Groups, Fields, and Vector Spaces

Homework #2 (2014-2015), 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.

A. 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.

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

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

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

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

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.

B. (optional) For any three groups H, K, and M, construct an isomorphism from $G_{left} = (H \times K) \times M$ into $G_{right} = H \times (K \times M)$. That is, show the results of applying φ to a typical element $g = (h \times k) \times m$ in G_{left} by displaying $\varphi(g)$ in G_{right}, and verify that the group structure of G_{right} is preserved. This result means that we don't care about parentheses in a triple (or larger) direct product, since G_{left} and G_{right} are indistinguishable.

For $g = (h \times k) \times m$, we define by $\varphi(g) = h \times (k \times m)$.
φ is invertible, as $\varphi^{-1}\big(h \times (k \times m)\big) = (h \times k) \times m$.

To show that φ is an isomorphism, we need to check that $\varphi(g_1) \circ_{G_{right}} \varphi(g_2) = \varphi(g_1 \circ_{G_{left}} g_2)$.
With $g_i = (h_i \times k_i) \times m_i$, the left hand side becomes
$\varphi(g_1) \circ_{G_{right}} \varphi(g_2) = \varphi\big((h_1 \times k_1) \times m_1\big) \circ_{G_{right}} \varphi\big((h_2 \times k_2) \times m_2\big) = \big(h_1 \times (k_1 \times m_1)\big) \circ_{G_{right}} \big(h_2 \times (k_2 \times m_2)\big)$.
The right hand side can be handled as follows, first applying the definition of the group operation in G_{left}, then the group operation in $H \times K$, then using the definition of φ, and then applying the definition of the group operation in $K \times M$, and then applying the definition of the group operation in G_{right}.

$$\varphi(g_1 \circ_{G_{left}} g_2) = \varphi\Big(\big((h_1 \times k_1) \times m_1\big) \circ_{G_{left}} \big((h_2 \times k_2) \times m_2\big)\Big)$$
$$= \varphi\Big(\big((h_1 \times k_1) \circ_{H \times K} (h_2 \times k_2)\big) \times \big(m_1 \circ_M m_2\big)\Big)$$
$$= \varphi\Big(\big((h_1 \circ_H h_2) \times (k_1 \circ_K k_2)\big) \times \big(m_1 \circ_M m_2\big)\Big)$$
$$= (h_1 \circ_H h_2) \times \big((k_1 \circ_K k_2) \times \big(m_1 \circ_M m_2\big)\big)$$
$$= (h_1 \circ_H h_2) \times \big((k_1 \times m_1) \circ_{K \times M} (k_2 \times m_2)\big)$$
$$= \big(h_1 \times (k_1 \times m_1)\big) \circ_{G_{right}} \big(h_2 \times (k_2 \times m_2)\big)$$

Interestingly, we never had to make use of the fact that *H*, *K*, or *M* was a group.

Note that B shows that the operation $\times$ is associative on the set of groups. Does this operation, along with the set of all groups, form a group?

No. Except for the trivial (one-element) group, there are no inverses.

Q2: Building larger groups from smaller ones: examples

Recall that $\mathbb{Z}_p$ is the group containing the elements $\{0,1,...,p-1\}$, 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 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: Automorphisms of groups

A. What are the automorphisms of $\mathbb{Z}_5$?

Since all of the elements of $\mathbb{Z}_5$ are multiples of 1 (in the sense that $\alpha 1$ is shorthand for $1+1+\ldots+1$, α times), we only need to determine what are the possibilities for $\varphi(1)$, since the remaining values of φ can be determined by $\varphi(\alpha) = \varphi(\alpha 1) = \alpha\varphi(1)$. Say φ_u is defined by $\varphi_u(1) = u$. Any such φ is a

homomorphism, since $\varphi_u(\alpha+\beta)=u(\alpha+\beta)$ (multiplication mod 5), while $\varphi_u(\alpha)+\varphi_u(\beta)=u\alpha+u\beta$, and these quantities are equal because of the distributive law (for ordinary multiplication). To determine whether it is an isomorphism, we need to find a φ_u^{-1}. This must be some φ_v, since its action is determined by how it acts on 1. If $\varphi_v=\varphi_u^{-1}$, then $\varphi_v\left(\varphi_u(1)\right)=1$, which means that $\varphi_v\left(u\right)=1$, and therefore that $vu=1$, with multiplication interpreted mod 5. Refer to homework Q2B of the first week. For modular arithmetic with prime modulus, multiplicative inverses exist for all nonzero integers. So for each $u\neq 0$ in $\mathbb{Z}_5$, $\varphi_u(k)=uk$ is an automorphism.

B. What are the automorphisms of $\mathbb{Z}_6$?

As in part A, we only need to determine what are the possibilities for $\varphi(1)$. Say $\varphi_u(1)=u$. It is invertible (i.e., an isomorphism) only if $uv=1 \pmod 6$ has a solution. See Q2B from last week. This requires that u is relatively prime to 6. So the only possibilities for *u* are 1 and 5, yielding two automorphisms for $\mathbb{Z}_6$: the trivial automorphism φ_1 that leaves every element unchanged, and the nontrivial automorphism φ_5, for which $\varphi_5(u)=5u=-u \pmod 6$.

C. What are the automorphisms of $\mathbb{Z}_2\times\mathbb{Z}_2$?

$\mathbb{Z}_2\times\mathbb{Z}_2$ has three elements that are not the identity: 0×1, 1×0, and 1×1. Each of these must have order 2, and combining any two of them via the group operation yields the third. So abstractly, they are all equivalent. Therefore, any permutation of these three nonzero elements is an automorphism of $\mathbb{Z}_2\times\mathbb{Z}_2$.

D. (Challenging, optional) What are the automorphisms of $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$?

Sketch: $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ has seven nonzero elements $a\times b\times c$ where at least one of *a*, *b*, and *c* are nonzero. All of these are order 2. They are abstractly equivalent. So an automorphism φ can take $0\times0\times1$ to any one of these seven elements. Once $\varphi(0\times0\times1)$ is assigned to any of these seven possibilities, say *g*, next show that φ can take $0\times1\times0$ to any of the remaining 6 possibilities, say *h*. At this point, note that $\varphi(0\times1\times1)$ must be equal to $g+h$, since
$\varphi(0\times1\times1)=\varphi\left((0\times0\times1)+(0\times1\times0)\right)=\varphi(0\times0\times1)+\varphi(0\times1\times0)=g+h$. But $\varphi(1\times0\times0)$ can still be assigned freely to any of the 4 nonzero elements of $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ that are not *g*, *h*, or $g+h$.
Conversely, once $\varphi(0\times0\times1)$, $\varphi(0\times1\times0)$, $\varphi(1\times0\times0)$ are assigned, then φ is determined on all of $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, since

$$\varphi(a\times b\times c)=\varphi\left(a(1\times0\times0)+b(0\times1\times0)+c(0\times0\times1)\right)$$
$$=\varphi\left(a(1\times0\times0)\right)+\varphi\left(b(0\times1\times0)\right)+\varphi\left(c(0\times0\times1)\right) \quad .$$
$$=a\varphi(1\times0\times0)+b\varphi(0\times1\times0)+c\varphi(0\times0\times1)$$

So there are a total of $168=7\bullet6\bullet4$ outer automorphisms of $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.