Extra Problems 1 Solutions

1. Let \( G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| a \in \mathbb{R}, a \neq 0 \right\} \). Determine whether \( G \) is a group under matrix multiplication.

Yes.

- Let \( A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}, B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G \) where \( a, b \in \mathbb{R} \) are both nonzero. Then
  \[
  AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix}
  \]
  where \( 2ab \neq 0 \), so \( AB \in G \).
- Since matrix multiplication is associative on \( M_2(\mathbb{R}) \), it is also associative on the subset \( G \) of \( M_2(\mathbb{R}) \).
- \( \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \in G \) is the identity element for \( G \) because for any \( A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G \),
  \[
  \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \begin{bmatrix} a & a \\ a & a \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}.
  \]
- Let \( A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G \). Then the inverse of \( A \) in \( G \) is \( \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix} \) because
  \[
  \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix} \begin{bmatrix} a & a \\ a & a \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}.
  \]

2. Let \( X \) be a nonempty set. Determine whether \( \mathcal{P}(X) \), the set of all subsets of \( X \), is a group under the union operation.

No. The union operation is a binary operation on \( \mathcal{P}(X) \) since the union of any two subsets of \( X \) is still a subset of \( X \), and the operation is associative as well. For any \( A \in \mathcal{P}(X) \), \( A \cup \emptyset = \emptyset \cup A = A \), so \( \emptyset \) is an identity element for this binary structure. However, inverses do not always exist: take any nonempty subset \( A \) of \( X \) (which exists since \( X \neq \emptyset \)). Then \( A \cup B \neq \emptyset \) for all \( B \in \mathcal{P}(X) \), so \( A \) does not have an inverse.

3. Let \( G \) be a group. Prove that if \((ab)^2 = a^2b^2\) for all \( a, b \in G \), then \( G \) is abelian.

**Proof.** Let \( G \) be a group, and suppose that for all \( a, b \in G \), \((ab)^2 = a^2b^2\). Then, using left and right cancellation laws,

\[
(ab)^2 = a^2b^2 \Rightarrow abab = aabb \Rightarrow bab = abb \Rightarrow ba = ab
\]
for all \( a, b \in G \). Therefore, \( G \) is abelian.

4. \((\S 4, \#41)\) Let \( G \) be a group and \( g \) be one fixed element of \( G \). Show that the map \( i_g \), such that \( i_g(x) = gxg^{-1} \) for \( x \in G \), is an isomorphism of \( G \) with itself.

Proof. Let \( G \) be a group and fix an element \( g \in G \).

- Since \( G \) is a group, there exists \( g^{-1} \in G \). The map \( i_g \) is bijective because it has an inverse, namely \( i_{g^{-1}} \): for any \( x \in G \),

\[
(i_g \circ i_{g^{-1}})(x) = i_g \left( g^{-1}x \left( g^{-1} \right)^{-1} \right) = i_g \left( g^{-1}xg \right) = g \left( g^{-1}xg \right) g^{-1} = x
\]

\[
(i_{g^{-1}} \circ i_g)(x) = i_{g^{-1}} \left( gxg^{-1} \right) = g^{-1} \left( gxg^{-1} \right) g = x.
\]

- Let \( x, y \in G \). Then

\[
i_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = i_g(x)i_g(y),
\]

so \( i_g \) satisfies the homomorphism property.

5. Determine with \( S \) is a subgroup of \( G \).

(a) \( G = \mathbb{Z} \) with addition, \( S = \mathbb{Z}^\geq \), the set of nonnegative integers

No. The inverse of 1 is -1, which is not \( \mathbb{Z}^\geq \).

(b) \( G = F \), the set of all real-valued functions on \( \mathbb{R} \), with addition, \( S = \{ f \in F \mid f(1) = 0 \} \)

Yes.

- Let \( f, g \in S \). Since \((f + g)(1) = f(1) + g(1) = 0 + 0 = 0 \), \( f + g \in S \).
- Let \( f_0 \) denote the identity element of \( F \) (so \( f_0(x) = 0 \) for all \( x \in \mathbb{R} \)). Then \( f_0(1) = 0 \), so \( f_0 \in S \).
- Let \( f \in S \). Then \((-f)(1) = -f(1) = -0 = 0 \), so \(-f \in S \).

(c) \( G = M_n(\mathbb{R}) \) with addition, \( S = \{ A \in M_n(\mathbb{R}) \mid A^t = -A \} \)

Yes.

- Let \( A, B \in S \). Then \((A + B)^t = A^t + B^t = -A + (-B) = -(A + B) \), so \( A + B \in S \).
- Since \( 0^t = 0 = -0, 0 \in S \).
- Let \( A \in S \). Then \((-A)^t = -A^t = -(A) \), so \(-A \in S \).

6. (a) Let \( G \) be a group and \( H, K \leq G \). Prove that \( H \cup K \leq G \) if and only if \( H \subseteq K \) or \( K \subseteq H \).
Proof. Let $G$ be a group and $H, K \leq G$.

($\Rightarrow$) Suppose that $H \cup K \leq G$. Say that $H \not\subseteq K$. Then there exists $h \in H$ such that $h \not\in K$. We will show that $K \subseteq H$. Let $k \in K$. Since $h \in H \subseteq H \cup K$, $k \in K \subseteq H \cup K$, and $H \cup K \leq G$, by closure we know $hk \in H \cup K$. Then $hk \in H$ or $hk \in K$. Assume $hk \in K$. Since $K$ is a subgroup and $k \in K$, $k^{-1} \in K$. Then by closure, $hk \in H$ or $hk \in K$.

($\Leftarrow$) Suppose that $H \subseteq K$ or $K \subseteq H$. If $H \subseteq K$, then $H \cup K = K \leq G$. Similarly, if $K \subseteq H$, then $H \cup K = H \leq G$.

(b) Give an example of a group $G$ and subgroups $H_1, H_2, H_3$ of $G$ such that $H_1 \cup H_2 \cup H_3 \leq G$ and $H_i \not\subseteq H_j$ for all $i \neq j$.

Take $G$ to be the Klein four-group $V = \{e, a, b, c\}$ and $H_1 = \langle a \rangle$, $H_2 = \langle b \rangle$, $H_3 = \langle c \rangle$. Then $H_1 \cup H_2 \cup H_3 = G$ but $H_i \not\subseteq H_j$ for all $i \neq j$.

7. Let $a$ be an element of a group $G$. If the order of $a$ is $n$, prove that $a^k = e$ if and only if $n$ divides $k$.

Proof. Let $a$ be an element of a group $G$ and suppose that the order of $a$ is $n$.

($\Rightarrow$) Say that $a^k = e$. By the division algorithm, there exist integers $q, r$ such that $k = nq + r$ and $0 \leq r < n$. Then

$$e = a^k = a^{nq + r} = (a^n)^q a^r = e^q a^r = a^r.$$  

If $r > 0$, then this would contradict that fact that $n$ is the smallest positive integer such that $a^n = e$. Therefore, $r = 0$, so $k = nq$ and hence $n$ divides $k$.

($\Leftarrow$) Suppose that $n$ divides $k$. Then there exists $l \in \mathbb{Z}$ such that $nl = k$. So $a^k = a^{nl} = (a^n)^l = e^l = e$.

8. Let $G$ be a cyclic group generated by an element $a$. If the order of $G$ is $n$, prove that the generators of $G$ are the elements of the form $a^r$ where $r$ is relatively prime to $n$.

Proof. Let $G$ be a cyclic group generated by an element $a$, and suppose $|G| = n$. Then

$$a^r \text{ generates } G \iff \text{the order of } a^r \text{ is } n$$

$$\iff \frac{n}{\gcd(n, r)} = n$$

$$\iff \gcd(n, r) = 1.$$
9. Let $\phi : G \to G'$ be an isomorphism of a group $\langle G, * \rangle$ with a group $\langle G', *' \rangle$. Prove that if $G$ is cyclic, then $G'$ is also cyclic.

Proof. Let $\phi : G \to G'$ be an isomorphism of a group $\langle G, * \rangle$ with a group $\langle G', *' \rangle$. Suppose that $G$ is cyclic, so $G = \langle a \rangle$ for some $a \in G$. Let $g' \in G'$. Since $\phi$ is bijective, there exists $g \in G$ such that $\phi(g) = g'$. Since $G$ is generated by $a$, $g = a^n$ for some $n \in \mathbb{Z}$. This gives us

$$g' = \phi(g) = \phi(a^n) = (\phi(a))^n$$

by the homomorphism property, so $\phi(a)$ generates $G'$ and hence $G'$ is cyclic. \qed

10. How many generators does $\mathbb{Z}_{103}$ have? How many distinct subgroups does it have? Use the fact that 103 is a prime number.

There are $103 - 1 = 102$ generators of $\mathbb{Z}_{103}$ and only two distinct subgroups of $\mathbb{Z}_{103}$, since there is exactly one subgroup for each positive divisor of 103.