Modern Algebra Lecture Notes

Rebekah Dix

October 19, 2018

Contents

1 Group Theory

1.1 Basic Definitions/Examples

Definition 1 (Group)**.** A set G with a binary operation $\star : G \times G \to G$ is a group if the following axioms are satisfied:

1. Associativity: $(a \star b) \star c = a \star (b \star c)$ for every $a, b, c \in G$.

2. Unit (or Identity): There exists an $e \in G$ such that $e \star a = a \star e = a$ for each a in G.

3. Inverse: For each $a \in G$ there is a $b \in G$ such that $a \star b = b \star a = e$.

Example 1 (Examples of Groups)**.** The following are examples of groups.

1. $G = \mathbb{R} \setminus \{0\} = \mathbb{R}^\star$ and $\star =$ multiplication.

2. $G = \mathbb{Z}$ and $\star =$ addition ($e = 0$ and $b = -a$).

3. $G = \{+1, -1\} \subset \mathbb{R}^\star$ and $\star =$ multiplication.

4. $G = S_3 = \{$ All bijective functions $f : \{1, 2, 3\} \to \{1, 2, 3\}\}$ and $\star =$ composition of functions. To check the axioms in this example:

   (a) Associativity: Holds because associativity is a basic property of composition

   (b) Unit Element: The element that maps 1 to 1, 2 to 2, and 3 to 3 is the unit element. This element moves each element to itself.

   (c) Inverse: S_3 is the set of bijections, so the definition of bijection implies there is an inverse by composition.

Definition 2 (Abelian/Commutative)**.** A group G is abelian or commutative if $a \star b = b \star a$ for all $a \in G$.

Example 2. (Examples of Abelian Groups)

1. Examples 1, 2, and 3 above are Abelian. The commutativity follows from the commutativity of addition and multiplication.

2. Example 4 is not Abelian. It's easy to find a pair of elements that don't commute under composition.

Not everything is a group.

Example 3. (Non-Examples of Groups)

1. $G = \mathbb{R}$ and $\star =$ maximum. For example, $2 \star \pi = \max(2, \pi) = \pi$. <u>Associativity</u> is satisfied. The order in which we take the maximum of a set of elements doesn't matter – we'll eventually find the largest element regardless. However, there is no <u>unit element</u>. The reason is that there is no smallest element in $\mathbb{R}$.

2. $G = \mathbb{R}_{\geq 0}$ and $\star =$ maximum. Associativity is satisfied. There is a unit element, namely 0 (observe that we've corrected the problem of not having a smallest element). Fix $g \in G$, and observe that $\max(g, 0) = \max(0, g) = g$. However, there need not be an inverse of each element. We can't take the maximum of some element $g > 0$ and 0 and get 0.

Claim 1. (The unit element is unique) Let G be a group and $\star$ its binary operation. Suppose that $e_1, e_2 \in G$ are both units elements. Then, $e_1 = e_2$.

Proof. Since e_1 and e_2 are unit elements, we know that for all $a \in G$, $a \star e_1 = e_1 \star a = e_1$ and $a \star e_2 = e_2 \star a = e_2$. Consider the product $e_1 \star e_2$. We know that $e_1 \star e_2 = e_2$ since e_2 is a unit element. Further, $e_1 \star e_2 = e_1$ since e_1 is a unit element. Therefore, $e_1 = e_2$. $\square$

Lemma 1. (Cancellation Law) For every group G and $a, b, c \in G$ that satisfy $ab = ac$, we have $b = c$.

Proof. Let x be the inverse of a. Then, $x(ab) = x(ac)$. Be associativity, we may write $(xa)b = (xa)c$. This simplifies to $1 \star b = 1 \star c$ or that $b = c$. $\square$

Corollary 1. (The inverse of a group element is unique) Let G be a group and let $a \in G$. If b and c are inverses of a, then $b = c$.

Proof. Since b and c are inverses of a, we know that $ab = 1 = ac$. Then by the Cancellation Law, we know $b = c$. $\square$

Exercise 1. Show that if $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Solution 1. Going back to the definition of a group and the axiom required to be an inverse element, we must show that $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = 1$. Then,

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1 \tag{1}$$

And,

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1} \cdot 1 \cdot b = b^{-1}b = 1 \tag{2}$$

Therefore, $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = 1$ so that $b^{-1}a^{-1}$ is the inverse of $(ab)^{-1}$.

Exercise 2. Give an example of $\tau \in S_3$ such that $\tau \neq 1$, $\tau^2 \neq 1$, and $\tau^3 \neq 1$.

Solution 2. Consider $\tau(1) = 2$, $\tau(2) = 3$, $\tau(3) = 4$, $\tau(4) = 1$. Then, $\tau^2(1) = 3$ and $\tau^3(1) = 4$. This is sufficient to show that $\tau \neq 1$, $\tau^2 \neq 1$, and $\tau^3 \neq 1$.

Definition 3. (The group $\mathbb{Z}/n\mathbb{Z}$) The group $\mathbb{Z}/n\mathbb{Z}$ is the set $\{0, 1, \ldots, n-1\}$. That is, the possible (integer) remainders upon dividing by n. Recall that the remainder is the smallest number that you subtract from the original number so that it becomes divisible by n.

Exercise 3. Calculate $5 + 6 + 3$ in $\mathbb{Z}/7\mathbb{Z}$.

Solution 3. $5 + 6 + 3 = 14 = 0$

Exercise 4. What is the inverse of 15 in $\mathbb{Z}/30\mathbb{Z}$.

Solution 4. Observe that $15 + 15 = 30 = 0$. Hence 15 is its own inverse.

1.1.1 Order

Definition 4. (Order of a group, order of an element of a group) Let G be a group. We call $|G|$ the order of G (i.e. the number of elements in G). Further, the least $d > 0$ such that $g^d = 1$ is called the order of $g \in G$.

Example 4. (Orders of groups)

- $|S_n| = n!$
- $|\mathbb{Z}/n\mathbb{Z}| = n$

Exercise 5. Calculate the order of 2 in $\mathbb{Z}/7\mathbb{Z}$.

Solution 5. The order of 2 is 7.

1.1.2 Direct Product

Given groups G, H we define a group structure on $G \times H$ by $(g_1, h_2)(g_2, h_2) = (g_1g_2, h_1h_2)$. The unit of $G \times H$ is $(1, 1) = (1_G, 1_H)$. The inverse of (g, h) is $(g, h)^{-1} = (g^{-1}, h^{-1})$. Questions about direct products will decompose into questions about the individual groups.

1.1.3 Symmetric Groups

Definition 5. (Cycle, Cycle Decomposition, Length, k-Cycle) A cycle is a string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers). The product of all the cycles is called the cycle decomposition. The length of a cycle is the number of integers which appear in it. A cycle of length k is called a k-cycle.

Claim 2. The order of a k-cycle is k.

Proof. Let $(i_1i_2 \dots i_k)$ be a k-cycle. By checking each index, observe that $(i_1i_2 \dots i_k)^k = id$. For any $d < k$, note that $(i_1i_2 \dots i_k)^d(i_1) = i_{d+1} \neq i_1$, since $d < k$. □

Claim 3. Disjoint cycles commute.

Proof. Let $\sigma = (s_1s_2 \dots s_k)$ and $\tau = (t_1t_2 \dots t_l)$ be disjoint cycles. Consider an index s_i in the first cycle and an index t_j in the second. Then

$$\sigma(\tau(s_i)) = \sigma(s_i) = s_{i+1} \tag{3}$$

and

$$\tau(\sigma(s_i)) = \tau(s_{i+1}) = s_{i+1} \tag{4}$$

Repeating this argument for all indices shows that

$$\sigma\tau = \tau\sigma \tag{5}$$

□

Example 5. $(236)(14) = (14)(236)$

1.1.4 Matrix Groups (General Linear Groups)

Example 6. Let $GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$ and let the binary operation be the multiplication of matrices. Let's check that the axioms are satisfied so that it is a group.

1. Associativity: Follows from basic properties of matrix multiplication.
2. Identity: Notice that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element.
3. Inverse: The condition $ad - bc \neq 0$ ensures that each element has an inverse.

For completeness, we also need to check that the product of two invertible matrices is again invertible (one quick proof of this uses the fact that taking a determinant is homomorphism. For instance $\det(A) = \det(A)\det(B)$, From this note that if both A and B have non-zero determinants, then AB also has a non-zero determinant). Also observe that this group is not abelian. More generally, for $n \geq 1$, we can define

$$GL_n(\mathbb{R}) = \left\{ n \times n \text{ matrix } A \middle| \det A \neq 0 \right\} \tag{6}$$

1.2 Subgroups

Definition 6. (Subgroup) A subset H of a group G is called a subgroup of G if the following axioms are satisfied

1. Identity: $1 \in H$ (we could also write $1_G \in H$).
2. Closed under products: $h_1 h_2 \in H$ for all $h_1, h_2 \in H$ (in words, the binary operation of G applied to elements of H keeps products in H).
3. Closed under inverses: $h^{-1} \in H$ for all $h \in H$.

In this case we write $H \leq G$. Observe that H is indeed a group.

Example 7. (Examples of Subgroups)

1. Define $H = \{(123), (132), id\} \subset S_3$. Let's check the 3 axioms required to be a subgroup.
   (a) Identity: Observe that $id \in H$.
   (b) Closed under products: Define $\sigma = (123)$. Then $\sigma^2 = (132)$ and $\sigma^3 = id$. Therefore, $\sigma \circ \sigma^2 = \sigma^3 = id \in H$ and so forth.
   (c) Closed under inverses: Observe that $(123)^{-1} = (321) = (132) \in H$.
2. Define $H = \{\lambda I_n | \lambda \in \mathbb{R} \setminus \{0\}\} \subset GL_n(\mathbb{R})$.

(a) Identity: Take $\lambda = 1$.

(b) Closed under products: Fix $\lambda_1, \lambda_2 \in R^\times$. Then $(\lambda_1 I)(\lambda_2 I) = (\lambda_1\lambda_2)I \in H$.

(c) Closed under inverses: Observe that $(\lambda I)^{-1} = \lambda^{-1}I \in H$.

3. Define $H = \{2, 4, 0\} \subset \mathbb{Z}/6\mathbb{Z}$.

   (a) Identity: 0 is in the set.

   (b) Closed under products: Note that $0 + 2 = 2 + 0 = 2 \in H$, $0 + 4 = 4 + 0 = 4 \in H$, and $2 + 4 = 4 + 2 = 0 \in H$.

   (c) Closed under inverses: Note that $2^{-1} = 4 \in H$ (because $2 + 4 = 0$) and of course $4^{-1} = 2 \in H$.

4. Define $H = \{\sigma_n \in S_n | \sigma(n) = n\} \subset S_n$ (the set of n-permutations which fix the last index).

   (a) Identity: $id \in H$ because the identity permutation fixes the last element.

   (b) Closed under products: Let $\sigma, \tau \in H$. Then $\sigma \circ \tau(n) = \sigma(\tau(n)) = \sigma(n) = n$. Therefore $\sigma\tau$ also fixes the last element.

   (c) Closed under inverses: Fix $\sigma \in H$. Since σ fixes n, it must also be that σ^{-1} fixes n. In words, σ takes n to n, so σ^{-1} must also take n to n.

Example 8. (Non-example of Subgroup) Define $H = \{\sigma \in S_3 | \sigma(1) \in \{1, 2\}\} \subset S_3$.

1. Identity: Satisfied.

2. Closed under products: Consider $\sigma = (123)$. Then $\sigma^2 = (132)$. But here, $\sigma(1) = 3$. Therefore this subset is not a subgroup.

1.3 Homomorphisms

Definition 7. (Homomorphism) Let G, H be groups. A function $\phi : G \to H$ is a homomorphism if for every $a, b \in G$, we have

$$\phi(ab) = \phi(a)\phi(b) \tag{7}$$

Note the the product ab on the left is computed in G and the product $\phi(x)\phi(y)$ is computed in H.

Example 9. (Examples of Homomorphisms)

1. Let $G = GL_n(\mathbb{R})$, $H = \mathbb{R}^\times$, $\phi : G \to H$. Define $\phi(A) = \det(A)$.

2. Let $G = \mathbb{Z}/7\mathbb{Z}$, $H = \{z \in \mathbb{C} : z^7 = 1\}$. Define

$$\phi(a) = e^{\frac{2\pi i a}{7}} \tag{8}$$

Then

$$\begin{aligned} \phi(ab) = \phi(a+b) &= e^{\frac{2\pi i(a+b-7k)}{7}} \\ &= e^{\frac{2\pi i a}{7}} e^{\frac{2\pi i b}{7}} e^{-2\pi i k} \\ &= e^{\frac{2\pi i a}{7}} e^{\frac{2\pi i b}{7}} \cdot 1 \\ &= \phi(a)\phi(b) \end{aligned}$$

Observe that ϕ is injective and surjective. ϕ is an isomorphism.

3. Define $\phi : G \to H$ for all $g \in G$, $\phi(g) = 1$.

4. Define $\phi : \mathbb{R}^{\times}_{>0} \to \mathbb{R}$, $\phi(x) = \log(x)$. Then

$$\phi(xy) = \log(xy) = \log(x) + \log(y) = \phi(x) \cdot \phi(y) = \phi(x) + \phi(y) \tag{9}$$

Claim 4. (Basic facts about homomorphisms) Let $\phi : G \to H$ be a homomorphism. Then

1. $\phi(1_G) = 1_H$ (the identity of G is mapped to the identity of H).
2. $\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in G$.

Proof. Observe that

1. $1 \cdot \phi(1) = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$. Then the (right) cancellation law gives that $1 = \phi(1)$.
2. $\phi(x^{-1})\phi(x) = \phi(x^{-1}x) = \phi(1) = 1$ and $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1) = 1$. Therefore, by definition, $\phi(x^{-1}) = \phi(x)^{-1}$.

□

Example 10. (Example of facts about homomorphisms) Take $\sigma = (123) \in S_3$. Define $\phi : \mathbb{Z}/3\mathbb{Z} \to S_3$ by $\phi(t) = \sigma^t$. Then $\phi(0) = id$ (we expected this from the above claim), $\phi(1) = \sigma$, $\phi(2) = \sigma^2$.

Claim 5. Let $\phi : G \to H$ be a homomorphism. Then $Im(\phi) = \{\phi(g) | g \in G\} \leq H$.

Proof. Let's check the axioms required for $Im(\phi)$ to be a subgroup.

1. Identity: Take $1 \in G$, then $\phi(1) = 1 \in Im(\phi)$.
2. Closed under products: $\phi(a)\phi(b) = \phi(ab) \in Im(\phi)$.
3. Closed under inverses: $\phi(a)^{-1} = \phi(a^{-1}) \in Im(\phi)$.

Therefore $Im(\phi)$ is a subgroup. $\square$

Example 11. (The group $n\mathbb{Z}$) For $n \geq 1$, define $n\mathbb{Z} = \{k \in \mathbb{Z} : k \text{ is divisible by } n\}$. Observe that $n\mathbb{Z} \leq \mathbb{Z}$. Let's check the axioms:

1. Identity: $0 \in n\mathbb{Z}$ because 0 is divisible by everything.
2. Closed under products: If x, y are divisible by n, then xy will also be divisible by n.
3. Closed under inverses: If x is divisible by n, then $-x$ is divisible by n.

Example 12. (Another homomorphism) Define $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\phi(k)$ is the remainder upon dividing k by n (clearly this remainder is in the set $\mathbb{Z}/n\mathbb{Z}$). Then ϕ is a homomorphism. We need to show that $\phi(a+b) = a+b$.

Observations about this example: Note that for each $k \in n\mathbb{Z}$, $\phi(k) = 0$. Moreover $\{k \in \mathbb{Z} : \phi(k) = 0\} = n\mathbb{Z}$. This motivates the following definition.

Definition 8. (Kernel) Let $\phi : G \to H$ be a homomorphism. Then

$$\ker(\phi) = \{g \in G : \phi(g) = 1\} \tag{10}$$

(note that 1 is the identity of H).

Claim 6. Let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi) \leq G$. That is, the kernel of ϕ is a subgroup of G.

Proof. Let's check the 3 axioms required to be a subgroup:

1. Identity: Since ϕ is a homomorphism, we know that $\phi(1_G) = 1_H$. Therefore $1_G \in \ker(\phi)$.
2. Closed under products: Let $a, b \in \ker(\phi)$. We want to show that $ab \in \ker(\phi)$, which means that $\phi(ab) = 1$. Then

   $$\phi(ab) = \phi(a)\phi(b) = 1 \cdot 1 = 1 \tag{11}$$

   Therefore $ab \in \ker(\phi)$ so that $\ker(\phi)$ is closed under products.
3. Closed under inverses: Let $a \in \ker(\phi)$. Then

   $$\phi(a^{-1}) = \phi(a)^{-1} = 1^{-1} = 1 \tag{12}$$

   Therefore $a^{-1} \in \ker(\phi)$.

$\square$

Example 13. (Examples of Kernels) The following are examples of kernels of homomorphisms:

1. The determinant is a homomorphism from $GL_n(\mathbb{R})$ to $\mathbb{R}^\times$. Then

$$\ker(\det) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\} \tag{13}$$

2. $\phi : S_3 \to \{\pm 1\}$ is a homomorphism. Define ϕ as

$$\begin{aligned}
&\phi(123) = \phi(132) = 1 \\
&\phi(12) = \phi(13) = \phi(23) = -1 \\
&\phi(id) = 1
\end{aligned}$$

   Then $\ker(\phi) = \{(123), (132), id\}$.

1.4 Cosets and Lagrange's Theorem

Example 14. (Equivalence Relation) Let G be a finite group and let $H \leq G$. Define a relation $\sim$ on G by $a \sim b$ if and only if there exists an $h \in H$ such that $a = bh$. This condition also means that $b^{-1}a \in H$. We show that $\sim$ is indeed an equivalence relation:

1. Reflexive ($\forall a \in G, a \sim a$): One way to see this is to recall that since H is a subgroup, we know that $a^{-1}a = 1 \in H$. Or simply, $a = a \cdot 1$ and $1 \in H$.

2. Symmetric ($\forall a, b \in G, a \sim b \implies b \sim a$): $a \sim b$ implies $b^{-1}a \in H$. We know that then $(b^{-1}a)^{-1} = a^{-1}b \in H$. Therefore $b \sim a$.

3. Transitive ($\forall a, b, c \in G, a \sim b, b \sim c \implies a \sim c$): $a \sim b$ implies $b^{-1}a \in H$ and $b \sim c$ implies $c^{-1}b \in H$. H is a subgroup, so it's closed under products. Thus $c^{-1}bb^{-1}a \in H$ or that $c^{-1}a \in H$. Therefore $a \sim c$.

Then let $[a] = \{b \in G | b \sim a\} = \{b \in G | \exists h \in H, b = ah\} = \{ah | h \in H\} = aH$. G can be written as a disjoint union of equivalence classes.

Definition 9. (Coset) Let $H \leq G$ and fixed $a \in G$. Let

$$\begin{aligned}
aH &= \{ah | h \in H\} \\
Ha &= \{ha | h \in H\}
\end{aligned}$$

These sets are called a left coset and right coset of H in G.

Write G/H for the set of left cosets $\{aH | a \in G\}$.

Example 15. (Cosets) If $a = 1$, then $aH = 1 \cdot H = H$. And, for any $a \in H$, $aH = H$: First observe that $aH \subset H$ since H is a subgroup. Indeed if $a, h \in H$, then $ah \in H$. Next we'll show $H \subset aH$. Fix $h \in H$. We want to show that $h \in aH$, or that it can written in the form $a'h'$ where $h' \in H$. To achieve this, write $h = e \cdot h = a(a^{-1}h)$. Note that $a^{-1}h \in H$ since H is a subgroup. Therefore $h \in aH$. Together these equivalences show that $aH = H$ when $a \in H$.

Claim 7. (All left cosets of H have the same size) Let $H \leq G$ be groups and let $a \in G$. Then $|[a]| = |aH| = |H|$

Proof. We can give a bijection between the two sets to show they have the same number of elements. To that end, define $f : H \to aH$ by $f(h) = ah$.

1. f is injective: Fix $h_1, h_2 \in H$ such that $f(h_1) = f(h_2)$. Then $ah_1 = ah_2$. Use the left cancellation law see that $h_1 = h_2$.

2. f is surjective: We need to show that for all $h' \in aH$ there exists an $h \in H$ such that $f(h) = h'$. Consider $h = a^{-1}h'$. Then $f(a^{-1}h') = aa^{-1}h' = h'$.

Thus f is a bijection. This result of course implies that $|aH| = |bH| = |H|$ for all $a, b \in H$. In words, all left cosets of H have the same size as H. □

Theorem 1. (Lagrange) Let G be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.

Proof. Using the above claim, define $f : H \to aH$ by $f(h) = ah$. Then it follows that $|[a]| = |aH| = |H|$. We can write G as a disjoint union of equivalence classes. Let k be the number of equivalence classes, and observe that they all have the same cardinality of as H. Therefore $|G| = k \cdot |H|$, so that $|H| \mid |G|$. □

Definition 10. (Index) If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the index of H in G and is denoted by $|G : H|$. Alternatively, $|G : H| = |G/H| = |\{aH | a \in G\}|$. If G is finite, the $|G : H| = \frac{|G|}{|H|}$.

Example 16. (Index when G finite) Let $G = S_3$ and $H = \{(123), (132), id\}$. H is a subgroup. Since G is finite, we can calculate the index of H in G as

$$|G : H| = \frac{|G|}{|H|} = \frac{6}{3} = 2 \tag{14}$$

Thus there are 2 left cosets of H in G. To write out G/H we need only find one other left coset other than the trivial coset. To do this, we can pick an element of G that is not in H. Then observe that

$$G/H = \{H, (12)H\} \tag{15}$$

You can verify that $(12)H = (13)H = (23)H$.

Example 17. (Index when G infinite) $\mathbb{R}_{>0} \subset \mathbb{R}^\times$. Then $|\mathbb{R}^\times : \mathbb{R}_{>0}| = 2$. Recall that this means that there are two left cosets of $\mathbb{R}_{>0}$ in $\mathbb{R}^\times$. We can enumerate these as follows

$$\mathbb{R}^\times / \mathbb{R}_{>0} = \{\mathbb{R}_{>0}, (-1) \cdot \mathbb{R}_{>0}\} \tag{16}$$

We can make an observation about the left cosets of $\mathbb{R}_{>0}$ more generally:

$$a\mathbb{R}_{>0} = sgn(a) \cdot \mathbb{R}_{>0} \tag{17}$$

Example 18. (Index of Permutation Group) As a slight abuse of notation, let S_3 be the set of permutations in S_4 for which the last index is fixed. Then, since S_3 is finite

$$|S_4 : S_3| = \frac{24}{6} = 4 \tag{18}$$

Therefore S_4/S_3 has 4 elements. To find the left cosets of S_3 in S_4, look for elements of S_4 that aren't in S_3. Intuitively, these are the permutations that *don't* fix 4. We can enumerate the left cosets as

1. $C_1 = \{\sigma \in S_4 | \sigma(4) = 4\}$ (this is the trivial coset)
2. $C_2 = \{\sigma \in S_4 | \sigma(4) = 3\}$
3. $C_3 = \{\sigma \in S_4 | \sigma(4) = 2\}$
4. $C_4 = \{\sigma \in S_4 | \sigma(4) = 1\}$

Note that we can write each of these cosets as (using C_2 as an example): τS_3, where $\tau(4) = 3$. We can pick any such τ that satifies this requirement, and the left cosets generated by the different choices of τ will be the same.

Definition 11. (Normal Subgroup) We say that a subgroup H of G is normal if $aH = Ha$ for every $a \in G$. Write $H \trianglelefteq G$. This means that the left and right cosets of a group of equivalent.

Claim 8. (Equivalent conditions to be a normal subgroup) Let $N \leq G$. Then $N \trianglelefteq G$ if one of the following holds:

1. $\forall g \in G, gN = Ng$
2. $\forall g \in G, gNG^{-1} = N$
3. $\forall g \in G, gNg^{-1} \subseteq N$
4. $\forall g \in G$ and $\forall n \in N, gng^{-1} \in N$

Example 19. (Non-example of a Normal Subgroup) Continuing the above example, let S_3 be the set of permutations in S_4 for which the last index is fixed [[Incomplete]].

Claim 9. (The Kernal of a Homomorphism is a Normal Subgroup) Let $\phi : G \to H$ be homomorphism. Then $\ker(\phi) \trianglelefteq G$.

Proof. (Easier Proof) We've already shown that $\ker \phi$ is a subgroup of G. To show that it is a normal subgroup, we will show that $gkg^{-1} \in \ker \phi$ for all $g \in G$ and $k \in \ker \phi$. This is equivalent to showing that $\phi(gkg^{-1}) = 1$ for all $g \in G$ and $k \in \ker \phi$. Then

$$\begin{aligned}
\phi(gkg^{-1}) &= \phi(g)\phi(k)\phi(g^{-1}) \\
&= \phi(g)\phi(g)^{-1} \\
&= 1
\end{aligned}$$

Therefore $gkg^{-1} \in \ker\phi$ for all $g \in G$ and $k \in \ker\phi$, so that $\ker\phi$ is a normal subgroup of G. $\square$

Proof. (Harder Proof) We will show that for all $a \in G$,

$$a\ker\phi = \{g \in G|\phi(g) = \phi(a)\} = \ker\phi a \tag{19}$$

Let $S = \{g \in G|\phi(g) = \phi(a)\}$ and fix and $a \in G$.

Let $at \in a\ker\phi$. Then

$$\phi(at) = \phi(a)\phi(t) = \phi(a) \tag{20}$$

Thus $a\ker\phi \subset S$.

Next let $g \in S$. Therefore $\phi(g) = \phi(a)$, so that $\phi(a^{-1})\phi(g) = 1 = \phi(a^{-1}g)$. Therefore $a^{-1}g \in \ker\phi$, so that $S \subset a\ker\phi$.

The proof for the right cosets is similar. Together, these inclusions show that $\ker\phi$ is a normal subgroup. $\square$

1.5 Cyclic Groups

Definition 12. (Cyclic Group) A group H is cyclic if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n|n \in \mathbb{Z}\}$. Write $H = \langle x \rangle$ and say H is generated by x.

An alternative definition is: Let G be a group and fix $x \in G$. Let H be the subset of G that contains all the powers of x. Then notice that $H = \{x^n|n \in \mathbb{Z}\}$ is a subgroup of G (the identity element must be in H since $x^0 = 1$, H is closed under products since adding exponents will keep us in H, and the inverse of x^n is x^{-n}, which is also in H). We call H the subgroup of G generated by x, $H = \langle x \rangle$, and H is cyclic.

Example 20. (Examples of Cyclic Groups)

1. Let $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$. Then

$$\langle x \rangle = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| n \in \mathbb{Z} \right\} \tag{21}$$

   You can see that taking positive powers of x continually increases the element in the upper-right hand corner. Finally, observe that

$$x^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \tag{22}$$

   Therefore the powers of the inverse of x are also included in $\langle x \rangle$.

2. Let $x = 3 \in \mathbb{Z}/6\mathbb{Z}$. Then $\langle x \rangle = \{0, 3\}$.

Claim 10. (Every cyclic group is isomorphic to either $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$.) For every group H for which there exists an $x \in H$ such that $H = \langle x \rangle$, there exists a bijective homomorphism (i.e. an isomorphism) $\phi : H \to C$ where $C = \mathbb{Z}$ or $C = \mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$.

Proof. There are two cases to consider.

1. The powers of x are distinct: Define $\phi : H \to \mathbb{Z}$ by $\phi(x^n) = n$. ϕ is bijective by construction. To check that ϕ is indeed a homomorphism, observe that

$$\phi(x^n \cdot x^m) = \phi(x^{n+m}) = n + m = \phi(x^n) + \phi(x^m) \tag{23}$$

2. The powers of x are not distinct: Suppose there is some $m \neq n$ such that $x^m = x^n$ (without loss of generality assume $m \leq n$). Then since $x^m = x^n$, we find that $x^m x^{-m} = x^n x^{-m}$. Therefore $x^{n-m} = 1$. Since there is some finite power of x that equals the identity, let k be the order of x. Define $\phi : H \to \mathbb{Z}/k\mathbb{Z}$ by $\phi(x^m) = r$, where r is the remainder upon dividing m by k. Surjectivity is clear by definition. To show ϕ is injective, we can use the fact that since ϕ is a homomorphism, it is injective if and only if $\ker \phi = 1$. Then

$$\begin{aligned} \ker \phi &= \{x^r : \phi(x^r) = 0\} \\ &= \{x^r : k \text{ divides } r\} \\ &= \{x^{kt} : t \in \mathbb{Z}\} \\ &= \{1\} && \text{(since } k \text{ is the order of } x\text{)} \end{aligned}$$

□

Claim 11. Let G be a finite cyclic group of order n. For every $m|n$ (m that divides n) there exists a unique subgroup H of G with $|H| = m$. Furthermore, H is cyclic.

Proof. Assume that $G = \mathbb{Z}/n\mathbb{Z}$. This is without generality since G is a finite cyclic group, and every finite cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Definite $H = \langle \frac{n}{m} \rangle$, Indeed, $H = \{0, \frac{n}{m}, \frac{2n}{m}, \ldots, \frac{(m-1)n}{m}\}$, and $|H| = m$. □

1.6 Dihedral Groups

For each $n \geq 3$, let D_n be the set of symmetries of the regular n-gon. A symmetry is a rigid motion of the n-gon which takes a copy of the n-gon, moves this copy through space, and places the copy back on the original n-gon so it exactly covers it.

In general, we consider two types of symmetries:

1. Rotational symmetries (denoted ρ)

2. Mirror symmetries (denoted by ϵ). There is a distinction in the mirror symmetries when n is even and when n is odd. When n is odd, the mirror symmetries (i.e. the line of symmetry in this case) all have the same form of starting from a vertex and going to the mid-point of the edge opposite of the vertex. When n is even, the lines of symmetry either go from a vertex to a vertex or from a mid-point of an edge to the mid-point of an edge.

For a regular n-gon, there are n rotational symmetries and n mirror symmetries. Therefore $|D_n| = 2n$.

Example 21. (D_3, Symmetries of a Triangle)

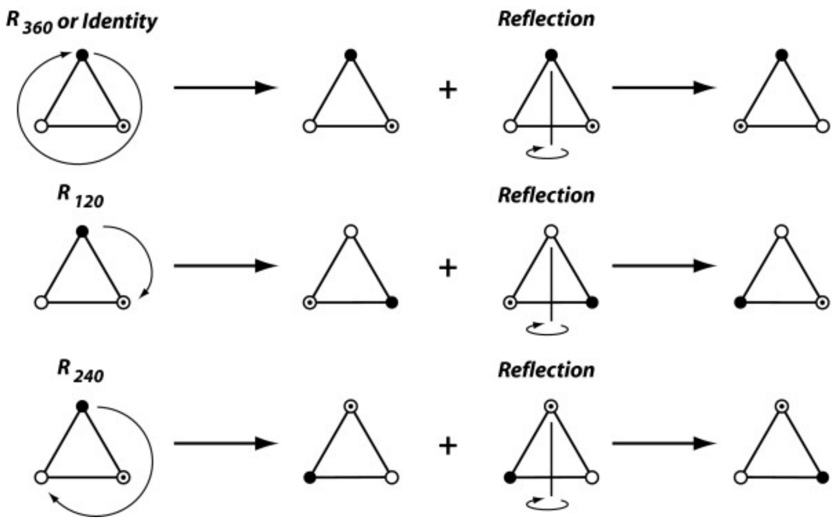

Figure 1: The symmetries of an equilateral triangle

Example 22. (D_4, Symmetries of a Square)

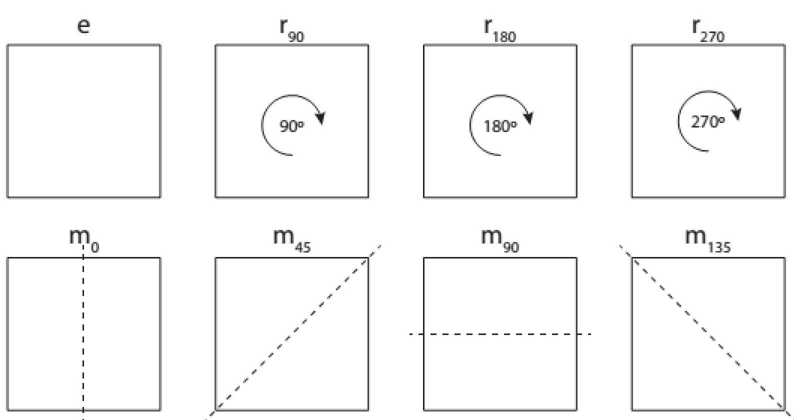

Figure 2: The symmetries of a square

Definition 13. (Dihedral Group, D_n) In general, D_n is a group with $2n$ elements, where the binary operation is composition. It contains two types of symmetries:

1. The rotation ρ is $\frac{2\pi}{n}$ radians clockwise. The set of all rotations is $\langle \rho \rangle = \{1, \rho, \rho^2, \ldots, \rho^{n-1}\}$.
2. Let ϵ be a vertical mirror symmetry. Then the set of all mirror symmetries is $\{\epsilon, \epsilon\rho, \epsilon\rho^2, \ldots, \epsilon\rho^{n-1}\}$.

Claim 12. (Important Identity) $\rho\epsilon = \epsilon\rho^{-1}$.

We use this relation to make computations in dihedral groups.

Claim 13. $\rho^i\epsilon = \epsilon\rho^{-i}$

Proof. By induction, using the above claim. □

Example 23. (Uniqueness of rotations/mirror symmetries) Can two elements in the mirror symmetry set be equal, or equal to an element in the set of rotations? No! Suppose $\epsilon\rho^i = \epsilon\rho^j$. Then $\rho^i = \rho^j$, which implies $i = j$. Now suppose $\epsilon\rho^i = \rho^j$, which implies $\epsilon = \rho^{j-i}$. However this implies ϵ is a rotation, which is nonsense.

Example 24. (Mirror Symmetries are a Coset) Observe that the set of mirror symmetries is simply $\epsilon\langle\rho\rangle$, thus they are a left coset of the cyclic group of rotations. Then

$$D_n/\langle\rho\rangle = \{\langle\rho\rangle, \epsilon\langle\rho\rangle\} \tag{24}$$

Since $|D_n| = 2n$ and $|\langle\rho\rangle| = n$, we know that by Lagrange's theorem, $[D_n : \langle\rho\rangle] = 2$.

Example 25. In D_5, compute (simplify)

$$\rho\epsilon^7\rho\epsilon\rho^2\epsilon\rho^{-3}\epsilon^{-1} \tag{25}$$

We know that $\rho\epsilon = \epsilon\rho^{-1}$, $\rho^5 = 1$, and $\epsilon^2 = 1$. Then, with the strategy of pushing ϵ to the left,

$$\begin{aligned}
\rho\epsilon^7\rho\epsilon\rho^2\epsilon\rho^{-3}\epsilon^{-1} &= \rho\epsilon\rho\epsilon\rho^2\epsilon\rho^2\epsilon && (\rho^{-3} = \rho^2, \epsilon^{-1} = \epsilon) \\
&= \rho\epsilon\rho\epsilon\rho^2\epsilon\rho\epsilon\rho^{-1} \\
&= \rho\epsilon\rho\epsilon\rho^2\epsilon\epsilon\rho^{-1}\rho^{-1} \\
&= \rho\epsilon\rho\epsilon\rho^2\rho^{-1}\rho^{-1} \\
&= \rho\epsilon\rho\epsilon \\
&= \rho\epsilon\epsilon\rho^{-1} \\
&= 1
\end{aligned}$$

1.7 Quotient Groups

Definition 14. (Quotient Group) Let G be a group and $N \trianglelefteq G$ (that is, N is a normal subgroup of G). Let $G/N = \{gN | g \in G\}$ be the set of left cosets of N in G. Then the quotient group of G by N is the group $(G/N, \cdot)$, where $\cdot$ is the binary operation on G/N defined for all $g_1N, g_2N \in G/N$ by $g_1Ng_2N = g_1g_2N$.

Claim 14. In the above definition, G/N is a group.

Proof. Binary operation well-defined: We need to check that $\cdot : G/N \times G/N \to G/N$, where $(g_1N, g_2N) \to g_1g_2N$ is well-defined (A function is well-defined if it gives the same result when the representation of the input is changed without changing the value of the input. In this context, we show that the definition of multiplication depends on only the cosets and not on the coset representatives). Suppose that $g_1N = g_1'N$ and $g_2N = g_2'N$, so we want to show $g_1g_2N = g_1'g_2'N$. Then $g_1N = g_1'N \iff (g_1')^{-1}g_1 \in N$ and $g_2N = g_2'N \iff (g_2')^{-1}g_2 \in N$. We then want to show $(g_1'g_2')^{-1}g_1g_2 \in N$. Then

$$
\begin{aligned}
(g_1'g_2')^{-1}g_1g_2 &= (g_2')^{-1}(g_1')^{-1}g_1g_2 \\
&= (g_2')^{-1}ng_2 && (n = (g_1')^{-1}g_1 \in N) \\
&= (g_2')^{-1}ng_2'(g_2')^{-1}g_2 \\
&= (g_2')^{-1}ng_2'n' && (n' = (g_2')^{-1}g_2 \in N) \\
&= (g_2')^{-1}g_2'n''n' && (N \text{ is normal}) \\
&= n''n' \in N
\end{aligned}
$$

Therefore the binary operation is indeed well-defined.

We now check the axioms required to be a group.

1. Identity: Observe that
$$1 \cdot N = N \tag{26}$$

2. Inverse: Observe that
$$(gN)^{-1} = g^{-1}N \tag{27}$$
because
$$gNg^{-1}N = gg^{-1}N = N \tag{28}$$

3. Associativity: Follows clearly from the associativity of G.
$$
\begin{aligned}
(g_1Ng_2N)(g_3N) &= (g_1g_2N)(g_3N) \\
&= g_1g_2g_3N \\
&= (g_1N)(g_2g_3N) \\
&= (g_1N)(g_2Ng_3N)
\end{aligned}
$$

Therefore G/H is a group. □

Example 26. (Examples of Quotient Groups)

1. $\mathbb{R}^\times/\mathbb{R}_{>0} = \{\mathbb{R}_{>0}, (-1)\cdot\mathbb{R}_{>0}\} \cong \{\pm 1\}$

2. $\mathbb{Z}/12\mathbb{Z} = \{0 + 12\mathbb{Z}, 1 + 12\mathbb{Z}, \ldots, 11 + 12\mathbb{Z}\}$

3. $(\mathbb{Z}/12\mathbb{Z})/\{0, 4, 8\} \cong \mathbb{Z}/4\mathbb{Z}$. Thus this quotient group has 4 elements (we can also see this from Lagrange's theorem). Also observe that this is a cyclic group.

1.8 Isomorphism Theorems

Theorem 2. (The First Isomorphism Theorem) If $\phi : G \to H$ is a homomorphism of groups, then $G/\ker(\phi) \cong Im\phi$.

Proof. Define $f : G/\ker(\phi) \to Im\phi$ by $f(a\ker(\phi)) = \phi(a)$. We first show f is indeed well-defined. To that end, pick $a\ker(\phi) = b\ker(\phi)$. Therefore there exists some $k \in \ker(\phi)$ such that $a = bk$. Then

$$\phi(a) = f(a\ker(\phi)) = f(bk\ker(\phi)) = f(b\ker(\phi)) = \phi(b) \tag{29}$$

Therefore f is well-defined. We now show f is an isomorphism.

1. f is a homomorphism:

$$\begin{aligned} f(a\ker(\phi)b\ker(\phi)) &= f(ab\ker(\phi)) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) && (\phi \text{ is a homomorphism}) \\ &= f(a\ker(\phi))f(b\ker(\phi)) \end{aligned}$$

2. f is surjective: Let $\phi(a) \in Im\phi$. Then $f(a\ker\phi) = \phi(a)$.

3. f is injective:

$$\begin{aligned} \ker(f) &= \{a\ker\phi : f(a\ker\phi) = 1_H\} \\ &= \{a\ker\phi : \phi(a) = 1_H\} \\ &= \{\ker\phi\} \end{aligned}$$

   Thus the kernal of f is trivial (the trivial left coset), so f is injective.

Therefore f is an isomorphism. □

Intuition for this theorem:

- This is a more general version of the rank-nullity theorem.
- Given vector spaces V, W and a linear transformation $A : V \to W$, this theorem says

$$dim(V/\ker A) = dim(range(A)) \tag{30}$$

  or that

$$dim(V) - nullity(A) = rank(A) \tag{31}$$

Example 27. (Examples of applications of first isomorphism theorem) Consider the following examples

1. $sgn : \mathbb{R}^{\times} \to \{\pm 1\}$. This is indeed a homomorphism. By the theorem, we know that

$$\mathbb{R}^{\times} / \ker(sgn) \cong \{\pm 1\} \tag{32}$$

   Then $\ker(sgn) = \mathbb{R}_{>0}$. This matches the previous example.

2. $\det : GL_2(\mathbb{R}) \to \mathbb{R}^{\times}$. The theorem implies

$$GL_2(\mathbb{R}) / \{A \in GL_2(\mathbb{R}) | \det(A) = 1\} \cong \mathbb{R}^{\times} \tag{33}$$

Theorem 3. (The Second or Diamond Isomorphism Theorem) Let $H \leq G$ and $K \trianglelefteq G$. Then $HK/K \cong H/H \cap K$.

Proof. Define $f : HK/K \to H/H \cap K$ by

$$f(hkK) = h(H \cap K) \tag{34}$$

We'll first show f is well-defined. Fix $hk, h'k' \in HK$ such that $hkK = h'k'K \in HK/K$. There $h = h'\tilde{k}$ for some $\tilde{k} \in K$. Then

$$h(H \cap k) = f(hkK) = f(h'\tilde{k}K) = h'(H \cap K) \tag{35}$$

Therefore f is well-defined, and we now show f is an isomorphism.

1. f is a homomorphism:

$$\begin{aligned} f(h_1k_1K \cdot h_2k_2K) &= f(h_1K \cdot h_2K) \\ &= f(h_1h_2K) \\ &= h_1h_2(H \cap K) \\ &= h_1(H \cap K)h_2(H \cap K) \\ &= f(h_1k_1K)f(h_2k_2K) \end{aligned}$$

2. f is surjective: Clear by the definition of f.

3. f is injective: We'll show the kernal of f is trivial (in this context, the trivial left coset).

$$\begin{aligned} \ker(f) &= \{hk \cdot K | f(hk \cdot K) = H \cap K\} \\ &= \{hk \cdot K | h(H \cap K) = H \cap K\} \\ &= \{hk \cdot K | h \in H \cap K\} && (h(H \cap K) = H \cap K \iff h \in H \cap K) \\ &= \{K\} \end{aligned}$$

□

1.9 Actions, Orbits, and Stabilizers

Definition 15. (Action) An action of a group G on X (or we say G acts on X) is a function $G \times X \to X$, $(g, x) \to gx$ where

1. $1_G x = x \quad \forall x \in X$
2. $g(hx) = (gh)x \quad \forall g, h \in G, \forall x \in X$

Example 28. (Group Actions)

1. Set: $\mathbb{R}^n$, Group: $GL_n(\mathbb{R})$, Action: $(A, v) \to Av$. In $\mathbb{R}^2$, we can see that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} av_1 + bv_2 \\ cv_1 + dv_2 \end{pmatrix} \in \mathbb{R}^2 \tag{36}$$

   Observe that the two axioms required to be an axiom are satisfied, since the identity matrix preserves vectors and matrix/vector multiplication is associative.

2. Set: $\{1, \ldots, n\}$, Group: S_n, Action: $(\sigma, i) \to \sigma(i)$. Observe that the two axioms are satisfied. The identity permutation fixes an index and the composition of permutations is associative.

3. Set: G, Group: G, Action: $(g, h) \to gh$. The identity element of G maps $1_G h = h$ and since G is a group, multiplication is associative.

4. Set: G, Group: G, Action: $(g, x) \to gxg^{-1}$. Let's verify the axioms:

   (a) Suppose $g = 1$. Then $(1, x) \to 1x1^{-1} = x$.

   (b) Observe that
$$g(h(x)) = g(hxh^{-1}) = g(hxh^{-1})g^{-1} \tag{37}$$
   and
$$(gh)(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} \tag{38}$$

5. Set: Set of all subgroups of G, Group: G, Action: $(g, H) \to gHg^{-1}$. We need to show that gHG^{-1} is a subgroup if H is a subgroup (this shows that $G \times (subgroup) \to (subgroup)$). Let's verify the axioms required to be a subgroup:

   (a) Identity: Note that $1 \in H$ since $H \leq G$. Thus $g1g^{-1} = 1 \in gHg^{-1}$.

   (b) Closed under products: Let $ghg^{-1}, gh'g^{-1} \in gHg^{-1}$. Then

$$\begin{aligned} (ghg^{-1})(gh'g^{-1}) &= ghh'g^{-1} \\ &= g\tilde{h}g^{-1} \in gHg^{-1} \qquad (H \text{ closed under multiplication}) \end{aligned}$$

   (c) Closed under inverses: Note that $(ghg^{-1})^{-1} = gh^{-1}g^{-1} \in H$ since H is closed under inverses.

Therefore gHg^{-1} is a subgroup. Now, let's verify the axioms to should this is indeed an action [[?]]:

(a) $1gHg^{-1} = gHg^{-1}$

(b) ??

6. Set: Pairs of distinct elements from $\{1, \ldots, n\}$, Group: S_n, Action: $\sigma(i, j) = (\sigma(i), \sigma(j))$.

Definition 16. (Orbit) Given $x \in X$ the orbit of x is

$$O(x) = O_x = \{gx | g \in G\} \tag{39}$$

This is the set of all elements that can be reached from x by applying elements from G.

Example 29. (Examples of Orbits)

1. Let $X = \{1, \ldots, n\}$. Suppose $G = S_n$. Then the orbit of each element is the whole set, X.

2. H is normal if and only if all if its orbits only contain one element [[?]].

Definition 17. (Stabilizer) The stabilizer of x is

$$G_x = Stab_G(x) = \{g \in G | gx = x\} \tag{40}$$

Claim 15. (The stabilizer of a group element in a subgroup) $G_x \leq G$

Proof. We verify the three axioms required to be a subgroup:

1. Identity: Note that $1x = x$, therefore $1 \in G_x$.

2. Closed under products: Let $a, b \in G_x$. We need to show that $ab \in G_x$, or that $(ab)x = x$. Then,
$$(ab)x = a(bx) = ax = x \tag{41}$$

3. Closed under inverses: Let $a \in G_x$. We know $ax = x$. Therefore, applying a^{-1} on the left, we get that $a^{-1}ax = a^{-1}x$. This simplifies to $x = a^{-1}x$. Thus $a^{-1} \in G_x$.

Thus G_x is a subgroup. $\square$

Theorem 4. (Orbit-Stabilizer Theorem) There is a bijection

$$f : G/G_x \to O_x \tag{42}$$

In words, there is a bijection between the collection of all cosets of the stabilizer and the orbit. In particular,

$$[G : G_x] = |O_x| \tag{43}$$

(Recall we defined $|G/G_x|$ to be $[G : G_x]$).

Proof. Define

$$f : G/G_x \to O_x \tag{44}$$

by

$$f(gG_x) = gx \tag{45}$$

We will first verify that f is well-defined. In this context, this means that the output of the function does not depend on what representative from the left coset is chosen. To that end, suppose $gG_x = hG_x$. We need to show that $gx = hx$. Equivalently, we need to show that $h^{-1}gx = x$, or that $h^{-1}g \in G_x$ (the stabilizer of x). However, this last characterization follows directly from the assumption that

$$gG_x = hG_x \tag{46}$$

We now show that f is subjective. This is clear from the definition of the function. To get an element gx, we simply need to input g.

We now show that f is injective (note here that f is not a homomorphism. Thus we cannot use the trick that f is injective if and only if its kernel is trivial). Suppose that $f(gG_x) = f(hG_x)$. Hence, $gx = hx$, so $h^{-1}gx = x$. Therefore, $h^{-1}g \in G_x$, which implies that $gG_x = hG_x$. □

Example 30. (Examples of Orbit-Stabilizer Theorem)

1. Suppose D_3 acts on the vertices of a triangle. That is, $G = D_3$ and $X = \{a, b, c\}$. Observe that $O_a = \{a, b, c\}$, because a rotation allows us to reach any other vertex starting from a. Next, $G_a = \{1, \text{ reflection at } a\}$. Observe that

$$[G : G_a] = \frac{|G|}{|G_a|} = \frac{6}{2} = 3 \tag{47}$$

   and

$$|O_a| = 3 \tag{48}$$

   Therefore the theorem holds.

2. Suppose S_5 acts on $\{1, 2, 3, 4, 5\}$. Then

$$G_5 \cong S_4 \tag{49}$$

   In words, the stabilizer of 5 is simply the set of permutations that keep 5 fixed, which is equivalent to the set of permutations of $\{1, 2, 3, 4\}$. Note that $O_5 = \{1, 2, 3, 4, 5\}$. And

$$[G : G_5] = \frac{|S_5|}{|G_5|} = \frac{120}{24} = 5 \tag{50}$$

   and

$$|O_5| = 5 \tag{51}$$

   Therefore the theorem holds.

Definition 18. (Transitive action) We say that an action of G on X is transitive if for every $x, y \in X$, there is an element $g \in G$ such that $gx = y$. In words, this means that we can arrive at y from x by applying an element from G.

Example 31. (Transitive actions)

1. The action of S_5 on $\{1, 2, 3, 4, 5\}$ is transitive.
2. The action of $GL_n(\mathbb{R})$ on $\mathbb{R}^n$ is not transitive. Consider the zero vector. Then any matrix we apply to the zero vector will still give us the zero vector. Thus, we cannot reach another vector in $\mathbb{R}^n$.
3. The multiplication action of G on itself is transitive. To get to y from x, we can apply $g = yx^{-1}$.

Definition 19. (Action induces equivalence relation) The action of any group G on X induces an equivalence relation by saying $x \sim y$ if there exists a $g \in G$ such that $gx = y$.

Proof. We'll show that this is indeed an equivalence relation. We need to verify three axioms:

1. Reflexive: We want to show that $x \sim x$. Let $g = 1$. Then $1 \cdot x = x$.
2. Symmetric: Suppose $x \sim y$. We want to show that $y \sim x$. Since $x \sim y$, there exists a $g \in G$ such that $gx = y$. This implies $x = g^{-1}y$. Therefore $y \sim x$.
3. Transitive: Suppose $x \sim y$ and $y \sim z$. We want to show that $x \sim z$. By definition, there exist $g, h \in G$ such that $gx = y$ and $hy = z$. Thus $hgx = z$. Since the binary operation of G is closed, we know $gh \in G$, so that $x \sim z$.

□

Remark 1. The equivalence class of $x \in X$ is the orbit of x, O_x.

Claim 16. An action is transitive if and only if there exists an $x \in X$ such that $O_x = X$. That is, all elements of X have the same equivalence class.

Proof. TODO □

Definition 20. (Conjugation action, conjugacy classes, conjugate) Consider the action of G on itself by $g(x) = gxg^{-1}$. We call this the conjugation action. The equivalence classes created by this action are called the conjugacy classes of G. We say that two elements in $x, y \in G$ are conjugate if they belong to the same conjugacy class.

Example 32. In S_5, the elements $(12)(34)$ and $(52)(13)$ are conjugate. In other words, there exists a $\sigma \in S_5$ such that

$$\sigma(12)(34)\sigma^{-1} = (52)(13) \tag{52}$$

One σ that works is

$$\sigma(1) = 5, \quad \sigma(2) = 2, \quad \sigma(3) = 1, \quad \sigma(4) = 3, \quad \sigma(5) = 4 \tag{53}$$

We can generate this σ by recalling that

$$\begin{aligned}\sigma(12)(34)\sigma^{-1} &= \sigma(12)\sigma^{-1}\sigma(34)\sigma^{-1} \\ &= (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))\end{aligned}$$

Thus we want to choose a σ such that these two cycles are equivalent to the two given cycles.

Definition 21. (Fixed points) For any element $g \in G$, let $X^g = \{x \in X | gx = x\}$. In words, this is the set of all elements in X such that g acts on them like the identity.

Example 33. (Fixed points)

1. Let $G = D_3$ and $X = \{a, b, c\}$ be the vertices of a triangle. Then $X^\rho = \emptyset$. However, the set of fixed points of the reflection through c is simply $\{c\}$.

2. Let $G = GL_2(\mathbb{R})$ and $X = \mathbb{R}^2$. Then

$$\begin{aligned} X^{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}} &= \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2 | \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2 | \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \right\} \\ &\qquad \text{(where the first and second coord are the same)} \\ &= span \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \end{aligned}$$

Theorem 5. (Burnside) Let G act on X. Suppose that G, X are finite. Then,

$$N = \text{ \# of orbits (equivalence classes) } = \frac{1}{|G|} \sum_{g \in G} |X^g| \tag{54}$$

Proof. Let's count

$$|\{(g, x) : gx = x\}| \tag{55}$$

in two ways.

1. By counting "over G" (i.e. how many elements each g contributes): For each g, this simply the number of points g fixes

$$\sum_{g \in G} |X^g| \tag{56}$$

2. By counting "over X": For each x, this is how many elements $g \in G$ that fix x:

$$\sum_{x \in X} |G_x| \tag{57}$$

By the orbit-stabilizer theorem, we know that

$$\frac{|G|}{|G_x|} = |O_x| \tag{58}$$

Therefore

$$\begin{aligned} \sum_{x \in X} |G_x| &= \sum_{x \in X} \frac{|G|}{|O_x|} \\ &= |G| \sum_{x \in X} \frac{1}{|O_x|} \\ &= |G| \sum_{\text{orbits}} \sum_{\text{elements}} \frac{1}{|O_x|} \\ &= |G| \sum_{\text{orbits}} 1 \\ &= |G|N \end{aligned}$$

Equating these two ways of counting the number of elements in the set proves the theorem. □

Exercise 6. In how many ways can one color the vertices of a square using 10 distinct colors? Or, how many orbits are there for the action of D_4 on the set of colorings of the vertices of a square using the colors.

Solution 6. We can use Burnside's theorem to complete this calculation.

Element $g \in G$	$\lvert X^g \rvert$
1	$10^4 = 10000$
ρ	10 (all vertices share same color)
ρ^2	$10^2 = 100$ (opposite vertices share same color)
ρ^3	10 (same as ρ)
Edge Reflection (x2)	$10^2 = 100$ (adjacent vertices across reflection line same)
Vertex Reflection (x2)	$10^3 = 1000$ (vertices not on reflection line same)

Then by Burnside's Theorem, we know that

$$N = \frac{1}{8}(10,000 + 10 + 100 + 10 + 2 \times 100 + 2 \times 1000) \tag{59}$$

Definition 22. (Free, faithful action) Let G be a group that acts on a set X.

1. The action is said to be faithful if for all $x \in X$

$$gx = x \implies g = 1 \tag{60}$$

   Thus the only element that acts like the identity is actually the identity $g = 1$.

2. The action is free if for all $g \in G$ and for all $x \in X$

$$gx = x \implies g = 1 \tag{61}$$

   This means all stabilizers are trivial. Or, any element which has a fixed point is the identity element.

Observations:

- If free, then faithful.

Example 34. (Free, faithful actions)

1. The action of G on itself by left multiplication is free.
2. The action of D_n on the vertices of an n-gon is faithful but not free.
3. Suppose $GL_2(\mathbb{R})$ acts on $\mathbb{R}^2$. This action is not free, but it is faithful. It's not free because the zero vector is always mapped back to the zero vector. It is faithful since $Av = v$ implies A is the identity matrix (to see this, consider $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $v = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$).

2 Quizzes

The course did not give solutions to any quizzes, homeworks, or midterms, so be wary of the solutions I've written below.

2.1 Quiz 1

Exercise 7. Give an example of $\sigma \in S_3$ such that σ has order 3.

Solution 7. Consider $\sigma = (123)$. Then $\sigma^2 = (132)$ and $\sigma^3 = (1)(2)(3)$. Therefore, $\sigma^1 \neq 1$, $\sigma^2 \neq 1$, but $\sigma^3 = 1$. Therefore, by definition, σ has order 3.

Exercise 8. Give an example of $\tau \in S_5$ such that τ has order 6.

Solution 8. Consider $\tau = (123)(45)$. Then $\tau^2 = (132)(4)(5)$, $\tau^3 = (1)(2)(3)(45)$, $\tau^4 = (123)(4)(5)$, $\tau^5 = (132)(45)$, $\tau^6 = (1)(2)(3)(4)(5)$.

2.2 Quiz 2

Exercise 9. Let $\tau \in S_6$. Show that

$$\tau \cdot (54132) \cdot \tau^{-1} = (\tau(5)\tau(4)\tau(1)\tau(3)\tau(2))$$

Solution 9. We can show this element by element. Observe that

$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(5)) = \tau \cdot (54132)(5) = \tau(4) \tag{62}$$

This shows that $\tau \cdot (54132) \cdot \tau^{-1}$ maps $\tau(5)$ to $\tau(4)$. Similarly,

$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(4)) = \tau \cdot (54132)(4) = \tau(1) \tag{63}$$
$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(1)) = \tau \cdot (54132)(1) = \tau(3) \tag{64}$$
$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(3)) = \tau \cdot (54132)(3) = \tau(2) \tag{65}$$
$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(2)) = \tau \cdot (54132)(2) = \tau(5) \tag{66}$$

Therefore $\tau \cdot (54132) \cdot \tau^{-1} = (\tau(5)\tau(4)\tau(1)\tau(3)\tau(2))$.

Exercise 10. Let G be a group and fix $g \in G$. Define $\phi : G \to G$ by $\phi(x) = gxg^{-1}$. Show ϕ is an isomorphism.

Solution 10.

1. ϕ is a homomorphism: Fix $x, y \in G$. Then

$$\begin{aligned}\phi(xy) &= g(xy)g^{-1} \\ &= gxg^{-1}gyg^{-1} \\ &= \phi(x)\phi(y)\end{aligned}$$

2. ϕ is injective: Fix $x, y \in G$, and suppose $\phi(x) = \phi(y)$. Then

$$\phi(x) = gxg^{-1} = gyg^{-1} = \phi(y) \tag{67}$$

   Then use the right and left cancellation laws we get that $x = y$.

3. ϕ is surjective: Fix $y \in G$ and consider $x = g^{-1}yg$. Then

$$\phi(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y \tag{68}$$

   Therefore, for all $y \in G$, we can find an $x = g^{-1}yg$ such that $\phi(x) = y$.

2.3 Quiz 3

Exercise 11. Let G be a group and define $\phi : G \to G$ by $\phi(g) = g^{-1}$ for $g \in G$. Show that ϕ is a homomorphism if and only if G is abelian.

Solution 11.

Exercise 12. Define $H = \{\sigma \in S_5 : \{\sigma(1), \sigma(2), \sigma(3)\} \in \{1,2,3\}\}$. Show that $H \leq S_5$ and calculate $[S_5 : H]$.

Solution 12. Since S_5 is a finite group, we can use Lagrange's theorem to find $[S_5 : H] = \frac{|S_5|}{|H|}$. $|S_5| = 5! = 120$. Then $|H| = 3! \times 2! = 12$. Therefore

3 Exams

3.1 Exam 1

4 Homework Exercises

4.1 Homework 1

Exercise 13. Show that the group S_3 is not abelian.

Solution 13. To show that S_3 is not abelian, we must find an $a, b \in S_3$ such that $ab \neq ba$. To this end, consider the permutations $a(1) = 2, a(2) = 3, a(3) = 1$ and $b(1) = 1, b(2) = 3, b(2) = 2$. Then, $a(b(1)) = 2$ but $b(a(1)) = 3$. Therefore, $ab \neq ba$, so S_3 is not abelian.

Exercise 14. Is the set $\mathbb{R}$ of real numbers with the binary operation of subtraction a group?

Solution 14. No. The associativity axiom fails. To see this, observe that $3 - (2 - 1) = 2$ but $(3 - 2) - 1 = 0$.

Exercise 15. Let G be a group, and take some $g \in G$. Show that the function f from G to itself defined by $f(x) = gx$ is injective (one-to-one).

Solution 15. Recall that f is injective if for all $a, b \in G$, $a \neq b$, we have that $f(a) \neq f(b)$. For the sake of reaching a contradiction, let $a, b \in G$, $a \neq b$, but suppose that $f(a) = f(b)$. Then $ga = gb$, by the definition of f. By the Cancellation Law, we must have that $a = b$, a contradiction.

Exercise 16. Give an example of $\sigma \in S_3$ such that $\sigma \neq 1$ and $\sigma\sigma \neq 1$.

Solution 16. Consider $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$. Then, $\sigma\sigma(1) = 3$. Therefore, $\sigma\sigma \neq 1$.

Exercise 17. Is the set of positive real numbers with the binary operation of multiplication a group?

Solution 17. Yes. Associativity follows from the associativity of the reals. The identity element is 1. Since we've excluded 0, each positive real does have an inverse.

Exercise 18. Show that the set $G = \{z \in \mathbb{C} : z^7 = 1\}$ is a group under multiplication.

Solution 18. We check each of the axioms:

1. Associativity: This follows from the associativity of $\mathbb{C}$.
2. Identity: Observe that $1 \in G$ since $1^7 = 1$. Fix $g \in G$, and under multiplication, $g \star 1 = 1 \star g = g$. Therefore, G has an identity.
3. Inverse: First observe that $0 \notin G$ since $0^7 = 0$. The inverse of $z \in G$ is simply z^{-1}. Since $z \in G$, we know that $z^7 = 1$. Then, $z^{-7} = 1^{-1} = 1$. Therefore, $z^{-7} \in G$ since $z^{-7} = 1$. Then $zz^{-1} = 1$, and the inverse of each $z \in G$ is also in G.
4. Closure of binary operation: Let $a, b \in G$, so that $a^7 = b^7 = 1$. Then $(ab)^7 = a^7 b^7 = 1$. Therefore $ab \in G$. (Remark: To show that $ab \in G$, we need to prove that $(ab)^7 = 1$. Therefore, in our proof, we can start with $(ab)^7$ directly.)

Exercise 19. Let G be a group in which $gg = 1$ for each $g \in G$. Show that G is abelian.

Solution 19. To show that G is abelian we must prove that for all $a, b \in G$, $ab = ba$. To that end, fix $a, b \in G$. Then $aabb = a^2b^2 = 1 \star 1 = 1 = (ab)^2 = abab$. Then by cancellation we have that $ab = ba$.

4.2 Homework 2

Exercise 20. How many elements does the group $S_3 \times \mathbb{Z}/5\mathbb{Z}$ have?

Solution 20. S_3 has $3! = 6$ elements. $\mathbb{Z}/5\mathbb{Z}$ has 5 elements. Thus $S_3 \times \mathbb{Z}/5\mathbb{Z}$ has $6 \times 5 = 30$ elements.

Exercise 21. Find the order of all elements in $\mathbb{Z}/10\mathbb{Z}$.

Solution 21. $|0| = 1$ (the order of an element is 1 iff that element is the identity). $|1| = 10$, $|2| = 5$, $|3| = 10$, $|4| = 5$, $|5| = 2$, $|6| = 5$, $|7| = 10$, $|8| = 5$, $|9| = 10$.

Exercise 22. What is the order of the permutation $(135)(26)(4798)$ in S_{10}?

Solution 22. The order of a permutation is the lcm of the lengths of the cycles in its cycle decomposition. Here, the cycle lengths are 3, 2, and 4. Therefore the order of this permutation is 12.

Exercise 23. Let $\sigma \in S_n$ be a k-cycle, and let $\tau \in S_n$. Prove that $\tau\sigma\tau^{-1}$ is also a k-cycle.

Solution 23. Let $\sigma = (i_1 i_2 \dots i_k)$. We claim that $\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\dots\tau(i_k))$ (which is also a k-cycle). We can calculate each element of $\tau\sigma\tau^{-1}$ to show that this is true. Consider how $\tau\sigma\tau^{-1}$ acts on $\tau(i_1)$:

$$\tau\sigma\tau^{-1}(\tau(i_1)) = \tau(\sigma(i_1)) = \tau(i_2) \tag{69}$$

Thus $\tau\sigma\tau^{-1}$ sends $\tau(i_1)$ to $\tau(i_2)$. A similar pattern holds for the other indices.

Exercise 24. Let $\sigma \in S_n$ be a k-cycle. Is σ^2 necessarily a k-cycle?

Solution 24. No. Consider this simple counterexample: (1234). Then $\sigma^2 = (13)(24)$. σ^2 is not a k-cycle.

Exercise 25. Let G be a group, and let $g \in G$ be an element of order d. Show that the order of g^{-1} is also d.

Solution 25. There are two cases to consider. First suppose that $|g| = \infty$. For the sake of reaching a contradiction, suppose that $|g^{-1}| < \infty$. Thus for some $m < \infty$ we have that $(g^{-1})^m = 1$ (this is the smallest m for which this is true). But then,

$$g^m = \mathbf{g}^{\mathbf{-1 \cdot m \cdot -1}} = ((g^{-1})^m)^{-1} = 1^{-1} = 1 \tag{70}$$

This is a contradiction. Therefore if $|g| = \infty$, then $|g^{-1}| = \infty$. In the second case, we suppose that $|g| = d$ and $|g^{-1}| = c$. We then show that $c = d$. First,

$$(g^d)^{-1} = (g^{-1})^d = 1 \tag{71}$$

Therefore $c \leq d$. Next,

$$g^c = ((\mathbf{g}^{\mathbf{c}})^{\mathbf{-1}})^{\mathbf{-1}} = ((g^{-1})^c)^{-1} = 1^{-1} = 1 \tag{72}$$

Therefore $d \leq c$. Together we get that $d = c$.

4.3 Homework 3

Exercise 26. Let G, H be groups, and let $\phi : G \times H \to G$ be the function defined by $\phi(g, h) = g$. Show that ϕ is a surjective homomorpishm.

Solution 26. First show that ϕ is a homomorphism. To see this, fix $(g_1, h_1), (g_2, h_2) \in G \times H$. Then, $\phi(g_1 g_2, h_1 h_2) = g_1 g_2 = \phi(g_1, h_1)\phi(g_2, h_2)$. Thus ϕ is a homomorphism. Next show ϕ is surjective. That is, we must show that for all $g \in G$, there exists a $(g', h') \in G \times H$ such that $\phi(g', h') = g$. To see this, consider (g, h'). Then $\phi(g, h') = g$. By the same logic, ϕ is clearly not injective. Consider (g_1, h_1) and (g_1, h_2) where $h_1 \neq h_2$. But $\phi(g_1, h_1) = g_1 = \phi(g_1, h_2)$. This demonstrates an instance for which $a_1 \neq a_2$ but $\phi(a_1) = \phi(a_2)$.

Exercise 27. Let ϕ be the function which maps every $A \in GL_n(\mathbb{R})$ to the transpose of its inverse. Show that ϕ is an isomorphism from $GL_n(\mathbb{R})$ to itself.

Solution 27. First show ϕ is a homomorphism. Fix $A, B \in GL_n(\mathbb{R})$. Then

$$\begin{aligned} \phi(AB) &= ((AB)^{-1})^T \\ &= (B^{-1}A^{-1})^T \\ &= (A^{-1})^T(B^{-1})^T \\ &= \phi(A)\phi(B) \end{aligned}$$

Next show ϕ is injective. That is, we will show that $\phi(A) = \phi(B)$ implies $A = B$. Then

$$\phi(AB) = \phi(A)\phi(B) = \phi(A)\phi(A)$$

Thus

$$(A^{-1})^T(B^{-1})^T = (A^{-1})^T(A^{-1})^T \tag{73}$$

Use the left cancellation law to show that $(B^{-1})^T = (A^{-1})^T$. This implies that $A = B$. Next show ϕ is surjective. That is, we must show that for all $B \in GL_n(\mathbb{R})$ there exists an $A \in GL_n(\mathbb{R})$ such that $\phi(A) = B$. Consider $A = (B^T)^{-1}$. Then

$$\begin{aligned} \phi((B^T)^{-1}) &= (((B^T)^{-1})^{-1})^T && (74) \\ &= B && (75) \end{aligned}$$

Therefore ϕ is an isomorphism.

Exercise 28. Let p be a prime number, and let G be a group of order p. Show that G has exactly two distinct subgroups.

Solution 28. Lagrange's Theorem tells us that if H is a subgroup of G, then $|H|$ divides $|G|$. Therefore the only possible orders for subgroups of G are 1 and p. Now note that G can only have one subgroup of order 1. This follows because the identity element must be in every subgroup. Next note that no subgroup can have an order greater than p since a subgroup must be a subset of G. Clearly the only subgroup of G with order p is G itself.

Exercise 29. Show that $H = \{\sigma \in S_5 : \{\sigma(1), \sigma(2)\} = \{1,2\}\} \leq S_5$, count the number of elements in it, and verify that Lagrange's theorem holds in this case.

Solution 29. It's fairly clear that H is a subgroup of G. Then, the number of elements in H is $2! \times 3! = 12$. The number of elements in $S_5 = 5! = 120$. Observe that $120/12 = 10$. Thus Lagrange's theorem holds.

Exercise 30. Let A be an abelian group, and define $\phi : A \to A$ by $\phi(a) = a^2$. Show that ϕ is a homomorphism.

Solution 30. Fix $a, b \in G$. Then

$$\begin{aligned} \phi(ab) &= (ab)^2 \\ &= (ab)(ab) \\ &= a^2b^2 && \text{(since } A \text{ is abelian)} \\ &= \phi(a)\phi(b) \end{aligned}$$

Exercise 31. Let G, H be groups, and let $\phi : G \to H$ be a homomorphism. Show that ϕ is injective if and only if $\ker(\phi) = \{1\}$.

Solution 31. First suppose ϕ is injective. Since f is a homomorphism, the identity element e of G is mapped to the identity element e' of H. Thus $\phi(e) = e'$. Let $g \in \ker(\phi)$. By definition $\phi(g) = e'$. Thus since ϕ is injective, we have that $\phi(e) = \phi(g)$ implies that $e = g$. Therefore the kernal is trivial.

Now suppose $\ker(\phi) = \{1\}$. Fix $g_1, g_2 \in G$ such that $\phi(g_1) = \phi(g_2)$. Then

$$\begin{aligned}
\phi(g_1 g_2^{-1}) &= \phi(g_1)\phi(g_2^{-1}) && (\phi \text{ is a homomorphism}) \\
&= \phi(g_1)\phi(g_2)^{-1} && (\text{property of homomorphism}) \\
&= 1
\end{aligned}$$

Therefore $g_1 g_2^{-1} \in \ker(\phi)$. Since we assumed $\ker(\phi) = \{1\}$, it must be that $g_1 g_2^{-1} = 1$. This implies that $g_1 = g_2$.

Exercise 32. Let G be a finite group with $|G| > 2$. Show that there are at least two distinct isomorphisms from G to itself.

Solution 32. *Incomplete.*

4.4 Homework 4

Exercise 33. Let H, K be normal subgroups of the group G. Show that $H \cap K$ is also a normal subgroup of G.

Solution 33. We will use this equivalent characterization of normal subgroups: For every $g \in G$ we have $gHg^{-1} \subset H$. Let $x \in H \cap K$ (we know this intersection is nonempty). Then the normality of H and K implies for all $g \in G$, $gxg^{-1} \in H \cap K$. Therefore $g(H \cap K)g^{-1} \subset H \cap K$ so that $H \cap K$ is normal.

Exercise 34. What is the index of the subgroup $3\mathbb{Z}$ in $\mathbb{Z}$?

Solution 34. $[\mathbb{Z} : 3\mathbb{Z}] = 3$. To see this, enumerate the left cosets of $3\mathbb{Z}$ as follows:

$$\begin{aligned}
3\mathbb{Z} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\
1 + 3\mathbb{Z} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\
2 + 3\mathbb{Z} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}
\end{aligned}$$

Exercise 35. Let H be a subgroup of G. Show the following conditions are equivalent.

1. H is a normal subgroup of G.
2. For every $g \in G$ we have $gHg^{-1} = H$
3. For every $g \in G$ we have $gHg^{-1} \subset H$

Solution 35. $1 \implies 2$: Since H is normal we have that for all $g \in G$, $Hg = gH$. This implies that $H = gHg^{-1}$.

$2 \implies 3$: This holds trivially.

$3 \implies 1$: We have that for every $g \in G$, we have $gHg^{-1} \subset H$. Let $h \in H$ and $g \in G$. Then

$$gh = ghg^{-1}g = h'g \in Hg \implies gH \subset Hg \tag{76}$$

Similarly,

$$hg = gg^{-1}hg = gh' \in gH \implies Hg \subset gH \tag{77}$$

Therefore, these two inclusions show that $gH = Hg$.

$1 \implies 3$: Suppose $gH = Hg$ for all $g \in G$. Fix $g \in G$ and $h \in H$. We want to show that $ghg^{-1} \in H$. To that end

$$ghg^{-1} = gg^{-1}h' = h' \in H \tag{78}$$

Therefore $gHg^{-1} \subset H$.

Exercise 36. Let $H \leq G$ and $K \trianglelefteq G$ be groups, and define the set

$$HK = \{hk : h \in H, k \in K\} \tag{79}$$

show $HK \leq G$.

Solution 36. We need to verify the three axioms required to be a subgroup:

1. Identity: Observe that $1 \in H \cap K$. Therefore $1 \in HK$.

2. Closed under Products: Since K is normal, we know for all $g \in G$, $gK = Kg$. This implies that for all $g \in G$ and $k \in K$, there exists a $k' \in K$ such that $gk = k'g$. Now consider $hk, h'k' \in HK$. We want to show their product is also in HK. Notice that in the product $hkh'k'$, the middle term kh' can be written as $h'k''$ for some $k'' \in K$. Therefore we can now consider the product $hh'kk''$. Since H and K are both subgroups, then $hh' = \tilde{h} \in H$ and $kk'' = \tilde{k} \in K$. Therefore by the definition of HK, $\tilde{h}\tilde{k} \in HK$.

3. Closed under Inverses: Let $hk \in HK$. We want to show that $(hk)^{-1} = k^{-1}h^{-1} \in HK$. Using a similar technique as above, the normality of K implies that we can find a $k' \in K$ such that $k^{-1}h^{-1} = h^{-1}k'$. Therefore $k^{-1}h^{-1} = h^{-1}k' \in HK$.

This three properties show that HK is a subgroup of G.

Exercise 37. Let H be the subset of upper-triangular matrices $GL_2(\mathbb{R})$. Show that H is a subgroup of $GL_2(\mathbb{R})$. Is it a normal subgroup?

Solution 37. We need to verify the three axioms required to be a subgroup:

1. Identity: Clearly $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an upper triangular matrix.

2. Closed under Products: Let $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$ be two upper triangular matrices. Their product is
$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cd \end{pmatrix} \tag{80}$$
which is clearly an upper triangular matrix.

3. Closed under Inverse: Let $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ be an upper triangular matrix. Its inverse is
$$\frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} \tag{81}$$
which is also an upper triangular matrix.

Therefore H is a subgroup of $GL_2(\mathbb{R})$.

H is not a normal subgroup. We showed that an equivalent condition for being a subgroup is that H must be closed under conjugation by elements of G. It's easy to find examples of conjugation which lead to matrices that are not upper triangular. Thus H is not a normal subgroup.

Exercise 38. Let G be a finite group, and let H be a nonempty subset of G such that for any $a, b \in H$ we have $ab \in H$. Show that H is a subgroup of H.

Solution 38. We need to verify the three axioms required to be a subgroup:

1. Identity: Proved in (3).

2. Closed under Products: This follows by the hypothesis of the claim.

3. Closed under Inverses: Since H is assumed nonempty, take an element $x \in H$. Since H is closed under products, we must have that all of the powers of x are in H. That is, $x, x^2, x^3, x^4, \ldots \in H$. Since G is assumed finite and H is a subset of G, H must also be finite. Therefore there must exist powers of x that are equal (pigeonhole principle). Let $m, n \in \mathbb{N}$ be the first such powers such that $x^m = x^n$, and without loss of generality, assume $m > n$. Next observe that $x^m = x^n$ implies $x^{m-n} = 1 \in H$ (this shows the identity is in H) which implies $x^{m-n-1} = x^{-1}$. Since $m > n$, we know that $m - n > 0$ or equivalently that $m - n \geq 1$. There are two cases to consider:
   (a) $m - n = 1$: In this case $x^{m-n-1} = x^{1-1} = 1 = x^{-1} \in H$.
   (b) $m - n > 1$: In this case $m - n - 1 > 0$, so that $x^{m-n-1} = x^{-1} \in H$ since x^{m-n-1} is a positive power of x and H is closed under products.

Exercise 39. Let H be the subset of matrices in $GL_3(\mathbb{R})$ whose determinant is positive. Show that H is a normal subgroup of $GL_3(\mathbb{R})$, and describe $GL_3(\mathbb{R})/H$.

Solution 39. We first verify that H is indeed a subgroup by verifying the three axioms:

1. Identity: The identity matrix has determinant 1, which is positive.
2. Closed under products: Take any $A, B \in H$. Recall from linear algebra that $\det(AB) = \det(A)\det(B) > 0$. therefore H is closed under taking products.
3. Closed under inverses: Take any $A \in H$. Recall from linear algebra the $\det(A^{-1}) = \frac{1}{\det(A)} > 0$. Therefore H is closed under inverses.

These three points show that H is indeed a subgroup.

To show that H is a normal subgroup, we will use the equivalent characterization that H is closed under conjugation by elements of G. Take any $A \in G$ and $B \in G$. Then $\det(BAB^{-1}) = \frac{\det(A)\det(B)}{\det(B)} = \det(A) > 0$. Therefore H is closed under conjugation by elements of G so that H is a normal subgroup.

Exercise 40. Say that a subgroup M of a group G is maximal if $M \subsetneq G$ and for every subgroup H of G that contains M we have either $H = M$ or $H = G$. For each of the following conditions on a finite group G, decide whether it implies that G is cyclic.

1. G has exactly one maximal subgroup.
2. G has exactly two maximal subgroups.
3. G has exactly three maximal subgroups.

Solution 40.

4.5 Homework 5

Exercise 41. Write down the order of each element in D_8.

Solution 41. Geometrically, it's clear that all the (8) mirror symmetries of D_8 have order 2 (we can undo a reflection by reflecting again). We can also show this as follows. Fix an i such that $0 \leq i \leq 8$. Then

$$(\epsilon\rho^i)(\epsilon\rho^i) = \epsilon\rho^i\rho^{-i}\epsilon = \epsilon^2 = 1 \tag{82}$$

Therefore $|\epsilon\rho^i| = 2$.

The orders of the rotational symmetries are as follows

$$
\begin{aligned}
|1| &= 1 \\
|\rho| &= 8 \\
|\rho^2| &= 4 \\
|\rho^3| &= 8 \\
|\rho^4| &= 2 \\
|\rho^5| &= 8 \\
|\rho^6| &= 4 \\
|\rho^7| &= 8
\end{aligned}
$$

Exercise 42. Define a function $\phi : D_n \to \{\pm 1\}$ by $\phi(x) = 1$ if x is a rotation and $\phi(x) = -1$ otherwise. Show that ϕ is a homomorphism.

Solution 42. Proof by cases.

Exercise 43. Let G be a group, and let

$$Aut(G) = \{f : G \to G | f \text{ is an isomorphism}\} \tag{83}$$

be the set of all isomorphisms from G to G. Show $Aut(G)$ is a group under the binary operation of composition of functions.

Solution 43. Observe that $Aut(G)$ is a subset of the set of all permutations of G. Therefore, we will prove that $Aut(G)$ is a subgroup of G.

Exercise 44. Let G be a group, and let

$$Z(G) = \{z \in G | zg = gz \text{ for all } g \in G\} \tag{84}$$

be the set of all elements in G which commute with all other elements. Define a function $f : G \to Aut(G)$ by

$$(f(g))(x) = gxg^{-1} \tag{85}$$

Show that f is a homomorphism and that $Ker(f) = Z(G)$

Solution 44. First show f is a homomorphism. Fix $x, y \in G$. Then,

$$
\begin{aligned}
(f(g))(xy) &= gxyg^{-1} \\
&= gxg^{-1}gyg^{-1} \\
&= (f(g))(x)(f(g))(y)
\end{aligned}
$$

Next,

$$\begin{aligned}
Ker(f) &= \{g \in G | (f(g))(x) = x, \quad \forall x \in G\} \\
&= \{g \in G | gxg^{-1} = x, \quad \forall x \in G\} \\
&= \{g \in G | gx = xg, \quad \forall x \in G\} \\
&= Z(G)
\end{aligned}$$

Exercise 45. Let G be a group, let $K \trianglelefteq G$, and let $H \leq G$. Show that $K \cap H \trianglelefteq H$.

Solution 45. Since K is a normal subgroup of G, we know that

$$gkg^{-1} \in K \quad \forall k \in K, \forall g \in G \tag{86}$$

Further, since H is a subgroup, we know if is closed under products. Fix $x \in H \cap K$.

$$gxg^{-1} \in H \quad \forall x \in H \cap K, \forall g \in H \tag{87}$$

But since $x \in K$, we know that $gxg^{-1} \in K$. Therefore $gxg^{-1} \in H \cap K \quad \forall x \in H \cap K, \forall g \in H$, so that $K \cap H \trianglelefteq H$.

Exercise 46. How many subgroups does a cyclic group of order 30 have?

Solution 46. For a finite cyclic group, we know there exists a unique subgroup for each divisor of the order. Thus, the divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30. The cyclic group of order 30 has 8 subgroups.

4.6 Homework 6

Exercise 47. Let G be a group, and let N be a normal subgroup of G. Define a function

$$\phi : G \to G/N \tag{88}$$

by $\phi(g) = gN$. Show that ϕ is a homomorphism, and that $\ker(\phi) = N$.

Solution 47. We'll first show that ϕ is a homomorphism. Let $a, b \in G$. Then,

$$\begin{aligned}
\phi(ab) &= abN \\
&= aNbN && \text{(definition of multiplication on quotient groups)} \\
&= \phi(a)\phi(b)
\end{aligned}$$

Thus ϕ is a homomorphism. Next,

$$\begin{aligned}\ker(\phi) &= \{g \in G | \phi(g) = 1\} \\ &= \{g \in G | gN = N\} \\ &= \{g \in N\} \\ &= N\end{aligned}$$

Therefore $\ker(\phi) = N$.

Exercise 48. Let G be a group, and let $g \in G$. Show that

$$\{1, g\} \trianglelefteq G \tag{89}$$

if and only if $g \in Z(G)$.

Solution 48. $\Rightarrow$ Suppose $G' = \{1, g\} \trianglelefteq G$. Then, $g'G' = G'g'$ for all $g' \in G$. We can explicitly write out these left and right cosets: $g'G' = \{g', g'g\}$ and $G'g' = \{g', gg'\}$. Therefore, it must be that $g'g = gg'$. This shows that $g \in Z(G)$. Another proof is as follows: Since $\{1, g\} \trianglelefteq G$, we know that $g'g(g')^{-1} \in \{1, g\}$ for all $g' \in G$. There are two cases to consider. Suppose $g'g(g')^{-1} = 1$. Then $g'g = g'$, or $g = 1$. Therefore $g \in Z(G)$. In the second case, suppose $g'g(g')^{-1} = g$. Then $g'g = gg'$. Thus $g \in Z(G)$.

$\Leftarrow$ Suppose $g \in Z(G)$. Then $gg' = g'g$ for all $g' \in G$. Therefore, $g'g(g')^{-1} = g \in \{1, g\}$. Similarly, $g'1(g')^{-1} = g'(g')^{-1} = 1 \in \{1, g\}$. Therefore $\{1, g\} \trianglelefteq G$.

Exercise 49. For any group G, show that $G/Z(G)$ is isomorphic to a subgroup of $Aut(G)$.

Solution 49. We will use the First Isomorphism Theorem to prove this statement. Let $\phi : G \to Aut(G)$ by

$$\phi(a) = aga^{-1} \tag{90}$$

First show ϕ is a homomorphism. To see this, fix $a, b \in G$, then for all $g \in G$,

$$\begin{aligned}\phi(ab)(g) &= (ab)g(ab)^{-1} \\ &= abgb^{-1}a^{-1} \\ &= a\phi(b)a^{-1} \\ &= \phi(a) \circ \phi(b)\end{aligned}$$

therefore ϕ is a homomorphism. Now we'll show that $\ker(\phi) = Z(G)$. However this is simple to see because

$$\begin{aligned}\ker(\phi) &= \{a \in G | aga^{-1} = g\} \\ &= \{a \in G | ag = ga\} \\ &= Z(G)\end{aligned}$$

Therefore, by the first isomorphism theorem, we have that

$$G/ker(\phi) \cong Im(\phi) \tag{91}$$

or in this context

$$G/Z(G) \cong Inn(G) \tag{92}$$

Exercise 50. For the action of $GL_2(\mathbb{R})$ on $\mathbb{R}^2$, find the orbit of each $v \in \mathbb{R}^2$.

Solution 50. There are two cases to consider. Suppose $v = 0$ (the zero vector). Then $O_v = \{0\}$. For $v \neq 0$, since each matrix in $GL_2(\mathbb{R})$ is invertible, we know that the nullspaces of these matrices are trivial. Conversely, $v \neq 0$ implies the action cannot map v to 0. Therefore, $O_v = \mathbb{R}^2 \{0\}$.

Exercise 51. For the action of $GL_2(\mathbb{R})$ on $\mathbb{R}^2$ describe the stabilizer of each $v \in \mathbb{R}^2$.

Solution 51. Everything stabilizes the zero vector. For a non zero vector v, it is stabilized by the matrix which has it as an eigenvector with corresponding eigenvalue of 1.

Exercise 52. Let G be a group, and let G act on itself by (left) multiplication. Show that the stabilizer of each element is trivial.

Solution 52. This follows from the fact that the identity element of G is unique. Thus, $1 \cdot g = g$ and uniqueness implies the stabilizer of each element of G is trivial.

Exercise 53. For the action of the dihedral group D_4 on the vertices of a square, determine the size of a vertex stabilizer.

Solution 53. The size of a vertex stabilizer is 2: the identity element and the mirror symmetry which passes through the opposite vertex. All other symmetries do not fix a vertex.

5 Honors Questions

Exercise 54. From homework 1, we showed that if $g^2 = 1$ for all $g \in G$ where G is a group, then G is abelian. Note that $ab = ba$ iff $aba^{-1}b^{-1} = 1$. Can we write $aba^{-1}b^{-1}$ as a product of squares $c_1c_2c_3\ldots$? (And then each $c_i^2 = 1$).

Solution 54.