Chapter 0 Preliminaries

Assumption You are familiar with the material in Chapter 0 (Math 214 material).

Notation: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Known results:

- Well-ordering principle; mathematical induction; complex numbers.
- Division algorithm on $\mathbb{Z}$: $\gcd(a, b) = \gcd(q_1, r_1) = \gcd(q_2, r_2) = \cdots$.
- Greatest common divisor $\gcd(a, b) = xa + yb$ with $x, y \in \mathbb{Z}$.
- A prime p divides ab implies $p|a$ or $p|b$;
- Fundamental Theorem of arithmetic.
- Functions (injective, surjective, bijective, composite, inverse functions; images, preimages).
- Equivalence relations (reflexive, symmetric, and transitive); partitions.
- modular arithmetic on $\mathbb{Z}_n = \{\overline{0}, \ldots, \overline{n-1}\}$ with operations $+$ and $\cdot$ modulo n.

Checking your readiness

- Please review Chapter 0 and your notes in Math 214.
- You are not ready if you have difficulty in these topics.
- Check your readiness by doing Homework 1.
- If you have troubles in doing it. Come to homework session, form study group, ...

Goal of this course

- Learn basic algebraic structures/proof techniques to study advanced mathematics and other subjects.
- What is algebra (vs. analysis, geometry, etc.)?
- Algebra concerns the study of *algebraic structures* arising in number systems, geometrical symmetry, quantum physics!
- An algebraic structure is a set of objects (such as numbers, or symmetric transformations, or function/matrix operations) with one or more (binary) operations.
- Examples
$$\mathbb{N} = \mathbb{Z}^+,\ \mathbb{Z},\ \mathbb{Q},\ \mathbb{Q}^+,\ \mathbb{Q}^*,\ \mathbb{R},\ \mathbb{R}^+,\ \mathbb{R}^*,\ \mathbb{C},\ \mathbb{C}^*,\ M_n(\mathbb{R}).$$

Examples of groups

We will first focus on algebraic structure with only one operation.

- The set of integer under addition.

  (G0) Closed. (G1) Associative. (G2) Identity. (G3) Inverse.

- The set of positive real numbers under multiplication.

- The set $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ under addition modulo n.

- The set of permutations over $S = \{1, \ldots, n\}$ under function compositions.

  (G4) Commutative (Abelian).

Chapter 1 Symmetry of squares and regular polygons

Examples of symmetry groups, subgroups, and group tables

- For a square, there are rotation symmetries: $R_0, R_{90}, R_{180}, R_{270}$, reflection symmstries: H, V, D, D'.
- These operations will "permute" the four corners of the square labeled by $1, 2, 3, 4$, and generate 8 different permutations $\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$ in S_4 (the group of all permutations of $\{1, 2, 3, 4\}$. See the table in p. 33.
- The eight opertaions will form the dihedral group D_4 under composition.
- In general, for an regular n-side polygon with $n \geq 3$, we can form a **dihedral group** D_n.

Chapter 2 Groups

- We will begin with a structure - *Group* - with only one operation $*$ in which we can solve the equation $a * x = b$.
- You will be amazed by the fact that very rich theory can be developed with a single operation satisfying some simple rules (axioms).

Definition of Binary operations A *binary operation* $*$ on a set G is a rule assigning every pair of elements $a, b \in G$ a *unique* element $c = a * b$ in G.

So, a binary operation is a function from $G \times G$ to G.

Examples ...

Definition of a group A binary structure $(G, *)$ is a group if

(G1) $*$ is associative,

(G2) there is an identity $e \in G$, and

(G3) for every $a \in G$, there is an "inverse"$a' \in G$ so that $a * a' = a' * a = e$.

Remarks

- (G0): $*$ is binary **must** be checked.
- By (G2), G is not empty. One needs to check (G2) before (G3).
- A group $(G, *)$ is Abelian if $*$ is commutative.
- Examples: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}^*, \cdot)$, ...

Properties Let $(G, *)$ be a group.

(a) The left and right cancellation law holds.

(b) The equation $a * x = b$ has a unique solution x for any $a, b \in G$, and so is the equation $y * a = b$.

(c) The identity in a group is unique.

(d) For each element in G, there is a unique inverse.

(e) (Socks-Shoes Property) $(a * b)' = b' * a'$ for any $a, b \in G$.

Isomorphisms and Group Tables

Group Isomorphism Two groups $(G_1, *_1)$ and $(G_2, *_2)$ are isomorphic if there is a bijection $\phi : G_1 \to G_2$ such that $\phi(a *_1 b) = \phi(a) *_2 \phi(b)$.

Example $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$; $(\mathbb{Z}_n, +)$ and $(\{z \in \mathbb{C} : z^n = 1\}, \cdot)$.

Remrak For groups of small sizes, we can use the group table to check isomorphism.

All two element groups are isomorphic to $(\mathbb{Z}_2, +)$**:**

$(\mathbb{Z}_2, +)$

$+$	0	1
0	0	1
1	1	0

$(\{1, -1\}, \cdot)$

$\cdot$	1	-1
1	1	-1
-1	-1	1

$(G, *)$

$\cdot$	e	a
e	e	a
a	a	e

All three element groups are isomorphic to ($\mathbb{Z}_3, +$).

$\mathbb{Z}_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$(G, *)$

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

There are two non-isomorphic four element groups.

$(\mathbb{Z}_4, +)$, and

the Klein 4-group $(K, *)$: the set of 2×2 diagonal orthogonal matrices under multiplication.

There are only one five element group $(\mathbb{Z}_5, +)$ up to isomorphism.