Ring Theory Examples

Jason Sass

April 23, 2023

Examples

Example 1. $(\mathbb{Q}, +, \cdot) =$ field
$(\mathbb{R}, +, \cdot) =$ field
$(\mathbb{C}, +, \cdot) =$ field
$\{a + b\sqrt{2} : a, b \in \mathbb{Q}\} =$ field

Proof. □

Exercise 2. Let $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Then $(S, +, *)$ is not a field.

Proof. Observe that $(S, +, *)$ is a commutative ring with unity $1 \neq 0$. Thus, S is a field iff every nonzero element of S is a unit. Hence, S is not a field iff there exists a nonzero element of S that is not a unit.

Let $x = \sqrt{2}$. Then $x = 0 + 1 * \sqrt{2}$, so $x \in S$ and $x \neq 0$. The element x is a unit iff there exists $y \in S$ such that $xy = 1$. Hence, x is not a unit iff there does not exist $y \in S$ such that $xy = 1$.

Suppose there exists $y \in S$ such that $xy = 1$. Then there exist integers a, b such that $y = a + b\sqrt{2}$. Thus,

$$\begin{aligned} 1 &= xy \\ &= \sqrt{2}(a + b\sqrt{2}) \\ &= a\sqrt{2} + 2b. \end{aligned}$$

Hence, $1 + 0\sqrt{2} = 1 = 2b + a\sqrt{2}$, so $1 = 2b$ and $0 = a$. Thus, $b = \frac{1}{2}$, so $b \notin \mathbb{Z}$. But, we have $b \in \mathbb{Z}$ and $b \notin \mathbb{Z}$, a contradiction. Therefore, does not exist $y \in S$ such that $xy = 1$. Thus, x is not a unit. Hence, there exists a nonzero element of S that is not a unit. Therefore, S is not a field. □

Exercise 3. The algebraic structure $(\mathbb{Z} \times \mathbb{Z}, +, *)$ is a commutative ring with unity $(1, 1)$ and is not a field.

Solution. The direct product of n copies of a commutative ring is a commutative ring. Hence, the direct product of 2 copies of a commutative ring is a commutative ring. Observe that $(\mathbb{Z}, +, *)$ is a commutative ring and $(\mathbb{Z} \times \mathbb{Z}, +, *)$

is the direct product of 2 copies of $(\mathbb{Z}, +, *)$. Therefore, $(\mathbb{Z}^2, +, *)$ is a commutative ring. Observe that the unity of $\mathbb{Z}^2$ is $(1, 1)$ and the zero of $\mathbb{Z}^2$ is $(0, 0)$ and $(1, 1) \neq (0, 0)$.

The ring $\mathbb{Z}^2$ is a field iff $\mathbb{Z}^2$ is a commutative ring and the unity is distinct from the zero element and every nonzero element of $\mathbb{Z}^2$ is a unit. Since $\mathbb{Z}^2$ is a commutative ring with unity $(1, 1) \neq (0, 0)$, then $\mathbb{Z}^2$ is a field iff every nonzero element of $\mathbb{Z}^2$ is a unit. Hence, $\mathbb{Z}^2$ is not a field iff there exists a nonzero element of $\mathbb{Z}^2$ that is not a unit.

Let $x = (1, 2) \in \mathbb{Z}^2$. Then $(1, 2) \neq (0, 0)$, so $(1, 2)$ is a nonzero element of $\mathbb{Z}^2$.

Suppose $(1, 2)$ is a unit of $\mathbb{Z}^2$. Then there exists an element $y \in \mathbb{Z}^2$ such that $xy = (1, 1)$. Since $y \in \mathbb{Z}^2$, then there exist integers a, b such that $y = (a, b)$.

Observe that

$$\begin{aligned}
(1,1) &= xy \\
&= (1,2)(a,b) \\
&= (a,2b).
\end{aligned}$$

Thus, $1 = a$ and $1 = 2b$, so $b = \frac{1}{2}$. Hence, $b \notin \mathbb{Z}$. Thus, we have $b \in \mathbb{Z}$ and $b \notin \mathbb{Z}$, a contradiction. Therefore, $(1, 2)$ is not a unit of $\mathbb{Z}^2$.

Hence, there exists a nonzero element of $\mathbb{Z}^2$ that is not a unit of $\mathbb{Z}^2$. Therefore, $(\mathbb{Z}^2, +, *)$ is not a field. $\square$

Exercise 4. What are all of the units in the ring $\mathbb{Z} \times \mathbb{Z}$?

Solution. We know that the ring $\mathbb{Z} \times \mathbb{Z}$ is not a field, so not every nonzero element is a unit. Hence, there are some nonzero elements of $\mathbb{Z} \times \mathbb{Z}$ which do not have multiplicative inverses in $\mathbb{Z} \times \mathbb{Z}$.

Let S be the set of all units of $\mathbb{Z} \times \mathbb{Z}$. Then $S = \{a \in \mathbb{Z} \times \mathbb{Z} : (\exists a^{-1} \in \mathbb{Z}^2)(aa^{-1} = (1, 1)\}$. Let $x \in S$. Then $x \in \mathbb{Z}^2$ and there exists $x^{-1} \in \mathbb{Z}^2$ such that $xx^{-1} = (1, 1)$. Thus, there exist integers a, b, c, d such that $x = (a, b)$ and $x^{-1} = (c, d)$. Hence,

$$\begin{aligned}
(1,1) &= xx^{-1} \\
&= (a,b)(c,d) \\
&= (ac,bd).
\end{aligned}$$

Thus, $1 = ac$ and $1 = bd$. Since a, b, c, d are integers, then this implies either $a = c = 1$ or $a = c = -1$ and either $b = d = 1$ or $b = d = -1$. Hence, $a = c$ and $b = d$, so $x = x^{-1}$ and 4 possibilities exist. Thus, x is either $(1, 1)$ or $(1, -1)$ or $(-1, 1)$ or $(-1, -1)$. Therefore, $S = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$. $\square$

Exercise 5. In any ring R, $(a + b)^2 = a^2 + 2ab + b^2$ iff R is commutative.

Proof. Let R be an arbitrary ring. Let $a, b \in R$.

We prove if $(a + b)^2 = a^2 + 2ab + b^2$, then R is commutative.

Suppose $(a + b)^2 = a^2 + 2ab + b^2$.

Observe that

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= (a^2+ab)+(ba+b^2)\\ &= (a^2+ab)+(b^2+ba)\\ &= ((a^2+ab)+b^2)+ba.\end{aligned}$$

Observe that

$$\begin{aligned}a^2+2ab+b^2 &= a^2+(ab+ab)+b^2\\ &= (a^2+ab)+(ab+b^2)\\ &= (a^2+ab)+(b^2+ab)\\ &= ((a^2+ab)+b^2)+ab.\end{aligned}$$

Thus, $((a^2+ab)+b^2)+ba = (a+b)^2 = a^2+2ab+b^2 = ((a^2+ab)+b^2)+ab$. Hence, $((a^2+ab)+b^2)+ba = ((a^2+ab)+b^2)+ab$. By the cancellation law for addition we obtain $ba = ab$.

Therefore, $ab = ba$ for all $a, b \in R$, so R is commutative.

We prove if R is commutative, then $(a+b)^2 = a^2+2ab+b^2$.

Suppose R is commutative. Then $ab = ba$.

Observe that

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= (a+b)a+(a+b)b\\ &= (a^2+ba)+(ab+b^2)\\ &= a^2+(ba+ab)+b^2\\ &= a^2+(ab+ab)+b^2\\ &= a^2+2ab+b^2.\end{aligned}$$

□

Exercise 6. Let R be a ring such that $a^2 = a$ for all $a \in R$. Then R is commutative and $a + a = 0$ for all $a \in R$.

We note that R is a **boolean ring**.

Proof. We prove $(\forall a \in R)(a + a = 0)$.

Let $a \in R$. Then

$$\begin{aligned}a+a &= (a+a)^2\\ &= (a+a)(a+a)\\ &= (a+a)a+(a+a)a\\ &= (a^2+a^2)+(a^2+a^2)\\ &= (a+a)+(a+a).\end{aligned}$$

Thus, $a + a = (a + a) + (a + a)$, so $(a + a) + 0 = (a + a) + (a + a)$. By the cancellation law for addition we obtain $0 = a + a$.

We prove R is commutative.

Let $a, b \in R$. Then

$$\begin{aligned} a + b &= (a + b)^2 \\ &= (a + b)(a + b) \\ &= a(a + b) + b(a + b) \\ &= (a^2 + ab) + (ba + b^2) \\ &= (a + ab) + (ba + b) \\ &= a + (ab + ba) + b \\ &= a + b + (ab + ba) \\ &= (a + b) + (ab + ba). \end{aligned}$$

Thus, $a + b = (a + b) + (ab + ba)$, so $(a + b) + 0 = (a + b) + (ab + ba)$. By the cancellation law for addition we obtain $0 = ab + ba$.

Since $x + x = 0$ for all $x \in R$, then in particular, $ab + ab = 0$. Thus, $ab + ab = 0 = ab + ba$. By the cancellation law for addition we obtain $ab = ba$. Therefore, $ab = ba$ for all $a, b \in R$, so $*$ is commutative. $\square$

Exercise 7. Let R be a commutative ring. For each $a \in R$ let $H_a = \{x \in R : ax = 0\}$. Then for every $x, y \in H_a, xy \in H_a$.

Proof. Let $x, y \in H_a$. Then $x, y \in R$ and $ax = 0$ and $ay = 0$. Observe that

$$\begin{aligned} 0 &= 0y \\ &= (ax)y \\ &= a(xy). \end{aligned}$$

Since R is closed under multiplication, then $xy \in R$. Thus, $xy \in R$ and $a(xy) = 0$, so $xy \in H_a$. $\square$

Exercise 8. Let $n \in \mathbb{N}, n > 1$ and $x^n = x$ for all x in a ring R. If $a, b \in R$ such that $ab = 0$, then $ba = 0$.

Proof. Let $a, b \in R$ such that $ab = 0$. Then

$$\begin{aligned} ba &= (ba)^n \\ &= (ba)(ba)...(ba)(ba) \\ &= b(ab)(ab)...(ab)a \\ &= b * 0 * 0 * ... * 0 * a \\ &= 0. \end{aligned}$$

Hence, $ba = 0$. $\square$

Integral domains

Exercise 9. Let D be an integral domain. If $a^2 = e$, then $a = \pm e$.

Proof. Let $a \in D$ such that $a^2 = e$.

Observe that $e^2 = e = a^2$. Thus, $e^2 - a^2 = 0$, so $(e+a)(e-a) = 0$. Since D is an integral domain, then either $e + a = 0$ or $e - a = 0$. Hence, either $a = -e$ or $a = e$, so $a = \pm e$. $\square$

Ideals

Exercise 10. The set $\{[0], [2], [4]\}$ is an ideal of $\mathbb{Z}_6$.

Solution. Let $R = \mathbb{Z}_6$ and $I = \{[0], [2], [4]\}$.

Observe that I is a cyclic subgroup of $(\mathbb{Z}_6, +)$ and $I = \{k[2]_6 : k \in \mathbb{Z}\} = [2k]_6 : k \in \mathbb{Z}\}$.

Let $x \in I$. Then $x = [2k]$ for some $k \in \mathbb{Z}$.

Let $a \in Rx$. Then $a = [r]_6 x$ for some $r \in \mathbb{Z}$. Thus, $a = [r]([2k]) = [(2k)r] = [2(kr)]$. Since $\mathbb{Z}$ is closed under multiplication and $k, r \in \mathbb{Z}$, then $kr \in \mathbb{Z}$. Hence, $a \in I$, by definition of I. Thus, $a \in Rx$ implies $a \in I$, so $Rx \subset I$.

Let $b \in xR$. Then $b = x[r]_6$ for some $r \in \mathbb{Z}$. Thus, $b = [2k][r] = [(2k)r] = [2(kr)]$. Since $\mathbb{Z}$ is closed under multiplication and $k, r \in \mathbb{Z}$, then $kr \in \mathbb{Z}$. Hence, $a \in I$, by definition of I. Thus, $a \in xR$ implies $a \in I$, so $xR \subset I$.

Therefore, $RI \subset I$ and $IR \subset I$.

Since $(I, +)$ is an abelian subgroup of $(R, +)$ and $RI \subset I$ and $IR \subset I$, then I is an ideal of R. Thus, the set $\{[0], [2], [4]\}$ is an ideal of $\mathbb{Z}_6$. $\square$

Exercise 11. If R is a field, then the only ideals of R are the zero ring and R itself.

Proof. Let R be a field. Let I be an ideal in R. Then either I is the zero ring or I is not the zero ring.

Suppose I is not the zero ring. Since I is an ideal, then $(I, +)$ is an abelian subgroup of $(R, +)$. Since I is not the zero group, then I must contain a nonzero element.

Let a be some nonzero element of I. Then $a \in I$ and $a \neq 0$. Since R is a field, then every nonzero element of R is a unit of R. Hence, in particular, a is a unit of R. Therefore, there exists $a^{-1} \in R$ such that $aa^{-1} = e$, where e is the unity of R. Since I is an ideal, then for every $x \in I, IR \subset I$. Thus, $aR \subset I$, where $aR = \{ar : r \in R\}$. Since $a^{-1} \in R$, then $aa^{-1} \in aR$. Hence, $e \in aR$. Thus, $e \in aR$ and $aR \subset I$, so $e \in I$. Therefore, $eR \subset I$, where $eR = \{er : r \in R\} = \{r : r \in R\} = R$. Hence, $R \subset I$. Since I is an ideal, then $I \subset R$. Thus, $I \subset R$ and $R \subset I$, so $I = R$.

Therefore, either I is the zero ring or I is the field R itself. $\square$

Exercise 12. Let G be a group such that $g^2 = e$ for all $g \in G$. Then G is abelian.

Solution. Given $(\forall g \in G)(g^2 = e)$.

To prove G is abelian, we must prove $(\forall a, b \in G)(ab = ba)$. $\square$

Proof. Let $a, b \in G$. Then $ab \in G$. Since $g^2 = e$ for all $g \in G$, then $a^2 = e$ and $b^2 = e$ and $(ab)^2 = e$.

Observe that $(ab)^2 = e = e{*}e = a^2b^2$. Thus, $(ab)(ab) = aabb$, so $abab = aabb$. We apply the right cancellation law to obtain $aba = aab$. We apply the left cancellation law to obtain $ba = ab$. Hence, $ab = ba$ for all $a, b \in G$, so $*$ is commutative. Therefore, G is abelian. $\square$

Proof. Let $a, b \in G$. Since G is closed under $*$, then $ab \in G$. Since $xx = e$ for all $x \in G$, then $x^{-1} = x$ by definition of inverse element. Thus, $a^{-1} = a$ and $b^{-1} = b$ and $(ab)^{-1} = ab$.

Observe that $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Thus, $ab = ba$. Since a, b are arbitrary then $ab = ba$ for all $a, b \in G$. Hence, $*$ is commutative, so $(G, *)$ is abelian. $\square$

Exercise 13. Let G be a group. Let $g_1, g_2, ..., g_n$ be elements of G. Then $(g_1g_2...g_n)^{-1} = g_n^{-1}g_{n-1}^{-1}...g_2g_1$.

Solution. Let $n \in \mathbb{Z}^+$. We must prove for all n, $(g_1g_2...g_n)^{-1} = g_n^{-1}g_{n-1}^{-1}...g_2g_1$. Thus, we define predicate $p(n) : (g_1g_2...g_n)^{-1} = g_n^{-1}g_{n-1}^{-1}...g_2g_1$. We prove by induction on n. $\square$

Proof. Let n be a positive integer.

Let $p(n)$ be the predicate $(g_1g_2...g_n)^{-1} = g_n^{-1}g_{n-1}^{-1}...g_2g_1$ defined over $\mathbb{Z}^+$.

We prove $(\forall n \in \mathbb{Z}^+)(p(n))$ by induction on n.

Basis: Since $(g_1)^{-1} = g_1^{-1}$, then $p(1)$ is true.

Induction: We must prove $(\forall m \in \mathbb{Z}^+)(p(m) \to p(m+1))$.

Suppose m is an arbitrary positive integer such that $p(m)$ is true. Then $(g_1g_2...g_m)^{-1} = g_m^{-1}g_{m-1}^{-1}...g_2g_1$.

Observe that

$$\begin{aligned}
(g_1g_2...g_mg_{m+1})^{-1} &= [(g_1g_2...g_m)g_{m+1}]^{-1} \\
&= g_{m+1}^{-1} * (g_1g_2...g_m)^{-1} \\
&= g_{m+1}^{-1} * (g_m^{-1}g_{m-1}^{-1}...g_2g_1) \\
&= g_{m+1}^{-1}g_m^{-1}g_{m-1}^{-1}...g_2g_1.
\end{aligned}$$

Thus, $p(m+1)$ is true.

Therefore, by induction, $(g_1g_2...g_n)^{-1} = g_n^{-1}g_{n-1}^{-1}...g_2g_1$ for all positive integers n. $\square$

Exercise 14. Let $G = \{x \in \mathbb{R} : x > 1\}$. Define $x * y = xy - x - y + 2$ for all $x, y \in G$. Then $(G, *)$ is a group.

Solution. To prove G is a group, we must prove:

1. $*$ is a binary operation on G.
2. $*$ is associative.
3. There exists an identity element in G.
4. Each element of G has an inverse in G. $\square$

Proof. Clearly, G is a nonempty set. To prove $*$ is a binary operation, we must prove G is closed under $*$.

Let x and y be arbitrary elements of G. Then x and y are real numbers such that $x > 1$ and $y > 1$. To prove G is closed under $*$, we must prove $x * y \in G$.

Note that $x*y = xy-x-y+2$ is a real number. Since $y > 1$, then $y-1 > 0$.

Observe that

$$\begin{aligned} x &> 1 \\ x(y-1) &> y-1 \\ xy-x &> y-1 \\ xy-x-y+1 &> 0 \\ xy-x-y+2 &> 1 \\ x*y &> 1. \end{aligned}$$

Hence, $x * y \in G$, as desired.

To prove $*$ is associative, let $x, y, z \in G$. We must prove $x*(y*z) = (x*y)*z$.

Observe that

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

Hence, $*$ is associative.

We prove 2 is the identity of G. Observe that $2 \in G$. Let a be an arbitrary element of G. Then $a*2 = a(2)-a-2+2 = 2a-a = a$ and $2*a = 2a-2-a+2 = a$. Hence, 2 is an identity of G.

We prove each element of G has an inverse. Let $a \in G$. Then $a \in \mathbb{R}$ and $a > 1$. Let $b = \frac{a}{a-1}$. Since $a-1 > 0$, then $a-1 \neq 0$. Hence, $b \in \mathbb{R}$. Since $0 > -1$, then $a > a-1$. Since $a-1 > 0$, we divide by $a-1$ to get $\frac{a}{a-1} > 1$. Thus, $b > 1$, so $b \in G$.

Observe that

$$
\begin{aligned}
a * b &= ab - a - b + 2 \\
&= (a-1)b - a + 2 \\
&= (a-1)\frac{a}{a-1} - a + 2 \\
&= a - a + 2 \\
&= 2
\end{aligned}
$$

and

$$
\begin{aligned}
a * b &= ab - a - b + 2 \\
&= ba - b - a + 2 \\
&= b * a.
\end{aligned}
$$

Therefore, $a * b = b * a = 2$, so b is an inverse of a. Hence, each element of G has an inverse in G.

Therefore, $(G, *)$ is a group. $\square$

Exercise 15. Let $(\mathbb{Z}_n^*, *)$ be the group of units of $\mathbb{Z}_n$. If $n \geq 3$, then there is an element $[a] \in \mathbb{Z}_n^*$ such that $[a]^2 = [1]$ and $[a] \neq [1]$.

Solution. Let $n \in \mathbb{N}$.

The statement to prove is P : if $n \geq 3$, then $(\exists [a] \in \mathbb{Z}_n^*)([a]^2 = [1] \wedge [a] \neq [a])$.

We try different values of n, like $n = 1, 2, 3, 4, 5, 6, ...$ We find that when $n < 3$, then $[1]^2 = [1]$, but $[1] = [1]$. Now, when $n \geq 3$, we find that $[n-1]^2 = [1]$. $\square$

Proof. Let n be a positive integer. Suppose $n \geq 3$. Since $n \in \mathbb{Z}$, then $n - 1 \in \mathbb{Z}$, so $[n-1] \in \mathbb{Z}_n$. Since $n|n$, then $n|(n-1+1)$, so $n|(n-1)-(-1)$. Hence, $n - 1 \equiv -1 \pmod{n}$, so $[n-1] = [-1]$. Observe that $[n-1]^2 = [n-1][n-1] = [-1][-1] = [(-1)(-1)] = [1]$. Since $[n-1] \in \mathbb{Z}_n$ and $[n-1][n-1] = [1]$, then $[n-1] \in \mathbb{Z}_n^*$.

Since $n \geq 3$, then $n - 2 \geq 1$. Since $n \geq 3$ and $n - 2 \geq 1$, then $n > 0$ and $n - 2 > 0$. Hence, n and $n - 2$ are positive integers and $n > n - 2$. Since $n|n-2$ implies $n \leq n - 2$, then $n > n - 2$ implies $n \not| n - 2$. Thus, since $n > n - 2$, then $n \not| n - 2$. Therefore, $n \not| (n-1) - 1$, so $n - 1 \not\equiv 1 \pmod{n}$. Thus, $[n-1] \neq [1]$.

Let $a = n - 1$. Then $[a] = [n-1]$. Since $[n-1] \in \mathbb{Z}_n^*$ and $[n-1]^2 = [1]$ and $[n-1] \neq [1]$, then there exists $[a] \in \mathbb{Z}_n^*$ such that $[a]^2 = [1]$ and $[a] \neq [1]$. $\square$

Exercise 16. Let a, b be any elements of a group $(G, *)$. Then $(aba^{-1})^n = ab^na^{-1}$, for any positive integer n.

Solution. We translate this into logical symbols.

Let the open sentence be $S(a, b, n) : (aba^{-1})^n = ab^na^{-1}$.

This assertion in logical symbols is:
$\forall(a, b \in G)\forall(n \in \mathbb{Z}^+)S(a, b, n)$.

Let $a, b \in G$. We must prove: $\forall(n \in \mathbb{Z}^+)S(a, b, n)$.

This universally quantified statement can be proven using mathematical induction. $\square$

Proof. We prove using induction.

Basis: For $n = 1$, the statement $(aba^{-1})^1 = aba^{-1} = ab^1a^{-1}$ is true.

Induction: We must prove $S_k \to S_{k+1}$ for any $k \geq 1$. That is we must show that if $(aba^{-1})^k = ab^ka^{-1}$, then $(aba^{-1})^{k+1} = ab^{k+1}a^{-1}$. We use direct proof. Suppose $(aba^{-1})^k = ab^ka^{-1}$. Observe that:

$$\begin{aligned}
(aba^{-1})^{k+1} &= (aba^{-1})^k(aba^{-1}) \\
&= (ab^ka^{-1})(aba^{-1}) \text{ (induction hypothesis)} \\
&= (ab^k)[a^{-1}(aba^{-1})] \text{ (* is associative in a group)} \\
&= (ab^k)[(a^{-1}a)(ba^{-1})] \text{ (* is associative in a group)} \\
&= (ab^k)[e(ba^{-1})] \text{ (defn of inverse element)} \\
&= (ab^k)(ba^{-1}) \text{ (defn of identity element)} \\
&= a(b^kb)a^{-1} \text{ (* is associative in a group)} \\
&= ab^{k+1}a^{-1}
\end{aligned}$$

Thus we have shown $(aba^{-1})^{k+1} = ab^{k+1}a^{-1}$. This completes the proof that $S_k \to S_{k+1}$ for $k \geq 1$. It follows by induction that $(aba^{-1})^n = ab^na^{-1}$ for all $n \in \mathbb{Z}^+$.

Since a, b are arbitrary then the statement $(aba^{-1})^n = ab^na^{-1}$ for all $n \in \mathbb{Z}^+$ is true for all $a, b \in G$. $\square$

Exercise 17. Let $(G, *)$ be a group. Define a relation $\sim$ on G for all $x, y \in G$ by $x \sim y$ iff there exists some $a \in G$ such that $y = axa^{-1}$. Then $\sim$ is an equivalence relation on G.

Solution. We must prove $\sim$ is reflexive, symmetric, and transitive.

Thus, we must prove:

1. reflexive: $(\forall x \in G)(x \sim x)$.
2. symmetric: $(\forall x, y \in G)(x \sim y \to y \sim x)$.
3. transitive: $(\forall x, y, z \in G)(x \sim y \land y \sim z \to x \sim z)$.

$\square$

Proof. Let x be an arbitrary element of G. To prove $\sim$ is reflexive, we must find some $a \in G$ such that $x = axa^{-1}$. Let $a = e$, where e is the identity element in G. Then $axa^{-1} = exe^{-1} = xe^{-1} = xe = x$. Hence, $\sim$ is reflexive.

Let x and y be arbitrary elements of G such that $x \sim y$. Then there exists some $a \in G$ such that $y = axa^{-1}$. Hence, $ya = ax$. To prove $y \sim x$, we must find some $b \in G$ such that $x = byb^{-1}$. Let $b = a^{-1}$. Observe that

$$\begin{aligned}
byb^{-1} &= a^{-1}y(a^{-1})^{-1} \\
&= a^{-1}ya \\
&= a^{-1}(ya) \\
&= a^{-1}(ax) \\
&= (a^{-1}a)x \\
&= ex \\
&= x.
\end{aligned}$$

Therefore, $\sim$ is symmetric.

Let x, y, and z be arbitrary elements of G such that $x \sim y$ and $y \sim z$. Then there exist elements a and b in G such that $y = axa^{-1}$ and $z = byb^{-1}$. To prove $x \sim z$, we must find some $c \in G$ such that $z = cxc^{-1}$. Let $c = ba$. Observe that

$$\begin{aligned}
cxc^{-1} &= (ba)x(ba)^{-1} \\
&= (ba)x(a^{-1}b^{-1}) \\
&= b(axa^{-1})b^{-1} \\
&= byb^{-1} \\
&= z.
\end{aligned}$$

Therefore, $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric, and transitive, then $\sim$ is an equivalence relation on G. □

Exercise 18. Let $(G, *)$ be a group. Let $a, b \in G$. If $(ab)^2 = a^2b^2$, then $ba = ab$.

Solution. We must prove if $(ab)^2 = a^2b^2$, then $ba = ab$. □

Proof. Let a and b be arbitrary elements of group G such that $(ab)^2 = a^2b^2$. We must prove $ba = ab$.

Observe that $aabb = a^2b^2 = (ab)^2 = (ab)(ab) = abab$. Hence, $aabb = abab$. By the left cancellation law, we have $abb = bab$. By the right cancellation law, we have $ab = ba$, as desired. □

Exercise 19. Let $\langle G, * \rangle$ be an abelian group. Let $H = \{a \in G : a^2 = e\}$. Then H is a subgroup of G.

Solution. We must prove H is a subgroup of G. Thus we must prove:

1. $H \subseteq G$.
2. H is closed under $*$.
3. $e \in H$.
4. $\forall a \in H. a^{-1} \in H$. □

Proof. Let $e \in G$ be the identity of group G.

Let $x \in H$. Then by definition of H, $x \in G$. Hence, $x \in H$ implies $x \in G$, so $H \subseteq G$.

Let $x, y \in H$. Then $x, y \in G$ and $x^2 = e$ and $y^2 = e$. Since G is closed under $*$, then $xy \in G$. Since G is abelian we know $(xy)^k = x^k y^k$ for any $k \in \mathbb{Z}$. Observe that $(xy)^2 = x^2 y^2 = ee = e$. Since $xy \in G$ and $(xy)^2 = e$, then $xy \in H$. Therefore, H is closed under $*$.

Since $e \in G$ and $e^2 = ee = e$, then by definition of H, $e \in H$.

Let $x \in H$. Then $x \in G$ and $x^2 = e$. Since G is a group then $x^{-1} \in G$. Observe that $(x^{-1})^2 = (x^2)^{-1} = e^{-1} = e$. Since $x^{-1} \in G$ and $(x^{-1})^2 = e$, then $x^{-1} \in H$. Therefore, for each $x \in H, x^{-1} \in H$.

Thus, H is a subgroup of G. □

Exercise 20. Let $(G, *)$ be a group. Let $a, b \in G$. Then $(aba^{-1})^n = ab^n a^{-1}$ for every positive integer n.

Solution. Let $p(n) : (aba^{-1})^n = ab^n a^{-1}$.

We must prove $(\forall n \in \mathbb{Z}^+)(p(n))$.

Thus, we prove by induction on n. □

Proof. Let a and b be arbitrary elements of group G.

Let $p(n) : (aba^{-1})^n = ab^n a^{-1}$.

We prove $(\forall n \in \mathbb{Z}^+)(p(n))$ by induction.

Basis:

Observe that $(aba^{-1})^1 = aba^{-1} = ab^1 a^{-1}$, so $p(1)$ is true.

Induction:

Suppose m is an arbitrary positive integer such that $p(m)$ is true.

To prove $p(m+1)$ is true, we must prove $(aba^{-1})^{m+1} = ab^{m+1}a^{-1}$.

Since $p(m)$ is true, then $(aba^{-1})^m = ab^m a^{-1}$.

Observe that

$$\begin{aligned}
(aba^{-1})^{m+1} &= (aba^{-1})^m (aba^{-1}) \\
&= (ab^m a^{-1})(aba^{-1}) \\
&= (ab^m)(a^{-1}a)(ba^{-1}) \\
&= (ab^m)(ba^{-1}) \\
&= ab^{m+1}a^{-1}.
\end{aligned}$$

Hence, by induction, $(aba^{-1})^n = ab^n a^{-1}$ for all positive integers n. □

Proposition 21. *Let $\langle G, * \rangle$ be a group. Let $g \in G$ be a fixed element. Then the map $i_g : G \mapsto G$ defined by $i_g(x) = g * x * g^{-1}$ for all $x \in G$ is an isomorphism of G with itself.*

Solution. We must prove i_g is an isomorphism of G with G. Thus we must prove:

1) i_g is one to one. To prove this we must show: $\forall a, b \in G . i_g(a) = i_g(b) \to a = b$.

2) i_g is onto. To prove this we must show: $\forall b \in G.\exists a \in G.i_g(a) = b$.
3) $(\forall a, b \in G)(i_g(a * b) = i_g(a) * i_g(b))$. □

Proof. Since $g \in G$ and G is a group, then $g^{-1} \in G$.

Let $a, b \in G$. Since G is closed under $*$ then $gag^{-1} \in G$ and $gbg^{-1} \in G$.

Suppose $i_g(a) = i_g(b)$. Then $gag^{-1} = gbg^{-1}$. By left cancellation law of G, $ag^{-1} = bg^{-1}$. By right cancellation law of G, $a = b$. Hence, $i_g(a) = i_g(b)$ implies $a = b$. Since a, b are arbitrary then $i_g(a) = i_g(b)$ implies $a = b$ is true for all $a, b \in G$. Therefore, i_g is one to one, by definition of injective function.

Suppose $b \in G$. Since $g \in G$ by definition of group $g^{-1} \in G$. Set $a = g^{-1}bg$. Since G is closed under $*$, then $a \in G$.

Observe that

$$\begin{aligned} i_g(a) &= i_g(g^{-1}bg) \\ &= g(g^{-1}bg)g^{-1} \\ &= (gg^{-1})b(gg^{-1}) \\ &= ebe \\ &= b \end{aligned}$$

Thus, there exists $a \in G$ such that $i_g(a) = b$. Since b is arbitrary then there exists $a \in G$ such that $i_g(a) = b$ for all $b \in G$. Therefore, by definition of surjective function, i_g is onto.

Since i_g is one to one and onto, then i_g is a bijective map.

Let $a, b \in G$. Observe that

$$\begin{aligned} i_g(a) * i_g(b) &= (g * a * g^{-1}) * (g * b * g^{-1}) \\ &= (g * a) * (g^{-1} * g) * (b * g^{-1}) \\ &= (g * a) * e * (b * g^{-1}) \\ &= (g * a) * (b * g^{-1}) \\ &= g * (a * b) * g^{-1} \\ &= i_g(a * b) \end{aligned}$$

Thus, $i_g(a) * i_g(b) = i_g(a * b)$. Since a, b are arbitrary then $i_g(a) * i_g(b) = i_g(a * b)$ for all $a, b \in G$. Therefore, by definition of isomorphism, $i_g : G \mapsto G$ is an isomorphism. □

Proposition 22. *Let $\langle G, \cdot\rangle$ be a group. If $\langle H, \cdot\rangle$ is a subgroup of $\langle K, \cdot\rangle$ and $\langle K, \cdot\rangle$ is a subgroup of $\langle G, \cdot\rangle$, then $\langle H, \cdot\rangle$ is a subgroup of $\langle G, \cdot\rangle$.*

Solution. Our hypothesis is: $\langle G, \cdot\rangle$ is a group and $\langle H, \cdot\rangle \leq \langle K, \cdot\rangle$ and $\langle K, \cdot\rangle \leq \langle G, \cdot\rangle$.

Our conclusion is: $\langle H, \cdot\rangle \leq \langle G, \cdot\rangle$.

To prove this claim, we can use the definition of subgroup.

Thus we must prove:

1. $H \subseteq G$.
2. $\langle H, \cdot\rangle$ is a group. □

Proof. Suppose $\langle G, \cdot \rangle$ is a group and $\langle H, \cdot \rangle \leq \langle K, \cdot \rangle$ and $\langle K, \cdot \rangle \leq \langle G, \cdot \rangle$. Since $\langle H, \cdot \rangle$ is a subgroup of $\langle K, \cdot \rangle$, then $H \subseteq K$. Since $\langle K, \cdot \rangle$ is a subgroup of $\langle G, \cdot \rangle$, then $K \subseteq G$. Thus, by the transitive property of the subset relation, $H \subseteq G$.

Since $\langle H, \cdot \rangle$ is a subgroup of $\langle K, \cdot \rangle$, then $\langle H, \cdot \rangle$ is a group under the binary operation $\cdot$ induced by $\langle K, \cdot \rangle$.

Since $\langle K, \cdot \rangle$ is a subgroup of $\langle G, \cdot \rangle$, then $\langle K, \cdot \rangle$ is a group under the binary operation $\cdot$ induced by $\langle G, \cdot \rangle$.

Hence, $\langle H, \cdot \rangle$ is a group under the binary operation $\cdot$ induced by $\langle G, \cdot \rangle$.

Therefore, $\langle H, \cdot \rangle$ is a subgroup of $\langle G, \cdot \rangle$. □

Proposition 23. *Let G be a group and a be one fixed element of G. Then $H_a = \{x \in G : xa = ax\}$ is a subgroup of G.*

Solution. Our hypothesis is: $\langle G, * \rangle$ is a group and $a \in G$ is fixed.

Our conclusion is: $H_a \leq G$.

We translate into logical symbols.

Let $H : \langle G, * \rangle$ is a group with $a \in G$ fixed.

Let $C : H_a \leq G$.

We must prove: $H \to C$.

Thus we must prove:

1. H_a is closed under $*$.
2. $e \in H_a$.
3. $\forall a \in H_a . a^{-1} \in H_a$. □

Proof. Let $\langle G, * \rangle$ be a group with $a \in G$ fixed. Let $H_a = \{x \in G : xa = ax\}$. Let $e \in G$ be the identity of G.

Let $g, h \in H_a$. Then $g, h \in G$ and $ga = ag$ and $ha = ah$. Since G is group, then G is closed under $*$, so $gh \in G$. Observe that

$$\begin{aligned} (gh)a &= g(ha) \\ &= g(ah) \\ &= (ga)h \\ &= (ag)h \\ &= a(gh) \end{aligned}$$

Thus, $(gh)a = a(gh)$, so $gh \in H_a$. Since g, h are arbitrary then $gh \in H_a$ for all $g, h \in H_a$. Therefore, H_a is closed under $*$.

By definition of identity element, $ea = ae = a$. Thus, by definition of H_a, $e \in H_a$.

Let $h \in H_a$. Then by definition of H_a, $h \in G$ and $ha = ah$. Since G is a group, by definition of group, $h^{-1} \in G$. Observe that

$$\begin{aligned} h^{-1}(ha)h^{-1} &= h^{-1}(ah)h^{-1} \\ (h^{-1}h)(ah^{-1}) &= (h^{-1}a)(hh^{-1}) \\ e(ah^{-1}) &= (h^{-1}a)e \\ ah^{-1} &= h^{-1}a \end{aligned}$$

Hence, $h^{-1}a = ah^{-1}$, so $h^{-1} \in H_a$ by definition of H_a. Since h is arbitrary then $h^{-1} \in H_a$ for all $h \in H_a$.

Therefore, $\langle H_a, * \rangle$ is a subgroup of $\langle G, * \rangle$. $\square$

Proposition 24. *If H and K are subgroups of abelian group G, then $\{hk : h \in H, k \in K\}$ is a subgroup of G.*

Solution. Let $M = \{hk : h \in H, k \in K\}$.

The hypothesis is:

G is an abelian group and H is a subgroup of G and K is a subgroup of G.

The conclusion is: $\langle M, * \rangle$ is a subgroup of $\langle G, * \rangle$.

We translate into logical symbols:

Let $H_1 : \langle G, * \rangle$ is an abelian group.

Let $H_2 : \langle H, * \rangle \leq \langle G, * \rangle$.

Let $H_3 : \langle K, * \rangle \leq \langle G, * \rangle$.

Let $C : \langle M, * \rangle \leq \langle G, * \rangle$.

The statement is: $H_1 \wedge H_2 \wedge H_3 \to C$.

We use direct proof. Thus we assume $H_1 \wedge H_2 \wedge H_3$ and show that C is true.

To prove C we must prove:

1. $M \subseteq G$.
2. M is closed under $*$.
3. $e \in M$.
4. $\forall a \in M . a^{-1} \in M$. $\square$

Proof. Suppose $\langle G, * \rangle$ is an abelian group and $\langle H, * \rangle \leq \langle G, * \rangle$ and $\langle K, * \rangle \leq \langle G, * \rangle$.

Let $M = \{hk : h \in H, k \in K\}$.

Let $a \in M$. Then $a = hk$ and $h \in H$ and $k \in K$. Since $\langle H, * \rangle$ is a subgroup of $\langle G, * \rangle$, then $H \subseteq G$. Since $\langle K, * \rangle$ is a subgroup of $\langle G, * \rangle$, then $K \subseteq G$. Since $h \in H$ and $H \subseteq G$, then $h \in G$. Since $k \in K$ and $K \subseteq G$, then $k \in G$. Since $\langle G, * \rangle$ is a group then $\langle G, * \rangle$ is closed under $*$. Thus, $hk \in G$, so $a \in G$. Hence, $a \in M$ implies $a \in G$. Since a is arbitrary then $a \in M$ implies $a \in G$ for all $a \in M$. Therefore, $M \subseteq G$.

Let $a, b \in M$. Then $a = h_1k_1$ and $b = h_2k_2$ and $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Observe that $ab = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2)$. Since H and K are groups, then H and K are each closed under $*$. Thus, $h_1h_2 \in H$ and $k_1k_2 \in K$. Hence, $(h_1h_2)(k_1k_2) \in M$, by definition of M. Therefore, $ab \in M$. Since a, b are arbitrary then $ab \in M$ for all $a, b \in M$. Thus, M is closed under $*$.

Let $e \in G$ be the identity of G. Since H and K are subgroups of G, then $e \in H$ and $e \in K$. Hence, $e * e \in M$, by definition of M. Since $e * e = e$, then $e \in M$.

Let $a \in M$. Then $a = hk$ and $h \in H$ and $k \in K$, by definition of M. Since $a \in M$ and $M \subseteq G$, then $a \in G$. Since G is a group then $a^{-1} \in G$. Observe that $a^{-1} = (hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1}$. Since $h \in H$ and H is a group then $h^{-1} \in H$. Since $k \in K$ and K is a group then $k^{-1} \in K$. Thus, $h^{-1}k^{-1} \in M$, by definition of M. Hence, $a^{-1} \in M$. Since a is arbitrary then $a^{-1} \in M$ for all $a \in M$.

Therefore, $\langle M, * \rangle$ is a subgroup of $\langle G, * \rangle$. $\square$

Proposition 25. *Let $\langle G, * \rangle$ be an abelian group. Let $H = \{a \in G : a^n = e, n \in \mathbb{Z}^+\}$. Then H is a subgroup of G.*

Solution. Our hypothesis is: $\langle G, * \rangle$ is an abelian group.

Our conclusion is: H is a subgroup of G.

We must prove: H is a subgroup of G.

To prove this we must show:

1. $H \subseteq G$.
2. H is closed under $*$.
3. $e \in H$.
4. $\forall x \in H. x^{-1} \in H$.

Note that H is simply a collection of all elements of G which have finite order. Thus, we're proving the set of all elements of an abelian group G which have finite order is a subgroup of G. $\square$

Proof. Let $e \in G$ be the identity of group G.

Observe that $H \subseteq G$.

Let $x, y \in H$. Then $x, y \in G$ and $x^m = e$ and $y^n = e$ for some $m, n \in \mathbb{Z}^+$. Since $x, y \in G$ and G is closed under $*$, then $xy \in G$. Since G is an abelian group we know $(xy)^k = x^k y^k$ for any $k \in \mathbb{Z}$. Observe that $(xy)^{mn} = x^{mn} y^{mn} = (x^m)^n y^{mn} = e^n y^{mn} = e y^{mn} = y^{mn} = y^{nm} = (y^n)^m = e^m = e$. Since $xy \in G$ and $(xy)^{mn} = e$ and $mn \in \mathbb{Z}^+$, then $xy \in H$. Since x, y are arbitrary then $xy \in H$ for all $x, y \in H$. Therefore, H is closed under $*$.

Since $e \in G$ and $e^1 = e$, then $e \in H$.

Let $x \in H$. Then $x \in G$ and $x^k = e$ for some $k \in \mathbb{Z}^+$. Since G is a group and $x \in G$, then $x^{-1} \in G$. Observe that $(x^{-1})^k = (x^k)^{-1} = e^{-1} = e$. Since $x^{-1} \in G$ and $(x^{-1})^k = e$, then $x^{-1} \in H$. Hence, for each $x \in H$, $x^{-1} \in H$.

Therefore, H is a subgroup of G. $\square$

Exercise 26. 1 is a generator of $\langle \mathbb{Z}_n, + \rangle$.

Solution. Observe that $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$. We know that $a = a \cdot 1$ for all $a \in \mathbb{Z}$. Hence, $0 = 0 \cdot 1, 1 = 1 \cdot 1, 2 = 2 \cdot 1, ...n-1 = (n-1) \cdot 1$. Thus, each element of $\mathbb{Z}_n$ is some integral multiple of $1 \in \mathbb{Z}_n$. Therefore, by definition of generator, 1 is a generator of $\mathbb{Z}_n$. Consequently, $\mathbb{Z}_n = \langle 1 \rangle = \{n \cdot 1 : n \in \mathbb{Z}\}$. Hence, $\langle \mathbb{Z}_n, + \rangle$ is cyclic. $\square$

Exercise 27. $\langle \mathbb{Q}^*, \cdot \rangle$ is not a cyclic group.

Solution. We must disprove that $\mathbb{Q}^*$ is cyclic. By definition of cyclic group $\mathbb{Q}^*$ is cyclic iff $\exists g \in \mathbb{Q}^*$ such that $\mathbb{Q}^* = \{g^n : n \in \mathbb{Z}\}$. We know $\mathbb{Q}^* = \{\frac{a}{b} : a, b \in \mathbb{Z}^*\}$. $\square$

Proof. We use proof by contradiction. Suppose $\exists g \in \mathbb{Q}^*$ such that $Q^* = \{g^n : n \in \mathbb{Z}\}$. Then $g = \frac{p}{q}$ and $p, q \in \mathbb{Z}^*$. Let $n \in \mathbb{Z}$. Either $|(\frac{p}{q})^n| < 1$ or $|(\frac{p}{q})^n| \geq 1$. There are two cases to consider.

Case 1: Suppose $|(\frac{p}{q})^n| < 1$.

Then no rational number greater than or equal to one can be represented by any power of g. For example, 2 cannot be represented by any power of g.

Case 2: Suppose $|(\frac{p}{q})^n| \geq 1$.

Then no positive rational number less than one can be represented by any power of g. For example, $\frac{1}{2}$ cannot be represented by any power of g.

Hence, in either case at least one nonzero rational number cannot be expressed as a power of g. Therefore, $g \in \mathbb{Q}^*$ cannot be a generator of $\mathbb{Q}^*$. Thus, there is no generator in $\mathbb{Q}^*$ that can generate all of $\mathbb{Q}^*$. Hence, $\langle \mathbb{Q}^*, \cdot \rangle$ is not cyclic. □

Exercise 28. A cyclic group with only one generator can have at most 2 elements.

Solution. The statement means: Let $\langle G, * \rangle$ be a cyclic group. If G has exactly one generator then G has at most 2 elements.

Let $P_1 : \langle G, * \rangle$ is a cyclic group.

Let $P_2 : G$ has exactly one generator.

Let $P_3 : |G| \leq 2$.

The statement to prove is: $P_1 \to (P_2 \to P_3)$.

We use direct proof. Thus we assume P_1.

We must prove: $P_2 \to P_3$.

We can use direct proof by assuming P_2 and proving P_3 or use proof by contrapositive and prove $\neg P_3 \to \neg P_2$. □

Proof. Let $\langle G, * \rangle$ be a cyclic group. Suppose G has exactly one generator. Let $g \in G$ be the unique generator of G. Since G is cyclic, by definition of cyclic group, $G = \langle g \rangle$.

Since G is a group, then the identity element exists. Let $e \in G$ be the identity element.

Thus, $g \in G$ and $e \in G$. Either $g = e$ or $g \neq e$.

We consider these cases separately.

There are two cases to consider.

Case 1: Suppose $g = e$.
Then $G = \langle g \rangle = \langle e \rangle$. Thus G is the trivial group, so $|G| = 1$.

Case 2: Suppose $g \neq e$.
Since G is a group, by definition of group, $g^{-1} \in G$. Either $g^{-1} = g$ or $g^{-1} \neq g$.

There are two cases to consider.

Case 2a: Suppose $g^{-1} = g$.
Then by definition of inverse element, $e = gg^{-1} = gg = g^2$. Thus $g^3 = g^2 g = eg = g$. Thus $g^4 = g^3 g = gg = e$. Thus $g^5 = g^4 g = eg = g$. Thus $g^6 = g^5 g = gg = e$, and so on.

Thus $g^{-2} = g^{-1}g^{-1} = gg = e$. Thus $g^{-3} = g^{-2}g^{-1} = eg = g$. Thus $g^{-4} = g^{-3}g^{-1} = gg = e$, and so on.

Hence, if n is even then $g^n = e$ and if n is odd then $g^n = g$. Technically we should use induction to prove that $g^n = e$ if n is even and $g^n = g$ if n is odd. Thus, $\langle g\rangle$ contains only two elements, g and e, so $|G| = |\langle g\rangle| = 2$.

Case 2b: Suppose $g^{-1} \neq g$.

Then $g^{-1} \neq e$ and $g^{-1} \neq g$. Hence, g^{-1} is some other element in G. Thus, e, g, and g^{-1} are distinct elements of G.

Hence G contains 3 elements, so $|G| > 2$.

Let $h \in G$ such that $h = g^{-1}$. Then $gh = hg = e$ and $h \neq e$ and $h \neq g$.

Thus, $G = \{e, g, h\}$.

We must determine g^2.

If $g^2 = e$, then $gg = e$ so $g^{-1} = g$. Thus, $g^{-1} = g$ and $g^{-1} \neq g$, a contradiction. Hence $g^2 \neq e$.

If $g^2 = g$, then $gg = g$. Since $eg = g = gg$, then by right cancellation law, $e = g$. Thus, $g = e$ and $g \neq e$, a contradiction. Hence, $g^2 \neq g$.

Thus, $g^2 \neq e$ and $g^2 \neq g$, so $g^2 = h$.

We must determine h^2.

If $h^2 = h$, then $hh = h$. Since $eh = h$, then $hh = eh$. Thus by right cancellation law, $h = e$. Since $h = g^{-1}$, then $g^{-1} = e$. Hence, $g^{-1} = e$ and $g^{-1} \neq e$, a contradiction. Therefore, $h^2 \neq h$.

If $h^2 = e$, then $hh = e$. Since h and g are inverses, then $hg = e$. Thus, $hh = hg$. By left cancellation law, $h = g$, so $g^{-1} = g$. Hence, $g^{-1} = g$ and $g^{-1} \neq g$, a contradiction. Therefore, $h^2 \neq e$.

Thus, $h^2 \neq h$ and $h^2 \neq e$, so $h^2 = g$.

Observe that $h^1 = h, h^2 = g, h^3 = h^2h = gh = e, h^4 = h^3h = eh = h, h^5 = hh = g, h^6 = gh = e, h^7 = eh = h, ...$ and so on. Also, $h^0 = e$ and $h^{-1} = g, h^{-2} = gg = h, h^{-3} = hg = e, h^{-4} = hh = g, h^{-5} = gg = h, h^{-6} = hg = e, ...$ and so on.

Thus, $\langle h\rangle = \{h^n : n \in \mathbb{Z}\} = G$, so h is a generator of G. Similarly, $\langle g\rangle = \{g^n : n \in \mathbb{Z}\} = G$, so g is a generator of G.

Hence, if $|G| > 2$, then G does not have a unique generator. $\square$

Proposition 29. *Let $a, b \in \mathbb{Z}^+$. The set of all linear combinations of a and b under addition is a cyclic group.*

Solution. Let $a, b \in \mathbb{Z}^+$. Let $S = \{ma + nb : m, n \in \mathbb{Z}\}$. We must prove $\langle S, +\rangle$ is a group.

We know that $S \subseteq \mathbb{Z}$ since $ma + nb \in \mathbb{Z}$. We know that $\langle \mathbb{Z}, +\rangle$ is a group.

Thus we can prove S is a subgroup of $\mathbb{Z}$ by proving:

1. $S \subseteq \mathbb{Z}$
2. S is closed under $+$.
3. $0 \in S$.
4. each $s \in S$ has an inverse $s^{-1} \in S$.

To prove 2) we must prove:

2a. $\forall r, s \in S. r + s \in S$.

To prove 4 we must prove:

4a. $\forall s \in S. -s \in S$.

We further prove S is cyclic. $\square$

Proof. Let $a, b \in \mathbb{Z}^+$. Let $S = \{ma + nb : m, n \in \mathbb{Z}\}$.

Suppose $s \in S$. Then $s = ma + nb$ and $m, n \in \mathbb{Z}$. Since $a, b \in \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{Z}$ then $a, b \in \mathbb{Z}$. Since $a, b, m, n \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under addition and multiplication, then $ma + nb \in \mathbb{Z}$. Hence, $s \in \mathbb{Z}$. Thus, $s \in S$ implies $s \in \mathbb{Z}$. Since s is arbitrary then $s \in S$ implies $s \in \mathbb{Z}$ for all $s \in S$. Therefore, by definition of subset, $S \subseteq \mathbb{Z}$.

Suppose $r, s \in S$. Then $r = m_1a + n_1b$ and $s = m_2a + n_2b$ and $m_1, m_2, n_1, n_2 \in \mathbb{Z}$. Since $m, m_2, n_1, n_2, a, b \in \mathbb{Z}$ and $\langle \mathbb{Z}, +, \cdot \rangle$ is a ring then $r + s = (m_1a + n_1b) + (m_2a + n_2b) = m_1a + (n_1b + m_2a) + n_2b = m_1a + (m_2a + n_1b) + n_2b = (m_1a + m_2a) + (n_1b + n_2b) = (m_1 + m_2)a + (n_1 + n_2)b$. Set $m_3 = m_1 + m_2$ and $n_3 = n_1 + n_2$. Since $\mathbb{Z}$ is closed under addition then $m_3, n_3 \in \mathbb{Z}$. By definition of S, $m_3a + n_3b \in S$. Since $r + s = m_3a + n_3b$ then $r + s \in S$. Since r, s are arbitrary then $r + s \in S$ for all $r, s \in S$. Hence, S is closed under $+$.

We know $0 \in \mathbb{Z}$ is the additive identity of group $\langle \mathbb{Z}, + \rangle$. Since $0 = 0(a+b) = 0a + 0b$, then $0 \in S$, by definition of S.

Suppose $s \in S$. Then $s = ma + nb$ and $m, n \in \mathbb{Z}$. Since $S \subseteq \mathbb{Z}$ then $s \in \mathbb{Z}$. Since $\langle \mathbb{Z}, + \rangle$ is a group we know the additive inverse of s is $-s \in \mathbb{Z}$. Set $t = -s$. Then $t \in \mathbb{Z}$ and $t = -(ma + nb) = -ma - nb = (-m)a + (-n)b$. Since $\langle \mathbb{Z}, + \rangle$ is a group and $m, n \in \mathbb{Z}$, then by definition of group, $-m, -n \in \mathbb{Z}$. Hence, by definition of S, $(-m)a + (-n)b \in S$. Thus, $t \in S$, so $-s \in S$. Since s is arbitrary then $-s \in S$ for all $s \in S$. Therefore, each element of S has an additive inverse in S.

Therefore $\langle S, + \rangle$ is a subgroup of $\langle \mathbb{Z}, + \rangle$.

Every subgroup of a cyclic group is cyclic. Since $\langle \mathbb{Z}, + \rangle$ is a cyclic group and $\langle S, + \rangle$ is a subgroup of $\langle \mathbb{Z}, + \rangle$, then $\langle S, + \rangle$ is cyclic.

Every cyclic group is abelian and $\langle S, + \rangle$ is cyclic. Therefore, $\langle S, + \rangle$ is abelian. $\square$

Proof. Let $a, b \in \mathbb{Z}^+$. Let $S = \{ma + nb : m, n \in \mathbb{Z}\}$. Since $\langle S, + \rangle$ is a cyclic group we show that $\gcd(a, b)$ is a generator of S.

Let $d = \gcd(a, b)$. We prove $d \in S$ and $S = \langle d \rangle = \{td : t \in \mathbb{Z}\}$.

Since $d = \gcd(a, b)$ then we know d is the least positive linear combination of a and b. Thus, $d = k_1a + k_2b$ for some $k_1, k_2 \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. By definition of $S, d \in S$.

We prove $S \subseteq \langle d \rangle$. Let $x \in S$. Then $x = ma + nb$ and $m, n \in \mathbb{Z}$. Since $d = \gcd(a, b)$ then $d|a$ and $d|b$, by definition of gcd. Hence, by definition of divisibility, $a = dq_1$ and $b = dq_2$ for some $q_1, q_2 \in \mathbb{Z}$. Observe that $x = m(dq_1) + n(dq_2) = (md)q_1 + (nd)q_2 = (dm)q_1 + (dn)q_2 = d(mq_1) + d(nq_2) = d(mq_1 + nq_2)$. Set $s = mq_1 + nq_2$. Then $x = ds = sd$. Since $m, n, q_1, q_2 \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under $+$ and $\cdot$ then $s \in \mathbb{Z}$. Since $x = sd$ and $s \in \mathbb{Z}$ then $x \in \langle d \rangle$, by definition of $\langle d \rangle$. Thus $x \in S$ implies $x \in \langle d \rangle$. Since x is arbitrary then $x \in S$ implies $x \in \langle d \rangle$ for all $x \in S$. Hence, $S \subseteq \langle d \rangle$.

We prove $\langle d \rangle \subseteq S$. Let $y \in \langle d \rangle$. Then $y = td$ and $t \in \mathbb{Z}$. Observe that $y = t(k_1a + k_2b) = tk_1a + tk_2b = (tk_1)a + (tk_2)b$. Since $tk_1, tk_2 \in \mathbb{Z}$ then $y \in S$, by definition of S. Thus $y \in \langle d \rangle$ implies $y \in S$. Since y is arbitrary then $y \in \langle d \rangle$ implies $y \in S$ for all $y \in \langle d \rangle$. Hence, $\langle d \rangle \subseteq S$.

Since $S \subseteq \langle d \rangle$ and $\langle d \rangle \subseteq S$ then $S = \langle d \rangle$. Since $d \in S$ and $S = \langle d \rangle = \{td : t \in \mathbb{Z}\}$, then d is a generator of S. $\square$

Proposition 30. *Let $\langle G, *, \cdot \rangle$ be a group. Let $a \in G$. If order(a) $= n$, then order(a^{-1}) $= n$.*

Proof. Suppose order(a) $= n$. Then $a^n = e$ and $n \in \mathbb{Z}^+$ by definition of finite order of an element. We know order $(a^{-1}) = n$ if $\gcd(-1, n) = 1$. The only positive divisor of -1 is 1 since $-1 = 1 * (-1)$. The set of divisors of n includes 1. Hence the set of common divisors of -1 and n is $\{1\}$. Therefore, the greatest common divisor of -1 and n is 1. Hence, $\gcd(-1, n) = 1$. Thus, order$(a^{-1}) = n$. $\square$

Proposition 31. *A cycle of length k in S_n has order k for all integers $n > 1$.*

Solution. We could use induction, but the proof leads nowhere, so we need to try another approach. Try using the definition of order of an element of a group.

Let S_n be the symmetric group and let $\sigma \in S_n$ be a cycle of length k. The longest cycle occurs when $k = n$ and the shortest cycle length is $k = 2$. Hence, $2 \leq k \leq n$.

To prove k is the order of σ, we must prove:
1. k satisfies $\sigma^x = e$ where $x \in \mathbb{Z}^+$.
2. $\neg(\exists m \in \mathbb{Z}^+)(m < k \wedge \sigma^m = e)$.

$\square$

Proof. Let n be an arbitrary integer greater than 1. Let σ be an arbitrary permutation of S_n. Let k be a positive integer. Suppose σ is a cycle of length k. Since the shortest cycle length is 2 and the longest cycle length in S_n is n, then $2 \leq k \leq n$.

We must prove k is the order of σ. Since σ is a cycle, then $\sigma = (1, 2, ..., k)$. Consider σ^k. In σ^k, each number i in σ is mapped k times repeatedly so that i maps back to itself. Hence, $\sigma^k(i) = i$ for each $i \in \{1, 2, ..., k\}$ so $\sigma^k = id$, where id is the identity permutation of S_n.

Suppose there is some positive integer m less than k such that $\sigma^m = id$. Then $\sigma^m(1) = 1$.

But $m < k$, so σ^m maps 1 to some element other than 1 because 1 never fully travels the entire cycle back to 1. Hence, $\sigma^m(1) \neq 1$. Thus, we have a contradiction that σ^m maps 1 to both 1 and to a number not equal to one. Therefore, there is no positive integer $m < k$ such that $\sigma^m = id$. $\square$

Proposition 32. *If $n > 2$, then S_n is nonabelian.*

Solution. We try various approaches and examples. If $n = 1$, then S_1 is isomorphic to the trivial group which is known to be abelian. If $n = 2$, then S_2 is isomorphic to $(\mathbb{Z}_2, +)$ which is a cyclic group and is therefore abelian. Hence, S_2 must be abelian. We know S_3 is nonabelian.

We must prove $(\forall n > 2)(S_n$ is nonabelian). We could try proof by induction, but that leads into difficulties. $\square$

Proof. Let n be an arbitrary integer greater than 2. Suppose S_n is abelian. Then $\sigma\tau = \tau\sigma$ for every pair of permutations $\sigma, \tau \in S_n$.

Since $n > 2$, then each permutation in S_n contains the transpositions $(1, 2)$ and $(1, 3)$. These transpositions may be regarded as elements of S_n since they each hold fixed any element in S_n that is greater than 3.

So, let $\sigma = (1, 2)$ and $\tau = (1, 3)$. Then $\sigma\tau = (1, 2)(1, 3) = (1, 3, 2) \neq (1, 2, 3) = (1, 3)(1, 2) = \tau\sigma$.

Therefore, there exist a pair of elements in S_n that do not commute. Hence, S_n is not abelian. □

Exercise 33. If G is a finite group with an element g of order 5 and an element h of order 7, then $|G| \geq 35$.

Solution. The hypothesis is:

G is a finite group.

$g, h \in G$ such that $|g| = 5$ and $|h| = 7$.

We must prove $|G| \geq 35$. □

Proof. Since G is a finite group, then the order of G is some positive integer, say n. We must prove $n \geq 35$.

Every element of a finite group has finite order. Moreover, the order of an element of a finite group divides the order of the group. Hence, $|g|$ divides n and $|h|$ divides n. Thus, $5|n$ and $7|n$, so n is a multiple of 5 and 7. Therefore, n is a multiple of 35. The least positive multiple of 35 is the least common multiple of 35, namely 35. Therefore, $n \geq 35$. □

Proposition 34. *Let H be a subgroup of G such that $[G : H] = 2$. If a and b are not in H, then $ab \in H$.*

Solution. We must prove $(\forall a, b \in G)(a \notin H \land b \notin H \to ab \in H)$.

□

Proof. Let $a, b \in G$ such that $a \notin H$ and $b \notin H$. Since $[G : H] = 2$, then there are two distinct left cosets of H in G. Since $e \in G$, then $eH = H$. Thus, one of the left cosets is H. Since $a \in aH$ and $a \notin H$, then $aH \neq H$. Since aH is a left coset and $aH \neq H$ and there are exactly two left cosets of H in G, then aH is the other left coset.

Let L_H be the collection of all left cosets of H in G. Then L_H is a partition of G and $L_H = \{H, aH\}$. Every element of G exists in exactly one left coset of H in G. Hence, every element of G is in either H or in aH. Since $a, b \in G$ and G is a group, then $ab \in G$.

Suppose $ab \notin H$. Then $ab \in aH$. Thus, there exists $h \in H$ such that $ab = ah$. By the left cancellation law we obtain $b = h$. Since $b = h$ and $h \in H$, then $b \in H$. Thus, we have $b \notin H$ and $b \in H$, a contradiction. Therefore, $ab \in H$. □

Exercise 35. Let H be a subgroup of G such that $[G : H] = 2$. Then $gH = Hg$ for all $g \in G$.

Solution. We must prove $(\forall g \in G)(gH = Hg)$. $\square$

Proof. Let $g \in G$. Since $[G : H] = 2$, then there are two distinct left cosets of H in G and there are two distinct right cosets of H in G. Since $e \in G$, then $eH = H$ is a left coset and $He = H$ is a right coset. Since $g \in G$, then gH is a left coset and Hg is a right coset.

Either $g \in H$ or $g \notin H$.

We consider these cases separately.

Case 1: Suppose $g \in H$.

Since $g \in gH$ and $g \in eH = H$, then g is in two left cosets. Every element of G lies in exactly one left coset. Thus, $gH = H$.

Since $g \in Hg$ and $g \in He = H$, then g is in two right cosets. Every element of G lies in exactly one right coset. Thus, $Hg = H$.

Therefore, $gH = H = Hg$, so $gH = Hg$.

Case 2: Suppose $g \notin H$.

Since $g \in gH$ and $g \notin H$, then $gH \neq H$. Thus, H and gH are distinct left cosets of H in G, so $L_H = \{H, gH\}$ is a partition of G.

Since $g \in Hg$ and $g \notin H$, then $Hg \neq H$. Thus, H and Hg are distinct right cosets of H in G, so $R_H = \{H, Hg\}$ is a partition of G.

We prove $gH = Hg$. Let $x \in gH$. Since $x \in gH$ and $gH \subset G$, then $x \in G$. Every element of G lies in exactly one left coset. Thus, since $x \in gH$, then $x \notin eH = H$. Every element of G lies in exactly one right coset. Thus, since $x \notin H$, then $x \in Hg$. Therefore, $x \in gH$ implies $x \in Hg$, so $gH \subset Hg$.

Let $y \in Hg$. Since $y \in Hg$ and $Hg \subset G$, then $y \in G$. Every element of G lies in exactly one right coset. Thus, since $y \in Hg$, then $y \notin He = H$. Every element of G lies in exactly one left coset. Thus, since $y \notin H$, then $y \in gH$. Therefore, $y \in Hg$ implies $y \in gH$, so $Hg \subset gH$.

Since $gH \subset Hg$ and $Hg \subset gH$, then $gH = Hg$.

Since $gH = Hg$ for all $g \in G$, then H is normal in G, so $H \lhd G$. $\square$

Proposition 36. *If H is a subgroup of a cyclic group G, then $\frac{G}{H}$ is cyclic.*

Proof. Suppose H is a subgroup of a cyclic group G. Every cyclic group is abelian. Since G is cyclic, then G is abelian. Every subgroup of an abelian group is normal. Since H is a subgroup of G and G is abelian, then H is normal. Therefore, $\frac{G}{H}$ is a group and $\frac{G}{H} = \{aH : a \in G\}$.

Since G is cyclic, then there exists $g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\}$. Since $g \in G$, then $gH \in \frac{G}{H}$. Let T be the cyclic group generated by gH. Then $T = \{(gH)^n : n \in \mathbb{Z}\}$.

Let $x \in \frac{G}{H}$. Then there exists $a \in G$ such that $x = aH$.

Since $a \in G$, then $a = g^n$ for some integer n. Therefore, $x = g^n H = (g * g * ... * g)H = (gH)(gH)...(gH) = (gH)^n$. Since n is an integer and $x = (gH)^n$, then $x \in T$. Hence, $x \in \frac{G}{H}$ implies $x \in T$, so $\frac{G}{H} \subset T$.

Let $y \in T$. Then there exists an integer m such that $y = (gH)^m$. Thus, $y = (gH)(gH)...(gH) = (gg...g)H = (g^m)H$. Since $g^m \in G$, then $y = (g^m)H \in \frac{G}{H}$. Thus, $y \in T$ implies $y \in \frac{G}{H}$, so $T \subset \frac{G}{H}$.

Since $\frac{G}{H} \subset T$ and $T \subset \frac{G}{H}$, then $\frac{G}{H} = T$. Thus, $\frac{G}{H} = \{(gH)^n : n \in \mathbb{Z}\}$. Since there exists $gH \in \frac{G}{H}$ such that $\frac{G}{H} = \{(gH)^n : n \in \mathbb{Z}\}$, then $\frac{G}{H}$ is cyclic. $\square$

Proposition 37. *Let G be a group. Let $g \in G$. Let $C(g) = \{x \in G : xg = gx\}$. Then $C(g)$ is a subgroup of G (called the* ***centralizer of*** *g). If g generates a normal subgroup of G, then $C(g)$ is normal in G.*

Proof. Observe that $C(g)$ is a subset of G. Let $a, b \in C(g)$. Then $a \in G$ and $ag = ga$ and $b \in G$ and $bg = gb$. We right multiply $ag = ga$ by b to get $agb = gab$. We left multiply $bg = gb$ by a to get $abg = agb$. Thus, $gab = agb = abg$, so $abg = gab$. Since G is a group and $a, b \in G$, then $ab \in G$. Since $ab \in G$ and $(ab)g = g(ab)$, then $ab \in C(g)$. Therefore, $C(g)$ is closed under the binary operation $*$.

Let e be the identity of G. Then $e \in G$ and $eg = g = ge$. Since $e \in G$ and $eg = ge$, then $e \in C(g)$.

Let $a \in C(g)$. Then $a \in G$ and $ag = ga$. Left multiply by a^{-1} to get $a^{-1}ag = a^{-1}ga$. Thus, $g = a^{-1}ga$. Right multiply by a^{-1} to get $ga^{-1} = a^{-1}gaa^{-1}$. Thus, $ga^{-1} = a^{-1}g$. Since $a^{-1} \in G$ and $a^{-1}g = ga^{-1}$, then $a^{-1} \in C(g)$.

Thus, $C(g)$ is a subgroup of G.

Suppose $\langle g \rangle$ is normal in G. Let $H = \langle g \rangle$. Then for all $g_1 \in G$ and all $h \in H$, $g_1 h g_1^{-1} \in H$.

To prove $C(g)$ is normal in G, we prove for all $g_1 \in G$ and all $h \in C(g)$, $g_1 h g_1^{-1} \in C(g)$. Let $g_1 \in G$ and $h \in C(g)$. Since $h \in C(g)$, then $h \in G$ and $hg = gh$. Let $x = g_1 h g_1^{-1}$. To prove $x \in C(g)$, we must prove $x \in G$ and $xg = gx$. Since $g_1, g_1^{-1}, h \in G$ and G is a group, then $x \in G$.

We must prove $xg = gx$. Since $x = g_1 h g_1^{-1}$ and H is normal in G, then $g_1 h g_1^{-1} \in H$, so $x \in H$.

$\square$

Exercise 38. $(\mathbb{Z}_6, +) \ncong (S_3, \circ)$.

Solution. We know that $|\mathbb{Z}_6| = 6$ and $|S_3| = 3! = 6$, but $\mathbb{Z}_6$ is abelian group, while S_3 is nonabelian. Thus, we conjecture that there does not exist an isomorphism. To prove this, let's suppose there does exist an isomorphism and derive a contradiction. $\square$

Proof. Suppose $\mathbb{Z}_6$ is isomorphic to S_3. Then there exists an isomorphism between $\mathbb{Z}_6$ and S_3.

Let $\phi : \mathbb{Z}_6 \mapsto S_3$ be some isomorphism. Then ϕ is a bijective homomorphism. Since ϕ is a homomorphism, then for every $[a], [b] \in \mathbb{Z}_6$, $\phi([a]+[b]) = \phi([a])\phi([b])$. Since S_3 is non abelian, then $\circ$ is not commutative. Therefore, there exist $\sigma, \tau \in S_3$ such that $\sigma\tau \neq \tau\sigma$. Since $\mathbb{Z}_6$ is abelian, then for every $[a], [b] \in \mathbb{Z}_6$, $[a] + [b] = [b] + [a]$.

Since ϕ is bijective, then ϕ is surjective. Therefore, since $\sigma \in S_3$, then there exists $[a] \in \mathbb{Z}_6$ such that $\phi([a]) = \sigma$. Similarly, since $\tau \in S_3$, then there exists $[b] \in \mathbb{Z}_6$ such that $\phi([b]) = \tau$.

Observe that $\sigma\tau = \phi([a])\phi([b]) = \phi([a] + [b]) = \phi([b] + [a]) = \phi([b])\phi([a]) = \tau\sigma$. Hence, we have $\sigma\tau = \tau\sigma$ and $\sigma\tau \neq \tau\sigma$, a contradiction.

Therefore, there is no isomorphism ϕ. Since no isomorphism exists between $\mathbb{Z}_6$ and S_3, then $\mathbb{Z}_6$ is not isomorphic to S_3. $\square$

Proposition 39. *$\langle \mathbb{Z}, +, \cdot \rangle$ is a ring.*

Proof. We know $\langle \mathbb{Z}, + \rangle$ is an abelian group. We know $\mathbb{Z}$ is closed under multiplication and $ab \in \mathbb{Z}$ is unique for all $a, b \in \mathbb{Z}$. Therefore, multiplication is a binary operation on $\mathbb{Z}$. Also, multiplication of integers is associative so $a(bc) = (ab)c$ for all $a, b, c \in \mathbb{Z}$. We know multiplication is distributive over addition. Thus, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in \mathbb{Z}$. $\square$

Fields

Exercise 40. Let $S = \{a, b\}$. Define addition on S by $a + a = a$ and $a + b = b = b + a$ and $b + b = b$. Define multiplication on S by $aa = ab = ba = a$ and $bb = b$. Then $(S, +, *)$ is a field.

Solution. To prove S is a field, we must prove S is a commutative division ring. Thus, we must prove $(S, +, *)$ is a ring with $1 \neq 0$ and $*$ is commutative and every nonzero element of S has a multiplicative inverse. Hence, we must prove

1. $(S, +)$ is an abelian group.
1a. addition is a binary operation on S.
1a1. S is closed under addition.
1a2. $x + y$ is unique for all $x, y \in S$.
1b. $+$ is associative.
1c. $+$ is commutative.
1d. there exists an additive identity in S.
1e. each element of S has an additive inverse.
2. multiplication is a binary operation on S.
2a1. S is closed under multiplication.
2a2. xy is unique for all $x, y \in S$.
2. $*$ is associative.
3. there exists a multiplicative identity 1
4. multiplication distributes over addition:
4a. left distributive : $a(b + c) = ab + ac$
4b. right distributive: $(a + b)c = ac + bc$.
5. $1 \neq 0$.
6. $*$ is commutative.
7. every nonzero element of S has a multiplicative inverse.

We can write out the addition and multiplication tables for S. Since $|S| = 2$, then $|S \times S| = |S||S| = 2 * 2 = 2^2 = 4$. Thus, there are 4 ordered pairs mapped by addition and mapped by multiplication.

$\square$

Proof. The sum of any pair of elements of S is a unique element of S. Hence, addition is a binary operation on S.

Since $a + b = b = b + a$, then addition is commutative.

We prove addition is associative.

There are $2^3 = 8$ cases to consider.

Case 1: Observe that $(a + a) + a = a + a = a + (a + a)$.

Case 2: Observe that $(a + a) + b = a + b = a + (a + b)$.

Case 3: Observe that $(a + b) + a = b + a = b = a + b = a + (b + a)$.

Case 4: Observe that $(a + b) + b = b + b = a = a + a = a + (b + b)$.

Case 5: Observe that $(b + a) + a = b + a = b + (a + a)$.

Case 6: Observe that $(b + a) + b = b + b = b + (a + b)$.

Case 7: Observe that $(b + b) + a = a + a = a = b + b = b + (b + a)$.

Case 8: Observe that $(b + b) + b = a + b = b = b + a = b + (b + b)$.

Thus, addition is associative.

Since $a + a = a$ and $a + b = b = b + a$, then a is an additive identity. Thus, a is a zero element of S.

Since $a + a = a$, then a is an additive inverse of a. Since $b + b = a$, then b is an additive inverse of b. Hence, each element of S has an additive inverse.

Therefore, $(S, +)$ is an abelian group.

The product of any pair of elements of S is a unique element of S. Hence, multiplication is a binary operation on S.

Since $ab = a = ba$, then multiplication is commutative.

We prove multiplication is associative.

There are $2^3 = 8$ cases to consider.

Case 1: Observe that $(aa)a = aa = a(aa)$.

Case 2: Observe that $(aa)b = ab = a = aa = a(ab)$.

Case 3: Observe that $(ab)a = aa = a(ba)$.

Case 4: Observe that $(ab)b = ab = a(bb)$.

Case 5: Observe that $(ba)a = aa = a = ba = b(aa)$.

Case 6: Observe that $(ba)b = ab = a = ba = b(ab)$.

Case 7: Observe that $(bb)a = ba = b(ba)$.

Case 8: Observe that $(bb)b = bb = b(bb)$.

Thus, multiplication is associative.

Since $ba = a = ab$ and $bb = b$, then b is a multiplicative identity. Since $a \neq b$, then the multiplicative identity is distinct from the additive identity. The only nonzero element in S is b. Since $bb = b$, then the multiplicative inverse of b is b. Hence, every nonzero element of S has a multiplicative inverse.

We prove the left distributive law holds in S.

There are $2^3 = 8$ cases to consider.

Case 1: Observe that $a(a + a) = aa = a = a + a = aa + aa$.

Case 2: Observe that $a(a + b) = ab = a = a + a = aa + ab$.

Case 3: Observe that $a(b + a) = ab = a = a + a = ab + aa$.

Case 4: Observe that $a(b + b) = aa = a = a + a = ab + ab$.

Case 5: Observe that $b(a + a) = ba = a = a + a = ba + ba$.

Case 6: Observe that $b(a + b) = bb = b = a + b = ba + bb$.

Case 7: Observe that $b(b + a) = bb = b = b + a = bb + ba$.

Case 8: Observe that $b(b+b) = ba = a = b+b = bb+bb$.

Thus, the left distributive law holds in S.

Let $x, y, z \in S$. Then $(x+y)z = z(x+y) = zx + zy = xz + yz$. Thus, the right distributive law holds in S. Hence, multiplication is distributive over addition in S.

Therefore, $(S, +, *)$ is a field. $\square$

Proof. Define $\phi : \mathbb{Z}_2 \to S$ by $\phi(0) = a$ and $\phi(1) = b$.

Clearly, ϕ is a function and ϕ is injective and surjective. Hence, ϕ is bijective.

We prove ϕ is a ring homomorphism. Observe that $\phi(0+0) = \phi(0) = a = a+a = \phi(0)+\phi(0)$ and $\phi(0+1) = \phi(1) = b = a+b = \phi(0)+\phi(1)$ and $\phi(1+0) = \phi(1) = b = b+a = \phi(1)+\phi(0)$ and $\phi(1+1) = \phi(0) = a = b+b = \phi(1)+\phi(1)$. Thus, ϕ preserves addition.

Observe that $\phi(0*0) = \phi(0) = a = aa = \phi(0)\phi(0)$ and $\phi(0*1) = \phi(0) = a = ab = \phi(0)\phi(1)$ and $\phi(1*0) = \phi(0) = a = ba = \phi(1)\phi(0)$ and $\phi(1*1) = \phi(1) = b = bb = \phi(1)\phi(1)$. Thus, ϕ preserves multiplication.

Since $\phi(1) = b$ and 1 is unity of $\mathbb{Z}_2$ and b is unity of S, then ϕ preserves the unity element of the rings.

Therefore, ϕ is a ring homomorphism. Since ϕ is bijective, then ϕ is a bijective ring homomorphism, so ϕ is a ring isomorphism. Hence, $(\mathbb{Z}_2, +, *) \cong (S, +, *)$. Since 2 is prime, then $\mathbb{Z}_2$ is a field. Hence, S is a field. $\square$

Exercise 41. Let $(F, +, *)$ be a field. Then $(x+1)^2 = x^2 + 2x + 1$ for all $x \in F$.

Proof. Let $x \in F$. Let 1 be the unity of F. Define $2 = 1+1$ and $2x = x+x$ and $x^2 = x * x$ for all $x \in F$. Then

$$\begin{aligned}
(x+1)^2 &= (x+1)(x+1) \\
&= (x+1)x + (x+1)*1 \\
&= (x*x + 1*x) + (x+1) \\
&= (x*x + x) + (x+1) \\
&= x*x + (x+x) + 1 \\
&= x^2 + 2x + 1.
\end{aligned}$$

$\square$