Shri Govind Guru University

B.Sc. Sem-5, Mathematics, Abstract Algebra: BSCC506B

Nishant Parmar

Department of Mathematics
Government Science College Chhotaudepur

Disclaimer:

The material provided in this file is purely for learning and sharing of knowledge purpose. Authors does not claim to cover all the prescribed syllabus. For reference and examination purpose the reference books prescribed in official syllabus of the university will be considered final.

Relation

Definition 1 (Relation)

For the nonempty subsets A and B, any subset S of $A \times B$ is called a *relation from A to B.*

For $a \in A$ and $b \in B$, $(a, b) \in S$, then we say that "a is related to b by the relation S"

The trivial relations $S = \phi$ and $S = A \times B$ are not very important. So from now whenever we use relation we mean proper relation. i.e. $S \neq \phi, \; S \neq A \times B$.

Example 1

Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$, then
$S = \{(1, a), (2, b), (3, a), (2, d)\}$ is a relation.

Example 2

Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$, then
$S = \{(1, a), (2, b), (3, a), (2, c)\}$ is a relation.

Example 3

Let $A = \{1, 2, 3\}$, then
$S = \{(1, 1), (2, 2), (3, 3), (2, 1)\}$ is a relation on A.

Example 4

For $\mathbb{Z}$, $S = \{(a, b) : a - b \text{ is odd number}\}$. Then S is a relation on $\mathbb{Z}$

Definition 2 (Equivalence Relation)

A relation S defined on a set A is said to be an *equivalence relation if it satisfies the following three properties.*

- *S is said to be reflexive if for each $a \in A$, aSa i.e. every element of A is related to itself.*
- *S is said to be symmetric if for each $a, b \in A$, $aSb \Rightarrow bSa$.*
- *S is said to be transitive if for each $a, b, c \in A$, aSb and $bSc \Rightarrow aSc$.*

Although we are free to use any notation, we'll mostly use $\sim$ to denote an equivalence relation.

Example 5

Let $A = \{1, 2, 3\}$, then
$S = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$ is an equivalence relation on A.

Example 6

Let $A = \{1, 2, 3\}$, then
$S = \{(1,1), (2,2), (3,3), (1,2), (2,1), (2,3), (3,2)\}$ is also an equivalence relation on A.

Example 7

Let $A = \{1, 2, 3\}$, then
$S = \{(1,1), (2,2), (3,3), (1,2)\}$ is NOT an equivalence relation on A.

Example 8

For $\mathbb{Z}$, $S = \{(a, b) : a - b \text{ is even number}\}$. Then S is an equivalence relation on $\mathbb{Z}$

Definition 3

Let $\sim$ be an equivalence relation on A and $a \in A$. Then the set $\{x \in A : x \sim a\}$ is called an *equivalence class of a. It is denoted by $cl(a)$ or $[a]$.*

Example 9

In example 5, $[1] = \{1, 2\}$. also, $[3] = \{3\}$

Example 10

In example 8,

$[0] = \{x \in \mathbb{Z} : x - 0 \text{ is even number}\} = \{x \in \mathbb{Z} : x \text{ is even number}\}$

Also, $[1] = \{x \in \mathbb{Z} : x - 1 \text{ is even number}\} = \{x \in \mathbb{Z} : x \text{ is odd number}\}$

Some important observations:

- For any $a \in A$, $a \in [a] \Rightarrow [a] \neq \phi$. Also $A \subset \bigcup_{a \in A} [a]$
- For each $a \in A$, $[a] \subset A \Rightarrow \bigcup_{a \in A} [a] \subset A$.
- Therefore, $A = \bigcup_{a \in A} [a]$.
- For $a, b \in A$, Let $a \sim b$.
  For any
  $x \in [a] \Rightarrow x \sim a \Rightarrow x \sim b (\because \sim$ is transitive$) \Rightarrow x \in [b] \Rightarrow [a] \subset [b]$
  Similarly for any
  $x \in [b] \Rightarrow x \sim b \Rightarrow x \sim a (\because \sim$ is symmetric and transitive$)$
  $\Rightarrow x \in [a] \Rightarrow [b] \subset [a]$
  Hence, if $a \sim b$ then $[a] = [b]$

Lemma 1

For $a, b \in A$ and an equivalence relation $\sim$ on A. Either $[a] = [b]$ or $[a] \cap [b] = \phi$ i.e. equivalence classes are either equal or disjoint.

As last point above we have showed that if $a \sim b$, then $[a] = [b]$. Now we will show that if $a \nsim b$, then $[a] \cap [b] = \phi$.
Suppose $a \nsim b$. but $x \in [a] \cap [b]$
$\Rightarrow x \in [a]$ and $x \in [b]$
$\Rightarrow x \sim a$ and $x \sim b$
$\Rightarrow a \sim x$ and $x \sim b$ ($\because \sim$ is symmetric)
$\Rightarrow a \sim b$ ($\because \sim$ is transitive)
Which contradicts our assumption. Hence, if $a \nsim b$, then $[a] \cap [b] = \phi$.
This proves the result.

Binary operations

Definition 4

For a nonempty set A, a mapping $A \times A$ is called a *binary operation on A.*

Example 11

The operation $*$ defined on $\mathbb{Z}$ as follows is a binary operation.
$m * n = m - n$ for $m, n \in \mathbb{Z}$

Example 12

The operation $*$ defined on $\mathbb{N}$ as follows is NOT a binary operation.
$m * n = m - n$ for $m, n \in \mathbb{N}$
Because, for $2, 3 \in \mathbb{N}$, $2 - 3 = -1 \notin \mathbb{N}$

Example 13

The operation $*$ defined on $\mathbb{N}$ as follows is a binary operation.
$m * n = min\{m, n\}$ for $m, n \in \mathbb{N}$

Definition 5

The binary operation $*$ on a nonempty set$A$ is said to be *commutative if* $a * b = b * a, \ \forall a, b \in A$

Example 14

The usual addition operation defined on $\mathbb{Z}$ is commutative. because for any $m, n \in \mathbb{Z}, \ m + n = n + m$.

Example 15

The usual multiplication operation defined on $\mathbb{R}$ is commutative. because for any $m, n \in \mathbb{R}, \ m.n = n.m$.

Example 16

The subtraction operation defined on $\mathbb{Z}$ in Example 11 is NOT commutative. because for any $2 - 3 = -1 \neq 3 - 2$.

Definition 6

The binary operation $*$ on a nonempty set$A$ is said to be *associative if*
$(a * b) * c = a * (b * c), \ \forall a, b, c \in A$

There are some operations which are not associative, but we'll not discuss them here. Most operation we shall use in this course are associative.

Definition 7

Suppose $*$ and o are two binary operations on a set S. If for every $a, b, c \in A$

$$a * (b \circ c) = (a * b) \circ (a * c)$$
$$(b \circ c) * a = (b * a) \text{o} (c * a)$$

then the binary operation $*$ is said to be distributive over o.

Example 17

Union and intersection are binary operations in $P(U)$ and for $A, B, C \in P(U)$, we have

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

Definition 8

Let $*$ be the binary operation in A. If for an element e in A and for each a of A, $a * e = e * a = a$, then e is called an identity element of A for binary operation $*$

Example 18

we know that e is a 0 for addition and e is a 1 for multiplication in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$.

Theorem 1

There can be at most one identity element for a binary operation $*$ on A.

Proof: If possible, suppose e and e' are the two identity elements for binary operation $*$ on A. Now e being an identity element, $e * e' = e'$. Similarly, e' being an identity element,

$$e * e' = e \quad \text{i.e.} \quad e = e'$$

Definition 9

Let e be the identity element for binary operation $*$ on A. If for a given element $x \in A$, there exists an element $y \in A$ such that $x * y = y * x = e$, then y is called an *inverse of* x. *Elements for inverse exist are called non-singular elements.*

Theorem 2

Theorem 5.3 .2 If the binary operation $*$ on A with identity e is associative, then a given element $a \in A$ can have at most one inverse.

Proof: If b and c are inverses of a in A, then, we have, $b * a = a * b = e$ and $c * a = a * c = e$. Now,

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$

Theorem 3

If for an associative binary operation o on $A, a \in A$ is nonsingular then its inverse a^{-1} is also non-singular and $\left(a^{-1}\right)^{-1} = a$

Proof : Here a being non-singular, a o $a^{-1} = a^{-1}$ o $a = e$. Thus, a^{-1} is also non-singular and its unique inverse is a, i.e. $\left(a^{-1}\right)^{-1} = a$

If $+$ is associative binary operation and a is non-singular element for $+$ then $-a$ is also non-singular with $-(-a) = a$

Theorem 4

For an associative binary operation $*$ on A, if a and b are non-singular then $a * b$ is also non-singular with $(a * b)^{-1} = b^{-1} * a^{-1}$

Proof: Here a and b being non-singular, a^{-1} and b^{-1} exist. Using associativity of $*$

$$\begin{aligned}(a * b) * \left(b^{-1} * a^{-1}\right) &= a * \left[b * \left(b^{-1} * a^{-1}\right)\right] \\ &= a * \left[\left(b * b^{-1}\right) * a^{-1}\right] \\ &= a * \left[e * a^{-1}\right] \\ &= a * a^{-1} \\ &= e\end{aligned}$$

Similarly, we have

$$\left(b^{-1} * a^{-1}\right) * (a * b) = e$$

Hence by definition, $(a * b)^{-1} = b^{-1} * a^{-1}$

Definition 10

A binary operation $*$ defined on A is said to satisfies

- the left cancellation law if for every $a, b, c \in A$

$a * b = a * c \Rightarrow b = c$.

- the right cancellation law if for every $a, b, c \in A$

$b * a = c * a \Rightarrow b = c$.

- It is said to satisfy the cancellation law if it satisfies both left and right cancellation law.

Theorem 5 (Division Algorithm)

For given $a, b(\neq 0) \in \mathbb{Z}$, *there exist unique integers* q *and* r *such that* $a = bq + r, 0 \leq r < |b|$

Here a is called the dividend, b the divisor, q the quotient, and r the remainder obtained on dividing a by b. Clearly, the remainder $r = 0$ iff b I a.

First we consider a special case of this theorem.

Theorem 6 (Spacial case of division algorithm)

For $a \in \mathbb{Z}$ *and* $b \in \mathbb{N}$, *there exist unique integers* q *and* r *such that* $a = bq + r, 0 \leq r < b$

Proof: Define the set $M = \{a + bx | x \in \mathbb{Z}\}$. For $a \geq 0, a + b > 0$ and $a + b \in M$. For $a < 0, a + b(-a) = a(1 - b) \geq 0$ (here $a < 0$ and $(1 - b)$ ≤ 0) and $a + b(-a) \in M$.

In both these possibilities for a, M contains non-negative integers and consequently the set $L = \{y \in M | y \geq 0\}$ is nonempty.

By the well-ordering principle, L has the least element, say, r. Here, $r \in L \subset M$ gives us $r \geq 0$ and for some x (say $x = -q$), $r = a - bq$ or $a = bq + r$.
Now we show that $r < b$. For $r \geq b, 0 \leq r - b = a - bq - b = a - b(q+1) \in M$ and hence $r - b \in L$, a contradiction to the definition of r Hence $r < b$ To prove uniqueness of q and r, suppose

$$a = bq + r, 0 \leq r < b$$

and

$$a = bq_1 + r_1, 0 \leq r_1 < b$$

We will show that $q = q_1$ and $r = r_1$. For $q < q_1, q$ and q_1 being integers, $(q+1) \leq q_1$. This gives us

$$0 \leq r_1 = a - bq_1 \leq a - b(q+1) = a - bq - b = r - b < 0$$

which is a contradiction.

Similarly $q_1 < q$ gives a contradiction. Hence $q = q_1$
Now, $bq + r = a = bq + r_1$ or $r = r_1$.
Proof of Theorem 5: For $b > 0$, this theorem follows from Theorem 6 For $b < 0, a$ and $|b|$ satisfy the hypothesis of Theorem 6.2 .4 and hence we get unique integers q_1 and r such that $a = |b|q_1 + r$ with $0 \leq r < |b|$.
For $b < 0, b = -b$. Taking $q = -q_1$, we have $a = bq + r$ with $0 \leq r < |b|$ and this completes the proof of the theorem.

Congruence Relation

Definition 11

For $n \in \mathbb{N}$, and integers $a, b \in \mathbb{Z}$, if $n|(a - b)$, then we say that a is congruent to b with respect to n. We write it as $a \equiv b(mod\ n)$.

Example 19

5 divides $13 - (-17) = 30$. Hence $13 \equiv -17(mod\ 5)$

Example 20

3 divides $11 - 2 = 9$. Hence $11 \equiv 2(mod\ 3)$

Lemma 2 (without proof)

For a fixed $n \in \mathbb{N}$, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Theorem 7

For a fixed $n \in \mathbb{N}$, congruence modulo n, equivalence relation has exactly n distinct eqivalence classes.

Proof: By division algorithm, $a = qn + r, 0 \leq r < n$. Hence $a - r = qn$ or $n|(a - r)$, i.e. $a \equiv r (\bmod n)$. By a known theorem,$[a] = [r]$.
Thus for a given integer a, we have a unique integer $r, 0 \leq r < n$ such that $[a] = [r]$. In other words, we have at most n distinct congruence classes namely $[0], [1], \ldots, [n - 1]$.
Now we show that these congruence classes are distinct. If possible, suppose two congruence classes say, $[i]$ and $[j]$ are equal. Here we can take $0 \leq i < j < n$. The $[i] = [j]$ gives $i \equiv j (\bmod n)$ or $n|(j - i)$ which is impossible as $(j - i)$ is less than n.
This contradictory result shows that we have exactly n distinct congruence classes $[0], [1], \ldots, [n - 1]$

Example 21

For $n = 5$, we have

$$\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} = \{5n | n \in \mathbb{Z}\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} = \{5n + 1 | n \in \mathbb{Z}\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} = \{5n + 2 | n \in \mathbb{Z}\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} = \{5n + 3 | n \in \mathbb{Z}\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\} = \{5n + 4 | n \in \mathbb{Z}\}
\end{aligned}$$

Also

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4] \text{ and } [i] \cap [j] = \phi$$
$$\text{for } i \neq j, 0 \leq i, j \leq 4$$

- We denote $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$, call it *the set of integers modulo n*
- We define addition $+_n$ and multiplication $\cdot_n$ in $\mathbb{Z}_n$ as follows.

For $[i], [j] \in \mathbb{Z}_n$

$$[i] +_n [j] = [i + j]$$
$$[i] \cdot_n [j] = [ij]$$

The addition and multiplication defined by the above equations are called addition modulo n and multiplication modulo n, respectively.

Example 22

$$[2] +_5 [8] = [10] = [0]; \quad [-3] +_5 [16] = [13] = [3]$$
$$[2] \cdot_5 [8] = [16] = [1]; \quad [-3] \cdot_5 [16] = [-48] = [2]$$

We can use tables for quickly evaluating modulo n operations.

Example 23 ($+_6$ operation on $\mathbb{Z}_6$)

$+_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Example 24 ($\cdot_6$ operation on $\mathbb{Z}_6$)

$\cdot_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Definition 12

If an operation $*$ defined on a nonempty set G satisfies the following postulates

1. $*$ is a binary operation on G
2. For $a, b, c \in G, a * (b * c) = (a * b) * c$(i.e. $*$ is associative)
3. There exists an element e in G such that $a * e = e * a = a$ for each $a \in G$ (i.e. there is existence of an identity element for G).
4. For each $a \in G$, there exists an element $a' \in G$ such that $a * a' = a' * a = e$ (i.e. there is existence of an inverse for each element)

then G is called a *group under the binary operation* $*$. *It is denoted by* $(G, *)$.
If $*$ *is commutative, i.e.* $a * b = b * a, \forall a, b \in G$. *Then* $(G, *)$ *is called a commutative group or abelian group.*

Example 25

$(\mathbb{Z}, +)$ where $+$ is usual addition of integers is a group.
Here 0 is identity element and $-a$ is inverse for any element a.
Similarly $(\mathbb{Q}, +)$,$(\mathbb{R}, +)$,$(\mathbb{C}, +)$ are also group.

Example 26

$(\mathbb{Q}^*, \cdot)$ where . is usual multiplication is a commutative group.$(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\})$.
Here 1 is identity element and $1/a$ is inverse for any element a.
Similarly $(\mathbb{R}^*, \cdot)$,$(\mathbb{C}^*, \cdot)$, are also commutative group.

Example 27

For a fixed positive integer n, $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$. Then $(\mathbb{Z}_n, +_n)$ is a commutative group.
$[0]$ is identity and $[n-i]$ is an inverse for $[i]$.

Example 28

For a fixed prime integer $p \in \mathbb{N}$, $\mathbb{Z}_n^* = \{[1], \ldots, [n-1]\}$. Then $(\mathbb{Z}_n^{;} \cdot_n)$ is a commutative group.

Example 29

For a fixed given positive integer n, the set $\mathbb{R}_n$ is defined as
$\mathbb{R}_n = \{z \in \mathbb{C} | z^n = 1\}$.$\mathbb{R}_n$ is the set of all n^{th} complex roots of unity. If $\rho = e^{2\pi i n}$, then $\mathbb{R}_n = \left\{\rho, \rho^2, \ldots, \rho^{n-1}, \rho^n = 1\right\}$.
$\mathbb{R}_n$ is a group under multiplication because
(i) For $a, b \in \mathbb{R}_n$ if $a = \rho^i$ and $b = \rho^j, 1 \leq i, j \leq n$ then $ab = \rho^{i+j}$ For $i + j \leq n, ab \in \mathbb{R}_n$.
For $i + j \geq n$, if $i + j = qn + r, 0 \leq r < n$ then
$ab = \rho^{i+j} = \rho^{qn+r} = (\rho^n)^q \rho^r = \rho^r \in \mathbb{R}_n$, i.e. multiplication becomes a binary operation in $\mathbb{R}_n$
(ii) $\mathbb{R}_n$ being a subset of $\mathbb{C}$, multiplication is associative.
(iii) $1 \in \mathbb{R}_n$ becomes an identity element for multiplication.
(iv) For $a = \rho^i \in \mathbb{R}_n, 1 \leq i < n, b = \rho^{n-i} \in \mathbb{R}_n$ with $ab = ba = 1$.
We will denote this group by $(\mathbb{R}_n;)$

Example 30

Let us denote $\mathbb{M}_n = \{[(a_{ij})]_{n\times n} : a_{ij} \in \mathbb{R}\}$ = the set of all $n \times n$ real matrices.
Under the operation matrix addition $+$, $(\mathbb{M}_n, +)$ is a group.
Where $n \times n$ zero matrix is an identity and for any element $[a_{ij}]_{n\times n}$ inverse is $[-a_{ij}]_{n\times n}$.

Example 31

Let us dentoe $GL_2(\mathbb{R})$ = general linear group of order 2 on $\mathbb{R}$ = Group of all 2×2 real invertible matrices with matrix multiplication operation.
A matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible iff it's determinant is non-zero. i.e. $ad - bc \neq 0$.
The identity matrix $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is identity of the group. And for any matrix A it's inverse matrix A^{-1} is inverse of that matrix in the group.

Elementary properties of a Group

Theorem 8

In a group G

(i) Identity element is unique.

(ii) Inverse of an element is unique.

(iii) If the inverse of an element a is denoted by a^{-1}*, then* $\left(a^{-1}\right)^{-1} = a$

(iv) For $a, b \in G, (a * b)^{-1} = b^{-1} * a^{-1}$

(v) Both cancellation laws hold good for $*$ *in* G*. That is, for* $a, b, c \in G$

$a * b = a * c$ *or* $b * a = c * a$ *implies* $b = c$

Theorem 9

Theorem 7.3.2 In a group G, the equations $a * x = b$ and $y * a = b$, where $a, b \in G$, have unique solutions.

$a * \left(a^{-1} * b\right) = \left(a * a^{-1}\right) * b$ (associative law)
$= e * b$ (definition of a^{-1})
$= b$ (property of e)
Thus $x = a^{-1} * b$ is a solution of $a * x = b$
To prove uniqueness of this solution, suppose $a * x = b$ and $a * x_1 = b$
Then $a * x = a * x_1$. By cancellation law in $G, x = x_1$
The equation $y * a = b$ can be considered in a similar way.

Equivalent definitions of a group

Theorem 10

If for a binary operation $*$ defined in G
(i) $*$ is associative
(ii) there exists an element $e_1 \in G$ such that $a * e_1 = a$ for each $a \in G$
(i.e. the existence of right identity in G), and
(iii) for each $a \in G$, there exists an element $b \in G$ such that $a * b = e_1$
(i.e. the existence of right inverse for each element in G),
then G is a group.

Proof: First, we prove the right cancellation law in G.
Suppose $x * a = y * a$ for $x, y, a \in G$. By assumption (iii), there exists an element $b \in G$ such that $a * b = e_1$. Now

$$(x * a) * b = (y * a) * b$$
$$x * (a * b) = y * (a * b) \qquad \text{(by assumption (i))}$$
$$x * e_1 = y * e_1$$
$$x = y \text{ (by assumption (ii))}$$

Also

$$\begin{aligned}(e_1 * a) * b &= e_1 * (a * b)^* \\ &= e_1 * e_1 \\ &= e_1 = a * b\end{aligned}$$

By the right cancellation law, $e_1 * a = a$. Thus for each $a \in G, a * e_1 = e_1 * a = a$, i.e. e_1 is an identity element in G. Again

$$\begin{aligned}(b * a) * b &= b * (a * b) \\ &= b * e_1 \\ &= b \\ &= e_1 * b\end{aligned}$$

Therefore by the right cancellation law, $b * a = e_1$. In other words, $a * b = b * a = e_1$ or b is an inverse of a. Thus each element in G has an inverse in G.

Hence, G is a group.

Theorem 11

If for a binary operation $*$ defined in G
(i) $*$ is associative and
(ii) For each $a, b \in G$, the linear equations $a * x = b$ and $y * a = b$ have solutions in G
then $(G, *)$ is a group.

Proof: Let $a \in G$. The linear equation $a * x = b$ has a solution in G for each a, b in G. In particular taking $b = a$, the equation $a * x = a$ has also a solution in G. If we denote this solution by e_1, then

$$a * e_1 = a$$

If c is any element of G, then the equation $y * a = c$ has a solution, say, y_1 in G, i.e. $y_1 * a = c$. Now

$$\begin{aligned} (y_1 * a) * e_1 &= c * e_1 \\ y_1 * (a * e_1) &= c * e_1 \\ y_1 * a &= c * e_1 \quad \text{by } (7.4.1) \\ c &= c * e_1 \end{aligned}$$

Thus $c = c * e_1$ for any element $c \in G$ or e_1 is a right identity for $*$ in G Also the equation $a * x = e_1$ has a solution in G. Clearly, this solution will be a right inverse of a, i.e. each element has a right inverse for $*$ in G. By Theorem 7.4.1, G is a group under $*$

Theorem 12

Let $*$ be a binary operation on a finite set G. If
(i) $*$ is associative and
(ii) both right and left cancellation laws hold for $*$ in G
then $(G, *)$ is a group.

Proof: Suppose $G = \{a_1, a_2, \ldots, a_n\}$. For any element $a \in G$

$$a * a_1, a * a_2, \ldots, a * a_n \in G$$

and hence

$$S = \{a * a_1, a * a_2, \ldots, a * a_n\} \subset G$$

The elements of S are distinct. Suppose $a * a_i = a * a_j, 1 \leq i < j \leq n$. By the left cancellation law, $a_i = a_j$ which is impossible as a_i and a_j are distinct elements of G.
Now $S \subset G, S$ and G both have n elements, i.e. $S = G$. Thus $a \in G = S$ implies $a = a * a_k$ for some k. Also $a * a = (a * a_k) * a = a * (a_k * a)$.
Again by the left cancellation law, $a = a_k * a$, i.e. $a = a_k * a = a * a_k$
If b is any element of G then

$$a * b = (a * a_k) * b = a * (a_k * b)$$

which gives $b = a_k * b$ by the cancellation law. Similarly $b * a_k = b$

In short, a_k is an identity element for $*$ in G $a_k \in G = S$ implies $a_k = a * a_j$ for some $a_j \in G$. Also

$$a_k * a = (a * a_j) * a \quad \text{or} \quad a * a_k = a * (a_j * a)$$

The cancellation law gives $a_k = a_j * a$, i.e. $a_k = a * a_j = a_j * a$.
In other words, each element has an inverse in G.
Thus G is a group under $*$.

Theorem 13

Theorem 7.5.2 *Suppose* $a, b \in G$. *If* $ab = ba$, *then (i)* $ab^n = b^n a$ *(ii)* $(ab)^n = a^n b^n$ *for each* $n \in \mathbb{N}$

Proof: We prove this theorem with the help of the first principle of mathematical induction.

(i) For $n = 1, ab = ba$ which is true by assumption. Now suppose the result is true for $n = k$, i.e. $ab^k = b^k a$. Then

$a\left(b^{k+1}\right) = a\left(b^k b\right)$ (by definition of power)

$= \left(ab^k\right) b$ (by associative law)

$= \left(b^k a\right) b$ (by assumption)

$= b^k(ab)$ (by associative law)

$= b^k(ba)$ (by assumption)

$= \left(b^k b\right) a$ (by associative law)

$= b^{k+1} a$ (by definition of power)

That is, the result is also true for $n = k + 1$

(ii) The result is obviously true for $n = 1$. Now suppose the result is true for $n = k$, i.e. $(ab)^k = a^k b^k$. Then

$$\begin{aligned} (ab)^{k+1} &= (ab)^k (ab) \\ &= \left(a^k b^k\right)(ab)^{\dagger +} \\ &= \left(a^k b^k a\right) b \\ &= \left(a^k a b^k\right) b \\ &= a^{k+1}\left(b^k b\right) \\ &= a^{k+1} b^{k+1} \end{aligned}$$

That is, the result is true for $n = k + 1$ as well.

Theorem 14

Suppose $a \in G$ and $m \in \mathbb{N}$. For each $n \in \mathbb{Z}$ (i) $a^m a^n = a^{m+n}$ (ii) $(a^m)^n = a^{mn}$

Proof : (i) We divide the proof into two cases according as $n \geq 0$ and $n < 0$

Case 1: Suppose $n \geq 0$ since $a^m a^0 = a^m e = a^m = a^{m+0}$, the result is true for $n = 0$. Also, the definition of power $a^{m+1} = a^m a$ shows that the result is true for $n = 1$ as well.

Now if the result is true for $n = k$, i.e. $a^m a^k = a^{m+k}$, then

$$\begin{aligned} a^{m+k+1} &= a^{(m+k)+1} \\ &= a^{m+k} a \\ &= \left(a^m a^k\right) a \\ &= a^m \left(a^k a\right) \\ &= a^m a^{k+1} \end{aligned}$$

Thus the result is true for $n = k + 1$. Hence it is true for each natural number n by the first principle of mathematical induction.
Case 2 : $n < 0$. Suppose $n = -p$ By the Law of Trichotomy, we have one of the three possibilities, namely

$$p = m \quad \text{or} \quad p > m \quad \text{or} \quad p < m$$

For $p = m$, and $n = -m$

$$\begin{aligned} a^{m+n} &= a^{m-m} \\ &= a^0 \\ &= e \\ &= e^m \\ &= \left(aa^{-1}\right)^m \\ &= a^m \left(a^{-1}\right)^m \\ &= a^m a^{-m} \\ &= a^m a^n \end{aligned}$$

If $p > m$, then $p = m + k$ for some positive integer k. Here

$$\begin{aligned}
a^{m+n} &= a^{m-p} \\
&= a^{-k} \\
&= \left(a^{-1}\right)^{k} \\
&= e\left(a^{-1}\right)^{k} \\
&= e^{m}\left(a^{-1}\right)^{k} \\
&= \left(aa^{-1}\right)^{m}\left(a^{-1}\right)^{k} \\
&= \left[a^{m}\left(a^{-1}\right)^{m}\right]\left(a^{-1}\right)^{k} \\
&= a^{m}\left[\left(a^{-1}\right)^{m}\left(a^{-1}\right)^{k}\right] \\
&= a^{m}\left(a^{-1}\right)^{p} \\
&= a^{m}\left(a^{-p}\right) \\
&= a^{m} \cdot a^{n}
\end{aligned}$$

Finally, if $p < m$, then $m = p + r$ for some positive integer r. Again

$$\begin{aligned} a^{m+n} &= a^{m-p} \\ &= a^{r} \\ &= a^{r} e^{r} e^{p} \\ &= a^{r} \left[\left(a a^{-1} \right)^{p} \right] \\ &= a^{r} \left[a^{p} \left(a^{-1} \right)^{p} \right] \\ &= \left(a^{r} a^{p} \right) \left(a^{-1} \right)^{p} \\ &= a^{r+p} \left(a^{-1} \right)^{p} \\ &= a^{m} \left(a^{-1} \right)^{p} \\ &= a^{m} a^{-p} \\ &= a^{m} \cdot a^{n} \end{aligned}$$

Thus we have $a^m a^n = a^{m+n}$ for each $n \in \mathbb{Z}$

(ii) Proof almost identical to the proof of part (i). Try it at home.

Theorem 15

Suppose G is finite group of order n. For $a \in G$, there exists a positive integer $r \leq n$ such that $a^r = e$

Proof: since $a^0, a^1, a^2, \ldots, a^n \in G$ and G has n elements, these $(n+1)$ elements cannot be distinct, i.e. at least two of them must be equal. In other words, $a^i = a^j$ for some i and j with $0 \leq i < j \leq n$. Hence $e = a^0 = a^i \cdot a^{-i} = a^j \cdot a^{-i} = a^{j-i}$ by result (i) of Theorem 14. If $j - i = r$ then $1 \leq r \leq n$ and $a^r = e$

Finite groups and their tables

Example 32

For $G = \{e, a, b\}$ consider the following table for operation $*$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

By using above table it is very easy to verify all the properties required for $(G, *)$ to be a group.

We have already checked another example of tables for $\mathbb{Z}_6$.