

# Algebra

D. Zack Garza

August 17, 2019

## Contents

<b>1</b>	<b>Major Theorems</b>	<b>1</b>
<b>2</b>	<b>Lecture 1 (Thu 15 Aug 2019)</b>	<b>1</b>
2.1	Definitions . . . . .	2
2.2	Preliminaries . . . . .	3
2.3	Cyclic Groups . . . . .	3
2.4	Homomorphisms . . . . .	4
2.5	Direct Products . . . . .	4
2.6	Finitely Generated Abelian Groups . . . . .	5
2.7	Fundamental Homomorphism Theorem . . . . .	5
2.7.1	The First Homomorphism Theorem . . . . .	5
2.7.2	The Second Theorem . . . . .	5
<b>3</b>	<b>Lecture 2</b>	<b>6</b>

---

## 1 Major Theorems

**Theorem 1** (Cauchy). For any prime  $p$  dividing the order of  $G$ , there is an element  $x$  of order  $p$  (and thus a subgroup  $H = \langle x \rangle$ ).

**Theorem 2** (Lagrange). If  $H \leq G$  is a subgroup, then  $|H| \mid |G|$ .

**Theorem 3** (Sylow 1). If  $|G| = n = \prod p_i^{a_i}$  as a prime factorization, then  $G$  has subgroups of order  $p_i^{a_i}$  for every  $i$ . Moreover, this holds for any  $1 \leq r \leq a_i$ .

theorem

## 2 Lecture 1 (Thu 15 Aug 2019)

We'll be using Hungerford's Algebra text.

## 2.1 Definitions

The following definitions will be useful to know by heart:

- The order of a group
- Cartesian product
- Relations
- Equivalence relation
- Partition
- Binary operation
- Group
- Isomorphism
- Abelian group
- Cyclic group
- Subgroup
- Greatest common divisor
- Least common multiple
- Permutation
- Transposition
- Orbit
- Cycle
- The symmetric group  $S^n$
- The alternating group  $A_n$
- Even and odd permutations
- Cosets
- Index
- The direct product of groups
- Homomorphism
- Image of a function
- Inverse image of a function
- Kernel
- Normal subgroup
- Factor group
- Simple group

Here is a rough outline of the course:

- Group Theory
  - Groups acting on sets
  - Sylow theorems and applications
  - Classification
  - Free and free abelian groups
  - Solvable and simple groups
  - Normal series
- Galois Theory
  - Field extensions
  - Splitting fields
  - Separability
  - Finite fields

- Cyclotomic extensions
- Galois groups
- Solvability by radicals
- Module theory
  - Free modules
  - Homomorphisms
  - Projective and injective modules
  - Finitely generated modules over a PID
- Linear Algebra
  - Matrices and linear transformations
  - Rank and determinants
  - Canonical forms
  - Characteristic polynomials
  - Eigenvalues and eigenvectors

## 2.2 Preliminaries

**Definition 1.** A **group** is an ordered pair  $(G, \cdot : G \times G \rightarrow G)$  where  $G$  is a set and  $\cdot$  is a binary operation, which satisfies the following axioms:

- Associativity:  $(g_1 g_2) g_3 = g_1 (g_2 g_3)$ ,
- Identity:  $\exists e \in G \ni ge = eg = g$ ,
- Inverses:  $g \in G \implies \exists h \in G \ni gh = gh = e$ .

**Example 1.**

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{Q}^\times, \times)$
- $(\mathbb{R}^\times, \times)$
- $(\text{GL}(n, \mathbb{R}), \times) = \{A \in \text{Mat}_n \ni \det(A) \neq 0\}$
- $(S_n, \circ)$

**Definition 2.** A subset  $S \subseteq G$  is a **subgroup** of  $G$  iff

1.  $s_1, s_2 \in S \implies s_1 s_2 \in S$
2.  $e \in S$
3.  $s \in S \implies s^{-1} \in S$

We denote such a subgroup  $S \leq G$ .

Examples of subgroups:

- $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$
- $\text{SL}(n, \mathbb{R}) \leq \text{GL}(n, \mathbb{R})$ , where  $\text{SL}(n, \mathbb{R}) = \{A \in \text{GL}(n, \mathbb{R}) \ni \det(A) = 1\}$

## 2.3 Cyclic Groups

**Definition 3.** A group  $G$  is **cyclic** iff  $G$  is generated by a single element.

**Exercise 1.** Show  $\langle g \rangle = \{g^n \ni n \in \mathbb{Z}\} \cong \bigcap \{H \leq G \ni g \in H\}$ .

**Theorem 4.** Let  $G$  be a cyclic group, so  $G \langle g \rangle$ .

- If  $|G| = \infty$ , then  $G \cong \mathbb{Z}$ .
- If  $|G| = n < \infty$ , then  $G \cong \mathbb{Z}_n$ .

**Definition 4.** Let  $H \leq G$ , and define a **right coset** of  $G$  by  $aH = \{ah \mid H \in H\}$ . A similar definition can be made for **left cosets**.

Then  $aH = bH \iff b^{-1}a \in H$  and  $Ha = Hb \iff ab^{-1} \in H$ .

Some facts:

- Cosets partition  $H$ , i.e.  $b \notin H \implies aH \cap bH = \{e\}$ .
- $|H| = |aH| = |Ha|$  for all  $a \in G$ .

**Theorem 5** (Lagrange). If  $G$  is a finite group and  $H \leq G$ , then  $|H| \mid |G|$ .

**Definition 5.** A subgroup  $N \leq G$  is **normal** iff  $gN = Ng$  for all  $g \in G$ , or equivalently  $gNg^{-1} \subseteq N$ . I denote this  $N \trianglelefteq G$ .

When  $N \trianglelefteq G$ , the set of left/right cosets of  $N$  themselves have a group structure. So we define

$$G/N = \{gN \mid g \in G\} \text{ where } (g_1N)(g_2N) = (g_1g_2)N.$$

Given  $H, K \leq G$ , define  $HK = \{hk \mid h \in H, k \in K\}$ . We have a general formula,

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

## 2.4 Homomorphisms

**Definition 6.** Let  $G, G'$  be groups, then  $\varphi : G \rightarrow G'$  is a **homomorphism** if  $\varphi(ab) = \varphi(a)\varphi(b)$ .

**Example 2.** •  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^{>0}, \cdot)$  where  $\exp(a+b) = e^{a+b} = e^a e^b = \exp(a) \exp(b)$ .

- $\det : (\text{GL}(n, \mathbb{R}), \times) \rightarrow (\mathbb{R}^\times, \times)$  where  $\det(AB) = \det(A) \det(B)$ .
- Let  $N \trianglelefteq G$  and  $\varphi G \rightarrow G/N$  given by  $\varphi(g) = gN$ .
- Let  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$  where  $\varphi(g) = [g] = g \bmod n$  where  $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

**Definition 7.** Let  $\varphi : G \rightarrow G'$ . Then  $\varphi$  is a **monomorphism** iff it is injective, an **epimorphism** iff it is surjective, and an **isomorphism** iff it is bijective.

## 2.5 Direct Products

Let  $G_1, G_2$  be groups, then define

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\} \text{ where } (g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2).$$

We have the formula  $|G_1 \times G_2| = |G_1||G_2|$ .

## 2.6 Finitely Generated Abelian Groups

**Definition 8.** We say a group is **abelian** if  $G$  is commutative, i.e.  $g_1, g_2 \in G \implies g_1 g_2 = g_2 g_1$ .

**Definition 9.** A group is **finitely generated** if there exist  $\{g_1, g_2, \dots, g_n\} \subseteq G$  such that  $G = \langle g_1, g_2, \dots, g_n \rangle$ .

This generalizes the notion of a cyclic group, where we can simply intersect all of the subgroups that contain the  $g_i$  to define it.

We know what cyclic groups look like – they are all isomorphic to  $\mathbb{Z}$  or  $\mathbb{Z}_n$ . So now we'd like a structure theorem for abelian finitely generated groups.

**Theorem 6.** Let  $G$  be a finitely generated abelian group. Then

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^s \mathbb{Z}_{p_i}^{\alpha_i}$$

for some finite  $r, s \in \mathbb{N}$  and  $p_i$  are (not necessarily distinct) primes.

**Example 3.** Let  $G$  be a finite abelian group of order 4. Then  $G \cong \mathbb{Z}_4$  or  $\mathbb{Z}_2^2$ , which are not isomorphic because every element in  $\mathbb{Z}_2^2$  has order 2 where  $\mathbb{Z}_4$  contains an element of order 4.

## 2.7 Fundamental Homomorphism Theorem

Let  $\varphi : G \rightarrow G'$  be a group homomorphism and define  $\ker \varphi = \{g \in G \mid \varphi(g) = e'\}$ .

### 2.7.1 The First Homomorphism Theorem

**Theorem 7.** There exists a map  $\varphi' : G/\ker \varphi \rightarrow G'$  such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \eta \downarrow & \nearrow \varphi' & \\ G/\ker \varphi & & \end{array}$$

That is,  $\varphi = \varphi' \circ \eta$ , and  $\varphi'$  is an isomorphism onto its image, so  $G/\ker \varphi = \text{im } \varphi$ . This map is given by  $\varphi'(g(\ker \varphi)) = \varphi(g)$ .

**Exercise 2.** Check that  $\varphi$  is well-defined.

### 2.7.2 The Second Theorem

**Theorem 8.** Let  $K, N \leq G$  where  $N \trianglelefteq G$ . Then

$$\frac{K}{N \cap K} \cong \frac{NK}{N}$$

*Proof.* Define a map  $K \xrightarrow{\varphi} NK/N$  by  $\varphi(k) = kN$ . You can show that  $\varphi$  is onto by looking at  $\ker \varphi$ ; note that  $kN = \varphi(k) = N \iff k \in N$ , and so  $\ker \varphi = N \cap K$ .  $\square$

### 3 Lecture 2