Solutions to Exercises from
"A Book of Abstract Algebra" by Charles C. Pinter

Eric Bailey

Contents

CHAPTER 2

Operations

A. Examples of Operations

1 $a * b = \sqrt{|ab|}$ is not an operation on $\mathbb{Q}$, because $2 * 1 = \sqrt{|2|}$, but $\sqrt{|2|} \notin \mathbb{Q}$.

2 $a * b = a \ln b$ is not an operation on $\mathbb{R}_{>0}$, because $\forall a, b \in \mathbb{R}_{>0}(b \leq 1 \to a \ln b \notin \mathbb{R}_{>0})$

3 If $a * b$ is a root of the equation $x^2 - a^2b^2 = 0$, $*$ is not an operation on $\mathbb{R}$, because $\forall a, b \in \mathbb{R}(a \neq 0 \wedge b \neq 0 \to x = \pm ab)$

4 Subtraction is an operation on $\mathbb{Z}$, because $\forall a, b \in \mathbb{Z}(a - b \in \mathbb{Z})$.

5 Subtraction is not an operation on $\mathbb{Z}_{\geq 0}$, because e.g. $0 - 1 \notin \mathbb{Z}_{\geq 0}$.

6 $a * b = |a - b|$ is an operation on $\mathbb{Z}_{\geq 0}$, because $\forall a, b \in \mathbb{Z}_{\geq 0}(|a - b| \in \mathbb{Z}_{\geq 0})$.

B. Properties of Operations

1 $x * y = x + 2y + 4$

(i) $*$ is not commutative.

$$\begin{aligned} x * y &= x + 2y + 4 \\ y * x &= y + 2x + 4 \\ x * y &\neq y * x \end{aligned}$$

(ii) $*$ is not associative.

$$\begin{aligned} x * (y * z) &= x * (y + 2z + 4) \\ &= x + 2(y + 2z + 4) + 4 \\ &= x + 2y + 4z + 12 \\ (x * y) * z &= (x + 2y + 4) * z \\ &= x + 2y + 4 + 2z + 4 \\ &= x + 2y + 2z + 8 \\ x + 2y + 4z + 12 &\neq x + 2y + 2z + 8 \end{aligned}$$

(iii) $\mathbb{R}$ does not have an identity element with respect to $*$.

$$\begin{aligned} x * e &= x \\ x + 2e + 4 &= x \\ 2e + 4 &= 0 \\ e &= -2 \\ e * x &= x \\ e + 2x + 4 &= x \\ e &= -x - 4 \neq -2 \end{aligned}$$

(iv) Since there is no identity element, there can be no inverses.

2 $x * y = x + 2y - xy$

(i) $*$ is not commutative.

$$\begin{aligned} x * y &= x + 2y - xy \\ y * x &= y + 2x - yx \\ x * y &\neq y * x \end{aligned}$$

(ii) $*$ is not associative.

$$\begin{aligned} x*(y*z) &= x*(y+2z-yz) \\ &= x+2(y+2z-yz)-x(y+2z-yz) \\ &= x+2y+4z-2yz-xy-2xz+xyz \\ (x*y)*z &= (x+2y-xy)*z \\ &= (x+2y-xy)+2z-(x+2y-xy)z \\ &= x+2y+2z-2yz-xy-xz+xyz \\ x*(y*z) &\neq (x*y)*z \end{aligned}$$

(iii) $\mathbb{R}$ does not have an identity element with respect to $*$.

$$\begin{aligned} x*e &= x \\ x+2e-xe &= x \\ 2e-xe &= 0 \\ e(2-x) &= 0 \\ e &= 0 \\ e*x &= x \\ e+2x-ex &= x \\ e+x-ex &= 0 \\ e(1-x) &= -x \\ e &= -x(1-x) \neq 0 \end{aligned}$$

(iv) Since there is no identity element, there can be no inverses.

3 $x*y=|x+y|$

(i) $*$ is commutative.

$$\begin{aligned} x*y &= |x+y| \\ y*x &= |y+x| = |x+y| \\ x*y &= y*x \end{aligned}$$

(ii) $*$ is not associative.

$$\begin{aligned} x*(y*z) &= x*|y+z| = |x+|y+z|| \\ (x*y)*z &= |x+y|*z = ||x+y|+z| \\ x=0, y<0 \to x*(y*z) &= |y+z| \\ (x*y)*z &= ||y|+z| \\ y<0 \to y \neq |y| \to |y+z| &\neq ||y|+z| \\ x*(y*z) &\neq (x*y)*z \end{aligned}$$

(iii) $\mathbb{R}$ has an identity element with respect to $*$.

$$\begin{aligned} x*e &= x \\ |x+e| &= x \\ e &= 0 \\ e*x &= x \\ |e+x| &= x \\ e &= 0 \end{aligned}$$

(iv) Every $x \in \mathbb{R}$ has an inverse with respect to $*$.

$$\begin{aligned} x * x' &= 0 \\ |x + x'| &= 0 \\ x' &= -x \\ x * (-x) &= |x - x| = 0 \\ (-x) * x &= |-x + x| = 0 \\ x * x' &= x' * x \end{aligned}$$

4 $x * y = |x - y|$

(i) $*$ is commutative.

$$\begin{aligned} x * y &= |x - y| \\ y * x &= |y - x| \\ x = y \to x * y &= 0 \\ y * x &= 0 \end{aligned}$$

If $x < y$ then $x = y + k$, and:

$$\begin{aligned} &x * y = |(y + k) - y| = |k| \\ &y * x = |y - (y + k)| = |-k| = |k| \\ &x * y = y * x \end{aligned}$$

If $x = y$:

$$\begin{aligned} &x * y = |y - y| = 0 \\ &y * x = |y - y| = 0 \\ &x * y = y * x \end{aligned}$$

If $x > y$ then $y = x + k$, and:

$$\begin{aligned} &x * y = |x - (x + k)| = |-k| = |k| \\ &y * x = |(x + k) - x| = |k| \\ &x * y = y * x \end{aligned}$$

(ii) $*$ is not associative.

$$\begin{aligned} x * (y * z) &= x * |y - z| \\ &= |x - |y - z|| \\ (x * y) * z &= |x - y| * z \\ &= ||x - y| - z| \end{aligned}$$

If $x = 0$ and $y < 0$:

$$\begin{aligned} x * (y * z) = |-|y - z|| = |y - z| &= \sqrt{(y - z)^2} \\ (x * y) * z = ||-y| - z| = ||y| - z| &= \sqrt{(|y| - z)^2} \\ |y| &\neq y \\ x * (y * z) &\neq (x * y) * z \end{aligned}$$

(iii) $\mathbb{R}$ does not have an identity element with respect to $*$.

$$\begin{aligned} x * e &= x \\ |x - e| &= x \\ e &= 2x \end{aligned}$$

(iv) Since there is no identity element, there can be no inverses.

5 $x * y = xy + 1$

(i) $*$ is commutative.

$$\begin{aligned} x*y &= xy+1 \\ y*x &= yx+1 = xy+1 \\ x*y &= y*x \end{aligned}$$

(ii) $*$ is not associative.

$$\begin{aligned} x*(y*z) &= x*(yz+1) \\ &= x(yz+1)+1 = xyz+x+1 \\ (x*y)*z &= (xy+1)*z \\ &= (xy+1)z+1 = xyz+z+1 \\ x*(y*z) &\neq (x*y)*z \end{aligned}$$

(iii) $\mathbb{R}$ does not have an identity element with respect to $*$.

$$\begin{aligned} x*e &= x \\ xe+1 &= x \\ xe &= x-1 \\ x &= 1-\frac{1}{x} \end{aligned}$$

(iv) Since there is no identity element, there can be no inverses.

6 $x*y = \max\{\,x,y\,\}$ = the larger of the two numbers x and y

(i) $*$ is commutative.

$$\begin{aligned} x*y &= \max\{\,x,y\,\} \\ y*x &= \max\{\,y,x\,\} = \max\{\,x,y\,\} \\ x*y &= y*x \end{aligned}$$

(ii) $*$ is associative.

$$\begin{aligned} x*(y*z) &= x*\max\{\,y,z\,\} \\ &= \max\{\,x,\max\{\,y,z\,\}\,\} = \max\{\,x,y,z\,\} \\ (x*y)*z &= (\max\{\,x,y\,\})*z \\ &= \max\{\,\max\{\,x,y\,\},z\,\} = \max\{\,x,y,z\,\} \\ x*(y*z) &= (x*y)*z \end{aligned}$$

(iii) $\mathbb{R}$ does not have an identity element with respect to $*$.

$$\begin{aligned} x*e &= x \\ \max\{\,x,e\,\} &= x \\ e &= \{n\in\mathbb{R} : n\leq x\} \end{aligned}$$

(iv) Since there is no identity element, there can be no inverses.

7 $x*y = \frac{xy}{x+y+1}$

(i) $*$ is commutative.

$$\begin{aligned} x*y &= \frac{xy}{x+y+1} \\ y*x &= \frac{yx}{y+x+1} = \frac{xy}{x+y+1} \\ x*y &= y*x \end{aligned}$$

(ii) $*$ is associative.

$$
\begin{aligned}
x*(y*z) &= x*(\frac{yz}{y+z+1}) \\
&= \frac{\frac{xyz}{y+z+1}}{x+\frac{yz}{y+z+1}+1} \\
&= \frac{xyz}{x(y+z+1)+yz+(y+z+1)} \\
&= \frac{xyz}{xy+xz+yz+x+y+z+1} \\
(x*y)*z &= \left(\frac{xy}{x+y+1}\right)*z \\
&= \frac{\frac{xyz}{x+y+1}}{\frac{xy}{x+y+1}+z+1} \\
&= \frac{xyz}{xy+z(x+y+1)+z+(x+y+1)} \\
&= \frac{xyz}{xy+xz+yz+x+y+z+1} \\
x*(y*z) &= (x*y)*z
\end{aligned}
$$

(iii) $\mathbb{R}$ does not have an identity element with respect to $*$.

$$
\begin{aligned}
x*e &= x \\
\frac{xe}{x+e+1} &= x \\
xe &= x(x+e+1) \\
e &= e+x+1
\end{aligned}
$$

(iv) Since there is no identity element, there can be no inverses.

C. Operations on a Two-Element Set

Let A be the two-element set $A = \{\, a, b \,\}$.

TABLE 1. 0_1

(x,y)	$x*y$
1 (a,a)	a
(a,b)	a
(b,a)	a
(b,b)	a

TABLE 2. 0_2

(x,y)	$x*y$
(a,a)	a
(a,b)	a
(b,a)	a
(b,b)	b

TABLE 3. 0_3

(x,y)	$x*y$
(a,a)	a
(a,b)	a
(b,a)	b
(b,b)	a

TABLE 4. 0_4

(x,y)	$x*y$
(a,a)	a
(a,b)	a
(b,a)	b
(b,b)	b

TABLE 5. 0_5

(x,y)	$x*y$
(a,a)	a
(a,b)	b
(b,a)	a
(b,b)	a

TABLE 6. 0_6

(x,y)	$x*y$
(a,a)	a
(a,b)	b
(b,a)	a
(b,b)	b

TABLE 7. 0_7

(x,y)	$x*y$
(a,a)	a
(a,b)	b
(b,a)	b
(b,b)	a

TABLE 8. 0_8

(x,y)	$x*y$
(a,a)	a
(a,b)	b
(b,a)	b
(b,b)	b

TABLE 9. 0_9

(x,y)	$x*y$
(a,a)	b
(a,b)	a
(b,a)	a
(b,b)	a

TABLE 10. 0_{10}

(x,y)	$x*y$
(a,a)	b
(a,b)	a
(b,a)	a
(b,b)	b

TABLE 11. 0_{11}

(x,y)	$x*y$
(a,a)	b
(a,b)	a
(b,a)	b
(b,b)	a

TABLE 12. 0_1

(x,y)	$x*y$
(a,a)	b
(a,b)	a
(b,a)	b
(b,b)	b

TABLE 13. 0_{13}

(x,y)	$x*y$
(a,a)	b
(a,b)	b
(b,a)	a
(b,b)	a

TABLE 14. 0_{14}

(x,y)	$x*y$
(a,a)	b
(a,b)	b
(b,a)	a
(b,b)	b

TABLE 15. 0_{15}

(x,y)	$x*y$
(a,a)	b
(a,b)	b
(b,a)	b
(b,b)	a

TABLE 16. 0_1

(x,y)	$x*y$
(a,a)	b
(a,b)	b
(b,a)	b
(b,b)	b

2 Commutativity

- 0_1 is commutative: $a*b=a=b*a$
- 0_2 is commutative: $a*b=a=b*a$
- 0_3 is not commutative: $a*b=a\neq b=b*a$
- 0_4 is not commutative: $a*b=a\neq b=b*a$
- 0_5 is not commutative: $a*b=b\neq a=b*a$
- 0_6 is not commutative: $a*b=b\neq a=b*a$
- 0_7 is commutative: $a*b=b=b*a$
- 0_8 is commutative: $a*b=b=b*a$
- 0_9 is commutative: $a*b=a=b*a$
- 0_{10} is commutative: $a*b=a=b*a$
- 0_{11} is not commutative: $a*b=a\neq b=b*a$
- 0_{12} is not commutative: $a*b=a\neq b=b*a$
- 0_{13} is not commutative: $a*b=b\neq a=b*a$
- 0_{14} is not commutative: $a*b=b\neq a=b*a$
- 0_{15} is commutative: $a*b=b=b*a$
- 0_{16} is commutative: $a*b=b=b*a$

3 Associativity

- 0_1 is associative:

$$\forall x,y\in A(x*y=a\to x*(y*z)=x*a=a=a*z=(x*y)*z)$$

- 0_2 is associative.

$$\begin{aligned}
a*(a*a)&=a*a=(a*a)*a\\
a*(a*b)&=a*a=a*b=(a*a)*b\\
a*(b*a)&=a*a=(a*b)*a\\
a*(b*b)&=a*b=(a*b)*b\\
b*(a*a)&=b*a=a*a=(b*a)*a\\
b*(a*b)&=b*a=a*b=(b*a)*b\\
b*(b*a)&=b*a=(b*b)*a\\
b*(b*b)&=b*b=(b*b)*b
\end{aligned}$$

- 0_3 is not associative: $b*(a*b)=b*a=b\neq a=b*b=(b*a)*b$

- 0_4 is associative.

$$\begin{aligned}
a*(a*a) &= a*a = (a*a)*a\\
a*(a*b) &= a*a = a*b = (a*a)*b\\
a*(b*a) &= a*b = a*a = (a*b)*a\\
a*(b*b) &= a*b = (a*b)*b\\
b*(a*a) &= b*a = (b*a)*a\\
b*(a*b) &= b*a = b*b = (b*a)*b\\
b*(b*a) &= b*b = b*a = (b*b)*a\\
b*(b*b) &= b*b = (b*b)*b
\end{aligned}$$

- 0_5 is not associative: $b*(a*b) = b*b = a \neq b = a*b = (b*a)*b$
- 0_6 is associative.

$$\begin{aligned}
a*(a*a) &= a*a = (a*a)*a\\
a*(a*b) &= a*b = (a*a)*b\\
a*(b*a) &= a*a = b*a = (a*b)*a\\
a*(b*b) &= a*b = (a*b)*b\\
b*(a*a) &= b*a = (b*a)*a\\
b*(a*b) &= b*b = (b*a)*b\\
b*(b*a) &= b*a = (b*b)*a\\
b*(b*b) &= b*b = (b*b)*b
\end{aligned}$$

- 0_7 is associative.

$$\begin{aligned}
a*(a*a) &= a*a = (a*a)*a\\
a*(a*b) &= a*b = (a*a)*b\\
a*(b*a) &= a*b = b*a = (a*b)*a\\
a*(b*b) &= a*a = b*b = (a*b)*b\\
b*(a*a) &= b*a = (b*a)*a\\
b*(a*b) &= b*b = (b*a)*b\\
b*(b*a) &= b*b = a*a = (b*b)*a\\
b*(b*b) &= b*a = a*b = (b*b)*b
\end{aligned}$$

- 0_8 is associative.

$$\begin{aligned}
a*(a*a) &= a*a = (a*a)*a\\
a*(a*b) &= a*b = (a*a)*b\\
a*(b*a) &= a*b = b*a = (a*b)*a\\
a*(b*b) &= a*b = b*b = (a*b)*b\\
b*(a*a) &= b*a = (b*a)*a\\
b*(a*b) &= b*b = (b*a)*b\\
b*(b*a) &= b*b = b*a = (b*b)*a\\
b*(b*b) &= b*b = (b*b)*b
\end{aligned}$$

- 0_9 is not associative: $a*(a*b) = a*a = b \neq a = b*b = (a*a)*b$

- 0_{10} is associative.

$$
\begin{aligned}
a*(a*a) &= a*b = b*a = (a*a)*a \\
a*(a*b) &= a*a = b*b = (a*a)*b \\
a*(b*a) &= a*a = (a*b)*a \\
a*(b*b) &= a*b = (a*b)*b \\
b*(a*a) &= b*b = a*a = (b*a)*a \\
b*(a*b) &= b*a = a*b = (b*a)*b \\
b*(b*a) &= b*a = (b*b)*a \\
b*(b*b) &= b*b = (b*b)*b
\end{aligned}
$$

- 0_{11} is not associative: $a*(a*a) = a*b = a \neq b = b*a = (a*a)*a$
- 0_{12} is not associative: $a*(b*a) = a*b = a \neq b = a*a = (a*b)*a$
- 0_{13} is not associative: $a*(a*a) = a*b = b \neq a = b*a = (a*a)*a$
- 0_{14} is not associative: $a*(b*a) = a*a = b \neq a = b*a = (a*b)*a$
- 0_{15} is not associative: $a*(a*a) = a*b = b \neq a = b*b = (a*a)*b$
- 0_{16} is associative:

$$\forall x, y \in A(x*y = b \to x*(y*z) = x*b = b = b*z = (x*y)*z)$$

4 Identity

- A does not have an identity element with respect to 0_1.
- A has an identity element with respect to 0_2.

$$
\begin{aligned}
x*e &= x \\
a*b &= a \\
b*b &= b \\
e &= b \\
e*x &= x \\
b*a &= a \\
b*b &= b \\
e &= b
\end{aligned}
$$

- A does not have an identity element with respect to 0_3.
- A does not have an identity element with respect to 0_4.
- A does not have an identity element with respect to 0_5.
- A does not have an identity element with respect to 0_6.
- A does not have an identity element with respect to 0_7.
- A has an identity element with respect to 0_8.

$$
\begin{aligned}
x*e &= x \\
a*a &= a \\
b*a &= b \\
e &= a \\
e*x &= x \\
a*a &= a \\
a*b &= b \\
e &= a
\end{aligned}
$$

- A does not have an identity element with respect to 0_9.

- A has an identity element with respect to 0_{10}.

$$\begin{aligned} x * e &= x \\ a * b &= a \\ b * b &= b \\ e &= b \\ e * x &= x \\ b * a &= a \\ b * b &= b \\ e &= b \end{aligned}$$

- A does not have an identity element with respect to 0_{11}.
- A does not have an identity element with respect to 0_{12}.
- A does not have an identity element with respect to 0_{13}.
- A does not have an identity element with respect to 0_{14}.
- A does not have an identity element with respect to 0_{15}.
- A does not have an identity element with respect to 0_{16}.

5 Since A only has identity elements with respect to 0_2, 0_8, and 0_{10}, the rest cannot have inverses. As it turns out, with respect to those three operations, it is not the case that every $x \in A$ has an inverse.

D. Automata: The Algebra of Input/Output Sequences

Let A be an alphabet and A^* be the set of all sequences of symbols in the alphabet A. There is an operation on A^* called *concatenation*: If $\mathbf{a}$ and $\mathbf{b}$ are in A^*, say $\mathbf{a} = a_1a_2...a_n$ and $\mathbf{b} = b_1b_2...b_m$, then

$$\mathbf{ab} = a_1a_2...a_nb_1b_2...b_m$$

The symbol λ denotes the empty sequence.

1 Concatenation is associative.

$$\begin{aligned} &a(bc) = a(b_1b_2...b_mc_1c_2...c_k) = a_1a_2...a_nb_1b_2...b_mc_1c_2...c_k \\ &(ab)c = (a_1a_2...a_nb_1b_2...b_m)c = a_1a_2...a_nb_1b_2...b_mc_1c_2...c_k \\ &a(bc) = (ab)c \end{aligned}$$

2 Concatenation is not commutative.

$$\begin{aligned} &ab = a_1a_2...a_nb_1b_2...b_m \\ &ba = b_1b_2...b_ma_1a_2...a_n \\ &ab \neq ba \end{aligned}$$

3 λ is the identity element for concatenation: $x\lambda = \lambda x = x$

CHAPTER 3

The Definition of Groups

A. Examples of Abelian Groups

1 $\langle \mathbb{R}, x * y = x + y + k \rangle$

(i) $*$ is commutative: $x * y = x + y + k = y + x + k = y * x$

(ii) $*$ is associative.

$$\begin{aligned} x(yz) &= x(y + z + k) = x + y + z + 2k \\ (xy)z &= (x + y + k)z = (xy)z \\ x(yz) &= (xy)z \end{aligned}$$

(iii) $\mathbb{R}$ has an identity element with respect to $*$.

$$\begin{aligned} xe &= x \\ x + e + k &= x \\ e &= -k \\ (-k)x &= x \\ -k + x + k &= x \end{aligned}$$

(iv) $\forall x \in \mathbb{R}(\exists x' \in \mathbb{R}(x * x' = -k))$

$$\begin{aligned} xx' &= -k \\ x + x' + k &= -k \\ x' &= -x - 2k \\ x'x &= xx' \qquad \text{due to commutativity} \end{aligned}$$

2 $\langle \mathbb{R}^*, x * y = \frac{xy}{2} \rangle$

(i) $*$ is commutative: $x * y = \frac{xy}{2} = \frac{yx}{2} = y * x$

(ii) $*$ is associative.

$$\begin{aligned} x * (y * z) &= x * (\frac{yz}{2}) = \frac{xyz}{4} \\ (x * y) * z &= (\frac{xy}{2}) * z = \frac{xyz}{4} \end{aligned}$$

(iii) $\mathbb{R}^*$ has an identity element with respect to $*$.

$$\begin{aligned} x * e &= \frac{xe}{2} = \frac{ex}{2} = e * x = x \\ e &= 2 \end{aligned}$$

(iv) $\forall x \in \mathbb{R}(\exists x' \in \mathbb{R}(x * x' = 2))$

$$\begin{aligned} x * x' &= \frac{xx'}{2} = \frac{x'x}{2} = x' * x = e = 2 \\ x' &= \frac{4}{x} \end{aligned}$$

3 $\langle \{ x \in \mathbb{R} : x \neq -1 \}, x * y = x + y + xy \rangle$

(i) $*$ is commutative: $x * y = x + y + xy = y + x + yx = y * x$

(ii) $*$ is associative.

$$\begin{aligned} x * (y * z) &= x * (y + z + yz) = x + (y + z + yz) + x(y + z + yz) = x + y + z + xy + xz + yz + xyz \\ (x * y) * z &= (x + y + xy) * z = (x + y + xy) + z + (x + y + xy)z = x + y + z + xy + xz + yz + xyz \end{aligned}$$

(iii) $\{ x \in \mathbb{R} : x \neq -1 \}$ has an identity element with respect to $*$.

$$\begin{aligned} x * e = x + e + xe = e + x + ex = e * x = x \\ e(x+1) &= 0 \\ e &= 0 \end{aligned}$$

(iv) Every element of $\{ x \in \mathbb{R} : x \neq -1 \}$ has an inverse with respect to $*$.

$$\begin{aligned} x * x' = x + x' + xx' = x' + x + x'x = e = 0 \\ x'(x+1) &= -x \\ x' &= -\frac{x}{x+1} \end{aligned}$$

4 $\langle \{ x \in \mathbb{R} : -1 < x < 1 \}, x * y = \frac{x+y}{xy+1} \rangle$

(i) $*$ is commutative: $x * y = \frac{x+y}{xy+1} = \frac{y+x}{yx+1} = y * x$

(ii) $*$ is associative.

$$\begin{aligned} x * (y * z) &= x * (\frac{y+z}{yz+1}) = \frac{x + (\frac{y+z}{yz+1})}{x(\frac{y+z}{yz+1}) + 1} = \frac{xyz + x + y + z}{xy + xz + yz + 1} \\ (x * y) * z &= \frac{x+y}{xy+1} * z \quad = \frac{(\frac{x+y}{xy+1}) + z}{(\frac{x+y}{xy+1})z + 1} = \frac{x + y + z + xyz}{xy + yz + xz + 1} \end{aligned}$$

(iii) $\{ x \in \mathbb{R} : -1 < x < 1 \}$ has an identity element w.r.t. $*$.

$$\begin{aligned} x * e &= \frac{x+e}{xe+1} = x \\ x + e &= x(xe+1) \\ e &= ex^2 \\ e(1-x^2) &= 0 \\ e &= 0 \\ x * 0 &= \frac{x+0}{(x \times 0) + 1} = x = \frac{0+x}{0x+1} = 0 * x \end{aligned}$$

(iv) Every element of $\{ x \in \mathbb{R} : -1 < x < 1 \}$ has an inverse with respect to $*$.

$$\begin{aligned} x * x' &= \frac{x + x'}{xx' + 1} = 0; \quad x + x' = 0; \quad x' = -x \\ x * (-x) &= \frac{x - x}{x(-x) + 1} = 0 = \frac{-x + x}{-x^2 + 1} = (-x) * x \end{aligned}$$

B. Groups on the Set $\mathbb{R} \times \mathbb{R}$

1 $(a, b) * (c, d) = (ad + bc, bd)$, on the set $\{ (x, y) \in \mathbb{R} \times \mathbb{R} : y \neq 0 \}$

(i) $*$ is commutative.

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

(ii) $*$ is associative.

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

(iii) $(e_1, e_2) = (0, 1)$

$$\begin{aligned}(a,b) * (e_1, e_2) &= (ae_2 + be_1, be_2)\\ &= (a,b)\end{aligned}$$

$$\begin{aligned}be_2 &= b\\ e_2 &= 1\end{aligned}$$

$$\begin{aligned}ae_2 + be_1 &= a\\ a + be_1 &= a\\ e_1 &= 0\end{aligned}$$

(iv) $(a', b') = \left(\frac{-a}{b^2}, \frac{1}{b}\right)$

$$\begin{aligned}(a,b) * (a', b') &= (ab' + ba', bb')\\ &= (0, 1)\end{aligned}$$

$$\begin{aligned}bb' &= 1\\ b' &= \frac{1}{b}\end{aligned}$$

$$\begin{aligned}ab' + ba' &= 0\\ \frac{a}{b} + ba' &= 0\\ ba' &= \frac{-a}{b}\\ a' &= \frac{-a}{b^2}\end{aligned}$$

$$\begin{aligned}(a,b) * \left(\frac{-a}{b^2}, \frac{1}{b}\right) &= \left(\frac{a}{b} + \frac{-a}{b}, b\left(\frac{1}{b}\right)\right)\\ &= (0, 1)\end{aligned}$$

2 $(a, b) * (c, d) = (ac, bc + d)$, on the set $\{\, (x, y) \in \mathbb{R} \times \mathbb{R} : x \neq 0 \,\}$
(i) $*$ is not commutative: $(c, d) * (a, b) = (ca, da + b) \neq (a, b) * (c, d)$
(ii) $*$ is associative.

$$\begin{aligned}[(a,b) * (c,d)] * (e,f) &= (ac, bc + d) * (e, f)\\ &= (ace, bce + de + f)\\ &= (a,b) * (ce, de + f)\\ &= (a,b) * [(c,d) * (e,f)]\end{aligned}$$

(iii) $(e_1, e_2) = (1, 0)$

$$\begin{aligned}(a,b) * (e_1, e_2) &= (ae_1, be_1 + e_2)\\ &= (a,b)\end{aligned}$$

$$\begin{aligned}ae_1 &= a\\ e_1 &= 1\end{aligned}$$

$$\begin{aligned}be_1 + e_2 &= b\\ b + e_2 &= b\\ e_2 &= 0\end{aligned}$$

(iv) $(a', b') = (\frac{1}{a}, \frac{-b}{a})$

$$\begin{aligned}(a,b) * (a',b') &= (aa', ba' + b') \\ &= (1,0)\end{aligned}$$

$$\begin{aligned}aa' &= 1 \\ a' &= \frac{1}{a}\end{aligned}$$

$$\begin{aligned}ba' + b' &= 0 \\ \frac{b}{a} + b' &= 0 \\ b' &= \frac{-b}{a} \\ (a,b) * (\frac{1}{a}, \frac{-b}{a}) &= (\frac{a}{a}, \frac{b}{a} - \frac{b}{a}) \\ &= (1,0)\end{aligned}$$

3 $(a,b) * (c,d) = (ac, bc + d)$, on the set $\{ (x,y) \in \mathbb{R} \times \mathbb{R} \}$

(i) $*$ is not commutative, as per 2(i).

(ii) $*$ is associative, as per 2(ii).

(iii) $(e_1, e_2) = (1,0)$, as per 2(iii).

(iv) a' is not defined $\forall a \in \mathbb{R}$, notably when $a = 0$.

4 $(a,b) * (c,d) = (ac - bd, ad + bc)$, on the set $\{ (x,y) \in (\mathbb{R} \times \mathbb{R}) \setminus \{ (0,0) \} \}$

(i) $*$ is commutative.

$$\begin{aligned}(c,d) * (a,b) &= (ca - db, cb + da) \\ &= (ac - db, ad + bc) \\ &= (a,b) * (c,d)\end{aligned}$$

(ii) $*$ is associative.

$$\begin{aligned}(a,b) * [(c,d) * (e,f)] &= (ac - bd, ad + bc) * (ce - df, cf + de) \\ &= (a(ce - df) - b(cf + de), a(cf + de) + b(ce - df)) \\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf) \\ &= (e(ac - bd) - f(ad + bc), f(ac - bd) + e(ad + bc)) \\ &= (ac - bd, ad + bc) * (e,f) \\ &= [(a,b) * (c,d)] * (e,f)\end{aligned}$$

(iii) $(e_1, e_2) = (?, ?)$

$$\begin{aligned}(a,b) * (e_1, e_2) &= (ae_1 - be_2, ae_2 + be_1) \\ &= (a,b)\end{aligned}$$

$$\begin{aligned}ae_2 + be_1 &= b \\ be_1 &= b - ae_2 \\ e_1 &= 1 - \frac{ae_2}{b}\end{aligned}$$

$$\begin{aligned}ae_1 - be_2 &= a \\ -be_2 &= a - ae_1 \\ be_2 &= ae_1 - a \\ e_2 &= \frac{ae_1 - a}{b}\end{aligned}$$

C. Groups of Subsets of a Subset

1 The identity element with respect to the operation $+$ is $\emptyset$.

$$A + I = (A - I) \cup (I - A) = A$$
$$= (A - \emptyset) \cup (I - \emptyset)$$

$$I = \emptyset$$

2 $\langle 2^D, + \rangle$ is a group, since $\forall A \in 2^D, A^{-1} = A$.

$$A + A^{-1} = \emptyset$$
$$(A - A^{-1}) \cup (A^{-1} - A) = \emptyset$$
$$A - A^{-1} = A^{-1} - A = \emptyset$$
$$A^{-1} = A$$

3 Let $D = \{ a, b, c \}$.

$$2^D = \{ \emptyset, \{ a \}, \{ b \}, \{ c \}, \{ a, b \}, \{ a, c \}, \{ b, c \}, \{ a, b, c \} \}$$

TABLE 1. $\langle 2^D, + \rangle$

$+$	$\emptyset$	$\{ a \}$	$\{ b \}$	$\{ c \}$	$\{ a, b \}$	$\{ a, c \}$	$\{ b, c \}$	$\{ a, b, c \}$
$\emptyset$	$\emptyset$	$\{ a \}$	$\{ b \}$	$\{ c \}$	$\{ a, b \}$	$\{ a, c \}$	$\{ b, c \}$	$\{ a, b, c \}$
$\{ a \}$	$\{ a \}$	$\emptyset$	$\{ a, b \}$	$\{ a, c \}$	$\{ b \}$	$\{ c \}$	$\{ a, b, c \}$	$\{ b, c \}$
$\{ b \}$	$\{ b \}$	$\{ a, b \}$	$\emptyset$	$\{ b, c \}$	$\{ a \}$	$\{ a, b, c \}$	$\{ c \}$	$\{ a, c \}$
$\{ c \}$	$\{ c \}$	$\{ a, c \}$	$\{ b, c \}$	$\emptyset$	$\{ a, b, c \}$	$\{ a \}$	$\{ b \}$	$\{ a, b \}$
$\{ a, b \}$	$\{ a, b \}$	$\{ b \}$	$\{ a \}$	$\{ a, b, c \}$	$\emptyset$	$\{ b, c \}$	$\{ a, c \}$	$\{ c \}$
$\{ a, c \}$	$\{ a, c \}$	$\{ c \}$	$\{ a, b, c \}$	$\{ a \}$	$\{ b, c \}$	$\emptyset$	$\{ a, b \}$	$\{ b \}$
$\{ b, c \}$	$\{ b, c \}$	$\{ a, b, c \}$	$\{ c \}$	$\{ b \}$	$\{ a, c \}$	$\{ a, b \}$	$\emptyset$	$\{ a \}$
$\{ a, b, c \}$	$\{ a, b, c \}$	$\{ b, c \}$	$\{ a, c \}$	$\{ a, b \}$	$\{ c \}$	$\{ b \}$	$\{ a \}$	$\emptyset$

D. A Checkerboard Game

TABLE 2. $\langle G, * \rangle$

$*$	I	V	H	D
I	I	V	H	D
V	V	I	D	H
H	H	D	I	V
D	D	H	V	I

As shown in the *Cayley table* above, the identity element is I and every element is its own inverse. Having shown that and granting associativity, $\langle G, * \rangle$ is a group.

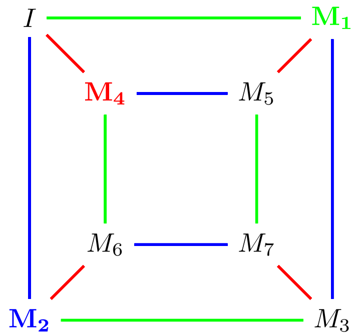
E. A Coin Game

TABLE 3. $\langle G, * \rangle$

$*$	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
I	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
M_1	M_1	I	M_3	M_2	M_5	M_4	M_7	M_6
M_2	M_2	M_3	I	M_1	M_6	M_7	M_4	M_5
M_3	M_3	M_2	M_1	I	M_7	M_6	M_5	M_4
M_4	M_4	M_6	M_5	M_7	I	M_2	M_1	M_3
M_5	M_5	M_7	M_4	M_6	M_1	M_3	I	M_2
M_6	M_6	M_4	M_7	M_5	M_2	I	M_3	M_1
M_7	M_7	M_5	M_6	M_4	M_3	M_1	M_2	I

As shown in the *Cayley table* above, the identity element is I and every element is invertible. Having shown that and granting associativity, $\langle G, * \rangle$ is a group. It is not commutative, because, for example $M_6 * M_4 = M_2$, while $M_4 * M_6 = M_1$, so $M_6 * M_4 \neq M_4 * M_6$.

FIGURE 1. $\langle r, s, t \mid r^2, s^2, t^2, (rs)^4, (st)^3, (rt)^2 \rangle$



F. Groups in Binary Codes

1 $(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (b_1, b_2, ..., b_n) + (a_1, a_2, ..., a_n)$, since the left-hand side is equivalent to $(a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$, which by commutativity is equivalent to $(b_1 + a_1, b_2 + a_2, ..., b_n + a_n)$, which is equivalent to $(b_1, b_2, ..., b_n) + (a_1, a_2, ..., a_n)$.

2

$$\begin{aligned}
1 + (1 + 1) = 1 + 0 = 1 = 0 + 1 = (1 + 1) + 1 \\
1 + (1 + 0) = 1 + 1 = 0 = 0 + 0 = (1 + 1) + 0 \\
1 + (0 + 1) = 1 + 1 = 0 = 1 + 1 = (1 + 0) + 1 \\
0 + (1 + 1) = 0 + 0 = 0 = 1 + 1 = (0 + 1) + 1 \\
1 + (0 + 0) = 1 + 0 = 1 = 1 + 0 = (1 + 0) + 0 \\
0 + (0 + 1) = 0 + 1 = 1 = 0 + 1 = (0 + 0) + 1 \\
0 + (1 + 0) = 0 + 1 = 1 = 1 + 0 = (0 + 1) + 0 \\
0 + (0 + 0) = 0 + 0 = 0 = 0 + 0 = (0 + 0) + 0
\end{aligned}$$

3

$$\begin{aligned}
(a_1, a_2, ..., a_n) + [(b_1, b_2, ..., b_n) + (c_1, c_2, ..., c_n)] &= (a_1, a_2, ..., a_n) + (b_1 + c_1, b_2 + c_2, ..., b_n + c_n) \\
&= (a_1 + b_1 + c_1, a_2 + b_2 + c_2, ..., a_n + b_n + c_n) \\
&= (a_1 + b_1, a_2 + b_2, ..., a_n + b_n) + (c_1, c_2, ..., c_n) \\
&= [(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n)] + (c_1, c_2, ..., c_n)
\end{aligned}$$

4 The identity element of $\mathbb{B}^n$, that is, the identity element for adding words on length n, is 0^n.

5 The inverse, with respect to word addition, of any word $(a_1, ..., a_n)$ is $(a_1, ..., a_n)$.

6 $\mathbf{a} + \mathbf{b} = \mathbf{a} + (-\mathbf{b})$, since $\mathbf{b} = -\mathbf{b}$. Thus $\mathbf{a} + \mathbf{b} = \mathbf{a} - \mathbf{b}$.

7

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

G. Theory of Coding: Maximum-Likelihood Decoding

TABLE 4. Parity check equations in C_1

1

C_1	a_4	a_1+a_3	$a_4=a_1+a_3$	a_5	$a_1+a_2+a_3$	$a_5=a_1+a_2+a_3$
00000	0	$0+0$	✓	0	$0+0+0$	✓
00111	1	$0+1$	✓	1	$0+0+1$	✓
01001	0	$0+0$	✓	1	$0+1+0$	✓
01110	1	$0+1$	✓	0	$0+1+1$	✓
10011	1	$1+0$	✓	1	$1+0+0$	✓
10100	0	$1+1$	✓	0	$1+0+1$	✓
11010	1	$1+0$	✓	0	$1+1+0$	✓
11101	0	$1+1$	✓	1	$1+1+1$	✓

2 (a)

$$C_2 = \{\, 000000, 001001, 010111, 011110, 100011, 101010, 110000, 111101 \,\}$$

TABLE 5. Distance in C_2

(b)

$d(\mathbf{a},\mathbf{b})$	000000	001001	010111	011110	100011	101010	110000	111101
000000		2	4	4	3	3	2	5
001001	2		4	4	3	3	4	3
010111	4	4		2	3	5	4	3
011110	4	4	2		5	3	4	3
100011	3	3	3	5		2	3	4
101010	3	3	5	3	2		3	4
110000	2	4	4	4	3	3		3
111101	5	3	3	3	4	4	3	

The minimum distance of the code C_2 is 2.

(c) Since the minimum distance is C_2, one error is sure to be detected in any codeword of C_2.

3 $C_3 = \{\, 0000, 0101, 1011, 1110 \,\}$ where $a_3 = a_1$ and $a_4 = a_1 + a_2$.

TABLE 6. Distance in C_3

$d(\mathbf{a},\mathbf{b})$	0000	0101	1011	1110
0000	0	2	3	3
0101	2	0	3	3
1011	3	3	0	2
1110	3	3	2	0

$$\min_{\mathbf{a}\in C_3, \mathbf{a}\neq\mathbf{b}} d(\mathbf{a},\mathbf{b}) = 2$$

4

- $11111 \to 11101$
- $00101 \to 00111$
- $11000 \to 11010$
- $10011 \to 10011$
- $10001 \to 10011$
- $10111 \to 10011$ *or* 00111

CHAPTER 4

Elementary Properties of Groups

A. Solving Equations in Groups

1

$$
\begin{aligned}
axb &= c \\
ax &= cb^{-1} \\
x &= a^{-1}cb^{-1}
\end{aligned}
$$

2

$$
\begin{aligned}
x^2b &= xa^{-1}c \\
xb &= a^{-1}c \\
x &= a^{-1}cb^{-1}
\end{aligned}
$$

3

$$
\begin{aligned}
acx &= xac \\
xacx &= x^2ac \\
x^2a &= bxc^{-1} \\
x^2ac &= bx
\end{aligned}
$$

$$
\begin{aligned}
xacx &= bx \\
xac &= b \\
x &= b(ac)^{-1}
\end{aligned}
$$

4

$$
x^3 = e
$$

$$
\begin{aligned}
ax^2 &= b \\
a &= bx \\
x &= b^{-1}a
\end{aligned}
$$

5

$$
\begin{aligned}
x^5 &= e \\
x^4 &= x^{-1}
\end{aligned}
$$

$$
\begin{aligned}
x^2 &= a^2 \\
x^4 &= a^2x^2 \\
x^{-1} &= a^2x^2 \\
e &= a^4x \\
\left(a^4\right)^{-1} &= x
\end{aligned}
$$

6

$$x^2a = (xa)^{-1}$$

$$\begin{aligned}(xax)^3 &= bx\\ xa(x^2a)(x^2a)x &= bx\\ xa(xa)^{-1}(xa)^{-1}x &= bx\\ (xa)^{-1}x &= bx\\ a^{-1}x^{-1}x &= bx\\ b^{-1}a^{-1} &= x\end{aligned}$$

B. Rules of Algebra in Groups

$$G = \langle \{\, I, A, B, C, D, K \,\}, \cdot \rangle$$

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$
$$\mathbf{C} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \qquad \mathbf{D} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \qquad \mathbf{K} = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$$

1 $\mathbf{A}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$ ... but $\mathbf{A} \neq e$, so $x^2 = e \not\Longrightarrow x = e$. ∎

2 $\mathbf{A}^2 = \mathbf{I}^2$, but $\mathbf{A} \neq \mathbf{I}$, so $x^2 = a^2 \not\Longrightarrow x = a$. ∎

3 $(\mathbf{AB})^2 = \mathbf{K}^2 = \mathbf{I}$, and $\mathbf{A}^2\mathbf{B}^2 = \mathbf{ID} = \mathbf{D}$, but $\mathbf{I} \neq \mathbf{D}$, so $(ab)^2 = a^2b^2$ is not true in every group G.[1] ∎

4 $x^2 = x \implies x = e$

$$\begin{aligned}x^2 &= x\\ xx &= x\\ xxx^{-1} &= xx^{-1}\\ xe &= e\\ x &= e\end{aligned}$$

∎

Table 1. $\langle \{\, I, A, B, C, D, K \,\}, \cdot \rangle$

5

$\cdot$	**I**	**A**	**B**	**C**	**D**	**K**
I	**I**					
A		**I**				
B			**D**			
C				**I**		
D					**B**	
K						**I**

As shown in the table, there does not exist an $x \in G$ such that $x = y^2$ for $y \in \{\, \mathbf{A}, \mathbf{C}, \mathbf{K} \,\}$.
Therefore $\neg\left(\forall x \in G,\ \exists y \in G\left(x = y^2\right)\right)$. ∎

6

$$\begin{aligned}y &= xz\\ x^{-1}y &= x^{-1}xz\\ z &= x^{-1}y\end{aligned}$$

Therefore, for all $x, y \in G$, there exists a $z \in G$ such that $y = xz$. ∎

[1] $(ab)^2 = a^2b^2$ is only true in abelian groups.

C. Elements That Commute

1 $a^{-1}b^{-1} = (ba)^{-1} = (ab)^{-1} = b^{-1}a^{-1}$

2 Since $a = b^{-1}ba = b^{-1}ab$, $ab^{-1} = (b^{-1}ab)b^{-1} = b^{-1}a$.

3 $a(ab) = a(ba) = (ab)a$

4 $(xax^{-1})(xbx^{-1}) = xa(x^{-1}x)bx^{-1} = x(ab)x^{-1} = x(ba)x^{-1} = xb(x^{-1}x)ax^{-1} = (xbx^{-1})(xax^{-1})$

5 $ab = ba \iff aba^{-1} = b$

PROOF. First, assume $ab = ba$. Multiplying by a^{-1} on the right shows $ab = ba \implies aba^{-1} = b$. Next, assume $aba^{-1} = b$. Multiplying by a on the right shows $aba^{-1} = b \implies ab = ba$. ■

6 $ab = ba \iff aba^{-1}b^{-1} = e$

PROOF. First, assume $ab = ba$. Multiplying by a^{-1} on the right yields $aba^{-1} = b$. Then multiplying by b^{-1} on the right yields $aba^{-1}b^{-1} = e$. Thus $ab = ba \implies x$. Next, assume $aba^{-1}b^{-1} = e$. Multiplying by b on the right yields $aba^{-1} = b$. Then multiplying by a^{-1} on the right yields $ab = ba$. Thus $aba^{-1}b^{-1} = e \implies ab = ba$ and $ab = ba \iff aba^{-1}b^{-1} = e$. ■

D. Group Elements and Their Inverses

1 $ab = e \implies ba = e$

PROOF. If $ab = e$, then $ab = aa^{-1}$, so by the cancellation law, $b = a^{-1}$ and $a = b^{-1}$. Thus, $bb^{-1} = e \implies ba = e$, as desired. ■

2 $abc = e \implies cab = e$ and $bca = e$.

PROOF. If $(ab)c = e$, then $(ab)c = (ab)(ab)^{-1}$, so by the cancellation law, $c = (ab)^{-1} = b^{-1}a^{-1}$ Thus, $(ab)^{-1}(ab) = e \implies c(ab) = e$, and $b(b^{-1}a^{-1})a = e \implies cba = e$. ■

3 ...

4 Let G be a group such that $xay = a^{-1}$ for all $a, x, y \in G$. Prove that $yax = a^{-1}$ as well.

PROOF. If $xay = a^{-1}$, then $(xay)a = a^{-1}a$, so by the definition of inversion, $(xay)a = e$. Thus $x^{-1}(xay)ax = x^{-1}ex$, so by associativity and the definition of the identity element, $(x^{-1}x)a(yax) = e \iff ea(yax) = e \iff a(yax) = e$. Multiply by a^{-1} on the left to obtain $a^{-1}a(yax) = a^{-1}e$, so by the definition of inversion, $yax = a^{-1}$. ■

5 Let $a = a^{-1}$, $b = b^{-1}$, and $c = c^{-1}$. If $ab = c$ show that $bc = a$ and $ca = b$ as well.

$$\begin{aligned} ab &= c \\ abb^{-1} &= cb^{-1} = cb \\ a &= cb \\ a^{-1} &= b^{-1}c^{-1} = bc \\ bc &= a \end{aligned}$$

$$\begin{aligned} ab &= c \\ b^{-1}a^{-1} &= c^{-1} \\ ba^{-1} &= c \\ ba^{-1}a &= ca \\ ca &= b \end{aligned}$$

6 Let $abc = (abc)^{-1}$, show that $bca = (bca)^{-1}$ and $cab = (cab)^{-1}$.

$$\begin{aligned} abc &= (abc)^{-1} \\ bca &= a^{-1}(abc)^{-1}a \\ &= a^{-1}(bc)^{-1} \\ &= (bca)^{-1} \end{aligned}$$

$$\begin{aligned} bca &= (bca)^{-1} \\ cab &= b^{-1}(bca)^{-1}b \\ &= b^{-1}(ca)^{-1} \\ &= (cab)^{-1} \end{aligned}$$

7 Let $a = a^{-1}$ and $b = b^{-1}$, show that $(ab)^{-1} = ba$.

PROOF. Replace a and b with their inverses on the right-hand side of $(ab)^{-1} = b^{-1}a^{-1}$ to obtain $(ab)^{-1} = ba$. ∎

8 $a = a^{-1} \iff a^2 = e$

PROOF. If $a = a^{-1}$, then $a^2 = e$ by multiplying by a on the right. If $a^2 = e$, then $a = a^{-1}$ by multiplying by a^{-1} on the right. ∎

9 Let $c = c^{-1}$. Prove $ab = c \iff abc = e$.

PROOF. If $ab = c$, then $ab = c^{-1}$, since $c = c^{-1}$. Multiply by c on the right to obtain $abc = e$. If $abc = e$, then $abc^{-1} = e$ since $c = c^{-1}$. Multiply by c on the right to obtain $ab = c$. ∎

E. Counting Elements and Their Inverses

1 Prove that in any finite group G, $2 \mid \left|\left\{ x \in G : x \neq x^{-1} \right\}\right|$.

PROOF. By definition, $G = \left\{ x \in G : x = x^{-1} \right\} \cup \left\{ x \in G : x \neq x^{-1} \right\}$.
Therefore, $\forall x \in G \left(x = x^{-1} \vee \left(x \neq x^{-1} \wedge \exists y \in G \left(y \neq x \wedge y = x^{-1}\right)\right)\right)$.
So, $\left|\left\{ x \in G : x \neq x^{-1} \right\}\right| = \left|\left\{ x_0, x_0^{-1}, x_1, x_1^{-1}, x_2, x_2^{-1}, x_3, x_3^{-1} ... \right\}\right| = 2k$. ∎

2 Prove $\left|\left\{ x \in G : x = x^{-1} \right\}\right|$ has the same parity as $|G|$.

PROOF. Since $|G| = \left|\left\{ x \in G : x = x^{-1} \right\}\right| + \left|\left\{ x \in G : x \neq x^{-1} \right\}\right|$,
and $\left|\left\{ x \in G : x \neq x^{-1} \right\}\right|$ is even, $\left|\left\{ x \in G : x = x^{-1} \right\}\right|$ has the same parity as $|G|$. ∎

3 Prove $2 \mid |G| \implies \exists x \in G \left(x \neq e \wedge x = x^{-1}\right)$.

PROOF. If $2 \mid |G|$ then $2 \mid \left|\left\{ x \in G : x = x^{-1} \right\}\right|$. Since $e = e^{-1}$, $2 \nmid \left|\left\{ x \in G : x \neq e \wedge x = x^{-1} \right\}\right|$ and thus $\exists x \in G \left(x \neq e \wedge x = x^{-1}\right)$. ∎

4 Given a finite abelian group $G = \{ e, a_1, a_2, ...a_n \}$, prove $(a_1a_2...a_n)^2 = e$.

$$\begin{aligned}(a_1a_2...a_n)^2 &= (a_1a_2...a_n)(a_1^{-1}a_2^{-1}...a_n^{-1})\\ &= a_1a_1^{-1}a_2a_2^{-1}...a_na_n^{-1}\\ &= ee...e\\ &= e\end{aligned}$$

∎

5 Prove $\forall x \in G \left(x \neq e \implies x \neq x^{-1}\right) \implies a_1a_2...a_n = e$.

PROOF. Assume $\forall x \in G \left(x \neq e \implies x \neq x^{-1}\right)$. Then $\forall x \in a_1a_2...a_n \left(\exists y \in a_1a_2...a_n \left(x \neq y \wedge y = x^{-1}\right)\right)$.
So $a_1a_2...a_n$ can be rewritten $a_1a_1^{-1}a_2a_2^{-}...a_{n/2}a_{n/2}^{-1}$, which reduces to e. ∎

6 Prove that if there is exactly one $x \neq e$ in G such that $x = x^{-1}$ then $a_1a_2...a_n = x$.

PROOF. $a_1a_2...a_n$ can be rewritten $xa_1a_1^{-1}a_2a_2^{-1}...a_{n/2}a_{n/2}^{-1}$, which is equivalent to xe. ∎

F. Constructing Small Groups

1 $a, b \in G$

(a) Prove $a^2 = a \implies a = e$.

PROOF. Assume $a^2 = a$. Divide by a to get $a = e$. ∎

(b) Prove $ab = a \implies b = e$.

PROOF. Assume $ab = a$. Multiply by a^{-1} on the left to get $a^{-1}ab = a^{-1}a \equiv b = e$. ∎

(c) Prove $ab = b \implies a = e$.

PROOF. Assume $ab = b$. Multiply by b^{-1} on the right to get $abb^{-1} = b^{-1} \equiv a = e$. ∎

2 ...

Explain why elements of each row in a Cayley table must be distinct.

3 There is exactly oneo group with three distinct elements.

TABLE 2. Multiplication Table for $\mathbb{Z}_3$

$\cdot$	**e**	**a**	**b**
e	e	a	b
a	a	b	e
b	b	e	a

4 There is exactly one group G with four elements, such that $\forall x \in G(xx = e)$.

TABLE 3. Multiplication Table for v_4

$\cdot$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

5 There is exactly one group G with four elements, such that $\exists x \in G(x \neq e \wedge xx = e)$ and $\exists y \in G(yy \neq e)$.

TABLE 4. Multiplication Table for v_4

$\cdot$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

6 ...

Explain why $\mathbb{Z}_3$ and V_4 are the only possible groups of order 4.

G. Direct Products of Groups

1 Prove that $G \times H$ is a group.

PROOF.

(G1)

$$\begin{aligned}(x_1, y_1)\left[(x_2, y_2)(x_3, y_3)\right] &= (x_1, y_1)(x_2x_3, y_2y_3)\\ &= (x_1x_2x_3, y_1y_2y_3)\\ &= (x_1x_2, y_1y_2)(x_3, y_3)\\ &= \left[(x_1, y_1)(x_2, y_2)\right](x_3, y_3)\end{aligned}$$

(G2) Let e_G be the identity element of G, and e_H the identity element of H. The identity element of $G \times H$ is (e_G, e_H).

$$(x, y)(e_G, e_H) = (xe_G, ye_H) = (x, y)$$

$$(e_G, e_H)(x, y) = (e_Gx, e_Hy) = (x, y)$$

(G3) $\forall (a, b) \in G \times H \left((a, b)^{-1} = (a^{-1}, b^{-1})\right)$

$$(a, b)(a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e_G, e_H) = e_{G\times H}$$

$$(a^{-1}, b^{-1})(a, b) = (a^{-1}a, b^{-1}b) = (e_G, e_H) = e_{G\times H}$$

■

Glossary

Cayley table: The multiplication table for a finite group.. 19