Groups, Fields, and Vector Spaces

Homework #2 (2020-2021), Answers

Q1: Putting together groups: Direct products

Let G and H be groups, with elements g, g', etc. in G and h, h', etc. in H, and group operations $\circ_G$ and $\circ_H$. We define the direct product of G and H, $G \times H$, as the set of ordered pairs (g,h), and the group operation $(g,h)\circ(g',h') = (g \circ_G g', h \circ_H h')$.

A. Show that $G \times H$ is a group.

For G1, associativity – we reduce the operations in $G \times H$ to the operations in G and H, use associativity in G and H, and then combine back to $G \times H$.

$\big((g,h)\circ(g',h')\big)\circ(g'',h'') =$

$(g \circ_G g', h \circ_H h')\circ(g'',h'') =$

$\big((g \circ_G g')\circ_G g''\big),\big((h \circ_H h')\circ_H h''\big) =$

$\big(g \circ_G (g' \circ_G g'')\big),\big(h \circ_H (h' \circ_H h'')\big) =$

$(g,h)\circ(g' \circ_G g'', h' \circ_H h'') =$

$(g,h)\circ\big((g',h')\circ(g'',h'')\big)$

For G2, we need to show that $G \times H$ has an identity element. The natural choice is (e_G, e_H):
$(g,h)\circ(e_G,e_H) = (g \circ_G e_G, h \circ_H e_H) = (g,h)$. The first equality is the definition of operations in $G \times H$, second equality uses the properties of the identity in G and H.

For G3, we need to find the inverse of (g,h) . The natural choice is to take inverses in G and H separately, i.e., $(g,h)^{-1} = (g^{-1}, h^{-1})$. . We then verify:
$(g,h)\circ(g^{-1},h^{-1}) = (g \circ_G g^{-1}, h \circ_H h^{-1}) = (e_G, e_H)$.

B. Show that the subset S_G consisting of elements in $G \times H$ of the form (g, e_H), (where e_H is the identity for H) is a subgroup of $G \times H$. Is it guaranteed to be a normal subgroup?

It is closed: $(g,e_H)\circ(g',e_H) = (g \circ_G g', e_H \circ_H e_H) = (g \circ_G g', e_H \circ_H e_H) \in S_G$. It contains the identity and inverses (refer to part A).
It is normal: say $b = (g',h')$. We need to show that, for any $(g,e_H) \in S_G$, then $b^{-1}\circ(g,e_H)\circ b$ is also in S_G.

$b^{-1}\circ(g,e_H)\circ b = (g'^{-1},h'^{-1})\circ(g,e_H)\circ(g',h') = (g'^{-1}\circ_G g \circ_G g', h'^{-1}\circ_H h') = (g'^{-1}\circ_G g \circ_G g', e_H)$, which is manifestly an element of S_G. Note that this also follows as a special case of Question 2, using the homomorphism $\varphi(g,h) = h$ from $G \times H$ into H, whose kernel is S_G.

C. Let $G = \mathbb{Z}_5$ and $H = \mathbb{Z}_2$. What is the size of $G \times H$? Consider the group D_5 of rotations and reflections of the regular pentagon (i. e., the identity, the four non-trivial rotations by multiples of $2\pi/5$, and the reflections across lines through one vertex and the midpoint of the opposite face). Are $G \times H$ and D_5 the same group? Why or why not?

They both have 10 elements, but they are not the same group. $G\times H$ is commutative, but D_5 is not.

Q2. Kernels and normal subgroups

The notes showed that if $\varphi : G\to H$ is a homomorphism and $\ker\varphi$ is the set of elements of G for which $\varphi(g)=e_H$, then $\ker\varphi$ is a subgroup of G. Show that $\ker\varphi$ is a normal subgroup.

We need to show that, if $b\in G$ and $g\in\ker\varphi$, then $b^{-1}gb\in\ker\varphi$. That is, we need to show that $\varphi(b^{-1}gb)=e_H$. This follows because φ is structure-preserving:

$$\begin{aligned}
&\varphi(b^{-1}\circ_G g\circ_G b)\\
&=\varphi(b^{-1})\circ_H \varphi(g)\circ_H \varphi(b)\\
&=\varphi(b^{-1})\circ_H e_H\circ_H \varphi(b)\\
&=\varphi(b^{-1})\circ_H \varphi(b)\\
&=\left(\varphi(b)\right)^{-1}\circ_H \varphi(b)\\
&=e_H
\end{aligned},$$

where the next-to-the-last equality follows from the fact that inverses in G are mapped to inverses in H.

Q3: Automorphisms

A. What are all the automorphisms of the rational numbers $\mathbb{Q}$ under addition?

0 must map to 0, since the identity is preserved. We show that the automorphism is determined by the value of $\varphi(1)$. Say $\varphi(1)=a$, for $a\in\mathbb{Q}$. Then $\varphi(n)=\varphi(1)+\ldots+\varphi(1)=n\varphi(1)=na$. Similarly, $m\varphi(1/m)=\varphi(1/m)+\cdots+\varphi(1/m)=\varphi(1)=a$, so $\varphi(1/m)=a/m$. Similarly, $\varphi(n/m)=n\varphi(1/m)=na/m$. As long as $a\neq 0$, it is invertible.

B. Are there automorphisms of the real numbers $\mathbb{R}$ (under addition) that do not correspond to automorphisms of $\mathbb{Q}$?

Yes: with $\varphi(1)=a$, there is still freedom to choose $\varphi(x)$ for an irrational x. This "problem" is cured by requiring that φ respects further structure of $\mathbb{R}$, e.g., multiplication, or, continuity.

C. What are all the automorphisms of $\mathbb{Q}^n=\mathbb{Q}\times\mathbb{Q}\times\cdots\times\mathbb{Q}$ under addition? (See Q1 for definition of the direct product $\times$)

Write an element of $\mathbb{Q}^n=\mathbb{Q}\times\mathbb{Q}\times\cdots\times\mathbb{Q}$ as $(x_1,\ldots,x_n)$, an ordered n-tuple of elements in $\mathbb{Q}$.
Say $\varphi\left((1,0,0,\ldots,0)\right)=(a_{11},a_{12},\ldots,a_{1n})$ etc.This determines $\varphi\left((x_1,0,\ldots,0)\right)=x_1\varphi\left((1,0,\ldots,0)\right)$ as in part A, and similarly $\varphi\left((0,1,0,\ldots,0)\right)=(a_{21},a_{22},a_{23},\ldots,a_{2n})$ determines $\varphi\left((0,x_2,\ldots,0)\right)=x_2\varphi\left((0,1,\ldots,0)\right)$, etc.
Once all the "one-hot" $\varphi\left((1,0,0,\ldots,0)\right)$, $\varphi\left((0,1,0,\ldots,0)\right)$, ..., $\varphi\left((0,0,0,\ldots,1)\right)$'s are specified, φ is determined on all of $\mathbb{Q}^n$ by $\varphi\left((x_1,\ldots,x_n)\right)=\varphi\left((x_1,0,\ldots,0)\right)+\varphi\left((0,x_2,\ldots,0)\right)+\ldots+\varphi\left((0,0,\ldots,x_n)\right)$. However, to guarantee that φ is invertible, we need to require that the rows $(a_{11},a_{12},\ldots,a_{1n})$, $(a_{21},a_{22},a_{23},\ldots,a_{2n})$, $(a_{n1},a_{n2},a_{n3},\ldots,a_{nn})$ are linearly independent. So the automorphism group is the group of invertible $n\times n$ matrices with rational entries. The operation in the automorphism group is matrix multiplication.

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

$\mathbb{Z}_2 \times \mathbb{Z}_2$ *has four elements: the identity* $e = (0,0)$, $a_1 = (1,0)$, $a_1 = (0,1)$, *and* $a_3 = (1,1)$. Each of the a's is of order 2, and the product of two distinct a's is the third a. So the a's are abstractly identical. So any permutation of the three a's is an automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$. (Consonant with part C, this is the same as the group of invertible 2×2 matrices with entries in $\mathbb{Z}_2$, and operations carried out mod 2:

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