

## 1. PRELIMINARIES

1.1. **basic structures.** First, I defined semigroups, monoids and groups.

**Definition 1.1.** A semigroup is a set  $S$  with an associative binary operation:

$$* : S \times S \rightarrow S$$

written  $(a, b) \mapsto ab$  so that  $a(bc) = (ab)c$  for all  $a, b, c \in S$ . A monoid is a semigroup  $M$  with a (two-sided) identity (or neutral element). This is defined to be an element  $e \in M$  so that

$$xe = ex = x$$

for all  $x \in M$ . A group is a monoid  $G$  with inverses. This means  $\forall x \in G, \exists y \in G$  s.t.

$$xy = yx = e.$$

$y = x^{-1}$  is called the inverse of  $x$ .

I gave examples similar to the following.

- (1) The set of positive integers is a semigroup under addition.
- (2)  $(\mathbb{Z}, \cdot)$  is a monoid.
- (3)  $(2\mathbb{Z}, +)$  is a group.

**Definition 1.2.** A homomorphism between two groups is a mapping  $\phi : G \rightarrow H$  so that

$$\phi(ab) = \phi(a)\phi(b).$$

**Theorem 1.3.** Any homomorphism of groups also takes identity to identity and inverse to inverse:

$$\begin{aligned}\phi(e_G) &= e_H \\ \phi(x^{-1}) &= \phi(x)^{-1}\end{aligned}$$

**Definition 1.4.** A subset  $H$  of a group  $G$  is called a subgroup if the following conditions hold:

- (1)  $H \neq \emptyset$  ( $H$  is nonempty.)
- (2)  $HH \subseteq H$  ( $H$  is closed under multiplication.)
- (3)  $H^{-1} \subseteq H$  ( $H$  is closed under inverse.)

The notation for subgroup is  $H \leq G$ .

Here I am using the notation:

$$AB = \{ab \mid a \in A, b \in B\}$$

Conditions (2) and (3) can be combined into one condition:

$$HH^{-1} = H.$$

**Theorem 1.5.** *The image  $\phi(G)$  of a homomorphism  $\phi : G \rightarrow H$  is a subgroup of  $H$ .*

*Proof.*  $K = \phi(G)$  is nonempty since it contains  $\phi(e_G) = e_H$ . It also satisfies the condition  $KK^{-1} = K$  since

$$\phi(G) = \phi(GG^{-1}) = \phi(G)\phi(G^{-1}) = \phi(G)\phi(G)^{-1}$$

by Theorem 1.3. □

The *left cosets* of  $H$  in  $G$  are the sets

$$aH = \{ah \mid h \in H\}$$

The set of left cosets is written  $G/H$ . For example,

$$\mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 2\mathbb{Z} + 1\}.$$

**Definition 1.6.** *A subgroup  $N \leq G$  is normal and we write  $N \trianglelefteq G$  if*

$$xNx^{-1} = N$$

*for all  $x \in G$ .*

**Theorem 1.7.** *A subgroup  $N \leq G$  is normal if and only if  $G/N$  is a group under the operation*

$$(aN)(bN) = abN.$$

**Definition 1.8.** *The kernel  $\ker \phi$  of a homomorphism  $\phi : G \rightarrow H$  is the set of all elements of  $G$  which go to the identity of  $H$ .*

**Theorem 1.9.**  $\ker \phi \trianglelefteq G$ . *Furthermore any normal subgroup  $N \trianglelefteq G$  is the kernel of some homomorphism  $G \rightarrow H$ .*

The homomorphism is just the quotient map  $q : G \rightarrow G/N$  given by  $q(a) = aN$ .

The rest of the discussion was focused on commutators and abelian quotient groups.

**1.2. commutators.** A group  $G$  is called *abelian* if  $ab = ba$  for all  $a, b \in G$ . This is the same as saying that the *commutator*

$$[a, b] := aba^{-1}b^{-1}$$

is trivial (equal to  $e$ ).

To define the commutator subgroup, I needed to recall the definition of a subgroup generated by a subset.

**Definition 1.10.** If  $S$  is a subset of a group  $G$  then the subgroup generated by  $S$ , written  $\langle S \rangle$ , is defined to be the intersection of all subgroups of  $G$  which contain  $S$ :

$$\langle S \rangle := \bigcap_{S \subseteq H \leq G} H.$$

**Definition 1.11.** The commutator subgroup (also called the derived subgroup)  $G' = [G, G]$  is the subgroup of  $G$  generated by all commutators  $[a, b]$ .

In general, if  $A, B \leq G$  then  $[A, B]$  is defined to be the subgroup of  $G$  generated by all commutators  $[a, b]$  where  $a \in A$  and  $b \in B$ .

**Theorem 1.12.**  $G' = [G, G]$  is a normal subgroup of  $G$ .

This follows immediately from the following two facts.

**Lemma 1.13.** (1)  $x \langle S \rangle x^{-1} = \langle S \rangle$   
 (2)  $x[a, b]x^{-1} = [xax^{-1}, xbx^{-1}]$ .

This lemma has a generalization:

**Lemma 1.14.** Given a homomorphism  $\phi : G \rightarrow H$ ,  $a, b \in G$ ,  $S \subseteq G$  we have:

- (1)  $\phi \langle S \rangle = \langle \phi(S) \rangle$ .
- (2)  $\phi[a, b] = [\phi(a), \phi(b)]$ .

Why is this a generalization of the previous lemma?

The main theorem about the commutator subgroup is the following.

**Theorem 1.15.** The image  $\phi(G)$  of a homomorphism  $\phi : G \rightarrow H$  is abelian if and only if the kernel of  $\phi$  contains the commutator subgroup

For this we need the following lemma whose proof is obvious.

**Lemma 1.16.**  $S$  is a subset of  $H \leq G$  iff  $\langle S \rangle$  is a subgroup of  $H$ .

*Proof of Theorem 1.15.* The argument which we did in class is reversible, i.e., “iff” at every step: For any  $a, b \in G$  we have

$$[\phi(a), \phi(b)] = \phi[a, b].$$

$\phi(G)$  is abelian iff the LHS is always  $e$ . But, the RHS is always equal to  $e$  iff  $[a, b] \in \ker \phi$  for all  $a, b \in G$  which, by Lemma 1.16, is equivalent to saying that  $G' \leq \ker \phi$ .  $\square$

The theorem has the following variation as an obvious corollary:

**Corollary 1.17.** Suppose that  $N \trianglelefteq G$ . Then  $G/N$  is abelian iff  $G' \leq N$ .