Part I: Groups and Subgroups

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

January 22

1 Intorduction and Examples

This sections attempts to give some idea of the "nature of abstract algebra". I will give a summary only. Please glance through the whole section in the textbook. Follwing are some of the main points:

1. The section provides a prelude to "binary operations", which we define in the next section.
2. To do this it discusses multiplication of complex numbers.
3. It gives **Euler Formula** that
$$e^{i\theta} = \cos\theta + i\sin\theta$$
4. Given any complex number $z \in \mathbb{C}$ we can write
$$z = |z|\, e^{i\theta}$$
5. It discusses the algebra of the **Unit Circle**.
   (a) The unit circle
$$U = \{z \in \mathbb{C} : |z| = 1\} = \{z \in \mathbb{C} : z = e^{i\theta} \quad where \quad \theta \in \mathbb{R}\}$$

(b) Note, for $z, w \in U$, the product $zw \in U$. We say the unit circle U is **closed under** multiplication.

(c) Define the map

$$f : [0, 2\pi) \longrightarrow U \qquad where \quad f(\theta) = e^{i\theta}.$$

Then, f is a bijection.

(d) In fact, $f(x + y) = f(x)f(y)$ sends sum to the product. Here, addition $x + y$ in $[0, 2\pi)$ is defined "modulo 2π".

6. We discuss the algebra of **Roots on Unity**. Fix a positive integer n.

(a) Let U_n be the set of all solutions of the equation $z^n = 1$ (in $\mathbb{C}$)

(b) write $\zeta = e^{\frac{2\pi i}{n}}$. Then

$$U_n = \{\zeta^0, \zeta^1, \zeta^2, \ldots, \zeta^{n-1}\}$$

(c) Define the map

$$\varphi : \mathbb{Z}_n \longrightarrow U_n \qquad by \quad \varphi(\overline{r}) = \zeta^r = e^{\frac{2\pi r i}{n}}$$

is a bijection. It needs a proof that φ is well defined.

(d) In fact, $\varphi(x + y) = \varphi(x)\varphi(y)$ sends sum to the product.

7. Also, $U_n \subseteq U$, the unit circle.

2 Binary Operation

Examples of "binary operations" are addition and multiplication, in all the situations where we worked with them:

$$\mathbb{Z}, \mathbb{Z}_n, \mathbb{R}, \mathbb{C}, \mathbb{M}_n(\mathbb{R}), \mathbb{M}_n(\mathbb{C})$$

where $\mathbb{M}_n(\mathbb{R}), \mathbb{M}_n(\mathbb{C})$ denote the set of matrices of size $n \times n$, with coefficients in $\mathbb{R}$ or $\mathbb{C}$. Similarly, multiplication on U, U_n are binary operations. They are called binary operations, because *to each ordered pair* (x, y) *they associate another element* $x + y$ *or* xy.

We give a formal definition of "binary operations".

Definition 2.1. Let S be a set. A **binary operation** $*$ on S is a mapping $* : S \times S \longrightarrow S$. For now, we use the notation $x * y := *(x, y)$.

Definition 2.2. Suppose $*$ is a binary operation on S and H be a subset of S. We say that H is **closed under** $*$, if for any $x, y \in H$ we also have $x * y \in H$. Notationally,

$$if \qquad x, y \in H \qquad \Longrightarrow \qquad x * y \in H.$$

Reading Assignment: §I.2 Examples 2.2-2.10.

Example 2.3 (§I.2, 2.7)**.** Let F be the set of all continuous real valued functions on $\mathbb{R}$. We give four binary operations:

1. Sum $(f + g)(x) = f(x) + g(x)$
2. Product $(fg)(x) = f(x)g(x)$
3. Composition $(fog)(x) = f(g(x))$
4. Subtraction $(f - g)(x) = f(x) - g(x)$
5. Note division f/g is not always defined (unless $g(x) \neq 0 \ \forall x$). So, division is not a binary operation on F.

§1. Properties of binary operations

Definition 2.4. A binary operation $*$ on S is said to be commutative,

$$if \qquad x * y = y * x \qquad \forall\ x, y \in S.$$

Remark or examples. As far as I can see, matrix multiplication and composition are the only "natural" binary operations that are not commutative. Most of the counter examples are artificially constructed.

1. On $\mathbb{Z}, \mathbb{Z}_n, \mathbb{R}, \mathbb{C}$ both addition and multiplication are commutative.
2. On $\mathbb{M}_n(\mathbb{R}), \mathbb{M}_n(\mathbb{C})$ additions are commutative. But multiplcation is NOT commutative. For example

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

   More generally,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ x & y \end{pmatrix} \neq \begin{pmatrix} a & b \\ x & y \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$LHS = \begin{pmatrix} x & y \\ a & b \end{pmatrix} \quad and \quad RHS = \begin{pmatrix} b & a \\ y & x \end{pmatrix}.$$

3. Let F be the set of all continuous functions on $\mathbb{R}$. Then
   (a) Addition $+$ is commutative.
   (b) Substraction is NOT commutative.
   (c) The composition is NOT commutative. Let $f(x) = e^x$ and $g(x) = x^2$. Then $fog(x) = e^{x^2}$ and $gof(x) = e^{2x}$. So, $fog \neq gof$.

Definition 2.5. A binary operation $*$ on S is siad to be **associative**

$$if \qquad a * (b * c) = (a * b) * c \qquad \forall\ a, b, c \in S.$$

Remaks and Examples.

1. First, only when an operation is associative, we do not need to use parentheses to specify order of multiplication. we can write $a * b * c$ for both $a * (b * c), (a * b) * c$.

2. I do not know (well I do) any natural example of binary operations, that is not associative.

Theorem 2.6. Let $\mathcal{F}(S)$ be the set of all functions $f : S \longrightarrow S$. Then, the compositions o is a binary operation on $\mathcal{F}(S)$. The composition is an associative binary operation.

Proof. It is straight forward. Look at the text book. ■

Corollary 2.7. Multiplication on $\mathbb{M}_n(\mathbb{R}), \mathbb{M}_n(\mathbb{C})$ are associative.

Proof. Let $\mathcal{L}(\mathbb{R}^n)$ be the set of all linear functions $\mathbb{R}^n \longrightarrow \mathbb{R}^n$. So, $\mathcal{L}(\mathbb{R}^n) \subseteq \mathcal{F}(\mathbb{R}^n)$. So, composition is associative in $\mathcal{L}(\mathbb{R}^n)$.

Recall, there is an 1-1 and onto correspondence between

$$\varphi : \mathbb{M}_n(\mathbb{R}) \longrightarrow \mathcal{L}(\mathbb{R}^n)$$

such that $\varphi(AB) = \varphi(A)\varphi(B)$. Now, we will use the associative property of the composition in $\mathcal{L}(\mathbb{R}^n)$. We have

$$\varphi((AB)C) = \varphi(AB)\varphi(C) = [\varphi(A)\varphi(B)]\varphi(C)$$

$$= \varphi(A)[\varphi(B)\varphi(C)] = \varphi(A)[\varphi(BC)] = \varphi(A(BC)).$$

Since, φ is 1-1, we have $(AB)C = A(BC)$. So, the matrix product is associative. The proof is complete. ■

2.1 Tables

For a finite set S, tables can be used to describe a binary operation.

Reading Assignment; Read examples 2.14-2.25.

Let me describe the addition and multiplication on $\mathbb{Z}_4$ by tables:

Addition Table				
$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Product Table				
$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Let me do the same for $\mathbb{Z}_5$:

Addition Table					
$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Product Table					
$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

3 Isomorphic Binary Structures

Abstract

We define isomorphic Binary Structures. Main point is, if two binary structures are isomorphic, then propertes of one translate over to properties of the other, via the isomorphism. So, if we know one we know the other. We do not have to study two of them seperately.

Definition 3.1. By a **binary structure** $\langle S, * \rangle$, we mean a set S with a binary operation $*$ on it.

Definition 3.2. Let $\langle S, * \rangle$ and $\langle T, *' \rangle$ be two binary structures.

1. A map $\varphi : S \longrightarrow T$ is called (a map of) or a **homomorphism of binary structures**

$$if \qquad \varphi(x * y) = \varphi(x) *' \varphi(y) \qquad \forall\, x, y \in S.$$

2. A map $\varphi : S \longrightarrow T$ is called an **isomorphism of binary structures**

$$if \qquad \varphi(x * y) = \varphi(x) *' \varphi(y) \qquad \forall\, x, y \in S.$$

   and if φ is a bijection.

   (*Emphasis in this section is on isomorphic structures; not on homomorphisms*)

Example 3.3. Let $U = \{z \in \mathbb{C} : |z| = 1\}$ be the unit circle. Then, with usual multiplication, $\langle U, \cdot \rangle$ is a binary structure.

On the interval $[0, 2\pi)$ the addition "*modulo* 2π provides a binary structure $([0, 2\pi), +)$. The map

$$\varphi : [0, 2\pi) \longrightarrow U \qquad defined\ by \qquad \varphi(t) = e^{it}$$

is an isomorphism of binary structures.

Example 3.4. Let n be a fixed positive mumber. Then,

$$\psi : \mathbb{Z}_n \longrightarrow U_n \qquad defined\ by \qquad \psi(\overline{k}) = e^{\frac{2k\pi i}{n}} \qquad (= \zeta^n)$$

is an isomorphism of binary structures.

Example 3.5. The mapping

$$\exp : \langle \mathbb{R}, + \rangle \longrightarrow \langle (0, \infty), \cdot \rangle \qquad defined\ by \qquad \exp(t) = e^t$$

is an isomorphism of binary structures. Its inverse

$$\ln : \langle (0, \infty), \cdot \rangle \longrightarrow \langle \mathbb{R}, + \rangle \quad t \mapsto \ln t$$

is also an isomorphism of binary structures.

Definition 3.6. Let $\langle S, * \rangle$ be a binary structure. An element $e \in S$ is called an **identity element for** $*$

$$if \qquad e * x = x * e = x \quad \forall\ x \in S.$$

Theorem 3.7. Let $\langle S, * \rangle$ be a binary structure. Then, $\langle S, * \rangle$ has at most one identity element.

Proof. Suppose e, ϵ be identity elements in S. We will prove that $e = \epsilon$.

$$\epsilon = \epsilon e \quad because\ e\ is\ identity.$$

Also

$$e = \epsilon e \quad because\ \epsilon\ is\ identity.$$

So, $\epsilon = e$. The proof is complete. ■

Theorem 3.8. Suppose $\varphi : S \longrightarrow T$ is an isomorphism of two binary structures $\langle S, * \rangle$ and $\langle T, *' \rangle$. Let $e \in S$ be the identity for $*$. Then $\varphi(e)$ is an identity in $\langle T, *' \rangle$.

Proof. For $x \in T$ we have to prove $x *' \varphi(e) = \varphi(e) *' x = x$. Since φ is onto, $\varphi(a) = x$ for some $a \in S$. We have

$$e * a = a * e = a. \qquad \textit{Apply } \varphi : \qquad \varphi(e) *' \varphi(a) = \varphi(a) *' \varphi(e) = \varphi(a).$$

Which is $\varphi(e) *' x = x *' \varphi(e) = x$. So, $\varphi(e)$ is an identity in T. The proof is complete. ■

We look at a few binary structures that are not isomorphic.

Example 3.9 (13.15)**.** 1. $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ are not isomorphic.

2. (**Added**): $\langle \mathbb{Q}, \cdot \rangle$ and $\langle \mathbb{Z}, \cdot \rangle$ are not isomorphic.

Proof.

1. This is because $\langle \mathbb{Q}, + \rangle$ is "divisible" by any positive integer n. It is divisible by 3 means, give any $y \in \mathbb{Q}$ there is an element $x \in \mathbb{Q}$ such that $x + x + x = y$, namely $x = y/3$. But $\langle \mathbb{Z}, + \rangle$ does not enjoy this property.
2. For the second statement note all nonzero elements is $\mathbb{Q}$ has an inverse, while that is not true for $\mathbb{Z}$.

Example 3.10 (Added)**.** $\langle \mathbb{R}, \cdot \rangle$ is not isomorphic to $\langle \mathbb{M}_2(\mathbb{R}), * \rangle$ where $*$ is usual multiplication. Among other things, the first one is commutative and the second one it not commutative.

Example 3.11 (3.17)**.** $\langle \mathbb{R}, \cdot \rangle$ and $\langle \mathbb{C}, \cdot \rangle$ are not isomorphic.

4 Groups

Definition 4.1. A **Group** $\langle G, * \rangle$ is a binary structure such that the following axioms holds:

1. Associativty holds:
$$(a * b) * c = a * (b * c) \qquad \forall\ a, b, c \in G.$$
2. G has an itentity element e, which means
$$e * a = a * e = a \qquad \forall\ a \in G$$
3. (**Inverse**)
$$\textit{For each } a \in G \quad \exists\ a' \in G \quad \ni \quad a * a' = a' * a = e.$$
This a' is called an/the inverse of a.

Remarks.

1. To check $\langle G, * \rangle$ is a group, we check the (0) G is closed under $*$, (1) $*$ is associative, (2) G has an identity, (3) each element has an inverse.
2. **Notation.** We usually denote the group $\langle G, * \rangle$ by G, when $*$ is understood.
3. The notation a' is not very normal. For most of the groups, the operation $*$ is denoted by addition $+$ or multiplication (like $x \cdot y$ of xy). If we use multiplicative notations, then a' is usually denoted by a^{-1}. If we use addive notation, then a' is usually denoted by $-a$. The additive notation $+$ is used, only when $*$ is commutative.

Definition 4.2. A Group $\langle G, * \rangle$ is said to be an **abelian group**, if $*$ is commutative.

Example 4.3 (4.2)**.** The unit circle U and the roots of unity U_n are groups under multiplication.

Reading Assignment: Read Example 4.4-4.14.

4.1 Elementary Properties of Groups

Theorem 4.4. Let G be a group. Then **left and right cancellation** holds. That means,

$$for \quad x, y, z \in G \qquad x*z = y*z \quad \Longrightarrow \quad x = y \qquad \textbf{(right Cancelleation)}$$

and

$$for \quad x, y, z \in G \qquad z*x = z*y \quad \Longrightarrow \quad x = y \qquad \textbf{(left Cancelleation)}$$

Proof. Let $x * z = y * z$. Multiply this equation by inverse z' of z, on the right. We get $(x * z) * z' = (y * z) * z'$. By associativity $x * (z * z') = y * (z * z')$, So, $x * e = y * e$ or $x = y$. This establishes the right cancellation.

To prove the left cancellation, multiply the equation $z * x = z * y$ by z' on the left. (**Exercise:** complete it). The proof is complete. ■

Theorem 4.5. Let G be a group and $a, b \in G$. Then

1. The equation $ax = b$ has a unique solution.
2. The equation $xa = b$ has a unique solution.

Proof. Let a' be an/the inverse of a. Then, $x = a' * b$ is a solution of the equation $ax = b$, becuase

$$a * (a' * b) = (a * a') * b = e * b = b.$$

So, the equation $a * x = b$ has a solution $x = a' * b$. Now suppose the equation $a * x = b$ has two solutions $x = x_1, x_2$. So, $a * x_1 = b$ and $a * x_2 = b$. So, $a * x_1 = a * x_2$. By left cancellation, $x_1 = x_2$. So, the equation $a * x = b$ has exactly one solution. So, the statement (1) is established. We prove statement (2) similarly (**exercise**). ■

Theorem 4.6. Let G be a group. Then

1. G has exactly one identity e.

2. Given $x \in G$ there is exactly one element x' such that

$$x * x' = x' * x = e.$$

This (unique) x' is called the inverse of x.

Proof. By definition of group, G has an identity $e \in G$ such that $x * e = e * x = x$ for all $x \in G$. The uniqueness follows from the uniqueness of identity for binary structures. (Please rewrite the proof). So, (1) is established.

Suppose $x \in G$. By the third property of groups, there is one element $x' \in G$ such that

$$x * x' = x' * x = e.$$

Suppose $x' \in G$ also satisfy the same property, i.e

$$x * x" = x" * x = e.$$

Then, clearly $x * x' = x * x"$. So, by left cancellation $x' = x"$. So, the uniqueness of the "inverse" of x is established. ■

Notations: Suppose G is a group.

1. When we use the multiplicative noation, the inverse of a will be denoted by a^{-1}. When we use the additive noation "+", the inverse of a will be denoted by $-a$.

Corollary 4.7. Let G be a group and $a, b \in G$. Then, $(a * b)^{-1} = b^{-1} * a^{-1}$. (*Recall, for inverses of matrices, we have seen the same.*)

Proof. We have

$$(a*b)*(b^{-1}*a^{-1}) = ((a*b)*b^{-1})*a^{-1} = (a*(b*b^{-1}))*a^{-1} = (a*e)*a^{-1} = a*a^{-1} = e.$$

Similarly, $(b^{-1} * a^{-1}) * (a * b) = e$. So, $(a * b) = b^{-1} * a^{-1}$. The proof is complete. ■

4.2 Finite Groups

Example 4.8. *1. Any singleton set $\{e\}$ can be given a group structure by defining $e * e = e$.*

2. Also, the subset $\{0\}$ of $\mathbb{Z}$ is a group under addition.

3. Also, the subset $\{1\}$ of $\mathbb{Z}$ is a group under multiplication.

4. All these groups are isomorphic (as in binary structures).

Example 4.9. 1. Any doubleton set $\{e, a\}$ can be given a group structure by defining multiplication by the table

*	e	a
e	e	a
a	a	e

2. $\mathbb{Z}_2$ is a group with two elements.

3. $\langle\{1, -1\}, \cdot\rangle$ is a group with two elements.

4. These groups are isomorphic.

5. In fact, any group G with two elements is isomprphic to $\mathbb{Z}_2$ (give a proof).

Example 4.10. Suppose G is a group of order three. Then $G \approx \mathbb{Z}_3$.
Proof. Let $G = \{e, a, b\}$, where e is the identity.

1. First, $ab \neq a$ and $ab \neq b$. So, $ab = e$.

2. Claim $a^2 = b$. This is because, $a^2 \neq e$ and $a^2 \neq a$.

3. Therefore, $G = \{e, a, a^2\}$. Now, $a^3 \neq a, a^3 \neq a^2$. So, $a^3 = e$.

4. So, the mapping $\varphi : \mathbb{Z}_3 \xrightarrow{\sim} G$ given by

$$\varphi(\overline{0}) = e, \varphi(\overline{1}) = a, \varphi(\overline{2}) = a^2$$

is an isomprphism.

The proof is complete. ■

Example 4.11. Suppose G is a group of order four. We will show that either $\mathbb{Z}_4 \approx G$ or G is the Klein group (to be defined).

Proof. Write $G = \{e, a, b, c\}$ where e is the identity. There are two cases:

1. First, $ab = e$ or
2. $ab = c$.

1. Suppose $ab = e$. In this case, we will prove $\mathbb{Z}_4 \approx G$.
   (a) Then, c is its own inverse or $c^2 = e$.
   (b) Claim $a^2 = c$. To see this, first note $a^2 \neq e$, $a^2 \neq a$. Further, if $a^2 = b$ then $a^3 = e$. Then, it would follow $a^3 = e$. That would imply $ac \notin \{e, a, a^2, c\} = G$, which is impossible. Therfore, $a^2 = c$. Similarly, $b^2 = c$.
   (c) So, $a^2 = b^2$ and hence $a^3 = b$. So, $G = \{e, a, a^2, a^3\}$.
   (d) Also note $a^4 = c^2 = e$.
   (e) So, the mapping $\varphi : \mathbb{Z}_4 \xrightarrow{\sim} G$ given by

   $$\varphi(\overline{0}) = e, \varphi(\overline{1}) = a, \varphi(\overline{2}) = a^2, \varphi(\overline{2}) = a^3$$

   is an isomprphism.

   The proof is complete. ■

2. Now suppose $ab = c$. In this case, a is its own inverse and b is its own inverse. So, c is its own inverse. So, $a^2 = b^2 = c^2 = e$. So, the multiplication table loos like:

Product Table				
$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	
b	b		e	
c	c			e

By cancellation property, no repeatation is allowed in any row or column. So, the multiplication table is completed as follows.

Product Table				
$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This group is called the **Klein Group**.

3. So, there are only two distinct groups of order 4.

4.3 Failure of Cancellation

Example 4.12. 1. Recall, in $\mathbb{R}$ cancellation fails for multiplcation. The zero is the problem: $0 * x = 0 * y = 0$ for all $x, y \in \mathbb{R}$.

2. For matrices, the cancellation property fails for multiplication: We have

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$$

So, cancellation property fails for matrix product.

5 Subgroups

First, we set up some notations:

1. Normally, we use addition $+$ or multiplication (like $x \cdot y$ or xy) to denote the binary operation $*$.
2. Only when the group G is known to be abelian, we use additive "$+$" notation.
3. If we use the additive notation $+$, then the identity is denoted by zero 0. The inverse of a is denoted by $-a$.
4. If we use the multiplicative notation, then the identity is denoted by "one" 1. The inverse of a is denoted by a^{-1}.
5. Suppose $n \geq 0$ is a non-negative integer. In the additive notation, $na = n \cdot a := a + a + \cdots + a$ denotes sum of a with itself n times. Also $-na = -(na)$. In multiplicative notation, $a^n := a \cdot a \cdots a$ product od a with itself n times. Also $a^{-n} := (a^n)^{-1}$.

Definition 5.1. For a group G, **order of** G is defined to be the number of elements in G. It is denoted by $|G|$. Obvioulsy, a group can have infinite order. For example $|\mathbb{Z}_n| = n$ and $|\mathbb{Z}| = \infty$.

5.1 Subgroups

Definition 5.2. Let G be a group. A subset H of G is called a **subgroup of** G, if H itself is a group under the operation inherited from G. For a subset H to be a subgroup G following should be satisfied:

1. H is closed under the binary operation in G. That means,

$$a, b \in H \qquad \Longrightarrow \qquad ab \in H.$$

2. The identity e of G is in H.
3. For $a \in H \quad \Longrightarrow \quad a^{-1} \in H$.

4. (**Remark.** *We do not need to check associativity in H, because it is inherited directly from G*).

If H is a subgroup of G, we write $H \leq G$. Further if, $H \neq G$ then we say H is a **proper subgroup** of G.

The Trivial Subgroups:
Let G be a group. Then, $\{e\}$ and G are two of its trivial subgroups.

Example 5.3. Following are subgroups:

1. $$\langle \mathbb{Z}, + \rangle \leq \langle \mathbb{Q}, + \rangle \leq \langle \mathbb{R}, + \rangle \leq \langle \mathbb{C}, + \rangle$$

   Each one on the left is a subgroup of any one on the right.

2. $$\langle \{1, -1\}, \cdot \rangle \leq \langle \mathbb{Q}^*, \cdot \rangle \leq \langle \mathbb{R}^*, \cdot \rangle \leq \langle \mathbb{C}^*, \cdot \rangle$$

   Each one on the left is a subgroup of any one on the right.

3. $$\langle U_n, \cdot \rangle \leq \langle U, \cdot \rangle \leq \langle \mathbb{C}^*, \cdot \rangle$$

   Each one on the left is a subgroup of any one on the right.

4. $\langle \{\overline{0}, \overline{2}\}, + \rangle$ is a subgroup of $\langle \mathbb{Z}_4, + \rangle$.

   More generally, let $n = kr$ be a positive integer, $k > 0, r > 0$. Then, $\langle \{\overline{0}, \overline{k}, \overline{2k}, \ldots, \overline{(r-1)k}\}, + \rangle$ is a subgroup of $\langle \mathbb{Z}_n, + \rangle$. Note

   $$\langle \{\overline{0}, \overline{k}, \overline{2k}, \ldots, \overline{(r-1)k}\}, + \rangle \approx \mathbb{Z}_r.$$

   So, one may loosely say $\mathbb{Z}_r$ is a subgroup of $\mathbb{Z}_n$.

5. Let $C[0,1]$ be set of all continuous functions on the interval $[0,1]$. Then $\langle C[0,1], + \rangle$ is a group. Let H be the set of all functions $f \in C[0,1]$ which vanishes on $(.25, .75)$. Then, H is a subgroup of $C[0,1]$. In fact, given any subset $X \subset [0,1]$, the set

   $$Z(X) = \{f \in C[0,1] : f_{|X} = 0\} \quad \textit{is a subgroup.}$$

6. Let $GL_n(\mathbb{R})$ be the set of all invertible matrices of order n. (*We know* $GL_n(\mathbb{R}) = \{A \in \mathbb{M}_n(\mathbb{R}) : \det A \neq 0\}$.) Then, $GL_n(\mathbb{R})$ is a group.
   (a) Let $SL_n(\mathbb{R}) = \{A \in \mathbb{M}_n(\mathbb{R}) : \det A = 1\}$. Then $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.
   (b) Let $O_n(\mathbb{R})$ be the set of all orthogonal matrices. (i. e. $A \in GL_n(\mathbb{R})$ such that $AA^T = I_n$.) Then $O_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.
   (c) Let $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) : \det A = 1\}$. Then $SO_n(\mathbb{R})$ is a subgroup of $O_n(\mathbb{R})$.
7. Similarly, let $GL_n(\mathbb{C})$ be the set of all invertible matrices of order n. (*We know* $GL_n(\mathbb{C}) = \{A \in \mathbb{M}_n(\mathbb{C}) : \det A \neq 0\}$.) Then, $GL_n(\mathbb{C})$ is a group.
   (a) Let $SL_n(\mathbb{C}) = \{A \in \mathbb{M}_n(\mathbb{C}) : \det A = 1\}$. Then $SL_n(\mathbb{C})$ is a subgroup of $GL_n(\mathbb{C})$.
   (b) Let $U_n(\mathbb{C})$ be the set of all unitary matrices. (i. e. $A \in GL_n(\mathbb{C})$ such that $A\bar{A}^T = I_n$.) Then $U_n(\mathbb{C})$ is a subgroup of $GL_n(\mathbb{C})$.
   (c) Let $SU_n(\mathbb{C}) = \{A \in U_n(\mathbb{C}) : \det A = 1\}$. Then $SU_n(\mathbb{C})$ is a subgroup of $U_n(\mathbb{C})$.

5.2 Cyclic Subgroups

Theorem 5.4. Let G be group and $a \in G$. Then $H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G. In fact, H is the smallest subgroup of G that contains a.

Proof. First, recall for a negative integer $k < 0$ we define $a^k := (a^{-k})^{-1}$. Now H is closed under product: for $m, n \in \mathbb{Z}$ we have $a^m \cdot a^n = a^{m+n} \in H$. The identity $e = e^0 \in H$. For $a^n \in H$, we have $(a^n)^{-1} = a^{-n} \in H$. So, H is a subgroup.

Now, suppose K is another subgroup of G that contains a. Since K is closed under multiplication $a^n \in K$ for all non-negative integers n. Again, for negative integers m we have $a^m = (a^{-m})^{-1} \in K$. So, $a^n \in K$, $\forall\ n \in \mathbb{Z}$. So, $H \subseteq K$. This establishes that H is the smallest subgroup of G that contains a. The proof is complete. ■

Definition 5.5. Let G be a group and $a \in G$.

1. Then, $H = \{a^n : n \in \mathbb{Z}\}$ is called the **cyclic subgroup** of G generated by a. This H is denoted by $\langle a \rangle$.

2. If $G = \langle a \rangle$ for some $a \in G$, then we say that G is a **cyclic group**.

3. **Remark.** So, a cyclic group is a group that is generated by one element. *In future, we will consider groups generated by a set of elements*.

Example 5.6. 1. $\langle \mathbb{Z}, + \rangle$ is cyclic, generated by 1 or -1.

$$\langle \mathbb{Z}, + \rangle = \langle 1 \rangle = \langle -1 \rangle$$

2. $\langle \mathbb{Z}_n, + \rangle = \langle 1 \rangle$ is cyclic. In fact, given any integer k so that $gcd(k, n) = 1$ we have $\langle \mathbb{Z}_n, + \rangle = \langle k \rangle$. (**Exercise.** *Give a proof.*)

3. The Klein group is not cyclic.(**Exercise.** *Give a proof.*)

4. U_n, the n^{th} roots of unity is cyclic. It is generated by the premitive root $\zeta = e^{\frac{2\pi i}{n}}$. (**Exercise.** *Give a proof.*)

6 Cyclic Groups

Abstract:*Any cyclic group is either isomorhic to* $\langle \mathbb{Z}, + \rangle$ *or isomorhic to* $\langle \mathbb{Z}_n, + \rangle$ *for some integer* $n \geq 1$*.*

6.1 Elementary Properties

Theorem 6.1. Every cyclic group is abelian.

Proof. Let $G = \langle a \rangle$ be a cyclic group generated by a. Then, for $x, y \in G$ we have $x = a^m, y = a^n$ for some $m, n \in \mathbb{Z}$. So,

$$xy = a^m \cdot a^n = a^{m+n} = yx.$$

The proof is complete. ■

Theorem 6.2 (Division Algorithm)**.** Suppose $m > 0$ is fixed positive integer. Then, for any integer $n \in \mathbb{Z}$ there are unique integers q, r such that

$$n = mq + r \qquad \text{with} \quad 0 \leq r < n.$$

Proof. Exercise.

Theorem 6.3. Let G be cyclic group. Then, any subgroup H of G is also cyclic.

Proof. Write $G = \langle a \rangle$. If $H = \{e\}$ then $H = \langle e \rangle$ is cyclic. Now assume $H \neq \{e\}$. Write

$$S = \{n \in \mathbb{Z}^+ : a^n \in H\}.$$

Since $H \neq \{e\}$, the set S is non-empty. Let m be the smallest integer in S. We calim the $g = a^m$ generates H. Notationally,

$$H = \langle a^m \rangle = \langle c \rangle$$

Obviously, $\langle a^m \rangle \subseteq H$. Now, let $x = a^n \in H$. Then $n = mq + r$ for some integer $0 \leq r < m$. Then $a^n = (a^m)^q a^r \quad$ *and* $\quad a^r =$

$(a^m)^{-q}a^n \in H$. Since $0 \le r < m$, by minimality of m, we have $r = 0$ and $n = mq$. So, $a^n = (a^m)^q \in \langle a^m \rangle$. So, $H \subseteq \langle a^m \rangle$. The proof is complete. ■

Corollary 6.4. Let H be subgroup of $\langle \mathbb{Z}, + \rangle$. Then $H = n\mathbb{Z}$, where n is the smallest positive integer in H. This n will be called the **positive generator** of H.

Proof. It follows directly from the above theorem (and its proof.) The proof is complete. ■

Exercise 6.5. Let r, s be two positive integers. Recall the definition of the greatest common divisor $gcd(r, s)$. Prove that $gcd(r, s)$ is the positive generator of the subgroup $H = \{nr + ms : m, n \in \mathbb{Z}\}$.

6.2 The Structure of Cyclic groups

Theorem 6.6. Let G be a cyclic group with generator a.

1. If G has finite order n then G is isomorphic to $\langle \mathbb{Z}_n, + \rangle$.
2. If G is infinite then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.

Proof. Suppose $G = \langle a \rangle$. Suppose G is finite. Then, there are integers $r < s$ such that $a^r = a^s$ and hence $a^{s-r} = e$. So, $a^m = e$ for some integer $m > 0$. So, the set $\{m : a^m = e \textit{ with } m > 0\}$ is nonempty.

$$\textit{Let} \qquad n = \min\{m : a^m = e \textit{ with } m > 0\}$$

Define $\varphi : \mathbb{Z}_n \longrightarrow G$ by assigning $\varphi(\overline{k}) = a^k$, where $k = 0, 1, 2, \ldots, n-1$.

First, φ is onto. To see this let $x = a^m \in G$. By division algorithm $m = nq + r$ for some $0 \le r \le n - 1$. So, $x = a^m = a^{nq+r} = (a^n)^q a^r = \varphi(\overline{r})$. It is established that φ is onto. Now, to prove that φ is one to one let $\varphi(\overline{r}) = \varphi(\overline{s})$ for some $0 \le r \le s \le n - 1$. So, $a^r = a^s$ and hence $a^{s-r} = e$. Since $0 \le s - r \le n - 1$, by minimality of n we have $s - r = 0$. So, φ is one to one. Also, note $\varphi(x + y) = \varphi(x)\varphi(y)$ for all

$x, y \in \mathbb{Z}_n$. So, it is established that G is isomorphic to $\mathbb{Z}_n$, as group structures.

Now suppose G is infinite. Define

$$\varphi : \mathbb{Z} \longrightarrow G \qquad by \qquad \varphi(r) = a^r.$$

It follows $\varphi(r+s) = a^{r+s} = a^r a^s = \varphi(r)\varphi(s)$. So, φ is a well defined homomorphism of the binary structures. In fact, φ is onto, because $G = \{a^r : r \in \mathbb{Z}\}$. Now we prove that φ is one to one. Suppose $\varphi(r) = \varphi(s)$. So, $a^r = a^s$. We assume $r \leq s$. So, $a^{s-r} = e$. Write $m = s - r \geq 0$. If $m > 0$, using division algorithm, it follows $G = \{e, a, a^2, \ldots, a^{m-1}\}$. Since G is infinite, this is not possible. So, $r = s$ and φ is one to one. So, φ is an isomorphism. The proof is complete.■

6.3 Subgroups of Finite Cyclic Groups

Theorem 6.7. Let $G = \langle a \rangle$ be a finite cyclic group of order n. Let $b = a^s$ and $H = \langle b \rangle$. Order of H is $|H| = \frac{n}{d}$ where $d = gcd(s, n)$

Proof. Read from the textbook.

1. In fact, we may assume

$$G = \langle \mathbb{Z}_n, + \rangle = \langle \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}, + \rangle \qquad \textit{with} \quad a = \overline{1}.$$

2. The statement of the theorem means, if $b = \overline{s}$ and $H = \langle \overline{s} \rangle$, then H has $\frac{n}{\gcd(s,n)}$ elements.

3. In the easy case, if $s|n$ then $d = \frac{n}{\gcd(s,n)} = n/s$ and

$$H = \langle \{\overline{0}, \overline{s}, \overline{2s}, \ldots, \overline{((d-1)s)}\}, + \rangle$$

4. Again, if $s \not| n$, then with $d = \frac{n}{\gcd(s,n)}$, whe have

$$H = \langle \{\overline{0}, \overline{s}, \overline{2s}, \ldots, \overline{((d-1)s)}\}, + \rangle$$

The proof is complete. ■

Reading Assignment: Read Examples 6.13, 6.15-6.17.

7 Generating Sets

Abstract: *Given a group and a subset $S \subseteq G$, we define the smallest subgroup H of G containing S. This H is called the subgroup of G generated by S.*

For a group G and $a \in G$ the subgroup generated by a was the cyclic group $H = \langle a \rangle$.

Theorem 7.1. Let G be a group. Suppose H_i is a set of subgroups of G indexed by $i \in I$. Then the intersection $H = \bigcap_{i \in I} H_i$ is a subgroups of G.

Proof. We have check three conditions (we do not need to check associativity).

1. First, we need to show H is closed under multiplication.

$$x, y \in H \Longrightarrow (x, y \in H_i \ \forall\ i \in I) \Longrightarrow (x \cdot y \in H_i \ \forall\ i \in I)$$

   because H_i are subgroups. So, $x \cdot y \in H$ and H is closed under multiplication.

2. We do not have to check associativity of multiplication in H, because it is inherited from G.

3. Again, since H_i are subgroups

$$(e \in H_i \ \forall\ i \in I) \Longrightarrow e \in H.$$

   So, $e \in H$, which satisfies the property of the identity in H.

4. Inverse: let $a \in H$.

$$a \in H \Longrightarrow (a \in H_i \ \forall\ i \in I) \Longrightarrow (a^{-1} \in H_i \ \forall\ i \in I)$$

   because H_i are subgroups. So, $a^{-1} \in H$, which satisfies the property of inverse in H.

So, H is a subgroup of G. The proof is complete.

■

Definition 7.2. Let G be a group and $S = \{a_i : i \in I\} \subseteq G$.

1. Then, the smallest subgroup $\mathcal{G}(S)$ of G is called the **subgroup generated by** S. So,

$$\mathcal{G}(S) = \bigcap\{H \leq G : S \subseteq H\}$$

   Note that there is one subgroup, namely G, of G that contains S. So, the right hand side in not an empty-intersection.

2. If $G = \mathcal{G}(S)$ we say that G is generated by S. We also say that G is generated by $\{a_i\}$.

3. If there is a finite set $S = \{a_1, a_2, \ldots, a_n\}$ that generates G then we say that G is **finitely generated**. If there is no such finite set, we say G is **infinitely generated**.

Theorem 7.3. Let G be a group and $S = \{a_i : i \in I\} \subseteq G$ is a subset. Let $\mathcal{G}(S)$ be the subgroup generated by S.

1. Write $S^{-1} = \{a_i^{-1} : i \in I\}$. Then, $\mathcal{G}(S)$ consists of all the "words" (of finite length) written with $S \cup S^{-1} = \{a_i, a_i^{-1} : i \in I\}$.

2. Note, such a "word" looks like $w = x_1 x_2 \cdots x_n$ where $x_j = a_i$ or $x_j = a_i^{-1}$ for some i. When adjacent "letters" are a_i and/or a_i^{-1}, we can combine them and write $w = y_1^{n_1} y_2^{n_2} \cdots y_r^{n_r}$ where $y_j = a_i$ for some i.

Proof. We only need to prove (1). Let H be the set consisiting of all such "words". Then

1. $S \subseteq H$ because a_i is an word of lenght one.
2. $e = a_i a_i^{-1} \in H$.
3. Let $w = x_1 x_2 \cdots x_n$ is a "word" $x_j = a_i$ or $x_j = a_i^{-1}$ for some i. Then $w^{-1} = x_n^{-1} x_{n-1}^{-1} \cdots x_2^{-1} x_1^{-1}$ is a "word" of the same kind. So, $w \in H$.

So, H is a subgroup of G containing S. Now, if K is a subgroup of G containing S, then each such "word" is in K. So, $H \subseteq K$. So, H is the smallest such group and $H = \mathcal{G}(S)$. The proof is complete. ■

Corollary 7.4. *Suppose G and S be as above (7.3). Assume G is abelian. Then,*

$$G = \{a_1^{n_1} a_2^{n_2} \cdots a_r^{n_r} : r \geq 0, n_i \in \mathbb{Z}, a_i \in S \textit{ are distinct}\}.$$

In additive notation:

$$G = \{n_1 a_1 + n_2 a_2 + \cdots + n_r a_r : r \geq 0, n_i \in \mathbb{Z}, a_i \in S \textit{ are distinct}\}.$$

Proof. Follows directly from (7.3), because we can switch the elements. The proof is complete. ■