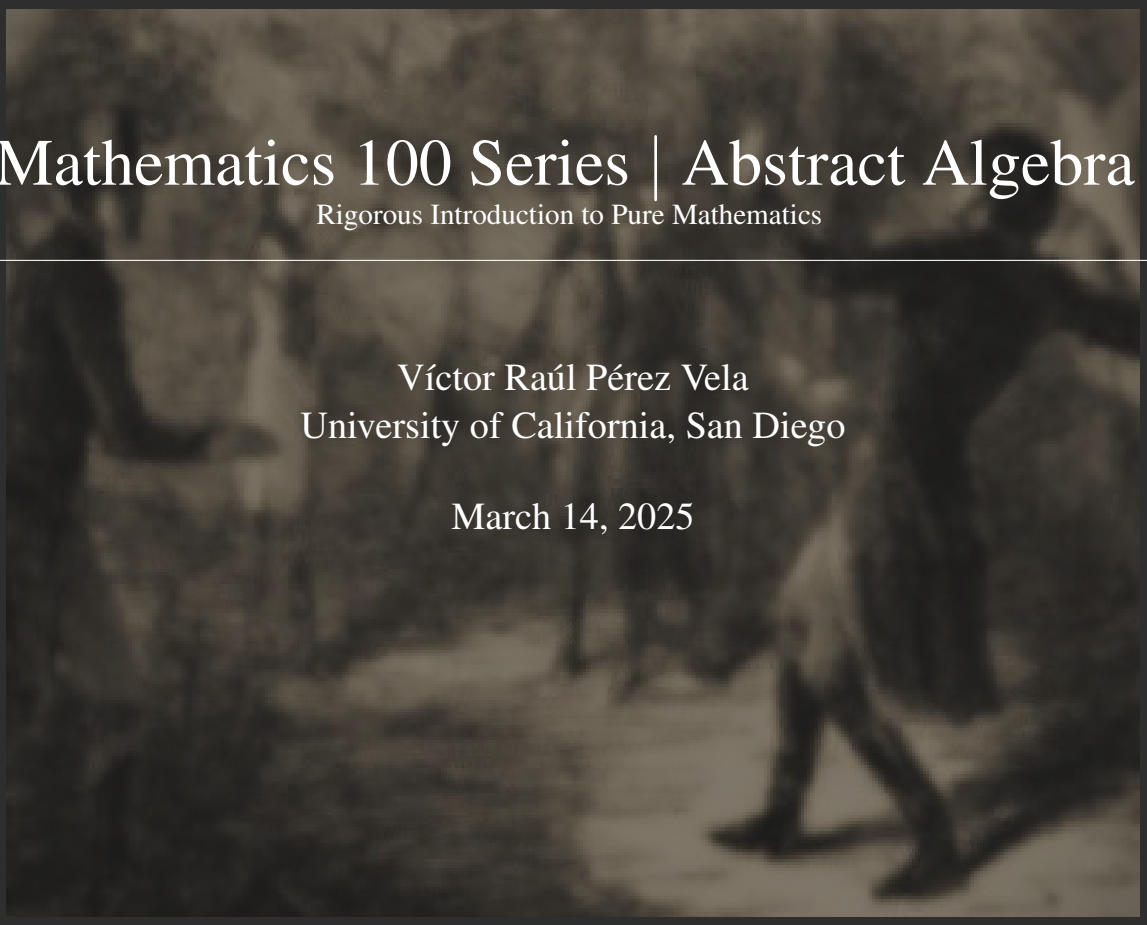
Mathematics 100 Series | Abstract Algebra

Rigorous Introduction to Pure Mathematics



Víctor Raúl Pérez Vela
University of California, San Diego

March 14, 2025

Pages left blank intentionally.

Mathematics 100 Series | Abstract Algebra

Rigorous Introduction to Pure Mathematics

Víctor Raúl Pérez Vela
University of California, San Diego

The efforts of most human-beings are consumed in the struggle for their daily bread, but most of those who are, either through fortune or some special gift, relieved of this struggle are largely absorbed in further improving their worldly lot. Beneath the effort directed toward the accumulation of worldly goods lies all too frequently the illusion that this is the most substantial and desirable end to be achieved; but there is, fortunately, a minority composed of those who recognize early in their lives that the most beautiful and satisfying experiences open to humankind are not derived from the outside, but are bound up with the development of the individual's own feeling, thinking and acting. The genuine artists, investigators and thinkers have always been persons of this kind. However inconspicuously the life of these individuals runs its course, none the less the fruits of their endeavors are the most valuable contributions which one generation can make to its successors.[1]

— Albert Einstein

[1] In letter (1 May 1935), Letters to the Editor, 'The Late **Emmy Noether**: Professor Einstein Writes in Appreciation of a Fellow-Mathematician,' *New York Times* (4 May 1935), 12.

Contents

Part I

Mathematics 100A: Group Theory

Chapter 1

Introduction to Groups

> Group theoretical methods, especially those involving characters and representations, pervade all branches of quantum mechanics.
> — George Mackey

1.1 Laws of Composition

The notion of a law of composition is a foundational piece of mathematics and life. A law of composition is indeed *any* rule on a set S that combines some pairs $a, b \in S$ to get another element in S.

Definition 1.1.0.1 (Law of Composition)**.** *A law of composition m, or a binary operation, is a function of the form $m : S \times S \to S$.*

It is often helpful to see what something isn't to understand what it is. So, for example, addition of odd numbers is not a law of composition because the addition of odd numbers does not give another odd number. Subtraction of natural numbers is not a law of composition because one could get a negative integer by subtracting natural numbers. Exponentiation of real numbers is not a law of compositions because in the case that you take a root of a negative number you get an imaginary number.

Examples: Addition and Multiplication
Addition over integers or real numbers are laws of composition because upon performing the operation, you receive an element from the same set.

$$a_{\mathbb{R}} : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \qquad a_{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$a_{\mathbb{R}}(x, y) = x + y \qquad a_{\mathbb{Z}}(x, y) = x + y$$

While these two are related, they are inherently different because $a_{\mathbb{Z}}$ only wants to 'eat' integers whereas $a_{\mathbb{R}}$ is 'omnivorous.' It has no problem in digesting whatever real, fractional, integer, natural number that you feed it.

Reproduction on species behaves as a law of composition. Two individuals of the same species retrieve another of the same species. Notice that reproduction is not a law of composition in the strict sense. That is because two species could develop a different species as mutations and evolution occur. On the other hand, *synthesis* as a chemical reaction on substances is a law of composition because two substances can be composed to form a new substance.

$$4Fe + 3O_2 + 6H_2O \to 4Fe(OH)_3$$

The above example raises important questions about how to deal with any given binary operation. With respect to the synthesis example, which operation takes precedence? Which goes first, $4Fe + 3O_2$ or $3O_2 + 6H_2O$ and does order matter? is $4Fe + 3O_2 + 6H_2O$ the same as $6H_2O + 3O_2 + 4Fe$? These questions motivate the following important definitions, associativity (definition 1.1.0.2) and commutativity (definition 1.1.0.3).

Definition 1.1.0.2 (Associativity)**.** *A law of composition $m : S \times S \to S$, $m(a, b) = ab$ is associative if for any $a, b, c \in S$ we have that $a(bc) = (ab)c$.*

Example: Combination of Debts is Associative
Suppose you owe the bank certain amounts. Combining these debts is a law of composition because we add these debts to get a debt. This invented law of composition is associative. Notice that if $1,000\$, 5,000\$, 10,000\$$ are debts you have, then you owe

$$1,000\$ + (5,000\$ + 10,000\$) = 16,000\$$$
$$(1,000\$ + 5,000\$) + 10,000\$ = 16,000\$$$

regardless of which debts you look at first.

As it turns out, associative behavior is *foundational* in mathematics. As group theory began emerging and many enthusiast wanted to define what a group is, they noticed that all the groups we'll discuss as well as all the groups they had found *were associative.* A very fundamental property of function composition, which is already permeating all of mathematics by itself, is its associativity.

Proposition 1.1.0.1 (Composition of Functions is Associative)**.** *Let $S := \{f \mid f : T \to T\}$ be the set of functions with domain and codomain T, and let $\circ$ denote composition of functions. Then:*

$$f \circ (g \circ h) = (f \circ g) \circ h, \quad \forall f, g, h \in S$$

Proof. First, take an arbitrary element $x \in T$, notice that this element gets mapped to the same element $f(g(h(x))) \in T$ regardless of the choice of which operation is done first. Therefore, since $f \circ (g \circ h)$ and $(f \circ g) \circ h$ retrieve the same result $f(g(h(x)))$, composition of functions is associative. □

Definition 1.1.0.3 (Commutativity)**.** *A law of composition $m : S \times S \to S$, $m(a, b) = ab$ is commutative if for any $a, b \in S$ we have that $ab = ba$.*

Example: Mixing Acrylic Paints is Commutative
Suppose you have acrylic paints. Mixing paints to get newly colored paints is a law of composition because you get a colored paint out of mixing 2 (or more) colored paints. This invented law of composition is commutative. Notice that if the law of composition were $\text{mix}(\text{color}_1, \text{color}_2)$ and you had paintings (Blue) and (Red) then the order of mixing

$$\text{mix}(\text{Blue}, \text{Red}) = \text{Purple}$$
$$\text{mix}(\text{Red}, \text{Blue}) = \text{Purple}$$

does not give different colors.

Commutativity is not as pervasive as associativity. It still appears frequently though. For example, The union and intersections of sets as laws of compositions are commutative.

Proposition 1.1.0.2 (Union and Intersection of sets is Commutative)**.** *Suppose A and B are arbitrary sets. Then $A \cap B = B \cap A$ as well as $A \cup B = B \cup A$.*

Proof. Suppose A and B are arbitrary sets. Then, by definition:

$$\begin{aligned} A \cap B &:= \{x : x \in A \wedge x \in B\} & A \cup B &:= \{x : x \in A \vee x \in B\} \\ B \cap A &:= \{x : x \in B \wedge x \in A\} & A \cup B &:= \{x : x \in B \vee x \in A\} \\ A \cap B &= B \cap A & A \cup B &= B \cup A \end{aligned}$$

□

Regaining focus on general laws of composition, I usually want to add and multiply and do many things many times and not once. So, can we find a way to combine multiple objects of one kind and get an object of the same kind and does it matter which combination is done first? Here, things get rigorous.

Proposition 1.1.0.3 (Associativity of n elements)**.** *Let an associative law of composition denoted $\cdot$ be given on a set S. There is a **unique way** to define, for all $n \in \mathbb{Z}$, the combination of n elements $a_1, a_2, \ldots, a_n \in S$, in that order, denoted as*

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n$$

which has the following properties:

i. The combination a_1 is just itself.

ii. The combination $a_1 \cdot a_2$ is given by the law of composition $\cdot$.

iii. For any $i \in \mathbb{N}$ such that $1 \leq i < n$, the combination of the n elements could be

$$a_1 \cdot \ldots \cdot a_n = (a_1 \cdot \ldots \cdot a_i) \cdot (a_{i+1} \cdot \ldots \cdot a_n)$$

*where the left hand side of (iii) shows that the right hand side can be split anywhere and still get the same **unique** result.*

Proof. We tackle by strong induction on n. Let $P(n)$ be the assertion that the product of the elements $a_1, a_2, \ldots, a_n$ in that order, is given by $a_1 \cdot \ldots \cdot a_n$. We know $P(1)$ is true because $a_1 = a_1$, so (i) holds. Also, when $n = 2$, we know that $P(2)$ is true by the definition of the law of composition which yields $a_1 \cdot a_2$, so (ii) holds as well. We use these as base case to see what happens for $n \geq 3$.
Suppose that we have defined the product of r elements for $r \in \mathbb{N}$ such that $r \leq n-1$ as $a_1 \cdot \ldots \cdot a_r$ and that this is the unique product which satisfied (iii). Thus, choosing $r = n-1$ we define the product of n elements by

$$a_1 \cdot \ldots \cdot a_n = (a_1 \cdot \ldots \cdot a_{n-1}) \cdot a_n \tag{1.1}$$

where the right hand side is a composition of defined terms only. Therefore, if a product satisfying (iii) existed, then it is given by Equation 1.1 because it is (iii) for $i = n-1$. Thus, if the product of n elements existed, it can be uniquely defined. Now we ought to verify $i < n-1$:

$$\begin{aligned} a_1 \cdot \ldots \cdot \ldots \cdot a_n &= (a_1 \cdot \ldots \cdot a_{n-1}) \cdot a_n && \text{(as defined in 1.1)} \\ &= (a_1 \cdot \ldots \cdot a_i) \cdot (a_{i+1} \cdot \ldots \cdot \ldots \cdot a_{n-1}) \cdot a_n && \text{(inductive hypothesis)} \\ &= (a_1 \cdot \ldots \cdot \ldots \cdot a_i) \cdot ((a_{i+1} \cdot \ldots \cdot a_{n-1}) \cdot a_n) && \text{(associativity)} \\ &= (a_1 \cdot \ldots \cdot a_i) \cdot (a_{i+1} \cdot \ldots \cdot a_n) && \text{(inductive hypothesis)} \end{aligned}$$

Therefore, by strong induction, the assertion $P(n)$ holds for all $n \in \mathbb{N}$. □

It is often useful, per the difficulty of proving that laws of composition are associative, to relate a given law of composition to composition of functions. We saw before that function composition is associative, so for example, matrix multiplication can be seen as some form of function composition making matrix multiplication itself an associative law of composition.

1.2 Identities and Inverses

There is way more juice in the idea of a law of composition. Yet this requires acquiring formality.

Definition 1.2.0.1 (Indentity)**.** *An identity e for a law of composition denoted $\cdot$ in a set S is an element $e \in S$ such that $e \cdot x = x \cdot e = x$, for all $x \in S$.*

Upon the binary operation, identities do not alter any other of the elements of the set nor themselves.

Examples: Various Identities:

- The number zero for addition of integers, rational, real, complex numbers.
- The number one for the same laws of composition.
- The identity matrix I_n for matrix multiplication of matrices in $\mathbb{R}^{n\times n}$.
- Performing a 360° rotation for the set of directions.
- the zero vector $\vec{0}_n$ for vector addition in $\mathbb{R}^n$.

All of thee operations yield no change. If I rotate 60° and then 360°, I only have 60°. If I added 0 to 15, I only have 15. Now, I could rotate 720°, does that mean that there exists many identities? Sadly, no.

Proposition 1.2.0.1 (Identities are Unique)**.** *Suppose e_L and e_R are left and right identities for a law of composition denoted $\cdot$ on S. Meaning, $e_L \cdot x = x \wedge x \cdot e_R = x, \forall x \in S$. Then $x_L = x_R$.*

Proof. Suppose x_L, x_R are identities. Then, $x_L \cdot x_R = x_L$ because x_R is an identity. But wait a second, x_L is also an identity, then $x_L x_R$ = x_R. Therefore, $x_L = x_R$. □

Many mathematicians denote identities as 1 if the law of composition is written multiplicatively, or 0 if the law of composition is written additively. Here, for generality, we denote it as e. When we deal with identities of different sets with laws of composition, say $(A, \cdot)$ and $(S, *)$, we employ the convention that if they had an identity we better call it e_A and e_S respectively.

Whenever an associative law of composition $\cdot$ on a set S has an identity e, we can define *inverses* for which the law of composition acting on an element and its inverse retrieves the identity.

Definition 1.2.0.2 (Inverses)**.** *Suppose an associative law of composition on S, denoted $\cdot$, has an identity e. If there exists some element $b \in S$ such that for some $a \in S$ we have $a \cdot b = b \cdot a = e$, then we say that b is an inverse of a.*

The inverse of an element a is also often denoted by a^{-1}. If additive notation is of your taste, we also may write it as $-a$. Now, we'll prove some rich properties of inverses.

Proposition 1.2.0.2 (Inverses are Unique)**.** *Suppose an associative law of composition on S, denoted $\cdot$, has an identity e. Let $a \in S$. If there exists $a_L^{-1}, a_R^{-1} \in S$ such that these are inverses of a, namely, $a_L{-}1 \cdot a = e$ and $a \cdot a_R{-}1 = e$, then $a_L^{-1} = a_R^{-1}$.*

Proof. Since a_L^{-1} and a_R^{-1} are inverses of a it follows that

$$a_L^{-1} = a_L^{-1} \cdot e = a_L^{-1} \cdot (a \cdot a_R^{-1}) = (a_L^{-1} \cdot a) \cdot a_R^{-1} = e \cdot a_R^{-1} = a_R^{-1}$$

□

Proposition 1.2.0.3 (Composition of Inverses)**.** *Suppose an associative law of composition on S, denoted as $\cdot$, has an identity e. If $a, b \in S$ both have inverses a^{-1}, b^{-1}, then the inverse of the composition is reversed, namely $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.*

Proof. We could prove this directly by showing that the element $b^{-1} \cdot a^{-1}$ together with $a \cdot b$ retrieve the identity e. However, for didactic purposes, we'll find it as if we didn't know it was the case. Therefore, if $a \cdot b$ has an inverse:

$$(a \cdot b) \cdot (a \cdot b)^{-1} = e$$

By the associtivity of the binary operation and associativity over multiple elements, we can carry out the following manipulations.

$$a^{-1} \cdot (a \cdot b) \cdot (a \cdot b)^{-1} = a^{-1} \cdot e$$

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

Performing this once more by multiplying b^{-1} on the left, we get the desired result

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

□

This last proposition is quite important. Matrix multiplication as a law of composition on n by n matrices does indeed follow this rule, for example. The proof relied on performing something that up to today you may be already well familiar with, cancellation. But such things that we perceive as obvious or 'mastered' are often the culprits which hide the scientific and mathematical advancement. Many instances of physical theories such as newtonian mechanics have arouse on revolutions by rethinking the very foundations of what we understand and took for granted. Furthermore, it is worthy to mention that if an element has either a 'left' or 'right' inverse, that does not necessarily mean that such an element is invertible. In fact, there are matrices that upon multiplication in either side retrieve an identity matrix in one but not in the other.

Proposition 1.2.0.4 (The Cancellation Law)**.** *Suppose $\cdot$ is an associative law of composition on a set S. Suppose there is an identity e and that all elements have an inverse. Let $a, b, c \in S$. If $a \cdot b = a \cdot c$ or if $b \cdot a = c \cdot a$, then $b = c$. If $a \cdot b = a$ or if $b \cdot a = a$, then $b = e$.*

Proof. Since all elements have an inverse, we could claim that such inverse for a is a^{-1}. Then, the multiple scenarios can be shown by using this fact:

Case 1	Case 2	Case 3	Case 4
$a \cdot b = a \cdot c$	$b \cdot a = c \cdot a$	$a \cdot b = a$	$b \cdot a = a$
$a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c$	$b \cdot a \cdot a^{-1} = c \cdot a \cdot a^{-1}$	$a^{-1} \cdot a \cdot b = a^{-1} \cdot a$	$b \cdot a \cdot a^{-1} = a \cdot a^{-1}$
$b = c$	$b = c$	$b = e$	$b = e$

Demonstrating all cases as stated. □

This cancellation law, be careful with it. You can't do $0 \cdot x = x \implies 0 = 1$ because the number zero has no well defined inverse under number multiplication as law of composition. That was in fact one of the common birthplace of 'paradoxes' in mathematics as these topics are often taken uncautiously. To conclude this section and begin making use of this built-up formality, more widely used notation will come handy. Power notation may be used for an associative law of composition $\cdot$ on a set S which has inverses and an identity. Let $a \in S$ be one of those invertible elements.

Examples: let $n, r, s \in \mathbb{N}$

$$\underbrace{a \cdot \ldots \cdot a}_{n \text{ times}} = a^n, \quad a^0 = e$$

$$\underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{n \text{ times}} = (a^{-1})^n = a^{-n}$$

$$\underbrace{(a \cdot \ldots \cdot a)}_{r \text{ times}} \cdot \underbrace{(a \cdot \ldots \cdot a)}_{k \text{ times}} = a^r \cdot a^k = a^{r+k}$$

for additive notation, a^n becomes na (1.2)

Next, we embark on presenting the main topic of this part, groups.

1.3 Groups and Subgroups

Historically, mathematicians found certain 'things' and noticed that they had the following peculiar characteristics and called them groups. Today, we define such characteristics first and then define groups to be those things which possess these characteristics.

Definition 1.3.0.1 (Group)**.** *A group $(G, *)$ is a set G together with a law of composition $*$ with the following properties.*

i. The law of composition $*$ is associative.

$$(a * (b * c) = (a * b) * c) \, (\forall a, b, c \in G)$$

ii. There exists an identity element $e \in G$.

$$(\exists e \in G)(\forall a \in G)(a * e = e * a = a)$$

iii. Every element $a \in G$ has an inverse.

$$(\forall a \in G)(\exists a^{-1} \in G)(a * a^{-1} = a^{-1} * a = e)$$

Therefore, to show that something is a group, we just have to show that it follows the 3 criteria. As a matter of fact, an implicit criteria to check is if the law of composition is indeed a law of composition.

Definition 1.3.0.2 (Abelian Groups)**.** *An abelian group is a group with a commutative law of composition.*

All groups have associative laws of composition per the definition of group. Not all groups are abelian, however. For example, a group of invertible matrices with matrix multiplication as binary operation is not abelian since matrix multiplication is not generally commutative.

Examples: Some Abelian Groups

- $\mathbb{Z}^+$ is the additive group of integers $(\mathbb{Z}, +)$ with addition as binary operation.
- $\mathbb{R}^+$ is the additive group of real numbers $(\mathbb{R}, +)$ with addition as binary operation.
- $\mathbb{R}^\times$ is the multiplicative group of real numbers $(\mathbb{R}/\{0\}, \times)$ with multiplication as binary operation. Notice that we had to remove 0 from the set of real numbers because it has no inverse under multiplication and it can never yield the identity.
- $\mathbb{C}^+, \mathbb{C}^\times$ the respective analogs on the complex plane. $(\mathbb{C}, +), (\mathbb{C}/\{0\}, \times)$ respectively.

Definition 1.3.0.3 (The General and Special Linear Groups)**.** *The general linear group is the group of invertible $n \times n$ matrices with matrix multiplication as law of composition. While the special linear group is the elements of the general linear group whose determinant equals 1 along with matrix multiplication as law of composition.*

$$GL_n(A) := \{M \in A^{n\times n} : \det(M) \neq 0\}, \quad SL_n(A) := \{M \in A^{n\times n} : \det(M) = 1\} \tag{1.3}$$

Where A could be $\mathbb{R}$ or $\mathbb{C}$ or whatever field denoting what the entries of the matrices in the group are.

The last definition shows something interesting. Sometimes, there are groups embedded whithin groups. This motivates the idea of a subgroup.

Definition 1.3.0.4 (Subgroup)**.** *A subset H of the set G of a group is a subgroup $(H, *)$ inheriting the law of composition $*$ of the group $(G, *)$ if it has the following properties.*

i. Closure: If $a, b \in H$, then $a * b \in H$

$$(a \in H \wedge b \in H) \Longrightarrow (a * b \in H)$$

ii. Identity: The identity $e \in G$ is also contained in H.

$$(e \in G) \Longrightarrow (e \in H)$$

iii. Inverses: Every element $a \in H$ has an inverse.

$$(\forall a \in H)(\exists a^{-1} \in H)(a * a^{-1} = a^{-1} * a = e)$$

Notice we had to make no mention of associativity as the group from which the subgroup emerged already induces the law of composition on the subgroup. Along with GL_n which has important subgroups, there is another group which carries important subgroups in it. Let M be the set of maps from a set T to itself. A map $f : T \to T$ has an inverse function if and only if it is bijective (injective and surjective.) In which case, we call f a permutation of T. The set of permutations of T forms a groups with function composition as associative binary operation.

The group of permutations of the indices $\{1, 2, \ldots, n\}$ is called the symmetric group, and is denoted by $S_n := \{f : \{1, \ldots, n\} \to \{1, \ldots, n\} |\ f \text{ is invertible}\}$.

A noticeable distinction is that groups have different sizes. The size of a group depends on the number of elements that the set has, the cardinality.

Definition 1.3.0.5 (Order of a Group)**.** *The order of a group G, denoted $|G|$, is the number of elements that G has. In other words, the cardinality of the set G.*

If the order of a group is infinite, like $\mathbb{R}^\times$ or $GL_n(\mathbb{C})$, we say the group is infinite. If it is finite, like S_n since there are $n!$ possible permutations, we say the group is finite.

Example: The Smallest Non-Abelian Group
The symmetric group of 3 indices $S_3 := \{f : \{1,2,3\} \to \{1,2,3\} | \ f \text{ is invertible}\}$ which has order $|S_3| = 3! = 3 \cdot 2 \cdot 1 = 6$ is the smallest group that is not commutative. To describe the elements of this groups, we can employ cycle notation. In this way, the element of S_3 that maps 1 to 2 and then maps 2 to 3 and then maps 3 back to 1 is greatly summarized as $(1\,2\,3)$. The composition of two elements, for example, $(1\,3)(2)$ which maps 1 to 3, 3 back to 1, and 2 to itself and $(1\,2\,3)$ as explained before is:

$$(1\,3)(2) \circ (1\,2\,3) = (1\,2)(3)$$

Because 1 maps to 2, and then 2 maps to itself. Now we check 2 maps to 3 and then 3 maps to 1. This concludes a full cycle $(1\,2)$. Finally, 3 maps to 1 and 1 maps to 3, such that 3 goes to itself. Now, as an exercise, try to determine what the composition $(1)(3\,2) \circ (1\,2)(3)$ yields. The composition you got should be (1 3 2). As a final reminder of how much **mathematicians like to shorten things**, if an element is sent to itself, we often not write it in disjoint cycle notation. Such that $(1)(3\,2)$ for example, is written as $(3\,2)$ for simplicity.

Something that you will want to do only for small groups is to use a multiplication table as the following:

$\circ$	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(13)	(23)
(13)	(13)	(123)	(1)	(132)	(23)	(12)
(23)	(23)	(132)	(123)	(1)	(12)	(13)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

Table 1.1: Cayley table of S_3

By selecting a permutation at the top margin and then choosing a permutation at the left margin, you can perform the composition by looking at the element which is in the same row and column as the former. **For example**, take the permutation $(1\,3\,2)$ on the top margin and then compose it with $(1\,3)$ by going down through the selected top column until coinciding with the selected left margin. You'll see, as before, that the composition yields again $(1\,2)$.

Two interesting subgroups of $\mathbb{C}^\times$ are $S_1 := \{z \in \mathbb{C} : |z| = 1\}$ the unit circle of the complex plane and also $\mu_n := \{z \in \mathbb{C} : z^n = 1\}$ the n roots of unity. $\mu_n \subseteq S_1 \subseteq \mathbb{C}^\times$

This finalizes the introductory discussion of groups and subgroups.

Chapter 2

Homomorphisms and Isomorphisms

2.1 Homomorphisms

In a nusthell, a homomorphism is a way to compare two groups for structural similarities.

Definition 2.1.0.1 (Homomorphism)**.** *A homomorphism is a function ϕ acting on two groups $(G, *)$ and $(S, \circ)$ such that for any elements $g_1, g_2 \in G$ we have:*

$$\phi : G \to S, \quad \phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2)$$

Written multiplicatively, we can write the homomorphism as $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$. The left-hand-side of the equation says to use the law of composition $*$ of $(G, *)$ and the right-hand-side of the equation says to use the other law of composition $\circ$ of the other group $(S, \circ)$. A homomorphism serves as a mapping compatible with the laws of composition of the groups, allowing to relate these two groups.

Examples: Some Homomorphisms

- The logarithm function $\log : \mathbb{R}_{>0} \to \mathbb{R}, \quad \log(x \cdot y) = \log(x) + \log(y)$
- The determinant function $\det : GL_n(\mathbb{R}) \to \mathbb{R}, \quad \det(AB) = \det(A)\det(B)$
- The modulus function $|\ | : \mathbb{C}^\times \to \mathbb{R}^\times, \quad |z \cdot w| = |z| \cdot |w|$

Proposition 2.1.0.1. *Let $\phi : G \to S$ be a group homomorphism. Then:*

i. Multiple Elements: $(a_1, \cdots, a_k \in G) \implies (\phi(a_1 \cdots a_k) = \phi(a_1) \cdots \phi(a_k))$

ii. Image of the Identity: $\phi(e_G) = e_S$

iii. Image of Inverses: $(\forall g \in G)(\phi(g^-1) = \phi(g)^{-1})$

Proof. For (i) we necessitate induction. Let the base case be that for two arbitrary $x, y \in G$, then $\phi(xy) = \phi(x)\phi(y)$. Then, by Corollary 1.1.0.3, we can find the image of $g_1, g_2, \ldots, g_k$ as:

$$\phi(g_1 g_2 \cdots g_{k-1} g_k) = \phi(g_1 g_2 \cdots g_{k-1})\phi(g_k)$$

So that we repeat this process until getting to

$$\phi(g_1 g_2 \cdots g_{k-1} g_k) = \phi(g_1) \cdots \phi(g_k)$$

Next, we show (ii) directly since $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$. Therefore, $e_S = \phi(e_G)$ by multipliying both sides by the inverse of $\phi(e_G)$. Finally, we can see (iii) arise directly from (ii) since $e_S = \phi(e_G) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$ which means that $\phi(x)^{-1} = \phi(x^{-1})$. □

For example, by using (iii) on the determinant homomorphism, we readily encounter that for some matrix $A \in GL_n\mathbb{R}$, the determinant of its inverse is

$$\det(A^{-1}) = \det(A)^{-1} = \frac{1}{\det(A)}$$

Another readily noticeable fact is that since 1 is the identity of $(\mathbb{R}_{>0}, \times)$ and 0 the identity of $(\mathbb{R}, +)$, property (ii) yields

$$\log(1) = 0$$

The trivial homomorphism $\phi : G \to S$ maps everything to the identity $e_s \in S$. This notion leads to the definition of the kernel.

Appendices

Appendix A

Homework Problems

A.1 Mathematics 100A Problems

A.1.1 Assignment Due January 8th, 2025

Problem 1:

Consider the law of composition $*$ on the set $\{\☺, \times, \square\}$ where $x * x = x$ but, if $x \neq y$, then $x * y$ is the other element.

a) Compute $(\☺ * \times) * \square$.

Since $x * y$ equals the other element (provided that $x \neq y$), and since $x * x = x$, then:

$$(\☺ * \times) * \square = (\square) * \square = \square$$

b) Compute $\☺ * (\times * \square)$.

Emphasis in the parentheses, because this law of composition (or binary operation) might not be associative:

$$\☺ * (\times * \square) = \☺ * (\☺) = \☺$$

c) A law of composition $\circ$ on a set S is *associative* if $(x \circ y) \circ z = x \circ (y \circ z)$ for all $x, y, z \in S$. Is $*$ associative?

Per the previous results, * is not associative because $(\☺ * \times) * \square \neq \☺ * (\times * \square)$.

d) A law of composition $\circ$ on a set S is *commutative* if $x \circ y = y \circ x$ for all $x, y \in S$. Is $*$ commutative?

Let $x, y \in \{\☺, \times, \square\}$. First, consider the case that $x = y$, then:

$$x * y = x * x = x = y = y * y = y * x$$

In such case, $x * y = y * x$.
Now, let's consider $x \neq y$.

$$\begin{aligned} x * y &= z_1, \quad z_1 \in \{\☺, \times, \square\} \setminus \{x, y\} \\ y * x &= z_2, \quad z_2 \in \{\☺, \times, \square\} \setminus \{x, y\} \end{aligned}$$

In that case, upon the availability of only one left element in $\{\☺, \times, \square\} \setminus \{x, y\}$, we have that $z_1 = z_2$. Thereby, * is commutative.

Problem 2:

Let $n \geq 2$, and consider the subsets $P = \{M \in M_n(\mathbb{R}) \mid \det M > 0\}$, $N = \{M \in M_n(\mathbb{R}) \mid \det M < 0\}$, and $Z = \{M \in M_n(\mathbb{R}) \mid \det M = 0\}$.

a) Does matrix multiplication give a law of composition on P? Why or why not?

Yes, because the binary operation retrieves a member of P. Suppose $A, B \in P$.

$$(\det(A) > 0 \wedge \det(B) > 0) \Longrightarrow (\det(A \cdot B) = \det(A) \cdot \det(B) > 0)$$

b) Does matrix multiplication give a law of composition on N? Why or why not?

No, because the binary operation retrieves an object not in N. Similarly as before, suppose $A, B \in N$.

$$(\det(A) < 0 \wedge \det(B) < 0) \Longrightarrow (\det(A \cdot B) = \det(A) \cdot \det(B) > 0)$$

c) Does matrix multiplication give a law of composition on Z? Why or why not?

Yes, suppose $A, B \in N$.

$$(\det(A) = 0 \wedge \det(B) = 0) \Longrightarrow (\det(A \cdot B) = \det(A) \cdot \det(B) = 0)$$

d) Give another subset of $M_n(\mathbb{R})$ on which matrix multiplication gives a law of composition.

The subset $R \subseteq M_n(\mathbb{R})$ defined as:

$$R := \{M \in M_n(\mathbb{R}) : \det(M) = 1\}$$

is a subset in which matrix multiplication gives a law of composition. Suppose $A, B \in R$, then:

$$\det(A \cdot B) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1$$

A.1.2 Assignment Due January 10th, 2025

Problem 1:

Let $*$ be a binary operation on a set S. Let $L \in S$ be a *left unit*, so that $L * x = x$ for all $x \in S$, and let $R \in S$ be a *right unit*, so that $x * R = x$ for all $x \in S$. Show that $L = R$, and conclude that $*$ is unital.

Proof. Let $*$ be a law of composition on S. Suppose that $L \in S$ is a left unit and $R \in S$ is a right unit. Therefore:

$$L * (x) = x = (x) * R, \quad \forall x \in S$$

Since $L, R \in S$, we have that:

$$L = (L) * R = L * (R) = R$$

Because the left and right units are equal, there is a unique unit. Thereby, $*$ is unital. □

Problem 2:

Let $*$ be an associative, unital binary operation on a set S. Let $x, y \in S$ both be invertible. Show that $x * y$ is also invertible.[Hint: Find its inverse. Be careful, since $*$ might not be commutative! If you are comfortable with matrices, see if you can remember how to find the inverse of a product of matrices.]

Suppose $x, y \in S$ are invertible and $e \in S$ is the unit. Since $*$ is associative, we have:

$$(x * y) * (x * y)^{-1} = e \Rightarrow (y^{-1} * x^{-1}) * (x * y) * (x * y)^{-1} = (y^{-1} * x^{-1}) * e$$

$$(x * y)^{-1} = y^{-1} * x^{-1}$$

Thereby, $x * y$ is invertible (with its inverse shown above).

A.1.3 Assignment Due January 13th, 2025

Problem 1

Let $*$ be an associative, unital binary operation on a set X. Let $G \subseteq X$ be the set of invertible elements in X. Prove that G is a group with the operation $*$. [Hint: What do you need to check? A previous homework problem should help with one of them.]

To prove that G with operation $*$ is a group, we have to prove that $(G, *)$ satisfies the following criteria:

i. The law of composition is associative.

ii. There is a unique identity e.

iii. Every element in the group has an inverse.

Proof. Let $G := \{g \in X : (\exists g^{-1} \in X)(g * g^{-1} = e = g^{-1} * g)\}$ be the set of invertible elements in X. The law of composition $*$ is associative for every element in X, therefore it also is on G, a subset of X. The unit $e \in X$ is also a unit on G as $e * x = e * x = e$ $\forall x \in G \subseteq X$. Notice e is an inverse to itself. Finally, every $g \in G$ has an inverse by the definition of G:

$$g_1 * g_2 \in G$$

$$(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}, \quad \text{where } g_1^{-1}, g_2^{-1} \in G$$

□

Problem 2

Let G be a group, and let Z be the set of elements that commute with every element of G. Specifically,

$$Z = \{z \in G \mid z * x = x * z \text{ for every } x \in G\}.$$

Verify that Z is a group with the binary operation $*$. This is called the *center* of G. [Hint: What do you need to check?]

Demonstrate the same criteria as in (A.1.3):

Proof. By the law of composition on the *group* $(G, *)$, $*$ is associative on $Z \subseteq G$. Furthermore, the identity e is still an identity for $(Z, *)$ because $e * x = e * x = x$ respects the commutativity property of $(Z, *)$. Notice e is an inverse to itself. Finally, inverses respect the commutative property:

$$z * x = x * z, \quad \forall x, z \in Z$$

$$(z * x)^{-1} = (x * z)^{-1}$$

$$x^{-1} * z^{-1} = z^{-1} * x^{-1}$$

Showing that commutativity holds for arbitrary $x, z \in Z$ □

A.1.4 Assignment Due January 15th, 2025

Problem 1

Let f, g, and h be as in the following table. Find each of the following compositions: $f \circ h$, $h \circ f$, $f \circ g \circ f$, $h \circ g \circ h$

m	1	2	3	4
$f(m)$	2	1	4	3
$g(m)$	2	4	3	1
$h(m)$	1	4	3	2

The compositions are shown in a similar table.

m	1	2	3	4
$(f \circ h)(m)$	2	3	4	1
$(h \circ f)(m)$	4	1	2	3
$(f \circ g \circ f)(m)$	3	1	2	4
$(h \circ g \circ h)(m)$	4	1	3	2

Problem 2

Prove that the set of nonzero integers with multiplication is cancellative. [Hint: Show that, if $ab = ac$, then either $a = 0$ or $b - c = 0$. You may use the fact that, if $xy = 0$, then either $x = 0$ or $y = 0$.]

Proof. We prove this by cases by using the fact that $xy = 0 \implies x = 0 \vee y = 0$. Since $a, b, c \in \mathbb{Z} \setminus \{0\}$, every following case makes the assumption that one of a, b, c has a multiplicative inverse.

Case 1: Using a^{-1}. Then:

$$ab = ac \Rightarrow a^{-1}ab = a^{-1}ac \Rightarrow b = c$$

Namely, $b - c = 0$.

Case 2: Using b^{-1}. Then:

$$ab = ac \Rightarrow abb^{-1} = acb^{-1} \Rightarrow a = a(cb^{-1}) \Rightarrow e = cb^{-1}$$

Namely, $c^{-1} = b^{-1}$ such that $cc^{-1} = e$. So $c = b$ by uniqueness of inverses.

Case 3: Using c^{-1}. Then:

$$ab = ac \Rightarrow abc^{-1} = acc^{-1} \Rightarrow a(bc^{-1}) = a(e) \Rightarrow bc^{-1} = e$$

Similarly to case 2, by uniqueness of inverses, $b = c$

Since in all cases cancellation holds, $(\mathbb{Z}, \cdot)$ is cancellative. □

A.1.5 Assignment Due January 17th, 2025

Problem 1

Let f, g, and h be as in the following table. Write each of the following in disjoint cycle notation. $f, \quad g, \quad ,h, \quad fh, \quad hf, \quad fgf, \quad hgh.$

m	1	2	3	4
$f(m)$	2	1	4	3
$g(m)$	2	4	3	1
$h(m)$	1	4	3	2

- $f = (1 \quad 2)(3 \quad 4)$
- $g = (1 \quad 2 \quad 4)(3)$
- $h = (1)(2 \quad 4)(3)$
- $f \circ h = (1 \quad 4 \quad 3 \quad 2)$
- $h \circ f = (1 \quad 2 \quad 3 \quad 4)$
- $f \circ g \circ f = (1 \quad 3 \quad 2)(4)$
- $h \circ g \circ h = (1 \quad 4 \quad 1)(3)$

Problem 2

Let $H \subseteq S_n$ be the set $H = \{f \in S_n \mid f(n) = n\}$ Verify that H is a subgroup of S_n.

Proof. To verify, confirm subgroup criteria:

i. Closure: $f, g \in H \Rightarrow f \circ g \in H$

ii. Identity: $\exists e \in H \forall f \in H : e \circ f = f \circ e$

iii. Inverses: $f \in H \Rightarrow f^{-1} \in H$

Closure:
Let $f, g \in H$. Thereby, $f(n) = n$ and $g(n) = n$. Notice that

$$(f \circ g)(n) = f(g(n)) = f(n) = n$$

which implies that $f \circ g \in H$.
Identity:
The identity $e \in S_n$ maps every element to itself. $e(n) = n$. Thus, $e \in H$.
Inverses:
Let $f^{-1} \in H$. Thereby, $f(n) = n$. The inverse f^{-1} should map images to their preimage. These happen to remain unaltered; therefore, $f^{-1}(n) = n \Rightarrow f^{-1} \in H$
All criteria has been met. Thus, this is a subgroup. □

A.1.6 Assignment Due January 22nd, 2025

Problem 1

In which of the following cases is H a subgroup of G? Briefly explain you answers.

a) $G = GL_n(\mathbb{C})$ and $H = GL_n(\mathbb{R})$.

b) $G = \mathbb{R}^\times$ and $H = \{1, -1\}$.

c) $G = \mathbb{Z}$ and H is the set of positive integers.

d) $G = \mathbb{R}^\times$ and H is the set of positive real numbers.

e) $G = GL_2(\mathbb{R})$ and H is the following set of matrices:

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R},\, a \neq 0 \right\}.$$

a) H is a subgroup of G with matrix multiplication as binary operation because they are both closed under matrix multiplication, they share the same identity I_n, matrix multiplication is associative in both cases, and both are closed under inverses (by the definition of General Linear Group)

b) Recall $(\mathbb{R}^\times, \times) = (\mathbb{R}\backslash\{0\}, \times)$. Notice the unit 1 is still in H and notice that H is closed. Finally, notice it is closed under inverses because for any element in H, said element is its own inverse. Thus, a subgroup (since multiplication is associative).

c) H is not a subgroup as it is not closed under inverses. (e.g. $5 + (-5) = 0$ yet $-5 \notin H$).

d) H is a group because it has identity 1, closed under positive real number multiplication, associative (even commutative), and closed under inverses as every positive real number has a positive real reciprocal.

e) Not a subgroup, the elements in H are not invertible.

Problem 2

Let $(G, *)$ be a group. Define a new group G°, where the set is the same as G, but the group law $\circ$ is defined by the formula $a \circ b = b * a$. Prove that G° is a group. [What do you need to check?]

To prove that G° is a group, we need to show closure, associativity, identities, and inverses.

Proof. Let $a, b, c \in G^\circ$. Firstly, notice the closure of G° by the fact that it has the same elements as G, so $a \circ b = b * a \in G \Rightarrow a \circ b \in G^\circ$. Also, notice that

$$(a \circ b) \circ c = (b * a) \circ c = c * b * a = a \circ (c * b) = a \circ (b \circ c)$$

showing $(G^\circ, \circ)$ is associative. Moreover, G° is also closed under inverses since G is a group, $a \circ a^{-1} = a^{-1} * a = e = a * a^{-1} = a^{-1} \circ a$. Finally, the identity $e \in G$ is also an identity of G° because $a \circ e = e * a = a = a * e = e \circ a$. Thus, all criteria met, G° is a group with law of composition $\circ$. □

Problem 3

Prove that, if a and b are positive integers whose sum is a prime p, then their greatest common divisor is 1.

Proof. Let $a, b \in \mathbb{N} \setminus \{0\}$ such that $a+b = p$ where p is a prime number. For a contradiction, assume that $\gcd(a, b) > d$ such that $d > 1$. Since d is a common divisor, there exist positive integers c_1, c_2 such that $a = c_1 d$ and $b = c_2 d$. Therefore:

$$a + b = c_1 d + c_2 d = d(c_1 + c_2) = p$$

Yet p was defined to be a prime number, for which writing it as a product of two integers is a contradiction. Therefore, if $a, b \in \mathbb{N} \setminus \{0\} : a+b = p$ such that p is prime, then their greatest common divisor is 1. □

A.1.7 Assignment Due January 24th, 2025

Problem 1

Show that $w : \mathbb{R} \to \mathbb{C}^\times$, $w(t) = e^{it}$ is a homomorphism. What is $\ker w$? what is the $\operatorname{im} w$?

Proof. Let $a, b \in \mathbb{R}$. Then:

$$w(ab) = e^{i(a+b)} = e^{ia}e^{ib} = w(a)w(b)$$

Thus, w is a homomorphism. □

Now, the kernel and the image of w are the following sets, by definition:

$$\ker w := \{x \in \mathbb{R} : w(x) = e_{\mathbb{C}^\times}\}$$
$$\operatorname{im} w := \{z \in \mathbb{C}^\times : (\exists x \in \mathbb{R})(w(x) = z)\}$$

Thereby, a more specific expression for these is:

$$\ker w = \{2\pi k \in \mathbb{R} : k \in \mathbb{Z}\}$$
$$\operatorname{im} w = S_1$$

That is because $e^{i2\pi k} = 1$ (the identity $e_{\mathbb{C}^\times}$ of $\mathbb{C}^\times$) for any integer k and S_1 is the unit circle as e^{it} is bound to be trapped in the unit circle of the complex plane for all $t \in \mathbb{R}$.

Problem 2

Let G and H be isomorphic groups.

a) Show that G and H have the same order.

b) Show that, if G is abelian, then H is abelian. [Recall: a group is *abelian* if the binary operation is commutative.]

c) Show that μ_6 and S_3 are not isomorphic.

a) Let G, H be isomorphic groups. Then G and H have the same order.

Proof. Since G and H are isomorphic, there is a bijective homomorphism $\Phi : G \to H$. Since Φ is bijective, it is both injective and surjective, which implies that G and H have the same cardinality, ergo, the same order. □

b) Let G, H be isomorphic. If G is abelian, then H is abelian.

Proof. Let $\circ$ and $*$ be the laws of composition of G and H, respectively. Since G and H are isomorphic, there is some bijective homomorphism $\Phi : G \to H$. Therefore, for $g_1, g_2 \in G$, and $h_1, h_2 \in H$ such that $h_1 = \Phi(g_1), \quad h_2 = \Phi(g_2)$ and since G is abelian:

$$\Phi(g_1 \circ g_2) = \Phi(g_2 \circ g_1) \implies \Phi(g_1) * \Phi(g_2) = \Phi(g_2) * \Phi(g_1)$$
$$\therefore h_1 * h_2 = h_2 * h_1$$

Thus, if G and H are isomorphic and G is abelian, then H is abelian too. □

c) Let $\mu_6 = \{z \in \mathbb{C} : z^6 = 1\}$ and $S_3 = \{f : \{1, 2, 3\} \to \{1, 2, 3\} \mid \text{f is bijective}\}$. Prove that μ_6 and S_3 are not isomorphic.

Proof. For the sake of a contradiction, suppose that μ_6 and S_3 are isomorphic. Then, there exists a bijective homomorphism $\Phi : \mu_6 \to S_3$. Since μ_6 is commutative (because complex number multiplication is commutative), we have that S_3 should be commutative too (by HW7, problem 2, part b). Anyhow, that conclusion is a contradiction because function composition (the binary operation of the symmetric group) is not commutative. Therefore, μ_6 and S_3 are not isomorphic. □

A.1.8 Assignment Due January 27th, 2025

Problem 1

Let $(G, *)$ be a group, and recall the group G° from Homework 6, Problem 2 (Problem A.1.6): its underlying set is the same set G, but $a \circ b = b * a$. We already showed that this is a group; now, show that it is isomorphic to G. [In order to prove that G and G° are isomorphic, you should build an isomorphism $G \to G^\circ$ or $G^\circ \to G$.]

Proof. Let $(G, *)$ and $(G^\circ, \circ)$ be groups such that $a \circ b = b * a$. Then, let $\Phi : G^\circ \to G$ be a group homomorphism such that $\Phi(x) = x^{-1}$. Notice that

$$\Phi(x \circ y) = (x \circ y)^{-1} = y^{-1} \circ x^{-1} = x^{-1} * y^{-1}$$

whereas

$$\Phi(x) * \Phi(y) = x^{-1} * y^{-1}$$

Thus, Φ is indeed a group homomorphism because $\Phi(x \circ y) = \Phi(x) * \Phi(y)$. Let's show that this group homomorphism is bijective, thus showing that there is a group isomorphism between these two groups. Let $g \in G^\circ$:

$$(\Phi(g))^{-1} = (g^{-1})^{-1} = g$$

Recall $g \in G$ because $G = G^\circ \Rightarrow G \subseteq G^\circ \wedge G \supseteq G^\circ$. Thus, Φ is invertible and a fuction is invertible if and only if it is surjective and injective (in short, bijective). As Φ is a bijective group homomorphism, it is an isomorphism and the groups G, G° are isomorphic. □

Problem 2

Fix $n \geq 1$. Show that every coset $a + n\mathbb{Z}$ contains a unique element $r \in \{0, 1, \ldots, n-1\}$. Use this to show that there are n cosets of $n\mathbb{Z}$ in $\mathbb{Z}$.

Proof. Let $a + n\mathbb{Z} := \{a + nz \in \mathbb{Z} : z \in \mathbb{Z}\}$ be a coset. Given any $a \in \mathbb{Z}$. By the division theorem, $a = nq + r$ for some quotient $q \in \mathbb{Z}$, and remainder $r \in \{0, 1, \ldots, n-1\}$. Suppose that $r_1, r_2 \in \{0, 1, \ldots, n-1\}$ such that both belong to the coset $a + n\mathbb{Z}$. Then:

$$(a \equiv r_1 \mod n) \wedge (a \equiv r_2 \mod n) \Longrightarrow r_1 \equiv r_2 \mod n$$

Therefore, $r_1 \equiv r_2 \mod n \Leftrightarrow n \mid (r_1 - r_2) \Leftrightarrow \exists k \in \mathbb{Z} : kn = r_1 - r_2$. Nonetheless, notice that since $r_1, r_2 \in \{0, 1, \ldots, n-1\}$, they necessarily have to be equal to each other such that $r_1 - r_2 = 0$. Thus, the element r is unique. Therefore, since every integer a can be uniquely represented with some *unique* remainder $r \in \{0, 1, \ldots, n-1\}$, there are $|\{0, 1, \ldots, n-1\}| = n$ cosets of $n\mathbb{Z} \in \mathbb{Z}$. □

A.1.9 Assignment Due January 29th, 2025

Problem 1

For each of the following, find a representative r of the coset with $0 \leq r < 12$

a) $143 + 12\mathbb{Z}$.

b) $-7 + 12\mathbb{Z}$.

c) $(143 + 12\mathbb{Z}) + (-7 + 12\mathbb{Z})$. Once you've found the representative, tell me which coset $(143 + 12\mathbb{Z}) + (-7 + 12\mathbb{Z})$ is.

d) $9 + 12\mathbb{Z}$.

e) $(143 + 12\mathbb{Z}) + (9 + 12\mathbb{Z})$. Once you've found the representative, tell me which coset $(143 + 12\mathbb{Z}) + (9 + 12\mathbb{Z})$ is.

f) $(-7 + 12\mathbb{Z}) + (9 + 12\mathbb{Z})$. Once you've found the representative, tell me which coset $(-7 + 12\mathbb{Z}) + (9 + 12\mathbb{Z})$ is.

a) 11 is a representative.

b) 5 is a representative.

c) 4 is a representative. Whereas $(143 + 12\mathbb{Z}) + (-7 + 12\mathbb{Z}) = 136 + 12\mathbb{Z} = 4 + 12\mathbb{Z}$.

d) 9 is a representative.

e) 8 is a representative. Whereas $(143 + 12\mathbb{Z}) + (9 + 12\mathbb{Z}) = 152 + 12\mathbb{Z} = 8 + 12\mathbb{Z}$.

f) 2 is a representative. Whereas $(-7 + 12\mathbb{Z}) + (9 + 12\mathbb{Z}) = 2 + 12\mathbb{Z}$.

Problem 2

Show that $\mathbb{Z}/n\mathbb{Z}$ is a group. [Hint: what do you have to show? For each property, you are going to need to use the fact that $\mathbb{Z}$ has that property in order to show that $\mathbb{Z}/n\mathbb{Z}$ has that property.]

Proof. I shall begin by demonstrating **closure**. For any two elements of $\mathbb{Z}/n\mathbb{Z}$, say $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$, since $a + b \in \mathbb{Z}$, it follows that $(a + b) + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$. **Associativity** is as well inherited from integer addition, thus, $\forall a, b, c \in \mathbb{Z}, \quad (a + b) + c = a + (b + c) \Rightarrow \cdots$

$$
\begin{aligned}
&(a + n\mathbb{Z} + b + n\mathbb{Z}) + c + n\mathbb{Z} \\
&\qquad\qquad (a + b) + n\mathbb{Z} + c + n\mathbb{Z} \\
&\qquad\qquad\quad (a + b + c) + n\mathbb{Z} \\
&\qquad\quad a + n\mathbb{Z} + ((b + c) + n\mathbb{Z}) \\
&\qquad\qquad\qquad\qquad a + n\mathbb{Z} + (b + n\mathbb{Z} + c + n\mathbb{Z})
\end{aligned}
$$

Furthermore, $\mathbb{Z}/n\mathbb{Z}$ is **identital** as it contains an identity element, namely, $0 + n\mathbb{Z}$. That is so because for any given $a \in \mathbb{Z}$:

$$a + n\mathbb{Z} + 0 + n\mathbb{Z} = 0 + n\mathbb{Z} + a + n\mathbb{Z} = a + n\mathbb{Z}$$

Finally, $\mathbb{Z}/n\mathbb{Z}$ is **closed under inverses** because for any element in it, say $a + n\mathbb{Z}$, there exists an inverse $-a + n\mathbb{Z}$ such that:

$$a + n\mathbb{Z} + (a + n\mathbb{Z})^{-1} = 0 + n\mathbb{Z} = (a + n\mathbb{Z})^{-1}a + n\mathbb{Z}$$
$$a + n\mathbb{Z} - a + n\mathbb{Z} = 0 + n\mathbb{Z} = -a + n\mathbb{Z} + a + n\mathbb{Z}$$

Since all of the criteria is met, $\mathbb{Z}/n\mathbb{Z}$ is indeed a group. □

A.1.10 Assignment Due February 3rd, 2025

Problem 1

Show that the function $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad \pi(a) = a + n\mathbb{Z}$ is a homomorphism.

Proof. Let $a, b \in \mathbb{Z}$. The law of composition of the group $(\mathbb{Z}, +)$ says that $a+b \in \mathbb{Z}$. The law of composition of the group $(\mathbb{Z}/n\mathbb{Z}, +)$ says that $(a+n\mathbb{Z})+(b+\mathbb{Z}) = (a+b)+n\mathbb{Z}$ which is an element of $\mathbb{Z}/n\mathbb{Z}$. To verify the homomorphism, let's ensure that $\pi(a+b) = \pi(a)+\pi(b)$:

$$\pi(a+b) = (a+b) + n\mathbb{Z}$$
$$\pi(a) + \pi(b) = (a + n\mathbb{Z}) + (b + n\mathbb{Z})$$
$$(a + n\mathbb{Z}) + (b + \mathbb{Z}) = (a + b) + n\mathbb{Z}$$

Therefore, $\pi(a+b) = \pi(a)+\pi(b)$, and the function π is indeed a group homomorphism. □

Problem 2

Let G be a cyclic group, and $\Phi : G \to H$ be a homomorphism. Prove that if Φ is surjective, then H is cyclic.

Proof. Since G is cyclic, and since Φ is surjective:

$$(\exists g \in G)(\langle g \rangle = G)$$
$$\wedge$$
$$(\forall h \in H)(\exists x \in \langle g \rangle)(\Phi(x) = h)$$

Thus, let $h \in H$. Since for all such h there exists some $x \in \langle g \rangle$ such that $x = g^k$ for some $k \in \mathbb{Z}$, we have that $h = \Phi(x) = \Phi(g^k)$.

$$h = \Phi(g^k) = \Phi(g^{k-1}) \cdot \Phi(g)$$
$$\vdots$$
$$h = \underbrace{\Phi(g) \cdot \ldots \cdot \Phi(g)}_{k \text{ times}}$$

Therefore, $h = \Phi(g)^k$ and since $\Phi(g) \in H$, it follows that for any $h \in H$ there exists a generator, $\Phi(g)$ say such that:

$$(\forall h \in H)(\exists m \in \mathbb{Z})(h = \Phi(g)^m).$$

Thus, $\langle \Phi(g) \rangle = H$. It means that H is a cyclic group given that Φ is a surjective homomorphism. □

Problem 3

For each element of $\mathbb{Z}/5\mathbb{Z}$, find its order, then decide whether or not it is a generator. Then do the same for each element of $\mathbb{Z}/6\mathbb{Z}$.

$\mathbb{Z}/5\mathbb{Z}$: The elements of $\mathbb{Z}/5\mathbb{Z}$ are the integers modulo 5. Namely, $a + 5\mathbb{Z}$ where a can be uniquely identified from the possible remainders $a \in \{0, 1, 2, 3, 4\}$.

- $(0 + 5\mathbb{Z})$ has order 1 because it always retrieves itself (it is a unit). $0 + 5\mathbb{Z} + 0 + 5\mathbb{Z} = 0 + 5\mathbb{Z}$. Thus, it can't be a generator.
- $(1 + 5\mathbb{Z})$ has order 5 because you can perform 5 times the operation until you get the same back. In essence, this in fact is a generator for $\mathbb{Z}/5\mathbb{Z}$.

$$1 + \underbrace{1 + \ldots + 1}_{\text{5 times}} = 1 + 5 \quad \wedge \quad 1 \equiv 6 \mod 5 \Rightarrow 1 \equiv 1 \mod 5$$

- $(2 + 5\mathbb{Z})$ is also a generator and has order 5 because adding five two's to 2 gives 12 which has remainder 2. It is a generator because it can retrieve all elements in $\mathbb{Z}/5\mathbb{Z}$.
- $(3 + 5\mathbb{Z})$ is also a generator and has order 5 because adding five three's to 3 gives 18 which has remainder 3. It is a generator because it can retrieve all elements in $\mathbb{Z}/5\mathbb{Z}$.
- $(4 + 5\mathbb{Z})$ is also a generator and has order 5 because adding five four's to 4 gives 24 which has remainder 4. It is a generator because it can retrieve all elements in $\mathbb{Z}/5\mathbb{Z}$.

$\mathbb{Z}/6\mathbb{Z}$:

- $(0 + 6\mathbb{Z})$ has order 1 as it is the unit and thus it is not a generator.
- $(1 + 6\mathbb{Z})$ has order 6 and it is a generator.
- $(2 + 6\mathbb{Z})$ has order 3 (since it divides 6) and thus not a generator. Another way to look at it is that $2 \cdot 3 = 6 \equiv 0 \mod 6$
- $(3 + 6\mathbb{Z})$ has order 2 and it is not a generator.
- $(4 + 6\mathbb{Z})$ has order 3 (because $4 + 4 \cdot 3 = 16$ which has remainder 4) and thus not a generator.
- $(5 + 6\mathbb{Z})$ has order 6 and it is a generator.

A.1.11 Assignment Due February 5th, 2025

Problem 1

For any group G, the identity function $\iota\colon G \to G$ is an isomorphism between G and itself. However, there are sometimes more!

a) Find a function $\iota : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ which is not the identity function, but which is an isomorphism.

b) How many isomorphisms $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ are there total?

(a) The function $\tau(x) = 5x \mod 6$ is an isomorphism. Let $x \in \mathbb{Z}/6\mathbb{Z}$, then:

$$\tau(x) = 5x \mod 6$$

This function is bijective and respects the group operation. To verify: - For any $a, b \in \mathbb{Z}/6\mathbb{Z}$:

$$\tau(a+b) = 5(a+b) \mod 6 = (5a+5b) \mod 6 = (5a \mod 6)+(5b \mod 6) = \tau(a)+\tau(b)$$

Therefore, $\tau(x) = 5x \mod 6$ is an isomorphism.

(b) There are 4 isomorphisms for $\mathbb{Z}/5\mathbb{Z}$. Since $\mathbb{Z}/5\mathbb{Z}$ is a cyclic group of order 5, any automorphism is determined by where it sends a generator. The generators of $\mathbb{Z}/5\mathbb{Z}$ are the elements $\{1, 2, 3, 4\}$. Each of these generators can be mapped to any other generator. Therefore, the isomorphisms are:

- $\tau(x) = x$
- $\tau(x) = 2x \mod 5$
- $\tau(x) = 3x \mod 5$
- $\tau(x) = 4x \mod 5$

Hence, there are 4 isomorphisms in total.

Problem 2

Let G be a group and H a subgroup. Show that $b^{-1}a \in H$ if and only if $b = ah$ for some $h \in H$.

Proof. I first show ($\Rightarrow$). Suppose that $b^{-1}a \in H$. Since H is a subgroup of G (inheriting its characteristics), it follows that $b^{-1}a = c$ for some $c \in H$ and $\exists b \in G$ because b^{-1} is guaranteed to have an inverse in G. Notice the same applies to a. Therefore:

$$b(b^{-1}a) = b(c) \Longrightarrow a = bc \Rightarrow b = ac^{-1} = ah$$

So, $b = ah$ for some $h \in H$.
To show ($\Leftarrow$), assume $b = ah$ for some $h \in H$ and $a, b \in G$. Since H is a subgroup and G a group, all these elements have an inverse in H. Thus:

$$b = ah \Longrightarrow b^{-1}bh^{-1} = b^{-1}ahh^{-1} \Longrightarrow b^{-1}a = h^{-1}$$

So, since $h^{-1} \in H$, also $b^{-1}a \in H$. □

A.1.12 Assignment Due February 7th, 2025

Problem 1

Let $G = S_4$, $V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Show that every left coset fV has a representative $f' \in fV$ with $f'(4) = 4$.

Proof. We have:

- $G = S_4 = \{f : \{1,2,3,4\} \to \{1,2,3,4\} \mid f \text{ is bijective}\}$, the symmetric group of 4 elements. It consists of all bijective functions from the set $\{1,2,3,4\}$ to itself. S_4 contains all the permutations of the set $\{1,2,3,4\}$.
- $V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \subseteq S_4$, known as the Klein four-group. It consists of the identity permutation e and three products of disjoint 2-cycles. This group is also abelian.

We want to show that every left coset fV has a representative $f' \in fV$ with $f'(4) = 4$, where $fV = \{fv : v \in V\}$. Note that for each $m \in \{1,2,3,4\}$, there exists some $v \in V$ such that $v(4) = m$; in order, they are $(1,4)(2,3)$ mapping 4 to 1, $(1,3)(2,4)$ mapping 4 to 2, $(1,2)(3,4)$ mapping 4 to 3, and e mapping 4 to 4.

Suppose $f \in S_4$ is any given permutation. We need to find some $h_f \in V$ such that $h_f(4) = f^{-1}(4)$. This is because any element in the left coset fV is of the form fv for $v \in V$. Since $h_f \in V$, we know $fh_f \in fV$. We choose h_f such that $h_f(4) = f^{-1}(4)$.

Now, let's construct f' such that $(fh_f)(4) = f(h_f(4))$. Since $h_f(4) = f^{-1}(4)$, we have:

$$(fh_f)(4) = f(f^{-1}(4)) = 4$$

Thus, $f' = fh_f$ is a representative of the left coset fV such that $f'(4) = 4$. □

Problem 2

Let G be a group and H a subgroup.

a) Show that the cardinality of any left coset is the same as the cardinality of H.

b) Let G be a finite group. Show that the order of G is a multiple of the order of H.

c) Let G have order 24 and H have order 4. What is the cardinality of the set G/H?

a) To show that any left coset aH has the same cardinality as H it suffices to find some bijection between H and aH. The function $f(h) = ah$, $f : H \to aH$ where $h \in H$ is bijective. Let's see why: f is surjective because the left coset $aH = \{ah : h \in H\}$ is made by all the elements of the form ah for all $h \in H$. In a nutshell, for any choice of h, we have that $f(h) = ah \in aH$. Notice that f is also injective: suppose $f(h_1) = ah_1 = ah_2 = f(h_2)$, then $a^{-1}ah_1 = a^{-1}ah_2 \Rightarrow h_1 = h_2$. Since f is injective and surjective, f is a bijection. Thus, the domain and codomain have the same cardinality.

b) We established earlier that all cosets of H have the same cardinality and thus same order. Furthermore, these cosets are disjoint because if they overlapped in one element g they would indeed be the same coset:

$$g \in a_1H \wedge g \in a_2H \Rightarrow g = a_1h_1 = a_2h_2 \Rightarrow a_1 = a_2h_2h_1^{-1} \Rightarrow a_1 \in a_2H$$

$$\Rightarrow a_1H = a_2H$$

Since the cosets of H are disjoint, they can together make up all the entirety of G. Namely,

$$G = \bigcup_{a_i \in G} a_iH$$

Therefore, the order of G is also the cardinality of this union of disjoint cosets. Since every coset has the same cardinality, and the index of H in G—the number of left cosets of a subgroup—denoted $[G : H]$ is the number of left cosets of H in G, it follows:

$$|G| = |H| \cdot [G : H]$$

c) The set of left cosets G/H has order $[G : H]$. So, it follows that $24 = 4 \cdot |G/H| \Rightarrow |G/H| = 6$.

A.1.13 Assignment Due February 10th, 2025

Problem 1

Show that, if H is a normal subgroup of G, then G/H is a group.

Proof. Suppose H is a normal subgroup. That means that $ghg^{-1} \in H$ for any $g \in G$ and $h \in H \subseteq G$. Then to show that the set of left cosets of H in G, namely G/H, is a group with coset multiplication as law of composition (since H is normal, 'it works'):
Closure: For any two elements $aH, bH \in G/H$, the law of composition on the left coset is another left coset because H is normal.

$$(aH) \cdot (bH) = \{ah_1bh_2 : h_1, h_2 \in H\} = \{ah_1h_2b : h_1, h_2 = h \in H\} = abH$$

Associativity: For $aH, bH, cH \in G/H$, we have

$$aH \cdot ((bH) \cdot (cH)) = aH \cdot (bcH) = abcH = (abH) \cdot cH = ((aH) \cdot (bH)) \cdot cH$$

which is inherited from the law of composition of G, where $a(bc) = (ab)c$ since G is a group.
Unital: G/H is unital because the unit of G, namely e_G,yields:

$$(aH) \cdot (e_GH) = (ae_G)H = aH = (e_Ga)H = (e_GH) \cdot (aH)$$

Invertible: All the elements in G/H have inverses by looking at the guaranteed inverses of the representatives from G.

$$(aH) \cdot (a^{-1}H) = (aa^{-1})H = H$$

Thereby, since all group criteria is met, G/H is a group under coset multiplication. □

Problem 2

Let G be a group and H be a normal subgroup of G. Show that the function $\pi\colon G \to G/H$ given by the formula $\pi(g) = gH$ is a homomorphism. What is the kernel of π? What is the image of π?

Proof. Let $\pi\colon G \to G/H$ be given by the formula $\pi(g) = gH$. Then, for $g_1, g_2 \in G$. Since G and G/H are groups, we have that the function π is a homomorphism since:

$$\pi(g_1g_2) = (g_1g_2)H = (g_1H) \cdot (g_2H) = \pi(g_1) \cdot \pi(g_2)$$

□

Now, to find the image and the kernel of the homomorphism.

- $\operatorname{im}\pi := \{gH : g \in G\} = G/H$, so π is surjective.
- $\ker\pi := \{g \in G : \pi(g) = H\} = H$

A.1.14 Assignment Due February 12th, 2025

Problem 1

Let G and H be the following two subgroups of $GL_3(\mathbb{R})$.

$$G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}, \qquad H = \left\{ \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid z \in \mathbb{R} \right\}.$$

Show that H is a normal subgroup of G.

Proof. Let $A \in G$ and $B \in H$. □

Problem 2

Let G and H be as in the previous problem. The vector space $\mathbb{R}^2$ can be viewed as a group when we use vector addition as our law of composition. Consider the function $\phi\colon G/H \to \mathbb{R}^2$ given by the formula.

$$\phi\left(\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} H \right) = (a, b).$$

Show that this function is well defined. [What does well defined mean? In order to compute $\phi(gH)$, I need to pick a representative of gH and do a computation with that element. If I take two different representatives g and g' of the same coset $gH = g'H$, then we should get the same result $\phi(gH) = \phi(g'H)$.]

Problem 3

Let G, H, and ϕ be as in the previous two problems. Show that ϕ is an isomorphism.

A.1.15 Assignment Due February 14th, 2025

Problem 1

Let G be the following subgroup of $\mathrm{GL}_3(\mathbb{R})$:

$$G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}.$$

The vector space $\mathbb{R}^2$ can be viewed as a group when we use vector addition as out law of composition. Consider the function $\pi\colon G \to \mathbb{R}^2$ given by the formula

$$\pi \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = (a, b).$$

Show that π is a homomorphism. Find $\ker \pi$ and show that π is surjective. What does the first isomorphism theorem say about this situation?

Problem 2

In this problem, we'll give another proof that kernels are normal. Let G and H be groups, let $\phi\colon G \to H$ be a homomorphism, and write $K = \ker \phi$.

a) Let $a \in G$. Show that the left coset aK is the set $\{g \in G \mid \phi(g) = \phi(a)\}$.

b) Let $a \in G$. Show that the right coset Ka is the set $\{g \in G\ mid \phi(g) = \phi(a)\}$.

c) Use the definition to conclude that K is a normal subgroup of G.

A.1.16 Assignment Due February 19th, 2025

Problem 1

Let $G = \mathrm{GL}_2(\mathbb{R})$. Then let $S = \mathrm{SL}_2(\mathbb{R})$ be the subgroup consisting of matrices of determinant 1. Show that S is normal in G. Then use the first isomorphism theorem to find a familiar group isomorphic to G/S. [Hint: is there a homomorphism that S is the kernel of?]

Problem 2

Let $G = \mathrm{GL}_2(\mathbb{R})$. Then let $S = \mathrm{SL}_2(\mathbb{R})$ be the subgroup consisting of matrices of determinant 1 and let D be the subgroup consisting of diagonal matrices. Find the subgroups SD and $S \cap D$ of G

Problem 3

Let $G = \mathrm{GL}_2(\mathbb{R})$. Then let $S = \mathrm{SL}_2(\mathbb{R})$ be the subgroup consisting of matrices of determinant 1 and let D be the subgroup consisting of diagonal matrices. Find familiar groups that are isomorphic to SD/S and to $D/S \cap D$. Compare these to the group you found in Problem 1.

A.1.17 Assignment Due February 19th, 2025

A.1.18 Assignment Due February 26th, 2025

Problem 1

Show that the k-cycle $(1, 2, \ldots, k)$ can be written as a product of transpositions as $(1, 2, \ldots, k) = (1, k)(1, k-1)\ldots(1, 3)(1, 2)$. For what k is $(1, 2, \ldots, k)$ even? For what k is it odd?

Proof. □

Problem 2

Let $x_1, x_2, \ldots, x_k$ be a collection of pairwise distinct element of $\{1, \ldots, n\}$. (This means that wach x_i is from that set, and, if $i \neq j$, $x_i \neq x_j$.) Write the k-cycle $(x_1, x_2, \ldots, x_k)$ as a product of transpositions. When is $(x_1, x_2, \ldots, x_k)$ even? when is it odd?

Problem 3

For each of the following elements of S_6, determine if it is even or odd.

a) $(1, 2)$

b) $(1, 2, 3)$

c) $(1, 2)(3, 4)$

d) $(1, 2, 3)(4, 5)$

e) $(1, 2, 3)(4, 5, 6)$

A.1.19 Assignment Due February 28th, 2025

Problem 1

Using only the rules that $r^n = e$, $s^2 = e$, and $s \cdot r \cdot s = r^{n-1}$, one can take any expression formed out of r's and s's, and turn it into one of the form $r^k s^\ell$ for $0 \leq k \leq n-1$, $0 \leq \ell \leq 1$. Do this for each of the following elements of $D_{2\cdot 5}$.

a) r^{103}

Since $r^n = e$, and $n = 5$, we have $r^5 = e$. Therefore, $r^{103} = r^{103 \mod 5} = r^3$.

b) s^7

Since $s^2 = e$, then $s^7 = (s^2)^3 s = es = s$

c) $s^7 r^{103}$

By the prior portions we have that $s^7 r^{103} = sr^3 = sr^3$

d) $rsrs$

$srs = r^{n-1} \Longrightarrow r(srs) = rr^{n-1} = r^n = e$

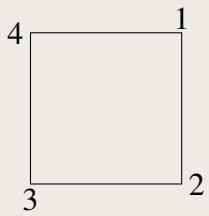
e) $r^3 s r^2 s r$

$r^3 s r^2 s r = r^3 s r^2 s r s s^{-1} = r^3 s r^2 r^{n-1} s^{-1} = r^3 s r r^n s^{-1} = r^3 s r s^{-1} s^2 s^{-2} = r^3 s r s s^{-2}$.
From here, notice that $s^2 = e \Longrightarrow (s^2)^{-1} = e$, therefore $r^3 s r s s^{-2} = r^3 r^{n-1} = r^n r^2 = r^2$

Problem 2

By labeling the vertices of a regular n-gon with the numbers 1 through n, we can view $D_{2\cdot n}$ as a subgroup of S_n. Note, by the statement in problem 1, that you can list all of the elements of $D_{2\cdot 4}$ and $D_{2\cdot 3}$ by listing expressions of the form $r^k s^\ell$ for $0 \leq k \leq n-1$, $0 \leq \ell \leq 1$.

a) Draw a square oriented so that its bottom edge is horizontal. Label the vertices of the square, starting with 1 on the top right vertex, and continuing clockwise in order. For each element of $D_{2\cdot 4}$, write which permutation of the set $\{1, 2, 3, 4\}$ it corresponds to in disjoint cycle notation. Is this all of S_4? [You don't have to draw the square on the paper you turn in, but it will help you visualize what's happening if you draw it somewhere.]

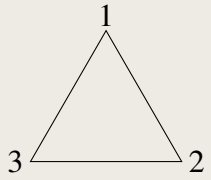


For a square, we have (counterclockwise):

r : $(1 \to 2 \to 3 \to 4 \to 1) = (1, 2, 3, 4)$
r^2 : $(1 \to 3, 2 \to 4) = (1, 3)(2, 4)$
r^3 : $(1 \to 4 \to 3 \to 2 \to 1) = (1, 4, 3, 2)$
s : Reflection about the vertical axis through vertices 1 and 3 $= (1, 3)(2, 4)$
sr : Reflection about the horizontal axis through vertices 2 and 4 $= (1, 4)(2, 3)$
sr^2 : Reflection about the diagonal axis through vertices 2 and 4 $= (1, 2)(3, 4)$
sr^3 : Reflection about the diagonal axis through vertices 1 and 3 $= (1, 3)(2, 4)$

These elements cover the symmetries of a square, but they do not form all of S_4, as S_4 contains 24 elements while $D_{2\cdot 4}$ contains only 8.

b) Draw an equilateral triangle oriented so that its bottom edge is horizontal. Label the vertices of the triangle, starting with 1 on the top vertex, and continuing clockwise in order. For each element of $D_{2\cdot 3}$, write which permutation of the set $\{1, 2, 3\}$ it corresponds to in disjoint cycle notation. Is this all of S_3? [You don't have to draw the triangle on the paper you turn in, but it will help you visualize what's happening if you draw it somewhere.]



For an equilateral triangle, we have:

r : $(1 \to 2 \to 3 \to 1) = (1, 2, 3)$
r^2 : $(1 \to 3 \to 2 \to 1) = (1, 3, 2)$
s : Reflection about the vertical axis through vertex 1 $= (1, 3)$
sr : Reflection about the axis through vertex 2 $= (1, 2)$
sr^2 : Reflection about the axis through vertex 3 $= (2, 3)$

These elements cover the symmetries of a triangle, and they do form all of S_3, as S_3 contains 6 elements while $D_{2\cdot 3}$ also contains 6 elements.

A.1.20 Assignment Due March 3rd, 2025

Problem 1

This problem is about how direct products of cyclic groups.

a) Show that $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ is cyclic.

b) Show that, if $\gcd(a, b) = 1$, then $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\ Z$ is cyclic.

c) Show that $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is not cyclic. [Hint: what is the largest order that an element could possibly have?]

d) Show that, if $\gcd(a, b) = d > 1$, then $\mathbb{Z}/a\mathbb{Z} \times\ Z/b\mathbb{Z}$ is not cyclic. [Hint: what is the largest order that an element could possibly have?]

a) Consider the element $(1, 1) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. The order of this element is the least common multiple of the orders of 1 in $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}$. Since the order of 1 in $\mathbb{Z}/3\mathbb{Z}$ is 3 and the order of 1 in $\mathbb{Z}/5\mathbb{Z}$ is 5, the order of $(1, 1)$ is $\mathrm{lcm}(3, 5) = 15$. Therefore, $(1, 1)$ generates the group $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$, showing that it is cyclic.

b) Let a and b be integers such that $\gcd(a, b) = 1$. Consider the element $(1, 1) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. The order of $(1, 1)$ is the least common multiple of the orders of 1 in $\mathbb{Z}/a\mathbb{Z}$ and $\mathbb{Z}/b\mathbb{Z}$. Since $\gcd(a, b) = 1$, the order of 1 in $\mathbb{Z}/a\mathbb{Z}$ is a and the order of 1 in $\mathbb{Z}/b\mathbb{Z}$ is b. Thus, the order of $(1, 1)$ is $\mathrm{lcm}(a, b) = ab$. Therefore, $(1, 1)$ generates the group $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, showing that it is cyclic.

c) Consider the elements of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. The order of any element (x, y) is the least common multiple of the orders of x in $\mathbb{Z}/4\mathbb{Z}$ and y in $\mathbb{Z}/6\mathbb{Z}$. The possible orders in $\mathbb{Z}/4\mathbb{Z}$ are $1, 2, 4$ and the possible orders in $\mathbb{Z}/6\mathbb{Z}$ are $1, 2, 3, 6$. Therefore, the largest possible order of an element in $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ is $\mathrm{lcm}(4, 6) = 12$. However, the group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ has 24 elements, but the largest order of any element is only 12. Therefore, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is not cyclic.

d) Let a and b be integers such that $\gcd(a, b) = d > 1$. Consider the elements of $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. The order of any element (x, y) is the least common multiple of the orders of x in $\mathbb{Z}/a\mathbb{Z}$ and y in $\mathbb{Z}/b\mathbb{Z}$. The largest order of any element in $\mathbb{Z}/a\mathbb{Z}$ is a/d and the largest order of any element in $\mathbb{Z}/b\mathbb{Z}$ is b/d. Therefore, the largest possible order of an element in $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ is $\mathrm{lcm}(a/d, b/d) = ab/d$. However, the group $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ has ab elements, but the largest order of any element is only ab/d. Therefore, $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ is not cyclic.

Problem 2

1. Let G and H be groups. We want to show that the set $\{e\} \times H = \{(e, h) \mid h \in H\}$ is a subgroup of the direct product $G \times H$ which is isomorphic to H.

   Proof. First, let's verify that $\{e\} \times H$ is a subgroup of $G \times H$. We need to check the subgroup criteria:

   (a) **Identity:** The identity element in $\{e\} \times H$ is (e, e_H), where e is the identity element in G and e_H is the identity element in H.
   (b) **Closure:** If $(e, h_1), (e, h_2) \in \{e\} \times H$, then $(e, h_1)(e, h_2) = (e, h_1 h_2) \in \{e\} \times H$.
   (c) **Inverses:** If $(e, h) \in \{e\} \times H$, then $(e, h)^{-1} = (e, h^{-1}) \in \{e\} \times H$.

   Therefore, $\{e\} \times H$ is a subgroup of $G \times H$.

   To show that $\{e\} \times H$ is isomorphic to H, define the map $\phi : H \to \{e\} \times H$ by $\phi(h) = (e, h)$. This map is a bijective homomorphism, and thus $\{e\} \times H \cong H$. □

2. Next, we need to show that $\{e\} \times H$ is a normal subgroup of $G \times H$.

   Proof. Let $(g, h) \in G \times H$ and $(e, h') \in \{e\} \times H$. Consider the conjugation:

   $$(g, h)(e, h')(g, h)^{-1} = (g, h)(e, h')(g^{-1}, h^{-1}) = (g, hh'h^{-1}).$$

   Since $hh'h^{-1} \in H$ for all $h' \in H$, it follows that $(g, h)(e, h')(g, h)^{-1} \in \{e\} \times H$. Thus, $\{e\} \times H$ is a normal subgroup of $G \times H$. □

3. We also need to show that $(G \times H)/(\{e\} \times H) \cong G$.

   Proof. Consider the quotient map $\pi : G \times H \to (G \times H)/(\{e\} \times H)$. Define the map $\psi : G \to (G \times H)/(\{e\} \times H)$ by $\psi(g) = \pi((g, e_H))$. This map is an isomorphism because the elements of $\{e\} \times H$ are cosets in the form $(g, h)\{e\} \times H = (g, h)(\{e\} \times H)$. Thus, $(G \times H)/(\{e\} \times H) \cong G$. □

4. Finally, we need to show that it is *not* true that, if a group L has a normal subgroup K, then $L \cong (L/K) \times K$.

   Proof. Consider the group $L = \mathbb{Z}/4\mathbb{Z}$ and the subgroup $K = \{0, 2\}$. Here, K is a normal subgroup of L and $L/K \cong \mathbb{Z}/2\mathbb{Z}$. If $L \cong (L/K) \times K$, we would have $L \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. However, $\mathbb{Z}/4\mathbb{Z}$ is cyclic while $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not. Therefore, $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, proving the statement. □

A.1.21 Assignment Due March 3rd, 2025

A.1.22 Assignment Due March 3rd, 2025

A.1.23 Assignment Due March 3rd, 2025

A.1.24 Assignment Due March 12th, 2025

Problem 1

Let G be a group and X a set on which G acts. G acts on the set of subsets of X by the formula

$$g \cdot S = \{g \cdot x \mid x \in S\} \quad \text{for all} \quad S \subseteq X.$$

Show that $g \cdot S$ and S have the same cardinality. [Recall that a set A has the same cardinality as a set B if there is a bijection $\phi\colon A \to B$.]

Proof. To show that $g \cdot S$ and S have the same cardinality, we construct a bijection $\phi : S \to g \cdot S$. Define $\phi(x) = g \cdot x$.

- **Surjective:** For any $y \in g \cdot S$, there exists $x \in S$ such that $y = g \cdot x$. Hence, ϕ is surjective.
- **Injective:** Suppose $\phi(x_1) = \phi(x_2)$. Then $g \cdot x_1 = g \cdot x_2$. Applying g^{-1} to both sides yields $x_1 = x_2$, so ϕ is injective.

Since ϕ is a bijection, $|g \cdot S| = |S|$. □

Problem 2

Let G be a group, acting on the set of subsets of G by conjugation. Show each of the following.

a) If H is a subgroup of G, then $g \cdot H$ is also a subgroup of G for any $g \in G$.

b) If $g \cdot H$ is a subgroup of G, then H is also a subgroup of G for any $g \in G$. [Note: you can prove this directly, or, if you're tricky, you can use part (a).]

c) For any subgroup H of G and any element $g \in G$, the two subgroups H and $g \cdot H$ are isomorphic. [Hint: Problem 1 can help you with part of this!]

a) Let $H \leq G$. For $g \in G$, consider gHg^{-1}:
   - **Closure:** For $ghg^{-1}, gh'g^{-1} \in gHg^{-1}$, their product is $g(hh')g^{-1} \in gHg^{-1}$.
   - **Inverses:** The inverse of ghg^{-1} is $gh^{-1}g^{-1} \in gHg^{-1}$.
   - **Identity:** $geg^{-1} = e \in gHg^{-1}$.

   Thus, gHg^{-1} is a subgroup.

b) If $gHg^{-1} \leq G$, then $H = g^{-1}(gHg^{-1})g$. By part (a), conjugating a subgroup by g^{-1} yields a subgroup, so $H \leq G$.

c) Define $\phi : H \to gHg^{-1}$ by $\phi(h) = ghg^{-1}$:
   - ϕ is a homomorphism: $\phi(h_1h_2) = gh_1h_2g^{-1} = \phi(h_1)\phi(h_2)$.
   - ϕ is bijective with inverse $\psi(k) = g^{-1}kg$, verifying $\psi(\phi(h)) = h$ and $\phi(\psi(k)) = k$.

   Hence, $H \cong gHg^{-1}$.

A.1.25 Assignment Due March 14th, 2025

Problem 1

We're going to finish the proof of Sylow Theorem 1. As promised, the trick is this: Let $|G| = p^e m$ with $e \geq 1$ and m not divisible by p. Let $S = \{X \subseteq G : |X| = p^e\}$. G acts on S by left multiplication, by the formula

$$g \cdot X = \{g \cdot x \mid x \in X\}.$$

We will find an element $X \in S$ with $|\operatorname{Stab}_G(X)| = p^e$; this $\operatorname{Stab}_G(X)$ will be our Sylow p-subgroup.

a) Recall that Little Lemma 2 states that $|S|$ is not divisible by p. Use this to conclude that there is some $X_0 \in S$ whose orbit $G \cdot X_0$ has cardinality not divisible by p. [Hint: What would happen if all of the orbits had cardinality divisible by p?]

b) Let X_0 be as above, and write $H = \operatorname{Stab}_G(X_0)$. Recall that Little Lemma 1 states that the order $|H|$ has to divide the cardinality $|X_0|$. What are the possible orders for H, in terms of the factorization $|G| = p^e m$?

c) Apply the orbit-stabilizer theorem. Of the possible orders for H that you found in part (b), which of them give you an orbit $G \cdot X_0$ whose cardinality is not divisible by p? Conclude by arguing that this H, which is the stabilizer of this X_0, is a Sylow p-subgroup.

Proof. a) The set S is partitioned into orbits under the action of G. If all orbits had cardinality divisible by p, then $|S|$ would be a sum of multiples of p, contradicting Little Lemma 2. Thus, there exists an orbit $G \cdot X_0$ with cardinality not divisible by p.

b) The stabilizer $H = \operatorname{Stab}_G(X_0)$ must have order dividing $|X_0| = p^e$. Therefore, the possible orders of H are p^k for $0 \leq k \leq e$.

c) By the orbit-stabilizer theorem, $|G \cdot X_0| = |G|/|H|$. For this to be not divisible by p, $|H|$ must cancel all p-factors in $|G|$, implying $|H| = p^e$. Hence, H is a Sylow p-subgroup. □

Problem 2

How many Sylow 5-subgroups are there of S_5? [Hint: $|S_5| = 120 = 2^3 \cdot 3 \cdot 5$. Use the third Sylow theorem to narrow down the possibilities, then see what you can do with what's left.]

The number of Sylow 5-subgroups of S_5 is $\boxed{6}$.