Modern Algebra Lecture Notes

Rebekah Dix

December 17, 2018

Contents

1 Group Theory **3**
1.1 Basic Definitions/Examples 3
1.1.1 Order 5
1.1.2 Direct Product 5
1.1.3 Symmetric Groups 5
1.1.4 Matrix Groups (General Linear Groups) 6
1.2 Subgroups 6
1.3 Homomorphisms 8
1.4 Cosets and Lagrange's Theorem 10
1.5 Cyclic Groups 13
1.6 Dihedral Groups 15
1.7 Quotient Groups 17
1.8 Isomorphism Theorems 18
1.9 Actions, Orbits, and Stabilizers 20
1.10 Multiplicative group of integers modulo n 27
1.11 p-Groups 31

2 Ring Theory **34**
2.1 Ring Basics 34
2.2 Matrix Rings 36
2.3 Subrings, Homomorphisms of Rings, and Ideals 37
2.4 Practice 40

3 Practice Quizzes **42**
3.1 Quiz 1 42
3.2 Quiz 2 42
3.3 Quiz 3 43
3.4 Quiz 4 44
3.5 Quiz 5 45

3.6 Quiz 6 46
3.7 Quiz 7 47
3.8 Quiz 8 47
3.9 Quiz 9 48
3.10 Quiz 10 49
3.11 Quiz 11 50

4 Practice Exercises **52**

4.1 Practice 1 52
4.2 Practice 2 53
4.3 Practice 3 54
4.4 Practice 4 56
4.5 Practice 5 59
4.6 Practice 6 61
4.7 Practice 7 63
4.8 Practice 8 66
4.9 Practice 9 67
4.10 Practice 10 69
4.11 Practice 11 70

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 $a \star b = b \star a = e$.

Note that the binary operation requires closure, by definition.

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 $a, b \in G$.

Example 2 (Examples of Abelian Groups)**.** The following are examples of 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)**.** The following are non-examples of groups.

1. $G = \mathbb{R}$ and $\star =$ maximum. For example, $2 \star \pi = \max(2, \pi) = \pi$. Associativity 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 unit element. 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.

Theorem 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, $e_1 = e_2$. □

Theorem 2 (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, $x(ab) = x(ac)$. By associativity, we may write $(xa)b = (xa)c$. This simplifies to $1 \star b = 1 \star c$ or that $b = c$. □

Theorem 3 (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 $b = c$. □

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).

Exercise 2. Give an example of $\tau \in S_4$ 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)**.** The following are examples of 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 $(g_1, h_2)(g_2, h_2) = (g_1 g_2, h_1 h_2)$. 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.

Theorem 4 (The order of a k-cycle is k.)**.**

Proof. Let $(i_1 i_2 \ldots i_k)$ be a k-cycle. By checking each index, observe that $(i_1 i_2 \ldots i_k)^k = id$. For any $d < k$, note that $(i_1 i_2 \ldots i_k)^d (i_1) = i_{d+1} \neq i_1$, since $d < k$. $\square$

Theorem 5 (Disjoint cycles commute.)**.**

Proof. Let $\sigma = (s_1 s_2 \dots s_k)$ and $\tau = (t_1 t_2 \dots t_l)$ 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)**.** The following are 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 $0 + 2 = 2 + 0 = 2 \in H$, $0 + 4 = 4 + 0 = 4 \in H$, $2 + 4 = 4 + 2 = 0 \in H$, $2 + 2 = 4 \in H$, and $4 + 4 = 2 \in H$.

   (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 $\phi(a)\phi(b)$ is computed in H.

Example 9 (Examples of Homomorphisms)**.** The following are 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

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

Theorem 6 (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, $\phi(x^{-1}) = \phi(x)^{-1}$.

$\square$

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), $\phi(1) = \sigma$, $\phi(2) = \sigma^2$.

Theorem 7 (Kernel of a homomorphism is a subgroup)**.** 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).

Theorem 8. 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 fix $a \in G$. Let

$$aH = \{ah | h \in H\}$$
$$Ha = \{ha | h \in H\}$$

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 $a \in H$.

Theorem 9 (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 10 (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.

Theorem 11 (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]].

Theorem 12 (The kernel 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. □

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. □

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)**.** The following are 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 $\langle x \rangle = \{0, 3\}$.

Theorem 13 (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

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

□

Theorem 14. 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 $|H| = m$. $\square$

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)**.**

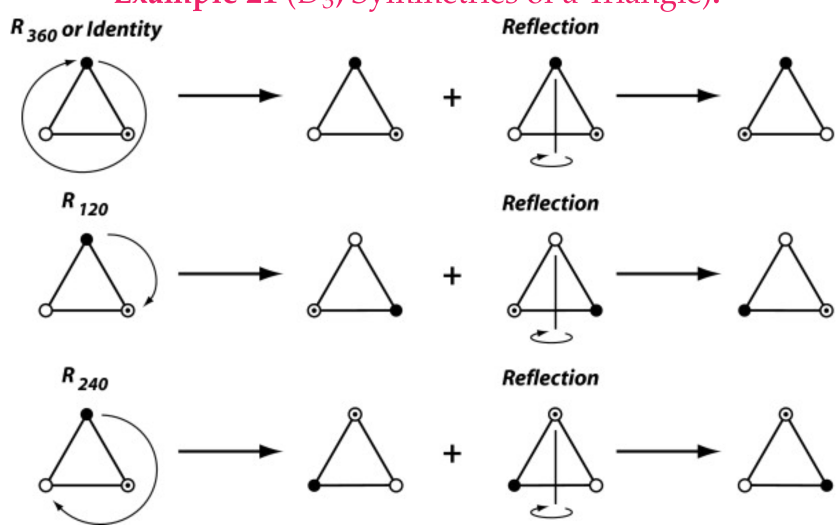

Figure 1: The symmetries of an equilateral triangle

Example 22 (D_4, Symmetries of a Square).

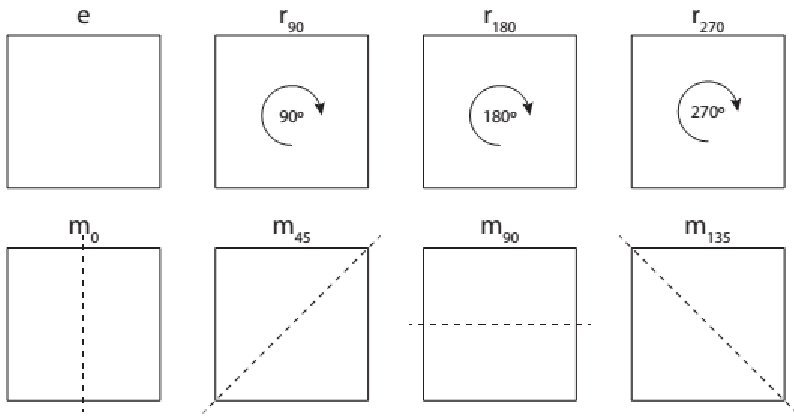

Figure 2: The symmetries of a square

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 $\langle\rho\rangle = \{1, \rho, \rho^2, \dots, \rho^{n-1}\}$.
2. Let ϵ be a vertical mirror symmetry. Then the set of all mirror symmetries is $\{\epsilon, \epsilon\rho, \epsilon\rho^2, \dots, \epsilon\rho^{n-1}\}$.

Theorem 15 (Important Identity for Dihedral Groups). $\rho\epsilon = \epsilon\rho^{-1}$.

We use this relation to make computations in dihedral groups.

Theorem 16. $\rho^i\epsilon = \epsilon\rho^{-i}$

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 $g_1Ng_2N = g_1g_2N$.

Theorem 17. *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. $\mathbb{Z}/12\mathbb{Z} = \{0 + 12\mathbb{Z}, 1 + 12\mathbb{Z}, \dots, 11 + 12\mathbb{Z}\}$
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 18 (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 kernel 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 19 (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 kernel 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, Isotropy Subgroup)**.** Let X be a G-set and $x \in X$. The stabilizer of x is

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

also called the isotropy subgroup of x.

Theorem 20 (The stabilizer of a group element is 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. □

Theorem 21 (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 surjective. 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.

Theorem 22. 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 23 (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 $g = 1$. Alternatively,

$$\cap_{x\in X} G_x = \{1\} \tag{61}$$

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

$$gx = x \implies g = 1 \tag{62}$$

Alternatively, this means all stabilizers are trivial. We have that for all $x \in X$,

$$G_x = \{1\} \tag{63}$$

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 $v = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$).

1.10 Multiplicative group of integers modulo n

Definition 23 (Coprime). An integer a is coprime to n if the only positive divisor of both a and n is 1.

Definition 24 ($(\mathbb{Z}/n\mathbb{Z})^\times$).

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{1 \leq a \leq n-1 | a \text{ coprime to } n\} \tag{64}$$

$n \geq 2$. This is called the multiplicative group of integers modulo n, where the binary operation is multiplication and taking the remainder upon dividing by n.

Example 35 ($(\mathbb{Z}/n\mathbb{Z})^\times$).

n	$((\mathbb{Z}/n\mathbb{Z})^\times)$
2	$\{ 1 \}$
3	$\{1 , 2\}$
4	$\{1, 3\}$
5	$\{1, 2, 3, 4\}$
6	$\{1, 5\}$

Example 36 (Computations in $(\mathbb{Z}/n\mathbb{Z})^\times$). Suppose $n = 5$. Then we consider $(\mathbb{Z}/5\mathbb{Z})^\times$.

1. $1 \cdot 2 = 2$
2. $2 \cdot 3 = 1$
3. $2 \cdot 2 = 4$
4. $3 \cdot 3 = 4$

Theorem 24. $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group.

Proof. We verify the axioms:

1. Unit: The unit element is 1, since 1 is coprime to every number and acts an identity under multiplication.

2. Inverse: Define a function for a fixed $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ by $f : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ where $f(x) = gx$. To show that g has an inverse, it suffices to show that f is surjective. If f is surjective, then there must exist some $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $gx = 1$. However, since $(\mathbb{Z}/n\mathbb{Z})^\times$ is finite, it is enough to show that g is injective (so that f must also be surjective.) suppose that $gx = gy$ for some $x, y \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then, for some $\alpha, \beta \in \mathbb{Z}$
$$gx - n\alpha = gy - n\beta \qquad \text{(equality of integers)}$$
this implies
$$g(x-y) = n(\alpha - \beta) \tag{65}$$
so that n divides $g(x-y)$. Next, recall that n is coprime to g (by the definition of the set/group), so $n|(x-y)$. However, since $x, y \in (\mathbb{Z}/n\mathbb{Z})^\times$, the difference in absolute value of x and y must be less than n. This implies that $x = y$, which proves injectivity.

□

Theorem 25 (Fermat's Little Theorem)**.** For a prime number p and $1 \leq x \leq p-1$, we have $x^{p-1} - 1$ is divisible by p.

Proof. Note that $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ (since p is prime and x is less than p). Let k be the order of x and consider
$$\langle x \rangle = \{1, x, x^2, \ldots, x^{k-1}\} \tag{66}$$
by Lagrange's theorem, $|\langle x \rangle|$ divides $|(\mathbb{Z}/n\mathbb{Z})^\times|$. Thus k divides $p-1$ (because $|\langle x \rangle|$ is k and$|(\mathbb{Z}/n\mathbb{Z})^\times|$ is $p-1$, since p is prime). Then there exists some t such that $p - 1 = k \cdot t$. Thus
$$x^{p-1} = x^{k \cdot t} = (x^k)^t = 1^t = 1 \pmod{p}$$
□

Theorem 26. Let $p \neq q$ be odd primes. Then
$$(\mathbb{Z}/pq\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \tag{67}$$

Proof. Define a homomorphism $\phi : (\mathbb{Z}/pq\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ by taking remainders for division by p and q separately.

Example 37. Suppose $p = 3$ and $q = 5$. Then $\phi(11) = (2, 1)$.

It suffices to check that $\phi : (\mathbb{Z}/pq\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is a homomorphism. This requires checking that ab reduces mod p to the product of the reductions of a and b.

Example 38. $p = 3$ and $q = 5$.

$$7 \cdot 11 = 77 = 2 \tag{68}$$

and

$$1 \cdot 2 = 2 \tag{69}$$

Next we'll show ϕ is injective. We'll show that $\ker \phi$ is trivial.

$$\begin{aligned}
\ker \phi &= \{1 \leq a \leq pq - 1 | \phi(a) = (1,1)\} \\
&= \left\{1 \leq a \leq pq - 1 \middle| p|(a-1), q|(a-1)\right\} \\
&= \left\{1 \leq a \leq pq - 1 \middle| pq|(a-1)\right\} \\
&= \{1\}
\end{aligned}$$

To show surjectivity, we'll show that the domain and the range have the same size (we can do this since we've already shown ϕ is injective.) Then

$$|(\mathbb{Z}/pq\mathbb{Z})^{\times}| = (p-1)(q-1) \tag{70}$$

and

$$|(\mathbb{Z}/pq\mathbb{Z})^{\times}| = pq - q - p + 1 \tag{71}$$

because there are pq total possible elements, but q are divisible by p, p divisible by q, and 1 element (pq) that is divisible by both p and q. □

Definition 25 (Permutation representation of action)**.** Let G be a group that acts on $\{1, \ldots, n\}$. Associated to the action is a homomorphism $\lambda : G \to S_n$, defined by

$$\lambda(g)(i) = gi \tag{72}$$

where the RHS is the action of g on i, $i \in \{1, \ldots, n\}$.

We need to confirm that λ is indeed a homomorphism.

Proof.

$$\begin{aligned}
\lambda(gh)(i) &= gh(i) \\
&= g(h(i)) && \text{(since action)} \\
&= \lambda(g)(h(i)) && \text{(definition of } \lambda\text{)} \\
&= \lambda(g)(\lambda(h)(i)) && \text{(definition of } \lambda\text{)}
\end{aligned}$$

□

For completeness, we should also check $\lambda(g)$ is indeed a permutation for every $g \in G$.

Proof. Incomplete (some weird proof with the inverse?) □

Theorem 27. If $\lambda : G \to S_n$ is a homomorphism, we can define an action of G on $\{1, \dots, n\}$ by

$$g(i) = \lambda(g)(i) \tag{73}$$

Proof. We check the two conditions required to be an action:

1. $1(i) = \lambda(1)(i) = id(i) = i$
2. $gh(i) = \lambda(gh)(i) = \lambda(g)(\lambda(h)(i)) = \lambda(g)(h(i)) = g(h(i))$

□

Example 39. Let D_4 action of the vertices of a square. We can enumerate the values of the homomorphism $\lambda : D_4 \to S_4$.

1. $\lambda(id) = id$
2. $\lambda(\rho) = (1234)$
3. $\lambda(\rho^2) = (13)(24)$
4. $\lambda(\rho^3) = (1432)$
5. $\lambda(\epsilon) = (12)(34)$
6. and so on

Theorem 28. Under the above assumptions: λ is injective if and only if the action of G on X (which we can think of as $\{1, \dots, n\}$) is faithful.

Proof. Since λ is a homomorphism, we can prove it is injective by showing its kernel is trivial. Then

$$\ker \lambda = \{g \in G | \lambda(g)(i) = i \quad \forall i \in X\} \tag{74}$$

Hence, $\ker \lambda = \{1\}$ if and only if the action is faithful. □

Theorem 29 (Cayley)**.** Let G be a group of order n. Then, there exists an injective homomorphism $\phi : G \to S_n$.

Proof. Consider the action of G on itself by (left) multiplication. Associated to this action is a homomorphism $\phi : G \to S_n$. This action is free (shown in homework), and therefore faithful, so ϕ is injective by the above claim. □

Example 40. Take $G = \mathbb{Z}/3\mathbb{Z} = \{1, 2, 3\}$ (where $3 = 0$). Then $\phi : G \to S_3$ has elements

1. $\phi(3) = id$
2. $\phi(2) = (132)$ (since $1 + 2 = 3$ and $3 + 2 = 5 = 2$ and $2 + 2 = 4 = 1$)
3. $\phi(1) = (123)$

Theorem 30. If $|G| = n$, then G is isomorphic to a subgroup of S_n. Indeed $\phi : G \to Im(\phi) \subset S_n$.

1.11 p-Groups

Definition 26 (p-Group)**.** Let p be a prime number. G is a p-group if $|G|$ is a power of p.

Theorem 31 (Cardinality of set of fixed points of action of set on p-group equals cardinality of set mod p)**.** Let G be a p-group that acts on a finite set X. Let $X^G = \cap_{g\in G} X^g$ where $X^g = \{x \in X | gx = x\}$, that is those $x \in X$ such that for all $g \in G$, $gx = x$. Then p divides $|X| - |X^G|$, that is

$$|X^G| \equiv |X| \quad (mod p) \tag{75}$$

Proof. Let $x_1, \ldots, x_m$ be the representatives for the orbits of G on X (recall that the the disjoint union of orbits of these representatives cover X). Let's partition these elements into those in X^G and those not. Thus suppose that $x_1, \ldots, x_k \in X^G$ and $x_{k+1}, \ldots, x_m \notin X^G$. Then

$$|X| = \sum_{i=1}^{m} |O(x_i)| = \sum_{i=1}^{k} |O(x_i)| \sum_{j=k+1}^{m} |O(x_j)| \tag{76}$$

Then

$$\sum_{i=1}^{k} |O(x_i)| = |X^G| \tag{77}$$

and by the orbit-stabilizer theorem

$$\sum_{j=k+1}^{m} |O(x_j)| = \sum_{j=k+1}^{m} \frac{|G|}{|G_{x_j}|} \tag{78}$$

Notice that $|G|$ is divisible by p. Further, $|G_{x_j}|$ must be divisible by p since it is a subgroup of G (this follows from Lagrange's theorem). Therefore, $|X|$ equals $|X^G|$ plus the sum of things divisible by p, so that we must have that p divides $|X| - |X^G|$. □

Theorem 32 (A p-group has a non-trivial center)**.** Let G be a p-group. Then $Z(G) \neq \{1\}$. In words, there has to be a non-trivial element of the group that commutes with everything else.

Proof. Let $X = G$ and consider the action of G on X by conjugation. By the above theorem, we know that p divides $|X| - |X^G|$. Therefore since p divides $|X|$, we must have that p divides $|X^G|$. Now

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

We always have that $1 \in Z(G)$. Now since p divides $|X^G|$, we must have that $Z(G) \neq \{1\}$, since no prime p divides 1. □

Corollary 1. Let p be a prime number and let G be a group of order p^2. Then G is abelian.

Proof. Consider $Z(G)$. By Lagrange's theorem, we must have that $|Z(G)| = p, p^2$ (the above theorem rules out 1. The only other possible divisors are p and p^2 since p is prime). There are two cases to consider.

1. Case 1: $|Z(G)| = p^2$. Then $Z(G) = G$. Thus since $Z(G)$ is abelian, G is abelian.
2. Case 2: $|Z(G)| = p$. Then by Lagrange's theorem, $|G/Z(G)| = p$ $G/Z(G)$ is cyclic (since $Z(G)$ is normal), Thus G is abelian.

$\square$

This same result need not hold for higher powers of p. For example, consider D_8. $2^3 = 8$. But $|D_8|$ is not abelian.

Theorem 33 (Cauchy)**.** Let G be a finite group and suppose that $p \big| |G|$ for some prime p. Then there exists an element of order p in G.

Proof. Let's start by proving the simple case of $p = 2$. Therefore $|G|$ is even. We can pair each element in G with its inverse. Note that $1 = 1^{-1}$ so the identity element is paired with itself. Since $|G|$ is even, there must exist $1 \neq g \in G$ such that $g = g^{-1}$. Then $g^2 = 1$. Thus there exists an element of order 2.

Let's now prove the general case. Define the set X as

$$X = \{(g_1, \ldots, g_p) | g_1 g_2 \cdots g_p = 1, \quad g_1, g_2, \ldots, g_p \in G\} \tag{79}$$

Then $\mathbb{Z}/p\mathbb{Z}$ acts on X by $a(g_1, \ldots, g_p)$ by cyclic rotation of a times of $(g_1, \ldots, g_p)$ where $a \in \{0, 1, \ldots, p-1\}$. $\square$

Example 41 (Example of Cauchy's Theorem)**.** Consider $G = S_5$. If $p = 3$, then (123) is an example of an element with order 3. If $p = 5$, then (12345) is an example of an element with order 5.

Summary of p-Groups

1. Any group of order p is cyclic.

Theorem 34 (Correspondence Theorem)**.** Let G, H be groups, and let $\phi : G \to H$ be a group homomorphism. Then there exists a correspondence (i.e. a bijection)

$$\{\text{Subgroups } K \text{ of } G \text{ containing } \ker \phi\} \iff \{\text{Subgroups } L \text{ of } H \text{ contained in } Im(\phi)\}$$

given by $K \mapsto \phi(K)$ and $L \mapsto \phi^{-1}(L)$. In addition, let K_1 and K_2 be subgroups of G containing $\ker(\phi)$ and L_1 and L_2 subgroups L of H contained in $Im(\phi)$.

1. $K_1 \leq K_2 \implies \phi(K_1) \leq \phi(K_2)$
2. $L_1 \leq L_2 \implies \phi^{-1}(L_1) \leq \phi^{-1}(L_2)$

and

1. $K_1 \leq K_2 \implies [K_2 : K_1] = [\phi(K_2) : \phi(K_1)]$
2. $L_1 \leq L_2 \implies [L_2 : L_1] = [\phi(L_2) : \phi(L_1)]$

Proof. □

Theorem 35 (Corollary of Correspondence Theorem)**.** Let G be a group and let $N \trianglelefteq G$. Then the subgroups of G/N are all of the form R/N for some $N \leq R \leq G$. Moreover,

$$[G : R] = [G/N : R/N] \tag{80}$$

Proof. □

Theorem 36 (Sylow's Theorem)**.** Let p be a prime number, let G be a finite group, and let p^n be the largest power of p that divides $|G|$. Then G contains a subgroup P of order p^n. P is called a p-Sylow subgroup of G.

Proof. Todo. □

Example 42 (Example of 2-Sylow subgroup of S_4)**.** What is a 2-Sylow subgroup of S_4? We are looking for a subgroup of S_4 which contains 8 elements. A natural candidate is D_4 acting on the vertices of a square. This action gives rise to a homomorphism λ from D_4 to S_4. Further, this homomorphism is injective (and also recall that this action should be faithful). Hence $Im\lambda \leq S_4$ of order 8.

Example 43 (Example of 3-Sylow subgroup of $\mathbb{Z}/45\mathbb{Z}$)**.** What is a 3-Sylow subgroup of $\mathbb{Z}/45\mathbb{Z}$? We are looking for a subgroup with 9 elements (since $3^2 = 9$ is the largest power of 3 that divides 45). Note that

$$\langle 5 \rangle = \{0, 5, 10, 15, \ldots, 35, 40\} \tag{81}$$

is a subgroup of order 9.

Theorem 37 (p-Sylow subgroups are conjugate)**.** Let G be a finite group and let P, Q be p-Sylow subgroups of G. Then there exists $g \in G$ such that $gPg^{-1} = Q$.

Proof. Recall that

$$gPg^{-1} = \{gtg^{-1} | t \in P\} \tag{82}$$

Let P act on $X = G/Q$ by

$$t(gQ) = tgQ, \quad (t \in P, g \in G) \tag{83}$$

Also note that

$$|X| = \frac{|G|}{|Q|} \tag{84}$$

is *not* divisible by p (since $|Q|$ is the largest power of p that divides $|G|$). Then

$$\begin{aligned}X^p &= \{x \in X | \forall t \in P, \quad tx = x\}\\ &= \{gQ | \forall t \in P, \quad tgQ = gQ\}\\ &= \{gQ | \forall t \in P, \quad g^{-1}tg \in Q\}\\ &= \{gQ | \forall t \in P, \quad t \in gQg^{-1}\}\\ &= \{gQ | P \subseteq gQg^{-1}\}\end{aligned}$$

By Theorem 31, $|X^p|$ is also not divisible by p. Further $X^p \neq \emptyset$. Therefore there exists a $g \in G$ such that $P \subset gQg^{-1}$. Then

$$\begin{aligned}|gQg^{-1}| &= |Q| && \text{(conjugation is a bijective operation)}\\ &= |P| && \text{(since both } p\text{-Sylow subgroups)}\end{aligned}$$

This implies that $gPg^{-1} = Q$. □

Observations about this theorem:

1. If the group is abelian, then the Sylow subgroups are unique.

Corollary 2 (p-Sylow subgroup unique if and only if normal subgroup.)**.** Let G be a finite group and let P be a p-Sylow subgroup of G. Then P is a unique p-Sylow subgroup if and only if $P \trianglelefteq G$.

Theorem 38 (Sylow's Theorem (General))**.** Let G be a finite group and p a prime. Suppose that p^r divides $|G|$. Then G has a subgroup H of order p^r. Moreover, every subgroup of order p^r is contained in a Sylow subgroup.

Proof. Todo. □

2 Ring Theory

2.1 Ring Basics

Definition 27 (Ring)**.** Let A be a set with two binary operations: addition and multiplication. A is called a ring if:

1. A is an abelian group under addition:
   (a) Addition associative: For all $a, b, c \in A$, $(a + b) + c = a + (b + c)$.
   (b) Additive identity: There exists a $0 \in A$ such that for all $a \in A$, $a + 0 = 0 + a = a$.
   (c) Additive inverse: For all $a \in A$, there exists a $b \in A$ such that $a + b = b + a = 0$.
   (d) Addition commutative: For all $a, b \in A$, $a + b = b + a$.

2. Multiplication associative: For all $a, b, c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

3. Multiplicative identity: There exists $1 \in A$ such that for all $a \in A$, $1 \cdot a = a \cdot 1 = a$.

4. Multiplication distributive: For all $a, b, c \in A$

   (a) $a \cdot (b + c) = a \cdot b + a \cdot c$.

   (b) $(b + c) \cdot a = b \cdot a + c \cdot a$.

Example 44 (Examples of Rings)**.** The following are examples of rings:

1. $A = \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

2. $A \in M_{n \times n}(\mathbb{R}) = \{n \times n \text{ matrices over } \mathbb{R}\}$.

3. $A = \mathbb{R}$

4. $A = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$, $n \geq 2$.

5. $A = \mathbb{R}[x] = \{\sum_{i=1}^{n} a_i x^i | a_i \in \mathbb{R}\}$ (the ring of polynomials with real coefficients).

Definition 28 (Commutative Ring)**.** A ring is called commutative if for all $a, b \in A$, $ab = ba$.

Definition 29 (Field)**.** A commutative ring is called a field if for all $a \neq 0$, $a \in A$, there exists a $b \in A$ such that $ab = ba = 1$.

Let $a \in A$ where A is a ring. Then we have the following simple claims:

Theorem 39 ($0 \cdot a = 0$)**.**

$$\begin{aligned} 0 \cdot a &= (0 + 0) \cdot a && \text{(0 additive identity)} \\ &= 0 \cdot a + 0 \cdot a && \text{(distributivity)} \end{aligned}$$

Then cancellation gives $0 = 0 \cdot a$.

Suppose $-a$ is the additive inverse of a.

Theorem 40 ($-a = (-1) \cdot a$)**.** We want to show that $(-1) \cdot a$ is the additive inverse of a. To that end

$$\begin{aligned} a + (-1) \cdot a &= 1 \cdot a + (-1) \cdot a && \text{(1 multiplicative identity)} \\ &= (1 + -1) \cdot a && \text{(distributivity)} \\ &= 0 \cdot a \\ &= 0 \end{aligned}$$

2.2 Matrix Rings

Definition 30 ($GL_n(F)$)**.** Let F be a field (e.g., $F = \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ (p prime)). Then

$$GL_n(F) = \{n \times n \text{ matrices over } F \text{ with non-zero determinant}\} \tag{85}$$

$GL_n(F)$ is clearly a group (under matrix multiplication).

Example 45 ($GL_n(\mathbb{Z}/p\mathbb{Z})$)**.** Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number. Take $p = 3$ and $n = 2$ and consider $GL_2(\mathbb{F}_3)$. As an example of multiplication in this ring, consider

$$\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \tag{86}$$

Exercise 7 (Cardinality of $GL_2(\mathbb{F}_p)$)**.** What is $|GL_2(\mathbb{F}_p)|$ where $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$.

Solution 7. Recall that

$$GL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{F}_p, \quad ad - bc \neq 0 \right\} \tag{87}$$

We'll count the number of matrices in this set as follows:

1. First observe that both a and b cannot be 0 (if they were, the matrix would not be invertible). Thus, with this constraint imposed, there are $p^2 - 1$ ways to choose a and b.

2. Next, when choosing c, d, we need to ensure that $ad - bc \neq 0$. Since either $a \neq 0$ or $b \neq 0$, we can as assume without loss of generality that $a \neq 0$. Thus, this means that

$$d \neq \frac{b}{a} \cdot c \tag{88}$$

   This imposes no restrictions on c, so that there are p ways to choose c. This clearly imposes one restriction on potential values of d, so that there are $p - 1$ ways to choose d.

3. In sum, we find that

$$|GL_2(\mathbb{F}_p)| = (p^2 - 1)p(p - 1) \tag{89}$$

Exercise 8 (p-Sylow subgroup of $GL_2(\mathbb{F}_p)$)**.** What is a p-Sylow subgroup of $GL_2(\mathbb{F}_p)$, and is it unique?

Solution 8. To find the order of a p-Sylow subgroup, we need to find the largest power of p that divides the order of $GL_2(\mathbb{F}_p)$. As calculated above, p divides $|GL_2(\mathbb{F}_p)|$ (but no larger power does). Cosider the subgroup defined by

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{F}_p \right\} \leq GL_2(\mathbb{F}_p) \tag{90}$$

However, this p-Sylow subgroup is *not* unique. Indeed, we can find another p-Sylow subgroup by taking the transpose of each matrix in the above subgroup. We can also recall that a p-Sylow subgroup is unique if and only if it is a normal subgroup, and this subgroup is not normal.

2.3 Subrings, Homomorphisms of Rings, and Ideals

Definition 31 (Subring)**.** Let A b a ring. We call $R \subset A$ a subring if the following conditions are satisfied:

1. Additive and multiplicative identity: $0, 1 \in R$.
2. Closed under addition: For all $a, b \in R$, $a + b \in R$.
3. Closed under multiplication: For all $a, b \in R$, $ab \in R$.
4. Closed under inverses (addition): For all $a \in R$, $-a \in R$.

We then write $R \leq A$.

Remark 2. If we know that $-1 \in R$, then we don't need condition 4 above, since we can use 3 to ensure the additive inverses are in R.

Example 46 (Example of subrings)**.** $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{C}[X]$

Definition 32 (Homomorphism of rings)**.** Let A, B be rings. A function $\phi : A \to B$ is called a homomorphism of rings if for all $a, b \in A$ the following conditions are satisfied:

1. $\phi(ab) = \phi(a)\phi(b)$
2. $\phi(a + b) = \phi(a) + \phi(b)$
3. $\phi(1_A) = 1_B$

Remark 3. In groups, this final condition immediately follows from the fact that group elements have inverses, However, rings needn't have multiplicative inverses, so we need this final condition.

Remark 4. Observe that (from 2) $\phi(0) = 0$ where the 0 on the LHS is the additive identity of A and the 0 on the RHS is the additive identity of B.

Example 47 (Examples of homomorphisms of rings)**.** The following are examples of homomorphisms of rings:

1. Polynomial evaluation homomorphism: $\phi_3 : \mathbb{R}[X] \to \mathbb{R}$ where $\phi_3(f) = f(3)$.
2. Inclusion: $i : \mathbb{Z} \to \mathbb{R}$ by $i(a) = a$.
3. Reduction mod p: $\phi : \mathbb{Z} \to \mathbb{F}_p$. Consider $p = 7$. Then $\phi(100) = 2$.

Definition 33 (Kernel of homomorphism of rings)**.** Suppose A, B are rings and let $\phi : A \to B$ be a ring homomorphism. Then

$$\ker(\phi) = \{a \in A | \phi(a) = 0\} = \phi^{-1}\{0\} \tag{91}$$

Theorem 41 (Homomorphism of rings injective injective if and only its kernel is trivial)**.** Suppose ϕ is a homomorphism of rings. Then ϕ is injective if and only if $\ker(\phi) = \{0\}$.

Example 48 (Kernel of homomorphism of rings)**.** Consider the polynomial evaluation homomorphism: $\phi_0 : \mathbb{R}[X] \to \mathbb{R}$ where $\phi_0(f) = f(0)$. Then

$$\ker(\phi_0) = \{\sum_{i=1}^{n} a_i x^i | a_i \in \mathbb{R}\} \tag{92}$$

That is, all polynomials *without* a constant offset.

Definition 34 (Ideal)**.** A subset I of a ring R is called an ideal if the following conditions are satisfied:

1. Additive identity: $0 \in I$, which assures I is non-empty.
2. Closed under addition: For all $a, b \in I$, $a + b \in I$.
3. Multiplication by elements of ring keeps us in ideal: For all $r \in R$ and $a \in I$, $ar, ra \in I$.

Example 49 (Examples of Ideals)**.** The following are examples of ideals.

1. For any ring R, R and $\{0\}$ are ideals.
2. $R = \mathbb{Z}$ and $I = \{\text{Even integers}\}$. Note that 0 is an even integer, the sum of two even integers is an even an integer, and the product of an even integer and any other integer is an even integer.
3. We can generalize this last example to any multiples of a certain integer (the last example was multiples of 2). $R = \mathbb{Z}$ and $I = n\mathbb{Z} = \{kn | k \in \mathbb{Z}\}$, $n \in \mathbb{Z}$.
4. $R = \{f : \mathbb{R} \to \mathbb{R}, f \text{ continuous}\}$ and $I = \{f \in R | f(0) = 0\}$. First note that R is a commutative ring, with the identity element being $f(x) = 1$ for all $x \in \mathbb{R}$ (note that multiplication is defined pointwise). This ideal is the kernel of a ring homomorphism. Indeed, let $\phi : R \to \mathbb{R}$, where $\phi(f) = f(0)$. Then $\ker(\phi) = I$.

Theorem 42 (Field has only 2 ideals: the trivial ideal and the field itself.)**.** If R is a field, then its ideals are R and $\{0\}$.

Proof. First note that in a field, $0 \neq 1$. Let $\{0\} \neq I \subseteq R$ be an ideal. Take an $0 \neq x \in I$. Since R is a field, x has a multiplicative inverse: there exists an $a \in R$ such that $ax = 1$. Then since I is an ideal and $a \in R$, $ax = 1 \in I$. But then for all $r \in R$, $r = r \times 1 \in I$, since $r \in R$ and $1 \in I$. Thus $I = R$, since $I \subseteq R$, but for all $r \in R$, $r \in I$. $\square$

Theorem 43 (There are only 2 ideals in $M_{n\times n}(\mathbb{R})$)**.**

Theorem 44 (Kernel of homomorphism of rings is an ideal of the ring which is the domain of the homomorphism)**.** Suppose A, B are rings and let $\phi : A \to B$ be a ring homomorphism. Then $\ker(\phi)$ is an ideal of A.

Proof. We verify the 3 conditions:

1. Identity: $0 \in \ker(\phi)$ because $\ker(0) = 0$.

2. Addition: Take $a, b \in \ker(\phi)$. We want to show that $(a+b) \in \ker(\phi)$, which means that $\phi(a+b) = 0$. To show this,
$$\phi(a+b) = \phi(a) + \phi(b) = 0 + 0 = 0 \tag{93}$$

3. Multiplication: Take $a \in \ker(\phi)$ and $r \in A$. We want to show that $ar, ra \in \ker(\phi)$, or that $\phi(ar) = \phi(ra) = 0$. To show this,
$$\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0 \tag{94}$$
and
$$\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0 \tag{95}$$

□

Theorem 45 (Ideal is an additive normal subgroup)**.** Suppose A is a ring and I is an ideal of A. Then I is an an additive normal subgroup A.

Proof. I is an ideal, so it is a subgroup of the ring under addition. By the definition of a ring, the elements of A under addition are an abelian group. Thus a subgroup of an abelian group is normal, so I is normal. □

Definition 35 (Multiplication on A/I)**.** Let A be a ring and $I \subset A$ an ideal. We define multiplication on A/I by
$$(I+a)(I+b) = I + ab \tag{96}$$
Further, A/I is a ring.

Theorem 46. Suppose $\phi : A \to A/I$ is a homomorphism of rings where $\phi(a) = I + a$. Then
$$\ker(\phi) = I \tag{97}$$

Proof. We prove this statement directly:
$$\begin{aligned}
\ker(\phi) &= \{a \in A | \phi(a) = 0\} \\
&= \{a \in A | \phi(a) = I + 0 = I\} && (I \text{ is the trivial element of the quotient}) \\
&= \{a \in A | I + a = I\} \\
&= \{a \in I\} \\
&= I
\end{aligned}$$

$\square$

2.4 Practice

Exercise 9. Is $(\mathbb{Z}/14\mathbb{Z})^{\times}$ cyclic?

Solution 9. Recall that

$$(\mathbb{Z}/14\mathbb{Z})^{\times} = \{1, 3, 5, 9, 11, 13\} \tag{98}$$

1 clearly can't generate the group. Try 3:

$$\begin{aligned} 3^1 &= 3 \\ 3^2 &= 9 \\ 3^3 &= 13 \\ 3^4 &= 11 \\ 3^5 &= 5 \\ 3^6 &= 1 \end{aligned}$$

Thus the group is cyclic since it is generated by 3.

Remark 5. Recall the following theorem: If G is a cyclic subgroup, then if m divides $|G|$, then G has a unique (cyclic) subgroup of order m. Thus, if we can find more than one subgroup of a particular order, then the group cannot be cyclic.

Exercise 10. How many subgroups does $\mathbb{Z}/20\mathbb{Z}$ have?

Solution 10. $\mathbb{Z}/20\mathbb{Z}$ is a cyclic subgroup of order 20. Thus it has a unique subgroup for each integer which divides the order of the subgroup. The divisors of 20 are $1, 2, 4, 5, 10, 20$, so 6 subgroups.

Exercise 11. Let G, H be finite groups. Suppose that $|G|, |H|$ are coprime (that is, no number apart from 1 which divides both). Let $\phi : G \to H$ be a homomorphism. Show that for all $g \in G$, $\phi(g) = 1$.

Solution 11. We need to show that $Im(\phi) = 1$. We know that $1_H \in Im(\phi)$, so this also implies that $|Im(\phi)| = 1$. We know that $Im(\phi) \leq H$. So by Lagrange's Theorem, $|Im(\phi)|$ divides the size of H. The first isomorphism theorem implies that

$$\frac{|G|}{|\ker(\phi)|} = |Im(\phi)| \tag{99}$$

Hence $|Im(\phi)|$ divides $|G|$. Coprimality assumption implies that $|Im(\phi)| = 1$.

Exercise 12. Let G be a group, take $g \in G$. Define

$$C_G(g) = \{x \in G | xg = gx\} \tag{100}$$

Solution 12. $C_G(g)$ is clearly a subset. We need to verify 3 axioms:

1. Identity: $1 \in C_G(g)$, since $1g = g1$ for all $g \in G$.
2. Closed under products: Take $a, b \in C_G(g)$. We want to show that $ab \in C_G(g)$. Take $g \in G$.
$$(ab)g = a(bg) = a(bg) = (ag)b = (ga)b = g(ab) \tag{101}$$
3. Closed under inverses: Let $a \in C_G(g)$. We want to show that $a^{-1} \in C_G(g)$.
$$a^{-1}g = a^{-1}g1 = a^{-1}gaa^{-1} = a^{-1}aga^{-1} = 1ga^{-1} = ga^{-1} \tag{102}$$

Exercise 13. Write
$$(12)(134)(13)(25) \tag{103}$$
as a product of disjoint cycles.

Solution 13. Pick a number and see where it goes.
$$(1425)(3) \tag{104}$$

Exercise 14. Let G, H be groups and let $\phi : G \to H$ be a surjective homomorphism. Suppose that G is abelian. Prove that H is abelian.

Solution 14. Let $a, b \in H$. Thus there exists $x, y \in G$ such that $\phi(x) = a$ and $\phi(y) = b$. Then
$$ab = \phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x) = ba \tag{105}$$

Exercise 15. Show that $\mathbb{Z}/12345\mathbb{Z}$ is not an integral domain.

Solution 15. 12345 is divisible by 5. Hence there exists $t \in \mathbb{Z}$ such that $5t = 12345$. Therefore, in $\mathbb{Z}/12345\mathbb{Z}$, $5t = 0$, but $5, t \neq 0$. Thus the group is not an integral domain.

Exercise 16. Let G be a finite group acting transitively on a finite set X with $|X| > 1$. Show that there exists $g \in G$ such that $gx \neq x$, for all $x \in G$.

Solution 16. We want to show that there exists a $g \in G$ such that $X^g = \varnothing$ (thus, no x fix g). Equivalently, there exists a $g \in G$ such that $|X^g| < 1$. By Burnside's theorem, the number of orbits of the action of G on X is
$$N = \frac{1}{|G|} \sum_{g \in G} |X^g| \tag{106}$$

Since the action is transitive, there is only one orbit. Thus,
$$|G| = \sum_{g \in G} |X^g| \tag{107}$$

For the identity element $g = 1$,
$$|X^g| = |X| > 1 \tag{108}$$
But to make the average less than 1, we meed to have a set with less than one element.

3 Practice Quizzes

The course did not give solutions to any practice quizzes, questions etc., so be wary of the solutions I've written below.

3.1 Quiz 1

Exercise 17. Give an example of $\sigma \in S_3$ such that σ has order 3.

Solution 17. 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 18. Give an example of $\tau \in S_5$ such that τ has order 6.

Solution 18. Consider $\tau = (123)(45)$. Then $\tau^2 = (132)(4)(5)$, $\tau^3 = (1)(2)(3)(45)$, $\tau^4 = (123)(4)(5)$, $\tau^5 = (132)(45)$, $\tau^6 = (1)(2)(3)(4)(5)$.

3.2 Quiz 2

Exercise 19. Let $\tau \in S_6$. Show that

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

Solution 19. We can show this element by element. Observe that

$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(5)) = \tau \cdot (54132)(5) = \tau(4) \tag{109}$$

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

$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(4)) = \tau \cdot (54132)(4) = \tau(1) \tag{110}$$
$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(1)) = \tau \cdot (54132)(1) = \tau(3) \tag{111}$$
$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(3)) = \tau \cdot (54132)(3) = \tau(2) \tag{112}$$
$$\tau \cdot (54132) \cdot \tau^{-1}(\tau(2)) = \tau \cdot (54132)(2) = \tau(5) \tag{113}$$

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

Exercise 20. 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 20. 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

$$\phi(x) = gxg^{-1} = gyg^{-1} = \phi(y) \tag{114}$$

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

$$\phi(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y \tag{115}$$

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

3.3 Quiz 3

Exercise 21. 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 21. First suppose ϕ is a homomorphism. Let $a, b \in G$. Then

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

Thus G is abelian.

Next suppose G is abelian. Fix $a, b \in G$. Note that $ab = ba$. Now,

$$\begin{aligned}\phi(ab) &= (ab)^{-1} && \text{(definition of } \phi\text{)} \\ &= b^{-1}a^{-1} \\ &= a^{-1}b^{-1} && \text{(}G\text{ abelian)} \\ &= \phi(a)\phi(b)\end{aligned}$$

Thus ϕ is a homomorphism, since for all $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Exercise 22. 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 22. Observe that H is a set of permutations that fix 4 and 5. We need to check the three subgroup axioms:

1. Identity: the identity permutation also fixes 4 and 5.
2. Closed under products: The product (under composition) of two permutations that fix 4 and 5 will also fix 4 and 5.
3. Closed under inverse: same as above.

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 $[S_5 : H] = 10$.

3.4 Quiz 4

Solution 23. Let G be a group and let $H, K \lhd G$. Show that $HK \lhd G$, where $HK = \{hk | h \in H, k \in K\}$. Show HK is a subgroup and normal.

Exercise 23. We first check the three axioms needed to be a subgroup:

1. Identity: Since H, K both subgroups, they each contain the identity. Thus, $1 \in H, 1 \in K$, so $1 \in HK$.
2. Closed under products: Let $a, b \in HK$. Thus there exist $h, h' \in H$ and $k, k' \in K$ such that $a = hk$ and $b = h'k'$. Since K is a normal subgroup in G, we know that for all $k \in K$ and $h' \in H \subseteq G$, there exists and $\tilde{h} \in H$ such that $kh' = \tilde{h}k$. Thus,
$$hkh'k' = h\tilde{h}kk' \tag{116}$$
Since H, K are each subgroups, they are closed under multiplication. Thus, $h\tilde{h}kk' = h''k'' \in HK$ for some $h'' \in H$ and $k'' \in K$. Thus HK is closed under products.
3. Closed under inverses: Let $g = hk \in HK$. Then $g^{-1} = (hk)^{-1} = k^{-1}h^{-1}$. Since K is a normal subgroup in G, for all $k^{-1} \in K$ and $h^{-1} \in H$, there exists a $\tilde{h} \in H$ such that
$$k^{-1}h^{-1} = \tilde{h}k^{-1} \tag{117}$$
Therefore $g^{-1} = \tilde{h}k^{-1} \in HK$. Thus $g^{-1} \in HK$, so that HK is closed under inverses.

Next we show the subgroup is normal. Let $a = hk \in HK$ and fix $g \in G$. Then
$$ghkg^{-1} = ghg^{-1}gkg^{-1} = (ghg^{-1})(gkg^{-1}) \tag{118}$$
Since H, K are normal in G, we can find a $\tilde{h}$ and $\tilde{k}$ such that $ghg^{-1} = \tilde{h}$ and $gkg^{-1} = \tilde{k}$. Thus, $ghkg^{-1} = \tilde{h}\tilde{k} \in HK$. Thus, $gag^{-1} \in HK$ for all $a \in HK$. Thus HK is a normal subgroup of G.

Exercise 24. Show that S_3 is not cyclic.

Solution 24. Cyclic groups are abelian. S_3 is not abelian, so not cyclic.

Exercise 25. Show that the subgroup of rotations is normal in D_n ($n \geq 3$).

Solution 25. Let P be the cyclic subgroup of rotations. Let $l \in P$. Thus, $l \in \rho^j$ for some j. We will show that $glg^{-1} \in P$ for all $g \in D_n$. There are two cases to consider. First suppose that g is a mirror symmetry. Then $g = \epsilon\rho^i$ for some i. In this case,

$$\begin{aligned} \epsilon\rho^i\rho^j(\epsilon\rho^i)^{-1} &= \epsilon\rho^i\rho^j\rho^{-i}\epsilon^{-1} \\ &= \epsilon\rho^i\rho^j\rho^{-i}\epsilon \\ &= \epsilon\rho^j\epsilon \\ &= \rho^{-j}\epsilon\epsilon \\ &= \rho^{-j} \in P \end{aligned}$$

since P cyclic and $\rho \in P$. For the second case, suppose g is rotation. Thus $g = \rho^i$ for some i. Then

$$\rho^i\rho^j\rho^{-i} = \rho^j \in P \tag{119}$$

Thus $g\rho^j g \in P$ for all $g \in D_n$, so that P is a normal subgroup.

3.5 Quiz 5

Exercise 26. Let H be a subgroup of $\{1, \rho, \ldots, \rho^{n-1}\}$. Show that $H \trianglelefteq D_n$.

Solution 26. We will show that for all $g \in D_n$ and for all $h \in H$, $ghg^{-1} \in H$. We will prove this by cases (whether g is a rotation or a mirror symmetry). Further, since $h \in H$, we know that $h = \rho^i$ for some $i \in \{0, 1, \ldots, n-1\}$.

1. Case 1: g is a rotation. Then $g = \rho^j$ for some $j \in \{0, 1, \ldots, n-1\}$. Then

$$ghg^{-1} = \rho^j\rho^i\rho^{-j} = \rho^i \in H \tag{120}$$

2. Case 2: g is a mirror symmetry. Then $g = \epsilon\rho^j$ for some $j \in \{0, 1, \ldots, n-1\}$. Then,

$$\begin{aligned} ghg^{-1} &= (\epsilon\rho^j)\rho^i(\epsilon\rho^j)^{-1} \\ &= \epsilon\rho^j\rho^i\rho^{-j}\epsilon^{-1} \\ &= \epsilon\rho^j\rho^i\rho^{-j}\epsilon \\ &= \epsilon\rho^i\epsilon \\ &= \epsilon\epsilon\rho^{-i} \\ &= \rho^{-i} \in H && \text{(since } H \text{ is a subgroup, contains inverses)} \end{aligned}$$

Exercise 27. Let τ be a reflection (a mirror symmetry). Show that $G = \{1, \tau\} \leq D_n$ but $\{1, \tau\} \ntrianglelefteq D_n$.

Solution 27. We first show that $G \leq D_n$. Therefore we must verify the three axioms.

1. Identity: Clearly $1 \in G$.
2. Closed under products: Observe that
   (a) $1 \cdot \tau = \tau \in G$
   (b) $\tau \cdot 1 = \tau \in G$
   (c) $1 \cdot 1 = 1 \in G$
   (d) $\tau \cdot \tau = \tau^2 = 1 \in G$ since τ is a mirror symmetry, we know $\tau^2 = 1$.
3. Closed under inverses: Note that $1^{-1} = 1 \in G$. Since τ is a mirror symmetry, we know $\tau = \tau^{-1} \in G$.

To show that G is not a normal subgroup, we will find an element $g \in D_n$ such that $g\tau g^{-1} \notin G$. Suppose $g = \tau\rho$. Then

$$\begin{aligned} g\tau g^{-1} &= \tau\rho\tau\rho^{-1}\tau^{-1} \\ &= \tau\rho\tau\rho^{-1}\tau \\ &= \tau\rho\rho\tau\tau \\ &= \tau\rho^2\tau^2 \\ &= \tau\rho^2 \end{aligned}$$

But we needn't have that $\tau\rho^2 \in G$.

3.6 Quiz 6

Exercise 28. Let G be a group that acts on a set X. Take $G = GL_2(\mathbb{R})$ and $X = \mathbb{R}^2$. The actions is $A(v) = Av$ where $A \in GL_2(\mathbb{R})$ and $v \in \mathbb{R}^2$. Let $H = \langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$. Find $O\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right)$.

Solution 28. Observe that the generator of H is a rotation. Thus the orbit is simply given by

$$\left\{ \begin{pmatrix} -2 \\ 1 \end{pmatrix}, \begin{pmatrix} -2 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right\} \tag{121}$$

Exercise 29. Let G be a group acting on a set X and let $x, y \in X$. Suppose that for some $g \in G$ we have $gx = y$. Show $gG_xg^{-1} = G_y$.

Solution 29. We show two inclusions.

1. $\subseteq$: First let $h \in G_x$. We want to show that $ghg^{-1} \in G_y$, so that $ghg^{-1}(y) = y$. Then

$$\begin{aligned} ghg^{-1}(y) &= gh(x) && (g(x) = y \text{ implies } x = g^{-1}(y)) \\ &= g(x) && (\text{since } h \in G_x) \\ &= y \end{aligned}$$

   Therefore $gG_xg^{-1} \subseteq G_y$.

2. $\supseteq$: Fix $h \in G_y$. We want to show that $h \in gG_xg^{-1}$, or that there exists some $h' \in G_x$ such that $h = gh'g^{-1}$. Let $h' = g^{-1}hg$, and we'll show $h' \in G_x$. Then

$$\begin{aligned} g^{-1}hg(x) &= g^{-1}h(y) \\ &= g^{-1}(y) && (\text{since } h \in G_y) \\ &= x \end{aligned}$$

   Thus $h' \in G_x$. This implies that$h = gh'g^{-1} \in gG_xg^{-1}$ so that $gG_xg^{-1} \supseteq G_y$.

3.7 Quiz 7

Exercise 30. In how many ways can we color the vertices of a 5-gon using 10 colors, up to equivalence.

Solution 30. We apply Burnside's formula, where N is the number of colorings (i.e. the number of orbits) and $G = D_5$:

$$N = \frac{1}{|G|} \sum_{g \in G} |X^g| \tag{122}$$

We'll solve this question for an arbitrary number of colors k. Consider a rotation. All the vertices must have the same color. Thus there are k possible colorings for a rotation, and there are 4 non-trivial rotations. Since 5 is odd, all mirror symmetries are alike, in that the mirror symmetry goes through a vertex and the mid-point of the opposite edge. For a 5-gon, this mirror symmetry allows for k^3 colorings. Thus, in sum we have

$$\frac{1}{10}(k^5 + 4 \times k + 5 \times k^3) \tag{123}$$

3.8 Quiz 8

Exercise 31. Show that $(\mathbb{Z}/13\mathbb{Z})^\times$ is cyclic.

Solution 31. Notice that 2 generates the group.

Exercise 32. Show that $(\mathbb{Z}/15\mathbb{Z})^\times$ is not cyclic.

Solution 32. Recall that if G is a cyclic subgroup, then if m divides $|G|$, then G has a unique (cyclic) subgroup of order m. Note that $|(\mathbb{Z}/15\mathbb{Z})^\times| = 8$. 2 divides 8 so if $(\mathbb{Z}/15\mathbb{Z})^\times$ is cyclic, then it must have a unique subgroup of order 2. However, we can find two. Consider $\{1, 14\}$ and $\{1, 4\}$. Each of these is a cyclic subgroup of order 2, therefore $(\mathbb{Z}/15\mathbb{Z})^\times$ is not cyclic.

3.9 Quiz 9

Exercise 33. Let G be a subgroup, let P be a subgroup of G of order 21, and let Q be a subgroup of G of order 40. Show that $P \cap Q = \{1\}$.

Solution 33. First notice that 21 and 40 are coprime. Next, we know that the order of an element in a group must divide the order of a group (immediate consequence of Lagrange's theorem). Thus P can have elements with orders $1, 3, 7, 21$. Q can have elements with orders 1, 2, 4, 5, 8, 10, 20, 40. Thus the only comment element to both P and Q can be the identity element.

Exercise 34. In how many (inequivalent) ways can one color the vertices of a regular hexagon (6-gon) using 10 colors?

Solution 34.

Solution 35. Let G be a group. Let $x, y \in G$ be two elements that belong to the same conjugacy class, and let $\phi : G \to A$ be a homomorphism to an abelian group A. Show that $\phi(x) = \phi(y)$. Now suppose $G = GL_2(\mathbb{R})$. Are

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \tag{124}$$

in the same conjugacy class?

Exercise 35. Since x, y are in the same conjugacy class, there must exist some $g \in G$ such that $gxg^{-1} = y$. Then

$$\begin{aligned} \phi(y) &= \phi(gxg^{-1}) \\ &= \phi(g)\phi(x)\phi(g^{-1}) \\ &= \phi(g)\phi(x)\phi(g)^{-1} \\ &= \phi(g)\phi(g)^{-1}\phi(x) && \text{(since } A \text{ is abelian)} \\ &= \phi(x) \end{aligned}$$

Take ϕ to be the determinant homomorphism. If the matrices are in the same conjugacy class, they must have the same determinant. The determinants are -1 and 1 respectively. Thus they are not in the same conjugacy class.

Exercise 36. Define

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{R} \right\} \tag{125}$$

Show that H is a subgroup of $GL_3(\mathbb{R})$ and that $Z(H)$ is isomorphic to $\mathbb{R}$.

Solution 36. We check the 3 axioms required to be a subgroup:

1. Identity: The identity matrix is unit upper triangular.
2. Closed under products: The product of two unit upper triangular matrices is also unit upper triangular.
3. Closed under inverses: The inverse of a unit upper triangular matrix is also a unit upper triangular matrix.

We next demonstrate an isomorphism between $Z(H)$ of $\mathbb{R}$.

3.10 Quiz 10

Exercise 37. Given an example of a 5-Sylow subgroup of S_{10}. Is it unique?

Solution 37. In the expansion of 10!, there are two powers of 5: 5 and 10. Thus, a 5-Sylow subgroup of S_{10} will have $5^2 = 25$ elements. Take two disjoint 5-cycles: $(1,2,3,4,5)$ and $(6,7,8,9,10)$. Now consider the subgroup generated by these two cycles:

$$H = \langle (1,2,3,4,5)(6,7,8,9,10) \rangle \tag{126}$$

Each element will be of the form $(1,2,3,4,5)^m(6,7,8,9,10)^n$ where $m,n \in \{0,1,2,3,4\}$. Disjoint cycles commute. Thus the subgroup has 25 elements.

The subgroup is not unique. A p-Sylow subgroup is unique if and only if $H \trianglelefteq G$. Take $(16) \in S_{10}$. Then consider

$$(1,6)(1,2,3,4,5)(6,7,8,9,10)(6,1) \tag{127}$$

This permutation sends 1 to 7, which can't happen with a permutation in H since the cycles are disjoint.

Exercise 38. Give an example of a 3-Sylow subgroup of D_6. Is it unique?

Solution 38. D_6 has 12 elements. The highest power of 3 that divides 12 is 1, so we are looking for a subgroup of size 3. We can take a subgroup of rotations:

$$H = \{1, \rho^2, \rho^4\} \tag{128}$$

This is indeed a subgroup since it contains the identity, is closed under products, and closed under inverse. This subgroup is normal, so it is unique.

3.11 Quiz 11

Exercise 39. Show that the ring $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain.

Solution 39. A commutative ring is an integral domain if for all $a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$. Consider the element $(0, 1)$ and $(1, 0)$. Then their product is $(0, 0)$, but neither is the additive identity.

Exercise 40. Show that the collection of polynomials whose coefficients sum up to 0 (call this set I) is an ideal in $\mathbb{R}[X]$.

Solution 40. We need to check three conditions:

1. Additive identity: Notice that the polynomial 0 has coefficients that add up to 0. Thus $0 \in I$.

2. Closed under addition: Let $a = \sum_{i=0}^{n} a_i x_i$ and $b = \sum_{i=0}^{m} x_i$ be two polynomials whose coefficients add up to 0. WLOG, assume $n \geq m$. The the sum of the coefficients of $a + b$ is
$$\sum_{i=0}^{m} (a_i + b_i) + \sum_{i=m+1}^{n} a_i = 0 \tag{129}$$

3. Multiplication by elements of ring keeps us in ideal: Let $r \in \mathbb{R}]X]$. Note that a polynomial evaluated at 1 gives us the sum of the coefficients. Thus
$$(ra)(1) = r(1)a(1) = r(1) \cdot 0 = 0 \tag{130}$$
and similar for ar.

Exercise 41. Show that $\mathbb{R}[X]^{\times} = \mathbb{R}[X]$.

Solution 41. The inverses of polynomials of order higher than 1 are not polynomials. So only 0th order polynomials (i.e., constants or real numbers) are invertible.

Exercise 42. Show that any field is an integral domain.

Solution 42. Let A be a field. A field is a a commutative division ring. Thus every non-zero element of A is invertible. So, take two elements $x, y \in A$, non-zero, such that $xy = 0$. Then
$$xy = 0 \implies x^{-1}xy = x^{-1}0 \implies y = 0 \tag{131}$$
which is a contradiction. So y must be zero, implying A is an integral domain.

Exercise 43. Show that $\mathbb{Z}$ has only one subring.

Solution 43. Let A be a subring of $\mathbb{Z}$. We show $A = \mathbb{Z}$. It's clear that $A \subseteq \mathbb{Z}$. Now we show $\mathbb{Z} \subseteq A$. Let $z \in \mathbb{Z}$. Since $0, 1 \in A$ (by definition of subring), $0 - 1 = -1 \in A$. But then $1 + 1 = 2 \in A$. By induction, we can construct any positive or negative integer.

Exercise 44. Show that $\mathbb{Z}^\times = \{\pm 1\}$.

Solution 44. It's clear that the only integers with inverses that are also integers are ± 1.

Exercise 45. Show that $\mathbb{Z}/123456789\mathbb{Z}$ is not an integral domain.

Solution 45. Notice that 123456789 is divisible by 3. Thus there exists some $t < 123456789$ such that $3t = 123456789 = 0$. Thus, there exist non-zero elements whose product is 0. Therefore the ring is not an integral domain.

Exercise 46. Show that $\mathbb{Z}/7\mathbb{Z}$ is an integral domain.

Solution 46. Any field is an integral domain, so we show that $\mathbb{Z}/7\mathbb{Z}$ is a field. First not that $\mathbb{Z}/7\mathbb{Z}$ is a commutative ring. Now we show that each non-zero element has a multiplicative inverse. Indeed,

$$\begin{aligned} 1 \cdot 1 &= 1 \\ 2 \cdot 4 &= 8 = 1 \\ 3 \cdot 5 &= 15 = 1 \\ 6 \cdot 6 &= 36 = 1 \end{aligned}$$

Thus $\mathbb{Z}/7\mathbb{Z}$ is a commutative division ring, so it is a field.

Exercise 47. Let $\phi : A \to B$ be a homomorphism of rings. Suppose that A is a field, and that B is nontrivial. Prove that ϕ is injective.

Solution 47. A homomorphism is injective if and only if its kernel is injective. Suppose there is a non-zero element $a \in \ker(\phi)$. Then $\phi(a) = 0$. Since A is a field, a has an inverse, call it b. Then

$$1 = \phi(1) = \phi(ab) = \phi(a)\phi(b) = 0 \cdot \phi(b) = 0 \tag{132}$$

which is a contradiction since B is nontrivial (so $0 \neq 1$).

Exercise 48. Show that for any ring A there exists a unique homomorphism $\tau : \mathbb{Z} \to A$.

Solution 48. We will construct a ring homomorphism and show it must be unique. By definition, we must have that

$$\tau(1) = 1 \tag{133}$$

Since a homomorphism must preserve addition, we must have that

$$f(0) = f(0) + f(0) \tag{134}$$

Thus cancellation gives that

$$f(0) = 0 \tag{135}$$

Next,

$$0 = f(0) = f(1 + -1) = f(1) + f(-1) \tag{136}$$

Therefore

$$f(-1) = -f(1) = -1_A \tag{137}$$

Now take a positive integer n:

$$n = 1 + \cdots + 1 \tag{138}$$

Thus we must have that (using repeatedly that ring homomorphisms preserve addition)

$$f(n) = f(1) + \cdots + f(1) \tag{139}$$

so that

$$f(n) = 1_A + \cdots + 1_A = n \tag{140}$$

And a negative integer can be written as

$$f(n) = -1_A + \cdots + -1_A \tag{141}$$

Thus we must have that

$$f(n) = n \tag{142}$$

which shows that the ring homomorphism must be unique.

4 Practice Exercises

4.1 Practice 1

Exercise 49. Show that the group S_3 is not abelian.

Solution 49. 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 50. Is the set $\mathbb{R}$ of real numbers with the binary operation of subtraction a group?

Solution 50. No. The associativity axiom fails. To see this, observe that $3 - (2 - 1) = 2$ but $(3 - 2) - 1 = 0$.

Exercise 51. 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 51. 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 52. Give an example of $\sigma \in S_3$ such that $\sigma \neq 1$ and $\sigma\sigma \neq 1$.

Solution 52. Consider $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$. Then, $\sigma\sigma(1) = 3$. Therefore, $\sigma\sigma \neq 1$.

Exercise 53. Is the set of positive real numbers with the binary operation of multiplication a group?

Solution 53. 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 54. Show that the set $G = \{z \in \mathbb{C} : z^7 = 1\}$ is a group under multiplication.

Solution 54. 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 55. Let G be a group in which $gg = 1$ for each $g \in G$. Show that G is abelian.

Solution 55. 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 Practice 2

Exercise 56. How many elements does the group $S_3 \times \mathbb{Z}/5\mathbb{Z}$ have?

Solution 56. 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 57. Find the order of all elements in $\mathbb{Z}/10\mathbb{Z}$.

Solution 57. $|0| = 1$ (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 58. What is the order of the permutation $(135)(26)(4798)$ in S_{10}?

Solution 58. 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 59. 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 59. Let $\sigma = (i_1 i_2 \ldots i_k)$. We claim that $\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\ldots\tau(i_k))$ (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 $\tau(i_1)$:

$$\tau\sigma\tau^{-1}(\tau(i_1)) = \tau(\sigma(i_1)) = \tau(i_2) \tag{143}$$

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

Exercise 60. Let $\sigma \in S_n$ be a k-cycle. Is σ^2 necessarily a k-cycle?

Solution 60. No. Consider this simple counterexample: (1234). Then $\sigma^2 = (13)(24)$. σ^2 is not a k-cycle.

Exercise 61. 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 61. 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,

$$g^m = \mathbf{g^{-1 \cdot m \cdot -1}} = ((g^{-1})^m)^{-1} = 1^{-1} = 1 \tag{144}$$

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,

$$(g^d)^{-1} = (g^{-1})^d = 1 \tag{145}$$

Therefore $c \leq d$. Next,

$$g^c = ((\mathbf{g^c})^{\mathbf{-1}})^{\mathbf{-1}} = ((g^{-1})^c)^{-1} = 1^{-1} = 1 \tag{146}$$

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

4.3 Practice 3

Exercise 62. 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 62. 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 63. 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 63. 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

$$(A^{-1})^T(B^{-1})^T = (A^{-1})^T(A^{-1})^T \tag{147}$$

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

$$\phi((B^T)^{-1}) = (((B^T)^{-1})^{-1})^T \tag{148}$$

$$= B \tag{149}$$

Therefore ϕ is an isomorphism.

Exercise 64. Let p be a prime number, and let G be a group of order p. Show that G has exactly two distinct subgroups.

Solution 64. 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 65. 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 65. 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 66. Let A be an abelian group, and define $\phi : A \to A$ by $\phi(a) = a^2$. Show that ϕ is a homomorphism.

Solution 66. 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 67. 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 67. 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 kernel 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 68. Let G be a finite group with $|G| > 2$. Show that there are at least two distinct isomorphisms from G to itself.

Solution 68. *Incomplete.*

4.4 Practice 4

Exercise 69. Let H, K be normal subgroups of the group G. Show that $H \cap K$ is also a normal subgroup of G.

Solution 69. 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 70. What is the index of the subgroup $3\mathbb{Z}$ in $\mathbb{Z}$?

Solution 70. $[\mathbb{Z} : 3\mathbb{Z}] = 3$. 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 71. 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 71. $1 \implies 2$: 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

$$gh = ghg^{-1}g = h'g \in Hg \implies gH \subset Hg \tag{150}$$

Similarly,

$$hg = gg^{-1}hg = gh' \in gH \implies Hg \subset gH \tag{151}$$

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

$$ghg^{-1} = gg^{-1}h' = h' \in H \tag{152}$$

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

Exercise 72. Let $H \leq G$ and $K \trianglelefteq G$ be groups, and define the set

$$HK = \{hk : h \in H, k \in K\} \tag{153}$$

show $HK \leq G$.

Solution 72. 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 73. 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 73. 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
$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cd \end{pmatrix} \tag{154}$$
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
$$\frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} \tag{155}$$
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 74. 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 74. 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 75. 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 75. 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 76. 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 76.

4.5 Practice 5

Exercise 77. Write down the order of each element in D_8.

Solution 77. 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

$$(\epsilon\rho^i)(\epsilon\rho^i) = \epsilon\rho^i\rho^{-i}\epsilon = \epsilon^2 = 1 \tag{156}$$

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 78. 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 78. Proof by cases.

Exercise 79. Let G be a group, and let

$$Aut(G) = \{f : G \to G | f \text{ is an isomorphism}\} \tag{157}$$

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 79. 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 80. Let G be a group, and let

$$Z(G) = \{z \in G | zg = gz \text{ for all } g \in G\} \tag{158}$$

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

$$(f(g))(x) = gxg^{-1} \tag{159}$$

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

Solution 80. 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 81. Let G be a group, let $K \trianglelefteq G$, and let $H \leq G$. Show that $K \cap H \trianglelefteq H$.

Solution 81. Since K is a normal subgroup of G, we know that

$$gkg^{-1} \in K \quad \forall k \in K, \forall g \in G \tag{160}$$

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

$$gxg^{-1} \in H \quad \forall x \in H \cap K, \forall g \in H \tag{161}$$

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

Solution 82. 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 Practice 6

Exercise 83. Let G be a group, and let N be a normal subgroup of G. Define a function

$$\phi : G \to G/N \tag{162}$$

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

Solution 83. 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 84. Let G be a group, and let $g \in G$. Show that

$$\{1, g\} \trianglelefteq G \tag{163}$$

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

Solution 84. $\Rightarrow$ 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 85. For any group G, show that $G/Z(G)$ is isomorphic to a subgroup of $Aut(G)$.

Solution 85. We will use the First Isomorphism Theorem to prove this statement. Let $\phi : G \to Aut(G)$ by

$$\phi(a) = aga^{-1} \tag{164}$$

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

$$G/ker(\phi) \cong Im(\phi) \tag{165}$$

or in this context

$$G/Z(G) \cong Inn(G) \tag{166}$$

Exercise 86. For the action of $GL_2(\mathbb{R})$ on $\mathbb{R}^2$, find the orbit of each $v \in \mathbb{R}^2$.

Solution 86. 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 87. For the action of $GL_2(\mathbb{R})$ on $\mathbb{R}^2$ describe the stabilizer of each $v \in \mathbb{R}^2$.

Solution 87. 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 88. Let G be a group, and let G act on itself by (left) multiplication. Show that the stabilizer of each element is trivial.

Solution 88. 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 89. For the action of the dihedral group D_4 on the vertices of a square, determine the size of a vertex stabilizer.

Solution 89. 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.

4.7 Practice 7

Exercise 90. In how many ways can one color the vertices of a 5-gon using 7 colors?

Solution 90. Let's first consider the fixed points of the mirror symmetries. Since a pentagon has an odd number of vertices, all of its mirror symmetries are of the form vertex to midpoint. Therefore, all mirror symmetries will behave the same. By the figure below, we see that we need vertices 2 and 5 to have the same color, 3 and 4 to be the same color, and 1 can be another color. Therefore, there are 7^3 fixed colorings for each mirror symmetry (of which there are 5).

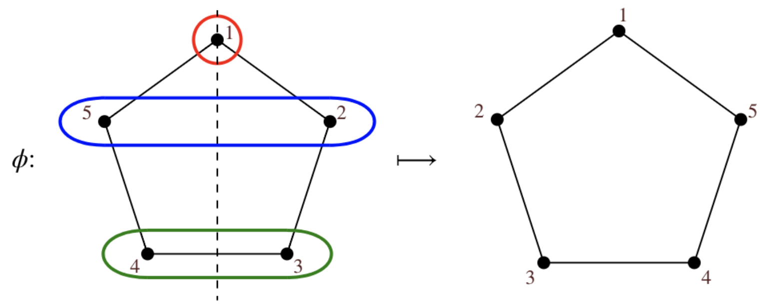

Figure 6.2.1. *The cycles in a vertex permutation.*

Figure 3: Pentagon Mirror Symmetries

Now let's consider the rotations. For ρ, all vertices must be the same color. Thus, there are 7 fixed colorings for ρ. Actually, for a pentagon, all rotations must consist of a single cycle (except the identity), so there are 7 fixed colorings for each rotation. The identity permutation fixes everything, so there are 7^5 possible colorings. Then by Burnside's theorem, the solution is

$$\frac{1}{10}(7^5 + 4 \times 7 + 5 \times 7^3) \tag{167}$$

Exercise 91. Verify by direct calculation that Burnside's formula for the number of orbits holds for the action of D_4 on the vertices of a square.

Solution 91. By inspection, there is only one orbit. The identity element has 4 fixed points. Then, the rotations have no fixed points/vertices. The two mirror symmetries that connect a vertex to a vertex each have two fixed points/vertices. The remaining two mirror symmetries (which go from midpoint to midpoint) have no fixed points. Therefore, by Burnside's formula, the number of orbits N of the action of D_4 on the vertices of a square is

$$\frac{1}{8}(4+0+0+0+0+2+0+2) = 1 \tag{168}$$

Exercise 92. Let a group G act on itself by conjugation. Show that the action is faithful if and only if $Z(G) = \{1\}$.

Solution 92. $\rightarrow$ Suppose the action is faithful. This means that if $gxg^{-1} = x$ for all $x \in G$, then $g = 1$. Then

$$\begin{aligned} Z(G) &= \{g \in G | gx = xg \quad \forall x \in G\} \\ &= \{g \in G | x = gxg^{-1} \quad \forall x \in G\} \\ &= \{1\} && \text{(since the action is faithful)} \end{aligned}$$

$\leftarrow$ Suppose $Z(G) = \{1\}$. Consider a $g \in G$ such that $gxg^{-1} = x$ for all $x \in G$. This implies $gx = xg$ for all $x \in G$, and that $g \in Z(G)$. Therefore $g = 1$, so that the action is faithful.

Exercise 93. Let G be a group such that $G/Z(G)$ is cyclic. Then G is abelian.

Solution 93. Since $G/Z(G)$ is cyclic, there exists an $x \in G$ such that $G/Z(G) = \langle xZ(G) \rangle$. Now fix $g \in G$. There must be some $m \in \mathbb{N}$ such that $gZ(G) = (xZ(G))^m = x^m Z(G)$. This implies that $(x^m)^{-1}g \in Z(G)$, so that there must exist some $z \in Z(G)$ such that $(x^m)^{-1}g = z$. This implies $g = x^m z$. Now consider another element $h \in G$. by the same logic, there must exist an $n \in \mathbb{N}$ and $z' \in Z(G)$ such that $h = x^n z'$. Then

$$\begin{aligned}
gh &= x^m z x^n z' \\
&= x^m x^n z z' && \text{(since } z \in Z(G)\text{)} \\
&= x^{m+n} z' z && \text{(combine powers and } z' \in Z(G)\text{)} \\
&= x^{n+m} z' z \\
&= x^n x^m z' z \\
&= x^n z' x^m z \\
&= hg
\end{aligned}$$

Therefore G is abelian.

Exercise 94. Let G be a group acting on a set X and let $x, y \in X$. Suppose that for some $g \in G$ we have $gx = y$. Show $gG_x g^{-1} = G_y$.

Solution 94. We show two inclusions.

1. $\subseteq$: First let $h \in G_x$. We want to show that $ghg^{-1} \in G_y$, so that $ghg^{-1}(y) = y$. Then

$$\begin{aligned}
ghg^{-1}(y) &= gh(x) && (g(x) = y \text{ implies } x = g^{-1}y) \\
&= g(x) && (\text{since } h \in G_x) \\
&= y
\end{aligned}$$

   Therefore $gG_x g^{-1} \subseteq G_y$.

2. $\supseteq$: Fix $h \in G_y$. We want to show that $h \in gG_x g^{-1}$, or that there exists some $h' \in G_x$ such that $h = gh'g^{-1}$. Let $h' = g^{-1}hg$, and we'll show $h' \in G_x$. Then

$$\begin{aligned}
g^{-1}hg(x) &= g^{-1}h(y) \\
&= g^{-1}(y) && (\text{since } h \in G_y) \\
&= x
\end{aligned}$$

   Thus $h' \in G_x$. This implies that$h = gh'g^{-1} \in gG_x g^{-1}$ so that $gG_x g^{-1} \supseteq G_y$.

Exercise 95. Let G be a group that acts transitively on a set X. Show that for every $x, y \in X$, we have $G_x \cong G_y$.

Solution 95. We can apply the above exercise to notice that $G_y = gG_x g^{-1}$, where $g(x) = y$ (this g exists by transitivity). We then define a function $\phi : G_x \to G_y = gG_x g^{-1}$ by

$\phi(h) = ghg^{-1}$. We claim that ϕ is an isomorphism (that is is a homomorphism which is injective and surjective).

Exercise 96. Let G be an abelian group that acts transitively and faithfully on a set X. Show that the action is free.

Solution 96.

4.8 Practice 8

Exercise 97. Write explicitly the injective homomorphism from $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ to S_4 given by Cayley's theorem.

Solution 97. Motivated by the proof of Cayley's theorem, we should consider the action of G on itself by (left) multiplication. Observe that $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ has 4 elements: $\{(0,0),(0,1),(1,0),(1,1)\}$. Also note that S_4 permutes 4 elements. This motivates labeling the 4 elements in $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ and using left multiplication to create permutations of elements. For example, call the elements 1, 2, 3, and 4. Then

$$\begin{aligned} 2+1 &= (0,1) = 2 \\ 2+2 &= (0,0) = 1 \\ 2+3 &= (1,1) = 4 \\ 2+4 &= (1,0) = 3 \end{aligned}$$

And we can view this as the permutation $(12)(43)$.

$$\begin{aligned} 3+1 &= (1,0) = 3 \\ 3+2 &= (1,1) = 4 \\ 3+3 &= (0,0) = 1 \\ 3+4 &= (0,1) = 2 \end{aligned}$$

And we can view this as the permutation $(13)(42)$.

$$\begin{aligned} 4+1 &= (1,1) = 4 \\ 4+2 &= (1,0) = 3 \\ 4+3 &= (0,1) = 2 \\ 4+4 &= (0,0) = 1 \end{aligned}$$

And we can view this as the permutation $(14)(32)$. Finally applying $(0,0)$ results in the identity permutation.

Exercise 98. Show that the group $(\mathbb{Z}/11\mathbb{Z})^\times$ is cyclic.

Solution 98. Observe that the element 2 generates $(\mathbb{Z}/11\mathbb{Z})^\times$.

Exercise 99. Show that the group $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic.

Solution 99. Recall that $(\mathbb{Z}/8\mathbb{Z})^\times = \{1,3,5,7\}$. Therefore $|(\mathbb{Z}/8\mathbb{Z})^\times| = 4$. We'll demonstrate two subgroups of order 2, which shows that the group cannot be cyclic. Consider $\{1,3\}$ and $\{1,5\}$. Both of these are (cyclic) subgroups of order 2, which means that $(\mathbb{Z}/8\mathbb{Z})^\times$ cannot be cyclic, since for each m which divides the order of $(\mathbb{Z}/8\mathbb{Z})^\times$, we must have a unique subgroup of order m.

Exercise 100. Find the inverse of each element in $(\mathbb{Z}/13\mathbb{Z})^\times$.

Solution 100. Make multiplication table.

4.9 Practice 9

Exercise 101. Write explicitly the elements of $Z(D_4)$ and of $Z(D_5)$.

Solution 101. More generally, the center of the Dihedral Group D_n is trivial when n is odd. When n is even, the center consists of the identity element together with the 180 degree rotation of the polygon.

Exercise 102. Let G be a group of order 60 that has a normal subgroup of N of order 10. Show that G has a subgroup of index 2.

Solution 102. (Sketchy) By Lagrange's theorem,

$$|G/N| = \frac{|G|}{|N|} = \frac{60}{10} = 6 \tag{169}$$

Then, Cauchy's theorem guarantees the existence of an element $H \leq G/N$ with order 3 (since 3 divides 6). Note that H is a subgroup of order 3. The index of this subgroup in G is then

$$[G/N : H] = \frac{|G|}{|N|} \cdot \frac{1}{|H|} = \frac{6}{3} = 2 \tag{170}$$

Exercise 103. Let G be an abelian group of order divisible by 14. Show that G has an element of order 14.

Solution 103. By Cauchy's theorem, we know there exists an element x of order 2 and an element y of order 7. We then claim that xy has order 14. This result generalizes. If G is an abelian group, and x and y are elements of G with orders m and n respectively, then if m and n are relatively prime, the order of the element xy is mn. We'll prove this more general statement. Note that

$$\begin{aligned}(xy)^{mn} &= x^{mn}y^{mn} && \text{(since } G \text{ is abelian)}\\ &= (x^m)^n(y^n)^m\\ &= 1\end{aligned}$$

Thus the order r of xy divides mn. Given that r is the order of xy, we also know that

$$1 = (xy)^r = x^r y^r \qquad \text{(since } G \text{ abelian)}$$

Further

$$1 = 1^n = x^{rn} y^{rn} = x^{rn}. \qquad \text{(since } y^n = 1\text{)}$$

Thus the order of x, m, divides rn. An analogous argument shows that the order of y, n, divides rm. Thus we get that mn divides r since m and n are relatively prime. Therefore $r = mn$, so that the order of xy is mn.

In the context of this problem, since 2 and 7 are relatively prime, we know that the order of xy is 14.

Exercise 104. Write explicitly the conjugacy classes of D_6 and D_7.

Solution 104. More generally, we can calculate the conjugacy classes of D_n as follows. The identity element always forms its own conjugacy class $\{1\}$. Consider a rotation ρ^k. First conjugate by another rotation ρ^m:

$$\rho^m \rho^k \rho^{-m} = \rho^k$$

Next conjugate by a reflection $\epsilon\rho^m$:

$$\begin{aligned} \epsilon\rho^m \rho^k (\epsilon\rho^m)^{-1} &= \epsilon\rho^m \rho^k \rho^{-m} \epsilon^{-1} \\ &= \epsilon\rho^m \rho^k \rho^{-m} \epsilon \\ &= \epsilon\rho^k \epsilon \\ &= \epsilon\epsilon\rho^{-k} \\ &= \rho^{-k} \end{aligned}$$

Thus, if n is odd, there will be $\frac{n-1}{2}$ conjugacy classes of size 2 that contain a rotation and its inverse rotation (i.e. $\{\rho^{\pm i}\}$). If n is even, there will be $\frac{n}{2} - 1$ conjugacy classes of size 2 that contain a rotation and its inverse rotation.

Consider the reflection ϵ. First conjugate by the rotation ρ^m:

$$\begin{aligned} \rho^m \epsilon \rho^{-m} &= \rho^m \rho^m \epsilon \\ &= \rho^{2m} \epsilon \\ &= \epsilon \rho^{-2m} \end{aligned}$$

Next conjugate by another reflection $\epsilon\rho^m$:

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

Thus, if n is odd, the reflections all fall in the same conjugacy class. If n is even, the reflections will fall into two conjugacy classes: the reflections where the rotation is an even power and the reflections where the rotation is an odd power.

For the specific cases requested:

$$\begin{aligned}D_6: &\quad \{1\},\{\rho,\rho^5\},\{\rho^2,\rho^4\},\{\rho^3\},\{\epsilon,\epsilon\rho^2,\epsilon\rho^4\},\{\epsilon\rho,\epsilon\rho^3,\epsilon\rho^5\}\\ D_7: &\quad \{1\},\{\rho,\rho^6\},\{\rho^2,\rho^5\},\{\rho^3,\rho^4\},\{\epsilon,\epsilon\rho,\dots,\epsilon\rho^6\}\end{aligned}$$

4.10 Practice 10

Let G be a group and let $H \leq G$.

Exercise 105. Show that

$$N_G(H) = \{g \in G | gHg^{-1} = H\} \tag{171}$$

is a subgroup of G. We say that $N_G(H)$ is the normalizer of H in G.

Solution 105. It is clear that $N_G(H)$ is a subset of G. We need to check three axioms:

1. Identity: clearly $1H1^{-1} = H$, since $1 \in H$.
2. Closed under products: let $a, b \in N_G(H)$. Then $aHa^{-1} = H$ and $bHb^{-1} = H$. Then,

$$(ab)H(ab)^{-1} = abHb^{-1}a^{-1} = aHa^{-1} = H \tag{172}$$

3. Closed under inverses. let $a \in N_G(H)$. Then

$$\begin{aligned}&aHa^{-1} = H \implies a^{-1}aHa^{-1} = a^{-1}H\\ &a^{-1}aHa^{-1}a = a^{-1}Ha\\ &a^{-1}Ha = H\end{aligned}$$

Exercise 106. Show that $H \subseteq N_G(H)$.

Solution 106. Let $h \in H$. Note that $h \in G$. Then,

$$hHh^{-1} = H \tag{173}$$

since $h \in H$. Thus $h \in N_G(H)$.

Exercise 107. Show that $N_G(H) = G$ if and only if $H \lhd G$.

Solution 107. Suppose $N_G(H) = G$. Thus $gHg^{-1} = H$ for all $g \in G$. This is precisely the definition of normality. Suppose $H \lhd G$. Then $gHg^{-1} = H$ for all $g \in G$, or that $N_G(H) = G$.

Exercise 108. Give an example where $H = N_G(H)$.

Solution 108.

Exercise 109. Find a 2-Sylow subgroup of S_5 and a 5-Sylow subgroup of S_{24}.

Solution 109. S_5 has order 120. The highest power of 2 that goes into 120 is $2^3 = 8$. Thus we are looking for a subgroup of order 8. Recall that S_5 permutes $\{1, 2, 3, 4, 5\}$. Further, D_4 permutes $\{1, 2, 3, 4\}$ and has 8 elements. Thus, D_4 is a 2-Sylow subgroup of S_5.

Next, S_{24} has order 24!. In the expansion of 24!, there are 4 terms divisible by 5: 5, 10, 15, 20. Thus, a 5-Sylow subgroup will have order 5^4. Take the disjoint cycles

$$(1, 2, 3, 4, 5), \quad (6, 7, 8, 9, 10), \quad (11, 12, 13, 14, 15), \quad (16, 17, 18, 19, 20) \tag{174}$$

Now consider the group generated by the product of these cycles

$$\langle (1, 2, 3, 4, 5)(6, 7, 8, 9, 10)(11, 12, 13, 14, 15)(16, 17, 18, 19, 20) \rangle \tag{175}$$

Each element in this subgroup will be of the form

$$(1, 2, 3, 4, 5)^a (6, 7, 8, 9, 10)^b (11, 12, 13, 14, 15)^c (16, 17, 18, 19, 20)^d \tag{176}$$

where $a, b, c, d \in \{0, 1, 2, 3, 4\}$. Thus the subgroup has 5^4 elements.

4.11 Practice 11

Exercise 110. Let A be a commutative ring. We say that $a \in A$ is invertible if there exists some $b \in A$ such that $ab = 1$. Denote by $A^\times$ the subset of invertible elements in A.

1. Show that $A^\times$ is abelian group.
2. Show that A is a field if and only if $A^\times = A \setminus \{0\}$.
3. Show that $\mathbb{R}[X]^\times = \mathbb{R}^\times$.

Solution 110. We prove each statement as follows:

1. Trivial.
2. Also trivial.
3. Any non-degenerate polynomial does not have an inverse that is also a polynomial.

Exercise 111. Let S be a set, and let $P(S)$ be the collection of all subset of S. Show that $P(S)$ is a commutative ring with respect to the binary operations of symmetric difference and intersection.