Contents

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 $\operatorname{inv} : G \to G$ 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 $\mathbb{Z}/6\mathbb{Z}\backslash\{0\}$.
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 $\phi(gg') = \phi(g)\phi(g')$.

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 $g \in G$.

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, 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.

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