Math 425: Abstract Algebra I
Theorems from the Textbook - Sections 2.5-2.10

Theorems

Theorem 2.5.1. *Let* $\phi\colon G \to H$ *be a group homomorphism. Then*

(a) $\phi(e_G) = e_H$ *(ϕ preserves identities)*

(b) $\phi(g^{-1}) = \phi(g)^{-1}\ \forall g \in G$ *(ϕ preserves inverses)*

(c) $\phi(g^k) = \phi(g)^k\ \forall g \in G, k \in \mathbb{Z}$ *(ϕ preserves powers)*

Corollary 1. *Let* $\phi\colon G \to H$ *be a homomorphism. If* $g \in G$ *has* $|g| = n < \infty$, *then* $|\phi(g)| < \infty$. *Moreover* $|\phi(g)|$ *divides* $|g|$.

Corollary 2. *If* $\alpha\colon G \to H$ *is a homomorphism, write* $\alpha(G) = \{\alpha(g) \mid g \in G\}$. *Then* $\alpha(G)$ *is a subgroup of* H.

Theorem 2.5.3. *Let* G, H, *and* K *denote groups.*

1. *The identity map* $1_G\colon G \to G$ *is an isomorphism for every group* G.

2. *If* $\sigma\colon G \to H$ *is an isomorphism then the inverse mapping* $\sigma^{-1}\colon H \to G$ *is an isomorphism.*

3. *If* $\sigma\colon G \to H$ *and* $\tau\colon H \to K$ *are isomorphisms then* $\tau\sigma\colon G \to K$ *is an isomorphism.*

Corollary 1. *This isomorphism relation,* $\cong$ *is an equivalence relation on groups. That is*

1. $G \cong G$,

2. *if* $G \cong H$, *then* $H \cong G$, *and*

3. *if* $G \cong H$ *and* $H \cong K$, *then* $G \cong K$.

Corollary 2. *If* G *is a group, then the set of all isomorphisms* $G \to G$ *forms a group under composition.*

Theorem 2.5.4. *Let* $\sigma\colon G \to G_1$ *be an isomorphism. Then* $o(\sigma(g)) = o(g)$ *for all* $g \in G$.

Theorem 2.5.5. *Every group* G *of order* n *is isomorphic to a subgroup of* S_n.

Theorem 2.6.1. *Let* H *be a subgroup of a group* G *and let* $a, b \in G$.

1. $H = He_G$.

2. $Ha = H$ *if and only if* $a \in H$.

3. $Ha = Hb$ *if and only if* $ab^{-1} \in H$.

4. *If $a \in Hb$, then $Ha = Hb$.*

5. *Either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.*

6. *The distinct right cosets of H partition G.*

Corollary 1. *Corresponding statements hold for left cosets. In particular, part (3) becomes*

$$aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow b^{-1}a \in H.$$

Lemma. *If $H \leq G$ and $a, b \in G$, then $|Ha| = |Hb|$.*

Theorem 2.6.2 (Lagrange's Theorem)**.** *Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$.*

Corollary 1. *If G is a finite group and $g \in G$, then $|g|$ divides $|G|$.*

Corollary 2. *If G is a group and $|G| = n$, then $g^n = e$ for all $g \in G$.*

Corollary 3. *If p is a prime, then every group of order p is cyclic. In fact, $G = \langle g \rangle$ for every non-identity element g in G, so the only subgroups of G are $\{e\}$ and G itself.*

Corollary 4. *Let H and K be finite subgroups of a group G. If $|H|$ and $|K|$ are relatively prime, then $H \cap K = \{e\}$.*

Corollary 5. *If H is a subgroup of a finite group G, then*

$$|G : H| = \frac{|G|}{|H|}.$$

Theorem 2.6.3. *Let G be a group of order $2p$, where p is prime. Then either G is cyclic or $G \cong D_p$, where D_p is the dihedral group of order $2p$.*

Theorem 2.8.1. *If G is a group, every subgroup of the center, $Z(G)$ is normal in G. In particular, $Z(G) \trianglelefteq G$.*

Theorem 2.8.2. *If G is abelian and $H \leq G$, then $H \trianglelefteq G$.*

Corollary 1. *If $G = \langle X \rangle$, a subgroup H is normal in G if and only if $xHx^{-1} \subseteq H$ for all $x \in X$. Similarly, if $a \in G$, then $\langle a \rangle \trianglelefteq G$ if and only if $gag^{-1} \in \langle a \rangle$ for all $g \in G$.*

Corollary 2. *If H is a subgroup of G, and if G has no other subgroups isomorphic to H, then H is normal in G.*

Theorem 2.8.3 (Normality Test)**.** *The following conditions are equivalent for a subgroup H of a group G.*

1. *$H \trianglelefteq G$.*

2. *$gHg^{-1} \subseteq H$ for all $g \in G$.*

3. *$gHg^{-1} = H$ for all $g \in G$.*

Theorem 2.8.4. *If $H \leq G$ with $|G : H| = 2$, then $H \trianglelefteq G$.*

Theorem 2.8.5. *Let H and K be subgroups of a group G.*

1. *If H or K is normal in G, then $HK = KH$ is a subgroup of G.*
2. *If both H and K are normal in G, then $HK \trianglelefteq G$ too.*

Theorem 2.8.6. *If $H \trianglelefteq G$ and $K \trianglelefteq G$ satisfy $H \cap K = \{e_G\}$, then $HK \cong H \times K$.*

Corollary 1. *If G is a finite group and $H, K \leq G$ with $H \cap K = \{e_G\}$, then $|HK| = |H||K|$.*

Corollary 2. *If G is a finite group and $H, K \trianglelefteq G$ with $H \cap K = \{e_G\}$ and $|HK| = |G|$, then $G \cong H \times K$.*

Corollary 3. *If m and n are relatively prime integers and G is a cyclic group of order mn, then $G \cong C_m \times C_n$.*

Corollary 4. *Let G be an abelian group of order p^2 for some prime p. Then either $G \cong C_{p^2}$ or $G \cong C_p \times C_p$.*

Theorem 2.8.7. *An abelian group $G \neq \{e_G\}$ is simple if and only if $|G|$ is prime.*

Theorem 2.8.8. *If $n \geq 5$, then A_n is simple.*

Theorem 2.9.1. *Let $K \trianglelefteq G$ and write $G/K = \{Ka \mid a \in G\}$, the set of right cosets of K. Then*

1. *G/K is a group under the operation $(Ka)(Kb) = Kab$.*
2. *The mapping $\varphi : G \to G/K$ defined by $\varphi(a) = Ka$ is an onto homorphism.*
3. *If G is abelian, then G/K is abelian.*
4. *If $G = \langle a \rangle$, then G/K is also cyclic with $G/K = \langle Ka \rangle$.*
5. *If $|G : K|$ is finite then $|G/K| = |G : K|$. If $|G|$ is finite, then $|G/K| = \frac{|G|}{|K|}$.*

Theorem 2.9.2. *If G is a group and $G/Z(G)$ is cyclic, then G is abelian.*

Theorem 2.9.3. *Let G be a group and let H be a subgroup of G.*

1. *G' is a normal subgroup of G and G/G' is abelian.*
2. *$G' \subseteq H$ if and only if H is normal in G and G/H is abelian.*

Theorem 2.10.1. *Let $\alpha \colon G \to H$ be a group homomorphism. Then*

1. *$\alpha(G)$ is a subgroup of H.*
2. *$\ker(\phi)$ is a normal subgroup of G*

Theorem 2.10.2. *If $K \trianglelefteq G$, then $K = \ker\phi$ where $\phi \colon G \to G/K$ is the coset mapping.*

Theorem 2.10.3. *Let $\alpha \colon G \to H$ be a group homomorphism. Then α is injective if and only if $\ker(\alpha) = \{e_G\}$.*

Theorem 2.10.4 (The First Isomorphism Theorem)**.** *Let $\alpha \colon G \to H$ be a group homomorphism and $K = \ker\alpha$ then $G/K \cong im(G) = \alpha(G)$.*

Theorem 2.10.5. *If G is any group then $G/Z(G) \cong \mathrm{Inn}(G)$, where $\mathrm{Inn}(G)$ is the set if inner automorphisms of G.*

Definitions

Definition. Let $(G, *)$ and $(H, \diamond)$ be groups. Then a mapping $\phi\colon G \to H$ is a *[group] homomorphism* if $\phi(g_1 * g_2) = \phi(g_1) \diamond \phi(g_2)$ for all $g_1, g_2 \in G$.

Definition. The *trivial homomorphism*,

$$\phi\colon G \to H, \quad \phi(g) = e_H \ \forall g \in G$$

Definition. A homomorphism that is both injective and surjective is called an *isomorphism*. If an isomorphism exists from G to H, we call G and H *isomorphic* and we write $G \cong H$.

Definition. Let $\phi : G \to H$ be a group homomorphism. The *image of* ϕ is denoted $\phi(G)$ or $\mathrm{im}(\phi)$ and is defined to be the set

$$\{\phi(g) \in H \mid g \in G\} = \{h \in H \mid \exists g \in G \text{ s.t. } \phi(g) = h\}.$$

Definition. Let $\phi : G \to H$ be a group homomorphism. The *kernel of* ϕ is denoted $\ker(\phi)$ and is defined to be the set

$$\{g \in G \mid \phi(g) = e_H\}.$$

Definition. Let G be a group. An *automorphism of* G is an isomorphism from G to itself. The set $\mathrm{Aut}(G)$ is the set of all automorphisms of G.

Definition. Let $H \leq G$ and let $a \in G$. Define the two sets

1. $H * a = \{h * a | h \in H\}$ called the *right coset of H by a.*

2. $a * H = \{a * h | h \in H\}$ called the *left coset of H by a.*

Definition. The *index* of H in G, denoted $|G : H|$, is defined to the number of distinct right (or left if you prefer) cosets of H in G.

Definition. A *regular n-gon* is an n-sided polygon whose sides are all congruent. Denote this figure by P_n.

Definition. A *symmetry* of P_n is any action on P_n by a sequence of flips and/or rotation which return P_n to its original position in the plane.

Definition. The *dihedral group* D_n is the group of symmetries of the figure P_n. (Operation is composition.)

Alternately, we may use the following definition.

Let $n \geq 2$. The *dihedral group* D_n is the group of order $2n$ presented as follows:

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, f, fr, fr^2, \ldots, fr^{n-1}\},$$

where $|r| = n$, $|f| = 2$, and $rf = fr^{-1}$.

Definition. A subgroup H of G is called a *normal subgroup* of G if $gH = Hg$ for all $g \in G$. If H is a normal subgroup of G, we might say H *is normal in* G and write $H \trianglelefteq G$.

Definition. If H is a subgroup of G and $g \in G$, we call gHg^{-1} a *conjugate* of H in G.

Definition. A group G is *simple* if its only normal subgroups are $\{e_G\}$ and G.

Definition. If K is a normal subgroup of the group G, then the group G/K is called the *factor group*, or *quotient group*, of G by K.

We call the homomorphism $\varphi : G \to G/K$ with $\varphi(a) = Ka$ the *coset map.*

Definition. For $a, b \in G$ we define the *commutator* of a and b to be

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

Definition. The *commutator subgroup* of G is the group

$$\begin{aligned} G' &= \{\text{all finite products of commutators from } G\} \\ &= \langle [a, b] \mid a, b \in G \rangle. \end{aligned}$$