3.2 SOLUTIONS

23. Find all cyclic subgroups of $\mathbf{Z}_{24}^{\times}$.

    Solution: You can check that $x^2 = 1$ for all elements of the group. Thus each nonzero element generates a subgroup of order 2, including just the element itself and the identity $[1]_{24}$.

24. In $\mathbf{Z}_{20}^{\times}$, find two subgroups of order 4, one that is cyclic and one that is not cyclic.

    Solution: To find a cyclic subgroup of order 4, we need to check the orders of elements in $\mathbf{Z}_{20}^{\times} = \{\pm 1, \pm 3, \pm 7, \pm 9\}$. It is natural to begin with [3], which turns out to have order 4, and so $\langle [3] \rangle$ is a cyclic subgroup of order 4.

    The element $[9] = [3]^2$ has order 2. It is easy to check that the subset $H = \{\pm[1], \pm[9]\}$ is closed. Since H is a finite, nonempty subset of a known group, Corollary 3.2.4 implies that it is a subgroup. Finally, H is not cyclic since no element of H has order 4.

25. (a) Find the cyclic subgroup of S_7 generated by the element $(1, 2, 3)(5, 7)$.

    Solution: We have $((1, 2, 3)(5, 7))^2 = (1, 3, 2)$, $((1, 2, 3)(5, 7))^3 = (5, 7)$,

    $((1, 2, 3)(5, 7))^4 = (1, 2, 3)$, $((1, 2, 3)(5, 7))^5 = (1, 3, 2)(5, 7)$, $((1, 2, 3)(5, 7))^6 = (1)$. These elements, together with $(1, 2, 3)(5, 7)$, form the cyclic subgroup generated by $(1, 2, 3)(5, 7)$.

    (b) Find a subgroup of S_7 that contains 12 elements. You do not have to list all of the elements if you can explain why there must be 12, and why they must form a subgroup.

    Solution: We only need to find an element of order 12, since it will generate a cyclic subgroup with 12 elements. Since the order of a product of disjoint cycles is the least common multiple of their lengths, the element $(1, 2, 3, 4)(5, 6, 7)$ has order 12.

26. In $G = \mathbf{Z}_{21}^{\times}$, show that

    $$H = \{[x]_{21} \mid x \equiv 1 \pmod 3\} \quad \text{and} \quad K = \{[x]_{21} \mid x \equiv 1 \pmod 7\}$$

    are subgroups of G.

    Solution: The subset H is finite and nonempty (it certainly contains $[1]_{21}$), so by Corollary 3.2.4 it is enough to show that H is closed under multiplication. If $[x]_{21}$ and $[y]_{21}$ belong to H, then $x \equiv 1 \pmod 3$ and $t \equiv 1 \pmod 3$, so it follows that $xy \equiv 1 \pmod 3$, and therefore $[x]_{21} \cdot [y]_{21} = [xy]_{21}$ belongs to H.

    A similar argument shows that K is a subgroup of $\mathbf{Z}_{21}^{\times}$.

27. Let G be an abelian group, and let n be a fixed positive integer. Show that $N = \{g \in G \mid g = a^n$ for some $a \in G\}$ is a subgroup of G.

    Solution: First, the subset N is nonempty since the identity element e can always be written in the form $e = e^n$. Next, suppose that g_1 and g_2 belong to N. Then there must exist elements a_1 and a_2 in G with $g_1 = a_1^n$ and $g_2 = a_2^n$, and so $g_1 g_2 = a_1^n a_2^n = (a_1 a_2)^n$. The last equality holds since G is abelian. Finally, if $g \in N$, with $g = a^n$, then $g^{-1} = (a^n)^{-1} = (a^{-1})^n$, and so g^{-1} has the right form to belong to N.

28. Suppose that p is a prime number of the form $p = 2^n + 1$.

    (a) Show that in $\mathbf{Z}_p^\times$ the order of $[2]_p$ is $2n$.

    Solution: Since $2^n + 1 = p$, we have $2^n \equiv -1 \pmod{p}$, and squaring this yields $2^{2n} \equiv 1 \pmod{p}$. Thus the order of $[2]$ is a divisor of $2n$, and for any proper divisor k of $2n$ we have $k \le n$, so $2^k \not\equiv 1 \pmod{p}$ since $2^k - 1 < 2^n + 1 = p$. This shows that $[2]$ has order $2n$.

    (b) Use part (a) to prove that n must be a power of 2.

    Solution: The order of $[2]$ is a divisor of $|\mathbf{Z}_p^\times| = p - 1 = 2^n$, so by part (a) this implies that n is a divisor of 2^{n-1}, and therefore n is a power of 2.

29. In the multiplicative group $\mathbf{C}^\times$ of complex numbers, find the order of the elements $-\dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}i$ and $-\dfrac{\sqrt{2}}{2} - \dfrac{\sqrt{2}}{2}i$.

    Solution: It is probably easiest to change these complex numbers from rectangular coordinates into polar coordinates. (See Appendix A.5 for a discussion of the properties of complex numbers.) Each of the numbers has magnitude 1, and you can check that

    $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i = \cos(3\pi/4) + i\sin(3\pi/4)$ and $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i = \cos(5\pi/4) + i\sin(5\pi/4)$.

    We can use Demoivre's Theorem (Theorem A.5.2) to compute powers of complex numbers. It follows from this theorem that $(\cos(3\pi/4) + i\sin(3\pi/4))^8 = \cos(6\pi) + i\sin(6\pi) = 1$, and so $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ has order 8 in $\mathbf{C}^\times$. A similar argument shows that $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$ also has order 8.

30. In the group $G = GL_2(\mathbf{R})$ of invertible 2×2 matrices with real entries, show that

    $$H = \left\{ \left[\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right] \middle| \, \theta \in \mathbf{R} \right\}$$

    is a subgroup of G.

    Solution: Closure: To show that H is closed under multiplication we need to use the familiar trig identities for the sine and cosine of the sum of two angles.

    $$\left[\begin{array}{cc} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{array} \right] \left[\begin{array}{cc} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{array} \right]$$

$$= \begin{bmatrix} \cos\theta\cos\phi - \sin\theta\sin\phi & -\cos\theta\sin\phi - \sin\theta\cos\phi \\ \sin\theta\cos\phi + \cos\theta\sin\phi & -\sin\theta\sin\phi + \cos\theta\cos\phi \end{bmatrix}$$

$$= \begin{bmatrix} \cos\theta\cos\phi - \sin\theta\sin\phi & -(\sin\theta\cos\phi + \cos\theta\sin\phi) \\ \sin\theta\cos\phi + \cos\theta\sin\phi & \cos\theta\cos\phi - \sin\theta\sin\phi \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{bmatrix} \in H.$$

Identity: To see that the identity matrix is in the set, let $\theta = 0$.

Existence of inverses: $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^{-1} = \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{bmatrix} \in H.$

31. Let K be the following subset of $GL_2(\mathbf{R})$.

$$K = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \, d = a, \;\; c = -2b, \;\; ad - bc \neq 0 \right\}$$

Show that K is a subgroup of $GL_2(\mathbf{R})$.

Solution: The closure axiom holds since $\begin{bmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ -2b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 - 2b_1b_2 & a_1b_2 + b_1a_2 \\ -2(a_1b_2 - b_1a_2) & a_1a_2 - 2b_1b_2 \end{bmatrix}$. The identity matrix belongs K, and $\begin{bmatrix} a & b \\ -2b & a \end{bmatrix}^{-1} = \dfrac{1}{a^2 + 2b^2} \begin{bmatrix} a & -b \\ -2(-b) & a \end{bmatrix}$.

Comment: We don't need to worry about the condition $ad - bc \neq 0$, since for any element in H the determinant is $a^2 + 2b^2$, which is always positive.

32. Compute the centralizer in $GL_2(\mathbf{R})$ of the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

Note: Exercise 3.2.14 in the text defines the centralizer of an element a of the group G to be $C(a) = \{x \in G \mid xa = ax\}$.

Solution: Let $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, and suppose that $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ belongs to the centralizer of A in $GL_2(\mathbf{R})$. Then we must have $XA = AX$, so doing this calculation shows that $\begin{bmatrix} 2a+b & a+b \\ 2c+d & c+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2a+c & 2b+d \\ a+c & b+d \end{bmatrix}$. Equating corresponding entries shows that we must have $2a+b = 2a+c$, $a+b = 2b+d$, $2c+d = a+c$, and $c+d = b+d$. The first and last equations imply that $b = c$, while the second and third equations imply that $a = b + d = c + d$, or $d = a - b$. On the other hand, any matrix of this form commutes with A, so the centralizer in $GL_2(\mathbf{R})$ of the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ is the subgroup $\left\{ \begin{bmatrix} a & b \\ b & a-b \end{bmatrix} \middle| \, a, b \in \mathbf{R} \text{ and } ab \neq a^2 + b^2 \right\}$.