Contents

1 Quick Recap on Group

1.1 Starting Simple with Algebraic Structure

i What are the algebraic properties of natural number $\mathbb{N} = \{1, 2, 3, \cdots\}$

ii What are the algebraic properties of whole numbers i.e $\mathbb{N} \cup \{0\} = \{0, 1, 2, \cdots\}$

iii What are the algebraic properties of integers $\mathbb{Z} = \{-3, -2, -1, 0, 1, 2, 3, \cdots\}$

iv What are the algebraic properties of rational numbers $\mathbb{Q} = \{\frac{a}{b} \in \mathbb{Z}, b \neq 0\}$

v What are the algebraic properties of real numbers $\mathbb{R}$

vi What are the algebraic properties of complex numbers

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$$

1.2 Modular Arithmetic

This is a new kind of group for the purpose of this class, (a.k.a clock arithmetic) for example, if the time is 9:00am, what time will it be in 5 hours time.

1.3 Abstracting Modular Arithmetic

Let

$$\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$$

And let

$$\mathbb{Z}_n \times \mathbb{Z}_n = \{(x, y) \mid x, y \in \mathbb{Z}_n\}$$

Define the binary operation

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

By
$+(x, y) = x + y \mod n$
That is, find the remainder when $x + y$ is divided by n.

Example

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$2 + 2 = 0 \text{ mod } 4$
$3 + 2 = 1 \text{ mod } 4$
Doing Modular Arithmetic in Mathematica

2 Sets and Functions Revised

2.1 Naive Set Theory

i Any collection of object is called a set

ii Including the set with no object "the empty set" denoted by $\emptyset = \{\}$

iii we say A is a subset of B if every element (or "member") of A is also an element of B.
Symbolically,

$$A \subseteq B \Leftrightarrow (x \in A \Rightarrow x \in B)$$

iv two sets are equal if they are both subset of each other symbolically,

$$A = B \Leftrightarrow (A \subseteq BandB \subseteq A)$$

Note: For any set A, $\emptyset \subseteq A$

v Operations on a set can be union, intersection, complement, e.t.c.

2.2 Functions

i Informally, given two non-empty sets A and B, we say that a "rule of assignment" f that takes inputs from A (the "domain") and "maps" each one to a unique element of B (the "co-domain") is called a function from A to B.
Written as

$$f : A \to B$$

ii The set of all possible output is called the image (or range) of f, and is denoted by $f(A)$

iii The function f is one-to-one ("injective") if

$$(f(a_1) = f(a_2) \Rightarrow a_1 = a_2) \Leftrightarrow (a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

iv The function f is onto ("surjective") if

$$B = f(A) \Leftrightarrow (\forall b \in B \exists a \in A \colon f(a) = b)$$

v If f is both one-to-one and onto, it is called a bijection. It is also invertible.

2.3 Composition of Functions

Given nonempty sets A, B, and C, and functions

$$\phi : A \to Band\psi : B \to C$$

The composition of both function ψ and ϕ is written by $\psi \circ \phi$ (or just $\psi\phi$) is defined by the formular

$$\psi\phi(a) = (\phi(a))$$

2.4 Some Basic Facts on Functions and Sets

i Let $\phi : A \to B$ and $\psi : B \to C$
If $A_1 \subseteq A$ and $A_2 \subseteq A$, then
$\phi(A_1 \cup A_2) = \phi(A_1) \cup \phi(A_2)$ and $\phi(A_1 \cap A_2) = \phi(A_1) \cap \phi(A_2)$
(Prove of the second part to be done in class)

ii if ϕ and ψ are onto, then $\psi\phi$ is onto

iii if ϕ and ψ are one-to-one, then $\psi\phi$ is one-to-one

iv if ϕ and ψ are bijections, then $\psi\phi$ is a bijection

v $(\psi\phi)^{-1} = \phi^{-1}\psi^{-1}$

Note these facts can be proved.

2.5 Equivalence Relations on Sets

Given a nonempty sets
Informally-speaking, an equivalence relation on S is a correspondence $\sim$ satisfying the following:
Reflexive Property:

$$(a \in S \Rightarrow a \sim b) \Leftrightarrow (b \sim a)$$

Symmetric Property: $(a, b \in S$ and $a \sim b) \Leftrightarrow b \sim a$

Transitive Property:

$(a, b, c \in S$ and $a \sim b$ and $b \sim a) \Rightarrow a \sim c$

A basic example is the equals on a set of numbers

A key fact: Equivalence relations induces partitions and vice versa.

Definition: Given a nonempty set S and an equivalence relation $\sim$ defined on S, the set S can be "partitioned" into a collection of disjoint sets whose union is S by defining a set A to be in iff all the members of A are equivalent to each other and only each other :

$$a, b \in A \Leftrightarrow a \sim b$$

Conversely, given a partition of S, we can define an equivalence relation $\sim$ on S by

$a \sim b \Leftrightarrow a, b \in A$ for some $A \in$