Groups, Fields, and Vector Spaces

Homework #2 (2018-2019), Answers

Q1: Building larger groups from smaller ones: the general setup

Say H and K are groups, with identity elements e_H *and* e_K *and group operations* $\circ_H$ *and* $\circ_K$*. We define the "direct product" of H and K, denoted* $G = H \times K$ *, as follows. The elements of G are ordered pairs of elements of H and K, with a typical element denoted* $g_i = h_i \times k_i$ *with* h_i *in H and* k_i *in K. We define an operation* $\circ_G$ *in G by* $(h_1 \times k_1) \circ_G (h_2 \times k_2) = (h_1 \circ_H h_2) \times (k_1 \circ_K k_2)$*, i.e., the elements of G combine component-wise, according to the operations in their respective groups.*

A note on terminology – direct product and direct sum – the terminology is very inconvenient. The "direct product" of two groups is synonymous with the "direct sum", which is denoted $G = H \oplus K$*. "Direct sum" (or "direct product") of groups are directly analogous to the "direct sum" or "direct product" construction for vector spaces. But unfortunately the term "direct product" is usually used for groups, and the term "direct sum" is usually used for vector spaces. To avoid confusion with other standard presentations, we will use this unfortunate convention. A further note – for combining an infinite number of groups (or vector spaces), there is a distinction between the direct sum and the direct product– but this is irrelevant to us.*

Show that the set of g_i *form a group, G.*

We need to demonstrate associativity, the existence of an identity element, and the existence of inverses.

G1: Associativity – this follows because the operation in *G* is component by component, and associativity holds in *H* and *K*. Formally, we decompose, then carry out the group operations in the component groups, then re-compose.

$$\left(g_1 \circ_G g_2\right) \circ_G g_3 = \left((h_1 \times k_1) \circ_G (h_2 \times k_2)\right) \circ_G (h_3 \times k_3) = \left((h_1 \circ_H h_2) \times (k_1 \circ_K k_2)\right) \circ_G (h_3 \times k_3)$$
$$= \left((h_1 \circ_H h_2) \circ_H h_3\right) \times \left((k_1 \circ_K k_2) \circ_K k_3\right),$$

where we have used the definition of the operation $\circ_G$. Since *H* and *K* are groups, their group operations are associative. So $\left((h_1 \circ_H h_2) \circ_H h_3\right) \times \left((k_1 \circ_K k_2) \circ_K k_3\right) = h_1 \circ_H \left(h_2 \circ_H h_3\right) \times k_1 \circ_K \left(k_2 \circ_K k_3\right)$.

We now invert the steps of the first line to reassemble elements in *G*:

$$\left(h_1 \circ_H (h_2 \circ_H h_3)\right) \times \left(k_1 \circ_K (k_2 \circ_K k_3)\right) = (h_1 \times k_1) \circ_G \left((h_2 \circ_H h_3) \times (k_2 \circ_K k_3)\right) = (h_1 \times k_1) \circ_G \left((h_2 \times k_2) \circ_G (h_3 \times k_3)\right)$$
$$= g_1 \circ_G \left(g_2 \circ_G g_3\right)$$

G2: Identity. We'll show that the identity in *G* is given by $e_G = e_H \times e_K$, where e_H and e_K are the identities for *H* and *K*. To see that it is a right identity, we consider an arbitrary $g = h \times k$:
$g \circ_G e_G = (h \times k) \circ_G (e_H \circ e_K) = (h \circ_H e_H) \times (k \circ_K e_K) = h \times k = g$, where the next-to-last equality holds because e_H and e_K are the identities for *H* and *K*. Left identity works similarly.

G3: Inverses. We'll show that the inverse of $g = h \times k$ is given by $g^{-1} = h^{-1} \times k^{-1}$, where h^{-1} and k^{-1} are the inverses of h and k in *H* and *K*, respectively:
$g \circ_G g^{-1} = (h \times k) \circ_G (h^{-1} \times k^{-1}) = (h \circ_H h^{-1}) \times (k \circ_K k^{-1}) = e_H \times e_K = e_G$, where the next-to-last equality holds because h^{-1} and k^{-1} are the inverses of h and k in *H* and *K*. Left inverse works similarly.

Q2: Building larger groups from smaller ones: examples

Recall that $\mathbb{Z}_p$ is the group containing the elements $\{0,1,\ldots,p-1\}$, with the group operation of addition mod p – the "cyclic group" of p elements. We denote the group operation by $+$, and use αx as a shorthand for $x + x + \ldots + x$ a total of α times.

A. How many elements are in $\mathbb{Z}_p \times \mathbb{Z}_q$?
pq. There are *p* elements in $\mathbb{Z}_p$ and *q* elements in $\mathbb{Z}_q$;every combination produces a different element of $\mathbb{Z}_p \times \mathbb{Z}_q$
B. Is $\mathbb{Z}_3 \times \mathbb{Z}_5$ isomorphic to $\mathbb{Z}_{15}$? Hint: let h be a non-identity element of $\mathbb{Z}_3$, and k be a non-identity element of $\mathbb{Z}_5$. What is the order of $h \times k$?
Use the hint. We know that the order of $h \times k$ must be a factor of the size of the group $\mathbb{Z}_3 \times \mathbb{Z}_5$, which is 15. So its order must be either 1, 3, 5, or 15. We also know that *h* is order 3 and *k* is order 5 (since their orders must divide the sizes of their groups). Using the shorthand of αx for $x + x + \ldots + x$ a total of α times, $3(h \times k) = 3h \times 3k = e_{\mathbb{Z}_3} \times 3k$, which is not the identity. Similarly, $5(h \times k) = 5h \times 5k = 2h \times 5k = 2h \times e_{\mathbb{Z}_5}$, also not the identity. So $h \times k$ must have order 15. We now have an isomorphism φ from $\mathbb{Z}_3 \times \mathbb{Z}_5$ to $\mathbb{Z}_{15}$ by mapping $h \times k$ to 1. This determines the entire mapping φ since each of the elements of $\mathbb{Z}_3 \times \mathbb{Z}_5$ must be equal to some $\alpha(h \times k)$ (by counting up the possibilities for $\alpha(h \times k)$).

C. Is $\mathbb{Z}_3 \times \mathbb{Z}_4$ isomorphic to $\mathbb{Z}_{12}$?
Yes argument in B works here.

D. Is $\mathbb{Z}_3 \times \mathbb{Z}_6$ isomorphic to $\mathbb{Z}_{18}$?
No. Every element of $\mathbb{Z}_3 \times \mathbb{Z}_6$ has order at most 6, since
$6(h \times k) = 6h \times 6k = 2(3h) \times 6k = 2e_{\mathbb{Z}_3} \times e_{\mathbb{Z}_6} = e_{\mathbb{Z}_3} \times e_{\mathbb{Z}_6}$, the identity of $\mathbb{Z}_3 \times \mathbb{Z}_6$.

E. Formulate a hypothesis for when $\mathbb{Z}_p \times \mathbb{Z}_q$ is isomorphic to $\mathbb{Z}_{pq}$, and (optionally) prove it.
If *p* and *q* are relatively prime, $\mathbb{Z}_p \times \mathbb{Z}_q$ is isomorphic to $\mathbb{Z}_{pq}$. Sketch of proof: if *p* and *q* are relatively prime, then the argument used in part *B* shows that the order of $h \times k$ is *pq* – since it must be both a multiple of *p* and a multiple of *q*. Conversely, say the largest common factor of *p* and *q* is some $r > 1$. Then *p* and *q* are both factors of $N = pq/r$. Then the order of every element of $\mathbb{Z}_p \times \mathbb{Z}_q$ *must be a factor of* $N = pq/r$, and therefore no element of $\mathbb{Z}_p \times \mathbb{Z}_q$ has order *pq*. On the other hand, the element

1 of $\mathbb{Z}_{pq}$ has order *pq*. So $\mathbb{Z}_p \times \mathbb{Z}_q$ and $\mathbb{Z}_{pq}$ have intrinsically different structure, and cannot be isomorphic.

Q3: Subgroups generated by the parity homomorphism

A. Consider the group of rotations and reflections of the square. Note that it has 8 elements. Label the corners of the square by W, X, Y, and Z in cyclic order. Which group elements correspond to even permutations, and which group elements correspond to odd permutations? Verify that the subset corresponding to even permutations is a subgroup.

Trivial motion: even permutation
Rotation by 90 deg: (WXYZ) or (WZYZ), odd permutations
Rotation by 180 deg: (WY)(XZ), even permutation
Mirror horizontally or mirror vertically: (WX)(YZ) or (WZ)(YX), even permutations
Mirror on diagonals: (WY) and (XZ), odd permutations
Subset of even permutations is the 180 deg rotation and the flips along the axes.

B. Same setup as above, but now label the edges of the square in cyclic order as p,q,r, and s. Which group elements correspond to even permutations, and which group elements correspond to odd permutations? Verify that the subset corresponding to even permutations is a subgroup.

Trivial motion: even permutation
Rotation by 90 deg: (pqrs) or (psrq), odd permutations
Rotation by 180 deg: (pr)(qs), even permutation
Mirror horizontally and mirror vertically: (pr) or (qs), odd permutations
Mirror on diagonals: (ps)(qr) and (pr)(qs), even permutations
Subset of even permutations is the 180 deg rotation and the flips along the diagonals.

C. Similar setup as above, but consider motions of a pentagon, with vertices labeled V, W, X, Y, and Z in cyclic order.

Trivial motion: even permutation
Rotation by 108 deg: (VWXYZ), (VZYXW), even permutations
Rotation by 216 deg: (VXZWY), (VYWZX), even permutations
Flip along one corner and one edge midpoint: (WZ)(XY), or (VX)(YZ), or (WY) (VZ), or (XZ)(VW), or (VY)(WX), all even permutations
Subset of even permutations is the entire group.