Solutions to Dummit and Foote's Abstract Algebra

By:

Dustin Smith

Contents

1 Introduction to Groups

1.1 Basic Axioms and Examples

Let G be a group.

1. Determine which of the following binary operations are associative:

   (a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$

   To be associative, $a \star (b \star c) = (a \star b) \star c$. Let $a, b, c \in G$. Then

$$\begin{aligned} a \star (b \star c) &= a - (b - c) \\ &= a - b + c \\ &= (a \star b) + c \\ &\neq (a - b) - c \\ &= (a \star b) \star c \end{aligned}$$

   Let $a = 1$, $b = 2$, and $c = 3$. Then $a \star (b \star c) = 2$ and $(a \star b) \star c = -4$. The binary operation is not associative.

   (b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$

   Let $a, b, c \in G$. Then

$$\begin{aligned} (a \star b) \star c &= a + b + ab + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \\ &= a + b + c + bc + ab + ac + abc \\ &= a + b + c + bc + a(b + c + bc) \\ &= a \star (b \star c) \end{aligned}$$

   Therefore, the binary operation is associative.

   (c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \frac{a+b}{5}$

   Let $a, b, c \in G$. Then

$$\begin{aligned} (a \star b) \star c &= \frac{\frac{a+b}{5} + c}{5} \\ &= \frac{a + b + 5c}{25} \\ &= \frac{b + 5c + a}{25} \\ &= \frac{\frac{b+5c}{5} + \frac{a}{5}}{5} \\ &\neq a \star (b \star c) \end{aligned}$$

   Let $a = 1$, $b = 2$, and $c = 3$. Then $(a \star b) \star c = \frac{18}{25}$ and $a \star (b \star c) = \frac{2}{5}$. The binary operation is not associative.

   (d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$.

   Let $a, b, c, d, e, f \in G$. Then

$$((a, b) \star (c, d)) \star (e, f) = (ad + bc, bd) \star (e, f)$$

$$
\begin{aligned}
&= ((ad+bc)f+bde, bdf) \\
&= (adf+bcf+bde, bdf) \\
&= (bcf+bde+adf, bdf) \\
&= (adf+b(cf+de), bdf) \\
&= (a,b) \star ((c,d) \star (e,f))
\end{aligned}
$$

The binary operation is associative.

(e) the operation $\star$ on $\mathbb{Q} \setminus \{0\}$ defined by $a \star b = \frac{a}{b}$

Let $a, b, c \in G$. Then

$$
\begin{aligned}
(a \star b) \star c &= \frac{\frac{a}{b}}{c} \\
&= \frac{a}{bc} \\
&= \frac{\frac{a}{c}}{b} \\
&\neq a \star (b \star c)
\end{aligned}
$$

Let $a = 1$, $b = 2$, and $c = 2$. Then $(a \star b) \star c = \frac{1}{6}$ and $a \star (b \star c) = \frac{3}{2}$. The binary operation is not associative.

2. Decide which of the binary operations in the preceding exercise are commutative.

(a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$

To be commutative, $a \star b = b \star a$.

$$
\begin{aligned}
a \star b &= a - b \\
&= -(b - a) \\
&= -(b \star a) \\
&\neq b \star a
\end{aligned}
$$

Let $a = 1$ and $b = 2$. Then $a \star b = -1$ and $b \star a = 1$. The binary operation is not commutative.

(b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$

$$
\begin{aligned}
a \star b &= a + b + ab \\
&= b + a + ba \\
&= b \star a
\end{aligned}
$$

The binary operation is commutative.

(c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \frac{a+b}{5}$

$$
\begin{aligned}
a \star b &= \frac{a+b}{5} \\
&= \frac{b+a}{5} \\
&= b \star a
\end{aligned}
$$

The binary operation is commutative.

(d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$.

$$
\begin{aligned}
(a,b) \star (c,d) &= (ad+bc, bd) \\
&= (cb+da, db \\
&= (c,d) \star (a,b)
\end{aligned}
$$

The binary operation is commutative.

(e) the operation $\star$ on $\mathbb{Q} \setminus \{0\}$ defined by $a \star b = \frac{a}{b}$

$$\begin{aligned} a \star b &= \frac{a}{b} \\ b \star a &= \frac{b}{a} \end{aligned}$$

Let $a = 1$ and $b = 2$. Then $a \star b = \frac{1}{2}$ and $b \star a = 2$. The binary operation is not commutative.

3. Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

Let $\bar{a}, \bar{b}, \ldots, \overline{n-1}$ be the residue classes of $\mathbb{Z}/n\mathbb{Z}$.

$$\begin{aligned} (a \star b) \star c &= (\bar{a} + \bar{b}) + \bar{c} \\ &= \overline{a+b} + \bar{c} \\ &= \overline{a+b+c} \\ &= \bar{a} + (\overline{b+c}) \\ &= \bar{a} + (\bar{b} + \bar{c}) \\ &= a \star (b \star c) \end{aligned}$$

The binary operation of addition on $\mathbb{Z}/n\mathbb{Z}$ is associative.

4. Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

Let $\bar{a}, \bar{b}, \ldots, \overline{n-1}$ be the residue classes of $\mathbb{Z}/n\mathbb{Z}$.

$$\begin{aligned} (a \star b) \star c &= (\bar{a}\bar{b})\bar{c} \\ &= \overline{abc} \\ &= \bar{a}(\bar{b}\bar{c}) \\ &= a \star (b \star c) \end{aligned}$$

5. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

For $n \geqslant 2$, the set of residue classes is $S = \{x : x \text{ belongs to one of the reside classes}, \bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. Then for any $a, b \in S$. Then $\mathbb{Z}/n\mathbb{Z}$ is closed under multiplication since $a \cdot b \equiv z \pmod n$ where z is an integer of lowest order in mod n. The identity element is one since $a \cdot 1 \equiv a \pmod n$. $\mathbb{Z}/n\mathbb{Z}$ is associative by problem 4. In order for $\mathbb{Z}/n\mathbb{Z}$ to be a group, we need to establish the existence of the inverse. We have that $0 \cdot a \equiv 0 \pmod n$ for all $a \in S$. That is, no element in the residue class of zero has an inverse. Therefore, $\mathbb{Z}/n\mathbb{Z}$ is not a group.

6. Determine which of the following sets are groups under addition:

(a) the set of all rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd

First, we need to determine if the set is closed under addition.

$$\frac{a}{2b+1} + \frac{c}{2d+1} = \frac{a(2d+1) + c(2b+1)}{(2b+1)(2d+1)}$$

The numerator is integer so the only worry is the denominator which needs to be odd. Now, $(2b+1)(2d+1) = 4bd + 2b + 2d + 1 = 2(2bd + b + d) + 1$ which is odd. Therefore, the set is closed under addition. Let e be the identity element. Then

$$\frac{a}{2b+1} + e = \frac{a}{2b+1} \Rightarrow e = 0$$

which establishes the existence of the identity element. Next, we need to show the existence of the inverse. Let x be the inverse element. Then

$$\frac{a}{2b+1} + x = e = 0 \Rightarrow x = \frac{-a}{2b+1}$$

which establishes the existence of the inverse element. Let b, d, and f be odd. That is, b, d, and f are of the form $2n+1$.

$$\begin{aligned}
(w \star y) \star z &= \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} \\
&= \frac{ad+cb}{bd} + \frac{e}{f} \\
&= \frac{(ad+cb)f + ebd}{dbf} \\
&= \frac{adf + cbf + ebd}{bdf} \\
&= \frac{adf + (cf+ed)b}{bdf} \\
&= \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) \\
&= w \star (y \star z)
\end{aligned}$$

Therefore, the set is associative, and we can say is a group under addition.

(b) the set of rational numbers in lowest terms whose denominators are even together with zero

This set is not closed under addition since $\frac{1}{6} + \frac{1}{6} = \frac{2}{3}$. Therefore, the set is not a group under addition.

(c) the set of rational numbers of absolute value < 1

This set is not closed under addition since $\frac{1}{2} + \frac{3}{4} = \left|\frac{5}{4}\right| > 1$. Therefore, the set is not a group under addition.

(d) the set of rational numbers of absolute value $\geqslant 1$ together with zero

This set is not closed under addition since $-1 + \frac{3}{2} = \left|\frac{1}{2}\right| < 1$. Therefore, the set is not group under addition.

(e) the set of rational numbers with denominators equal to 1 or 2

Let $m = \frac{a}{1}$ and $n = \frac{b}{2}$. Then $m + n = \frac{a}{1} + \frac{b}{2} = \frac{2a+b}{2}$ which has a denominator of 2 if $2a+b$ is odd. If $2a+b$ is even, then we can write it as $2r$ so $m+n = \frac{r}{1}$ which has denominator one. Therefore, the set is close under addition. Let e be the identity and t belong to the set; that is, t has denominator of one or two. Then $t + e = t$ so $e = 0$. Let x be the inverse. Then $t + x = e$ so $x = -t$. Let a, b, and c be rationals that belong to the set. Since $\mathbb{Q}$ is associative, this set is associative. Therefore, this set is a group under addition.

(f) the set of rational numbers with denominators equal to 1, 2, or 3

This set is not closed under addition since $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$. Therefore, this set is not a group under addition.

7. Let $G = \{x \in \mathbb{R} \mid 0 \leqslant x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$ (that is, $x \star y = x + y - [x + y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that $\star$ is a well defined binary operation on G and that G is an abelian group under $\star$ (called the real numbers modulo one).

We have two cases to consider for $[x + y]$. Since $x, y < 1$, we can have that

$$[x+y] = \begin{cases} 0, & x, y < 0.5 \\ 1, & \text{if either } x,\, y, \text{ or both are } > 0.5 \end{cases}$$

For $[x + y] = 0$, we have that $x, y < 0.5$ so $0 \leqslant x + y < 1$ and $x \star y \in G$. For the second case, $x + y < 2$ since $x, y < 1$. Then $x \star y = x + y - [x + y] < 2 - 1 = 1$ so $x \star y \in G$. Hence, $\star$ is well defined. Let e be the identity element. Then $x \star e = x$. Let $x \in G$. Then

$$\begin{aligned}
x \star e &= x + e - [x + e] \\
&= x + e && \text{(for } [x+e] = 0)
\end{aligned}$$

Therefore, $e = 0$.

$$= x + e - 1 \qquad \text{(for } [x+e] = 1)$$

In the second case, we would get $e = 1$ which clearly doesn't exist in G so $e = 0$ is the identity element. Let v be the inverse element in G. Then $x \star v = e = 0$.

$$\begin{aligned} x \star v &= x + v - [x+v] \\ &= x + v \qquad \text{(for } [x+v] = 0) \end{aligned}$$

Therefore, $v = -x$.

$$= x + v - 1 \qquad \text{(for } [x+v] = 1)$$

In the second case, we get that $v = 1 - x \in G$ since $x \in G$. Recall that the identity element is unique. That is, if $v = -x$, when $x = 0$, $v = 0$ and the inverse would be the identity element. Therefore, $v = 1 - x$. Let $x, y, z \in G$. Then

$$\begin{aligned} x \star (y \star z) &= x + (y \star z) - [x + (y \star z)] \\ &= x + y + z - [y+z] - [x + y + z - [y+z]] \\ &= x + y + z - [y+z] - [x+y+z] + [y+z] \qquad (1.1) \\ &= x + y + z - [x+y+z] \\ &= x + y + z - [x+y] - [x+y+z] + [x+y] \\ &= x + y + z - [x+y] - [x+y+z-[x+y]] \\ &= (x + y - [x+y]) + z - [(x+y-[x+y]) + z] \\ &= (x \star y) + z - [(x \star y) + z] \\ &= (x \star y) \star z \end{aligned}$$

Equation (1.1) occurs since if $x \in \mathbb{R}$ and $n \in \mathbb{Z}^+$, then $[x+n] = [x] + n$. Therefore, $\star$ is associative.

$$\begin{aligned} x \star y &= x + y - [x+y] \\ &= y + x - [y+x] \\ &= y \star x \end{aligned}$$

Therefore, $\star$ is commutative and G is an abelian group.

8. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

   (a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).

   Let $z_1, z_2 \in G$. Then there exist $n, m \in \mathbb{Z}^+$ such that $z_1^n = 1$ and $z_2^m = 1$. Now, take $(z_1 z_2)^{mn} = z_1^n z_2^m = 1 \cdot 1 = 1$; therefore, G is closed under multiplication. Since $1^1 = 1$, we have that $1 \in G$. With multiplication, $1 \cdot z^n = z^n$ for $z^n \in G$. Thus, $1 = e$ is the identity element in G. Since $\mathbb{C}$ is a field, multiplication is associative; hence, G is associative which we can easily show as well.

$$\begin{aligned} z_1^n (z_2 z_3)^{pq} &= z_1^n z_2^p z_3^q \\ &= (z_1^n z_2^p) z_3^q \\ &= (z_1 z_2)^{np} z_3^q \end{aligned}$$

   Let be x the inverse element. Then

$$\begin{aligned} z^n x &= e \\ x &= z^{-n} \\ z^n z^{-n} &= z^n \left(z^n\right)^{-1} \\ &= 1 \cdot 1^{-1} \\ &= 1 \end{aligned}$$

   The inverse element $x = z^{-n}$. Therefore, G is a group under multiplication; moreover, G is an abelian group since $\mathbb{C}$ is a field and multiplication is commutative in $\mathbb{C}$ so it is commutative in G.

(b) Prove that G is not a group under addition.

Let $z_1, z_2 \in G$ and $n, m \in \mathbb{Z}^+$. Then

$$z_1^n + z_2^m = 1 + 1 = 2.$$

Therefore, G is not close under addition so G cannot be a group.

9. Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

(a) Prove that G is a group under addition.

Let $a + b\sqrt{2}, c + d\sqrt{2} \in G$. Then $a + b\sqrt{2} + c + d\sqrt{2} = a + c + (b + d)\sqrt{2} \in G$ since $\mathbb{Q}$ is closed under addition so $a + c, b + d \in \mathbb{Q}$. G is associative since $\mathbb{R}$ is associate. $0 \in G$ since $0 = 0 + 0\sqrt{2}$. Let $x \in G$. Then $x + 0 = x$ so 0 is the identity element $e \in G$. For all $a, b \in \mathbb{Q}$ and $a + b\sqrt{2} \in G$, we have $-a - b\sqrt{2} \in G$ and $a + b\sqrt{2} - a - b\sqrt{2} = 0$; therefore, $-a - b\sqrt{2}$ is the inverse element in G. Hence, G is a group under addition.

(b) Prove that the nonzero elements of G are a group under multiplication. ("Rationalize the denominators" to find multiplicative inverses.)

Let $a, b, c, d \in \mathbb{Q} \setminus \{0\}$. Then $a + b\sqrt{2}, c + d\sqrt{2} \in G$.

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (bc + ad)\sqrt{2}$$

and since $ac + 2bd, bc + ad \in \mathbb{Q}$, $ac + 2bd + (bc + ad)\sqrt{2} \in G$ so G is closed under multiplication. Since $\mathbb{R}$ is associative, G is associative. $1 \in G$ since $1 = 1 + 0\sqrt{2}$. For all $a, b \in \mathbb{Q} - \{0\}$ and $a + b\sqrt{2} \in G$, $(a + b\sqrt{2})(1) = a + b\sqrt{2}$. That is, 1 is the identity element $e \in G$.

$$\begin{aligned}(a + b\sqrt{2})(x) &= e \\ x &= \frac{1}{a + b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\end{aligned}$$

The inverse element is $\frac{1}{a + b\sqrt{2}} \in G$ since $\frac{a}{a^2 - 2b^2}, \frac{-b}{a^2 - 2b^2} \in \mathbb{Q}$ and $a^2 - 2b^2 = 0 \notin \mathbb{Q}$ since $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

10. Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

We have to prove two statements.

(a) If a finite group is abelian, then its group table is a symmetric matrix.

Let G be a finite group with $|G| = n$ and $g_i, g_j \in G$ for $i \neq j$. The group table is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.

$$\begin{bmatrix} g_1g_1 & g_1g_2 & \cdots & g_1g_n \\ g_2g_1 & g_2g_2 & \cdots & g_2g_n \\ \vdots & & \ddots & \vdots \\ g_ng_1 & g_ng_2 & \cdots & g_ng_n \end{bmatrix}$$

Since G is abelian, $g_i g_j = g_j g_i$. A symmetric matrix is $\mathbf{A} = \mathbf{A}^\mathsf{T}$ or when $a_{ij} = a_{ji}$. Since $a_{ij} = g_i g_j = g_j g_i = a_{ji}$, the group table is symmetric. Thus, if a finite group is abelian, then its group table is symmetric.

(b) If a group table is a symmetric matrix, then its finite group is abelian.

Let $\mathbf{A}$ be the symmetric $n \times n$ group table matrix. Then $a_{ij} = a_{ji}$. Let $g_i, g_j \in G$ where $g_i g_j = a_{ij}$. Since $\mathbf{A}$ is symmetric, $a_{ij} = g_i g_j = a_{ji} = g_j g_i$. Therefore, $g_i g_j = g_j g_i$ so G is abelian. Additionally, since a symmetric matrix is finite and square, $|G| = n$. If a group table is a symmetric matrix, then its finite group is abelian.

11. Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

Let G be set congruence classes of $\mathbb{Z}/12\mathbb{Z}$. Then $G = \{\bar{0}, \bar{1}, \ldots, \overline{11}\}$. The order of $\bar{0}$ is one since $0 \equiv 0 \pmod{12}$. The order of $\bar{1}$ is twelve since $\underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{12 \text{ times}} \equiv 0 \pmod{12}$. By similar means, we have that $|\bar{2}| = 6$, $|\bar{3}| = 4$, $|\bar{4}| = 3$, $|\bar{5}| = 12$, $|\bar{6}| = 2$, $|\bar{7}| = 12$, $|\bar{8}| = 3$, $|\bar{9}| = 4$, $|\overline{10}| = 6$, and $|\overline{11}| = 12$.

12. Find the orders of each elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\bar{1}, \overline{-1}, \bar{5}, \bar{7}, \overline{-7}, \overline{13}$.

The order of $|\bar{1}| = 1$ and the order of $|\overline{-1}| = 2$. The order of the others are $|\bar{5}| = 2$, $|\bar{7}| = 2$, $|\overline{-7}| = 2$, and $|\overline{13}| = 1$.

13. Find the orders of each element of the additive group $(\mathbb{Z}/36\mathbb{Z})$: $\bar{1}, \bar{2}, \bar{6}, \bar{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

$$
\begin{aligned}
|\bar{1}| &= 36 & |\bar{2}| &= 18 \\
|\bar{6}| &= 6 & |\bar{9}| &= 4 \\
|\overline{10}| &= 18 & |\overline{12}| &= 3 \\
|\overline{-1}| &= 36 & |\overline{-10}| &= 18 \\
|\overline{-18}| &= 2
\end{aligned}
$$

14. Find the orders of the following elements of the mutliplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\bar{1}, \overline{-1}, \bar{5}, \overline{13}, \overline{-13}, \overline{17}$.

$$
\begin{aligned}
|\bar{1}| &= 1 & |\overline{-1}| &= 2 \\
|\bar{5}| &= 6 & |\overline{13}| &= 6 \\
|\overline{17}| &= 2
\end{aligned}
$$

15. Prove that $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$ for all $a_1, a_2, \ldots, a_n \in G$.

Since G is a group, $a_i a_i^{-1} = a_i^{-1} a_i = e$ where e is the identity element. Let's multiple by $(a_1 a_2 \cdots a_n)$ on the left and right hand side. Then

$$
\begin{aligned}
(a_1 a_2 \cdots a_n)(a_1 a_2 \cdots a_n)^{-1} &= (a_1 a_2 \cdots a_n) a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1} \\
e &= a_1 a_2 \cdots a_n a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1} \\
&= a_1 a_2 \cdots a_{n-1} e a_{n-1}^{-1} \cdots a_1^{-1} \\
&= e
\end{aligned}
$$

16. Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either one or two.

First, let's consider if $x^2 = 1$, then $|x|$ is either one or two. Since x^2 is the multiplicative identity element, the maximum order of x is two. However, if the order of x is one, then $1^2 = 1$. That is, the order of x can be either one or two. Now, suppose that if $|x|$ is either one or two, then $x^2 = 1$. If the of order of x is two, then $x^2 = 1$. If the of order of x is one, then $x^1 = 1$ so $x^2 = x^1 x^1 = (1)(1) = 1$. Thus, $x^2 = 1$.

17. Let x be an element of G. Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

Since $|x| = n$, $x^n = e$ where e is the identity element. Let's multiple by x^{-1} on the right and left so we have

$$x^n x^{-1} = e x^{-1} \Rightarrow x^{n-1} = x^{-1}.$$

18. Let $x, y \in G$. Prove that $xy = yx$ if and only if $y^{-1} x y = x$ if and only if $x^{-1} y^{-1} x y = 1$.

Since $x, y \in G$, we have that $x^{-1}, y^{-1} \in G$ and $y y^{-1} = y^{-1} y = e$ where e is the identity element so

$$
\begin{aligned}
xy &= yx \\
y^{-1} x y &= y^{-1} y x && \text{(mulitple by } y^{-1} \text{ on the left)} \\
y^{-1} x y &= e x \\
y^{-1} x y &= x \\
x^{-1} y^{-1} x y &= 1 && \text{(mulitple by } x^{-1} \text{ on the left)}
\end{aligned}
$$

To prove the other direction, we simply start from $x^{-1} y^{-1} x y = 1$ and work back up since $x, y \in G$.

19. Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.
   (a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.
   (b) Prove that $(x^a)^{-1} = x^{-a}$.
   (c) Establish item 19(a) for arbitary integers a and b (positive, negative or zero).

20. For x an element in G show that x and x^{-1} have the same order.

   Let $|x| = n$. Then $x^n = e$. Since $x^n \in G$, $x^{-n} \in G$. Then

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

   Therefore, $|x^{-1}| = n$.

21. Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some integer $k \geqslant 1$.

   Since n is odd, we can wrie $n = 2k - 1$ where $k \in \mathbb{Z}$. Now, $x^n = x^{2k-1} = x^{2k}x^{-1} = e$ so $x^{2k} = x$.

22. If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

   Let $|x| = n$. Then

$$\begin{aligned}
x^n &= (g^{-1}xg)^n \\
&= \underbrace{(g^{-1}xg)\cdots(g^{-1}xg)}_{n \text{ times}} \\
&= g^{-1}x^n g \\
&= g^{-1}eg \\
&= g^{-1}g \\
&= e
\end{aligned}$$

   Thus, $|g^{-1}xg| = n = |x|$. Now, suppose $|x| = \infty$ and $|g^{-1}xg| = n$. Then

$$g^{-1}x^n g = e \Rightarrow gg^{-1}x^n gg^{-1} = geg^{-1} \Rightarrow x^n = e$$

   which is a contradiction. That is, if $|x| = \infty$, then so does $|g^{-1}xg|$. From above, we have that $|ab| = |g^{-1}(ab)g|$.

$$\begin{aligned}
|ab| &= |g^{-1}(ab)g| && (\text{Let } g = b^{-1}a) \\
&= |ba^{-1}(ab)b^{-1}a| \\
&= |ba|
\end{aligned}$$

23. Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t, prove that $|x^s| = t$.

   Since the order of x is n, we have

$$\begin{aligned}
x^n &= x^{st} \\
&= (x^s)^t \\
|x^s| &= t && (\text{since } x^n = (x^s)^t = e)
\end{aligned}$$

24. If a and b are *commuting* elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. (Do this by induction for positive n first.)

   Since a and b commute, $ab = ba$. Let $n = 1$. Then $(ab)^1 = ab$. Suppose this is true for $k \leqslant n$. Then $(ab)^k = a^k b^k$.

$$(ab)^k(ab) = a^k b^k ab$$

$$
\begin{aligned}
&= a^k \underbrace{b \cdots b}_{k \text{ times}} ab \\
&= a^k \ \underbrace{b \cdots b}_{k-1 \text{ times}} \ abb \\
&= \vdots \\
&= a^k bab^{k-1} b \\
&= a^k abb^k \\
&= a^{k+1} b^{k+1}
\end{aligned}
$$

By the prinicple of mathematical induction, $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}^+$. For any $n < 0$, we have

$$
\begin{aligned}
(ab)^n &= ((ab)^{-n})^{-1} \\
&= (a^{-n} b^{-n})^{-1} \\
&= a^n b^n
\end{aligned}
$$

25. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

    Since $x^2 = 1$, we have
    $$x^2 = xx = e \Rightarrow x = x^{-1}$$
    Therefore, for all $x \in G$, $x = x^{-1}$. Let $x, y \in G$. Then

    $$
    \begin{aligned}
    xy &= (xy)^{-1} \\
    &= y^{-1} x^{-1} \\
    &= yx && (\text{since } x = x^{-1})
    \end{aligned}
    $$

    Thus, G is abelian.

26. Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, that is, for all $h, k \in H$, $hk, h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset H is a called a *subgroup* of G).

    Since $h, k \in H$, $h \star k \in H$. Therefore, H is closed under the operation of star. Let e be the identity element. Then $e = hh^{-1} = h^{-1}h \in H$ where h^{-1} is the inverse. Let $h, k, m \in H$.

    $$
    \begin{aligned}
    (h \star k) \star m &= (hk) \star m \\
    &= (hk)m \\
    &= hkm \\
    &= h(km) \\
    &= h \star (km) \\
    &= h \star (k \star m)
    \end{aligned}
    $$

    Thus, H is associative under $\star$, and a subgroup since for all $h \in H$, h^{-1} exist, H is closed under star, associative, and $e \in H$.

27. Prove that if $x \in G$ then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of G (called the *cyclic subgroup* of G generated by x).

    Let H be the cyclic subgroup. Since $0 \in \mathbb{Z}$, $x^0 = 1 \in H$ so H is not empty. Let $x^n, x^m \in H$. Then $x^n x^m = x^{n+m} \in H$ so H is closed. Since G is a group and $x \in G$, $x^{-1} \in G$. Then since $x^n \in H$, we have $(x^n)^{-1} = x^{-n} \in H$ where x^{-n} is the inverse element. Now $x^n x^{-n} = x^{-n} x^n = e \in H$ where e is the identity element.

    $$
    \begin{aligned}
    (x^n x^m) x^t &= (x^{n+m}) x^t \\
    &= x^{n+m} x^t \\
    &= x^{n+m+t}
    \end{aligned}
    $$

$$= x^n(x^{m+t})$$
$$= x^n(x^m x^t)$$

Therefore, H is non empty, closed, posses both an identity and inverse elements, and is associative so H is a subgroup of G.

28. Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product (as defined in example 6). Verify all the group axioms for $A \times B$.

   (a) prove that the associative law holds: for all $(a_i, b_i) \in A \times B$, $i = 1, 2, 3$ $(a_1, b_1)\big[(a_2, b_2)(a_3, b_3)\big] = \big[(a_1, b_1)(a_2, b_2)\big](a_3, b_3)$,

$$\begin{aligned}(a_1, b_1)\big[(a_2, b_2)(a_3, b_3)\big] &= (a_1, b_1)(a_2a_3, b_2b_3)\\ &= (a_1a_2a_3, b_1b_2b_3)\\ &= ((a_1a_2)a_3, (b_1b_2)b_3)\\ &= \big[((a_1a_2), (b_1b_2))\big](a_3, b_3)\\ &= \big[(a_1, b_1)(a_2, b_2)\big](a_3, b_3)\end{aligned}$$

   (b) prove that $(1, 1)$ is the identity of $A \times B$, and

   Let $a, b \in A \times B$. Then $(a, b)(1, 1) = (a \cdot 1, b \cdot 1) = (a, b)$ and $(1, 1)(a, b) = (1 \cdot a, 1 \cdot b) = (a, b)$. Thus, $(1, 1)$ is the identity element in $A \times B$.

   (c) prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

   Let $a, b \in A \times B$. Then $(a, b)(a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (1, 1)$ and $(a^{-1}, b^{-1})(a, b) = (a^{-1}a, b^{-1}b) = (1, 1)$. Thus, (a^{-1}, b^{-1}) is the identity element in $A \times B$.

29. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

Suppose that $A \times B$ is abelian and let $a, b \in A$ and $\alpha, \beta \in B$. Since $A \times B$ is abelian, for all $(a, \alpha), (b, \beta) \in A \times B$, we have

$$(a, \alpha)(b, \beta) = (ab, \alpha\beta) = (b, \beta)(a, \alpha) = (ba, \beta\alpha)$$

so $(ab, \alpha\beta) = (ba, \beta\alpha)$. Since $ab = ba$ and $a, b \in A$, A is abelian since a and b commute. Similarly, B is abelian since $\alpha\beta = \beta\alpha$. Now suppose that A and B are abelian where $a, b \in A$ and $\alpha, \beta \in B$. Then $ab = ba$ and $\alpha\beta = \beta\alpha$.

$$\begin{aligned}(a, \alpha)(b, \beta) &= (ab, \alpha\beta)\\ &= (ba, \beta\alpha) && \text{(since A and B are abelian)}\\ &= (b, \beta)(a, \alpha)\end{aligned}$$

Thus, $A \times B$ is abelian.

30. Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

$$\begin{aligned}(a, 1)(1, b) &= (a \cdot 1, 1 \cdot b)\\ &= (a, b)\\ &= (1 \cdot a, b \cdot 1)\\ &= (1, b)(a, 1)\end{aligned}$$

Hence, $(a, 1)$ and $(1, b)$ commute. Let the order of $|(a, 1)| = n$, $|(1, b)| = m$, and $|(a, 1)(1, b)| = r$. Let $d = [a, b]$ where $[a, b]$ is the LCM. Since $d = [a, b]$, $d \mid a$ and $d \mid b$ or $at = d$ and $bs = d$. Then

$$\big[(a, 1)(1, b)\big]^d = (a, 1)^d(1, b)^d = (1, 1)$$

Suppose $d \neq r$. Then $r < d$ such that $d \mid r \Rightarrow rh = d$ and $(a, 1)^r(1, b)^r = (1, 1)$. Since $(a, 1)^r = (1, 1)$ and $(1, b)^r = (1, 1)$, $r \mid a$ and $r \mid b$. Thus, r is a multiple of a and b, but $r < d$ which contradicts the fact that d is LCM. Therefore, $r = d$ and the LCM is the order of (a, b).

31. Prove that any finite group G of even order contains an element of order 2. (Let $t(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G - t(G)$ has order 2.)

32. If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce $|x| \leqslant |G|$.

    Let $x \in G$ and $0 \leqslant m < r \leqslant n-1$. Suppose $x^m = x^r$. Then $x^m x^{-r} = e$ or $x^{m-r} = e$. Since $m, r \in \{0, 1, \ldots, n-1\}$ and $m < r$, $m - r < n$, thus the order of $|x| \neq n$ which is a contradicition. No two elements are of the same order so they are distinct and G has at least n elements. Therefore, $|x| \leqslant |G|$.

33. Let x be an element of finite order n in G.
    (a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.
    (b) Prove that if $n = 2k$ and $1 \leqslant i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

34. If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$ are all distinct.

35. If x is an element of finite order n in G, use the Division Algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup of G generated by x).

36. Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by exercise 32, every element has order $\leqslant 3$). Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

1.2 Dihedral Groups

In these exercises, D_{2n} has the usual presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

1. Compute the order of each of the elements in the following groups:
    (a) D_6

    The elements of D_6 are $\{1, r, r^2, s, sr, sr^2\}$. The first four elements orders are obviously $|1| = 1$, $|r| = 2$, $|r^2| = 3$, and $|s| = 2$. Now, we have that

    $$(sr)(sr) = s(rs)r = s(sr^{-1})r = s^2 = 1$$

    so $|sr| = 2$ and

    $$(sr^2)(sr^2) = s(sr^{-2})r^2 = 1$$

    so $|sr^2| = 2$ as well.

    (b) D_8

    The elements of D_8 are $\{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.

$\|1\| = 1$	$\|s\| = 2$
$\|r\| = 4$	$\|sr\| = 2$
$\|r^2\| = 2$	$\|sr^2\| = 2$
$\|r^2\| = 4$	$\|sr^3\| = 2$

    Table 1.1: Orders of the elements in D_8.

    (c) D_{10}

    The elements of D_{10} are $\{1, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$. The order of the elements in D_{10} are $|1| = 1$, $|r^i| = 5$ for $i = 1, \ldots, 4$ and $|sr^j| = 2$ for $j = 0, \ldots, 5$.

2. Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

   Since $x \in D_{2n}$, $x = s^i r^j$ where $i = 0, 1$ and $j = 0, \ldots, n$. If $i = 0$, then x is a power of r so $i = 1$.

$$rx = rsr^j = sr^{-1}r^j = sr^j r^{-1} = xr^{-1}$$

3. Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

   Let x be an element of D_{2n} which is not a power of r. Then $x = sr^m$ where $0 \leqslant m < n$.

$$(sr^m)(sr^m) = s(r^m s)r^m = s(sr^{-m})r^m = 1$$

   Thus, every element of D_{2n} which is not a power of r has order 2. Suppose that $\langle s, sr \rangle$ are generators for D_{2n} and we know that $\langle r, s \rangle$ are generators. It is obvious that $s \in \langle s, sr \rangle$. Now $s(sr) = r \in \langle s, sr \rangle$ so $\langle s, sr \rangle$ generate D_{2n}.

4. If $n = 2k$ is even and $n \geqslant 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonindentity element of D_{2n} which commutes with all elements of D_{2n}.

   Since $z = r^k \in D_{2n}$, we have that $r^k r^k = r^{2k} = (r^k)^2 = 1$ so $|z| = 2$. Let $x = s^i r^j$ where $i = 0, 1$ and $0 \leqslant j < n$. When $i = 0$, $x = r^j$.

$$xr^k = r^j r^k = r^{j+k} = r^{k+j} = r^k r^j = r^k x$$

   so r^k commutes with x when $i = 0$. Now let $i = 1$. Then $x = sr^j$. Recall that $r^k r^k = 1$ so $r^k = r^{-k}$.

$$xr^k = sr^j k^k = sr^{k+j} = sr^k r^j = r^{-k} sr^j = r^k x$$

   Thus, r^k commutes with x for $i = 0, 1$. Suppose $x = s^i r^m$ commutes with all elements of D_{2n} where $i = 0, 1$. When $i = 1$, $x = sr^m$.

$$sr^m r = sr^{m+1} \quad \text{and} \quad rsr^m = sr^{-1}r^m = sr^{m-1}$$

   so $m + 1 \equiv m - 1 \pmod{n}$ so both $m + 1$ and $m - 1$ need to be a mutliple of n.

$$2 \equiv 0 \pmod{n}$$

   but $n \geqslant 4$ so $2 \not\equiv 0 \pmod{n}$. When $i = 1$, sr^m doesn't commute with r. Now let $i = 0$. Then $x = r^m$.

$$sr^m = r^m s = r^{-m} s$$

   so $2m \equiv 0 \pmod{n}$; therefore, $m = 0$ or $2m = nt$. If $m = 0$, then $r^m = 1$ which is the identity element. Now when $2m = nt$, $0 \leqslant m < n$ so $t = 1$ and $2m = n$. Since $2m = n$, $m = k$. So $sr^k = r^{-k}s = r^k s$. Thus, the only elements that commute in D_{2n} are the identity and r^k.

5. If n is odd and $n \geqslant 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}.

   From item 4, we know that for $s^i r^m$ must statisfy $2m \equiv 0 \pmod{n}$ for $n \geqslant 3$. Therefore, $m = 0$ or $2m = nt$ so again $t = 1$ since $0 \leqslant m < n$.

$$2m = n = 2p + 1$$

   which is a contradiction since $2m$ is even and $2p + 1$ is odd for $p \in \mathbb{Z}$. Thus, the only element that commutes is the identity element.

6. Let x and y be elements of order two in and group G. Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, t satisfy the same relations on G as s, r do in D_{2n}).

   Since $|x| = |y| = 2$, we have that $x = x^{-1}$ and $y = y^{-1}$.

$$tx = xyx = xy^{-1}x^{-1} = xt^{-1}$$

7. Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1\rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order two computed in item 3. (Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and b follow from those for r and s.)

   Since $a = s$ and $b = sr$, we have that $a^2 = s^2 = 1$ and $b^2 = (sr)(sr) = 1$, respectively. Now $ab = ssr = r$ so $(ab)^n = r^n = 1$.

   $$r(sr) = abb = ab^2 = a = s \Rightarrow rsr = s \Rightarrow rs = sr^{-1}$$

   Now $b^2 = (sr)(sr) = s(rs)ss(sr^{-1})r = 1$.

8. Find the order of the cyclic subgroup D_{2n} generated by r.

   The order of r in D_{2n} is $|r| = n$ so $\langle r\rangle = \{1, r, r^2, \ldots, r^{n-1}\}$. Then $|\langle r\rangle| = n$.

In each of the exercise 9 to 13, you can find the order of the group of rigid motions in $\mathbb{R}^3$ (also called the group of rotations) of the given Platonic solid by following the proof for the order of D_{2n}: find the number of positions to which an adjacent pair of vertices can be sent. Alternatively, you can find the number of places to which a given face may be sent and, once a face is fixed, the number of positions which a vertex on that face may be sent.

9. Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

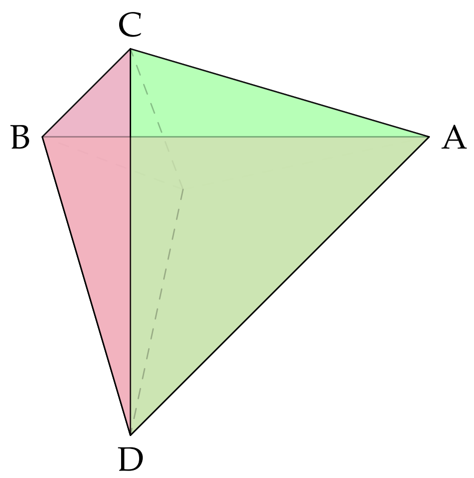

Figure 1.1: Tetrahedron

   Let's consider the point A. Then A has four possible places it can be sent which includes the original location of A. Once A is determined, B has three possibilities. With A and B determined, C and D are determined. Therefore, the order of G is $|G| = 4 \cdot 3 = 12$.

10. Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.

    With a cube, let vertices $1, 2, 3, 4$ be in plane. Then vertice 1 has eight possible moves. Since 2 is in plane with one, it has only three possible moves. Once vertice 1 and 2 are determine, the other vertices are determined. The order G is $|G| = 8 \cdot 3 = 24$.

11. Let G be the group of rigid motions in $\mathbb{R}^3$ of a octahedron. Show that $|G| = 24$.

    An octahedron has 6 points and 8 faces. Let vertices $1, 2, 3$ be in plane. Vertice 1 can be sent to six locations. Once 1 is determine, 2 has four possible locations. With 1 and 2 determined, the other vertices are determined. Thus, the order of G is $|G| = 6\dot{4} = 24$.

12. Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.

    A dodecahedron has 12 faces and 20 vertices. Let vertices $1, 2, 3, 4, 5$ be in plane. Vertice 1 can be sent to 20 locations. Vertice 2 can be set to three locations. After 2 is determined along with one, the other vertices are determined. Then the order of G is $|G| = 20 \cdot 3 = 60$.

13. Let G be the group of rigid motions in $\mathbb{R}^3$ of a icosahedron. Show that $|G| = 60$.

14. Find a set of generators for $\mathbb{Z}$.

    Every integer can be generated by repeated addition of ± 1. Therefore, $\mathbb{Z} = \langle 1 \rangle$.

15. Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.

    The elements of $\mathbb{Z}/n\mathbb{Z}$ are the classes $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ which are mutliplies of $\bar{1}$. The generator and relation is $\mathbb{Z}/n\mathbb{Z} = \langle z \mid z^n = 1 \rangle$.

16. Show that the group $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1y_1)^2 = 1 \rangle$ is the diheral group D_4 (where x_1 may be replaced by the letter r and y_1 by the letter s). [Show that the last relation is the same as: $x_1y_1 = y_1x_1^{-1}$.]

    In D_4, the order of r is two. We have that $x_1^2 = r^2 = 1$ and $y_1^2 = s^2 = 1$.

$$\begin{aligned}
(x_1y_1)^2 &= rsrs &&= 1 \\
&= (rsrs)s &&= s \\
&= (rsr)r^{-1} &&= sr^{-1} \\
&= rs &&= sr^{-1} \\
&= x_1y_1 &&= y_1x_1^{-1}
\end{aligned}$$

17. Let X_{2n} be the group whose presentation is

$$X_{2n} = \langle x, y \mid x^n = y^2 = 1, xy = yx^2 \rangle.$$

   (a) Show that if $n = 3k$, then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s.

   We can wrtie x as
$$xy^2 = xyy = yx^2y = yyx^4 \Rightarrow x = x^4 \Rightarrow x^3 = 1$$
   Therefore, the order of x is three. Now $x^n = r^{3k} = (r^3)^k = 1^k = 1$ and $y^2 = s^2 = 1$. The distinct elements of $X_{2n} = \{1, x, x^2, y, yx, yx^2\}$ so the $|X_{2n}| = 6$. When x and y are replaced by r and s, we obtain the same generators as D_6.

   (b) Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case, deduce that X_{2n} has order 2. [Use the fact that $x^n = 1$ and $x^3 = 1$.]

18. Let Y be the group whose presentation is

$$Y = \langle u, v \mid u^4 = v^3 = 1, uv = v^2u^2 \rangle.$$

   (a) Show that $v^2 = v^{-1}$. [Use the relation $v^3 = 1$.]

   (b) Show that v commutes with u^3. [Show that $v^2u^3v = u^3$ by writing the left hand side as $(v^2u^2)(uv)$ and using the relations to reduce this to the right hand side. Then use item 18(a).]

   (c) Show that v commutes with u. [Show that $u^9 = u$ and then use item 18(b).]

   (d) Show that $uv = 1$. [Use item 18(c) and the last relation.]

   (e) Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$. [Use item 18(d) and the equation $u^4v^3 = 1$.]