

# Algebra

D. Zack Garza

August 15, 2019

## Contents

<b>1 Lecture 1 (Thu 15 Aug 2019)</b>	<b>1</b>
1.1 Cyclic Groups . . . . .	2
1.2 Homomorphisms . . . . .	2
1.3 Direct Products . . . . .	2
1.4 Finitely Generated Abelian Groups . . . . .	3

---

## 1 Lecture 1 (Thu 15 Aug 2019)

Definition: 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:

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

Some examples of groups:

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

Definition: 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:

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

## 1.1 Cyclic Groups

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

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

Theorem: Let  $G$  be a cyclic group, so  $G = \langle g \rangle$ .

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

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

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

Definition:  $N \leq G$  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  $G/N = \{gN \mid g \in G\}$  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,

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

## 1.2 Homomorphisms

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

Examples:

- $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^{>0}, \cdot)$  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  $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ .

Definitions: 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.

## 1.3 Direct Products

Let  $G_1, G_2$  be groups, then define  $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$  where  $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$ .

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

## 1.4 Finitely Generated Abelian Groups

We say a group is *abelian* if  $G$  is commutative, i.e.  $g_1, g_2 \in G \implies g_1g_2 = g_2g_1$ .

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 f.g. groups.

Theorem: Let  $G$  be a f.g. 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.

Examples:

- 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.