HW 2 Solutions

1 Computations

1. Write down every element of $\mathbb{Z}_3 \times \mathbb{Z}_3$, and write down its inverse. (For one example, note that the element $(0,0)$ has inverse $-(0,0) = (0,0)$.)

   Solution.
   - $(0,0)$ has inverse $-(0,0) = (0,0)$,
   - $(1,0)$ has inverse $-(1,0) = (2,0)$,
   - $(2,0)$ has inverse $-(2,0) = (1,0)$,
   - $(0,1)$ has inverse $-(0,1) = (0,2)$,
   - $(1,1)$ has inverse $-(1,1) = (2,2)$,
   - $(2,1)$ has inverse $-(2,1) = (1,2)$,
   - $(0,2)$ has inverse $-(0,2) = (0,1)$,
   - $(1,2)$ has inverse $-(1,2) = (2,1)$, and
   - $(2,2)$ has inverse $-(2,2) = (1,1)$.

   □

2. Write down every multiple of $(1,1)$ in the group $\mathbb{Z}_6 \times \mathbb{Z}_3$.

   Solution. $\{n(1,1) \mid n \in \mathbb{Z}\} = \{(1,1),(2,2),(3,0),(4,1),(5,2),(0,0)\}$. □

3. Write down three elements (a,b) of $\mathbb{Z}_6 \times \mathbb{Z}_3$ with the property

   $$|\{n(a,b) \mid n \in \mathbb{Z}\}| = 3.$$

   Solution. There are 8 such elements: $(2,0),(4,0),(0,1),(2,1),(4,1),(0,2),(2,2),(4,2)$. □

4. For now and for the rest of the class, for any positive integer n, we will write

   $$\mathbb{B}^n = \overbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}^{n \text{ times}}.$$

   Furthermore, in this situation only, we will allow ourselves to omit commas and parentheses when writing elements of these sets; as an example, we will write $1100 \in \mathbb{B}^4$.

   (a) How many elements of $\mathbb{B}^3$ have exactly two 1s?
   (b) How many elements of $\mathbb{B}^4$ have exactly two 1s?
   (c) How many elements of $\mathbb{B}^5$ have exactly two 1s?
   (d) Let $n \in \mathbb{Z}_{\geq 2}$. Write down a formula for the number of elements of $\mathbb{B}^n$ with exactly two 1s. (No proof required.)

   Solution. (a) 3.
   (b) 6.
   (c) 10.
   (d) There is more than one way to write down a formula, but one could write:

   $$\binom{n}{2} = \frac{n(n-1)}{2},$$

   or one could define a sequence by setting $a_2 = 1$, and defining, for all $n \in \mathbb{Z}_{\geq 2}$:

   $$a_{n+1} = a_n + n.$$

   □

2 Proofs

(I) Let G be a group with identity elements e_1, e_2. Prove that $e_1 = e_2$.

Proof. Note that by the definition of identity element,

$$\begin{aligned} e_1 &= e_1 e_2 && (e_2 \text{ is an identity, so we scale } e_1 \text{ by } e_2 \text{ on the right}) \\ &= e_2 && (e_1 \text{ is } \textit{also} \text{ an identity, so we scale } e_2 \text{ by } e_1 \text{ on the left}). \end{aligned}$$

□

(II) Let G, H be groups. Prove that if G, H are both abelian, then $G \times H$ is abelian.

Proof. Choose any $(a, b), (c, d) \in G \times H$. Note that

$$\begin{aligned} (a,b)(c,d) &= (ac, bd) && (\text{definition of products of groups}) \\ &= (ca, db) && (\text{both } G \text{ and } H \text{ are abelian}) \\ &= (c,d)(a,b) && (\text{definition of products of groups}). \end{aligned}$$

□

(III) Let G be a group, and let $g, h \in G$. Assume that

$$\text{for all } x \in G, \text{ we have } xg = gx.$$

Prove that

$$\text{for all } x \in G, \text{ we have } x\left(hgh^{-1}\right) = \left(hgh^{-1}\right)x.$$

Proof. Let's write e for the identity element of G. Choose any $x \in G$ and note that

$$\begin{aligned} x\left(hgh^{-1}\right) &= ((xh)\, g)\, h^{-1} && (\text{associativity}) \\ &= (g\,(xh))\, h^{-1} && (\text{by hypothesis, applied to } (xh)) \\ &= (gx)\left(hh^{-1}\right) && (\text{associativity}) \\ &= gx && (\text{definition of inverse}) \\ &= gex && (\text{definition of identity}) \\ &= g\left(hh^{-1}\right)x && (\text{definition of inverse}) \\ &= (gh)\left(h^{-1}x\right) && (\text{associativity}) \\ &= (hg)\left(h^{-1}x\right) && (\text{by hypothesis, applied to } h) \\ &= \left(hgh^{-1}\right)x && (\text{associativity}). \end{aligned}$$

□

(IV) One might remark that for any positive integer n, every element of $\mathbb{B}^n$ is its own inverse. Prove: if G is a group with the property that every element is its own inverse, then G is abelian.

Proof. Let e be the identity of G. Choose any $g, h \in G$ and note

$$\begin{aligned} gh &= (gh)e && (\text{definition of identity}) \\ &= gh((hg)(hg)) && (\text{by hypothesis, applied to } hg) \\ &= g(hh)ghg && (\text{associativity}) \\ &= geghg && (\text{by hypothesis, applied to } h) \\ &= (gg)hg && (\text{definition of identity}) \\ &= ehg && (\text{by hypothesis, applied to } g) \\ &= hg && (\text{definition of identity}), \end{aligned}$$

so G is abelian. □

(V) Let G, H be groups with identities, e_G, e_H, respectively. Prove that $\{(e_G, h) \mid h \in H\}$ is a subgroup of $G \times H$. (A similar proof shows that $\{(g, e_H) \mid g \in G\}$ is a subgroup of $G \times H$, but you don't need to write this up.)

Proof. Let's write K for $\{(e_G, h) \mid h \in H\}$.

- Since $(e_G, e_H) \in K$, we see $K \neq \varnothing$.
- Choose any $(e_G, h_1), (e_G, h_2) \in K$, then note that

$$(e_G, h_1)(e_G, h_2) = (e_G e_G, h_1 h_2) = (e_G, h_1 h_2) \in K.$$

- Finally, if we choose any $(e_G, h) \in K$, we recall that the inverse of (e_G, h) is $\left(e_G, h^{-1}\right)$; and $\left(e_G, h^{-1}\right)$ is in K by definition of K.

Thus, we see that K is a subgroup of $G \times H$ by the subgroup test. □