Hungerford: Algebra

I.1. Semigroups, Monoids and Groups

3. Is it true that a semigroup which has a \textit{left} identity element and in which every elements has a \textit{right} inverse is a group?

Solution Not necessarily. Here is an example of such a semigroup but not a group. Let \( S = \{ A, B \} \), where

\[
A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}.
\]

Since \( AA = A, AB = B, BA = A \) and \( BB = B \), matrix multiplication is a binary operation \( S \), in which \( A \) is a left identity of \( S \), and \( A \) is a right inverse for every element in \( S \). As matrix multiplication is associative, \( S \) is a semigroup with the desired properties. However, as \( BA \neq B \), the semigroup \( S \) does not have an identity, and so \( S \) is not a group.

4. Write out a multiplication table for the group \( D_4^* \).

Solution

\[
\begin{array}{cccccccc}
I & R & R^2 & R^3 & T_x & T_y & T_{13} & T_{24} \\
I & I & R & R^2 & R^3 & T_x & T_y & T_{13} & T_{24} \\
R & R & R^2 & R^3 & I & T_{13} & T_{24} & T_y & T_x \\
R^2 & R^2 & R^3 & I & R & T_y & T_x & T_{24} & T_{13} \\
R^3 & R^3 & I & R & R^2 & T_{24} & T_{13} & T_x & T_y \\
T_x & T_x & T_{24} & T_y & T_{13} & I & R^2 & R^3 & R \\
T_y & T_y & T_{13} & T_x & T_{24} & R^2 & I & R & R^3 \\
T_{13} & T_{13} & T_x & T_{24} & T_y & R & R^3 & I & R^2 \\
T_{24} & T_{24} & T_y & T_{13} & T_x & R_3 & R & R_2 & I \\
\end{array}
\]

8. (a) The relation given by \( a \sim b \iff a - b \in \mathbb{Z} \) is a congruence relation on the additive group \( \mathbb{Q} \).

(b) The set \( \mathbb{Q}/\mathbb{Z} \) of equivalence classes is an infinite abelian group.

Sketch of Proof

(reflexive) \( a \sim a \), since \( \forall a \in \mathbb{Q}, a - a = 0 \in \mathbb{Z} \).

(symmetric) If \( a - b \in \mathbb{Z} \), then \( b - a = -(a - b) \in \mathbb{Z} \) as well, \( a \sim b \) implies \( b \sim a \).
(transitive) Assume that both \(a \sim b\) and \(b \sim c\). Then \(a - b, b - c \in \mathbb{Z}\). It follows that 
\[a - c = (a - b) + (b - c) \in \mathbb{Z},\] 
and so \(a \sim c\).
(congruence relation) Let \(a_1 \sim a_2\) and \(b_1 \sim b_2\). We want to show that \(a_1 + b_1 \sim a_2 + b_2\).
But this follows from \((a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in \mathbb{Z}\).
(b) By Theorem 1.5, it suffices to show that \(\mathbb{Q}/\mathbb{Z}\) has infinitely many elements. Note that is \(m, n \in \mathbb{Z}\) with \(m > n > 1\), then \(1/m\) and \(1/n\) are in distinct equivalence classes, and so 
\(\phi : \mathbb{Z}^+ \to \mathbb{Q}/\mathbb{Z}\) by \(\phi(n) = 1/n\) is an injective map. Therefore, \(\mathbb{Q}/\mathbb{Z}\) contains a subset with as many elements as \(\mathbb{Z}\).

10. Let \(p\) be a prime and let \(\mathbb{Z}(p^\infty)\) be the following subset of the group \(\mathbb{Q}/\mathbb{Z}\):
\[
\mathbb{Z}(p^\infty) = \{a/p^i \in \mathbb{Q}/\mathbb{Z}| a, b \in \mathbb{Z} \text{ and } b = p^i \text{ for some } i \geq 0\}.
\]Show that \(\mathbb{Z}(p^\infty)\) is an infinite subgroup under addition operation of \(\mathbb{Q}/\mathbb{Z}\).

**Sketch of Proof** Pick and two elements \(a/p^i\) and \(b/p^j\) in \(\mathbb{Z}(p^\infty)\). We may assume that \(0 \leq i \leq j\). Then 
\[
\frac{a}{p^i} + \frac{b}{p^j} = (ap^{j-i} + b)/p^j \in \mathbb{Z}(p^\infty),
\]
and so addition is a binary operation in \(\mathbb{Z}(p^\infty)\). As a subset of \(\mathbb{Q}/\mathbb{Z}\), addition in \(\mathbb{Z}(p^\infty)\) is associative and commutative. Since \(\bar{0} = 0/p \in \mathbb{Z}(p^\infty)\) is the identity, and since for any \(a/p^i \in \mathbb{Z}(p^\infty)\), the additive inverse \(-a/p^i\) is also in \(\mathbb{Z}(p^\infty)\), \(\mathbb{Z}(p^\infty)\) is a group.

11. The following conditions on a group \(G\) are equivalent: (i) \(G\) is abelian; (ii) \((ab)^2 = a^2b^2\), \(\forall a, b \in G\); (iii) \((ab)^{-1} = a^{-1}b^{-1}\), \(\forall a, b \in G\); (iv) \((ab)^n = a^nb^n\), \(\forall n \in \mathbb{Z}\) and \(\forall a, b \in G\); (v) \((ab)^n = a^nb^n\), for three consecutive integers \(n\) and \(\forall a, b \in G\). Show that \((v) \Rightarrow (i)\) is false if "three" is replaced by "two".

**Sketch of Proof** (i) \(\Rightarrow\) (ii): \((ab)^2 = abab = aabb = a^2b^2\). (ii) \(\Rightarrow\) (i): Apply cancellation laws to \(abab = aabb\) to get \(ab = ba\). (i) \(\Rightarrow\) (iii): From \(ab = ba\), we have \((ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}\). (iii) \(\Rightarrow\) (i): Since \(ba(ab)^{-1} = baa^{-1}b^{-1} = e\), it follows by the uniqueness of inverse that \(ab = ba\). (i) \(\Rightarrow\) (iv): From (ii), (iii) and by induction on \(|n|\), we have \((an)^n = a^n b^n\). (vi) \(\Rightarrow\) (v): (v) is a special case of (vi). (v) \(\Rightarrow\) (i): Suppose that \((ab)^n = a^nb^n\) for \(n = k - 1, k, k + 1\). Then \(a^k b^k = (ab)^k = ab(\bar{a}b)^{k-1} = aba b^{-1}b^{-1}\). Apply this to get \((ab)^{k+1} = a^{k+1}b^{k+1} = a(a^k b^k)b = a^2b a^{-1}b^{-1}b = a^2b a^{-1}a b^{-1}b = a^2b a^{-1}(ab)^k\).

**Cancel** \((ab)^k\) from the right and \(a\) from the left to get \(b = aba^{-1}\), and so \(ba = ab\).

**Examples:** For any group \(G\), we always have \((ab)^0 = a^0 b^0\) and \((ab)^1 = a^1 b^1\). In particular,
this holds for any nonabelian group \( G \). If we are not allow to use 0 and 1, then we can consider \( G = D_4^* \), in which \((ab)^4 = e = a^4b^4\), and \((ab)^5 = ab = a^5b^5\).

14. If \( G \) is a finite group with even order, then \( G \) contains an element \( a \neq e \) such that 
\[ a^2 = e. \]

**Sketch of Proof** Define a relation on \( G \) such that \( \forall g_1, g_2 \in G, \ g_1 \) is related to \( g_2 \) if and only if \( g_1 = g_2 \) or \( g_1 = g_2^{-1} \). Verify that this is an equivalence relation, and the equivalence class containing \( g \) is \([g] = \{g, g^{-1}\}\). Note that for any \( g \in G - \{e\}, \ g^2 = e \) if and only if \(|[g]| = 1\). By contradiction, assume that for any \( a \neq e, \ a^2 \neq e \). Then every equivalence class contains exactly two elements, except the one containing \( e \), in which it has only one element. As the equivalence classes yields a partition of \( G \), \( G \) must have an odd order, contrary to the assumption that \(|G|\) is even.

15. Let \( G \) be a nonempty finite set with an associative binary operation such that for all \( a, b, c \in G, \ ab = ac \Rightarrow b = c \) and \( ba = ca \Rightarrow b = c \). Then \( G \) is a group. Show that this conclusion may be false if \( G \) is infinite.

**Sketch of Proof** (Comments before proof: If we can show the existence of the identity \( e \), then by Preposition 1.4, \( G \) is a group. Therefore, it suffices to show that \( G \) has an identity.) Let \( G = \{a_1, a_2, \ldots, a_n\} \). Define \( f : G \mapsto G \) by \( f(a_i) = a_1a_i \), \( 1 \leq i \leq n \). Since left cancellation law holds, \( f \) is an injection, and since \( G \) is finite, \( f \) is a bijection. Therefore, for some \( a \in G, \ a_1a = a_1 \). We shall show that \( aa_i = a_i = a_i a \) for any \( i \).

For any \( a_i \in G, \ a_1aa_i = a_1a_i \), and so by left cancellation law, we have \( aa_i = a_i \). In particular, we have \( aa_1 = a_1 \). For any \( a_i \in G, \ a_1aa_1 = a_1a_1 \), and so by right cancellation law, we have \( a_i a = a_i \).

**Example:** Let \( G \) be the set of all positive integers with addition. Then both cancellation laws hold but \( G \) is not a group.