Part III

Homomorphism and Factor Groups

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

January 22

13 Homomorphisms

In this section the author defines group homomorphisms. I already defined homomorphisms of groups, but did not work with them.

In general, "morphism" refers to maps $f : X \longrightarrow Y$ of objects with certain structures that **respects the structure**. We already defined the homomorhisms of binary structures. In set theory, morphisms $f : X \longrightarrow Y$ are just the set-maps. In topology, morphisms $f : X \longrightarrow Y$ are called the continuous functions. In algebra morphisms are called "homomorphisms". In this textbook, homomorhisms of binary structures were already defined. You also know about "linear homomorphisms" in the category of vectors spaces.

In this section G, G' will denote two groups. We use multiplication notations. The identity of G, G' will be denoted by e, e', respectively.

Definition 13.1. We have the following definitions:

1. (*Recall*) a map $\varphi : G \longrightarrow G'$ of groups G, G', is called a homomorphism, if
$$\forall\ a, b \in G \qquad\qquad \varphi(ab) = \varphi(a)\varphi(b).$$

2. Let $\varphi : G \longrightarrow G'$ be a homomorphism of groups. Then, **image of φ** is defined by $\varphi(G) = \{\varphi(g) : g \in G\}$.
3. Let $\varphi : G \longrightarrow G'$ be a homomorphism of groups. Then, the **kernel of φ** is defined as $\ker(\varphi) = \varphi^{-1}(\{e'\}) = \{g \in G : \varphi(g) = e'\}$.

Theorem 13.2. Let $\varphi : G \longrightarrow G'$ be homomorphism of groups.

1. Then, the image $\varphi(G)$ is a subgroup of G'.
2. And, the kernel $\ker(\varphi)$ is a subgroup of G.

Proof. Exercise.

The Trivial Homomorphisms:

1. Let G, G' be groups. Define

$$\varphi : G \longrightarrow G' \qquad by \qquad \varphi(a) = e' \quad \forall a \in G.$$

   Proof. Clearly, $\varphi(ab) = e' = e'e' = \varphi(a)\varphi(b)$. The proof is complete. ■

2. Then identity map $I : G \longrightarrow G$ given by $I(a) = a$ $\forall a \in G$ is a homomorphism.

Reading Assignment: Read Examples 13.3-13.10. This is very important. I will run through them.

Example 13.3 (13.3)**.** Let $\varphi : S_n \longrightarrow \mathbb{Z}_2$ be define as

$$\varphi(\sigma) = \begin{cases} 0 & if\ \sigma\ is\ even \\ 1 & if\ \sigma\ is\ odd \end{cases}$$

1. Note, φ is surjective.
2. The kernel $\ker(\varphi) = A_n$.

Example 13.4 (13.4)**.** Let $\mathcal{F} = C([0,1])$ be the additive group of all continuous real valued functions and $c \in [0,1]$ be fixed point. Let

$$\varphi : \mathcal{F} \longrightarrow \mathbb{R} \quad \text{be defined by} \quad \varphi(f) = f(c)$$

(*to be called the* **evaluation map**, *at* c). That means, $\varphi(f) = f(c)$ for $f \in F$. Then φ is a homomorphism.

Example 13.5 (13.5)**.** Let A be an $n \times n$ matrix. Then the map $\mathbb{R}^n \longrightarrow \mathbb{R}^n$ given by $\varphi(\mathbf{x}) = A\mathbf{x}$ is a homomorphism from the additive group $\mathbb{R}^n$ to itself.

Remark. Note, a vector space V is a group under addition.

Example 13.6 (13.6)**.** Let $GL_n(\mathbb{R})$ be the multiplicative group of invertible matrices of order n with coefficients in $\mathbb{R}$. Then the determinant map
$\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ is a homomorphism.

1. This map is onto.
2. The kernel of the determinant homomorphisn is $SL_n(\mathbb{R})$, the matrices of determinat 1.
3. This is the only example, in this list, with non-commutative groups, other than the symmetric group S_n (13.3).

Exercise 13.7 (13.7)**.** Describe all the homomorphisms $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$.

Example 13.8. Projection π_i to the $i^{th}-$coordinate of the direct product of groups is a homomorphism.

$$\pi_i : G_1 \times G_2 \times \cdots \times G_n \longrightarrow G_i \qquad\qquad (g_1, g_2, \ldots, g_n) \mapsto g_i.$$

Example 13.9 (13.9)**.** Let $F = C([0,1])$ be the additive group of all continuous real valued functions. The integration function

$$\Delta : C([0,1]) \longrightarrow \mathbb{R} \quad \textit{given by} \quad f \mapsto \int_0^1 f(x)dx$$

is a homomorphism of groups.

Question. What is the kernel of this homomorphism?

Question. Could we formulate a similar example of a group homomorphim using derivative $f \mapsto \frac{df}{dx}$?

Example 13.10 (13.10 Reduction Modulo n)**.** Let

$$\gamma : \mathbb{Z} \longrightarrow \mathbb{Z}_n \quad be\ defined\ by \quad \gamma(r) = \overline{r}.$$

Then, γ is a homomorphism.

Question. What is the kernel of this homomorphism?

13.1 Properties of Homomorphisms

Theorem 13.11. Let $f : G \longrightarrow G'$ be a homomorphism of groups. (As above, e, e' will denote the identity of G and G' respectively.) Then,

1. $f(e) = e'$.
2. $\forall a \in G$, we have $f(a^{-1}) = f(a)^{-1}$.
3. If H is a subgroup of G then $f(H)$ is a subgroup of G'.
4. The kernel $\ker(f)$ is a subgroup of G.
5. If K is a subgroup of G' then $f^{-1}(K)$ is a subgroup of G.

Proof. The proof is routine.

1. We have $f(e) = f(ee) = f(e)f(e)$. By cancellation, (1) is established.
2. We have

   $$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1}), \qquad \textit{similarly} \quad e' = f(a^{-1})f(a).$$

   So, (2) is established.
3. We have $e' = f(e) \in f(H)$. So, e' is also an identity of $f(H)$. Let $y \in f(H)$. Then, $y = f(a)$ for some $a \in H$. So, From (2), $y^{-1} = f(a^{-1}) \in f(H)$, because $a^{-1} \in H$. So, (3) is established.
4. (4) follows from (5).
5. Now proeve (5). First, $e' = f(e) \in K$. So, $e \in f^{-1}(K)$. Let $a \in f^{-1}(K)$. So, $f(a) \in K$. So, $f(a^{-1}) = f(a)^{-1} \in K$. So, $a^{-1} \in f^{-1}(K)$. So, (4) is established.

The proof is complete. ■

Theorem 13.12. Let $f : G \longrightarrow G'$ be a homomorphism of groups. Let $H = \ker(f)$ and $a \in G$. Then,

$$f^{-1}(\{f(a)\}) = aH = Ha.$$

In particular, the left and right cosets are same.

Proof. Recall (defnition from §0) that $f^{-1}(\{f(a)\}) = \{x \in G : f(x) = f(a)\}$. Now,

$$x \in f^{-1}(\{f(a)\}) \Longleftrightarrow f(x) = f(a) \Longleftrightarrow f(a^{-1}x) = f(a^{-1})f(x) = e'$$

$$\Longleftrightarrow a^{-1}x \in \ker(f) = H \Longleftrightarrow x \in aH.$$

So,

$$f^{-1}(\{f(a)\}) \subseteq aH \quad and \quad aH \subseteq f^{-1}(\{f(a)\}).$$

So, $f^{-1}(\{f(a)\}) = aH$. Similarly, $f^{-1}(\{f(a)\}) = Ha$. The proof is complete.■

Example 13.13 (13.16)**.** The absolute value (length) function

$$ab : \mathbb{C}^* \longrightarrow \mathbb{R}^+ \qquad z \mapsto |z|$$

is a groups homomorphism, from the multiplicative group of nonzero complex numbers to the multiplicative group of positive real numbers.

1. The kernel of this homomorphism is $ab^{-1}\{1\} = U$ is the unit circle.
2. Also $ab^{-1}\{r\} = C_r$ is the circle of radius r. This is the left coset $C_r = zU$ for any $z \in \mathbb{C}$ with $|z| = r$.

Example 13.14 (13.17)**.** Let $\mathcal{D}(\mathbb{R})$ be the additive group of all differentiable functions, $f : \mathbb{R} \longrightarrow \mathbb{R}$, *with continuous derivative.* Let $\mathcal{F}$ be the additive group of all continuous functions $f : \mathbb{R} \longrightarrow \mathbb{R}$. Let

$$\Delta : \mathcal{D}(\mathbb{R}) \longrightarrow \mathcal{F} \qquad be\ defined\ by \quad \Delta(f) = \frac{df}{dx}.$$

1. Then, Δ is a homomorphism.

2. Then $\ker(\Delta) = \{f \in \mathcal{D}(\mathbb{R}) : \frac{df}{dx} = 0\}$, which is the set of all constant functions $\mathcal{C}$.

3. The coset of a function $g \in \mathcal{D}(\mathbb{R})$ is
$$\left\{ f \in \mathcal{D}(\mathbb{R}) : \frac{df}{dx} = g' \right\} = \{g + c : c \in \mathbb{R}\} = g + \mathcal{C}.$$

Corollary 13.15. Let $\varphi : G \longrightarrow G'$ be a homomorphism of groups. Then φ is injective if and only if $\ker(\varphi) = \{e\}$. (*Therefore, from now on, to check that φ is injective, we would only check.*)
$$\varphi(g) = e' \qquad \Longrightarrow \qquad g = e.$$

Proof. ($\Rightarrow$): Suppose φ is injective. Let $x \in \ker(\varphi)$. Then $\varphi(x) = e' = \varphi(e)$. So, $x = e$. So, it is established that $\ker(\varphi) = \{e\}$.

($\Leftarrow$): Suppose $\ker(\varphi) = \{e\}$. We want to prove φ is injective. Let $\varphi(x) = \varphi(y)$. Then, $\varphi(xy^{-1}) = e'$. So, $xy^{-1} \in \ker(\varphi) = \{e\}$ or $xy^{-1} = e$. So, $x = y$. The proof is complete. ■

Corollary 13.16. Let $\varphi : G \longrightarrow G'$ be a mapping of groups. To check that φ is an isomorphism, we have to do the following:

1. Prove φ is a homomorphism.
2. Show $\ker(\varphi) = \{e\}$
3. Show φ is onto.

Normal Subgroups:

Definition 13.17. Let G is a group and H be a subgroup of G. We say that H is a **normal subgroup** of G if
$$gH = Hg \ \forall \ g \in G.$$

If follows from (13.12) that kernel of any homomorphism is normal.

14 Factor Groups

Given a normal subgroup H of G, we define a group structure of the set of (left) cosets of H. I wrote "left" within parenthesis, because for normal subgroups, the left cosets and the right cosets are same.

The textbook gives more than two pages of motivational discussison.

Remark/Prelude: Let me provide my prelude for "factor" groups. "Factor groups" would also be referred to as the "quotient group", in future. Given an object G is a category $\mathcal{C}$ and a subobject H of G, there will be an attempt to define the "quotient object" G/H. For example, in topology, quetient of the inteval $G = [0, 1]$ by the subobject $\{0, 1\}$ is the circle.
In group theory, we can define factor groups G/H, only when H is a normal subgroup of G, as follows.

Definition 14.1. Let G is a group and H is a normal subgroup of G.

1. Let G/H denote the set of all left (right) cosets of H in G. "G/H" is read as "G **mod** H" or "G **modulo** H"

2. On the set G/H define a binary operation on G/H as follows:

$$aH * bH := (ab)H.$$

It seems, this operation depends on the choices of repersentatives a from aH and b from bH. For a definition to make sense, we need to show that it does not depend on such choices of representativs.

So, let $aH = xH$ and $bH = yH$. We will show $(ab)H = (xy)H$. First, since $x \in aH, y \in bH$ we have $x = ah_1, y = bh_2$ for some $h_1, h_2 \in H$. So, $xy = ah_1bh_2$.

Since $Hb = bH$ (why?) we have $h_1b = bh_3$ for some $h_3 \in H$. So,

$$xy = ah_1bh_2 = ab(h_3h_2) \in abH. \qquad So, \quad (xy)H \subseteq (ab)H.$$

$$Similalry, \quad (ab)H \subseteq (xy)H. \quad So, \quad (ab)H = (xy)H.$$

Therefore, this binary operation on G/H is **well defined.**

3. **Notation.** Since $a(bH) = (ab)H$, we will write $abH := (ab)H$.

4. It follows, G/H is a group under this binary operation.

   Proof. We check all the conditions:

   (a) The opertion is well defined and G/H is closed under this operation.

   (b) (**Assiciative**): We have

   $$(aH{*}bH){*}cH = (abH){*}cH = abcH = (aH)(bcH) = (aH)(bH{*}cH).$$

   (c) (**Identity**): $eH = H$ is the identity: $(eH)(aH) = aH = (aH)(eH)$

   (d) (**Inverse**): The inverse of aH is $a^{-1}H$:

   $$(aH)(a^{-1}H) = (aa^{-1})H = H \quad and \quad (a^{-1}H)(aH) = (a^{-1}a)H = H.$$

   So, it is established that G/H is a group under this binary operation. The proof is complete. ■

This group G/H is called the **factor/quotient group** of G by H.

14.1 Fundamental Homomorphism Theorem

Theorem 14.2 (14.9)**.** Let H be a normal subgroup of G. Then, the map

$$\gamma : G \longrightarrow G/H \quad defined\ by \quad \gamma(a) = aH$$

is a group homomorphism. Further, $\ker(\gamma) = H$.

Proof. Clearly,

$$\gamma(ab) = abH = (ah)(bH) = \gamma(a)\gamma(b).$$

So, γ is a homomorphism.

Also, clearly, $H \subseteq \ker(\gamma)$. If $a \in \ker(\gamma)$ then $\gamma(a) = aH = H$. So, $a \in H$. Therefore, $H \subseteq \ker(\gamma)$. So, $H = \ker(\gamma)$. The proof is complete. ■

Theorem 14.3 (14.11)**.** Let $\varphi : G \longrightarrow G'$ be a homomorphism of groups and $H = \ker(\varphi)$. Let $\gamma : G \longrightarrow G/H$ be the "canonical" homomorphism defined above. Then,

1. There is a homomorhism $f : G/H \longrightarrow G'$ such that $\varphi = f\gamma$. Diagramtically,

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\gamma"'] & G' \\ G/H \arrow[ur, dashed, "f"'] & \end{tikzcd}$$

commutes.

   We say, φ **factors through** G/H.

2. In fact, f is injective.

3. f induces and isomorphism $G/H \xrightarrow{\sim} \varphi(G)$ from G/H to image of φ.

Proof. First, define $f : G/H \longrightarrow G'$ by $f(aH) = \varphi(a)$.

1. To see f is well defined, let $xH = aH$. So, $a \in aH$ and $x = ah$ for some $h \in H$. So,

$$\varphi(x) = \varphi(ah) = \varphi(a)\varphi(h) = \varphi(a)e' = \varphi(a).$$

   So, f is well defined. Also

$$f((aH)(bH)) = f(abH) = \varphi(ab) = \varphi(a)\varphi(b) == f(aH)f(bH).$$

   So, f is a well defined homomorphism.

2. Let $f(aH) = e'$, So, $\varphi(a) = e'$ and $a \in \ker(\varphi) = H$, which is the identity of G/H. So, by (13.15) f is injective.

3. Clealy, image of f is $\varphi(G)$. So, f is bijective from G/H to $\varphi(G)$, hence and isomorphism.

The proof is complete. ∎

Corollary 14.4 (Extra)**.** Let $\varphi : G \longrightarrow G'$ be a homomorphism of groups and K be a normal subgroup of G and $K \subseteq \ker(\varphi)$. Let $\gamma : G \longrightarrow G/K$ be the "canonical" homomorphism defined above. Then, there is a homomorhism $f : G/K \longrightarrow G'$ such that $\varphi = f\gamma$. Diagramtically,

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\gamma"'] & G' \\ G/K \arrow[ur, dashed, "f"'] & \end{tikzcd} \qquad \textit{commutes.}$$

We say, φ factors through G/K.

Proof. Similar to the above. ■

14.2 Normal Subgroups and Inner Automorphisms

We give different characterizations of normal subgroups. Let me introduce some obvious notations:

Notations 14.5. Let G be a group and S, T are subsets of G. Define

1. $$ST = \{gh : g \in S, h \in T\}$$

   ST is a subset of G.

2. So, $gH = \{g\}H$.

3. Similarly, we define product STU of subsets of G.

Theorem 14.6. Let H be a subgroup fo G. Then the following conditions are equivalent:

1. H is a normal sugroup of G.

2. $gHg^{-1} = H \quad \forall g \in G$.

3. $gHg^{-1} \subseteq H \quad \forall g \in G$.

Proof. It is obvious that (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3). Now suppose (3) holds. So, For $g \in G$ we have $gHg^{-1} \subseteq H$. So, $gH \subseteq Hg$. Also, the given equation, when applied to g^{-1} we have $g^{-1}Hg \subseteq H$. So, $Hg \subseteq gH$. So, $gH = Hg$ and (1) is established. The proof is complete. ■

Example 14.7 (14.14)**.** Let G be a commutative group. Then, any subgroup H is a normal subgroup of G.

Definition 14.8. Let G be a group.

1. A homomorphism $f : G \longrightarrow G$ is called and Endomorphism of G.

2. An isomorphism $f : G \longrightarrow G$ is called and Automorphism of G.

3. For $g \in G$, define $i_g : G \longrightarrow G$ by $i_g(x) = gxg^{-1}$ for all $x \in G$. Then i_g is an automorphism of G. Such an automorphism is called an inner automorphism of G.

4. Note, a subgroup of G is normal if and only if $i_g(H) = H \ \forall g \in G$.

15 Factor Group Computation and Simple Gropus

In this section, we discuss some examples.

Example 15.1 (15.2 Edited)**.** (**A trivial example**) Let G be a group. Then $\{e\}$ is a normal subgroup of G. Also, $G \xrightarrow{\sim} G/\{e\}$ is an isomorphism.

Example 15.2 (15.3 edited)**.** (**A trivial example**) Let G be a group. Then, G itself is normal subgroup of G. Also $G/G \approx \{1\}$, the one element group.

Example 15.3 (15.4)**.** The alternating geoup A_n is a normal subgroups of the symmetric group S_n. Also, $S_n/A_n \approx \mathbb{Z}_2$.

Example 15.4 (15.7)**.** Compute $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,1)\rangle \approx \mathbb{Z}_4$.

Example 15.5 (15.8)**.** Let H, K be two group and $G = H \times K$. Then $H \times \{e\}$ is normal in G and $G/H \times \{e\} \approx K$.

Theorem 15.6. A factor groups of a cyclic group is cyclic.

Example 15.7 (15.10)**.** Compute $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,2)\rangle \approx \mathbb{Z}_4 \times \mathbb{Z}_2$.

Example 15.8 (15.11)**.** Compute $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(2,3)\rangle \approx \mathbb{Z}_4 \times \mathbb{Z}_3 \approx \mathbb{Z}_{12}$.

Example 15.9 (15.12)**.** Compute $(\mathbb{Z} \times \mathbb{Z})/\langle(1,1)\rangle \xrightarrow{\sim} \mathbb{Z}$ given by $\overline{(x,y)} \mapsto x - y$.

If diagrams would help, see the textbook.

15.1 Simple Groups

Definition 15.10. *A group is called* **simple***, if it is nontrivial and has no nonrivial normal subgroups.*

We skip the rest of this subsection.

15.2 Center and Commutator Subgroups

We define two important subgroups of a group G.

Definition 15.11. Let G be a group. Define the **center** $Z(G)$ of G as follows:

$$Z(G) = \{g \in G : zg = gz \ \forall g \in G\}.$$

1. So, the center $Z(G)$ consists of all elements $z \in G$ that commutes with every other elements og G.
2. First the identity $e \in Z(G)$.
3. It is easy to check that $Z(G)$ is a subgroup of G and it is abelian.

   Proof. Exercise
4. If G is abelian, then $Z(G) = G$.

Remark. Let G be a group and $a, b \in G$. Then

$$ab = ba \iff aba^{-1}b^{-1} = e.$$

Definition 15.12. Let G be a group.

1. For $a, b \in G$ write $[a, b] := aba^{-1}b^{-1}$. Such an expression is called a commutator of G. Note, $[a, b]^{-1} = [b, a]$ is also a commutator.
2. The **commutator subgroup** of G is defined to be the subgroup $[G : G]$ generated by all the commutators $[a, b]$ of G. So, the commutator:

$$[G, G] = \{[a_1, b_1][a_2, b_2] \cdots [a_k, b_k] : k \geq 0 \quad \textit{and} \quad a_i.b_i \in G\}$$

$$= \left\{ \prod_{i=1}^{k} [a_i, b_i] : k \geq 0 \quad \textit{and} \quad a_i.b_i \in G \right\}$$

Proof. Let the RHS be donoted bt S. Obviously, S contains all the commutatiors. S is closed under multiplication. $e = [e, e] \in S$. Also, S is closed under inverse. So, S is a subgroup.

Also, if H is subgroup, containing all the commutators then $S \subseteq H$. So, $[G, G] = S$. The proof is complete. ■

3. If G is commutative then $[G, G] = \{e\}$.

Theorem 15.13. Let G be a group. Then,

1. $[G, G]$ is a normal subgroup of G.
2. $G/[G, G]$ is commutative.
3. If N is a normal subgroup of G and G/N is abelian, then $[G, G] \subseteq N$.

Proof.

1. let $g \in G$. We will prove $g^{-1}[G, G]g \subseteq [G, G]$. First,

$$g^{-1}[a, b]g = g^{-1}(aba^{-1}b^{-1})g = (g^{-1}aba^{-1})e(b^{-1}g)$$
$$= (g^{-1}aba^{-1})(gb^{-1}bg^{-1})(b^{-1}g) = ((g^{-1}a)b(g^{-1}a)^{-1}b^{-1})(bg^{-1}b^{-1}g)$$
$$[g^{-1}a, b][b, g^{-1}] \in [G, G].$$

Now let $x \in [G, G]$. Then $x = \prod_{i=1}^{k}[a_i, b_i]$ for some $a_i, b_i \in G$. So,

$$g^{-1}xg = \prod_{i=1}^{k}((g^{-1}[a_i, b_i]g)$$

Since each factor $g^{-1}[a_i, b_i]g \in [G, G]$ we have $g^{-1}xg \in [G, G]$. So, it is established that $g^{-1}[G, G]g \subseteq [G, G]$. So, $[G, G]$ is a normal subgroup of G and (1) is proved.

2. We want to prove $(a[G, G])(b[G, G]) = (b[G, G])(a[G, G])$. That means, to prove $ab[G, G] = ba[G, G]$. That means, to prove $a^{-1}b^{-1}ab[G, G] = [G, G]$, which is true because $a^{-1}b^{-1}ab \in [G, G]$. So, $G/[G, G]$ is commutative and (2) is established.

3. For $a, b \in G$ we have $(aN)(bN) = (bN)(aN)$ or $abN = baN$ or $a^{-1}b^{-1}abN = N$. So, $[a^{-1}, b^{-1}] = a^{-1}b^{-1}ab \in N$. Replacing a by a^{-1} and b by b^{-1} we have $[a, b] \in N$ for all $a, b \in G$.. So, each commutator of G is in N so, $[G, G] \subseteq N$. So, (3) is established.

The proof is complete. ■

16 Group Action of Sets

Let X ba a set. Let G be the group of all bijections $\varphi : X \longrightarrow X$. So, $G = \{\varphi : \varphi : X \longrightarrow X \textit{ a bijection}\}$. Then, G acts on X in the the following sense:

$$\varphi \in G \textit{ acts on } X : \quad x \mapsto \varphi(x) \in X.$$

In subsequent notations, $\varphi(x) =: \varphi * x$ be viewed as some kind of "multiplication".

Definition 16.1. Let G be a group and X be a set. Let $* : G \times X \longrightarrow X$ be a function. For $x \in X, g \in G$ we use the notation $gx := g * x$. Such a map $*$ is called an **action of G** on X if

1. $ex = x \; \forall \; x \in X$.
2. For $g_1, g_2 \in G$ and $x \in X$ we have $(g_1 g_2)x = g_1(g_2 x)$.

In this case, we also say that X is a **$G-$set**.

Example 16.2 (16.2)**.** Let $\mathcal{S}(X)$ denote the set of all permutaions (bijections) $\sigma : X \longrightarrow X$. Let H be a subgroup of $\mathcal{S}(X)$. Then, X is a $H-$set by the action $* : H \times X \longrightarrow X$ that sends $(\sigma, x) \mapsto \sigma(x)$. So, we will write $\sigma x := \sigma(x)$.

Theorem 16.3. Let G be a group and X be a $G-$set. For $g \in G$ define

$$\sigma_g : X \longrightarrow X \qquad by \qquad \sigma_g(x) = gx \quad for \quad x \in X.$$

1. Then, σ_g is a permutation of X.
2. The map $\varphi : G \longrightarrow \mathcal{S}(X)$ define by $\varphi(g) = \sigma_g$ is a group homomorphism.

Proof. In fact, inverse of σ_g is $\sigma_{g^{-1}}$. For $x \in X$ we have

$$\sigma_{g^{-1}} o \sigma_g(x) = \sigma_{g^{-1}}(gx) = g^{-1}(gx) = (g^{-1}g)x = ex = x.$$

So, $\sigma_{g^{-1}} o \sigma_g = I_X$ and similalry, $\sigma_g o \sigma_{g^{-1}} = I_X$. So, σ_g has a (set theoretic) inverse. Therefore, σ_g is a bijection (permutation). So, (1) is established.

Fors, $g_1, g_2 \in G$ we have $\varphi(g_1g_2) = \sigma_{g_1g_2}$ For $x \in X$ we have

$$\sigma_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = \sigma_{g_1} o \sigma_{g_2}(x).$$

So,

$$\varphi(g_1g_2) = \sigma_{g_1g_2} = \sigma_{g_1} o \sigma_{g_2} = \varphi(g_1)\varphi(g_2).$$

Therefore, φ is a homomorphism. The proof is complete. ■

Definition 16.4. Let X be a $G-$set.

1. We say G **acts faithfully on X**, if

$$for\ g \in G, \quad gx = x\ \forall\ x \in X \quad \Longrightarrow \quad g = e.$$

   In words, if only e leaves every element of X fixed.

2. We say **G is transitive**, if for each $x_1, x_2 \in X$, there is an element $g \in G$ such that $gx_1 = x_2$.

Lemma 16.5. Let X be a $G-$set. Let $N = \{g \in G : gx = x\ \forall\ x \in X\}$. *That means, N is the subgroup of G that acts trivially (as identity) on X.* Then

1. N is a normal subgroup of G.
2. The action of G on X induces an action of G/N on X.
3. The action of G/N on X is faithful.

Proof.

1. First, let $g, h \in N$. Then, for $x \in X$ we have $ghx = gx = x$. So, $gh \in N$ and N is closed under multiplication. By definition of the action, the identity $e \in N$. Also, for $g \in N$ and $x \in X$ we have $gx = x$. Apply g^{-1}, we have $g^{-1}(gx) = g^{-1}x$ or $x = g^{-1}x$. So, $g^{-1} \in N$. So, N is also closed under inverse, hence is a subgroup of G.

   Now let $g \in G$ and $h \in N$. For $x \in X$ we have $(g^{-1}hg)x = g^{-1}gx = ex = x$. So, $g^{-1}Ng \subseteq N$ and N is a normal subgroup of G. So, (1) is established.

2. For $gN \in G/N$ define the action $gN * x = gx$ for $x \in X$. We, first need to show that this is well defined. Suppose $gN = fN$. Then $f = gh$ for some $h \in N$. So, for $x \in X$, we have $fc = ghx = gx$. So, $gN * x = gx$ is well defined. Clearly, for $x \in X$, $N * x = e * x = x$ and $(gNfN) * x = (gfN) * x = (gf)x = g * (f * x) = gN(fN * x)$. This establishes (2) that this is a $G-$action on X.

3. Now suppose $gN * x = x$ for some $g \in G$ and for all $x \in X$. This means, $gx = x \ \forall x \in X$. So, $g \in N$ and $gN = N$ the identity in G/N. So, the action of G/N is faithful. So, (3) is established.

The proof is complete. ■

Example 16.6 (16.4, 16.5)**.** Let G be a group and H be a subgroup. Then G is a $H-$set. For $g \in H$ and $x \in G$ the action is defined by $g * x = gx$.

In particular, G is a $G-$set.

Example 16.7 (16.6)**.** Let V be a vector space of $\mathbb{R}$. Then V is a R^*-set by scalar multiplication.

Example 16.8 (16.8)**.** Read about the action of D_4 on the sides, diagonals and horizonatal and vertical axes.

16.1 Isotropy Subgroups

.

Definition 16.9. Let X be a $G-$set and $x \in X, g \in G$. Define

$$X_g = \{z \in X : gz = z\} \qquad \textit{and} \qquad G_x = \{f \in G : fx = x\}.$$

X_g is the subset of fixed points of g. G_x is the subgroup of elements that leave x-fixed.

Theorem 16.10. Let X be a $G-$set and $x \in X$. Then G_x is a normal subgroup of G.

Proof. The proof is simialr to (16.5). ■

Definition 16.11. Let X be a $G-$set and $x \in X$. Then, G_x is called the isotropy subgroup of x.

16.2 Orbits

Theorem 16.12. Let X be a $G-$set. For $a, b \in X$ define $a \sim b$ if there is a $g \in G$ such that $ga = b$. Then, $\sim$ is an equivalence relation on X.

Proof. We check the three conditions.

1. (**Reflexive**): For $x \in X$ we have $ex = x$. So, $x \sim X$.
2. **Symmetric**): Suppose $x \sim y$. Then $gx = y$ for some $g \in G$. Multiplying by g^{-1}, we have $x = g^{-1}y$. So, $y \sim x$. So, $\sim$ is reflexive.
3. (**Transitive**): Suppose $x \sim y \sim Z$. Then, $fx = y, gy = z$ for some $f, g \in G$. So, $gfx = z$. So, $x \sim z$ and $\sim$ is transitive.

The proof is complete. ■

Definition 16.13. Let X be a $G-$set and $x \in X$. The equivalence class of x is called the **orbit of x under** G. In fact, the orbit of x is $Gx = \{gx : g \in G\}$.

Notations. Recall, the cardinality of a set X is denoted by $|X|$. For a subgroup H of G, the index of H in G is denoted by $(G : H)$.

Theorem 16.14. Let X be a $G-$set and $x \in X$. Then

1. $|Gx| = (G : G_x)$.
2. If G is finite, then $|Gx|$ divides $|G|$.

Proof. (Here x is fixed.) Let G/G_x denote the set of left cosets of G_x. (G_x *may not be normal in* G.) Define the map

$$\varphi : G/G_x \longrightarrow Gx \quad by \quad \varphi(gG_x) = gx.$$

Then, φ is a well defined bijection. To see this let $gG_x = fG_x$. Then $f = gh$ for some $h \in G_x$. Since $h \in G_x$, $hx = x$. So, $fx = (gh)x = g(hx) = gx$. This establishes that φ is well defined.

Give $y \in Gx$ we have $y = gx$ for some $g \in G$. So, $\varphi(gG_x) = gx = y$. So, φ is onto. Now let $\varphi(gG_x) = \varphi(fG_x)$. That means, $gx = fx$. So, $(f^{-1}g)x = x$. So, $f^{-1}g \in G_x$ and hence $gG_x = fG_x$. So, φ is one to one (injective). So, φ is bijective. Therefore $|Gx| = (G : G_x)$.

Since $(G : G_x)$ divides $|G|$, so does $|Gx|$. The proof is complete. ■

17 Application of $G-$sets to Counting

We skip this section, for now.