Section 3.3

Problem # 23

Let R be the equivalence relation on G defined by xRy if and only if there exists an element a in G such that $y = a^{-1}xa$. If $x \in Z(G)$, find $[x]$, the equivalence class containing x.

Solution

It is given that $x \in Z(G)$. Therefore $\forall y \in G$, $xy = yx$. By the definition of an equivalence relation if xRy then yRx. Therefore

$$xRy \implies y = a^{-1}xa \tag{1}$$
$$yRx \implies x = a^{-1}ya \tag{2}$$

and

$$\begin{aligned} x &= a^{-1}ya \\ &= a^{-1}(a^{-1}xa)a \\ &= a^{-1}(xa^{-1}a)a \\ &= a^{-1}xea \\ &= a^{-1}xa \end{aligned} \tag{3}$$

From the above we can say that, given xRy

$$\begin{aligned} x = a^{-1}ya &= a^{-1}xa \\ aa^{-1}ya &= aa^{-1}xa \\ ya &= xa \\ y &= x \end{aligned} \qquad \text{so by Theorem 3.4e} \tag{4}$$

Therefore for the equivalence relation R, $[x] = \{x\}$.

Problem # 25

Let G be a group and $Z(G)$ its center. Prove or disprove that if ab is in $Z(G)$, then $ab = ba$.

Solution

It is given that $ab \in Z(G)$ and therefore commutes with every element in G.

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

Problem # 26

Let A be a given nonempty set. As noted in Example 2 of Section 3.1, $S(A)$ is a group with respect to mapping composition. for a fixed element a in A, let H_a denote the set of all $f \in S(A)$ such that $F9a) = a$. Prove that H_a is a subgroup of $S(A)$.

Solution

Part (a)

For any element $a \in A$ the identity mapping e must have $e(a) = a$. H_a contains all such mapping so it must contain the identity mapping.

Part (b)

The inverse f^{-1} of any mapping f such that $f(a) = a$ must also have the property $f^{-1}(a)$. Therefore H_a contains inverses.

Part (c)

Consider two mappings f and g in H_a. Then

$$\begin{aligned}(f \circ g)a &= f(g(a)) \\ &= f(a) \\ &= a\end{aligned} \tag{5}$$

Therefore the composition of any two arbitrary functions in H_a is also in H_a and H_a is closed under composition of mappings. H_a has satisfied all of the necessary conditions and is thus a group with respect to mapping composition.

Problem # 29

Let G be an abelian group. For a fixed positive integer n, let

$$G_n = \{a \in G \mid a = x^n \text{ for some } x \in G\}.$$

Prove that G_n is a subgroup of G.

Solution

Part (a)

G_n contains the identity element e for any integer n because $e = e^n$ for any n.

Part (b)

For $a, b \in G$, $a = z^n$ and $b = y^n$ for some $z, y \in G$. Then

$$\begin{aligned} ab &= z^n y^n \\ &= (zy)^n \end{aligned} \tag{6}$$

We know that the product zy is in G because G is a group and thus closed. Therefore $ab = x^n$ for some $x \in G$, namely for $x = zy$. So ab is in G_n and G_n is closed.

Part (c)

Let $a = x^n$ for some $x \in G$. G is a group so a has an inverse a^{-1} in G. So

$$\begin{aligned} e &= aa^{-1} \\ &= x^n a^{-1} \\ &= x^n (x^n)^{-1} \\ &= x^n (x^{-1})^n \\ &= a(x^{-1})^n \end{aligned} \tag{7}$$

So $a^{-1} = (x^{-1})^n$. $(x^{-1})^n$ is in G_n because we know that x^{-1} is in G. Therefore G_n contains inverses. Having satisfied all the necessary conditions, G_n is a subgroup of G.

Problem # 41

Let G be a cyclic group, $G = \langle a \rangle$. Prove that G is abelian.

Solution

For any two $x, y \in G$ there exist some $m, n \in \mathbb{Z}$ such that $x = a^m$ and $y = a^n$. Then

$$\begin{aligned} xy &= a^m a^n \\ &= a^{m+n} \\ &= a^{n+m} \\ &= a^n a^m \\ &= yx \end{aligned} \tag{8}$$

Therefore $G = \langle a \rangle$ is abelian.

Problem # 45

Assume that G is a finite group, and let G be a nonempty subset of G. Prove that H is closed if and only if H is a subgroup of G.

Solution

Part (a)

First assume that H is a subgroup of G. Then by definition of a group H is closed.

Part (b)

Assume that H is closed and that for some $x \in H$, $x^{-1} \notin H$. H is a subset of a finite group so therefore the order of H is some integer n. Then for the product xy where y is any arbitrary element in H there are n possible values of y. y is not x^{-1} so we know that $xy \neq e$ and there are thus $n-1$ possible values of xy. This implies that for some $y, z \in H$ $xy = xz$ but $y \neq z$. However, this contradicts Theorem 3.4e which tells us that for $x, y, z \in G$, $xy = xz$ means that $y = z$. So there cannot exist an element in H such that its inverse is not in H. Therefore H satisfies the necessary conditions and is a subgroup of G.

Section 3.4

Problem # 11f

According to Exercise 33 of Section 3.1, if n is prime, the nonzero elements of Z_n form a group U_n with respect to numtiplication. For $n = 19$, show that this group U_n is cyclic.

Solution

$$
\begin{array}{rrrr}
[2] = [2]^1 & [3] = [2]^{13} & [4] = [2]^2 & [5] = [2]^{16} \\
[6] = [2]^{14} & [7] = [2]^6 & [8] = [2]^3 & [9] = [2]^8 \\
[10] = [2]^{17} & [11] = [2]^{12} & [12] = [2]^{15} & [13] = [2]^5 \\
[14] = [2]^7 & [15] = [2]^{11} & [16] = [2]^4 & [17] = [2]^{10} \\
[18] = [2]^9 & & &
\end{array}
$$

It has been shown that [2] is a generator for $\mathbb{U}_{19}$ and therefore $\mathbb{U}_{19}$ is cyclic.

Problem # 12f

Find all distinct generators of the group U_{19} described in Exercise 11.

Solution

By Theorem 3.28 we know that a^m is a generator for a cyclic group of order n if and only if $(m, n) = 1$. We know from 11f that $a = 2$ is a generator of $\mathbb{U}_{19}$. $\mathbb{U}_{19}$ has order 18. Therefore the distinct generators of $\mathbb{U}_{19}$ are given by

$$[2]^1, [2]^5, [2]^7, [2]^{11}, [2]^{13}, [2]^{17}$$

$$=$$

$$[2], [13], [14], [15], [3], [10]$$

Problem # 33

If G is a cyclic group, prove that the equation $x^2 = e$ has at most two distinct solutions in G.

Solution

Let $G = \langle a \rangle$ be a cyclic group of order n. Let x be an element of G such that $x^2 = e$. x can be written as a^{2k} for some $k \in \mathbb{Z}$. So

$$
\begin{aligned}
e &= x^2 \\
&= (a^k)^2 \\
&= a^{2k}
\end{aligned}
\tag{9}
$$

We know that $a^0 = e$ so by Theorem 3.21 $2k \equiv 0 \mod n$. If $2 \nmid n$ then the only solution is $k = 0$. Therefore x must equal $a^0 = e$. In the case that $2 \mid n$ The solutions are $n = 0, \frac{n}{2}, -\frac{n}{2}$. We know by theorem 3.28 that $a^n = a^{-n}$ so the last two solutions are the same. Therefore there are at most two solutions.

Problem # 35

If G is a cyclic group of order p and p is a prime, how many elements in G are generators of G?

Solution

G is cyclic so we know that $G = \langle a \rangle$ for some $a \in G$. By the statment made on page 178 we know that G has $\phi(p)$ generators. When p is prime, $\phi(p) = p - 1$ so G has $p - 1$ generators.

Problem # 41

Let G be an abelian group. Prove that the set of all elements of finite order in G forms a subgroup of G. This subgroup is called the torsion subgroup of G.

Solution

Let H be the set of all elements of finite order in G.

Part (a)

The order of e is 1 so $e \in H$ and H is not empty.

Part (b)

For $x, y \in H$ let $o(x) = n$ and $o(y) = m$. Then

$$\begin{aligned} (xy)^{nm} &= x^{nm}y^{nm} \\ &= (x^n)^m(y^m)^n \\ &= e^m e^n \\ &= e \end{aligned} \tag{10}$$

There exists an integer nm such that $(xy)^{nm} = e$ so $\langle xy \rangle$ is finite and H is closed.

Part (c)

By Theorem 3.28, because $(1, -1) = 1$, $\langle x \rangle = \langle x^{-1} \rangle$. So if $x \in H$ then $x^{-1} \in H$. So H contains inverses.
H has satisfied all of the necessary conditions and is thus a subgroup of G.

Problem # 42

Let d be a positive integer and $\phi(d)$ the Euler-phi function. Use corollary 3.27 and the additive groups $\mathbb{Z}_d$ to show that

$$n = \sum_{d|n} \phi(d)$$

where the sum has one term for each positive divisor d of n.

Solution

Suppose that n is the order of some cyclic group G. Corollary 3.27 says that the distinct subgroups of finite cyclic group $G = \langle a \rangle$ are given by $\langle a^d \rangle$ where d is a positive divisor of n and that $\langle a^d \rangle$ has order k where $n = dk$. The function $\phi(d)$ tells us the number of distinct generators of a group of order d. Because the function is applied to every divisor of n the original expression is equivalent to writing

$$n = \sum_{kd=n} \phi(k)$$

This summation takes the total number of generators of each distinct subgroup of G and adds them together. We know that every element of G is the generator of a subgroup of G. So taking the sum of the number of generators for each distinct subgroup of G is equivalent to the number of elements in G which is equivalent to n.