b
	a	b

15)
$*$		
	b	b
	b	a

16)
$*$		
	b	b
	b	b

Eight operations are commutative. See tables 1, 2, 7, 8, 9, 10, 15 and 16. Eight operations are associative. See tables 1, 2, 4, 6, 7, 8, 10 and 16. Six operations are both commutative and associative. See tables 1, 2, 7, 8, 10 and 16. For four operations there exists an identity in S. See tables 2, 7, 8 and 10. For four operations there exists a zero in S. See tables 1, 2, 8 and 16. For two operations there exist both an identity and a zero in S. See tables 2 and 8.

5.3 Definition and Examples of Groups

Definition 5.3.1 [Group]

A **group** is a pair $(G, *)$ consisting of a (non-empty) set G together with a defined binary operation $*$ that satisfies following axioms:

1. *Associativity:* $\forall a, b, c \in G, a * (b * c) = (a * b) * c$
2. *Identity:* $\exists e \in G, \forall a \in G, \ such\ that\ e * a = a = a * e$
3. *Inverse:* $\forall a \in G, \exists a^{-1} \in G, \ such\ that\ a^{-1} * a = e = a * a^{-1}$

Notation Remark

1. If binary operation in the group is multiplication $(G, .)$, for $a, b \in G$ we write $a.b$. In this case we denote the identity element by 1 and the inverse of $a \in G$ with a^{-1}.

2. If binary operation in the group is addition $(G, +)$, for $a, b \in G$ we write $a + b$. In this case we denote the identity element by 0 and the inverse of $a \in G$ with $-a$.

3. For the sake of simplicity, when it is clear what the binary operation is, then the group $(G, *)$ may be referred to by its *underlying set* G alone and for $a, b \in G$ we write $a.b$ or even simpler ab instead of $a * b$.

Remark Some books mention *closure* as first property, but since we defined binary operation to be a function $G \times G \to G$, closure is direct consequence of a binary operation.

2. The empty set does not admit a group structure because it does not contain the identity element.

3. An identity element $e \in G$ is a condition for all elements of the group since it depends on the binary operation $*$ not on the elements, whereas an inverse element $a^{-1} \in G$ is defined relative to a single element of G.

4. The order of axioms 3 and 4 in the definition above is important, since it is impossible to talk about an inverse of an element until existence of an identity is unknown.

5. In the definition of a group G we do not require commutativity as the composition of functions is not commutative.

Definition 5.3.2 A group G is called **abelian**[2](or commutative), if the group operation is commutative . That is,

$$a * b = b * a \quad \forall a, b \in G$$

If the group we are considering is abelian we frequently use additive notation, and for non-abelian group we use multiplicative notation. The reason for this distinction is that we are used to multiplication being non-commutative (multiplication of matrices and of permutations are non-commutative).

Definition 5.3.3 The order of a group G, denoted by $|G|$, is the number of elements in G.

If $|G|$ is a finite number, then the group is a finite group. If $|G|$ is infinite and if its elements are labeled by n continuous real parameters, then G is a **Continuous group or Topological group** with dimension n.

1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}^n, +), (n\mathbb{Z}, +)$ are examples of group structures on familiar number systems. The inverse of $x \in$ is $-x$. Lets check $(\mathbb{Z}, +)$ for example,

(a) $+$ is a binary operation on $\mathbb{Z}, i.e. + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

(b) Numbers addition is associative $a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Z}$

(c) $\exists\, 0 \in \mathbb{Z}$ satisfying $0 + n = n + 0 = n \quad \forall n \in \mathbb{Z}$

(d) $\forall n \in \mathbb{Z}\ \exists - n \in \mathbb{Z}$ such that $(-n) + n = n + (-n) = 0$

2. $(\mathbb{N}, +)$ is not a group, since it does not contain inverse element, $-n \notin \mathbb{N}$.

3. Let $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ the set of all non-zero real numbers. $(\mathbb{R}^*, .)$ is a group. Also as $(\mathbb{Q}^*, .)$,$(\mathbb{C}^*, .)$ with the identity element being 1 and the inverse of x being $\frac{1}{x}$

4.

5.4 Groups of modular arithmetic

Recall congruent class mod n

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\} = \{[0], [1], \ldots, [n-1]\}$$

Convention

[2]In the honors of norwegian mathematician Niels Henrik Abel (1802-1829).

1. For the sake of simplicity, I drop the overline for the element $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ but we mean as before the set of equivalence classes not just single elements.

2. Since it is clear, we may use just $+$ and $.$ instead of $+_n$ and $._n$ respectively.

$(\mathbb{Z}_n, +_n)$ forms a group, Because

1. $+$ is a binary operation on $\mathbb{Z}_n, i.e. + : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$.
2. $a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Z}_n$
3. $\exists\, 0 \in \mathbb{Z}$ satisfying $0 + n = n + 0 = n \quad \forall n \in \mathbb{Z}_n$
4. $\forall a \in \mathbb{Z}_n \;\; \exists(-a) = (n - a) \in \mathbb{Z}$ such that $(-a) + a = a + (-a) = 0$

$\mathbb{Z}_n$ is called the **cyclic group** of order n.

But $(\mathbb{Z}_n, ._n)$ is not a group, Because for example 0 does not have a multiplicative inverse.

The Cayley table of addition and multiplication for the *set* $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is as follows.

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\cdot_8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Only $(\mathbb{Z}_n, +_n)$ is a group.

Here we use some terminology to make a multiplicative group out of $\mathbb{Z}_n$.

Definition 5.4.1 Let $a \in \mathbb{Z}_n$. a is called a **unit** if there is an element $b \in \mathbb{Z}_n$ such that

$$ab = 1 \pmod{n}$$

We denote the set of all units in $\mathbb{Z}_n$ by U_n. We call U_n the **group of units of** $\mathbb{Z}_n$.

Theorem 5.4.2 $a \in \mathbb{Z}_n$ has a unit $\iff$ $(a, n) = 1$.

Proof $\Longleftarrow$ Suppose $a \in \mathbb{Z}_n$ has a unit, so $ak = 1$ for some $k \in \mathbb{Z}_n$ or $ak = 1 \pmod{n}$. Therefore, $ak - 1 = mn$ for some $m \in \mathbb{Z}$. So, $ak - mn = 1$
This is a linear combination of a and n which gives 1. Therefore $(a, n) = 1$.

$\Longrightarrow$ Conversely, suppose $(a, n) = 1$. There exists $k \; and \; m$ such that $ak + mn = 1$. That is, $ak = 1 \pmod{n}$ or

$$ak = 1 \text{ for some } k \in \mathbb{Z}_n$$

Corollary 5.4.3 For $n \geq 2$, $U_n = \phi(n) = \{a \in \mathbb{Z}_n : (a, n) = 1\}$.

In number theory the order of U_n is obtained from, is called the *Euler totient function* $\phi(n)$.

$\phi(n)$ is the of numbers which are relatively prime to n.

In particular, U_p, where p is a prime is a group with $p - 1$ elements. namely

$$U_p = \{1, 2, \ldots, p - 1\}$$

Here, the group of units of $\mathbb{Z}_8$

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

It is easy to check that each element of this group is self-inverse.

5.5 Groups of permutation

Next chapters

5.6 Basic Properties Of Groups

Theorem 5.6.1 Let G be a group and $a, b, c, \in G$. Then

(i) $\exists! e \in G$.

(ii) $\forall a \in G \; \exists! a^{-1} \in G$.

(iii) If $ab = ac$ then $b = c$. (left cancellation law)

(iv) If $ba = ca$ then $b = c$. (right cancellation law)

Proof (i) Suppose e_1 and e_2 are identities of G.

$e_1.a = a.e_1 = a \qquad \& \qquad e_2.a = a.e_2 = a$

Put e_2 instead of a, we have

$$e_1.e_2 = e_1 = e_2.e_1 = e_2$$

(ii) Suppose $a \in G$ has two inverses $b, c \in G$

$$b = be = b(ac) = (ba)c = ec = c$$

(iii) Suppose $ab = ac$.

$$a^{-1}(ab) = a^{-1}(ac)$$

By associative law,

$$\begin{aligned} (a^{-1}a)b &= (a^{-1}a)c \\ eb &= ec \\ b &= c \end{aligned}$$

(iv) The proof is similar to (iii)

Corollary 5.6.2

Theorem 5.6.3 [The Generalized Associative Law] Let $*$ be an associative binary operation on a set A. If $a_1, a_2, \ldots, a_n$ is a sequence of $n \geq 3$ elements of A, then the product

$$a_1 * a_2 * \cdots * a_n$$

is unambiguous; that is, the same element will be obtained regardless of how parentheses are inserted in the product (in a legal manner).

Proof The general case can be proved by induction on n. Do it as an excersice.

The Generalized Associative Law allows us to define integral powers of an element $a \in G$ inductively.

$$a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ times}}$$

Definition 5.6.4 For any $a \in G$ we define

$$a^n = \left\{ \begin{array}{ll} a^n & \text{for } n > 0 \\ e & \text{for } n = 0 \\ (a^{-1})^n & \text{for } n < 0 \end{array} \right\}$$

In additive group

$$na = \underbrace{a + a + \cdots + a}_{n \text{ times}}$$

For any $a \in G$ we define

$$na = \left\{ \begin{array}{ll} na & \text{for } n > 0 \\ 0 & \text{for } n = 0 \\ -na & \text{for } n < 0 \end{array} \right\}$$

Theorem 5.6.5 Let G be a group and $a, b, c, \in G$. Then

$(i)\ \forall a \in G\ \ (a^{-1})^{-1} = a$

$(ii)\ \forall a, b \in G\ \ (ab)^{-1} = b^{-1}a^{-1}$

Proof (i) If $a \in G$ then since

$$aa^{-1} = a^{-1}a = e$$

a is an inverse of a^{-1}. Since inverses are unique then $(a^{-1})^{-1} = a$.

(ii) Let x be the inverse of ab. Then $(ab)x = e$ By associativity, we have $a(bx) = aa^{-1}$. By left cancellation law, we have $bx = a^{-1}$. But

$$bx = ea^{-1} = b(b^{-1}a^{-1})$$

using left cancellation again $x = (b^{-1}a^{-1})$. Therefore, $(ab)^{-1} = (b^{-1}a^{-1})$.

Proposition 5.6.6 *If G is a group and $a, b \in G$ each of the equations $ax = b$ and $xa = b$ has a unique solution in G.*

Proof

$$x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b$$
$$x = xe = x(aa^{-1}) = (xa)(a^{-1}) = ba^{-1}$$

These are unique since inverses are unique.

$$a^{-1}b = ba^{-1}$$

Corollary 5.6.7 If G is a group and $a, b \in G$. if either $ab = e$ or $ba = e$ then $b = a^{-1}$.

Theorem 5.6.8 [Laws of Exponents for Groups] Let G be a group with identity e. Then $\forall a, b \in G$ and $n, m \in \mathbb{Z}$ we have

(i) $a^n a^m = a^{n+m}$

(ii) $(a^n)^{-1} = a^{-n}$

(iii) $(a^n)^m = a^{nm}$

(iv) $(a^n)^m = a^{nm}$

(v) $(ab)^n = a^n b^n$ if $ab = ba$

Proof Exersice

According to these facts, we have an improtant result about Cayley table (multiplication table) of a finite group.

Lemma 5.6.9 *Let $G = \{a_1, a_2, \ldots, a_n\}$ be a finite group. Then in any row and column of the multiplication table of G, each element of G appears exactly once.*

Assume that the elements $a_1, a_2, \ldots, a_n$ of G are distinct. The $i - th$ row of the multiplication table is

$$a_i a_1, a_i a_2, \ldots, a_i a_n$$

All these elements are distinct as listed. Indeed, if $a_i a_j = a_i a_k$ for $j \neq k$, then the Cancelation Lemma implies that $a_j = a_k$ contradicting the assumption that $a_j \neq a_k$ for $j \neq k$. Hence the n elements are all distinct, so each element of must appear, and it can only appear once.

Proof Exersice

Niels Henrik Abel (1802-1829)

Was a Norwegian mathematician who was born on Augusts'5 1802 and Died 6 April 1829. He entered the cathedral school at the age of 13. Anew mathematics teacher, Bront Michael Holmloe saw his talent in mathematics and encouraged him to study the subject to advanced level. Bernt Holmboe supported Abel with a scholarship to remain at school and raised many from his friends to enable him to study at the Royal Fredrick University. Abel started working on the quintic equation in radicals At the age of 19, he solved a problem that had vexed leading mathematicians for hundreds of year. He proved that, unlike the situation for equations of degree 4 or less, there is no finite formula for the solution of the general fifth degree equation. This question had been unresolved for 250 years. Most of his work was done in six or seven years of his working life. Abel thought that he had solved the problem and submitted his work for publication. Unable to find an error and understand his arguments he was asked by the editor to illustrate his method. In 1824, during the process of illustration he discovered an error. This discovery led Abel to a proof that no such solution exists. He also worked on elliptic functions and essence revolutionized the theory of elliptic functions. He traveled to Paris and Berlin in order to find a teaching position .Then poverty took its toll, and Abel died from tuberculosis on April, 1829. Two days later a letter from Crelle reached his address, conveying the news of his appointment to the professor ship of mathematics at the University of Berlin. Abel is honored by such terms as Abelian group and Abelian function.

Chapter 6

Subgroup And Cyclic group

> *By a small sample we may judge of the whole piece.*
>
> Miguel De Cervantes, *New Scientist*

6.1 Subgroup

Despite of the basic definiton of a group, it has a very reach structure. Recognition of these structures help us to recognize the entire group. We are interested in breaking up a group into smaller peaces which have the same structure as a group, and instead of studying the whole group consider those smaller peaces. For some reason as I mentioned we restrict those peaces to be groups themselves.

Definition 6.1.1 Let $(G, *)$ be a group. H is a **Subgroup** of a group $(G, *)$ if $H \subseteq G$, and $(H, *)$ is a group.

We usually write to denote that H is a subgroup of G.

If $H \leq G$ and $\{e\} \subset H \subset G$ we say that H is a *proper subgroup* of G and we write $H < G$.

Remark Note that form the definition it arise that the subset H is a subgroup of G with respect to the same operation that makes G a group. For example $\mathbb{Z}_n \subset \mathbb{Z}$ but $\mathbb{Z}_n \nleq \mathbb{Z}$.

The trivial subgroup e and G are always subgroups of G. Because according

to *axiom of extensionality* every set is subset of itself so $G \leq G$ and since G is a group, it is a subgroup of itself.

A subgroup is therefore a group which sits inside the original group.

Since $(H, *)$ is a subgroup it must satisfy group properties. That is,

1. *Closure:* $\forall a, b \in H \; ab \in H$.
2. *Associativity:* $a(bc) = (ab)c$
3. *Identity* : $e_H = e_G$
4. *Inverse*: $\forall a \in H, \exists a^{-1} \in H, \; such \; that, a * a^{-1} = a^{-1} * a = e_H$

But we do not need to check all of them. Only two condition 1 and 4 are sufficient. Because :

1.If a set is associativity every subset of it is associativity again.

2.If $a \in H$ and $a^{-1} \in H$ then $aa^{-1} = a^{-1}a = e \in H$

Lets make it as a theorem.

Theorem 6.1.2 Let G be a group. $H \subseteq G$ is a group if and only if

$(i) \; \forall a, b \in H \; ab \in H$.

$(ii) \; \forall a \in H \; a^{-1} \in H$.

Proof

$\Longrightarrow$ If H is a subgroup then obviously $(i), (ii)$ are hold.

$\Longleftarrow$ Assume $(i), (ii)$ are hold. From $(i), (ii)$ and substituting $b = a^{-1}$ we can conclude $e \in H$. So H is a subgroup.

This theorem holds in general group whether finite or infinite. But in finite case it is just enough to check *Closure*.

Theorem 6.1.3 Let G be a *finite* group. $H \subseteq G$ is a group if and only if

$(i) \; \forall a, b \in H \; ab \in H$.

Proof

$\Longrightarrow$ If H is a subgroup then by definition it is closed.

$\Longleftarrow$ We are assuming that H is closed, so it needs to contain at least an element.
If H only contains e, trivially H is a subgroup.
If H contains an element $a \neq e$. Since H is closed, the elements

$a^2 = a.a$, $a^3 = a.a.a\ldots$, $a^n = a.a\ldots a$ are in H.

Since G is finite, the powers of a must coincide somewhere, so for some $1 \leq m < n$ we have

$$a^m = a^n$$
$$a^{n-m} = e$$

Therefore, $e \in H$. We also have $a^{n-m-1} = a^{-1} \in H$.

Hence, H is a subgroup of G.

Corollary 6.1.4 (The Subgroup Criterion) Let G be a group and let H be a nonempty subset of G. Then

$$H \leq G \iff ab^{-1} \in H \ \ \forall a, b \in H$$

Proof $\implies$ *Suppose* $H \leq G$, and $a, b \in H$. Then $b^{-1} \in H$, so $ab^{-1} \in H$ since H is closed.

$\impliedby$ Suppose $ab^{-1} \in H \ \ \forall a, b \in H$. Since $H \neq \emptyset$ take $a = b$.

Then $e = aa^{-1} \in H$. Since e $\in H$, for any $a \in H, a^{-1} = ea^{-1} \in H$.

Now if $a, b \in H$, then $b^{-1} \in H$, therefore $ab = a(b^{-1})^{-1} \in H$. Hence $H \leq G$

Example 6.1.5

1. The set $2\mathbb{Z} = (Even\ integers, +)$ is a subgroup of $(\mathbb{Z}, +)$. Because

(a) *Closure* : $\forall a, b \in 2\mathbb{Z}\ a = 2n,\ b = 2m$ for some $n, m \in \mathbb{Z}$.

(b) *Inverse* : $\forall a \in 2\mathbb{Z}\ a = 2n$ for some $n \in \mathbb{Z},$ and $-a = -2n = 2(-n) \in 2\mathbb{Z}$.

Therefore, $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$.

2. In general $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. Both are subgroups of $(\mathbb{Q}, +)$.

$$n\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q}$$

3. The subset $H = \{0, 2\}$ is the only proper subgroup of $\mathbb{Z}_4$, because it is closed

$$0 +_n 0 = 0, \quad 0 +_n 2 = 2 +_n 0 = 2, \quad 2 +_n 2 = 0$$

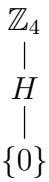
and contains inverses

$$0 +_n 0 = 2 +_n 2 = 0$$

If H is any other subgroup that contains another element, say 1, it must contains

$$1 +_n 1 = 2, \quad 1 +_n 1 +_n 1 = 3, \quad 1 +_n 1 +_n 1 +_n 1 = 0$$

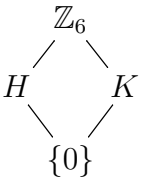
so H is includes entire group, That is $H = \mathbb{Z}_4$.



Definition 6.1.6 If G is a group and S is the set of all subgroups of it, then $(G, \subseteq)$ is called a *subgroup lattice*. The largest subgroup is at the top, the smallest is at the bottom, and the relationship between two subgroups $K \subseteq H$ given by a vertical line.

Lattice of a subgroup and **Cayley Diagrams** are the best way of visualizing a group.

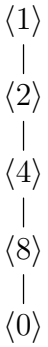
Example: $H = (\{0, 2, 4\}, +_6)$ and $K = (\{0, 3\}, +_6)$ are subgroups of $(\mathbb{Z}_6, +_6)$.



Example 6.1.7 Draw the subgroup lattice of $(\mathbb{Z}_{16}, +_{16})$. The subgroups of $\mathbb{Z}_{16}$ are $\langle 0\rangle, \langle 2\rangle, \langle 4\rangle, \langle 8\rangle, \langle 1\rangle = \mathbb{Z}_{16}$

The only chain is $\langle 0\rangle < \langle 8\rangle < \langle 4\rangle < \langle 2\rangle < \langle 1\rangle$.

The lattice of subgroups is :



The union of subgroups is not necessarily a subgroup, but the intersection of subgroups is always a subgroup.

Example 6.1.8

1. $2\mathbb{Z} \leq \mathbb{Z}$ and $3\mathbb{Z} \leq \mathbb{Z}$ but $2\mathbb{Z} \cup 3\mathbb{Z} \nleq \mathbb{Z}$ since, $2 + 3 = 5 \nleq 2\mathbb{Z} \cup 3\mathbb{Z}$.

2. Consider $(\mathbb{R}^2, +)$ which forms a group. The following sets are subgroups of $\mathbb{R}^2$.

$$A = \{(a, 0)|a \in \mathbb{R}\} \qquad and \qquad B = \{(0, b)|b \in \mathbb{R}\}$$

But $A \cup B$ is not a subgroup because it's not closed under addition. That is, $(a, 0) \in A$ and $(0, b) \in B$, but

$$(a, 0) + (0, b) = (a, b) \notin A \cup B$$

Theorem 6.1.9 The intersection of any arbitrary collection of subgroups of a group is again a subgroup.

Proof $Let\{H_i\}_{i\in I}$ be an be an arbitrary collection of subgroups of a group G. We show $\bigcap_{i\in I} H_i$ is also a subgroup of G.

Since $\forall i \in I,\ e \in H_i$, we have $e \in \bigcap_{i\in I} H_i$. So $\bigcap_{i\in I} H_i \neq \emptyset$ and $\bigcap_{i\in I} H_i \subseteq G$. Now let $a, b \in \bigcap_{i\in I} H_i$,so we have $a, b \in H_i$ for all $i \in I$. Then $ab^{-1} \in H_i$ for all $i \in I$, since each H_a is a subgroup.

This shows that $ab^{-1} \in H_i$ for all $i \in I$. From the subgroup criterion

$$\bigcap_{i\in I} H_i \leq G$$

6.2 Cyclic Group

There is a certain kind of group which arise when we collect the set of all integral exponents of an element $a \in G$ which forms a subgroup of G.

Theorem 6.2.1 Let G be a group and $a \in G$. Then the set

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

is a subgroup of G. Also $\langle a \rangle$ contains a and is the smallest subgroup of G that contains a.

Proof The set $\langle a\rangle$ is nonempty since $a^0 = e \in \langle a\rangle$.
$\forall x, y \in \langle a\rangle \quad x = a^m \; and \; y = a^n$ for some integers m and n. Then

$$xy^{-1} = a^m a^{-n} = a^{m-n} \in \langle a\rangle.\blacksquare$$

Since $a = a^1$ it is clear that $a \in \langle a\rangle$. If H is any subgroup of G that contains a, since H is closed under taking products and taking inverses, $a^n \in \langle a\rangle$ for every $n \in \mathbb{Z}$. So $\langle a\rangle \subseteq H$. That is, every subgroup of G that contains a also contains $\langle a\rangle$. This implies that $\langle a\rangle$ is the smallest subgroup of G that contains a.

Definition 6.2.2 Let a be an element of the group G. Define

$$\langle a\rangle = \{a^n : n \in \mathbb{Z}\} = \{\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots\}$$

And in additive group

$$\langle a\rangle = \{na : n \in \mathbb{Z}\} = \{\ldots, -3a, -2a, -a, 0a, a, 2a, 3a, \ldots\}$$

We call $\langle a\rangle$ the **cyclic subgroup of** G **generated by** a.

Remark Note that

$$\langle a\rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots\}.$$

In particular, $a = a^1$ and $e = a^0$ are in $\langle a\rangle$.

Definition 6.2.3 A group G is **Cyclic** if $\exists a \in G$, such that,

$$G = \langle a\rangle = \{a^n : n \in \mathbb{Z}\}$$

Definition 6.2.4 Let $a \in G$. the order of a is the smallest positive integer $n \in \mathbb{N}$ such that $a^n = e$. That is,

$$\mathrm{o}(a) = \min\{n \in \mathbb{N} \,|\, a^n = e\}$$

If there exists such n we say that a has **finite order**.
And we define If $a^n \neq e$ for all $n \in \mathbb{N}$, we say that a has **infinite order** and we define

$$\mathrm{o}(a) = \infty.$$

In either case we call $\mathrm{o}(a)$ the **order** of a is denoted by $\mathrm{o}(a)$ or $|a|$.

Example 6.2.5 $(\mathbb{Z}, +)$ is a cyclic group of infinite order.

$$\langle 1\rangle = \langle -1\rangle = \langle \mathbb{Z}\rangle$$

2. $(\mathbb{Z}_n, +)$ is a cyclic group of finite order.

$$\langle \{a : (a, n) = 1\} \rangle = \langle \mathbb{Z}_n \rangle$$

3. The cyclic subgroup of $\mathbb{C}^*$ generated by i is

$$\langle i \rangle = \{\ldots, i^{-4}, i^{-3}, i^{-2}, i^{-1}, i^0, i^1, i^2, i^3, i^4, \ldots\} = \{i, -1, -i, 1\}$$

Example 6.2.6 Let $G = \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

$$\langle 1 \rangle = \{n : n \in \mathbb{Z}\} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = \mathbb{Z}_{12}$$
$$\langle 2 \rangle = \{2n : n \in \mathbb{Z}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} = \{0, 2, 4, 6, 8, 10\}$$
$$\langle 3 \rangle = \{3n : n \in \mathbb{Z}\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = \{0, 3, 6, 9\}$$
$$\langle 4 \rangle = \{4n : n \in \mathbb{Z}\} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\} = \{0, 4, 8\}$$
$$\langle 5 \rangle = \{5n : n \in \mathbb{Z}\} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} = \mathbb{Z}_{12}$$
$$\langle 6 \rangle = \{6n : n \in \mathbb{Z}\} = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\} = \{0, 6\}$$
$$\langle 7 \rangle = \{7n : n \in \mathbb{Z}\} = \{\ldots, -21, -14, -7, 0, 7, 14, 21, \ldots\} = \mathbb{Z}_{12}$$

$\mathrm{o}(1) = 12$, $\mathrm{o}(2) = 6$, $\mathrm{o}(3) = 4$, $\mathrm{o}(4) = 3$, $\mathrm{o}(5) = 12$ and $\mathrm{o}(6) = 2$, etc.

Exersice In $\mathbb{Z}_{12}$, show that if $(a, n) = d$, then

$$\langle a \rangle = \langle d \rangle$$

For example, $\langle 8 \rangle = \langle 4 \rangle$ since $(8, 12) = 4$ and $\langle 5 \rangle = \langle 1 \rangle$ since $(5, 12) = 1$.

This is not an accident that order of each element divides the order of the group. According to Lagrange theorem not just in cyclic group, but in every finite group the order of each element and the order of each subgroup divides the order of group.

We see the subgroup generated by $\langle 2 \rangle$ is a subgroup of the entire set $\mathbb{Z}_{12}$, also as $\langle 3 \rangle$,$\langle 4 \rangle$,$\langle 6 \rangle$,$\langle 8 \rangle$,$\langle 9 \rangle$,$\langle 10 \rangle$.

But the subgroup generated by $\langle 1 \rangle$,$\langle 5 \rangle$,$\langle 7 \rangle$,$\langle 11 \rangle$ generates the entire set $\mathbb{Z}_{12}$.

Lemma 6.2.7 *Let a be an element of finite order n in a group G. Then*

(i) the elements $e, a, a^2, \ldots, a^{n-1}$ are distinct and $\mathrm{o}(a) = |\langle a \rangle|$;

(ii) every the elements $a \in G$ has finite order;

(iii) If $i, j \in \mathbb{Z}$, then $a^i = a^j \iff i \equiv j \pmod{n}$;

(iv) $a^m = e \iff n|m$.

Proof

(i) Suppose $a^i = a^j$ for some $i, j \in \mathbb{N}$. Without loss of generality assume $0 \leq i < j \leq n-1$. Then

$$a^{j-i} = a^j a^{-i} = a^i a^{-i} = e$$

But $j - i < n$, so $a^{j-i} = e$ contradicts the fact that $\mathrm{o}(a) = n$ It shows that $\langle a \rangle$ contains exactly n elements, that is, $\mathrm{o}(a) = |\langle a \rangle|$.

(ii) By (i) we have, $a^{j-i} = e$. So $\mathrm{o}(a) \leq j - i$, therefore a has finite order.

(iii) Exersice

$(iv) \Longleftarrow$ If $n|m$ then $m = nk$. Then

$$a^m = a^{nk} = (a^n)^k = e^k = e$$

$\Longrightarrow$ Suppose $a^m = e$. If $m \geq n$, we can use Division algorithm, $m = nq + r$ with $0 \leq r < n$. Then

$$a^m = a^{nq+r} = a^{nq} a^r = (a^n)^q a^r = e a^r = a^r$$

So, $a^r = e$.
contradicting the assumption that n is the smallest natural number such that $a^n = e$. Hence, $r = 0$ and $n|m$.

Theorem 6.2.8 Every cyclic group is abelian.

Proof let $a, b \in G$. Since G is cyclic, there exists an element $g \in G$ that generates each element in G. So, $a = g^i, b = g^j$.

$$ab = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = ba$$

However, the converse of this theorem does not hold. That is, not every abelian group is cyclic. Here we give an important example of an abelian group which is not cyclic.

Klein 4-group[1]

[1] Also simply called the 4-group, and denoted V or V_4 for vierergruppe, "four-group" in German. It is named for the mathematician Felix Christian Klein.

Consider the set $V_4 = \{e, a, b, c\}$. Define $\circ$ to be the composition of functions by means of following multiplication table.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

From the table we have, $a^2 = b^2 = c^2$ and $ab = c, bc = a, ca = b$.

It is easy to show that all the elements of V_4 can be generated by just two elements, a, b. That is

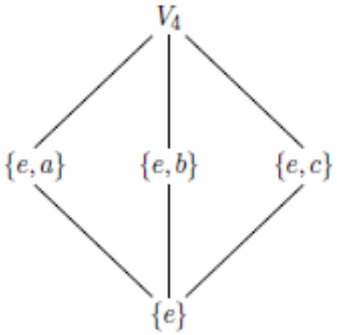
$$V_4 = \langle\, a, b \mid a^2 = b^2 = (ab)^2 \,\rangle$$

$(V_4, \circ)$ is an abelian group. But it is not a cyclic group because, non of its elements is of order $4, i.e.$ not a single element can generates the entire group.

$$\langle e\rangle = \{e\}, \quad \langle a\rangle = \{e, a\}, \quad \langle b\rangle = \{e, b\}, \quad \langle c\rangle = \{e, c\}$$

We will show later this group has a geometric interpretation, it represents the group of symmetries of a rectangle.

The subgroup lattice of V_4 is as follows.



6.3 Isomorphism

Chapter 7

Matrix Group And The Group Of Circle

> *The universe is an enormous direct product of representations of symmetry groups.*
>
> Steven Weinberg ,

Let $M_n(K)$ or $M(n,k)$ be the set of all $n \times n$ matrices with entries from K. And let K denote each one of the following: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ where p is a prime number.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix}$$

We denote (i,j) entry of an $n \times n$ matrix A by a_{ij} .

Recall the identity I_n of usual addition and multiplication of matrices .

Recall the determinant function det: $M_n(K) \to k$.

Theorem 7.0.1 det: $M_n(K) \to k$ has the following properties.

(i) $\forall A, B \in M_n(K), \quad detAB = detA.detB.$

(ii) $detI_n = 1.$

(iii) $A \in M_n(K)$ is invertible $\iff$ $detA \neq 0$.

Proof Exersice

$(M_n(K), +)$ is a group. Because:

1. *Closure:* $\forall A, B, C \in M_n(K), + : A + B \longmapsto C$
2. *Associativity:* $\forall A, B, C \in M_n(K), A + (B + C) = (A + B) + C$
3. *Identity:* $\exists I_n \in M_n(K), \forall A \in M_n(K),\ s.t.\ I_n + A = a = A + I_n$
4. *Inverse:* $\forall A \in M_n(K), \exists A^{-1} \in M_n(K),\ s.t.\ A^{-1} + A = I_n = A + A^{-1}$

But $(M_n(K), \times)$ is not a group. Because:

1. *Closure:* $\forall A, B, C \in M_n(K), \times : A \times B \longmapsto C$
2. *Associativity:* $\forall A, B, C \in M_n(K), A \times (B \times C) = (A \times B) \times C$
3. *Identity:* $\exists I_n \in M_n(K), \forall A \in M_n(K),\ s.t.\ I_n \times A = a = A \times I_n$

But $A \in M_n(K)$ is invertible $\iff$ $detA \neq 0$. So it does not hold for all $A \in M_n(K)$.

Therefore, $(M_n(K), \times)$ does not form a group.

But as always in mathematics we would like to forget about the bad point and make a group out of that. Since the only problem is that it might be $det = 0$ we consider the matrices with non-zero determinant.

Let $GL_n(K)$ denote the set of all invertible matrices with entries in K.

$$GL_n(K) = \{A \in M_n(K) : detA \neq 0\}$$

$GL_n(K)$ is a group under matrix multiplication, which is called the General Linear Group of degree n over K.

Since if $A, B \in GL_n(K)$, then $det(AB) = detA.detB \neq 0$ so $AB \in GL_n(K)$.

In special case when $n = 2$ and $K = \mathbb{R}$

$$GL_2(\mathbb{R}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0\}$$

The inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$ is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

This is the group of linear transformation in 2-Dimensional Euclidean plane which maps $\begin{pmatrix} x \\ y \end{pmatrix}$ to $\begin{pmatrix} x' \\ y' \end{pmatrix}$, where

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

The special linear group, $SL_n(K)$ is the group of all matrices with $det = 1$.

$$SL_n(K) = \{A \in GL_n(K) : detA = 1\}$$

This got the name special since if we consider $GL_n(K)$ as invertible linear transformation from K to itself, then the elements of $SL_n(K)$ are those transformations which preserve volime and orientation.

The Orthogonal subset of $GL_n(K)$ is defined by

$$O_n(K) = \{A \in GL_n(K) : AA^T = 1\}$$

from $AA^T = 1$ we have $det(A) = \pm 1$.

The subgroup of $O_n(K)$ which has determinant 1 forms a group itself.

$$SO_n(K) = \{A \in O_n(K) : detA = 1\}$$

$SO_n(K)$ is called the Special orthogonal group. It is easy to show that each $A \in SO_n(R)$ is of the form

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \theta \in [0, 2\pi]$$

$SO_n(R)$ is the group of rotation in 2-Dimensional Euclidean plane.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

We note that Matrix group are examples of continous or Lie group. We do not want to get into the detail since it is not a book in Lie Algebra or Topological group, but consider the fact that The determinant det: $M_n(K) \to k$ is a continuous function.

We note that Matrix group are examples of continous or Lie group. We do not want to get into the detail since it is not a book in Lie Algebra or Topological

group, but consider the fact that The determinant det: $M_n(K) \to k$ is a continuous function.

We also define another matrices which have a group structure like, Euclidean group $E(n)$, Unitary group $U(n)$, Special unitary group $SU(n)$, Symplectic $Sp(n)$ and etc.

$$U_n(C) = \{U \in GL_n(C) : UU^T = 1\}$$

The elements of $U_1(C)$ includes just numbers.

$$U_1(C) = \{e^{i\theta} : \quad \theta \in [0, 2\pi]\}$$

The subset of $U_n(C)$ which has determinant 1, forms a group called $SU_n(C)$. It is easy to show that every $U \in SU_2(C)$ has the following form

$$U = \left\{ \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}, \quad |a^2| + |b^2| = 1 \right\}$$

The matrix subgroup chain is as follows

$$SO_n(R) \leq O_n(R) \leq GL_n(R) \leq GL_n(C)$$
$$SU_n(C) \leq U_n(C) \leq GL_n(C)$$

We can consider $GL_n(K)$ as a subgroup of $GL_{n+1}(K)$ by identifying the $n \times n$ matrix $A = [a_{ij}]$ with

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \leq \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} & 0 \\ a_{21} & a_{22} & \cdots & a_{2m} & \vdots \\ \vdots & \vdots & \ddots & \vdots & \\ a_{n1} & a_{n2} & \cdots & a_{nm} & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

$GL_n(K)$ is closed in $GL_{n+1}(K)$, hence $GL_n(K)$ is a matrix subgroup of $GL_{n+1}(K)$.

We can consider $GL_n(K)$ as a subgroup of $GL_{n+1}(K)$ by identifying the $n \times n$ matrix $A = [a_{ij}]$ with

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \leq \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} & 0 \\ a_{21} & a_{22} & \cdots & a_{2m} & \vdots \\ \vdots & \vdots & \ddots & \vdots & \\ a_{n1} & a_{n2} & \cdots & a_{nm} & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

$GL_n(K)$ is closed in $GL_{n+1}(K)$, hence $GL_n(K)$ is a matrix subgroup of $GL_{n+1}(K)$.

Chapter 8

Symmetric Group

> *The Universe is built on a plan the profound symmetry of which is somehow present in the inner structure of our intellect*
>
> Paul Valery ,

One of the first group that came into study is the group of permutations. Permutations groups were used in mathematics before the abstract concept of a group had been formulated. Indeed in the 19th century "group" was synonymous with "group of permutations". In fact the key role of permutations of the roots of an equation for solving them by Lagrange was the reason that we defined the notion of a group. And later as it turns out by Cayley theorem that every group can be regarded as a subgroup of the full permutations.

We will now study one-to-one correspondences in more detail, particularly for finite sets.

Definition 8.0.2 Let A be a non-empty set. A function $\sigma : A \to A$ is called a ***permutation*** of A if σ is both one-to-one and onto (bijection).

The set of all permutations of A will be denoted by Sym(A).

The set of all permutations of the finite set $\{1, 2, \ldots, n\}$ will be denoted by S_n.

If σ and τ are elements of S_n we define their product $\sigma\tau$ to be the composition of σ and τ, that is,

$$\sigma\tau(i) = \sigma(\tau(i)) \quad \text{for all } i \in [n].$$

Convention

1. We use lower case Greek letters such as σ, τ, α, β, etc., to indicate elements of S_n.
2. For each integer $n \geq 1$ we let $[n] = \{1, 2, \ldots, n\}$.

Let $[n] = \{1, 2, \ldots, n\}$, and let S_n denote the set of all permutations of $[n]$ to itself. Then S_n is a group under composition of functions. Because

1. $\forall \sigma, \tau \in S_n \Longrightarrow \sigma\tau \in S_n$.
2. $\forall \sigma, \tau, \pi \in S_n \Longrightarrow \sigma(\tau\pi) = (\sigma\tau)\pi$.
3. $id \in S_n$.
4. $\forall \sigma \in S_n \Longrightarrow \sigma^{-1} \in S_n$.

S_n is called *symmetric group of degree* n .

8.1 Cycle Decomposition

We think of each permutation as a map $\sigma : [n] \to [n]$ that rearrange the order of the elements. For example, $\sigma : \{1, 2, 3, 4\} \to \{2, 3, 1, 4\}$ is a permutation. In terms of functions, it is nothing more than a function that

$$\sigma(1) = 2 \qquad \sigma(2) = 3 \qquad \sigma(3) = 1 \qquad \sigma(4) = 4$$

So σ is a function which it is determined by $\sigma(1), \sigma(2), \sigma(3), \sigma(4)$.

A Simpler notation for the permutation σ which sends $i \to \sigma(i)$ is the *two line* or *two row* representation.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Where each $\sigma(i)$ is the image of i under σ , $i \in [n]$

Since σ is injective, $\sigma(1), \sigma(2), \ldots, \sigma(n)$ are all different and therefore include all n elements of the set A, so each element of A must appear once and only once in the second row.

The identity of S_n, which is called *identity permutation*, sends every element to itself, is

$$id = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

And the inverse of an arbitrary permutation is

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

To count the number of elements of S_n, if we define an element $\sigma \in S_n$, there are n possible choices for the value of first element $\sigma(1)$. Since σ is bijective, that leaves $(n-1)$ remaining choices for $\sigma(2)$, then $(n-2)$ choices for $\sigma(3)$, and so on. In particular,

$$|S_n| = n(n-1)(n-2)\dots 1 = n!$$

8.2 Composition of two permutations

For now we just get to some calculation in S_n in order to understand some facts about the Group.

Example 8.2.1 Let and τ be defined as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

It follows that

$$\begin{array}{rclcll} \sigma\tau(1) & = & \sigma(\tau(1)) & = & \sigma(1) & = 3 \\ \sigma\tau(2) & = & \sigma(\tau(2)) & = & \sigma(3) & = 4 \\ \sigma\tau(3) & = & \sigma(\tau(3)) & = & \sigma(2) & = 1 \\ \sigma\tau(4) & = & \sigma(\tau(4)) & = & \sigma(4) & = 2 \end{array}$$

Thus we have

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

But

$$\begin{array}{rclcll} \tau\sigma(1) & = & \tau(\sigma(1)) & = & \tau(3) & = 2 \\ \tau\sigma(2) & = & \tau(\sigma(2)) & = & \tau(1) & = 1 \\ \tau\sigma(3) & = & \tau(\sigma(3)) & = & \tau(4) & = 4 \\ \tau\sigma(4) & = & \tau(\sigma(4)) & = & \tau(2) & = 3 \end{array}$$

Thus we have

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

Note that $\sigma\tau \neq \tau\sigma$, $i.e.$, multiplication of permutations is not commutative.

There is a more compact and convinent way to use insead of two line representation. Note that in every permutation the first line is the same and only the second line is different. So we could use a simpler form called *Cycle Notation*.

First we use some terminology.

Definition 8.2.2 The fixed points of a permutation σ are the elements $i \in \{1, 2, \ldots, n\}$ such that $\sigma(i) = i$.

Definition 8.2.3 Let $i_1, i_2, \ldots, i_k$ be k distinct elements from $\{i_1, i_2, \ldots, i_n\}$. The cycle of length k or a k-cycle $(i_1, i_2, \ldots, i_k)$ is a permutation $\sigma \in S_n$ such that

$$\begin{array}{rcl} \sigma(i_1) & = & i_2 \\ \sigma(i_2) & = & i_3 \\ \sigma(i_3) & = & i_4 \\ \vdots & \vdots & \vdots \\ \sigma(i_{k-1}) & = & i_k \\ \sigma(i_k) & = & i_1 \end{array}$$

and leaving all the other elements of $\{1, \ldots, n\}$. That is,

$$\sigma(i) = i \qquad i \notin \{i_1, i_2, \ldots, i_k\}$$

If $k = 1$ then the cycle $= (i_1)$ is just the identity element in S_n.

k is called the length of the cycle.

Definition 8.2.4 Let $\sigma \in S_n$. the order of a permutation σ is the smallest positive integer $n \in \mathbb{N}$ such that $\sigma^n = (1)$. That is,

$$\mathrm{o}(\sigma) = \min\{n \in \mathbb{N} \,|\, \sigma^n = (1)\}$$

Remark A k-cycle can be written in k different ways, since

$$(a_1\ a_2\ \ldots\ a_k) = (a_2\ a_3\ \ldots\ a_k\ a_1) = \cdots = (a_k\ a_1\ \ldots\ a_{k-1})$$

Example 8.2.5

For example, the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ means $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 2$.

In cycle notation we start with something, say for example the smallest integer and write what it is maps to as a cycle. Here 1 maps to 3, so we have for now $(1\ 3)$. And 3 maps to 4 so we have $(1\ 3\ 4)$ and at last 4 maps to 2, $(1\ 3\ 4\ 2)$. Since nothing is left the cycle is over, and we encoded every useful information in the two line representation.

In fact,

$$\begin{aligned} \sigma(1) &= 3 \\ \sigma^2(1) &= \sigma(\sigma(1)) = 4 \\ \sigma^3(1) &= \sigma^2(\sigma(1)) = 2 \\ \sigma^4(1) &= \sigma^3(\sigma(1)) = 1 \end{aligned}$$

That is , powers of $\sigma(1)$ generates the entire permutation. But it is not always as so as we shall see.

So we can write it as

$$(1\ 3\ 4\ 2) = (3\ 4\ 2\ 1) = (4\ 2\ 1\ 3) = (2\ 1\ 3\ 4)$$

$\sigma^4 = (1)$ so the order of the group is $m = 4$.

Theorem 8.2.6 Define a relation $\sim$ on the set $\{1, 2, \ldots, n\}$ by

$$i \sim j \iff \sigma^m(i) = j$$

Then $\sim$ is an equivalence relation. The equivalence classes would have the following form.

$$[i] = \{i, \sigma(i), \sigma^2(i), \sigma^3(i), \ldots, \sigma^m(i) = i\}$$

Proof Exersice

One of the advanteges of a equivalence relation as we proved is that it splits up the set into disjoint classes which we called equivalence classes. Here the equivalence classes are exactly what we have defined a **cycles**.

Example 8.2.7 Let's consider the permutation $\tau \in S_{11}$ given by

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 7 & 6 & 4 & 1 & 2 & 5 & 9 & 8 & 11 & 10 \end{pmatrix}$$

$$\left(\begin{array}{rcl} \sigma(1) & = & 3 \\ \sigma^2(1) & = & \sigma(3)=6 \\ \sigma^3(1) & = & \sigma(6)=2 \\ \sigma^4(1) & = & \sigma(2)=7 \\ \sigma^5(1) & = & \sigma(7)=5 \\ \sigma^6(1) & = & \sigma(5)=1 \end{array}\right)\left(\begin{array}{rcl} \sigma(8) & = & 9 \\ \sigma^2(8) & = & \sigma(9)=8 \end{array}\right)\left(\begin{array}{rcl} \sigma(10) & = & 11 \\ \sigma^2(10) & = & \sigma(11)=10 \end{array}\right)$$

The equivalence classes or cycles are:

$$\begin{aligned} [1] &= \{1,3,6,2,7,5\} \\ [8] &= \{8,9\} \\ [10] &= \{10,11\} \end{aligned}$$

In equivalence class language

$$\tau/\sim = \{[1],[8],[10]\}$$

So we can write it as

$$(1\ 3\ 6\ 2\ 7\ 5)(8\ 9)(10\ 11)$$

It is not a cycle, since is the product of three cycles. We can ignore the fixed points of a permutation, here 4 is maps to itself, (4).

Lemma 8.2.8 *Let $\sigma \in S_n$ have order m . Then for all integers i, j we have*

$$\sigma^i = \sigma^j \iff i \equiv j \pmod{m}$$

Proof σ have order m, so m is the smallest positive integer such that $\sigma^m = (1)$.

$\Longrightarrow$ If $\sigma^i = \sigma^j$ then $\sigma^{i-j} = (1)$. Using the division algorithm we can have $i - j = qm + r$ for integers q, r with $0 \leq r < m$. Then

$$\sigma^{i-j} = \sigma^{qm+r} = (\sigma^m)^q\sigma^r = \sigma^r$$

we have $r = 0$ because m is the smallest positive integer such that $\sigma^m = (1)$. Thus $m|(i-j)$ and so $i \equiv j \pmod{m}$.

$\Longleftarrow$ If $i \equiv j \pmod{m}$, then $i = j + km$ for some k .

$$\sigma^i = \sigma^{j+km} = \sigma^j\sigma^{km} = \sigma^j(\sigma^m)^k = \sigma^j$$

We know that equivalence classes of a set are either identical or disjoint. As cycles are just equivalence classes, so we can define the consept of being disjoint for cycles.

Definition 8.2.9 Let $\sigma = (a_1\ a_2\ \dots\ a_k)$ and $\tau = (b_1\ b_2\ \dots\ b_k)$ be cycles in S_n. Then σ and τ are said to be disjoint if $a_i \neq b_j\ \forall i, j$.

That is, if the elements moved by one are left fixed by the other

For example, in the last example $(1\ 3\ 6\ 2\ 7\ 5)(8\ 9)(10\ 11)$, these three cycles are disjoint. But $(7\ 3\ 6)$ and $(2\ 6\ 1)$ are not since they both have the number 6 in common.

Here we are going to point out two important facts.

First of all, every equivalence relation partition a set into equivalence classes. It is the same as saying, if we have a permutation it can be written as disjoint cycles.

Theorem 8.2.10 Every permutation on a finite set can be written uniquely, except for order of cycles or the different ways a cycle is written, as a product of disjoint cycles.

Proof Exercise.

$$(2\ 3) = (1\ 2)(2\ 3)(1\ 3).$$

$$(2\ 3) = (1\ 2)(1\ 2)(2\ 3).$$

As we pointed out permutations are not abelian. As we proved every permutation can be written as a product of disjoint cycles. But if two cycles are disjoint, they commute.

Theorem 8.2.11 If σ and τ are disjoint cycles in S_n then $\sigma\tau = \tau\sigma$.

Proof Let $A = \{a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k, c_1, c_2, \dots, c_k\}$ and let $\sigma = (a_1\ a_2\ \dots\ a_k)$ and $\tau = (b_1\ b_2\ \dots\ b_k)$ be cycles in S_n.
where $\{a_1, a_2, \dots, a_k\} \cap \{b_1, b_2, \dots b_k\} = \emptyset$

For any element $x \in A$, we note

- If $x \notin \{a_i\}$, then $x\sigma = x$. Then $(x\sigma)\tau = x\tau = (x\tau)\sigma$.
- If $x \notin \{b_i\}$, then $x\tau = x$. Then $(x\sigma)\tau = x\sigma = (x\tau)\sigma$.

Hence, $\sigma\tau = \tau\sigma$.

Example 8.2.12 Let $\sigma, \tau \in S_9$ be given by $\sigma = (2\ 5\ 3\ 6)$, $\tau = (1\ 4\ 7\ 9)$.

To show that they commute we have to show that

$$\sigma\tau(i) = \tau\sigma(i) \quad \forall i \in \{1, 2, 3, \ldots, 9\}$$

$$\sigma\tau(1) = \sigma(4) = 4$$

$$\tau\sigma(1) = \tau(1) = 4$$

So

$$\sigma\tau(1) = \tau\sigma(1)$$

Since σ fixes 1 we have $\sigma(1) = 1$.

Also for 2 :

$$\sigma\tau(2) = \sigma(2) = 5$$

$$\tau\sigma(2) = \tau(5) = 5$$

So

$$\sigma\tau(2) = \tau\sigma(2)$$

Similary for all $i \in \{1, 2, 3, \ldots, 9\}$ we have $\sigma\tau(i) = \tau\sigma(i)$.

Every permutation is a product of transpositions.

Definition 8.2.13 A cycle of length 2 is called a transposition. A transposition $(i\ j)$ is a permutation that interchanges i and j and leaves other elements fixed.

$$(i\ j) = (j\ i)$$

Lemma 8.2.14 *Every permutation $\sigma \in S_n$ is a product of (not necessarily disjoint) transpositions.*

Proof It is enough to show that every cycle is a product of transpositions, since every permutation is a product of cycles.

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \ldots (a_1\ a_3)(a_1\ a_2)$$

We can write it in several ways for example,

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_2)(a_2\ a_3) \ldots (a_{k-2}\ a_{k-1})(a_{k-1}\ a_k)$$

Example 8.2.15 If $n = 1$, then $|S_1| = 1! = 1$. Thus, S_1 only contains the identity permutation.

$$S_1 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = e \right\}$$

2. If $n = 2$, then $|S_2| = 2! = 2$. Thus, S_2 contains the identity permutation and a transposition.

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = e \ , \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\,2) \right\}$$

3. If $n = 3$, then $|S_3| = 3! = 6$. Thus, S_3 contains :

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e \ , \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\,3) \ , \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3) \ , \right.$$

$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2) \ , \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) \ , \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2) \right\}$$

The multiplication for S_3 can be written down as follows

	e	$(1\,2\,3)$	$(1\,3\,2)$	$(2\,3)$	$(1\,3)$	$(1\,2)$
e	e	$(1\,2\,3)$	$(1\,3\,2)$	$(2\,3)$	$(1\,3)$	$(1\,2)$
$(1\,2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$	e	$(1\,2)$	$(2\,3)$	$(1\,3)$
$(1\,3\,2)$	$(1\,3\,2)$	e	$(1\,2\,3)$	$(1\,3)$	$(1\,2)$	$(2\,3)$
$(2\,3)$	$(2\,3)$	$(1\,3)$	$(1\,2)$	e	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,3)$	$(1\,3)$	$(1\,2)$	$(2\,3)$	$(1\,3\,2)$	e	$(1\,2\,3)$
$(1\,2)$	$(1\,2)$	$(2\,3)$	$(1\,3)$	$(1\,2\,3)$	$(1\,3\,2)$	e

We usually show the odd cycles and the even cycles with τ and σ respectivly.

	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_3	τ_1	τ_2
σ_2	σ_2	e	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	e	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	e

It is easy to show that all the elements of S_3 can be generated by just two elements, any τ, σ. That is

$$\langle \sigma_1, \tau_1 \rangle = S_3$$

There is also an interesting relation between elements of S_3

$$\tau_1^2 = \tau_2^2 = \tau_3^2 = e$$

$$\sigma_1^3 = \sigma_2^3 = e$$

$$\sigma_1^2 = \sigma_2, \qquad \sigma_2^2 = \sigma_1$$

$$\sigma_1\tau_1 = \tau_2$$

$$\sigma_1^2\tau_1 = \tau_3$$

Now we can construct a table by using only the genetators of S_3.

	e	σ_1	σ_1^2	τ_1	$\sigma_1\tau_1$	$\sigma_1^2\tau_1$
e	e	σ_1	σ_1^2	τ_1	$\sigma_1\tau_1$	$\sigma_1^2\tau_1$
σ_1	σ_1	σ_1^2	e	$\sigma_1^2\tau_1$	τ_1	$\sigma_1\tau_1$
σ_1^2	σ_1^2	e	σ_1	$\sigma_1\tau_1$	$\sigma_1^2\tau_1$	τ_1
τ_1	τ_1	$\sigma_1\tau_1$	$\sigma_1^2\tau_1$	e	σ_1	σ_1^2
$\sigma_1\tau_1$	$\sigma_1\tau_1$	$\sigma_1^2\tau_1$	τ_1	σ_1^2	e	σ_1
$\sigma_1^2\tau_1$	τ_3	τ_1	$\sigma_1\tau_1$	σ_1	σ_1^2	e

More generally, we can write S_3 as a set of generators with the a relation between them.

$$S_3 = \langle \sigma_1, \tau_1;\ \sigma_1^3 = \tau_1^2 = e,\ \sigma_1\tau_1 = \tau_1\sigma_1^2 \rangle$$

Remark Note that the generators are not unique, for example one could write $\langle \sigma_1, \tau_2 \rangle = S_3$ or $\langle \sigma_1^2, \tau_1 \rangle = S_3$.

8.3 The Alternating group

We saw that the decomposition of permutations into transpositions are not unique up to order, but it is unique up to **parity**. For example,

$$(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2).$$

$$(1\ 2\ 3\ 4) = (1\ 4)(7\ 2)(7\ 2)(1\ 3)(1\ 2)(1\ 2)(1\ 2).$$

The number of transpositions in both of decomposition are odd.

$$(1\ 2\ 3) = (1\ 3)(1\ 2).$$

$$(1\ 2\ 3) = (2\ 4)(2\ 4)(1\ 3)(5\ 3)(5\ 3)(1\ 2)(1\ 3)(1\ 3).$$

The number of transpositions in both of decomposition are even.

This gives us an important result.

Definition 8.3.1 A permutation $\sigma \in S_n$ is called even if it can be written as a product of an even number of transpositions, and odd if it can be written as a product of an odd number of transpositions.

We define the function sgn : $S_n \to \{1, -1\}$ by

$$\text{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

Example 8.3.2 The permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 7 & 5 & 6 & 8 & 3 \end{pmatrix}$$

is even. Because

$$\pi = (1\ 2)(3\ 4\ 7)(5)(6) = (1\ 2)(3\ 8)(3\ 7)(3\ 4)$$

is the product of 4 (even number) transposition.

Remark. Given a square matrix $A = [a_{ij}] \in M_{n\times n}$. The determinant of A may be defined by the sum over all permutations of n elements (i.e., over the symmetric group)

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

For $n = 2$, $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ we have only two permutations $S_2 = \{e, (1\ 2)\}$.

$$\det(A) = \text{sgn}(e) a_{11} a_{22} + \text{sgn}(1\ 2) a_{12} a_{21}$$

Since $\text{sgn}(e) = 1$ and $\text{sgn}(1\ 2) = -1$ we obtain

$$\det(A) = a_{11} a_{22} - a_{12} a_{21}$$

$$\det(A) = \text{sgn}(e) a_{11} a_{22} + \text{sgn}(1\ 2) a_{12} a_{21}$$

For $n = 3$,

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

we have 6 permutations .

$$S_3 = \{e, (2\ 3), (1\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2)\}$$

In this case the determinant is :

$\det(A) = \text{sgn}(e)a_{11}a_{22}a_{33} + \text{sgn}(1\ 2)a_{12}a_{21}a_{33} + \text{sgn}(1\ 3)a_{13}a_{22}a_{31} + \text{sgn}(2\ 3)a_{11}a_{23}a_{32} + \text{sgn}(1\ 2\ 3)a_{12}a_{23}a_{31} + \text{sgn}(1\ 3\ 2)a_{13}a_{21}a_{32} = a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} + a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} - a_{13}a_{21}a_{32}$

Theorem 8.3.3 A permutation $\sigma \in S_n$ cannot be both even and odd. It is either even or odd.

Proof Suppose that σ is both even and odd that is $\sigma = \tau_1\ \tau_2\ \ldots\ \tau_k\ = \pi_1\ \pi_2\ \ldots\ \pi_l$, where k is even and l odd. Since every transposition is its own inverse, this would imply that

$$e = \tau_1\ \tau_2\ \ldots\ \tau_k\ \pi_l\ \pi_{l-1}\ \ldots\ \pi_1$$

Since $k + l$ is odd, this contradicts the fact that the identity permutation is even.

Definition 8.3.4 The set of all even permutations in S_n is denoted by A_n called the alternating group of degree n. That is,

$$A_n = \{\sigma \in S_n : \text{sgn}(\sigma) = 1\}$$

Theorem 8.3.5 The set A_n is a subgroup of S_n, $A_n \leq S_n$.

Proof $id \in A_n$. If $\sigma \in A_n$ then $\sigma^{-1} \in A_n$.

Therefore $\forall \sigma, \tau \in A_n \implies \sigma\tau^{-1} \in A_n$.

Theorem 8.3.6 If A_n denotes the set of even and B_n denotes the set of odd permutations in S_n, Show

$$|A_n| = |B_n| = \frac{|S_n|}{2} = \frac{|n!|}{2}$$

Proof Let $\sigma \in S_n$. Define a function $\phi : A_n \to B_n$, by $\phi(\tau) = \sigma\tau$. There is a one-to-one correspondence between the number of elements of these two sets. Becasue

- Injective : $\phi(\tau_1) = \phi(\tau_2) \implies \sigma\tau_1 = \sigma\tau_2 \implies \tau_1 = \tau_2$.
- Surjective : Let $\pi \in S_n$. That is π is an odd permutation so $\sigma\pi$ is an even permutation. $\pi = \sigma^2 = \phi(\sigma\pi)$.

Hence, $|A_n| = |B_n|$.

We have $A_n \cup B_n = S_n$ and $A_n \cap B_n = \emptyset$.

$|S_n| = |A_n| = |B_n| = 2|A_n|$. Therefore,

$$|A_n| = \frac{|S_n|}{2} = \frac{|n!|}{2} \qquad \square$$

Example 8.3.7

$$S_1 = \{e\}$$
$$A_1 = \{e\}$$

$$S_2 = \{e,\ (1\ 2)\}$$
$$A_2 = \{e\}$$

$$S_3 = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (2\ 3),\ (1\ 3),\ (1\ 2)\}$$
$$A_3 = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$$

8.4 Dihedral Groups and Symmetries Of Objects

As we mentioned groups can be used to determine or measure symmetry. By symmetry of an object we mean transformations(bijections) that do not change the object. To write it more formally, we need some terminology. Here we consider objects in Euclidean geometry of the plane $\mathbb{R}^2$.

Definition 8.4.1 An **isometry** or rigid motion of $\mathbb{R}^2$ is a permutation σ of $\mathbb{R}^2$ that preserves distance and maps the object into itself. That is, if d is a metric

$$\sigma(F) = F \iff \sigma \text{ is a symmetry of } F$$

$$d(x, y) = d(\sigma(x), \sigma(y)) \ \ \forall x, y \in F$$

Using composition of bijections as the binary operation, it is easy to show that the set of rigid motions of the plane forms a group. There are only three kinds of rigid motions: *parallel translations, rotations about a point, reflections across a line*. Now given a figure in the plane $F \subseteq \mathbb{R}^2$, the symmetry group of F is the set of rigid motions of the plane mapping F to F. This means, the symmetry group of F must map the origin of F to itself. So the set of symmetries does not contain translations any more, it just consists of rotations and reflections.

There is another approach to this intention. Consider the object as a **graph**. A graph is an ordered pair $G = (V, E)$ consisting of a set V of vertices together with a set E of edges.

In this case $E \subseteq V \times V$. E is the subset of cartisean product of vertices. Becasue an edge is related with 2 vertices. If 2 vertices connected there is an edge between them. The elements of E are of the form

$$E = \{(V_i, V_j)\ ,\ V_i \neq V_j \text{ and } V_i, V_j \in V\}$$

The pair (V_1, V_2) is called an edge. When $(V_1, V_2) \in E$, we say V_1, V_2 are connected. Here we consider edges as unordered pais, that is $(V_1, V_2) = (V_2, V_1)$.

If we represent the elements of V as points of the plane, and draw a line between $(V_1, V_2) \in E$ we have an geometric object. It turns out we can consider a graph as a group $(G, *)$ which $G = V$ and $* = E$ acts a binary operation. So we can define the group of permuations for a graph (V, E) to be the set of all permutations of $V \to V$ that preserves connectedness. That is, the set of all $\sigma \in S_V$ such that

$$(x, y) \in E \iff (\sigma(x), \sigma(y)) \in E$$

This set is a subgroup of S_V, and it is equal to S_V if every two vertic is connected.

Proposition 8.4.2 *An isometry of the plane $\mathbb{R}^2$ forms a group, called the Euclidean group.*

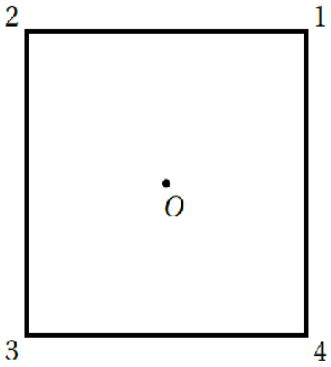
Lemma 8.4.3 *If F is a geometric object in $\mathbb{R}^2$ then the set of symmetries of F forms a subgroup of S_n called the symmetry group of F, which is denoted by $Sym(F)$ or D_{2n} or D_n.*

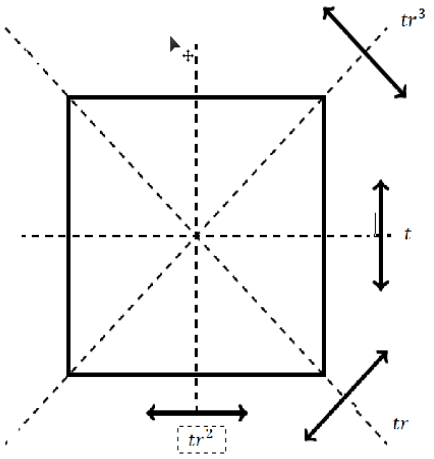
Examples

If B is a butterfly

then Sym$(B) = \{e, \tau\}$ where τ is the reflection in the axis of symmetry.

While cyclic groups describe objects that have only rotational symmetry, dihedral groups describe objects that have both rotational and bilateral symmetry.





A simple example occurs by taking F to be a cyclic group.

Now let F be a regular n-gon, That is a convex polygon with n sides of equal length and n angles of the same size. For example, a regular 3-gon is an equilateral triangle, and a regular 4-gon is a square.

It is convenient to label the vertices of the n-gon by $1, 2, \ldots, n$, so that each symmetry may be represented by a permutation of $\{1, 2, \ldots, n\}, i.e.$, by an element of S_n.

Let S be a square in the plane, that is a regular polygon with $n = 4$. Then there are exactly eight symmetries of S. These are

1. e : the identity.
2. r : a rotation of $\frac{\pi}{2}$ around the center.
3. r^2 : a rotation of π around the center.
4. r^3 : a rotation of $\frac{3\pi}{2}$ around the center.
5. t : a reflection over one of the sides.
6. tr : the composition of t and r.
7. tr^2 : the composition of t and r^2.
8. tr^3 : the composition of t and r^3.

$$D_8 = \{e, r, r^2, r^3, t, rt, r^2t, r^3t\}$$

$$r^4 = f^2 = e, frf = r^{-1}$$

The square is symmetric about its axises, we call this kind of symmetry a reflection. Let t denote reflection about horizontal axis and v about vertical axis. But we do not need to write down the symmetries that come from v, because every such symmetry can be obtained by composition of two rotation and reflection.

Corollary 8.4.4 We do not need 2 reflection as a basis that span the group of symmetries, the composition of a rotation and a reflection generate the entire group.

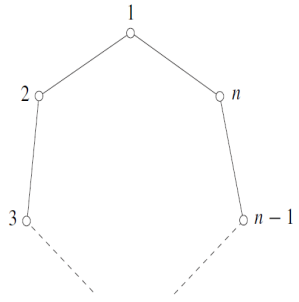
This is the group table for the symmetry group of a square D_8.

	e	r	r^2	r^3	t	rt	r^2t	r^3t
e	e	r	r^2	r^3	t	rt	r^2t	r^3t
r	r	r^2	r^3	e	rt	r^2t	r^3t	t
r^2	r^2	r^3	e	r	r^2t	r^3t	t	rt
r^3	r^3	e	r	r^2	r^3t	t	rt	r^2t
t	t	r^3t	r^2t	rt	e	a^3	a^2	a
rt	rt	t	r^3t	r^2t	r	e	r^3	r^2
r^2t	r^2t	rt	t	a^3t	r^2	r	e	r^3
r^3t	r^3t	r^2t	rt	t	r^3	r^2	r	e

It turns out that D_8 is a non-abelian group since for example, $rt \neq tr$. But $rt = tr^3$.

In general,a regular n-gon has $2n$ different symmetries: n rotational and n reflectional symmetries.

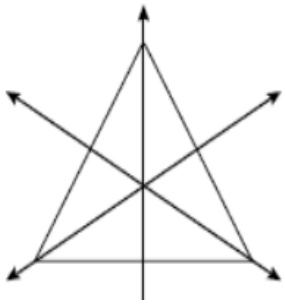
- If n is odd each axis of symmetry connects the midpoint of one side to the opposite vertix.
- If n is even there are $\frac{n}{2}$ axies of symmetry connecting the midpoint of opposite side and $\frac{n}{2}$ axies of symmetry connecting opposite vertices.



we can explicitly, write a formula depending on the 2 generators.

$$D_{2n} = \{e, r, r^2, \ldots, r^{n-1}, t, rt, r^2t, \ldots, r^{n-1}t\}$$
$$r^n = f^2 = e, frf = r^{-1}$$

Now consider the simplest polygon : An equilateral triangle



The set of symmetries of an equilateral triangle forms a group with 6 elements.

$|D_3| = 6$ and this is the same as the permutation group on 3 elements, $|S_3| = 6$. The first question that comes up is:

Is the symmetry of a polygon is permutation of vertices like what we have for an equilateral triangle ?

NO. Not every permutation is a symmetry because in a square we cannot swap two opposite vertix but not swap the others. There is no action on Euclidean plane to do that but in triangle it is all of permutation. If you increase sides, you do not get S_n group for its symmetry, but dihedral group.

The second question: Is it just happen for a triangle that has permutations of vetices for its symmetry group? The permutation group has $n!$ elements and the dihedral group has $2n$ elements. They happen to be equal $n! = 2n$ if if $n = 3$. Does it have any other solution? not in integers but in $\mathbb{R}$.

$$n! = \Gamma(n+1) = n\Gamma(n) = \int_0^\infty t^n e^{-t}\, dt = 2n$$
$$\Gamma(n) = 2$$

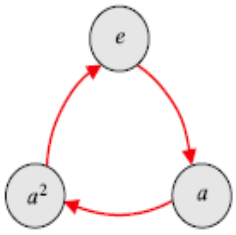
The solutions of this integral equation are:

$$n_1 = 3,\ n_2 = -3.9784,\ n_3 = -3.0763,\ n_4 = 0.4428$$

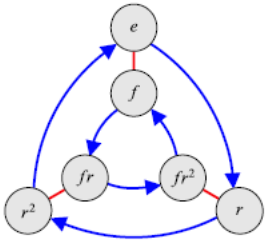
What do they mean? can we define a negative number to be a side?

8.5 Cayley Diagrams

A Cayley diagram is a graph that visualize a group. There is one vertice in the graph for each element in the group, and the edges (arrows) show how the generators act on the elements of the group. That is, if the group has two generators, a and b, then there will be one type of arrow for generator a and another type of arrow for generator b. Here is a Cayley diagram of a group; you can see that it fits this description.



Cyclic group C_3 (or $\mathbb{Z}_3$)



Symmetric group S_3

Chapter 9

Cosets and Lagrange's Theorem

> *It might be difficult, at this point, for students to see the extreme importance of this result [Lagrange's Theorem]. As we penetrate the subject more deeply they will become more and more aware of its basic character.*
>
> I. N. HERSTEIN, *Topics in Algebra*

9.1 Coset

Recall the notion of congruence in arithmetic. Two integers a, b are congruent if they have the same remainder divided by n. That is,

$$a \sim b \iff a \equiv b \pmod{n}$$

We showed that congruence modulo n is an equivalence relation, and every such relation partitions a set into equivalence classes. The consept of equivalence relation is very powerful and has many applications.

Equivalence relation is not restricted to sets only but it can be generalized to any group, since groups are just special kinds of sets. Note that in congruence relation, the integers $\mathbb{Z}$ is a group and $n\mathbb{Z}$ is a subgroup. In group theory language $a, b \in \mathbb{Z}$ are equivalent if their difference is in the subgroup $n\mathbb{Z}$. That is,

$$a \sim b \iff a - b \in n\mathbb{Z}$$

Using this similarity we now define equivalence relation in a group.

Definition 9.1.1 Let G be a group and $H \leq G$. Define a relation $\sim_R$ on G by

$$a \sim_R b \iff ab^{-1} \in H$$

This relation $a \sim_R b$ is an equivalence relation, because

- (i) Reflexivity: Since $e \in H$ and $e = aa^{-1}$, we have $a \sim_R a$.
- (ii) Symmetry: if $a \sim_R b$ then $ab^{-1} \in H$ then $(ab^{-1})^{-1} = ba^{-1} \in H$ so $b \sim_R a$.
- (iii) Transitivity: if $a \sim_R b$ and if $b \sim_R c$ then $ab^{-1} \in H$ and $bc^{-1} \in H$. But $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$. Hence $a \sim_R c$.

Since $\sim_R$ is an equivalence relation on the group G, the equivalence classes partition G.

$$\begin{aligned}[a] = \{b \in G \mid a \sim_R b\} &= \{b \in G \mid ab^{-1} \in H\} \\ &= \{b \in G \mid ab^{-1} = h \in H\} \\ &= \{hb \mid h \in H\}\end{aligned}$$

Note that since the group might be non-abelian we could define another equivalence relation on G, which is

$$a \sim_L b \iff a^{-1}b \in H$$

$$\begin{aligned}[a] = \{b \in G \mid b \sim_L a\} &= \{b \in G \mid b^{-1}a \in H\} \\ &= \{b \in G \mid b^{-1}a = h \in H\} \\ &= \{bh \mid h \in H\}\end{aligned}$$

Remark Note that both of $\sim_L$ and $\sim_R$ are equivalence relations but one cannot be implied by another, so these two relations partition a group G in two different way.

Definition 9.1.2 Let G be a group and let H be a subgroup of G. For each element $a \in G$. The set

$$aH = \{ah \mid h \in H\}.$$

is called the **left coset of** H **in** G determined by a.

Similarly, the **right coset** H **in** G determined by a is the set

$$Ha = \{ha \mid h \in H\}.$$

Remark In the case of additive notation the left and right cosets of H in G determined by a is written respectivly

$$a + H = \{a + h \mid h \in H\}$$

$$H + a = \{h + a \mid h \in H\}$$

Here we give some important properties of cosets. The properties are given for left cosets. Similar properties hold for right cosets.

Theorem 9.1.3 Let H be a subgroup of G, and $a, b \in G$. Then, the following statements hold.

(i) $a \in aH$.

(ii) $aH = H \iff a \in H$.

(iii) $aH = bH \iff a \in bH$.

(iv) $aH = bH$ or $aH \cap bH$.

(v) $aH = bH \iff a^{-1}b \in H$.

(vi) $|aH| = |bH|$.

(vii) $aH = Ha \iff a \in H = aHa^{-1}$.

$(viii)$ $aH \leqslant G \iff a \in H$.

Proof

(i) Since $H \leqslant G, e \in H$. $a = ae \in aH$.

(ii) $\implies$ Suppose $aH = H$, prove $a \in H$. From $(i), a \in aH$ but $aH = H$ hence $a \in H$.

$\impliedby$ Assume that $a \in H$ and show that $aH = H$. By clousre of H we have $aH \subseteq H$.To show that $H \subseteq aH$, let $h \in H$. Then, since $a \in H$ and $h \in H$, we know that $a^{-1}h \in H$. Thus, $h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$.

(iii) If $aH = bH$, then $a = ae \in aH = bH$. Conversely, if $a \in bH$ we have $a = bh$ where $h \in H$, and therefore $aH = (bh)H = b(hH) = bH$.

(iv) from (iii) if $c \in aH \cap bH$, then $cH = aH$ and $cH = bH$.

$(v) aH = bH \iff a \in bH \iff a = bh \iff ab^{-1} = h \iff ab^{-1} \in H.$

(vi) There is a bijection between $|Ha|$ and $|Hb|$. The correspondence

$\phi : Ha \to Hb$ which maps $ha \mapsto hb$ is clearly onto. It is one-to-one because :

$ha = h' \iff h = h' \iff hb = h'b \iff \phi(ha) = \phi(h'a)$

$(vii)\ aH = Ha \iff (aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = H$

$(viii)\ aH \leqslant G \iff e \in aH \iff e = ah \iff a = h^{-1} \in H.$

Remark Suppose $G = \{a_1, a_2, \ldots, a_n\}$ is a group with n elements and $H \leq G$. Then if we form the list of *all* cosets of H in G we have

$$a_1H, a_2H, \ldots, a_nH.$$

That is, some of these cosets may have repeated several times. But as we proved in part (iii)

$$a_iH = a_jH \iff a_i \in a_jH$$

But as noted in the above examples some of the cosets in this list are repeated several times. If we remove all repetitions from the list we are left with what we shall call the *distinct* cosets of H in G. If there are s distinct cosets we may denote them by $a_1H, a_2H, \ldots, a_sH$.

Definition 9.1.4 The number of distinct left cosets of H in G is called the index of H in G, and is denoted by $[G : H]$.

Bibliography

[1] Lang, S., Algebra (3rd edition). Reading, Mass. : Addison-Wesley Publishing Co. , Inc., 1993.

[2] T. W. Hungerford, *Algebra*, Springer Verlag, 1980.

[3] I. Stewart Why Beauty Is Truth: History of Symmetry,2007.

[4] E.Lim, *Basic Algebra I and II*, (SSymmetry in physics), King's college London, 2013.

[5] J. A. Gallian, *Contemporary Abstract Algebra*, (Third Edition), D.C. Heath, 1994.

[6] J. B. Fraleigh, *A First Course in Abstract Algebra*, (Fifth Edition), Addison-Wesley, 1994.

[7] G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, A. K. Peters Ltd., 1997.

[8] I. N. Herstein, *Topics in Algebra*, (Second Edition), Blaisdell, 1975.

[9] G. D. Birkhoff and T. C. Bartee, *Modern Applied Algebra*, McGraw-Hill Book Company, 1970.

[10] L. Dornhoff and F. Hohn, *Applied Modern Algebra*, Macmillan, 1978.

[11] B. L. Van der Waerden, *Modern Algebra*, (Seventh Edition, 2 vols), Fredrick Ungar Publishing Co., 1970.

[12] I. Stewart Why Beauty Is Truth: History of Symmetry,2007.

[13] E.Lim, *Basic Algebra I and II*, (SSymmetry in physics), King's college London, 2013.

[14] N. Jacobson, *Basic Algebra I and II*, (Second Edition, 2 vols), W. H. Freeman and Company, 1989.