# Contents

# Abstract Algebra Toolbox Solution File

Howard Xiao

## 1 Groups

### Tool 1: Group Operation Checking

**Solution 1.1: Exercise 1.1**

1. Since $[(a_1, b_1) \star (a_2, b_2)] \star (a_3, b_3) = (a_1b_2 + b_1a_2, b_1b_2) \star (a_3, b_3) = (a_1b_2b_3 + b_1a_2b_3 + a_3b_1b_2, b_1b_2b_3)$, and $(a_1, b_1) \star [(a_2, b_2) \star (a_3, b_3)] = (a_1, b_1) \star (a_2b_3 + a_3b_2, b_2b_3) = (a_1b_2b_3 + a_2b_1b_3 + a_3b_1b_2, b_1b_2b_3)$, we know that $\star$ is associative.
2. Since $(a \star b) \star c = \frac{a}{b} \star c = \frac{a}{bc}$, and $a \star (b \star c) = a \star \frac{b}{c} = \frac{ac}{b} \neq \frac{a}{bc}$, we know that $\star$ is not associative.
3. From 1., we know that $(a_1, b_1) \star (a_2, b_2) = (a_1b_2 + b_1a_2, b_1b_2)$, and $(a_2, b_2) \star (a_1, b_1) = (a_1b_2 + b_1a_2, b_1b_2)$, hence $\star$ is commutative.
4. It is commutative, since $a \star b = \frac{a+b}{5} = \frac{b+a}{5} = b \star a$ for all $a, b \in \mathbb{Q}$.
5. Consider three residue classes $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$, then we know that $([a]+[b])+[c] = [a+b+c] = [a]+([b]+[c])$, hence addition is associative. Also, since $[a] + [b] = [a + b] = [b + a] = [b] + [a]$, we know that addition is also commutative.
6. Since $(ab)c = ac = a$ and $a(bc) = ab = a$, we know that this operation is associative. Since $ab = a \neq ba = b$, we know that it is not commutative.

## Tool 2: Group or Not a Group?

**Solution 1.2: Exercise 1.2**

1. Since $e \cdot e = e$, we know that $e^{-1} = e$, $e$ is invertible. Thus, $e \in S$. Also, for any invertible elements $a, b \in G$, $(ab) \star (b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e$, we know that $ab$ is invertible. Therefore, $S$ is closed under $\star$. Since $\star$ is associative on $G$, it is also associative for $S$. Finally, for any invertible $a \in G$, we know that $a^{-1} \star a = e$, hence $a^{-1}$ is also invertible.
2. For all $n > 1$, there is no multiplicative inverse for $0 \in \mathbb{Z}/n\mathbb{Z}$, hence $\mathbb{Z}/n\mathbb{Z}$ is not a group.
3.
(a) Not a group, since $\frac{1}{2} + \frac{1}{2} = 1$ which has absolute value equal to 1, hence this set is not closed under addition.
(b) Is a group, since addition in rational numbers is associative. The additive inverses of any rational number with denominator either 1 or 2 is another rational number with denominator either 1 or 2. Adding two rational numbers with denominator 1 or 2 results in another one with denominator 1 or 2. 0 can be think of $0 = \frac{0}{1}$, which is the identity element in this group.
(c) This is a group. Consider any two rational numbers $\frac{p_1}{q_1}, \frac{p_2}{q_2}$ in lowest terms such that $q_1, q_2$ are odd. Then, $\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1q_2+p_2q_1}{q_1q_2}$, which is a rational number with odd denominator, hence after reducing to lowest term, it still has odd denominator. Therefore, the set is closed under addition. Since the additive inverse of a rational with odd denominator is still a rational with odd denominator, and $0 = \frac{0}{1}$ has odd demonimator as above, also since addition is associative for $\mathbb{Q}$, we know that this set is a group.
4. Since given $0 \leq x, y < 1$, we know that $0 \leq x \star y < 1$, hence $G$ is closed under $\star$. Next, since $x \star (1-x) = 1 - \lfloor 1 \rfloor = 0$, we know that $x^{-1} = 1-x$ for all $x \in G$, thus inverse exists for all $x \in G$ under $\star$. Then, for $x = 0$, $0 \star y = y - \lfloor y \rfloor = y - 0 = y$ for all $y \in G$, thus 0 is the identity element for operation $\star$. Finally, since $(x \star y) \star z = (x+y-\lfloor x+y \rfloor) \star z = (x+y-\lfloor x+y \rfloor)+z-\lfloor (x+y-\lfloor x+y \rfloor)+z \rfloor = x+y+z-\lfloor x+y+z \rfloor$ and $x \star (y \star z) = x \star (y+z-\lfloor y+z \rfloor) = x+(y+z-\lfloor y+z \rfloor)-\lfloor x+(y+z-\lfloor y+z \rfloor) \rfloor = x+y+z-\lfloor x+y+z \rfloor$, we know that $\star$ is associative. Therefore $G$ is a group. Finally, since $x \star y = x+y-\lfloor x+y \rfloor = y+x-\lfloor y+x \rfloor = y \star x$, $G$ is an abelian group.
5. Suppose $A \times B$ is an abelian group. Then, we know that $(a_1, b_1) \star (a_2, b_2) = (a_1 \star a_2, b_1 \star' b_2) = (a_2, b_2) \star (a_1, b_1) = (a_2 \star a_1, b_2 \star' b_1)$, hence $a_1 \star a_2 = a_2 \star a_1$ for all $a_1, a_2 \in A$, and $b_1 \star' b_2 = b_2 \star' b_1$ for all $b_1, b_2 \in B$, thus $A, B$ are both abelian.
If $A, B$ are both abelian, consider any $(a_1, b_1), (a_2, b_2) \in A \times B$, we know that $(a_1, b_1) \star (a_2, b_2) = (a_1 \star a_2, b_1 \star' b_2) = (a_2, b_2) \star (a_1, b_1) = (a_2 \star a_1, b_2 \star' b_1)$, hence $A \times B$ is abelian.
Note: in the above, we use $\star$ to symbolize operation on $A$ and $A \times B$, and $\star'$ to denote operation on $B$.

## Tool 3: Order of Group Elements

**Solution 1.3: Exercise 1.3**

1. Since $1^1 = 1$, $|1| = 1$. Since $2^n = 0 \in \mathbb{Z}/6\mathbb{Z}$, $|2| = \infty$. Since $3^n = 3 \in \mathbb{Z}/6\mathbb{Z}$, $|3| = \infty$. Since $4^n = 4 \in \mathbb{Z}/6\mathbb{Z}$, $|4| = \infty$. Since $5^2 = 1 \in \mathbb{Z}/6\mathbb{Z}$, $|5| = 2$.
2. Since $x^2 = e \in G$, we know that $|x| \leq 2$. Since if $x = e$, $e^2 = e$, and in this case $x$ has order 1, $|x|$ is either 1 or 2.
3. Suppose $|x| = n$, i.e. $x^n = e$, and we know that $x^n \cdot (x^{-1})^n = e$, hence $(x^{-1})^n = e$, $|x^{-1}| \leq n$. If $|x^{-1}| = m < n$, we know that $(x^{-1})^m = e$, and since $(x^{-1})^m \cdot x^m = e$, $x^m = e$, which is impossible. Therefore, $|x^{-1}| = |x| = n$.
4. Firstly, since $x^n = x^{st} = (x^s)^t = e$, we know that $|x^s| \leq t$. Suppose $|x^s| = m < t$, then we know that $(x^s)^m = x^{sm} = e$, which is impossible since $sm < n = st$. Thus, $|x^s| = t$.
5. We simply need to show that $e, x, \ldots, x^{n-1}$ are all different to prove the claim. Suppose $x^i = x^j$ for some $0 \leq i, j \leq n-1$, suppose $i < j$. Then, we know that $x^{-i}x^i = x^{-i}x^j = x^{j-i} = e$, and we have $0 \leq j - i \leq n - 1 < n$, which is impossible.
6. Given any $a, b \in G$ where $G$ is a group, suppose $|ab| = n < \infty$. Then, we know that $(ab)^n = a(ba)^{n-1}b = e$, thus $(ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1}$. Therefore, $(ba)^n = e$, $|ba| \leq n$. Suppose $|ba| = m < n$, then we know that $(ba)^m = b(ab)^{m-1}a = e$, similarly we know that $(ab)^m = e$, which is impossible since $m < n$. Hence, $|ba| = n = |ab|$.
Suppose $|ab| = \infty$ and $|ba| = n < \infty$, then from above, we know that $(ab)^n = e$, which is impossible. Hence, in this case, $|ab| = |ba| = \infty$.
7. Firstly we know that $(a, 1) \star (1, b) = (a \star 1, 1 \star b) = (1 \star a, b \star 1) = (1, b) \star (a, 1)$, hence they commutes in $A \times B$. Then, suppose $|(a, b)| = n$, thus $(a, b)^n = [(a, 1) \star (1, b)]^n = (a, 1)^n \star (1, b)^n = (a^n, b^n) = (1, 1)$. Therefore, we know that $n$ is the smallest $n$ satisfying $a^n = 1 = b^n$. Suppose $|a| = x$ and $|b| = y$. We know that for $m = lcm(x, y)$, $a^m = b^m = 1$, hence $n \leq m = lcm(x, y)$. Suppose $n < m$, then either $x \nmid n$ or $y \nmid n$. If $x \nmid n$, we can find $n = px + r$, where $r < x$, which means $a^n = a^{px+r} = a^{xp} \cdot a^r = a^r = 1$, which is impossible since $r < x$. Similarly for the case $y \nmid n$. Thus, we have shown that $n = lcm(x, y)$.
8. Suppose $x^i = x^j$ for some $i, j \in \mathbb{N}$, and suppose $i < j$. Then, we know that $x^{j-i} = e$, which means $|x| \leq j - i < \infty$, which is impossible.
9. Suppose the operation defined for $G$ is $\star$. Then, $G$ must be closed under $\star$. Consider $a \star b$, since $a \star b = a$ or $a \star b = b$ implies $b = 1$ or $a = 1$ respectively, which both are impossible, we know that $a \star b = c$. Similarly, $b \star a = c$, $a \star c = c \star a = b$, $b \star c = c \star b = a$. Consider $a^2$ under $\star$. $a^2 \neq a$ since $a \neq 1$. If $a^2 = b$ or $a^2 = c$, we know that $a^3 \neq 1$, which is impossible since $|a| \leq 3$. Therefore, $a^2 = 1 = b^2 = c^2$. Thus, the operation $\star$ is uniquely determined and from above we know that $G$ is abelian under $\star$.

## Tool 4: Arithmetic of Group Elements

**Solution 1.4: Proof of Theorem 1.1**

1. Suppose we have $e, e'$ being identities of $G$. Then, we know that $ee' = e' = e$.
2. Suppose $g \in G$ has inverses $g^{-1}, g^{-1\prime}$. Then, we know that $g^{-1}g = e$, multiply both sides by $g^{-1\prime}$, we get $g^{-1}(gg^{-1\prime}) = g^{-1} = g^{-1\prime}$.
3. Since $g \cdot g^{-1} = e$, and by 2., we know that ${g^{-1}}^{-1} = g$.

**Solution 1.5: Proof of Theorem 1.2**

Suppose $g, x, y \in G$ for some group $G$ and $gx = gy$, then multiply by $g^{-1}$ on the left on both sides we get $x = y$. Similarly if $xg = yg$, multiply by $g^{-1}$ on the right on both sides we get $x = y$.

**Solution 1.6: Exercise 1.4**

1. Since $(a_1 \star \cdots \star a_n) \star (a_n^{-1} \star \cdots a_1^{-1}) = e$ by associativity of $\star$, by Theorem 1.1, we know that $(a_1 \star \cdots \star a_n)^{-1} = (a_n^{-1} \star \cdots a_1^{-1})$.
2. Given group $G$, $x, y \in G$. Suppose $xy = yx$, then multiply both sides on the left by $y^{-1}$, we get $y^{-1}xy = x$. Multiply both sides on the left by $x^{-1}y^{-1}$, we get $x^{-1}y^{-1}xy = e$.
Suppose $y^{-1}xy = x$, multiply both sides on the left by $y$, we get $xy = yx$.
Suppose $x^{-1}y^{-1}xy = e$, multiply both sides on the left by $yx$, we get $xy = yx$.
3. Suppose $x^2 = e$ for all $x \in G$ for some group $G$. Hence, we know by Theorem 1.1 that $x = x^{-1}$ for all $x \in G$. Suppose $x, y \in G$. Then, $(xy)^2 = xyxy = e$, thus $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Therefore, $G$ is abelian.
4. If $xyz = e$, then we know that $yz = x^{-1}$ by Theorem 1.1. Hence, $yzx = x^{-1}x = e$. However $yxz$ is not always true. Pick any non-abelian group where $xy \neq yx$, then we know that $xyz \neq yxz$ by Theorem 1.2.