Section 3.2

Problem # 15

Prove that if $x = x^{-1}$ for all x in the group G, then G is abelian.

Solution

For any $x, y \in G$ xy is in G by the definition of a group and $(xy)(xy) = e$. Therefore

$$\begin{aligned} xy &= xey \\ &= x((xy)(xy))y \\ &= (xx)yx(yy) \\ &= eyxe \\ &= yx \end{aligned} \tag{1}$$

Therefore the group is abelian.

Problem # 16

Suppose $ab = ca$ implies $b = c$ for all elements a, b, and c in a group G. Prove that G is abelian.

Solution

$$\begin{aligned} ab &= abe \\ &= ab(a^{-1}a) \\ &= (aba^{-1})a \end{aligned} \tag{2}$$

this implies that $b = aba^{-1}$. Therefore

$$\begin{aligned} ba &= (aba^{-1})a \\ &= ab(a^{-1}a) \\ &= abe \\ &= ab \end{aligned} \tag{3}$$

and thus G is abelian.

Problem # 17

Let a and b be elements of a group G. Prove that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$.

Solution

Let G be an abelian group. Then ab = ba and

$$\begin{aligned}(ab)^{-1} &= (ba)^{-1} \\ &= a^{-1}b^{-1}\end{aligned} \tag{4}$$

Now let a and b be elements of a group G such that $(ab)^{-1} = a^{-1}b^{-1}$. Then $(ab)^{-1} = (ba)^{-1}$. Assume that $ab \neq ba$. Thus

$$\begin{aligned}(ab)^{-1}ab &\neq (ab)^{-1}ba \\ e &\neq (ba)^{-1}ba \\ &\neq e\end{aligned} \tag{5}$$

This is a contradiction. Therefore ab must equal ba and G is therefore abelian.

Problem # 18

Let a and b be elements of a group G. Prove that G is abelian if and only if $(ab)^2 = a^2b^2$.

Solution

Let G be an abelian group. Therefore

$$\begin{aligned}(ab)^2 &= (ab)(ab) \\ &= abab \\ &= a(ba)b \\ &= a(ab)b \\ &= aabb \\ &= a^2b^2\end{aligned} \tag{6}$$

Now let a and b be two elements in a group G such that $(ab)^2 = a^2b^2$. Then

$$\begin{aligned}abab &= aabb \\ a^{-1}abab &= a^{-1}aabb \\ ebab &= eabb \\ bab &= abb \\ babb^{-1} &= abbb^{-1} \\ bae &= abe \\ ba &= ab\end{aligned} \tag{7}$$

Therefore G is abelian.

Problem # 19

Use mathematical induction to prove that if a is an element of a group G, then $(a^{-1})^n = (a^n)^{-1}$ for every positive integer n.

Solution

(a) For $n = 1$

$$\begin{aligned} (a^{-1})^n &= (a^n)^{-1} \\ (a^{-1})^1 &= (a^1)^{-1} \\ a^{-1} &= a^{-1} \end{aligned} \tag{8}$$

This is true.

(b) Assume the statement is true for $n = k$: $(a^k)^{-1} = (a^{-1})^k$.

(c) For $n = k + 1$

$$\begin{aligned} (a^{k+1})^{-1} &= (aa^k)^{-1} \\ &= (a^k)^{-1}a^{-1} \\ &= (a^{-1})^k a^{-1} \\ &= (a^{-1})^{k+1} \end{aligned} \tag{9}$$

It follows from the inductive hypothesis that $(a^{-1})^n = (a^n)^{-1}$ for every positive integer n.

Problem # 20

Let a and b be elements of a group G. Use mathematical induction to prove each of the following statements for all positive integers n.

- If the operation is multiplication, then $(a^{-1}ba)^n = a^{-1}b^n a$.
- If the operation is addition and G is abelian, then $n(a + b) = na + nb$.

Solution

Part (a)

(a) For $n = 1$, $(a^{-1}ba)^1 = a^{-1}b^1 a$. This is clearly true.

(b) Assume it is true for $n = k$: $(a^{-1}ba)^k = a^{-1}b^k a$.

(c) For $n = k + 1$

$$\begin{aligned} (a^{-1}ba)^{k+1} &= (a^{-1}ba)(a^{-1}ba)^k \\ &= (a^{-1}ba)(a^{-1}b^k a) \\ &= a^{-1}b(aa^{-1})b^k a \\ &= a^{-1}beb^k a \\ &= a^{-1}bb^k a \\ &= a^{-1}b^{k+1}a \end{aligned} \tag{10}$$

It follows from the inductive hypothesis that $(a^{-1}ba)^n = a^{-1}b^n a$.

Part (b)

(a) For $n = 1$, $1(a + b) = 1(a) + 1(b)$. This is clearly true.

(b) Assume it is true for $n = k$: $k(a + b) = ka + kb$

(c) For $n = k + 1$

$$\begin{aligned}(k+1)(a+b) &= k(a+b) + 1(a+b) \\ &= (ka+kb) + (a+b) \\ &= (ka+a) + (kb+b) \\ &= (k+1)a + (k+1)b\end{aligned} \tag{11}$$

It follows from the inductive hypothesis that $n(a + b) = na + nb$.

Problem # 22

Use mathematical induction to prove that if $a_1, a_2, \ldots, a_n$ are elements of a group G, then $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$. (This is the general form of the reverse order law for inverses.)

Solution

Part (a)

For $n = 1$, $(a_1)^{-1} = a_1^{-1}$.

Part (b)

Assume the statement is true for $n = k$.

Part (c)

For $n = k + 1$

$$\begin{aligned}(a_1 \cdots a_{k+1})^{-1} &= ((a_1 \cdots a_k)a_{k+1})^{-1} \\ &= a_{k+1}^{-1}(a_1 \cdots a_k)^{-1} \\ &= a_{k+1}^{-1}(a_k^{-1} \cdots a_1^{-1}) \\ &= a_{k+1}^{-1} a_k^{-1} \cdots a_2^{-1} a_1^{-1}\end{aligned} \tag{12}$$

It follows from the inductive hypothesis that the statement is true for all $n \geq 1$.

Problem # 23

Let G be a group that has even order. Prove that there exists at least one element $a \in G$ such that $a \neq e$ and $a = a^{-1}$.

Solution

Assume that for some group G with even order there does not exist an element $a \in G$ such that $a \neq e$ and $a = a^{-1}$. The order of G is even so there exists some integer n such that $o(G) = 2n$. Therefore, selecting some arbitrary $x \in G$, n pairs of inverses can be removed from G until the identity e and x are the only remaining elements of G. We know from the definition of a group that G initially contained x^{-1} and, because we removed two elements at a time and we know inverses are unique, we know that we have not removed x^{-1}. Therefore either $xe = e$ or $xx = e$. By the definition of e we know that $xe = x$. Therefore $xx = e$ and $x = x^{-1}$. This contradicts our assumption. Therefore, there does exist an element in G that does not equal e and is its own inverse.

Problem # 24

Prove or disprove that every group of order 3 is abelian.

Solution

Let $X = \{e, a, b\}$ be an arbitrary group of order 3. By the definition of a group, $ab \in X$. Therefore $ab = a$, $ab = b$, or $ab = e$. The first case implies that $b = e$. This is impossible because we know e is unique. The second case is impossible because it implies that $a = e$. Therefore $ab = e$. This means that a and b are each others inverses and $e = ab = ba$. So the group is abelian.

Problem # 25

Prove or disprove that every group of order 4 is abelian.

Solution

Let $X = \{e, a, b, c\}$ be an arbitrary group of order 4. By definition of a group, $ab \in X$. Therefore $ab = a$, $ab = b$, $ab = c$, or $ab = e$. The first two cases are impossible for the same reason demonstrated in the previous problem. Therefore either $ab = c$ or $ab = e$. If $ab = e$ then a and b are each other's inverses and $e = ab = ba$. If $ab = c$ then ba cannot equal e and must equal c. In all cases $ab = ba$. Therefore all groups of order 4 are abelian.

Section 3.2

Problem # 8

Find a subset of $\mathbb{Z}$ that is closed under addition but is not a subgroup of the additive group $\mathbb{Z}$.

Solution

$\mathbb{Z}^+$

Problem # 10

Let $n > 1$ be an integer, and let a be a fixed integer. Prove or disprove that the set

$$H = \{x \in \mathbb{Z} \mid ax \equiv 0 \pmod{n}\}$$

is a subgroup of G.

Solution

H is not empty because $0 \in H$ for all n and a. 0 is the identity element under addition so H always contains e.
Select arbitrary elements $x, y \in H$. $n \mid xa$ and $n \mid ya$. $(y + z)a = ya + za$ and $n \mid (ya + za)$. Therefore $y + z$ is in H and H is closed under addition.
The inverse of z under addition is $-z$. If $n \mid z$ then $n \mid -z$. We know that $n \mid z$ so therefore $n \mid -z$ and $-z$ is also in H.
H has met all of the necessary requirements and is thus a subgroup of G under addition.

Problem # 12

Prove or disprove that $H = \{h \in G \mid h^{-1} = h\}$ is a subgroup of the group G if G is abelian.

Solution

e is an element of H so therefore H is nonempty and contains the identity element.
Each element of H is its own inverse, so every element of H has an inverse.
G is abelian so for any $a, b \in H$, $ab = ba$. Therefore

$$\begin{aligned} ab(ab) &= ab(ba) \\ abab &= aea \\ abab &= aa \\ (ab)(ab) &= e \end{aligned} \tag{13}$$

Therefore $(ab)^{-1} = (ab)$. We know ab is an element of G because G is closed and we have shown that ab is its own inverse. So $(ab) \in H$. Thus H is closed under multiplication.
H has satisfied all of the necessary conditions and is thus a subgroup of G.

Problem # 13

Let G be an abelian group with respect to multiplication. Prove that each of the following subsets H of G is a subgroup of G.

(a) $H = \{x \in G \mid x^2 = e\}$.

(b) $H = \{x \in G \mid x^n = e\}$ for a fixed positive integer n.

Solution

Part (a)

$x^2 = e$ implies that $x^{-1} = x$ and H is a subgroup of G by the result of problem #12.

Part (b)

H is nonempty because $e^n = e$ so $e \in H$.
For two elements a and b in H.

$$\begin{aligned} (ab^{-1})^n &= a^n(b^n)^{-1} \\ &= e(e^{-1}) \\ &= e \end{aligned} \tag{14}$$

Thus for any $a, b \in H$, $ab^{-1} \in H$. H has satisfied the necessary conditions and thus is a subgroup of G.

Problem # 19

Prove that each of the following subsets H of $SL(2, \mathbb{R})$ is a subgroup of $SL(2, \mathbb{R})$.

(a) $H = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \middle| a \in \mathbb{R} \right\}$

(b) $H = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \middle| a^2 + b^2 = 1 \right\}$

Solution

Part (a)

The inverse matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is an element of H.

$$\begin{bmatrix} 1 & a_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_1 + a_2 \\ 0 & 1 \end{bmatrix}$$

a_1 and a_2 are both in $\mathbb{R}$ so $a_1 + a_2$ is also in $\mathbb{R}$. $1(1) - 0(a_1 + a_2$, so H is closed under multiplication.
For any a_1

$$\begin{bmatrix} 1 & a_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a_1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e$$

If a_1 is in $\mathbb{R}$ then so is $-a_1$ so every member of H has an inverse in H.
H has satisfied the necessary requirements and therefore is a subgroup of $SL(2,\mathbb{R})$.

Part (b)

The inverse matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is an element of H.

$$\begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 - b_1b_2 & -a_1b_2 - b_1a_2 \\ b_1a_2 + b_2a_1 & -b_1b_2 + a_1a_2 \end{bmatrix}$$

$$\begin{aligned}(a_1a_2 - b_1b_2)^2 + (b_1a_2 + b_2a_2)^2 &= (a_1a_2)^2 - 2a_1a_2b_1b_2 + (b_1b_2)^2 + (b_1a_2)^2 + 2b_1a_2b_2a_1 + (b_2a_1)^2 \\ &= a_1^2a_2^2 + b_1^2b_2^2 - 2a_1a_2b_1b_2 + b_1^2a_2^2 + b_2^2a_1^2 + 2b_1a_2b_2a_1 \\ &= a_1^2a_2^2 + b_1^2a_2^2 + b_1^2b_2^2 + b_2^2a_1^2 \\ &= a_2^2(a_1^2 + b_1^2) + b_2^2(b_1^2 + a_2^2) \\ &= a_2^2(1) + b_2^2(1) \\ &= a_2^2 + b_2^2 \\ &= 1 \end{aligned} \tag{15}$$

Therefore H is closed under multiplication.

For any values of a and b

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} a & b \\ (a^2-1)b^{-1} & (1-b^2)a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{aligned} a(1-b^2)a^{-1} - b(a^2-1)b^{-1} &= 1 - b^2 - a^2 + 1 \\ &= 1 - (b^2 + a^2) + 1 \\ &= 1 - 1 + 1 \\ &= 1 \end{aligned} \tag{16}$$

So the inverse is an element of H.
Having satisfied all of the necessary conditions, H is a subgroup of $SL(2,\mathbb{R})$.