3.1 Definitions and Examples

Alex L.

October 5, 2024

Def: A **homomorphism** $\varphi : A \to B$, where $(A, *), (B, \cdot)$ are groups, is a mapping from A to B such that for all $x, y \in A$, $\varphi(x * y) = \varphi(x) \cdot \varphi(y)$

Ex: Let $G = \mathbb{Z}$ under addition, and let $H = \mathbb{Z}_n$, the cyclic group of order n under multiplication ($x^n = x$), and define a mapping $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ by $\varphi a = x^a$.

To show that φ is a homomorphism, we show that $\varphi(a + b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b)$. Note that φ is surjective (every element in the image of φ is covered).

The fiber (inverse image) of a given $x^a \in \mathbb{Z}_n$, then, is the set of numbers in $\mathbb{Z}$ that have a modulo n of a, and the fibers of φ are the sets of numbers with the same residual of modulo n.

Since φ is a homomorphism, this implies that any group operation performed on the cyclic group $\mathbb{Z}_n$ will have a corresponding group operation on the fibers of φ in G. We can use these interactions to make a new group out of the fibers of φ.

Def: Given groups G and H, with the homomorphism $\varphi : G \to H$, the **kernel of** φ denoted ker φ is the set of elements $g \in G$ such that $\varphi(g) = 1_H$ (the identity of H). The kernel is also known as the fiber of φ over the identity of H.

Prop: Let G and H be groups and $\varphi : G \to H$

1. $\varphi(1_G) = 1_H$
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$
3. $\varphi(g^n) = \varphi(g)^n \;\forall\, n \in \mathbb{Z}$
4. ker $\varphi < G$ (is a subgroup of)
5. $\text{im}(\varphi)$, the image of G under φ, is a subgroup of H

Proof:

1. $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$. Left multiply by the inverse of $\varphi(1_G)$ on both sides. Since they are inverses and elements of H, you are left with $1_H = \varphi(1_G)$
2. $\varphi(1_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$. Substitute $\varphi(1_G)$ for 1_H. Left multiply by $\varphi(g)^{-1}$ to get $\varphi(g)^{-1} = \varphi(g^{-1})$
3. Proof by induction. $\varphi(g^1) = \varphi(g) = \varphi(g)^1$. Assume that $\varphi(g^n) = \varphi(g)^n$. $\varphi(g^{n+1}) = \varphi(g^n \cdot g) = \varphi(g^n) \cdot \varphi(g^1) = \varphi(g)^n \cdot \varphi(g)^1 = \varphi(g)^{n+1}$
4. Subgroup Criterion: Show that the subset is nonempty, is closed, and has inverses. (Shortcut: show that any element and any inverse of an element (xy^{-1} under the group operation is a member of the subgroup. By setting both elements to be the same, we can deduce that there are inverses, and by setting it to all other group members, we can deduce that it is closed.) $1_G \in$ ker φ, therefore it is nonempty. Assume that $x, y \in$ ker φ. Then, $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = 1_H 1_H = 1_H$, therefore $xy^{-1} \in$ ker φ.
5. Subgroup Criterion: $\varphi(1_G) \in$ im (φ), so the set is nonempty. Let $x, y \in$ im (φ), such that $x = \varphi(a)$ and $y = \varphi(b)$ for some $a, b \in G$. Then, $xy^{-1} = \varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}) \in$ im (φ), so im (φ) is a group.

Def: Given a homomorphism $\varphi : G \to H$ with a kernel K, the **quotient group**, G/K, read G mod K, is the group of fibers of φ in G, with the identity of K. Keep in mind that the elements of the quotient groups are fibers, essentially sets of elements in G, but they are treated as single elements in the quotient group.

Prop: Let $\varphi : G \to H$ be a homomorphism of G to H with kernel K. Let $X \in G/K$ be a fiber above an element $a \in H$ ($X = \varphi^{-1}(a)$.

1. For any $u \in X$, $X = \{uk \mid k \in K\}$
2. For any $u \in X$, $X = \{ku \mid k \in K\}$

Proof:

1. To prove equality of sets, we need to prove that they are subsets of each other. To prove that $uK \subseteq X$, we can show that $\varphi(uk) = \varphi(u)\varphi(k) = \varphi(u)1_H = \varphi(u)$, and since $\varphi(u) \in X$, by definition, $\varphi(u) = a$. Therefore, all elements of $uK \in X$. To prove the opposite, first we show that $k \in K$ when $k = u^{-1}g$, where $u, g \in X$. $\varphi(k) = \varphi(u^{-1})\varphi(g) = \varphi(u^{-1})\varphi(g) = a^{-1}a$(because $u, g \in X$) $= 1_G$, therefore $k = u^{-1}g \in K$. If we left multiply both sides by u, we get $uk = g$, and since $uk \in uK$, we show that $g \in uK$, therefore $X \subseteq uK$.

2. Repeat the same thing but inverted to get this proof.

This shows that by having a kernel and one element of a fiber, we can reconstruct the entire fiber.

Def: For any $N \leq G$ and any $g \in G$, $gN = \{gn \mid n \in N\}$ is called a left coset of N in G and $Ng = \{ng \mid n \in N\}$ is called a right coset. Any element of a coset is called a representative of the coset.

Theorem: Let G be a group and let K be the kernel of a homomorphism from G to another group. The set whose elements are left cosets of K in G with operation $uK \cdot vK = uvK$ forms a group, G/K. Also, let any elemet $u_1 \in uK$ and $v_1 \in vK$, then $u_1v_1 \in uvK$, so the multiplication doesn't care about what element in each coset you choose. The same statement is true with right cosets.

Proof: Let $\varphi : G \to H$ be the homomorphism mapping G to another group, H, and let $X, Y \in G/K$, and be left cosets of K. $\varphi(X) = a_H$ and $\varphi(y) = b_H$, and let $Z = XY$. Therefore, $Z = \varphi^{-1}(a_H)\varphi^{-1}(b_H)$, so, $Z = \varphi^{-1}(a_Hb_H)$. Now, let $u \in X$ and $v \in Y$. We want to show that $uv \in Z$. $\varphi(u)\varphi(v) = ab$, so $\varphi(uv) = ab$, and if we apply φ^{-1} to both sides, we get $uv = \varphi^{-1}(ab)$, which means that $uv \in Z$. This shows that the set G/K is closed. $\varphi^{-1}(1_H) = \varphi^{-1}(a)\varphi^{-1}(a^{-1}) = XY$ where $X, Y \in G/K$. Therefore, $K = XY$ for some $X, Y \in G/K$, so it has inverses. Therefore, it is a group.

Ex:

1. A homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ has fibers $a + n\mathbb{Z}$, the residue classes of $\mathbb{Z}$ mod n. The group $\mathbb{Z}/n\mathbb{Z}$ has the operation of addition of representatives.

2. If $\varphi : G \to H$ is an isomorphism (there is a one to one mapping of elements of G to elements of H, a bijective homomorphism), then ker $\varphi = 1_G$) and the quotient group is $G/1_G \cong G$.

3. Let G be any group, and $H = 1$, the group of order 1, and $\varphi : G \to H$ by $\varphi(g) = 1_H$ for all $g \in G$. Then, the quotient group would be $G/G = \{1\}$. The map is called a trivial homomorphism.

4. Let $G = \mathbb{R}^2$ under vector addition and let $H = \mathbb{R}$ under addition, and let $\varphi : \mathbb{R}^2 \to \mathbb{R}$ by $\varphi((x_G, y_G)) = x_H$. φ is a projection onto the x-axis. We will show that φ is a homomorphism. Let $a = (x_a, y_a), b = (x_b, y_b) \in \mathbb{R}^2$. $\varphi(a + b) = \varphi((x_a + x_b, y_a + y_b)) = x_a + x_b$. $\varphi(a) + \varphi(b) = \varphi((x_a, y_a)) + \varphi((x_b, y_b)) = x_a + x_b$. Rhese two statements are equal, therefore, $\varphi(a + b) = \varphi(a) + \varphi(b)$. Now, ker φ is $x = 0$, the y-axis, and the cosets are vertical lines.

5. Let $G = Q_8$, the quaternion group, and let $H = V_4$, the Klein 4-group. Define $\varphi : G \to H$ as $\varphi(\pm 1) = 1$, $\varphi(\pm i) = a$, $\varphi(\pm j) = b$, $\varphi(\pm k) = c$. Now, let $x, y = \pm 1_G$. $\varphi(x \cdot y) = \varphi(\pm 1) = 1_H$. Additionally, $\varphi(x) \cdot vphi(y) = 1_H \cdot 1_h = 1_H$. When $x = i$, and $y \in \pm 1$, $\varphi(x \cdot y) = \varphi(\pm x) = a$. $\varphi(x) \cdot \varphi(y) = 1_H \cdot a = a$, and symmetry applies to j and k. If $x = i$ and $y = j$, then $\varphi(x \cdot y) = \varphi(k) = c$. $\varphi(x) \cdot \varphi(y) = a \cdot b = c$. Symmetry shows this is true for j and k, and since the function doesn't care about signs on elements, it is also true for the negatives as well. Lastly, if $x = y = i$, $\varphi(x \cdot y) = \varphi(-1) = 1_H$. $\varphi(x) \cdot \varphi(y) = a_H \cdot a_H = 1_H$. The same is true for negatives and j and k. Evidently, φ is a homomorphism from G to H.

Prop: Let $N \leq G$. The set of left cosets of N in G forms a partition (all elements of G are in exactly one coset). Also, for all $u, v \in G$, $uN = vN$ if and only if $v^{-1}u \in N$ and $uN = vN$ if and only if u and v are representatives of the same coset.

Proof: Since N is a subgroup of G, $1 \in N$, so all elements of G are in a coset of N because if $g \in G$, $g \cdot 1 \in gN$, a coset of N. Now, we want to show that it is not possible for an element to be part of two cosets unless those cosets are equal. Suppose that two cosets uN and vN had $uN \cap vN \neq \varnothing$. Let x be an element in this intersection. Then, $x = un = vm$ for some $n, m \in N$. Right multiply by n^{-1} to get $x = u = vmn^{-1}$. Note that $mn^{-1} \in N$ because N is a group. Now, for any element $ut \in uN$, $ut = vmn^{-1} \in vN$ because $mn^{-1}t \in N$.

Prop: Let $N \leq G$.

1. The operation on the set of left cosets of N in G described by $uN \cdot vN = uvN$ is only well defined if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.

2. If the operation is well defined, the set of left cosets is a group with identity $1N$ and inverse of gN being $g^{-1}N$

Proof:

1. Assuming that the operation is well defined, we want to show that $gng^{-1} \in N$ is nessecarily true. By extension, $u, u_1 \in uN$ and $v, v_1 \in vN$, then $uvN = u_1v_1N$. Therefore, if $g \in G$ and $n \in N$, $1g^{-1}N = ng^{-1}N$. Since $1 \in N$, $ng^{-1} \cdot 1 \in ng^{-1}N$. Simplifying both sides, we get $ng^{-1} \in g^{-1}N$. Then, left multiplying by g gets us $gng^{-1} \in N$.

2. Associativity holds because $uN(vNwN) = uNvwN = uvwN = uvNwN = (uNvN)wN$. The rest is pretty self explanatory.

Def: The element $gng^{-1} \in G$ is called the **conjugate** of $n \in N$ by g. The set $gNg^{-1} = \{gng^{-1} | n \in N\}$ is called the **conjugate** of N by g.

Def: The element g is said to **normalize** N if $gng^{-1} = N$. A subgroup N of a group G is called normal if every element of G normalizes N, if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup, we will write $N \trianglelefteq G$.

Theorem: Let $N \leq G$. THe following statements are equivalent:

1. $N \trianglelefteq G$

2. $N_G(N) = G$ (the normalizer of N in G is G)

3. $gN = Ng$ for all $g \in G$

4. The operation $uN \cdot vN = uvN$ makes the set of left cosets into a group

5. $gNg^{-1} \subseteq N$ for all $g \in G$

Proof:

1. We will compare all statements to this statement

2. By definition, the normalizer of a set N in the group G is the set of all elements that fulfill $gNg^{-1} = N$. Since in this scenario, all elements in G fulfill the statement, this is equivalent.

3. By right multiplying by g^{-1} we get $gNg = N$ for all $g \in G$ which is the same as statement 1.

4. The operation is well defined if it is a group, in which case, we will refer to the first part of the previous proposition.

5. Right multiply by g to get $gN \subseteq Ng$. Since cosets have equal cardinality, $gNg^{-1} = N$

Prop: A subgroup N of group G is normal if and only if it is the kernel of some homomorphism.

Proof: If $\ker \varphi = N$, for some homomorphism φ, then $gN = Ng$, since $\varphi(gn)$ wheen $n \in N$ evaluates to $\varphi(g) \cdot 1_H$, and likewise with right multiplication. By right multiplying by g^{-1}, we get $gng^{-1} = N$, which means it is normal.

Def: Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the natural projection of G onto G/N. If $\bar{H} \leq G/N$ is a subgroup of G/N, the complete preimage of $\bar{H}$ in G is the preimage of $\bar{H}$ under natural projection homomorphism.

(The complete preimage is a set with N because $1 \in H$)

We now have a way of identifying kernels of homomoprhisms without needing an external homomorphism to map to, by just finding the normal sets of a given group. When $N_G(N) = G$, it is a kernel, and any result other than that measures how close it is to being a subgroup.

Exercises:

1. Let $\varphi : G \to H$ be a homomorphism and let $E \leq H$. Prove that $\varphi^{-1}(E) \leq G$. If $E \trianglelefteq H$, prove that $\varphi(E) \trianglelefteq H$. Deduce that $\ker \varphi \trianglelefteq G$.
   Proof: Let $a, b \in \varphi^{-1}(E)$. $\varphi(a)$ and $\varphi(b)$ are in E. Since E is a group, $\varphi(a)\varphi(b)^{-1} \in E$ as well. Therefore, $\varphi(ab^{-1}) \in E$, which means $ab^{-1} \in \varphi^{-1}(E)$, which means the preimage of E is a group. Now suppose we have an element $g\ inG$. This means that $\varphi(g) \in H$. Since $E \trianglelefteq H$, this means that $hE = Eh$ for all $h \in H$. As such, this means that $\varphi(g)E = E\varphi(g)$, which implies that $g\varphi^{-1}(E) = \varphi^{-1}(E)g$ for any $g \in G$, which means that φ^{-1}E$\trianglelefteq G$. The kernel of φ is normal in G because the image of the kernel, the identity of H, forms a subgroup in H.

2. Let $\varphi : G \to H$ be a homomorphism with kernel K and let $a, b \in \varphi(G)$. Let $X, Y \in G/K$ and let $X = \varphi^{-1}(a)$ and $Y = \varphi^{-1}(b)$. Let $u \in X$. If $XY = Z$, and $w \in Z$, prove there is some $v \in Y$ such that $uv = w$.
   Proof: We want to show that $u^{-1}w \in Y$. Let c be some element in H such that $\varphi(Z) = C$ If $XY = Z$ this implies that $ab = c$. Since $u \in X$, $\varphi(u^{-1}) = \varphi(u)^{-1} = a^{-1}$, and since $w \in Z$, $\varphi(w) = c$. If $ab = c$, then by left multiplying by a^{-1}, we get $b = a^{-1}c$. By applying φ to $u^{-1}w = y$, we get that $b = a^{-1}c$. These two statements are equivalent.

3. Let A be an abelian group and let $B \leq A$. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.
   Proof: Since every element $a \in A$ satisfies $aB = Ba$, by virtue of A being abelian, then every subgroup of an abelian

group is normal. Therefore, $a_1Ba_2B = (a_1a_2)B = (a_2a_1)B = a_2Ba_1B$, and the multiplication of left cosets in A/B is commutative, so A/B is abelian.

4. Prove that in the quotient group G/N, $(gN)^a = g^aN$ for all $a \in \mathbb{Z}$
Proof: $(gN)^a = gN \cdot gN \cdot gN \cdot ...gN = (g^2)N \cdot gN \cdot gN \cdot gN....gN = ... = (g^a)N$

5. Use the preceeding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$ (and gN has infinite order if no such positive integer exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of $g \in G$.
Proof: The order of gN is a, the smallest integer that satisfies $(gN)^a = N$. This is equivalent to $g^aN = N$ by the preceeding exercise. To fulfill the relationship, $g^a = e$, which means that $g^a \in N$. An example to show that the order of gN may be strictly smaller than the order of g is to let $g \in N$ but also $g \neq e$. Then, the order of gN is one because it is the identity, but the order of g is greater than one.

6. Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ ($\mathbb{R}^\times$ is the real numbers without zero) by letting $\varphi(x) = \frac{x}{|x|}$. Describe the fibers of φ and prove that φ is a homomorphism.
Proof: The fibers of φ are the positive numbers, and the negative numbers. $\varphi(a) \cdot \varphi(b) = \varphi(ab)$ because if you choose two numbers with the same sign, the outcome will be 1, and if you choose numbers with differing signs, the outcome will be -1.

7. Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.
Proof: Every $r \in \mathbb{R}$ can be expressed as a sum of $\frac{r}{2} + \frac{r}{2}$. The kernel of π is the point $(0, 0)$, and the fibers of π form L shapes with corners on the y-axis and extending infinitely downwards at a 45° angle on either side.

8. Let $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$ be the map sending x to the absolute value of x. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and fibers of φ.
Proof: Let $a, b \in \mathbb{R}^\times$. $\varphi(a)\varphi b = |a||b| = |ab| = \varphi ab$. The kernel of φ is $\{-1, 1\}$ and the fibers are real numbers and their negative counterparts.

9. Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a + bi) = a^2 + b^2$. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ geometrically (as subsets of the complex plane).
Proof: $\varphi(z_1 + z_2) = \varphi(a_1 + a_2 + i(b_1 + b_2)) = ...$