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 $\text{inv} : G \to G$ 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 $\mathbb{Z}/6\mathbb{Z}$.
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 $s, t \in \mathbb{N}$.
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}. 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.