Contents

1 Groups **2**
Tool 1: Group Operation Checking 2
Tool 2: Group or Not a Group? 3
Tool 3: Order of Group Elements 3
Tool 4: Arithmetic of Group Elements 4
Tool 5: Dihedral Group Computation 5
Tool 6: Rigid Motion Group Order for 3D spaces 6
Tool 7: Computations on Cycles and Permutations 7
Tool 8: Order of Cycles 8
Tool 9: Usage of Various Examples of Groups 9
Tool 10: Group Homomorphisms and their Properties 10
Tool 11: Group Isomorphisms and their Properties 12
Tool 12: Automorphisms and their Properties 13
Tool 13: Group Action: Does this act? 14
Tool 14: Orbits, Stablizer and Centralizer 16
Tool 15: Subgroup or Not a Subgroup? 17
Tool 16: Cyclic Subgroups and Their Generators 18
Tool 17: Cyclic or Not Cyclic? 20
Tool 18: Understanding Groups from Generators 20
Tool 19: Normal Subgroups 21
Tool 20: Cosets and Lagrange 22

Abstract Algebra Toolbox

Howard Xiao

1 Groups

Tool 1: Group Operation Checking

Concepts used for this tool are:

Definition 1.1: Groups

A **group** is a set G with an operation $\star : G \times G \to G$ defined, denoted $(g, h) \mapsto g \star h$ for all $g, h \in G$; an *identity* for this operation (denoted e) such that $e \star g = g \star e = g$ for all $g \in G$ and an operation $\text{inv} : G \to G$ such that $g \mapsto g^{-1}$, where $g \star g^{-1} = g^{-1} \star g = e$.
The operation $\star$ must be **associative**, i.e. for all $g, h, k \in G$, $g \star (h \star k) = (g \star h) \star k$.

Definition 1.2: Abelian Groups

A group G is called **abelian** if the operation $\star$ defined for the group is **commutative**, i.e. for all $g, h \in G$, $g \star h = h \star g$.

Some examples of this type of questions follow:

Exercise 1.1: Tool 1

1. Check whether $\star$ defined on $\mathbb{Z} \times \mathbb{Z}$ such that $(a, b) \star (c, d) = (ad + bc, bd)$ is associative.
2. Check whether $\star$ defined on $\mathbb{Q} \setminus \{0\}$ such that $a \star b = \frac{a}{b}$ is associative.
3. Check whether $\star$ defined in 1. is commutative.
4. Check whether $\star$ defined on $\mathbb{Q}$ such that $a \star b = \frac{a+b}{5}$ is commutative.
5. Prove that addition of residue classes of $\mathbb{Z}/n\mathbb{Z}$ is associative and commutative.
6. Prove that the law of composition defined on any set S by $ab = a$ for all $a, b \in S$ is associative, but not commutative.

Further exercises can be found on Exercises of Dummit and Foote section 1.1, and Artin exercises for Chapter 2 Section 1.

Tool 2: Group or Not a Group?

This tool follows from Tool 1 since verifying operation of the group candidate is important. See definition 1.1 and 1.2 for concepts.

Exercise 1.2: Tool 2

1. Let G be a group with operation $\star$ and identity e. Prove that the set $S \subset G$ consisting of all invertible elements in G is a group.
2. Prove that for all $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ with multiplication operation is *not* a group.
3. Determine what sets are a group under the addition operation:
(a) Set of rational numbers with absolute value less than 1.
(b) Set of rational numbers with denominators 1 or 2.
(c) Set of rational numbers in lowest terms whose denominator is odd.
4. Let $G = \{x \in \mathbb{R} : 0 \leq x < 1\}$, and for all $x, y \in G$ we define $x \star y = x + y - \lfloor x + y \rfloor$, where $\lfloor x + y \rfloor$ is the floor operator. Prove that with $\star$, G is an abelian group.
5. Prove that $A \times B$ is an abelian group if and only if both A, B are abelian groups.

Further exercises can be found on Exercises of Dummit and Foote section 1.1, and Artin exercises for Chapter 2 Section 2.

Tool 3: Order of Group Elements

The concepts for this tool are the following:

Definition 1.3: Order of a group element

Given a group G and element $g \in G$, the **order** of g, denoted $|g|$, is the smallest natural number $n \in \mathbb{N}$ such that $g^n = e \in G$. If such an n does not exist, we say $|g| = \infty$.

Definition 1.4: Order of a group

Given a group G, the **order** of this group is the cardinality of G as a set.

The two above definitions should not be confused. Examples of this tool's usage follow:

Exercise 1.3: Using Order

1. Find the orders of each element in the multiplicative group $\mathbb{Z}/6\mathbb{Z}\setminus\{0\}$.
2. Let $x \in G$ for G be a group. Then, if $x^2 = e \in G$, show that $|x|$ is either 1 of 2.
3. Given any group G and $x \in G$, show that x, x^{-1} have same order.
4. Suppose $x \in G$ for some group G and $|x| = n = st$ for some natural numbers $s, t \in \mathbb{N}$. Prove that $|x^s| = t$.
5. Suppose $x \in G$ for some group G, $|x| = n < \infty$, then show that $|G| > n$.
6. Prove that for all a, b in group G, $|ab| = |ba|$.
7. Prove that elements $(a, 1)$ and $(1, b)$ commutes in group $A \times B$, and the order of (a, b) is the least common multiple of $|a|$ and $|b|$.
8. Prove that given group G, some element $x \in G$. If $|x| = \infty$, show that $x, x^2, \ldots, x^n, \ldots$ for all $n \in \mathbb{N}$ is distinct.
9. Let $G = \{1, a, b, c\}$ of order 4, show that if every element in G has order less than or equal to 3, the operation defined for G is unique, and under this operation, G is abelian.

Further exercises can be found on Exercises of Dummit and Foote section 1.1, and Artin exercises for Chapter 2 Section 2.

Tool 4: Arithmetic of Group Elements

This tool builds on Tool 3, and the following concepts:

Theorem 1.1: Properties of G

1. The identity $e \in G$ is unique.
2. The inverse g^{-1} for each $g \in G$ is unique.
3. ${g^{-1}}^{-1} = g$ for all $g \in G$.

Proof. The proof of this theorem is very straightforward, hence will be left as an exercise (solution is provided in the solution file). □

Theorem 1.2: Cancellation Laws

Given a group G, and $g, x, y \in G$, if $gx = gy$, then $x = y$. Similarly, if $xg = yg$, $x = y$.

Proof. Proof is very simple, solution provided in solution file. □

Examples of using this tool follow:

Exercise 1.4: Tool 4

1. Prove that $(a_1 \star \cdots \star a_n)^{-1} = a_n^{-1} \star \cdots \star a_1^{-1}$, for $a_1, \ldots, a_n \in G$ for some group G.
2. Given a group G and given $x, y \in G$, prove that $xy = yx$ if and only if $y^{-1}xy = x$, and if and only if $x^{-1}y^{-1}xy = e$.
3. Prove that given group G, if $x^2 = e$ for all $x \in G$, then G is abelian.
4. Given a group G and $x, y, z \in G$. If $xyz = e$, is $yzx = e$ always true? Is $yxz = e$ always true? Come up with proofs/counter examples.

Further exercises can be found on Exercises of Dummit and Foote section 1.1, and Artin exercises for Section 2.

Tool 5: Dihedral Group Computation

Usage of this tool depends on the understanding of the concept of groups. Concepts used for this tool are:

Definition 1.5: Symmetries

Given a regular n-gon, we define the set of symmetries the set of rotations and reflections defined on this n-gon. Symmetries sometimes are also called "rigid motions".

Definition 1.6: Elementary Rotation

Given a regular n-gon, labelling each of the vertices from 1 to n counterclockwise. We define the elementary rotation (denoted ρ) to be the rotation that takes $x \mapsto x + 1$ for all $x \in \{1, \ldots, n-1\}$ and $n \mapsto 1$.

Theorem 1.3: Dihedral Group

The set of symmetries for any regular n-gon is a group under the operation of composition, called **Dihedral group**.

Proof. We need to observe a few things.
1. All rotations are of the form $\rho, \rho^2, \ldots, \rho^{n-1}$ plus the identity $e = \rho^n$, which represents not permuting the vertices of the n-gon at all.
2. If n is even, the set of reflections are reflections with axis the line through midpoints of two opposite sides (Type I) and reflections with axis a diagonal (Type II); if n is odd, the set of reflections are reflections with axis the line through a vertex and the midpoint of its opposite side.

Now we are ready to prove the theorem. Firstly, rotation compose with rotation will result in another rotation by 1. Let us consider rotation ρ compose with some reflection s. If n is odd, label each point of the n-gon, and suppose the reflection axis fixes point x, and through the midpoint of side a, $a+1$. Then, we know $(s\circ\rho)(x-1) = s(x) = x$, $(s\circ\rho)(x) = s(x+1) = x-1$, and $(s \circ \rho)(a) = s(a+1) = a$. In this case, $s \circ \rho$ is the reflection with axis fixing a and through the midpoint of side x and $x-1$.
If n is even, also label each point of the n-gon. Suppose s is Type I reflection with axis through midpoint of $a-1$, a and midpoint of $b+1$, b. Then, $(s \circ \rho)(a-1) = s(a) = a-1$, $(s \circ \rho)(b) = s(b+1) = b$, hence $s \circ \rho$ is the Type II reflection through diagonal joining $a-1$ and b. Suppose s is a Type II reflection with axis through diagonal joining a, b. Then, we know that $(s\circ\rho)(a-1) = s(a) = a$, $(s\circ\rho)(a) = s(a+1) = a-1$, $(s\circ\rho)(b-1) = s(b) = b$, $(s \circ \rho)(b) = s(b+1) = b-1$. In this case, $s \circ \rho$ is a Type I reflection with axis through midpoints of sides $a, a-1$ and $b, b-1$.
Similar for $\rho \circ s$ in both cases, we now know that reflections compose with rotations will result in reflections (and vice versa).
We will leave for exercise that the composition of two reflections is either identity or a rotation. (See solution file for solution). □

Theorem 1.4: D_{2n}

The order of Dihedral Group for any regular n-gon is $2n$, and this group is denoted D_{2n}.

Proof. From above proof, if n is odd, there are n rotations and n reflections, resulting a total of $2n$ symmetries. If n is even, there are n rotations, $\frac{n}{2}$ Type I reflections and $\frac{n}{2}$ Type II reflections, resulting a total of $2n$ symmetries. □

Examples of using this tool follow:

Exercise 1.5: Dihedral Group

1. Let r be any rotation, and s be any reflection on a regular n-gon. Prove that $rs = sr^{-1}$.
2. Let r be any rotation on regular n-gon, s be any element in D_{2n} that is not a power of r. Show that $rs = sr^{-1}$.
3. If n is odd and $n \geq 3$, show that e is the only element that commutes with all other elements in D_{2n}.
4. Let x, y be elements of order 2 in any group G. Prove that if $t = xy$ then $tx = xt^{-1}$, i.e. if $|t| < \infty$, x, t satisfy same relation as $r, s \in D_{2n}$. Similarly for y, t.

Further exercises can be found on Exercises of Dummit and Foote section 1.2.

Tool 6: Rigid Motion Group Order for 3D Spaces

The concepts follow from the definition of rigid motion (Definition 1.5), and the intuition that rigid motion is the movement that maintains the shape and volume.
Some examples of this tool are below:

Exercise 1.6: Tool 6

1. Compute the order of the group of rigid motions of a cube.
2. Compute the order of the group of rigid motions of a tetrahedron.
3. Compute the order of the group of rigid motions of a octahedron.
4. Prove that the order of the group of rigid motions of a space with x faces and y edges on each face is xy.

After proving 4. above, there is no need for any further exercises since you have already mastered these problems with this result.

Tool 7: Computations on Cycles and Permutations

Concepts needed for this tool follow:

Definition 1.7: Symmetric Group S_n

Given a finite set X labelled that $X = \{1, 2, \ldots, n\}$. We call the group of bijections $\tau : X \to X$ the symmetric group (permutation group). The fact that this is a group can easily be shown since composition of bijections is still a bijection, and bijection has inverse.

Theorem 1.5: Order of S_n

The order of S_n is $n!$

Proof. The proof here is left as an exercise (See solution file for solutions). □

Definition 1.8: Cycles

We use cycle notation $(a_1 a_2 \ldots a_n)$ to denote the permutation of $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $\ldots a_n \mapsto a_1$. We call this an n-cycle. A convention for this notation is that $a_1 < a_2 < \ldots a_n$. It can be observed that each cycle is an element in S_n if considered all other elements in X that are not in the cycle is mapped to themselves.

Definition 1.9: Composition of Cycles

We write cycles $(a_1a_2\dots a_n)(b_1b_2\dots b_m)\cdots$ to denote cycle composition. This is equivalent to first apply the cycle from the right most position and move to the left sequentially on the set X.

Theorem 1.6: S_n is non-abelian

S_n is a non-abelian group for all $n \geq 3$.

Proof. It is very straightforward, as we observe that $(12)(13) = (132)$ but $(13)(12) = (123)$. □

Theorem 1.7: Disjoint Cycles Commute

If we have two cycles $(a_1a_2\dots a_n), (b_1b_2\dots b_m)$ such that $\{a_1, a_2, \dots, a_n\} \cap \{b_1, b_2, \dots, b_m\} = \emptyset$, then $(a_1a_2\dots a_n)(b_1b_2\dots b_m) = (b_1b_2\dots b_m)(a_1a_2\dots a_n)$.

Proof. Since these permutations do not interfere with each other, it does not matter what order they are applied to the set. □

Examples of using this tool follow:

Exercise 1.7: Tool 7

1. List all elements of S_3 in cycle notation, and compute their orders (Refer to tool 3 for order computation, order computation is further illustrated in Tool 8).
2. Compute $(135)(123)$.
3. Find the order of $(13456)(27)(389)$. Prove that the order of a cycle written in disjoint cycle notations is the least common multiple of the lengths of the cycles.
4. Given $n, m \in \mathbb{N}$ such that $n \geq m$. Prove that the number of m cycles in S_n is $\frac{n(n-1)\cdots(n-m+1)}{m}$.
5. Show that if $n \geq 4$, then the number of permutation who can be written as the multiplication of two disjoint 2-cycles is $\frac{n(n-1)(n-2)(n-3)}{8}$.

Further exercises can be found on Dummit and Foote Exercise 1.3.

Tool 8: Order of Cycles

The concepts for this tool is already explained in Tool 3 and Tool 7. The main goal is to familiarize the type of questions.

Exercise 1.8: Tool 8

1. Write out the cycle decomposition for every element of order 4 in S_4.
2. Prove that given an m-cycle $\sigma = (a_1 \dots a_m)$, then for all $i \in \{1, 2, \dots m\}$, $\sigma^i : a_x \mapsto a_{(x+i \mod m)}$.
3. Show that an element of order 2 must have a cycle decomposition of commuting 2-cycles.
4. Let $p < n$ be any prime. Show that an element in S_n of order p must have a cycle decomposition of commuting p-cycles. Give counterexamples to this claim when p is not a prime.
5. If $\tau = (12)(34)(56)(78)$, determine whether there exists an n-cycle ($n \geq 8$) σ such that $\sigma^k = \tau$ for some $k \in \mathbb{N}$.
6. Repeat 5. for $\tau = (12)(345)$ and $n \geq 5$.

Further exercises can be found on Dummit and Foote Exercise 1.3.

Tool 9: Usage of Various Examples of Groups

The concepts are mainly about what are some examples of groups, which are summarized below:

Example 1.1: Examples of Groups

1. $\mathbb{Z}$ ($\mathbb{Q}, \mathbb{R}$ with addition). This is very easy to verify, as we have assumed associative laws and additive inverses on $\mathbb{Z}$, $\mathbb{Q}, \mathbb{R}$ and the identity is 0.
2. $\mathbb{Z}/n\mathbb{Z}$ is a group under addition. (shown in Tool 1)
3. S_n is an example of a group.
4. The group of rigid motions on regular n-gon is another example.
5. Any field is a group by definition.
6. We denote $GL(n, \mathbb{F})$ to be all invertible $n \times n$ matrices with entries in $\mathbb{F}$. This is a group under matrix multiplication, since multiplication of two invertible matrices gives another invertible matrix, and identity matrix is invertible and is the identity for this group.
7. Similarly, we denote $SL(n, \mathbb{F})$ to be all $n \times n$ matrices with determinant 1 and entries in $\mathbb{F}$. This is also a group under matrix multiplication, since multiplication of two det 1 matrices gives another det 1 matrix, and identity matrix is det 1 and is the identity for this group.
8. We also denote $O(n, \mathbb{F})$ to be all orthogonal $n \times n$ matrices, i.e. all $n \times n$ matrices A (with entries in $\mathbb{F}$) such that $A^T A = I$.
9. We call the group established in Exercise 1.3.9 the "Klein-4" group.
10. We have another example, called the "Quarternion Group", denoted $\mathbb{H}$ or Q_8, which is the set of elements $\{\pm 1, \pm i, \pm j, \pm k\}$ such that $1^2 = (-1)^2 = 1$, $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, and $ik = j = -ki$.

Examples of using this tool follow:

Exercise 1.9: Tool 9

1. Write out each element of $GL_2(\mathbb{F}_2)$, and show that this group is non-abelian. ($\mathbb{F}_2$ is a field with only 2 elements $0, 1$.)
2. Show that $GL(n, F)$ is finite if and only if F is finite.
3. Let G be the set of all 2×2 upper triangular matrices in $\mathbb{R}$. Prove that G is a group.
4. Compute the order of each element in Q_8.

Further exercises can be found on Dummit and Foote Exercises 1.4 and 1.5.

Tool 10: Group Homomorphisms and their Properties

Concepts needed for this tool are the following, plus understanding of previous tools, especially Tool 4 and Tool 9:

Definition 1.10: Group Homomorphism

Given two groups G, H, a (group) homomorphism is a map $\phi : G \to H$ such that for all $g, g' \in G$, we have $\phi(gg') = \phi(g)\phi(g')$.

Definition 1.11: G

ven a homomorphism $\phi : G \to H$, we define the "kernel" of ϕ to be $\{g \in G : \phi(g) = e_H\}$,

Theorem 1.8: Properties of Homomorphism

If we have $\phi : G \to H$ is a homomorphism between two groups, then we know that:
1. $\phi(e_G) = e_H$, where e_G, e_H represents the identities for G and H respectively.
2. $\phi(g^{-1}) = (\phi(g))^{-1}$ for all $g \in G$.

Proof. Proof of this theorem is straight-forward, hence only included in solution file. □

Examples of using this tool follow:

Exercise 1.10: Tool 10

1. Show that the "conjugate" map $\phi : G \to G$ such that $\phi(g) = g_0 g g_0{}^{-1}$ for some specific $g_0 \in G$ for all $g \in G$, is a homomorphism.
2. Show that the inverse map $\phi : G \to G$ such that $g \mapsto g^{-1}$ for all $g \in G$ is a group homomorphism if and only if G is abelian.
3. Show that for any homomorphism $\phi : G \to H$, any $g \in G$, $\phi(g^n) = (\phi(g))^n$ for all $n \in \mathbb{N}$.
4. Define $\pi : \mathbb{R}^n \to \mathbb{R}$ to be the projection onto first coordinate, i.e. $(x_1, \ldots, x_n) \mapsto x_1$. Prove that this is a group homomorphism.
5. Prove that if $\phi : G \to G'$ is a homomorphism and surjective, then if G is abelian then G' is abelian.
6. Define $f : \mathbb{R} \to \mathbb{C} \setminus 0$, where $\mathbb{R}$ is treated as an additive group, and $\mathbb{C} \setminus \{0\}$ is treated as a multiplicative group. $f(x) = e^{ix}$. Prove that in this case f is a homomorphism.
7. Consider $\phi : S \to \mathbb{R} \setminus \{0\}$ where S is the set of all 2×2 upper triangular matrices of $\mathbb{R}$. Define $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a^2$. Prove that ϕ is a group homomorphism if $\mathbb{R} \setminus \{0\}$ is considered as a multiplicative group.
8. Prove that the image of a homomorphism is a group.

Further exercises can be found on Dummit and Foote Exercise 1.6 and Artin Exercise 2.5.

Tool 11: Group Isomorphisms and their Properties

Concepts used for this tool are the following:

Definition 1.12: Isomorphisms

A map $\phi : G \to H$ is an isomorphism if ϕ is a bijective homomorphism. If there exists such a ϕ, we call G and H "isomorphic" to each other, denoted $G \cong H$.

Theorem 1.9: Properties of Isomorphisms

Given $\phi : G \to H$ an isomorphism, we have:
1. $|G| = |H|$
2. G is abelian if and only if H is abelian.
3. For all $x \in G$, $|x| = |\phi(x)|$.

Proof. 1. Suppose $|G|$ is finite, then $|H| = |G|$ must also be finite given by the definition of bijectivity. If $|G|$ is infinite, then $|H|$ must also be infinite, hence $|G| = |H|$.
2. We prove two directions: if G is abelian, for all $x, y \in H$, we know that $x = \phi(a), y = \phi(b)$ for some $a, b \in G$, and we know that $xy = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = yx$, hence H is abelian. The other direction follows exactly the same way by swapping G and H above.
3. Suppose $|x| = n$, i.e., $x^n = e$, then we know that $\phi(x^n) = \phi(e) = e = (\phi(x))^n$ by previous exercises on homomorphisms, thus, we know that $|\phi(x)| \leq n$. We also know that if $(\phi(x))^m = e$, then $\phi(x^m) = e$, since ϕ is a bijection, $x^m = e \in G$, thus $|x| \leq |\phi(x)| \leq n$, hence $|\phi(x)| = |x| = n$. □

Examples of using this tool follow:

Exercise 1.11: Tool 11

1. Prove that the multiplicative groups $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ are not isomorphic.
2. Prove that the additive groups of $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.
3. Prove that D_8 and Q_8 are not isomorphic.
4. For groups A, B, prove that $A \times B \cong B \times A$.
5. Prove that ϕ is an isomorphism if and only if ϕ is a surjective homomorphism with kernel e.
6. Show that if ϕ is an isomorphism, ϕ^{-1} is also an isomorphism.
7. Describe all homomorphisms from $\mathbb{Z}^+ \to \mathbb{Z}^+$, and indicate which are injective, surjective or bijective(isomorphism).

Further exercises can be found on Dummit and Foote Exercise 1.6 and Artin Exercise 2.6.

Tool 12: Automorphisms and their Properties

Concepts of this tool follow closely from Tool 10 and Tool 11, with new concepts follow:

Definition 1.13: Automorphisms

If G is a group, isomorphisms from G to itself are called automorphisms.

Example 1.2: Examples of Automorphisms

1. If $G = \mathbb{Z}^+$, we have found in previous exercises that $\phi = id$ and $\phi'(n) = -n$ are two automorphisms on G.
2. If G is abelian, we know that $\phi : g \mapsto g^{-1}$ is homomorphism. Besides, for all $g \in G$, we know that $\phi^{-1}(g) = g^{-1}$, thus we know that ϕ is bijective, hence an automorphism.
3. Fix a $g_0 \in G$, we know that the map $C_{g_0} : g \mapsto g_0 g {g_0}^{-1}$ is a homomorphism. Given $g \in G$, we know that ${C_{g_0}}^{-1}(g) = g_0^{-1} g g_0$, hence C_{g_0} is also an automorphism.

Definition 1.14: Inner and Outer Automorphisms

e call the automorphisms that has form C_{g_0} for some $g_0 \in G$ the inner automorphisms. We say that the automorphisms that are not inner are outer automorphisms. The set of inner automorphisms are denoted $inn(G)$.

Theorem 1.10: $inn(G)$

$inn(G)$ is a group. If G is abelian, $inn(G) = \{id\}$.

Proof. The proof of this theorem is very direct from definition, hence is left as an exercise (see solution file for solutions). □

Theorem 1.11

Consider the map $\phi : G \to Aut(G)$ that $g \mapsto C_g$, this map is a homomorphism, with image $inn(G)$.

Proof. Firstly, Consider the map $C_{gg'}$, $C_{gg'}(x) = gg'x(gg')^{-1} = g(g'xg'^{-1})g^{-1} = C_g(x) \circ C_{g'}(x)$. Thus, we know that $\phi(gg') = C_{gg'} = C_g \circ C_{g'} = \phi(g) \circ \phi(g')$, hence ϕ is a homomorphism. The image is $inn(G)$ by definition. □

Examples of using this tool follow:

Exercise 1.12: Tool 12

1. Prove that the map $A \mapsto (A^T)^{-1}$ is an automorphism of $GL(n, \mathbb{R})$.
2. Prove that the set of automorphisms is a group.
3. Prove that for any fixed $k \in \mathbb{Q}^+$, the map $q \mapsto kq$ for all $q \in \mathbb{Q}$ is an outer automorphism on $\mathbb{Q}$ for $k \neq 1$.

Further exercises can be found on Dummit and Foote Exercise 1.6 and Artin Exercise 2.6.

Tool 13: Group Action: Does this act?

Concepts of this tool are provided below.

Definition 1.15: Group Action

An action of a group G on a set A is a map $G \times A \to A$ such that $(g, a) \mapsto g \cdot a \in A$, where $(gh)a = g(ha)$ for all $g, h \in G, a \in A$ and $ea = a$ for all $a \in A$.

Example 1.3: G Acting on itself

1. Consider the action $(g, x) \mapsto gx$ for all $g \in G, x \in G$, this is an action of G on itself. The proof is simple, hence left as exercise (see solution file). We call this action the "left translation" or "left regular action" of G.
2. Consider the map $(g, x) \mapsto xg$, this is not an action. The map $(g, x) \mapsto xg^{-1}$ is an action. Both of this can be shown easily, hence left as exercise (see solution file). We call the second action the "right translation" or "right regular action" of G.
3. The map $(g, x) \mapsto gxg^{-1}$ is an action of G on itself, since $(gh)x = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g(hx)$ for all $x, g, h \in G$ and $ex = exe^{-1} = x$ for all $x \in G$. This action is called conjugation.

Theorem 1.12: Permutation Representation of Actions

Suppose group G acts on a finite set A. Fix a g and consider the map $\sigma_g : a \mapsto ga$ for all $a \in A$, then this is a permutation on A. Furthermore, the map from G to S_A: $g \mapsto \sigma_g$ is a homomorphism. In fact, if we have a homomorphism $\phi : G \to S_A$, we can define $ga = \phi(g)(a)$, and in this case G acts on A. The homomorphism between G and S_A is called the permutation representation associated with the action on A.

Proof. Firstly, consider $\sigma_{g^{-1}}$, then we know that $\sigma_{g^{-1}}(a) = g^{-1}a$, hence $\sigma_g \circ \sigma_{g^{-1}} = id$, therefore, σ_g has an inverse, which means that it is bijective. Besides, we know that $\sigma_g : A \to A$, hence it is a permutation on A. Also, given $g, g' \in G$, we have that $(\sigma_{g'} \circ \sigma_g)(a) = g'ga = \sigma_{g'g}(a)$, hence we know that the map from G to S_A: $g \mapsto \sigma_g$ is a homomorphism.
Next, given the homomorphism $\phi : G \to S_A$, we know that $(gh)a = \phi(gh)(a) = \phi(g)\phi(h)(a) = \phi(g)(ha) = g(ha)$ for all $g, h \in G, a \in A$. Besides, $ea = \phi(e)(a) = id(a) = a$, hence in this case $ga = \phi(g)(a)$ is an action of G on A. □

Examples of using this tool follow:

Exercise 1.13: Tool 13

1. Given a vector space V over a field F, prove that F acts on V by scalar multiplication.
2. Show that $\mathbb{Z}^+$ acts on itself by $z \cdot a = z + a$.
3. Prove that the kernel of the action of group G on set A set of $a \in A$ such that there exists $g \in G$ where $ga = a$ is the same as the kernel of the corresponding permutation representation.
4. Show that the group of rigid motions of a tetrahedron is isomorphic to a group inside of S_4.
5. Show that group multiplication is a self-action of any group G.

Further exercises can be found on Dummit and Foote Exercise 1.7.

Tool 14: Orbits, Stablizer and Centralizer

Concepts of this tool closely follow from Tool 13, with new concepts follow:

Definition 1.16: Orbit

If a group G acts on a set A, for each $a \in A$, the orbit of a is $\{ga : g \in G\}$, denoted $G \cdot a$.

Definition 1.17: Stablizer

If a group G acts on a set A, for each $a \in A$, the stablizer of a is $\{g \in G : ga = a\}$, denoted $Stab_G(a)$.

Definition 1.18: Centralizer and Center

If a group G acts on a set $A \subset G$, the centralizer of A is $C_G(A) = \{g \in G : ga = ag \forall a \in A\}$. The self-action group multiplication's centralizer is called the center of the group, i.e. $C_G(G)$, denoted $Z(G)$.

Theorem 1.13: Properties of Centralizer and Center

1. If G is abelian, for any $A \subset G$, we get $C_G(A) = G$, in particular $Z(G) = G$.
2. $C_G(A)$ is a group for any $A \subset G$.

Proof. 1. Since G is abelian, $ga = ag$ for all $a \in A, g \in G$ by definition. Hence, $C_G(A) = G$, in particular $Z(G) = G$.
2. Let $A \subset G$ be any set. First of all, since $ea = a = ae$, we know that $e \in C_G(A)$, next if $g, g' \in C_G(A)$, we know that $ga = ag, g'a = ag'$, thus $gg'a = gag' = agg'$, thus $gg' \in C_G(A)$. Similarly, $g^{-1}a = (a^{-1}g)^{-1} = (ga^{-1})^{-1} = ag^{-1}$, thus $g^{-1} \in C_G(A)$. Associative laws follow from group operation of G, hence we know that $C_G(A)$ is a group for any $A \subset G$. □

Examples of this tool follow:

Exercise 1.14: Tool 14

1. Compute the center of D_{2n} for any odd n.
2. Let $G = SO(2)$ which are matrices in $O(2)$ with determinant equal to 1. This is the group of "rotations" in 2D. Prove that this group acts on S^3, the unit sphere in $\mathbb{R}^3$ by rotation on the x-y plane, fixing z-axis. Compute the orbit of any $s \in S$. For $s \neq N, S$ where N, S is the north and south poles of S^3, what is the stablizer of x under this action?
3. Prove that $C_G(Z(G)) = G$.
4. What is the center of $GL(n, \mathbb{R})$?

Further exercises can be found on Dummit and Foote Exercise 1.7 and Artin's Algebra Exercise 2.5.

Tool 15: Subgroup or Not a Subgroup?

Some concepts used in this tool are from Tool 9 and Tool 14. Other concepts of this tool are the following:

Definition 1.19: Subgroup

Given a group G, $H \subset G$ is a subgroup of G if H is a group with the same operation defined for G, i.e for all $h, k \in H$, $hk \in H, h^{-1} \in H$. e is automatically in H since $h \in H, h^{-1} \in H, hh^{-1} = e \in H$. We write $H \leq G$.

Theorem 1.14: Criterion of Subgroup

Suppose $H \subset G$, $H \neq \emptyset$ and G is a group. Then, we know that $H \leq G$ if and only if for all $h, k \in H$, $hk^{-1} \in H$.

Proof. Firstly, suppose $H \leq G$. Then we know that for all $h, k \in H$, $k^{-1} \in H$, hence $hk^{-1} \in H$.
Suppose $hk^{-1} \in H$ for all $h, k \in H$. Then, we have that $hh^{-1} = e \in H$, and thus since $e, h \in H$, $eh^{-1} = h^{-1} \in H$. Similarly, $k^{-1} \in H$, and we get $h(k^{-1^{-1}}) = hk \in H$, hence $H \leq K$. □

Definition 1.20: Generators

Given a group G, $g_1, \ldots, g_m \in G$, we denote $< g_1, \ldots, g_m >$ to be the smallest subgroup H of G containing $g_1, \ldots, g_m$. We call $g_1, \ldots, g_m$ the generators of H (not unique).

Theorem 1.15: Properties of Generators

1. Finite group has a minimum set of generators.
2. Given a group G, $| < g > | = |g|$ for all $g \in G$.

Proof. 1. We can find a procedure of finding the minimum set of generators for a finite group $G = \{g_1, \dots g_n\}$, namely we first consider $< g_1 >$. If $< g_1 > \neq G$, we add in g_2 and consider $< g_1, g_2 >$ until $< g_1, \dots, g_m > = G$. This is the set of minimum number of generators.
2. We know that $< g > = \{g, g^2, g^3, \dots, \}$. If $|g| = n < \infty$, we know that $g^n = e$, hence $< g > = \{g, g^2, \dots, g^n = e\}$ and $| < g > | = n = |g|$. If $|g| = \infty$, we know that $g, g^2, \dots$ are all different elements of G, thus $| < g > | = \infty = |g|$. □

Examples of using this tool follow:

Exercise 1.15: Tool 15

1. Prove that whether the set of complex numbers $\{a + ai : a \in \mathbb{R}\}$ is a subgroup of $\mathbb{C}$.
2. Prove that for $n \in \mathbb{Z}^+$, whether the set of rational numbers whose denominators divide n is a subgroup of $\mathbb{Q}$.
3. Prove that whether the set of reflections of D_{2n} is a subgroup or not.
4. Prove that whether the set of real numbers whose square is rational is a subgroup of $\mathbb{R}$ under addition or not.
5. Prove that given group $|G| = n$, G cannot have a subgroup H with $|H| = n - 1$.
6. Let G be an abelian group. Prove that $\{g \in G : |g| < \infty\}$ is a subgroup of G (called torsion subgroup).
7. Suppose $H \leq G, K \leq G$, then $H \cup K \leq G$ if and only if $H \subset K$ or $K \subset H$. Prove that $H \cap K \leq G$.
8. Show that $H \leq C_G(H)$ if and only if H is abelian.

Further exercises can be found on Dummit and Foote Exercise 2.1-2.2 and Artin's Algebra Exercise 2.2.

Tool 16: Cyclic Subgroups and Their Generators

Concepts of this tool closely follow from the discussion of generators of Tool 15 and the discussion of order in Tool 3. Other concepts follow:

Definition 1.21: Cyclic Groups

A group G is cyclic if it can be generated by a single element, i.e. $G =< x >$ for some $x \in G$.

Theorem 1.16: Properties of Cyclic Groups

1. Suppose G, H are cyclic groups of the same order. Then they are isomorphic.
2. For $G =< x >$, if $|x| = n < \infty$, then $G =< x^a >$ if and only if $(n, a) = 1$, if $|x| = \infty$, then $G =< x^a >$ if and only if $a = \pm 1$.
3. For a cyclic group G, every subgroup $J \leq G$ is cyclic.
4. Given a cyclic group G, suppose $|G| = | < x > | = \infty$, then for any $a, b \in \mathbb{Z}$, $a \neq b$, we have $< x^a > \neq < x^b >$.
5. Given a cyclic group G with $|G| = n < \infty$, for every $a \mid n$, there is a unique subgroup $K \leq G$ such that $|K| = a$.

Proof. 1. Consider $G =< x >, H =< y >$, since $|G| = |H|$, we know that $G = \{x, x^2, \ldots, x^n, \ldots\}$, $H = \{y, y^2, \ldots, y^n, \ldots\}$. Consider the map $\phi : G \to H$ such that $\phi(x^a) = y^a$. Clearly this is bijective since we know that $x, x^2, \ldots$, $y, y^2, \ldots$ are all distinct and $|G| = |H|$. Also since $\phi(x^a x^b) = \phi(x^{a+b}) = y^{a+b} = y^a y^b = \phi(x^a)\phi(x^b)$, thus ϕ is a homomorphism. Therefore, ϕ is an isomorphism, hence $G \cong H$.
2. We are proving two cases. Firstly, suppose $|G| = \infty$, by construction $a = 1$ works for $G =< x >$, similarly, since $G = \{x^n : n \in \mathbb{Z}\} = \{x^{-n} : n \in \mathbb{Z}\}$, we know that $G =< x^{-1} >$. Next, consider $a \neq \pm 1$, then we know that $< x^a >= \{x^{an} : n \in \mathbb{Z}\}$. However, in this case $x \notin < x^a >$ since otherwise, we have $x = x^{an}$ for some $n \in \mathbb{Z}$ and $x^{an-1} = e$, which is impossible as $|G| = \infty$, hence in this case $< x^a > \neq G$. Therefore, $G =< x^a >$ if and only if $a = \pm 1$. Suppose $|G| = n < \infty$. Suppose $G =< x^a >$ for some a, this means that $\{x^a, x^{2a}, \ldots, x^{(n-1)a}\}$ are all distinct. In particular, it means $x^{ma} = x$ for some $m \in \mathbb{Z}$, hence $n \mid ma - 1$, which suggests that $(a, n) = 1$. If $(a, n) = 1$ for some $a \in \mathbb{Z}$, we know that by Bezout's identity, we have $ma + kn = 1$, thus $yma + kyn = y$, and we know that $x^{yma+kyn} = x^y = x^{yma} \cdot x^{kyn} = x^{a(ym)}$ for all $1 \leq y \leq n$, hence we know that every $x^y = x^{ab}$ for some $b \in \mathbb{Z}$, therefore, $G \subset < x^a >$. However, we also have $< x^a > \subset G$, hence $G =< x^a >$ in this case.
3. Given a cyclic group $G =< x >$, consider $J \leq G$. Suppose $J = \{x^{m_1}, x^{m_2}, \ldots\}$ such that $m_1 < m_2 < \ldots$. Let $a = m_1$. Suppose $x^b \in J, a < b$. Let $d = (a, b)$. Firstly by Bezout's identity, we know that $ka + qb = d$, hence we have $x^{ka} \cdot x^{qb} = x^d$, $x^d \in J$. However $d \leq a$, hence we know that $d = a$ as we have ordered elements in J. Therefore, for all $b > a$, $(a, b) = a$, we have shown that $J =< x^a >$, which is cyclic.
4. Suppose by contradiction that for some $a, b \in \mathbb{Z}$, $a \neq b$, but $< x^a >=< x^b >$. Hence, we know that $x^b = x^{an} = x^{an}$, thus $x^{an-b} = e$, hence $|x| = an - b$, however this means that $| < x > | = |x| = an - b < \infty$, which gives us a contradiction.
5. Firstly, we know that $K \leq G$, so K is cyclic, $K =< x^m >$ for some $m \in \mathbb{Z}$ and such that m is the smallest power of x that generates K. Thus, we have $\{x^m, x^{2m}, \ldots, x^{(a-1)m}\}$ since $|K| = a$. What we left to prove is

that m is unique. We know that $x^{am} = e$, hence $n \mid am$, $\frac{n}{a} \mid m$. Let $k = \frac{n}{a}$. Hence, we know that $< x^m > \subset < x^k >$. However, we also have $| < x^m > | = | < x^k > | = a$, which means that $< x^m > = < x^k >$, but since $m \geq k$ and m is the smallest power of x that generates K, we know that $m = k$. Therefore, we have shown the uniqueness of K.

□

Examples of using this tool follow:

Exercise 1.16: Tool 16

1. Find all subgroups of $Z_{45} = < x >$ and give a generator for each.
2. Find all generators of $\mathbb{Z}/202\mathbb{Z}$.
3. Find all cyclic groups of D_8, and find a proper subgroup of D_8 that is not cyclic.
4. Let $Z_{36} = < x >$. For which integers does the isomorphism $\phi_a : 1 \mapsto x^a$ extend to a well defined homomorphism from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{36}? Can it be surjective?
5. Show that if H is any group and h is an element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.
6. Let Z_n be a cyclic group of order n. For each integer $a \in Z_n$, define $\sigma_a : x \mapsto x^a$ for all $x \in Z_n$. Prove that σ_a is an automorphism of Z_n if and only if $(a, n) = 1$. Prove that every automorphism of Z_n is equal to some σ_a.
7. Prove that above $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that $a \mapsto \sigma_a$ is an isomorphism from $(\mathbb{Z}/n\mathbb{Z})^\times$ to $Aut(Z_n)$, where Aut is the automorphism group.
8. Describe all groups G that contain no proper subgroup.

Further exercises can be found on Dummit and Foote Exercise 2.3 and Artin's Algebra Exercise 2.4.

Tool 17: Cyclic or Not Cyclic?

Concepts of this tool closely follow from Tool 16.
Examples of using this tool follow:

Exercise 1.17: Tool 17

1. Prove that $Z_2 \times Z_2$, $\mathbb{Z} \times \mathbb{Z}$ are not cyclic.
2. Prove that $\mathbb{Z} \times Z_2$ is not isomorphic to $\mathbb{Z}$.
3. Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.
4. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for $n \geq 3$.

Further exercises can be found on Dummit and Foote Exercise 2.3.

Tool 18: Understanding Groups from Generators

Concepts of this tool mainly follow Tool 15 about generators. There is still one more thing to note:

Definition 1.22: Groups generated by set

We define $< S >$ be the group generated by set S, namely considering all elements of S as generators and $< S >$ is the group generated. G is finitely generated is $G =< S >$ for some finite S.

Examples of using this tool follow:

Exercise 1.18: Tool 18

1. Prove that if H is a subgroup of G, then $< H >=< H - \{1\} >= H$.
2. Prove that $S_4 =< (1234), (1243) >$.
3. Prove that $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\}$.
4. Prove that although $|SL_2(\mathbb{F}_3)| = |S_4| = 24$, they are not isomorphic.
5. Prove that $\mathbb{Q}$ is not finitely generated.

Further exercises can be found on Dummit and Foote Exercise 2.4.

Tool 19: Normal Subgroups

The concepts used in this tool follow:

Definition 1.23: Normal Subgroups

Given a group G, a subgroup $H \leq G$ is called normal if $ghg^{-1} \in H$ for all $g \in G, h \in H$. This can also be noted as $gHg^{-1} = H$, i.e. $gH = Hg$. The notation for H being a normal subgroup is $H \trianglelefteq G$.

Definition 1.24: Normalizer

Let $N \leq G$ be a subgroup of the group G. We define the normalizer of N in G (denoted $N_G(N)$) to be the set that $\{g \in G : gng^{-1} \in N$ for all $n \in N$. $\}$.

Theorem 1.17: Kernel of Homomorphism is Normal

Given a homomorphism $\phi : G \to H$ where G, H are groups. Then, $Ker(\phi) \trianglelefteq G$.

Proof. Suppose $x \in Ker(\phi)$, $g \in G$. We are trying to show that $gxg^{-1} \in Ker(\phi)$. We know that $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)e\phi(g^{-1}) = \phi(gg^{-1}) = e$, thus $gxg^{-1} \in Ker(\phi)$, and we are done. □

Examples of using this tool follow:

Exercise 1.19: Tool 19

1. Suppose $\phi : G \to H$ is a homomorphism, $K \trianglelefteq H$. Show that $\phi^{-1}(K) \trianglelefteq G$.
2. Prove that given group G, if $N \trianglelefteq G$ and $H \leq G$, then $N \cap H \trianglelefteq H$.
3. Let N be a finite subgroup of G. Show that $gNg^{-1} \subset N$ if and only if $gNg^{-1} = N$.
4. Let $N \leq G$ and $g \in G$, where G is a group. Prove that $gN = Ng$ if and only if $g \in N_G(N)$.
5. Prove that $SL_n(F) \trianglelefteq GL_n(F)$.
6. Let G be a group. Prove that $N =< x^{-1}y^{-1}xy : x, y \in G >$ is normal in G. N is called the "commutator" of G.
7. Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $xy = yx$ for all $x \in H, y \in K$.

Further exercises can be found on Dummit and Foote Exercises 3.1.

Tool 20: Cosets and Lagrange

Definition 1.25: Cosets

A coset is a set of the form $Hg = \{hg : h \in H\}$ for fixed $g \in G$, $H \leq G$. This is called the "right cosets" of H, we can define similarly for the "left cosets".

Theorem 1.18: Different cosets do not intersect

If two cosets Hg, Hg' intersect, then they are the same.

Proof. Suppose $Hg \cap Hg' \neq \emptyset$. Assume $hg = h'g'$. Then, we know that $g = h^{-1}h'g'$, hence $g \in Hg'$. Therefore, $Hg \subset Hg'$. Similarly, we know that $g' = h'^{-1}hg$, hence $g' \in Hg$, and we have $Hg' \subset Hg$, hence $Hg = Hg'$. □

Theorem 1.19: Coset Cardinality

Given $H \leq G$, we have $|Hg| = |H|$ for all $g \in G$.

Proof. Suppose $h_1 g = h_2 g$, then we know that $h_1 = h_2$ by cancellation law. Hence, we know that $hg, h'g$ is different as long as $h \neq h'$. Therefore, $|Hg| = |H|$. □

Theorem 1.20: Lagrange Theorem

Given group G and $H \leq G$, the right cosets of H partition G, i.e. $G = \cup Hg_i$, where g_i are the representatives of each coset. Hence, if $|G| < \infty$, then $|H| \mid |G|$. We denote $[G : H] = \frac{|G|}{|H|}$, called the "index" of H in G. We finally get $|G| = [G : H] \cdot |H|$.

Proof. Firstly, by previous theorems, we know that different cosets do not intersect and both have cardinality of $|H|$. We know that G is the disjoint union of different Hg_i's, where each of them have the cardinality of $|H|$. Therefore, $|H| \mid |G|$, and $|G| = [G : H] \cdot |H|$. □

Theorem 1.21: Abelian G has same left and right cosets

Suppose G is an abelian group, then given $H \leq G$, $gH = Hg$.

Proof. The proof of this theorem is very straight-forward, hence left as an exercise with solutions in solution file. □

Examples of using this tool follow:

Exercise 1.20: Tool 20

1. Suppose that $[G : H] = 2$, prove that $H \trianglelefteq G$. Show by example that $[G : H] = 3$ by H is not a normal subgroup of G.
2. If $|G| = 13$, find all subgroups $H \leq G$.
3. Does every group whose order is a power of prime p contain an element of order p?
4. Does a group of order 35 contain an element of order 5 and another element of order 7?
5. Prove that if H and K are finite subgroups of G whose orders are relatively prime, then $H \cap K = 1$.
6. Suppose H, K are subgroups of finite index in a possibly infinite group G, where $[G : H] = m$, $[G : K] = n$. Prove that $lcm(m, n) \leq [G : H \cap K] \leq mn$. Deduce that if m, n are relatively prime then $[G : H \cap K] = [G : H][G : K]$.
7. Let $H \leq G$. Define the map $x \mapsto x^{-1}$ for all $g \in G$. Prove that this map sends every left coset of H to a right coset of H, and gives a bijection between left and right cosets.
8. Let G be a finite group and suppose $H \leq G$, $N \trianglelefteq G$. Prove that if $|H|$ and $|N|$ are relatively prime then $H \leq N$.
9. Use Lagrange's Theorem in the multiplicative group $\mathbb{Z}/n\mathbb{Z}$ to prove Euler's Theorem that $a^{\phi(n)} \equiv 1 \mod n$ for all a relatively prime to n, where ϕ denotes the Euler totient function.

Dummit and Foote Exercise 3.2 and Artin's Algebra Exercise 2.8.