Algebra Note

Miliyon T.
Addis Ababa University
Department of Mathematics
http://www.albohessab.weebly.com

Contents

1 Introduction

1.1 Sets

Definition 1.1 (Equality of sets)**.** For any two sets A and B; $A = B \Leftrightarrow A \subseteq B$ and $B \subseteq A$.

1.2 Functions

Let $f : A \to B$. Then the diagram of functions

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "h"'] & & B \arrow[dl, "g"] \\ & C & \end{tikzcd}$$

is said to be commutative if $g \circ f = h$. Similarly, the diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"'] & B \arrow[d, "g"] \\ C \arrow[r, "k"'] & D \end{tikzcd}$$

is said to be commutative if $g \circ f = k \circ h$.
If $f : A \to B$

1. $S \subset A,\ f(S) = \{f(x) : x \in S\}$.
2. $T \subset B,\ f^{-1}(T) = \{x \in A : f(x) \in T\}$.
3. $S \subset A \Rightarrow S \subset f^{-1}(f(S))$. If f is $1-1$, then $S = f^{-1}(f(S))$.
4. $T \subset B \Rightarrow T \subset f(f^{-1}(T))$. If f is onto, then $T = f(f^{-1}(T))$.

If $A \xrightarrow{f} B \xrightarrow{g} C$, then $g \circ f : A \to C$

1. If f, g is $1-1$, so is $g \circ f$.
2. If f, g is onto, $g \circ f$ is onto.

Definition 1.2 (Equivalence relation)**.** A relation R on a set A is an equivalence relation if it satisfies

(i) Reflexive: $(a, a) \in R,\ \forall a \in A$.

(ii) Symmetric: $(a, b) \in R \Rightarrow (b, a) \in R,\ \forall a, b \in A$.

(iii) Transitive: $(a, b), (b, c) \in R \Rightarrow (a, c) \in R,\ \forall a, b, c \in A$.

Definition 1.3. $\bar{a} = \{x \in A : x \sim a\} = \{x \in A : (x, a) \in R\}$ is the equivalence class determined by a.

$$\bar{a} = \bar{b} \Leftrightarrow a \sim b\ i.e.(a, b) \in R.$$

Proposition 1.4. *For any $a, b \in A$ either $\bar{a} = \bar{b}$ or $\bar{a} \cap \bar{b} = \emptyset$.*

Definition 1.5. $A/R =$ The set of all equivalence class in A.

Example 1.6. Let $m > 0$ be an integer. Congruence modulo m is an equivalence relation on $\mathbb{Z}$ which has precisely m equivalence classes.

Definition 1.7 (Choice)**.** Let $A_i : i \in I$ be a non-empty family of sets indexed by I. The cartesian product of the sets A_i is the set of all functions

$$f : I \to \bigcup_{i \in I} A_i$$

such that $f(i) \in A_i \ \forall i \in I$. It is denoted by $\prod_{i \in I} A_i$

$$\prod_{i \in I} A_i = \{f : f : I \to \cup A_i \text{ such that } f(i) \in A_i\}.$$

Definition 1.8 (WOA)**.** Every non empty subset of positive integer has a least element.

Definition 1.9 (PMI)**.**

Theorem 1.10 (Division Algorithm)**.** *If $a, b \in \mathbb{Z}$ and $b \neq 0$, then $\exists!$ integers q, r such that*

$$a = qb + r, \qquad 0 \leq r < |b|.$$

Theorem 1.11 (Bezout's Lemma)**.**

2 Groups

2.1 Basic Definitions

Definition 2.1 (Binary operation)**.** Let $G \neq \emptyset$ a binary operation on G is a function from $G \times G \to G$.

Definition 2.2 (Groupoid)**.** A non-empty set G together with a binary operation on G.

Definition 2.3 (Semi-Group)**.** A non-empty set G together with a binary operation on G which is associative.

Definition 2.4 (Monoid)**.** A semi group which contains a two sided identity.

Definition 2.5 (Group)**.** A Monoid G such that for every $a \in G$, there exists a two sided inverse.

Notation 2.6. $|G|$ = order of the group. If $|G| < \infty$, then G is finite otherwise infinite.

Theorem 2.7. *If G is a monoid the identity element e is unique*

Proof. Let e and e' be two identity elements, then

$$e = ee' = e'e = e'$$

□

Theorem 2.8. *If G is a group, then*

i) *$c \in G$ and $cc = c \Rightarrow c = e$.*

ii) $\forall a, b, c$

$$\begin{array}{ll} \text{(Left cancelation)} & ab = ac \Rightarrow b = c \\ \text{(Right cancelation)} & ba = ca \Rightarrow b = c \end{array}$$

iii) *For each $a \in G$ the inverse is unique.*

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

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

vi) *For all $a, b \in G$, the equation $ax = b$, $ya = b$ have a unique solution $x = a^{-1}b$ and $y = ba^{-1}$.*

Proposition 2.9. *Let G be a semigroup. Then G is a group iff*

1. *$\exists e \in G$ such that $ea = a$, $\forall a \in G$.*
2. *For each $a \in G$, there exists $a^{-1} \in G$ such that $a^{-1}a = e$.*

Proof. □

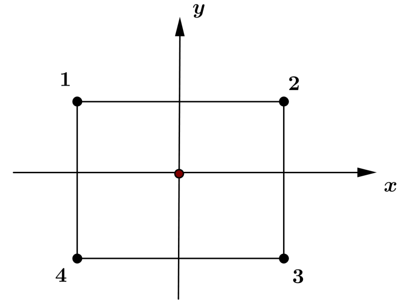
Proposition 2.10. *Let G be a semigroup. Then G is a group iff the equations $ax = b$ and $ya = b$ have solutions in G.*

Proof. □

Example 2.11. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ are groups.
$(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ are monoids.

Example 2.12. Consider a square with vertices consecutively numbered $1, 2, 3, 4$ and centered at the origin of the x, y plane. Let $D_4^* = \{R, R^2, R^3, I, T_x, T_y, T_{1,3}, T_{2,4}\}$ where

R is a counter clockwise rotation about 90°
R^2 is a counter clockwise rotation about 180°
R^3 is a counter clockwise rotation about 270°
I is a counter clockwise rotation about 360°
T_x is a reflection about $x-$axis
T_y is a reflection about $y-$axis
$T_{1,3}$ is a reflection about the line through 1&3
$T_{2,4}$ is a reflection about the line through 2&4



$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \; R = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \; R^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \; R^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$
$$T_x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \; T_y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \; T_{1,3} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \; T_{2,4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

For $v, u \in D_4^*$, $uv = u \circ v$ transformation v followed by u. Claim: D_4^* is a non-abelian group of order 8. The Cayley Table for D_4^* is

$\circ$	I	R	R^2	R^3	T_x	T_y	$T_{1,3}$	$T_{2,4}$
I	I	R	R^2	R^3	T_x	T_y	$T_{1,3}$	$T_{2,4}$
R	R	R^2	R^3	I	$T_{2,4}$	$T_{1,3}$	T_x	T_y
R^2	R^2	R^3	I	R	T_y	T_x	$T_{2,4}$	$T_{1,3}$
R^3	R^3	I	R	R^2	$T_{1,3}$	$T_{2,4}$	T_y	T_x
T_x	T_x	$T_{1,3}$	T_y	$T_{2,4}$	I	R^2	R	R^3
T_y	T_y	$T_{2,4}$	T_y	$T_{1,3}$	R^2	I	R^3	R
$T_{1,3}$	$T_{1,3}$	T_y	$T_{2,4}$	T_x	R^3	R	I	R^2
$T_{2,4}$	$T_{2,4}$	T_x	$T_{1,3}$	T_y	R	R^3	R^2	I

Table 1: $(D_4^*, \circ)$ [uv: u from row and v from column.]

2.2 Homomorphisms

Definition 2.13. Let G and H be semigroups. A function $f : G \to H$ is a homomorphism if

$$f(ab) = f(a)f(b), \qquad \forall a, b \in G.$$

If f is **injective**, then f is a **monomorphism**. If f is **surjective**, then f is an **epimorphism**. If f is **bijective**, then f is an **isomorphism**.

Definition 2.14. G and H are said to be isomorphic if there is an isomorphism between them.

Notation 2.15. If G and H are isomorphic we write $G \cong H$.

Definition 2.16. A homomorphism $f : G \to G$ is called an endomorphism.

Definition 2.17. An isomorphism $f : G \to G$ is called an automorphism.

Lemma 2.18. *If G and H are groups with identities e_G and e_H respectively, then*
i) $f(e_G) = e_H$.
ii) $f(a^{-1}) = [f(a)]^{-1}$

Proof. Exercise □

Example 2.19. Let G be an abelian group. Define $f : G \to G$ by $f(x) = x^2$. Show that f is a homomorphism.

Example 2.20. Define $f : G \to G$ by $f(x) = x^{-1}$. Show that f is an automorphism.

Definition 2.21. Let $f : G \to H$ be a homomorphism of groups, then $\ker f = \{x \in G : \ f(x) = e\}$
$A \subset G,\ f(A) = \{f(x) : x \in A\}$
$B \subset H,\ f^{-1}(B) = \{x \in G : f(x \in B)\}$

Theorem 2.22. *If $f : G \to H$ is a homomorphism of groups, then*

1. *f is a monomorphism iff $\ker f = \{e\}$.*
2. *f is an isomorphism iff $\exists$ a homomorphism $f^{-1} : H \to G$ such that $f \circ f^{-1} = I_H$ and $f^{-1}f = I_G$.*

Proof. (1) Exercise
(2) ($\Rightarrow$) Suppose f is an isomorphism i.e. f is $1-1$, onto, monomorphism. Since f is bijective, there exist f^{-1} which is also bijective.
Claim: f^{-1} is homomorphism. □

2.3 Subgroups

Definition 2.23. Let G be a group and $\emptyset \neq H \subset G$ that is closed under the binary operation of G, then H is said to be a subgroup of G if H by itself is a group.

Notation 2.24. If H is a subgroup of G, we write $H \leq G$.

Example 2.25 (Trivial subgroups)**.** Let G be a group, then $\{e\}$ and G are subgroups of G.

Example 2.26. Consider $(\mathbb{Z}, +)$, then for $k \in \mathbb{Z}$, $(k\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

Example 2.27. Consider $(\mathbb{Z}_6, \oplus_6)$

Proposition 2.28. *If p is prime, then $\mathbb{Z}_p$ has no proper subgroups.*

Theorem 2.29. *Let $f : G \to H$ be a homomorphism of groups, then*

1. *$\ker f \leq G$,*
2. *$A \leq G \Rightarrow f(A) \leq H$, (In particular; $imf \leq H$)*
3. *$B \leq H \Rightarrow f^{-}(B) \leq G$.*

Proof. Exercise □

Example 2.30. Let G be a group $Aut(G) = \{f : G \to G, f \text{ is an isomorphism}\}$. Show $(Aut(G), \circ)$ is a group.

Theorem 2.31. *Let $\emptyset \neq H \subset G$, $H \leq G$ iff $ab^{-1} \in H, \forall a, b \in H$.*

Corollary 2.32. *Let G be a group and $\{H_i : i \in \Delta\}$ be a non-emptyset family of subgroups of G. Then $\bigcap_{i \in \Delta} \leq G$.*

Definition 2.33. Let G be a group and $X \subset G$. Let $\{H_i : i \in \Delta\}$ be a non-emptyset family of subgroups of G containing X(i.e. $X \subset H_i, \forall i \in \Delta$). Then $\bigcap_{i \in \Delta} H_i$ is called the subgroup of G generated by the set X and denoted by $\langle X \rangle$.

Notation 2.34. If $X = \{a_1, a_2, \dots, a_n\}$, then $\langle X \rangle = \langle a_1, a_2, \dots, a_n \rangle$.

Definition 2.35. If $G = \langle a_1, a_2, \dots, a_n \rangle$, then we say that G is finitely generated.

Remark 2.36. $\langle \emptyset \rangle = \{e\}$.

Theorem 2.37. *Let G be a group and $\emptyset \neq X \subset G$. Then $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ where $a_i \in X$ and $n_i \in \mathbb{Z}$.*
In particular, for all $a \in G$, $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

2.4 Cyclic groups

Definition 2.38. A group G is said to be cyclic if $G = \langle a \rangle$ for some $a \in G$.

Proposition 2.39. *The only subgroups of* $(\mathbb{Z}, +)$ *are of the form* $(k\mathbb{Z}, +)$ *for* $k \in \mathbb{Z}$.

Example 2.40. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle \Rightarrow \mathbb{Z}$ is cyclic.

Example 2.41. The group $\{1, -1, i, -i\}$ under multiplication is a cyclic group.

Theorem 2.42. *Every infinite cyclic group is isomorphic to the additive group* $\mathbb{Z}$ *and every finite cyclic group of order* m *is isomorphic to the additive group* $\mathbb{Z}_m$.

Proof. Let G be a cyclic group. Then $G = \langle a \rangle$. Define $\alpha : \mathbb{Z} \to G$ by $\alpha(k) = a^k$. Claim :- α is an epimorphism. i) Homomorphism: $\alpha(k_1 + k_2) = a^{k_1+k_2} = a^{k_1} \cdot a^{k_2} = \alpha(k_1)\alpha(k_2)$ ii) Onto: Let $x \in \langle a \rangle$. Then $x = a^k$ for some $k \in \mathbb{Z} \Rightarrow \alpha(k) = x$.
Hence α is an epimorphism.
Consider $\ker \alpha$

□

2.5 Permutations

Definition 2.43. Let $I_n = \{1, 2, \ldots, n\}$. $S_n = \{\sigma | \sigma : I_n \to I_n \text{ bijective}\}$. The elements of S_n are called **permutations**.

Definition 2.44. Let $i_1, i_2, \ldots, i_r$ $(r \leq n)$ be distinct elements of I_n. Then $(i_1 i_2 \cdots i_r)$ denotes a permutation that maps $i_1 \to i_2, i_2 \to i_3, \cdots, i_{r-1} \to i_r$ and fixes every other element. $(i_1 i_2 \cdots i_r)$ is called a cycle of length r. A cycle of length two is called **transposition**.

Definition 2.45. The permutations $\sigma_1, \sigma_2, \ldots, \sigma_r$ of S_n are said to be **disjoint** for each $1 \leq i \leq r$ and every $k \in I_n$ if

$$\sigma_i(k) \neq k \Rightarrow \sigma_j(k) = k, \text{ for every } j \neq i.$$

Theorem 2.46. *If* τ *and* σ *are disjoint, then* $\tau\sigma = \sigma\tau$.

Proof. First assume $\sigma(i) \neq i$. Then $\tau(i) = i$ by definition because σ and τ are disjoint, and therefore $\sigma(\tau(i)) = \sigma(i)$. On the other hand, because permutations are injective, $\sigma(i) \neq i$ means that $\sigma(\sigma(i)) \neq \sigma(i)$, so $\tau(\sigma(i)) = \sigma(i)$, again because σ and τ are disjoint. Since $\sigma\tau(i)$ and $\tau\sigma(i)$ both equal $\sigma(i)$, they are equal.

Next assume $\sigma(i) = i$. Then it may be that $\tau(i) \neq i$, in which case proceed as in the previous case with τ and σ interchanged.

Finally if $\sigma(i) = i$ and $\tau(i) = i$, then obviously $\sigma\tau(i) = i = \tau\sigma(i)$.

Since there's always one of these cases that holds, and $\sigma\tau(i) = \tau\sigma(i)$ in each of them, it holds always. □

Theorem 2.47. *Every non-identity*

Corollary 2.48. *Every permutation in* S_n

Definition 2.49. A permutation $\tau \in S_n$ is said to be **even**(resp. **odd**) if τ can be written as a product of **even**(resp. **odd**) number of transpositions.

$$\operatorname{sgn}(\tau) = \begin{cases} 1 & \text{if } \tau \text{ is even.} \\ -1 & \text{if } \tau \text{ is odd.} \end{cases}$$

Theorem 2.50. *A permutation in* $S_n (n \geq 2)$ *can not be both even and odd.*

Theorem 2.51. *For each* $n \geq 2$, *let* A_n *be the set of all even permutations of* S_n. *Then*

i) $A_n \lhd S_n$

ii) $[S_n : A_n] = 2$

iii) $|A_n| = |S_n|/2 = n!/2$

Proof. Consider the group $(\{1, -1\}, \cdot)$. Define the map $f : S_n \to \{-1, 1\}$ by $f(\sigma) = \operatorname{sgn}(\sigma)$.

□

2.6 Isomorphism Theorems

Theorem 2.52 (First Isomorphism Theorem). *If $f : G \to H$ is a group homomorphism, then*

$$\ker f \lhd G \qquad \text{and} \qquad G/\ker f \cong im\ f$$

i.e. if $\ker f = K$ and $\phi : G/K \to im\ f \leq H$ is given by $\phi : aK \mapsto f(a)$, then ϕ is an isomorphism.

Remark 2.53. The following diagram describes the proof of the first isomorphism theorem, where $\pi : G \to G/K$ is the natural map $\pi : a \mapsto aK$.

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H \\ & G/H \arrow[ur, "\phi"'] & \end{tikzcd}$$

Proof. □

Theorem 2.54 (Second Isomorphism Theorem). *If N and K are subgroups of a group G with $N \lhd G$, then NK is a subgroup, $N \cap K \lhd K$, and*

$$K/(N \cap K) \cong NK/N.$$

Proof. □

Theorem 2.55 (Third Isomorphism Theorem). *If H and K are normal subgroups of a group G with $K \leq H$, then $H/K \lhd G/K$ and*

$$(G/K)/(H/K) \cong G/H.$$

Proof. □

2.7 Sylow Theorems

Theorem 2.56 (Cauchy). *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Definition 2.57 (p-group). A group in which every element has order a power (≥ 0) of some fixed prime p is called a p-group. If H is a subgroup of a group G and H is a p-group, H is said to be a p-subgroup of G. In particular $\langle e \rangle$ is a p-subgroup of G for every prime p since $|\langle e \rangle| = 1 = p^0$.

Definition 2.58 (Sylow p-subgroup). A subgroup P of a group G is said to be a sylow p-subgroup of G if P is a maximal p subgroup of G. i.e. $P \leq H \leq G$ with H a p-subgroup of G, then $P = H$.

Corollary 2.59. *A finite group G is a p-group if and only if $|G|$ is a power of p.*

Theorem 2.60 (First Sylow Theorem). *Let G be a group of order $p^n m$, with $n > 1$, p prime, and $(p, n) = 1$. Then G contains a subgroup of order p^i for each $1 < i < n$ and every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}.*

Corollary 2.61. *Let G be a group of order $p^n m$ with p prime, $n \geq 1$ and $(m, p) = 1$. Let H be a p-subgroup of G.*
(i) H is a Sylow p-subgroup of G if and only if $|H| = p^n$.
(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.
(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Theorem 2.62 (Second Sylow Theorem). *If H is a p-subgroup of a finite group G, and P is any Sylow p-subgroup of G, then there exists $x \in G$ such that $H \leq xPx^{-1}$ In particular, any two Sylow p-subgroups of G are conjugate.*

Theorem 2.63 (Third Sylow Theorem). *If G is a finite group and p a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.*

2.8 Classification of Finite Groups

We shall classify up to isomorphism all groups of order pq (p,q primes) and all groups of small order $n \leq 23$.

Order	Distinct Groups
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$, $\mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, D_3
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$, $\mathbb{Z}_2 \bigoplus \mathbb{Z}_4$, $\mathbb{Z}_8$, Q_8, D_4
9	$\mathbb{Z}_3 \bigoplus \mathbb{Z}_3$, $\mathbb{Z}_9$
10	$\mathbb{Z}_{10}$, D_5
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_6$, $\mathbb{Z}_{12}$, A_4, D_6, T
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$, D_7
15	$\mathbb{Z}_{15}$
16	$\mathbb{Z}_{16}$,
17	$\mathbb{Z}_{17}$,
18	$\mathbb{Z}_{18}$,
19	$\mathbb{Z}_{19}$,
20	$\mathbb{Z}_{20}$,
21	$\mathbb{Z}_{21}$,
22	$\mathbb{Z}_{22}$,
23	$\mathbb{Z}_{23}$,

3 Rings

3.1 Definition and elementary properties

Definition 3.1.

Example 3.2.

Definition 3.3.

Notation 3.4.