

## 3.3 SOLUTIONS

16. Show that  $\mathbf{Z}_5 \times \mathbf{Z}_3$  is a cyclic group, and list all of the generators for the group.

*Solution:* By Proposition 3.3.4 (b), then order of an element  $([a]_5, [b]_3)$  in  $\mathbf{Z}_5 \times \mathbf{Z}_3$  is the least common multiple of the orders of the components. Since  $[1]_5, [2]_5, [3]_5, [4]_5$  have order 5 in  $\mathbf{Z}_5$  and  $[1]_3, [2]_3$  have order 3 in  $\mathbf{Z}_3$ , the element  $([a]_5, [b]_3)$  is a generator if and only if  $[a]_5 \neq [0]_5$  and  $[b]_3 \neq [0]_3$ . There are 8 such elements, which can easily be listed.

*Comment:* The other 7 elements in the group will have at least one component equal to zero. There are 4 elements of order 5 (with  $[0]_3$  as the second component) and 2 elements of order 3 (with  $[0]_5$  as the first component). Adding the identity element to the list accounts for all 15 elements of  $\mathbf{Z}_5 \times \mathbf{Z}_3$ .

17. Find the order of the element  $([9]_{12}, [15]_{18})$  in the group  $\mathbf{Z}_{12} \times \mathbf{Z}_{18}$ .

*Solution:* Since  $\gcd(9, 12) = 3$ , we have  $o([9]_{12}) = o([3]_{12}) = 4$ . Similarly,  $o([15]_{18}) = o([3]_{18}) = 6$ . Thus the order of  $([9]_{12}, [15]_{18})$  is  $\text{lcm}[4, 6] = 12$ .

18. Find two groups  $G_1$  and  $G_2$  whose direct product  $G_1 \times G_2$  has a subgroup that is not of the form  $H_1 \times H_2$ , for subgroups  $H_1 \subseteq G_1$  and  $H_2 \subseteq G_2$ .

*Solution:* In  $\mathbf{Z}_2 \times \mathbf{Z}_2$ , the element  $(1, 1)$  has order 2, so it generates a cyclic subgroup that does not have the required form.

19. In the group  $G = \mathbf{Z}_{36}^\times$ , let  $H = \{[x] \mid x \equiv 1 \pmod{4}\}$  and  $K = \{[y] \mid y \equiv 1 \pmod{9}\}$ . Show that  $H$  and  $K$  are subgroups of  $G$ , and find the subgroup  $HK$ .

*Solution:* It can be shown (as in Problem 3.2.26) that the given subsets are subgroups. A short computation shows that  $H = \{[1], [5], [13], [17], [25], [29]\}$  and  $K = \{[1], [19]\}$ . Since  $x \cdot [1] \neq x \cdot [19]$  for  $x \in G$ , the set  $HK$  must contain 12 elements, and so  $HK = G$ .

20. Show that if  $p$  is a prime number, then the order of the general linear group  $\text{GL}_n(\mathbf{Z}_p)$  is  $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ .

*Solution:* We need to count the number of ways in which an invertible matrix can be constructed. This is done by noting that we need  $n$  linearly independent rows. The first row can be any nonzero vector, so there are  $p^n - 1$  choices.

There are  $p^n$  possibilities for the second row, but to be linearly independent of the first row, it cannot be a scalar multiple of that row. Since we have  $p$  possible scalars, we need to omit the  $p$  multiples of the first row. Therefore the total number of ways to construct a second row independent of the first is  $p^n - p$ .

For the third row, we need to subtract  $p^2$ , which is the number of vectors in the subspace spanned by the first two rows that we have chosen. Thus there

are  $p^n - p^2$  possibilities for the third row. This argument can be continued, giving the stated result. (A more formal proof could be given by induction.)

21. Find the order of the element  $A = \begin{bmatrix} i & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -i \end{bmatrix}$  in the group  $GL_3(\mathbf{C})$ .

*Solution:* For any diagonal  $3 \times 3$  matrix we have

$$\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}^n = \begin{bmatrix} a^n & 0 & 0 \\ 0 & b^n & 0 \\ 0 & 0 & c^n \end{bmatrix},$$

It follows immediately that the order of  $A$  is the least common multiple of the orders of the diagonal entries  $i$ ,  $-1$ , and  $-i$ . Thus  $o(A) = 4$ .

22. Let  $G$  be the subgroup of  $GL_2(\mathbf{R})$  defined by

$$G = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \mid m \neq 0 \right\}.$$

Let  $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and  $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ . Find the centralizers  $C(A)$  and  $C(B)$ , and show that  $C(A) \cap C(B) = Z(G)$ , where  $Z(G)$  is the center of  $G$ .

*Solution:* Suppose that  $X = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$  belongs to  $C(A)$  in  $G$ . Then we must have  $XA = AX$ , and doing this calculation shows that

$$\begin{bmatrix} m & m+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m & b+1 \\ 0 & 1 \end{bmatrix}.$$

Equating corresponding entries shows that we must have  $m + b = b + 1$ , and so  $m = 1$ . On the other hand, any matrix of this form commutes with  $A$ , and so  $C(A) = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \mid b \in \mathbf{R} \right\}$ .

Now suppose that  $X = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$  belongs to  $C(B)$ . Then  $XB = BX$ , and so

$$\begin{bmatrix} -m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -m & -b \\ 0 & 1 \end{bmatrix}.$$

Equating corresponding entries shows that we must have  $b = 0$ , and so  $C(B) = \left\{ \begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix} \mid 0 \neq m \in \mathbf{R} \right\}$ .

This shows that  $C(A) \cap C(B)$  is the identity matrix, and since any element in the center of  $G$  must belong to  $C(A) \cap C(B)$ , our calculations show that the center of  $G$  is the trivial subgroup, containing only the identity element.