ALGEBRA- I(Introduction)

G. Kalaimurugan

Department of Mathematics

Thiruvalluvar University, Vellore -632 115.

March 9, 2020

Definition

Definition

1. A binary operation $\star$ on a set G is a function $\star : G \times G \longrightarrow G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$

Definition

1. A binary operation $\star$ on a set G is a function $\star : G \times G \longrightarrow G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$
2. A binary operation $\star$ on a set G is associative if for all $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.

Definition

1. A binary operation $\star$ on a set G is a function $\star : G \times G \longrightarrow G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$
2. A binary operation $\star$ on a set G is associative if for all $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.
3. If $\star$ is a binary operation on a set G we say elements a and b of G commute if $a \star b = b \star a$. We say $\star(orG)$ is commutative if for all $a, b \in G, a \star b = b \star a$.

Definition

Definition

1. A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

Definition

1. A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
   - $(a \star b) \star c = a \star (b \star c)$, for all $a, b, c \in G$, i.e., $\star$ is associative,

Definition

1. A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
   - $(a \star b) \star c = a \star (b \star c)$, for all $a, b, c \in G$, i.e., $\star$ is associative,
   - there exists an element e in G, called an identity of G, such that for all $a \in G$ we have $a \star e = e \star a = a$,

Definition

1. A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
   - $(a \star b) \star c = a \star (b \star c)$, for all $a, b, c \in G$, i.e., $\star$ is associative,
   - there exists an element e in G, called an identity of G, such that for all $a \in G$ we have $a \star e = e \star a = a$,
   - for each $a \in G$ there is an element a^{-1} of G, called an inverse of a, such that $a \star a^{-1} = a^{-1} \star a = e$

Definition

1. A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
   - $(a \star b) \star c = a \star (b \star c)$, for all $a, b, c \in G$, i.e., $\star$ is associative,
   - there exists an element e in G, called an identity of G, such that for all $a \in G$ we have $a \star e = e \star a = a$,
   - for each $a \in G$ there is an element a^{-1} of G, called an inverse of a, such that $a \star a^{-1} = a^{-1} \star a = e$
2. The group $(G, \star)$ i s called abelian (or commutative) if $a \star b = b \star a$ for all $a, b \in G$.

Proposition

If G is a group under the operation $\star$, then

Proposition

If G is a group under the operation $\star$, then

1. *the identity of G is unique*

Proposition

If G is a group under the operation $\star$, then

1. *the identity of G is unique*
2. *for each $a \in G, a^{-1}$ is uniquely determined*

Proposition

If G is a group under the operation $\star$, then

1. *the identity of G is unique*
2. *for each $a \in G, a^{-1}$ is uniquely determined*
3. *$(a^{-1})^{-1} = a$ for all $a \in G$*

Proposition

If G is a group under the operation $\star$, then

1. *the identity of G is unique*
2. *for each $a \in G, a^{-1}$ is uniquely determined*
3. $(a^{-1})^{-1} = a$ *for all* $a \in G$
4. $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$

Proposition

If G is a group under the operation $\star$, then

1. *the identity of G is unique*
2. *for each $a \in G, a^{-1}$ is uniquely determined*
3. *$(a^{-1})^{-1} = a$ for all $a \in G$*
4. *$(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$*
5. *for any $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 \star a_2 \star \ldots \star a_n$ is independent of how the expression is bracketed (this is called the generalized associative law).*

Definition

For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.

A presentation for the dihedral group D_{2n} (using the generators and relations) is then $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Definition

For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.

A presentation for the dihedral group D_{2n} (using the generators and relations) is then $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Remark

Definition

For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.

A presentation for the dihedral group D_{2n} (using the generators and relations) is then $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Remark

- $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$

Definition

For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.

A presentation for the dihedral group D_{2n} (using the generators and relations) is then $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Remark

- $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$
- $|s| = 2$.

Definition

For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.

A presentation for the dihedral group D_{2n} (using the generators and relations) is then $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Remark

- $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$
- $|s| = 2$.
- $s \neq r^i$ for any i

Definition

For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.

A presentation for the dihedral group D_{2n} (using the generators and relations) is then $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Remark

- $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$
- $|s| = 2$.
- $s \neq r^i$ for any i
- $sr^i \neq sr^j$, for all $0 \leq i, j \leq n-1$ with $i \neq j$, so $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$

Definition

For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.

A presentation for the dihedral group D_{2n} (using the generators and relations) is then

$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Remark

- $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$
- $|s| = 2$.
- $s \neq r^i$ for any i
- $sr^i \neq sr^j$, for all $0 \leq i, j \leq n-1$ with $i \neq j$, so

  $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$
- $r^i s = sr^{-i}$, for all $0 \leq i \leq n$.

Problem

Compute the order of each of the elements in the following groups: (a) D_6 (b) D_8 (c) D_{10}.

Problem

Compute the order of each of the elements in the following groups: (a) D_6 (b) D_8 (c) D_{10}.

Solution

Recall that every element of D_{2n} can be represented uniquely as $s^i r^j$ for some $i = 0, 1$ and $0 \leq j < n$. Moreover, $r^i s = sr^{-i}$ for all $0 \leq i \leq n$. From this we deduce that $(sr^i)(sr^i) = ssr^{-i}r^i = 1$, so that sr^i has order 2 for $0 \leq i \leq n$ (a)

$D_6 = \{1, r, r^2, s, sr, sr^2\}$, Let the order of an element α is denoted by $|\alpha|$. Then $|1| = 1, |r| = 3, |r^2| = 3, |s| = |sr| = |sr^2| = 2$. (b)In D_8,

$|1| = 1, |r| = 4, |r^2| = 2, |r^3| = 4, |s| = |sr| = |sr^2| = |sr^3| = 2$. (c) In D_{10},

$|1| = 1, |r| = |r^2| = |r^3| = |r^4| = 5, |s| = |sr| = |sr^2| = |sr^3| = |sr^4| = 2$.

Problem

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

Problem

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

Solution

Every element $x \in D_{2n}$ is of the form $x = s^i r^j$ where $i = 0, 1$ and $0 \leq j < n$. If $i = 0$ we have that x is a power of r; thus $x = sr^j$ for some $0 \leq j < n$. Hence

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

Problem

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

Solution

Every element $x \in D_{2n}$ is of the form $x = s^i r^j$ where $i = 0, 1$ and $0 \leq j < n$. If $i = 0$ we have that x is a power of r; thus $x = sr^j$ for some $0 \leq j < n$. Hence

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

Problem

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

Problem

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

Solution

Every element $x \in D_{2n}$ is of the form $x = s^i r^j$ where $i = 0, 1$ and $0 \leq j < n$. If $i = 0$ we have that x is a power of r; thus $x = sr^j$ for some $0 \leq j < n$. Hence

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

Problem

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

Solution

We have $xt^{-1} = x(xy)^{-1} = xy^{-1}x^{-1} = xyx = tx$ since x and y have order 2.

Problem

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

Problem

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

Solution

We know that $|r| = n$. Thus, the elements of subgroup A are precisely $1, r, r^2, \ldots, r^{n-1}$;

thus $|A| = n$

Definition

Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\phi : G \to H$ such that $\phi(x \star y) = \phi(x) \diamond \phi(y)$ for all $x, y \in G$, is called a *homomorphism*.

Definition

Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\phi : G \to H$ such that $\phi(x \star y) = \phi(x) \diamond \phi(y)$ for all $x, y \in G$, is called a *homomorphism*.

Definition

The map $\varphi : G \to H$ is called an isomorphism and G and H are said to be *isomorphic* or of the same *isomorphism type*, written $G \cong H$, if

Definition

Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\phi : G \to H$ such that $\phi(x \star y) = \phi(x) \diamond \phi(y)$ for all $x, y \in G$, is called a *homomorphism*.

Definition

The map $\varphi : G \to H$ is called an isomorphism and G and H are said to be *isomorphic* or of the same *isomorphism type*, written $G \cong H$, if

1. φ is a homomorphism (i.e.,$\varphi(xy) = \varphi(x)\varphi(y)$), and

Definition

Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\phi : G \to H$ such that $\phi(x \star y) = \phi(x) \diamond \phi(y)$ for all $x, y \in G$, is called a *homomorphism*.

Definition

The map $\varphi : G \to H$ is called an isomorphism and G and H are said to be *isomorphic* or of the same *isomorphism type*, written $G \cong H$, if

1. φ is a homomorphism (i.e.,$\varphi(xy) = \varphi(x)\varphi(y)$), and
2. φ is a bijection.

Let G and H be groups. Solve the following problems.

Problem

Let $\varphi : G \to H$ be a homomorphism. (a) Prove that $\varphi(xn) = \varphi(x)n$ for all $n \in \mathbb{Z}^+$. (b) Do part (a) for $n = -1$ and deduce that $\varphi(xn) = \varphi(x)n$ for all $n \in \mathbb{Z}$.

Let G and H be groups. Solve the following problems.

Problem

Let $\varphi : G \to H$ be a homomorphism. (a) Prove that $\varphi(xn) = \varphi(x)n$ for all $n \in \mathbb{Z}^+$. (b) Do part (a) for $n = -1$ and deduce that $\varphi(xn) = \varphi(x)n$ for all $n \in \mathbb{Z}$.

Solution

(a) We proceed by induction on n. For the base case, $\varphi(x^1) = \varphi(x) = \varphi(x)^1$. Suppose the statement holds for some $n \in \mathbb{Z}^+$; then

$\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = \varphi(x)^n\varphi(x) = \varphi(x)^{n+1}$, so the statement holds for $n + 1$. By induction, $\varphi(x^n) = \varphi(x)^n foralln \in \mathbb{Z}^+$.

(b)First, note that $\varphi(x) = \varphi(1_G \cdot x) = \varphi(1_G) \cdot \varphi(x)$. By right cancellation, we have $\varphi(1_G) = 1_H$. Thus $\varphi(x^0) = \varphi(x)^0$. Moreover, $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1) = 1$; thus by the uniqueness of inverses, $\varphi(x^{-1}) = \varphi(x)^{-1}$. Now suppose n is a negative integer. Then $\varphi(x^n) = \varphi((x^{-n})^{-1}) = \varphi(x^{-n})^{-1} = (\varphi(x)^{-n})^{-1} = \varphi(x)^n$. Thus $\varphi(x^n) = \varphi(x)^n$ for all $x \in G$ and $n \in \mathbb{Z}$.

Problem

If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian.

Problem

If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian.

Solution

Let $\varphi : G \to H$ be a group isomorphism.

($\Rightarrow$) Suppose G is abelian, and let $h_1, h_2 \in H$. Since φ is surjective, there exist $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Now we have

$h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \varphi(g_2g_1) = \varphi(g_2)\varphi(g_1) = h_2h_1$. Thus h_1 and h_2 commute; since $h_1, h_2 \in H$ were arbitrary, H is abelian.

($\Leftarrow$) Suppose H is abelian, and let $g_1, g_2 \in G$. Then we have

$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \varphi(g_2)\varphi(g_1) = \varphi(g_2g_1)$. Since φ is injective, we have $g_1g_2 = g_2g_1$. Since $g_1, g_2 \in G$ were arbitrary, G is abelian.

Problem

Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Problem

Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Solution

We know that no bijection $\mathbb{Q} \to \mathbb{R}$ exists, so no such isomorphism exists.

Problem

Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Solution

We know that no bijection $\mathbb{Q} \to \mathbb{R}$ exists, so no such isomorphism exists.

Problem

Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π.

Problem

Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Solution

We know that no bijection $\mathbb{Q} \to \mathbb{R}$ exists, so no such isomorphism exists.

Problem

Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π.

Solution

To show that π is a homomorphism, let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$. Then

$\pi((x_1, y_1) \cdot (x_2, y_2)) = \pi((x_1x_2, y_1y_2)) = x_1x_2 = \pi((x_1, y_1)) \cdot \pi((x_2, y_2))$.

Now we claim that $\ker \pi = 0 \times \mathbb{R}.(\subseteq) If (x, y) \in \ker \pi$ then we have $x = \pi((x, y)) = 0$.

Thus $(x, y) \in 0 \times \mathbb{R}.(\supseteq)$ If $(x, y) \in 0 \times \mathbb{R}$, we have $x = 0$ and thus $\pi((x, y)) = 0$. Hence $(x, y) \in \ker \pi$.

Problem

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Problem

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Solution

($\Rightarrow$) Suppose G is abelian. Then $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b)$, so that φ is a homomorphism.

($\Leftarrow$) Suppose φ is a homomorphism, and let $a, b \in G$. Then

$ab = (b^{-1}a^{-1})^{-1} = \varphi(b^{-1}a^{-1}) = \varphi(b^{-1})\varphi(a^{-1}) = (b^{-1})^{-1}(a^{-1})^{-1} = ba$, so that G is abelian.

Problem

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Solution

($\Rightarrow$) Suppose G is abelian. Then $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b)$, so that φ is a homomorphism.

($\Leftarrow$) Suppose φ is a homomorphism, and let $a, b \in G$. Then

$ab = (b^{-1}a^{-1})^{-1} = \varphi(b^{-1}a^{-1}) = \varphi(b^{-1})\varphi(a^{-1}) = (b^{-1})^{-1}(a^{-1})^{-1} = ba$, so that G is abelian.

Problem

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Problem

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Solution

($\Rightarrow$) Suppose G is abelian. Then $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b)$, so that φ is a homomorphism.

($\Leftarrow$) Suppose φ is a homomorphism, and let $a, b \in G$. Then

$ab = (b^{-1}a^{-1})^{-1} = \varphi(b^{-1}a^{-1}) = \varphi(b^{-1})\varphi(a^{-1}) = (b^{-1})^{-1}(a^{-1})^{-1} = ba$, so that G is abelian.

Problem

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Solution

($\Leftarrow$) Suppose G is abelian. Then $\varphi(ab) = abab = a^2b^2 = \varphi(a)\varphi(b)$, so that φ is a homomorphism.

Definition

A group action of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

Definition

A group action of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$, and

Definition

A group action of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$, and
2. $1 \cdot a = a$, for all $a \in A$.

Definition

A group action of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$, and
2. $1 \cdot a = a$, for all $a \in A$.

Definition

Let the group G act on the set A. For each fixed $g \in G$ we get a map σ_g. defined $\sigma_g : A \to A$ by $\sigma_g(a) = g \cdot a$. Then,

Definition

A group action of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$, and
2. $1 \cdot a = a$, for all $a \in A$.

Definition

Let the group G act on the set A. For each fixed $g \in G$ we get a map σ_g. defined $\sigma_g : A \to A$ by $\sigma_g(a) = g \cdot a$. Then,

1. for each fixed $g \in G, \sigma_g$ is a permutation of A, and

Definition

A group action of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$, and
2. $1 \cdot a = a$, for all $a \in A$.

Definition

Let the group G act on the set A. For each fixed $g \in G$ we get a map σ_g. defined $\sigma_g : A \to A$ by $\sigma_g(a) = g \cdot a$. Then,

1. for each fixed $g \in G, \sigma_g$ is a permutation of A, and
2. the map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism. This homomorphism called the *permutation representation* associated to the given action.

Example

Let $ga = a$, for all $g \in G, a \in A$. Properties 1 and 2 of a group action follow immediately. This action is called the *trivial action* and G is said to act trivially on A. Note that distinct elements of G induce the same permutation on A (in this case the identity permutation). The associated permutation representation $G \to S_A$ is the trivial homomorphism which maps every element of G to the identity. If G acts on a set B and distinct elements of G induce distinct permutations of B, the action is said to be *faithful.* A faithful action is therefore one in which the associated permutation representation is injective. The *kernel* of the action of G on B is defined to be $\{g \in G | gb = b$ for all $b \in B\}$, namely the elements of G which fix all the elements of B. For the trivial action, the kernel of the action is all of G and this action is not faithful when $|G| > 1$.

Example

Let $ga = a$, for all $g \in G, a \in A$. Properties 1 and 2 of a group action follow immediately. This action is called the *trivial action* and G is said to act trivially on A. Note that distinct elements of G induce the same permutation on A (in this case the identity permutation). The associated permutation representation $G \to S_A$ is the trivial homomorphism which maps every element of G to the identity. If G acts on a set B and distinct elements of G induce distinct permutations of B, the action is said to be *faithful.* A faithful action is therefore one in which the associated permutation representation is injective. The *kernel* of the action of G on B is defined to be $\{g \in G | gb = b$ for all $b \in B\}$, namely the elements of G which fix all the elements of B. For the trivial action, the kernel of the action is all of G and this action is not faithful when $|G| > 1$.

Problem

Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$

Example

Let $ga = a$, for all $g \in G, a \in A$. Properties 1 and 2 of a group action follow immediately. This action is called the *trivial action* and G is said to act trivially on A. Note that distinct elements of G induce the same permutation on A (in this case the identity permutation). The associated permutation representation $G \to S_A$ is the trivial homomorphism which maps every element of G to the identity. If G acts on a set B and distinct elements of G induce distinct permutations of B, the action is said to be *faithful.* A faithful action is therefore one in which the associated permutation representation is injective. The *kernel* of the action of G on B is defined to be $\{g \in G | gb = b$ for all $b \in B\}$, namely the elements of G which fix all the elements of B. For the trivial action, the kernel of the action is all of G and this action is not faithful when $|G| > 1$.

Problem

Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$

Solution

Let $a \in \mathbb{Z}$. We have $0 \cdot a = 0 + a = a$. Now let $z_1, z_2 \in \mathbb{Z}$. Then

Problem

Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R}x\mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Problem

Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R}x\mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Solution

Let $(x, y) \in \mathbb{R} \times \mathbb{R}$. We have $0 \cdot (x, y) = (x + 0y, y) = (x, y)$. *Now let* $r_1, r_2 \in \mathbb{R}$. Then

$$r_1 \cdot (r_2 \cdot (x, y)) = r_1 \cdot (x + r_2 y, y) = (x + r_2 y + r_1 y, y) = (x + (r_1 + r_2)y, y) = (r_1 + r_2) \cdot (x, y)$$

Problem

Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R}x\mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Solution

Let $(x, y) \in \mathbb{R} \times \mathbb{R}$. We have $0 \cdot (x, y) = (x + 0y, y) = (x, y)$.*Nowlet*$r_1, r_2 \in \mathbb{R}$. Then

$r_1 \cdot (r_2 \cdot (x, y)) = r_1 \cdot (x + r_2 y, y) = (x + r_2 y + r_1 y, y) = (x + (r_1 + r_2)y, y) = (r_1 + r_2) \cdot (x, y)$

Problem

Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G (a) the kernel of the action, (b) $\{g \in G | ga = a\}$ - this subgroup is called the *stabilizer* of a in G.

Solution

we need to show that the identity belongs to the set and that each is closed under multiplication and inversion. (a) Note that $1 \in Ksince1 \cdot a = aforalla \in A$. Now suppose $k_1, k_2 \in K, andleta \in A$. Then $(k_1 k_2) \cdot a = k_1 \cdot (k_2 \cdot a) = k_1 \cdot a = a$, so that $k_1 k_2 \in K$. Now let $k \in Kanda \in A$; then $k^{-1} \cdot a = k^{-1} \cdot (k \cdot a) = (k^{-1} k) \cdot a = 1 \cdot a = a, sothatk^{-1} \in K$. Thus K is a subgroup of G.

(b) We have $1 \in S$ since $1 \cdot a = a$. Now suppose $s_1, s_2 \in S$; then we have $(s_1 s_2) \cdot a = s_1 \cdot (s_2 \cdot a) = s_1 \cdot a = a$, so that $s_1 s_2 \in S$. Now let $s \in S$; we have $s^{-1} \cdot a = s^{-1} \cdot (s \cdot a) = (s^{-1} s) \cdot a = a$, so that $s^{-1} \in S$. Thus S is a subgroup of G.

Definition

Let G be a group. The subset H of G is a subgroup of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Definition

Let G be a group. The subset H of G is a subgroup of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Example

Definition

Let G be a group. The subset H of G is a subgroup of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Example

1. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.

Definition

Let G be a group. The subset H of G is a subgroup of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Example

1. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.
2. Any group G has two subgroups: $H = G$ and $H = \{1\}$; the latter is called the trivial subgroup and will henceforth be denoted by 1 .

Definition

Let G be a group. The subset H of G is a subgroup of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Example

1. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.
2. Any group G has two subgroups: $H = G$ and $H = \{1\}$; the latter is called the trivial subgroup and will henceforth be denoted by 1 .
3. If $G = D_{2n}$ is the dihedral group of order $2n$, let H be $\{1, r, r^2, ..., r^{n-1}\}$, the set of all rotations in G. Since the product of two rotations is again a rotation and the inverse of a rotation is also a rotation it follows that H is a subgroup of D_{2n} of order n.

Proposition

(The Subgroup Criterion) A subset H of a group G is a subgroup if and only if

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Proposition

(The Subgroup Criterion) A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$, and

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Proposition

(The Subgroup Criterion) A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$, and
2. for all $x, y \in H, xy^{-1} \in H$

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Proposition

(The Subgroup Criterion) A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$, and
2. for all $x, y \in H, xy^{-1} \in H$

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Problem

Show that the following subsets of the dihedral group D_8 are actually subgroups: (a) $\{1, r^2, s, sr^2\}$, (b) $\{1, r^2, sr, sr^3\}$

Solution

(a) We have

$r^2r^2 = 1, r^2s = sr^2, r^2sr^2 = s, sr^2 = sr^2, ss = 1, ssr^2 = r^2, sr^2r^2 = s, sr^2s = r^2$, and $sr^2sr^2 = 1$, so that this set is closed under multiplication. Moreover, $(r^2)^{-1} = r^2, s^{-1} = s$, and $(sr^2)^{-1} = sr^2$, so this set is closed under inversion. Thus it is a subgroup.

(b) We have

$r^2r^2 = 1, r^2sr = sr^3, r^2sr^3 = sr, srr^2 = sr^3, srsr = 1, srsr^3 = r^2, sr^3r^2 = sr, sr^3sr = r^2$, and $sr^3sr^3 = 1$, so that this set is closed under multiplication. Moreover, $(r^2)^{-1} = r^2, (sr)^{-1} = sr$, and $(sr^3)^{-1} = sr^3$, so this set is closed under inversion. Thus it is a subgroup.

Solution

(a) We have

$r^2r^2 = 1, r^2s = sr^2, r^2sr^2 = s, sr^2 = sr^2, ss = 1, ssr^2 = r^2, sr^2r^2 = s, sr^2s = r^2$, and $sr^2sr^2 = 1$, so that this set is closed under multiplication. Moreover, $(r^2)^{-1} = r^2, s^{-1} = s$, and $(sr^2)^{-1} = sr^2$, so this set is closed under inversion. Thus it is a subgroup.

(b) We have

$r^2r^2 = 1, r^2sr = sr^3, r^2sr^3 = sr, srr^2 = sr^3, srsr = 1, srsr^3 = r^2, sr^3r^2 = sr, sr^3sr = r^2$, and $sr^3sr^3 = 1$, so that this set is closed under multiplication. Moreover, $(r^2)^{-1} = r^2, (sr)^{-1} = sr$, and $(sr^3)^{-1} = sr^3$, so this set is closed under inversion. Thus it is a subgroup.

Problem

Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Solution

(a) We have

$r^2r^2 = 1, r^2s = sr^2, r^2sr^2 = s, sr^2 = sr^2, ss = 1, ssr^2 = r^2, sr^2r^2 = s, sr^2s = r^2$, and $sr^2sr^2 = 1$, so that this set is closed under multiplication. Moreover, $(r^2)^{-1} = r^2, s^{-1} = s$, and $(sr^2)^{-1} = sr^2$, so this set is closed under inversion. Thus it is a subgroup.

(b) We have

$r^2r^2 = 1, r^2sr = sr^3, r^2sr^3 = sr, srr^2 = sr^3, srsr = 1, srsr^3 = r^2, sr^3r^2 = sr, sr^3sr = r^2$, and $sr^3sr^3 = 1$, so that this set is closed under multiplication. Moreover, $(r^2)^{-1} = r^2, (sr)^{-1} = sr$, and $(sr^3)^{-1} = sr^3$, so this set is closed under inversion. Thus it is a subgroup.

Problem

Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Solution

Under these conditions, there exists a nonidentity element $x \in H$ and an element $y \notin H$. Consider the product xy. If $xy \in H$, then since $x^{-1} \in H$ and H is a subgroup, $y \in H$, a

Problem

Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Problem

Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Solution

The ($\Leftarrow$) direction is clear. To see ($\Rightarrow$), suppose that $H \cup K$ is a subgroup of G and that $H \not\subseteq K and K \not\subseteq H$; that is, there exist $x \in H$ with $x \notin K$ and $y \in K$ with $y \notin H$. Now we have $xy \in H \cup K$, so that either $xy \in H$ or $xy \in K$. If $xy \in H$, then we have $x^{-1}xy = y \in H$, a contradiction. Similarly, if $xy \in K$, we have $x \in K$, a contradiction. Then it must be the case that either $H \subseteq K$ or $K \subseteq H$.

Problem

Let G be a group. (a) Prove that if H and K are subgroups of G, then so is $H \cap K$.

(b) Prove that if $\{H_i\}_{i \in I}$ is a family of subgroups of G then so is $\bigcap_{i \in I} H_i$.(or)Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable)

Problem

Let G be a group. (a) Prove that if H and K are subgroups of G, then so is $H \cap K$.

(b) Prove that if $\{H_i\}_{i \in I}$ is a family of subgroups of G then so is $\bigcap_{i \in I} H_i$.(or)Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable)

Solution

(a) Note that $H \cap K$ is not empty since $1 \in H \cap K$. Now suppose $x, y \in H \cap K$. Then since H and K are subgroups, we have $xy^{-1} \in H$ and $xy^{-1} \in K$ by the subgroup criterion; thus $xy^{-1} \in H \cap K$. By the subgroup criterion, $H \cap K$ is a subgroup of G.

(b) Note that $\bigcap_{i \in I} H_i$ is not empty since $1 \in H_i$ for each $i \in I$. Now let $x, y \in \bigcap_{i \in I} H_i$. Then $x, y \in H_i$ for each $i \in I$, and by the subgroup criterion, $xy^{-1} \in H_i$ for each $i \in I$. Thus $xy^{-1} \in \bigcap_{i \in I} H_i$. By the subgroup criterion, $\bigcap_{i \in I} H_i$ is a subgroup of G.

We now introduce some important families of subgroups of an arbitrary group G which in particular provide many examples of subgroups. Let A be any nonempty subset of G.

Definition

Define $C_G(A) = \{g \in G | gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the *centralizer* of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A.

We now introduce some important families of subgroups of an arbitrary group G which in particular provide many examples of subgroups. Let A be any nonempty subset of G.

Definition

Define $C_G(A) = \{g \in G | gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the *centralizer* of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A.

Definition

Define $Z(G) = \{g \in G | gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G . This subset of G is called the *center* of G .

Definition

Define $gAg^{-1} = \{gag^{-1} | a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G | gAg^{-1} = A\}$.

Definition

Define $gAg^{-1} = \{gag^{-1} | a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G | gAg^{-1} = A\}$.

Example

If G is abelian then all the elements of G commute, so $Z(G) = G$. Similarly, $C_G(A) = N_G(A) = G$ for any subset A of G since $gag^{-1} = gg^{-1}a = a$ for every $g \in G$ and every $a \in A$.

Definition

Define $gAg^{-1} = \{gag^{-1} | a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G | gAg^{-1} = A\}$.

Example

If G is abelian then all the elements of G commute, so $Z(G) = G$. Similarly, $C_G(A) = N_G(A) = G$ for any subset A of G since $gag^{-1} = gg^{-1}a = a$ for every $g \in G$ and every $a \in A$.

Definition

if G is a group acting on a set S and s is some fixed element of S, the *stabilizer* of s in G is the set $G_s = \{g \in G | g \cdot s = s\}$.

Problem

Prove that $C_G(A) = \{g \in G | g^{-1}ag = a \text{ for all } a \in A\}$.

Problem

Prove that $C_G(A) = \{g \in G | g^{-1}ag = a \text{ for all } a \in A\}$.

Solution

By definition, $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$.

($\subseteq$) If $g \in C_G(A)$, then $gag^{-1} = a$ for all $a \in A$. Left multiplying by g^{-1} and right multiplying by g, we have that $a = g^{-1}ag$ for all $a \in A$.

($\supseteq$) If $g \in G$ such that $g^{-1}ag = a$ for all $a \in A$, then left multiplying by g and right multiplying by g^{-1} we have that $a = gag^{-1}$ for all $a \in A$.

Problem

Prove that $C_G(A) = \{g \in G | g^{-1}ag = a \text{ for all } a \in A\}$.

Solution

By definition, $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$.

($\subseteq$) If $g \in C_G(A)$, then $gag^{-1} = a$ for all $a \in A$. Left multiplying by g^{-1} and right multiplying by g, we have that $a = g^{-1}ag$ for all $a \in A$.

($\supseteq$) If $g \in G$ such that $g^{-1}ag = a$ for all $a \in A$, then left multiplying by g and right multiplying by g^{-1} we have that $a = gag^{-1}$ for all $a \in A$.

Problem

Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$

Problem

Prove that $C_G(A) = \{g \in G | g^{-1}ag = a \text{ for all } a \in A\}$.

Solution

By definition, $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$.

($\subseteq$) If $g \in C_G(A)$, then $gag^{-1} = a$ for all $a \in A$. Left multiplying by g^{-1} and right multiplying by g, we have that $a = g^{-1}ag$ for all $a \in A$.

($\supseteq$) If $g \in G$ such that $g^{-1}ag = a$ for all $a \in A$, then left multiplying by g and right multiplying by g^{-1} we have that $a = gag^{-1}$ for all $a \in A$.

Problem

Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$

Solution

First we show that $C_G(Z(G)) = G$.

($\subseteq$) is clear. ($\supseteq$) Suppose $g \in G$. Then by definition, for all $a \in Z(G)$, we have $ga = ag$. That is, for all $a \in Z(G)$, we have $a = gag^{-1}$. Thus $g \in C_G(Z(G))$.

Since $C_G(Z(G)) \leq N_G(Z(G))$ and $N_G(Z(G)) = G$

Problem

Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Problem

Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Solution

Let $x \in C_G(B)$. Then for all $b \in B, xbx^{-1} = b$. Since $A \subseteq B$, for all $a \in A$ we have $xax^{-1} = a$, so that $x \in C_G(A)$. Thus $C_G(B) \subseteq C_G(A)$, and hence $C_G(B) \leq C_G(A)$

Problem

Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Solution

Let $x \in C_G(B)$. Then for all $b \in B, xbx^{-1} = b$. Since $A \subseteq B$, for all $a \in A$ we have $xax^{-1} = a$, so that $x \in C_G(A)$. Thus $C_G(B) \subseteq C_G(A)$, and hence $C_G(B) \leq C_G(A)$

Problem

Let H be a subgroup of order 2 in G . Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$, then $H \leq Z(G)$.

Problem

Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Solution

Let $x \in C_G(B)$. Then for all $b \in B, xbx^{-1} = b$. Since $A \subseteq B$, for all $a \in A$ we have $xax^{-1} = a$, so that $x \in C_G(A)$. Thus $C_G(B) \subseteq C_G(A)$, and hence $C_G(B) \leq C_G(A)$

Problem

Let H be a subgroup of order 2 in G . Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$, then $H \leq Z(G)$.

Solution

Say $H = \{1, h\}$.

We already know that $C_G(H) \subseteq N_G(H)$. Now suppose $x \in N_G(H)$; then $\{x1x^{-1}, xhx^{-1}\} = \{1, h\}$. Clearly, then, we have $xhx^{-1} = h$. Thus $x \in C_G(H)$. Hence $N_G(H) = C_G(H)$.

If $N_G(H) = G$, we have $C_G(H) = G$. Then $ghg^{-1} = h$ for all $h \in H$, so that $gh = hg$ for all $h \in H$ and thus $H \leq Z(G)$

Problem

Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

Problem

Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

Solution

If $A = \emptyset$, the statement is vacuously true since $N_G(A) = G$. If A is not empty, let $x \in Z(G)$. Then $xax^{-1} = a$ for all $a \in A$, so that $xAx^{-1} = A$. Hence $x \in N_G(A)$.

Definition

A group H is *cyclic* if H can be generated by a single element, i.e. , there is some element $x \in H$ such that $H = \{x^n | n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).

Definition

A group H is *cyclic* if H can be generated by a single element, i.e. , there is some element $x \in H$ such that $H = \{x^n | n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).

Remark

In additive notation H is cyclic if $H = \{nx | n \in \mathbb{Z}\}$. In both cases we shall write $H = \langle x \rangle$ and say H is generated by x (and x is a generator of H). A cyclic group may have more than one generator. For example, if $H = \langle x \rangle$, then also $H = \langle x^{-1} \rangle$.

Proposition

If $H = \langle x \rangle$, then $|H| = |x|$(where if one side of this equality is infinite, so is the other). More specifically (1) if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of H, and (2) if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.

Proposition

If $H = \langle x \rangle$, then $|H| = |x|$(where if one side of this equality is infinite, so is the other). More specifically (1) if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of H, and (2) if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.

Proposition

Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m .

Proposition

If $H = \langle x \rangle$, then $|H| = |x|$(where if one side of this equality is infinite, so is the other). More specifically (1) if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of H, and (2) if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.

Proposition

Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m .

Theorem

Let $H = \langle x \rangle$ be a cyclic group. Then every subgroup H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.

Problem

Find all cyclic subgroups of D_8 . Find a proper subgroup of D_8 which is not cyclic.

Problem

Find all cyclic subgroups of D_8 . Find a proper subgroup of D_8 which is not cyclic.

Solution

We have the following.

(1) $\langle 1\rangle = \{1\}$ (2)$\langle r\rangle = \{1, r, r^2, r^3\}$ (3)$\langle r^2\rangle = \{1, r^2\}$ (4)$\langle r^3\rangle = \{1, r, r^2, r^3\}$

(5)$\langle s\rangle = \{1, s\}$ (6)$\langle sr\rangle = \{1, sr\}$ (7)$\langle sr^2\rangle = \{1, sr^2\}$ (8)$\langle sr^3\rangle = \{1, sr^3\}$. We know that

$\{1, r^2, s, r^2s\}$ is a subgroup of D_8, but is not on the above list, hence is not cyclic.

Problem

Find all cyclic subgroups of D_8 . Find a proper subgroup of D_8 which is not cyclic.

Solution

We have the following.

(1) $\langle 1\rangle = \{1\}$ (2)$\langle r\rangle = \{1, r, r^2, r^3\}$ (3)$\langle r^2\rangle = \{1, r^2\}$ (4)$\langle r^3\rangle = \{1, r, r^2, r^3\}$

(5)$\langle s\rangle = \{1, s\}$ (6)$\langle sr\rangle = \{1, sr\}$ (7)$\langle sr^2\rangle = \{1, sr^2\}$ (8)$\langle sr^3\rangle = \{1, sr^3\}$. We know that $\{1, r^2, s, r^2s\}$ is a subgroup of D_8, but is not on the above list, hence is not cyclic.

Problem

Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{P^n} = 1$ then $|x| = p^m$ for some $m \leq n$.

Solution

We prove a lemma.

Lemma: Let G be a group and $x \in G$ an element of finite order, say, $|x| = n$. If $x^m = 1$, then n divides m. **Proof:** Suppose to the contrary that n does not divide m; then by the Division Algorithm there exist integers q and r such that $0 < r < |n|$ and $m = qn + r$. Then we have $1 = x^m = x^{qn+r} = (x^n)^q + x^r = x^r$. But recall that by definition n is the least positive integer with this property, so we have a contradiction. Thus n divides m.

Solution

We prove a lemma.

Lemma: Let G be a group and $x \in G$ an element of finite order, say, $|x| = n$. If $x^m = 1$, then n divides m. **Proof:** Suppose to the contrary that n does not divide m; then by the Division Algorithm there exist integers q and r such that $0 < r < |n|$ and $m = qn + r$. Then we have $1 = x^m = x^{qn+r} = (x^n)^q + x^r = x^r$. But recall that by definition n is the least positive integer with this property, so we have a contradiction. Thus n divides m.

Problem

Let G be a finite group and let $x \in G$.

(1) Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some integer a.

(2) Show conversely that if $gxg^{-1} = x^a$ for some integer a, then $g \in N_G(\langle x \rangle)$. [Hint: Show first that $gx^k g^{-1} = (gkg^{-1})^k = x^{ak}$ for any integer k, so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. If x has order n, show that the elements $gx^i g^{-1}$ are distinct for $i \in \{0, 1, \ldots, n-1\}$, so that $|g\langle x \rangle g^{-1}| = |\langle x \rangle| = n$ and conclude that $g\langle x \rangle g^{-1} = \langle x \rangle$.]

Solution

(1) Let $g \in N_G(\langle x \rangle)$. By definition, we have $gxg^{-1} \in \langle x \rangle$, so that $gxg^{-1} = x^a$ for some integer a.

(2) We prove some lemmas. **Lemma 1:** Let G be a group and let $x, g \in G$. Then for all integers k, $gx^k g^{-1} = (gxg^{-1})^k$. **Proof:** First we prove the conclusion for nonnegative k by induction on k. If $k = 0$, we have $gx^0 g^{-1} = gg^{-1} = 1 = (gxg^{-1})^0$. Now suppose the conclusion holds for some $k \geq 0$; then

$gx^{k+1}g^{-1} = gxx^k g^{-1} = gxg^{-1}gx^k g^{-1} = gxg^{-1}(gxg^{-1})^k = (gxg^{-1})^{k+1}$. By induction, the conclusion holds for all nonnegative k. Now suppose $k < 0$; then

$gx^k g^{-1} = (gx^{-k}g^{-1})^{-1} = (gxg^{-1})^{-k^{-1}} = (gxg^{-1})^k$. Thus the conclusion holds for all integers k. $\square$

Lemma 2: Let G be a group and let $x, g \in G$ such that $gxg^{-1} = x^a$ for some integer a. Then $g\langle x \rangle g^{-1}$ is a subgroup of $\langle x \rangle$. **Proof:** Let $gx^k g^{-1} \in g\langle x \rangle g^{-1}$; by Lemma 1 we have $gx^k g^{-1} = (gxg^{-1})^k = x^{ak}$, so that $gxg^{-1} \in \langle x \rangle$. Thus $g\langle x \rangle g^{-1} \subseteq \langle x \rangle$. Now let $gx^b g^{-1}, gx^c g^{-1} \in g\langle x \rangle g^{-1}$. Then

$gx^b g^{-1}(gx^c g^{-1})^{-1} = gx^b g^{-1} gx^{-c} g^{-1} = gx^{b-c} g^{-1} \in g\langle x \rangle g^{-1}$. By the Subgroup

Lemma 3:

Let G be a group and let $x, g \in G$ such that $gxg^{-1} = x^a$ for some integer a and such that $|x| = n, n \in \mathbb{Z}$. Then $gx^i g^{-1} aredistinctfori \in \{0, 1, \ldots, n-1\}$. **Proof:** Choose distinct $i, j \in \{0, 1, \ldots, n-1\}$. By a previous exercise, $x^i \neq x^j$. Suppose now that $gx^i g^{-1} = gx^j g^{-1}$; by cancellation we have $x^i = x^j$, a contradiction. Thus the $gx^i g^{-1}$ are distinct. $\square$

Now to the main result; suppose $gxg^{-1} = x^a$ for some integer a. Since G has finite order, $|x| = n$ for some n. By Lemma 2, $g\langle x\rangle g^{-1} \leq \langle x\rangle$, and by Lemma 3 we have $|g\langle x\rangle g^{-1}| = |\langle x\rangle|$. Since G is finite, then, we have $g\langle x\rangle g^{-1} = \langle x\rangle$. Thus $g \in N_G(\langle x\rangle)$.

Proposition

If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.

Proposition

If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.

Proof.

This is an easy application of the subgroup criterion (see [**?**]). Let $K = \cap_{H \in \mathcal{A}} H$. Since each $H \in \mathcal{A}$ is a subgroup, $1 \in H$, so $1 \in K$, that is, $K \neq \emptyset$. If $a, b \in K$, then $a, b \in H$, for all $H \in \mathcal{A}$. Since each H is a group, $ab^{-1} \in H$, for all H, hence $ab^{-1} \in K$. Then $K \leq G$. □

Proposition

If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.

Proof.

This is an easy application of the subgroup criterion (see [**?**]). Let $K = \cap_{H \in \mathcal{A}} H$. Since each $H \in \mathcal{A}$ is a subgroup, $1 \in H$, so $1 \in K$, that is, $K \neq \emptyset$. If $a, b \in K$, then $a, b \in H$, for all $H \in \mathcal{A}$. Since each H is a group, $ab^{-1} \in H$, for all H, hence $ab^{-1} \in K$. Then $K \leq G$. □

Definition

If A is any subset of the group G define $\langle A \rangle = \cap_{A \subseteq H, H \leq G}$. This is called the subgroup of G generated by A.

Problem

Let G be a group. Prove that if $H \leq G$ is a subgroup then $\langle H \rangle = H$.

Problem

Let G be a group. Prove that if $H \leq G$ is a subgroup then $\langle H \rangle = H$.

Solution

That $H \subseteq \langle H \rangle$ is clear. Now suppose $x \in \langle H \rangle$. We can write x as a finite product $h_1 h_2 \cdots h_n$ of elements of H; since H is a subgroup, then, $x \in H$.

Problem

Let G be a group. Prove that if $H \leq G$ is a subgroup then $\langle H \rangle = H$.

Solution

That $H \subseteq \langle H \rangle$ is clear. Now suppose $x \in \langle H \rangle$. We can write x as a finite product $h_1 h_2 \cdots h_n$ of elements of H; since H is a subgroup, then, $x \in H$.

Problem

Let G be a group, with $A \subseteq B \subseteq G$. Prove that $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$.

Problem

Let G be a group. Prove that if $H \leq G$ is a subgroup then $\langle H \rangle = H$.

Solution

That $H \subseteq \langle H \rangle$ is clear. Now suppose $x \in \langle H \rangle$. We can write x as a finite product $h_1 h_2 \cdots h_n$ of elements of H; since H is a subgroup, then, $x \in H$.

Problem

Let G be a group, with $A \subseteq B \subseteq G$. Prove that $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$.

Solution

Let $\mathcal{A} = \{H \leq G \mid A \subseteq H\}$ and $\mathcal{B} = \{H \leq G \mid B \subseteq H\}$. Since $A \subseteq B$, we have $A \subseteq H$ whenever $B \subseteq H$; thus $\mathcal{B} \subseteq \mathcal{A}$. By definition, we have $\langle A \rangle = \cap \mathcal{A}$ and $\langle B \rangle = \cap \mathcal{B}$. We know from set theory that $\cap \mathcal{A} \subseteq \cap \mathcal{B}$, so that $\langle A \rangle \subseteq \langle B \rangle$.

Now since $\langle A \rangle$ is itself a subgroup of G, we have $\langle A \rangle \leq \langle B \rangle$.

Now suppose $G = \langle x \rangle$ is cyclic. Then $\{x\} \subsetneq G$, but we have $\langle x \rangle = \langle G \rangle$.

Problem

Let G be a group and let $H \leq G$ be an abelian subgroup. Show that $\langle H, Z(G)\rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H)\rangle$ is not abelian

Problem

Let G be a group and let $H \leq G$ be an abelian subgroup. Show that $\langle H, Z(G)\rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H)\rangle$ is not abelian

Solution

We begin with a lemma.

Lemma: Let G be a group, $H \leq G$ an abelian subgroup. Then every element of $\langle H, Z(G)\rangle$ is of the form hz for some $h \in H$ and $z \in Z(G)$. **Proof:** Recall that every element of $\langle H, Z(G)\rangle$ can be written as a (finite) word $a_1 a_2 \cdots a_k$ for some integer k and $a_i \in H \cup Z(G)$. We proceed by induction on k, the length of a word in $H \cup Z(G)$. If $k = 1$, we have $x = a_1$; if $a_1 \in H$ we have $x = a_1 \cdot 1$, and if $a_1 \in Z(G)$ we have $x = 1 \cdot a_1$. Now suppose all words of length k can be written in the form hz, and let $x = a_1 a_2 \cdots a_{k+1}$ be a word of length $k+1$. By the induction hypothesis we have $a_2 \cdots a_{k+1} = hz$ for some $h \in H$ and $z \in Z(G)$. Now if $a_1 \in H$, we have $x = (a_1 h) \cdot z$, and if $a_1 \in Z(G)$, then $x = h \cdot (a_1 z)$. By induction, every element of $\langle H, Z(G)\rangle$ is of the

Problem

Let G be a group and $H \leq G$. Show that $H = \langle H \setminus \{1\} \rangle$.

Problem

Let G be a group and $H \leq G$. Show that $H = \langle H \setminus \{1\} \rangle$.

Solution

We have $H \setminus \{1\} \subseteq \langle H \setminus \{1\} \rangle$. If $H = 1$, then $\langle H \setminus \{1\} \rangle = \langle \emptyset \rangle = 1 = H$. If $H \neq 1$, there exists some nonidentity $h \in H$. So $h \in H \setminus \{1\}$, so that $hh^{-1} = 1 \in \langle H \setminus \{1\} \rangle$. Thus $H \subseteq \langle H \setminus \{1\} \rangle$.

Now if $x \in \langle H \setminus \{1\} \rangle$, we can write $x = a_1 a_2 \cdots a_n$ for some integer n and group elements $a_i \in H \setminus \{1\}$; since H is a subgroup, then, $x \in H$.