Topics in Algebra, Chapter 2 Solutions

David Sillman

2022

2.3 - Groups

(1a) $G = (\mathbb{Z}, -)$ does not form a group because it does not satisfy associativity:

$$a - (b - c) = a - b + c \qquad (a - b) - c = a + b - c$$

(1b) $G = (\mathbb{Z}, \cdot)$ does not form a group because it does not contain multiplicative inverses for all integers,

$$ab = 1 \quad \Leftrightarrow \quad a = b = \pm 1$$

(1c) $G = (\{a_i\}, \cdot)$ forms a group because it satisfies (1) closure, (2) associativity, (3) identity and (4) inverse:

$$a_i \cdot a_j = a_{i+j} \quad \text{s.t.} \quad 0 \leq i + j \leq 6 \tag{1}$$

$$a_i \cdot (a_j \cdot a_k) = a_i \cdot a_{j+k} = a_{i+j+k} = a_{i+j} \cdot a_k = (a_i \cdot a_j) \cdot a_k \tag{2}$$

$$a_i \cdot a_0 = a_{i+0} = a_i = a_{0+i} = a_0 \cdot a_i \tag{3}$$

$$a_i \cdot a_{7-i} = a_{i+7-i} = a_0 = a_{7-i+i} = a_{7-i} \cdot a_i \tag{4}$$

2.3 - Groups

(1d) $G = (\mathbb{Q}^{\text{odd}}, +)$ forms a group because it satisfies (1) closure, (2) associativity, (3) identity and (4) inverse:

$$\frac{a}{b}, \frac{a'}{b'} \in \mathbb{Q}^{\text{odd}} \quad \Rightarrow \quad \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'} \in \mathbb{Q}^{\text{odd}} \tag{1}$$

$$\frac{a}{b} + \left(\frac{a'}{b'} + \frac{a''}{b''}\right) = \left(\frac{a}{b} + \frac{a'}{b'}\right) + \frac{a''}{b''} \tag{2}$$

$$\frac{a}{b} + \frac{0}{1} = \frac{0}{1} + \frac{a}{b} = \frac{a}{b} \tag{3}$$

$$\frac{a}{b} + \frac{-a}{b} = \frac{-a}{b} + \frac{a}{b} = \frac{0}{b} = \frac{0}{1} \tag{4}$$

2.3 - Groups

(2) If G is abelian, then we can expand, commute and regroup terms:

$$(a \cdot b)^n = (a \cdot b) \cdots (a \cdot b) = a \cdots a \cdot b \cdots b = a^n \cdot b^n$$

(3) Expanding and disassociating the product, we get $(a \cdot b)^2 = (a \cdot b)(a \cdot b) = a \cdot b \cdot a \cdot b$. For the equality $a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b = a^2 \cdot b^2$ to hold, we can left-multiply by a^{-1} and right-multiply by b^{-1}:

$$a^{-1} \cdot a \cdot b \cdot a \cdot b \cdot b^{-1} = a^{-1} \cdot a \cdot a \cdot b \cdot b \cdot b^{-1}$$
$$\Downarrow$$
$$b \cdot a = a \cdot b$$

Which shows that every pair $a, b \in G$ must commute, which means G is abelian.

2.3 - Groups

(4) Let $i \in \mathbb{Z}$ be the least of the 3 consecutive integers which satisfy the equation. If $i = 0$, then the result of problem (3) trivially proves the result. Otherwise, if $i > 0$, then let $x = (a \cdot b)^i = a^i \cdot b^i$. Then, we have $x \cdot a \cdot b = a \cdot x \cdot b$. We cancel the rightmost b on both sides, giving $a \cdot x = x \cdot a$, which means we can move a from one side of x to the other. This implies that

$$a^2 \cdot x \cdot b^2 = x \cdot (a \cdot b)^2$$
$$a \cdot x \cdot a \cdot b^2 = x \cdot (a \cdot b)^2$$
$$x \cdot a^2 \cdot b^2 = x \cdot (a \cdot b)^2$$
$$a^2 \cdot b^2 = (a \cdot b)^2$$

Which then gives us the statement from problem (3), which trivially shows that $a \cdot b = b \cdot a$ for any pair $a, b \in G$. Therefore, G is abelian.

2.3 - Groups

(5) If we don't have $a^{i+2} \cdot b^{i+2} = (a \cdot b)^{i+2}$, then we can still show that $a \cdot x = x \cdot a$ with $x = a^i \cdot b^i = (a \cdot b)^i$. Canceling out x now only gives us the trivial tautology,

$$
\begin{aligned}
a \cdot x \cdot b &= x \cdot a \cdot b \\
x \cdot a \cdot b &= x \cdot a \cdot b \\
a \cdot b &= a \cdot b
\end{aligned}
$$

Which does not necessitate nor imply that $a \cdot b = b \cdot a$, and so we don't guarantee that G is abelian.

2.3 - Groups

(6) In S_3, we have two elements (transpositions) $a = (1\ 2)$ and $b = (2\ 3)$ satisfying $a^2 = e$ and $b^2 = e$. They multiply to give $a \cdot b = (1\ 2) \cdot (2\ 3) = (1\ 2\ 3)$. Squaring each and multiplying them gives:

$$a^2 \cdot b^2 = e \cdot e = e$$

Whereas multiplying them, then squaring, gives:

$$(a \cdot b)^2 = (1\ 2\ 3)^2 = (1\ 3\ 2) \neq e$$

(7) The elements of order 2 in S_3 are the *transpositions* and identity, which are

$$(1\ 2)^2 = (2\ 3)^2 = (1\ 3)^2 = e^2 = e$$

The elements of order 3 in S_3 are the *shifts* and identity, which are

$$(1\ 2\ 3)^3 = (1\ 3\ 2)^3 = e^3 = e$$

2.3 - Groups

(8) First, I argue that $a^i = a^j$ for two positive integers, $0 < i < j$. This comes from the fact that G has a finite number of elements, $|G| \in \mathbb{N}$, and so for multiplication by a to be closed, a^i must be one of the $|G|$ elements for all $i \in \mathbb{Z}$. By the pigeonhole principle, $a^{|G|}$ must be in $\{e, a, a^2, \ldots, a^{|G|-1}\}$. Therefore, we have $a^i = a^{|G|}$ for some $0 \leq i < |G|$.

With this equality, we can left-multiply through by $(a^i)^{-1}$, which gives $a^{|G|-i} = e$, where $|G| - i$ is a positive integer, which proves the result.

2.3 - Groups

(9a) If G has 3 elements, then either it contains:

$$G = \{e, a, a^{-1}\} \qquad \text{with } a \neq a^{-1}$$
$$G = \{e, a, b\} \qquad \text{with } a = a^{-1} \text{ and } b = b^{-1}$$

The former is trivially abelian. In the latter, we must try to assign the element $a \cdot b$. If $a \cdot b = a$ or $a \cdot b = b$, then this implies $b = e$ or $a = e$, respectively. To avoid contradiction, we assign $a \cdot b = e$. Inverting both sides gives $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = b \cdot a = e$, which means $a \cdot b = b \cdot a$, so G is abelian.

2.3 - Groups

(9b) If G has 4 elements, then we can consider the act of left-multiplying by any non-identity element $a \in G$ as a map, $l : G \to G$ which maps $e \mapsto a$ and $a^{-1} \mapsto e$. This defines assignments for two of the four elements of G. Neither of the two remaining elements, $x, y \in G$ can be mapped to themselves, as this would imply $a = e$. All of the above argument holds for the right-multiplication map, $r : G \to G$, and so the act of left- and right-multiplication in G are identical, meaning $a \cdot b = b \cdot a$. So, G is commutative.

2.3 - Groups

(9c) Suppose G has 5 elements. If we choose a non-identity element $a \in G$ at random, there are two cases:

(i) $a^5 = e$: in this case, every element is expressible as a^i, and so $a^i \cdot a^j = a^j \cdot a^i$ by associativity, so G is trivially abelian.

(ii) $a^i = e$ for $1 < i < 5$: in this case, for any other element $b \in G$, we need $a \cdot b, b \cdot a, a \cdot b \cdot a \in G$. If we assume non-abelian properties, we require that all of these products be distinct, and so G must contain at least $G = \{e, a, b, a \cdot b, b \cdot a, a \cdot b \cdot a\}$, which is more than 5 elements, so we have a contradiction.

Therefore, any 5-element group must be abelian.

2.3 - Groups

(10) Indeed, if every element $a \in G$ satisfies $a^{-1} = a$, then $a \cdot b \in G$ satisfies $a \cdot b = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = b \cdot a$, and so G is abelian.

(11) Let $|G| = 2n$ and $\phi : G \to G$ be the map which sends $a \mapsto a^{-1}$, which is a bijection satisfying $\phi^2(a) = a$. Trivially, $\phi(e) = e$. This means there remain $2n - 1$ unassigned elements in the domain and range. Each new assignment $\phi(a) = a'$ assigns $\phi(a') = a$, and so assignments can only be made in pairs. Ultimately, when there remains only 1 unassigned element $x \in G$, we must assign $\phi(x) = x$ for that x. Therefore, any even-order group G must have some $a \in G$ satisfying $a^2 = e$.

2.3 - Groups

(12) Taking the expression $a \cdot e = a$ and right-multiplying by $y(a)$ gives us $a \cdot e \cdot y(a) = a \cdot y(a) = e$, which shows $e \cdot a = a \cdot e$. Substitution on the left gives $a \cdot y(a) \cdot a = a$, which associates to give $a \cdot (y(a) \cdot a) = a$, so $y(a) \cdot a = e$. Therefore, both inverses and the identity commute. So, G is a group.

(13) Consider the set $G = \mathbb{Z}$ closed under the associative product $a \cdot b = a$. Trivially, we have $a \cdot 1 = a$, and the $y(a)$ which satisfies $y(a) \cdot a = 1$ will be $y(a) = 1$ for all a. Clearly, this satisfies all conditions without forming a group, as neither identity nor inverses are unique.