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,

$$a \cdot x \cdot b = x \cdot a \cdot b$$
$$x \cdot a \cdot b = x \cdot a \cdot b$$
$$a \cdot b = a \cdot b$$

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.

2.3 - Groups

(14) The cancellation properties tell us that $x \cdot a = y \cdot a \Rightarrow x = y$. This means that both the left- and right-multiplication maps $l_a : x \mapsto a \cdot x$, $r_a : x \mapsto x \cdot a$ are injective, and because their domains and codomains are *finite*, the maps are bijective. Thus, the cosets $aG = Ga = G$.

This also means that, for any element $a \in G$, there must be some element $\varepsilon(a) \in G$ which solves $a \cdot \varepsilon(a) = a$.
Left-multiplying both sides by any other element $b \in G$ shows that this $\varepsilon(a)$ must be universal, as $b \cdot a \cdot \varepsilon(a) = b \cdot a$. Therefore, there must be an identity element $e \in G$.

Similarly, there must be an element a^{-1} in G which solves $a \cdot a^{-1} = e$ for any a. Right-multiplying by a and re-associating, we see that this a^{-1} also solves $a \cdot (a^{-1} \cdot a) = e \cdot a = a = a \cdot e$, and so inverses are included in G for every element.

2.3 - Groups

(15a) We know that remainder classes, $[i], [j] \in J_p$ are finite and satisfy associativity and closure under multiplication. To show cancellation is satisfied, we first note that every integer i has $\gcd(i, p) = 1$, meaning there exist integers a, b solving $ai + bj = 1$, meaning there is an $[a] \in J_p$ which multiplies with $[i]$ to yield the remainder class $[1]$, and so we can use:

$$\begin{aligned} [i] \cdot [j] &= [i] \cdot [k] \\ [a] \cdot [i] \cdot [j] &= [a] \cdot [i] \cdot [k] \\ [1] \cdot [j] &= [1] \cdot [k] \\ [j] &= [k] \end{aligned}$$

The same argument shows that right cancellation is satisfied. So, by problem (14), the integers modulo p are a group under multiplication.

2.3 - Groups

(15b) We write the set of coprime-to-n integers as C_n. This set still satisfies the invariant that $\gcd(i, n) = 1$ for any $i \in C_n$. Therefore, each and every element can be made to solve $[i] \cdot [i^{-1}] = [1]$ which, as in part (a), entails both cancellation properties.

(16) Consider J_p for prime p under the associative product $a * b = a$. Clearly, left-multiplication is injective, thus bijective, and so we have the right-cancellation property, $a \cdot b = c \cdot b$ implies $a = c$ by definition. We don't have the left-cancellation property, as the value of $b * a$ has nothing to do with the right operand. As a result, as discussed in problem (13), this associative product does not a group make.

2.3 - Groups

(17) The set of integers, $\mathbb{Z}$, under multiplication is associative, closed and satisfies both cancellation properties. However, because there is no method of inverting an arbitrary integer into another integer, e.g. solving $x \cdot y = 1$ with x or y being greater than 1. Therefore, $(\mathbb{Z}, \cdot)$ cannot be a group and we have an infinite example which fails the conclusion of problem (14).

(18) We construct a non-abelian group G_n of order $|G_n| = 2n$ via the actions of *rotation* and *reflection* on a regular n-gon. This group has the act r of rotating by $2\pi/n$ radians (shifting vertex indices) which satisfies $r^n = e$. The group is completed by including reflection f across one of its n interior angle bisectors, which satisfies $f^2 = e$. Clearly, reflections and rotations do not commute, but do generate all $2n$ rigid transformations of a regular n-gon, which is a nonabelian group.

2.3 - Groups

(19) If we use $n = 3$, then the base case is proven by the definition of associativity: $a_1 \cdot a_2 \cdot a_3 = a_1 \cdot (a_2 \cdot a_3) = (a_1 \cdot a_2) \cdot a_3$.

If we suppose the result holds for any collection of $n \leq k$ elements a_i, then any bracketing of $a_1 \cdot a_2 \cdot \cdots \cdot a_k$ will result in the same product. Right-multiplying by a_{k+1} produces the product $a_1 \cdot a_2 \cdot \cdots \cdot a_k \cdot a_{k+1}$. Any means of bracketing this product will result in some product of bracketed products, each with size less than k, meaning each of them can be bracketed any way we want without changing the value. Therefore, we've shown the result for $n = k + 1$. So, by induction, associativity means we can re-bracket any product without affecting the value of the product.

2.3 - Groups

(20) First, we note closure. Because $\det(\mathbf{A}), \det(\mathbf{B}) \in \mathbb{Q}$, we have that $\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B}) \in \mathbb{Q}$ because the rationals are closed under multiplication. Associativity is inherited from the process of matrix multiplication. We still contain the identity $\mathbf{I}_2$ in the set, so we have an $\mathbf{AI} = \mathbf{IA} = \mathbf{A}$. Moreover, because $\det(\mathbf{A}^{-1}) = 1/\det(\mathbf{A})$ which is also rational, $\mathbf{A}$ being in the set implies that $\mathbf{A}^{-1}$ is also in it. Therefore, the set is a group.

2.3 - Groups

(21) We note closure by the fact that the lower-left element of **AB** will be $a_{0,0} \cdot 0 + 0 \cdot b_{1,1} = 0$, so the product is in the set. Associativity is again inherited from the process of matrix multiplication. Indeed, the identity $\mathbf{I}_2$ is in the set as well. Lastly, the inverse of a given matrix will fit the same upper-triangular footprint, so inverses are closed as well:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & -b/da \\ 0 & 1/d \end{pmatrix}$$

Any given product in this group will take the form,

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix}$$

Because it need not be the case that $ab' + bd' = ba' + db'$, the group is not abelian.

2.3 - Groups

(22) The product,

$$\mathbf{AB} = \begin{pmatrix} ab & 0 \\ 0 & a^{-1}b^{-1} \end{pmatrix} = \begin{pmatrix} ba & 0 \\ 0 & b^{-1}a^{-1} \end{pmatrix} = \mathbf{BA}$$

illustrates both the closure and abelian properties of the group. Associativity follows from the process of matrix multiplication. It contains the identity $\mathbf{I}_2$, and we have inverses

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$$

and so the set is an abelian group.

2.3 - Groups

(23) We construct the subgroup $H \subset G$,

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

It is closed, associative, contains the identity and inverses (every element is idempotent), and is fully contained in G. Therefore, it is a subgroup of order 4.

2.3 - Groups

(24) Enforcing the determinant condition, our set can contain,

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}$$

Associativity is inherited from matrix multiplication, and the identity is present. Closure can be intuited from the "determinant-as-area" interpretation of the determinant condition; a sequence of linear maps which scale the area of regions by an odd factor must also scale the area of regions by an odd factor. The last two elements are inverse to one another, while the first four are their own inverses. Thus, G is a group.

2.3 - Groups

(25a) Let $\gamma : J_3 \to \mathcal{P}(J_3 \times J_3)$ be a function which maps $[k] \in J_3$ to the pairs of elements $[i], [j] \in J_3$ satisfying $[i][j] = [k]$. The total number of elements in $M_2(J_3)$ will be $3^4 = 81$, but some of these do not satisfy $ad - bc \neq 0$. We now note that $\gamma([0]) = \{([i], [0]), ([0], [i]) \mid [i] \in J_3\}$, so $|\gamma([0])| = 2 \cdot 2 + 1 = 5$. Therefore, there are $5 \cdot 5 = 25$ cases in which $ad = 0, bc = 0$ and so $ad - bc = 0$, which brings satisfactory cases down to $81 - 25 = 56$. Lastly, we have

$$\gamma([1]) = \{([1], [1]), ([2], [2])\}$$
$$\gamma([2]) = \{([1], [2]), ([2], [1])\}$$

And so there are $2 \cdot 2 = 4$ cases of each instance wherein $ad = bc = 1$ and $ad = bc = 2$, which subtract off another $4 + 4 = 8$ instances, bringing $o(G)$ down to 48. Every such element now satisfies $ad - bc \neq 0$, and $o(G) = 48$ as desired.

2.3 - Groups

(25b) We note that $ad - bc = 2$ if $(ad, bc) \in \{(2, 0), (1, 2), (0, 1)\}$. Because we've computed γ-values for each of these remainder classes in the last problem, we can subtract them off by case. In the $(2, 0)$ and $(0, 1)$ cases, we have $2 \cdot 5 = 10$ matrices each, bringing our total down to $48 - 20 = 28$. In the last case, we have $2 \cdot 2 = 4$ unsatisfactory cases, leaving the total $28 - 4 = 24$, so our new size is $o(G) = 24$.

2.3 - Groups

(26a) We can consider constructing an element of G as choosing one of the $p^2 - 1$ nonzero vectors in $J_p \times J_p$, then choosing another linearly independent nonzero vector. Each nonzero vector has p multiples which are not linearly independent, so this means each of our $(p^2 - 1)$ first vectors can be paired with $(p^2 - p)$ partners, which constructs $(p^2 - 1)(p^2 - p)$ elements of G. So,

$$o(G) = (p^2 - 1)(p^2 - p)$$

(26b) If we once again fix our first row to be one of $(p^2 - 1)$ nonzero vectors, we then will have as many options for the second row as there are solutions to $[a]x - [b]y = 1$, which is p solutions. This tells us that our subgroup will have size,

$$o(H) = (p^2 - 1)p$$

2.5 - Subgroups

(1) Because both H and K are subgroups, $e \in H$ and $e \in K$, so $e \in H \cap K$. If any a, b are in H and in K, then to enforce closure in both subgroups $ab \in H$, $ab \in K$, so $ab \in H \cap K$. Likewise, inverses are contained in $H \cap K$. Thus, $H \cap K$ must be a subgroup.

By this argument (and associativity of intersection), one can inductively prove that any finite sequence of intersections will yield a subgroup. In the infinite case, the only element which must necessarily appear in any subgroup of G is e, so the smallest infinite intersection can result in (e), the trivial subgroup. Therefore, even infinite intersections will yield a subgroup.

2.5 - Subgroups

(2) Suppose, for the sake of contradiction, that there exists a non-idempotent element $a \in G$, i.e. one that satisfies $a^n \neq e$. Then we construct the following sequence $\{S\}_k$ of abelian subgroups for $k > 1$:

$$S_k = \left\{ \left(a^{\pm ik}\right) \mid i \in \mathbb{Z} \right\}$$

The intersection of all of these subgroups, $\bigcap_k \{S\}_k$ cannot contain any non-identity a^n. If it did, it would imply that S_{n+1} contained a^n, which can only be the case if n is a multiple of $n+1$, which is absurd. Thus, the intersection subgroup $\bigcap_k \{S\}_k = (e)$. This contradicts our assumption, so every element of G must have finite order.

2.5 - Subgroups

(3) If we assume that G is infinite, then by the contrapositive of problem (2), G must have a nontrivial subgroup and so we have a contradiction. So, G is finite.

The finitude of G implies that there exists an $a \in G$ which satisfies $a^{o(G)} = a$. If $o(G) = pq$ is composite, then $b = a^p \in G$ generates a subgroup (b) with $b^q = e$ implying an order of $o((b)) = q$, so we have a nontrivial subgroup. Therefore, by contradiction, G must have a prime order.

2.5 - Subgroups

(4a) Because $e \in H$, we have that $aea^{-1} = aa^{-1} = e \in aHa^{-1}$. Moreover, $(aha^{-1})^{-1} = ah^{-1}a^{-1}$, which is in aHa^{-1} because $h^{-1} \in H$. Multiplying two elements in aHa^{-1} results in a product,

$$(aha^{-1})(ah'a^{-1}) = ah(a^{-1}a)h'a^{-1} = ahh'a^{-1}$$

which is also in the set. So, we have closure, identity, and inverse so aHa^{-1} is a subgroup of G.

(4b) We denote $\sigma : H \to aHa^{-1}$ as the *canonical map* which sends $\sigma(h) = aha^{-1}$. Due to the cancellation property in H as a group, this map is injective and thus a bijection. Because the domain and codomain are finite, $o(H) = o(aHa^{-1})$.

2.5 - Subgroups

(5) If G is abelian, then $aH = Ha$ and so there is an obvious bijection (and thus one-to-one correspondence) between left- and right-cosets via the identity map.

We already know that there is a one-to-one correspondence between the elements of G with one another via the injective inverse map $\iota : g \mapsto g^{-1}$. Likewise, we can map the left-cosets to the right-cosets via $I : GH \to HG$ which sends $I(aH) = H\iota(a) = Ha^{-1}$ injectively. Thus, there is a one-to-one correspondence between the left- and right-cosets via I.

2.5 - Subgroups

(6a) The two right-cosets are

$$He = \{e, a^2, a^4, a^6, a^8\} \qquad Ha = \{a, a^3, a^5, a^7, a^9\}$$

(6b) There are five right-cosets:

$$He = \{e, a^5\} \qquad Ha = \{a, a^6\}$$
$$Ha^2 = \{a^2, a^7\} \qquad Ha^3 = \{a^3, a^8\}$$
$$Ha^4 = \{a^4, a^9\}$$

(6c) We interpret G as S_3 and H as $\{e, (2\ 3)\}$. We then have three right-cosets:

$$He = \{e, (2\ 3)\} \qquad H(1\ 2) = \{(1\ 2), (1\ 3\ 2)\}$$
$$H(1\ 3) = \{(1\ 3), (1\ 2\ 3)\}$$

2.5 - Subgroups

(7a) The two left-cosets are

$$eH = \{e, a^2, a^4, a^6, a^8\} \qquad aH = \{a, a^3, a^5, a^7, a^9\}$$

(7b) There are five left-cosets:

$$eH = \{e, a^5\} \qquad aH = \{a, a^6\}$$
$$a^2H = \{a^2, a^7\} \qquad a^3H = \{a^3, a^8\}$$
$$a^4H = \{a^4, a^9\}$$

(7c) We interpret G as S_3 and H as $\{e, (2\ 3)\}$. We then have three left-cosets:

$$eH = \{e, (2\ 3)\} \qquad (1\ 2)H = \{(1\ 2), (1\ 2\ 3)\}$$
$$(1\ 3)H = \{(1\ 3), (1\ 3\ 2)\}$$

2.5 - Subgroups

(8) No; in case (c), the left-coset $(1\ 2)H$ is not a right-coset Ha for any $a \in S_3$.