Do the following exercises from the text:
Chapter 3, Section 3.4: 1 (b), (f); 16, 28, 33, 40, 43, 46

1. Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

   (b) $5x + 1 \equiv 13 \pmod{23}$

   ▶ **Solution.** This can be viewed as an equation in equivalence classes modulo 23. That is, the equation is $[5][x] + [1] = [13]$ in $\mathbb{Z}_{23}$. Since 23 is prime, $[5]$ has a multiplicative inverse in $\mathbb{Z}_{23}$. This can be calculated by applying Euclid's Lemma, starting by dividing 23 by 5:

$$\begin{aligned} 23 &= 4 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

   Thus, $\gcd(23,\, 5) = 1$ and reversing the calculation gives

$$\begin{aligned} 1 &= 1 \cdot 3 - 2 \\ &= 3 - (5 - 1 \cdot 3) = 2 \cdot 3 - 5 \\ &= 2(23 - 4 \cdot 5) - 5 \\ &= 2 \cdot 23 - 9 \cdot 5 \end{aligned}$$

   Therefore, $[5]^{-1} = [-9] = [14]$ since $-9 + 23 = 14$. The equation $[5][x] + [1] = [13]$ is equivalent to the equation $[5][x] = [13] - [1] = [12]$, and multiplying this by $[5]^{-1} = [14]$ gives

$$[x] = [5]^{-1}[12] = [14][12] = [14 \cdot 12] = [168] = [7],$$

   where the last equality is obtained by dividing 168 by 23 $(168 - 23 \cdot 7 + 7)$. The congruence equality $[x] = [7]$ is equivalent to $x = 7 + 23k$ for $k \in \mathbb{Z}$, so all solutions of the original congruence are all integers of the form $x = 7 + 23k$. ◀

   (f) $3x \equiv 1 \pmod{6}$

   ▶ **Solution.** Suppose that $3x \equiv 1 \pmod{6}$. This means that $3x - 1 = 6k$ for some $k \in \mathbb{Z}$. Then $3(x - 2k) = 1$ which means that 3 divides 1, which is not true in the integers. Thus, there are no $x \in \mathbb{Z}$ satisfying this equation. ◀

16. Give a specific example of some group G and elements g, $h \in G$ where $(gh)^n \neq g^n h^n$.

   ▶ **Solution.** Any elements g, h of a group G such that $gh \neq hg$ will work. For a concrete example let $G = \mathrm{GL}_2(\mathbb{R})$, let $g = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $h = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Then $gh = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ so $(gh)^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ while

$$g^2h^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

◀

28. If G is a group and a, $b \in G$, then the equation $xa = b$ has a unique solution in G.

Proof. If $x = ba^{-1}$ then $xa = (ba^{-1})a = b(a^{-1}a) = be = b$ so $x = ba^{-1}$ is a solution to $xa = b$. To see that this is the only solution to the equation, suppose $x \in G$ and $xa = b$. Multiplying on the right by a^{-1} gives $(xa)a^{-1} = ba^{-1}$ and, by associativity, $(xa)a^{-1} = x(aa^{-1}) = xe = x$. Thus ba^{-1} is the unique solution to the group equation $xa = b$. □

33. Let G be a group and suppose that $(ab)^2 = a^2b^2$ for all a and b in G. Prove that G is an abelian group.

Proof. The group G is abelian if $ab = ba$ for all a and b in G. Thus, let a and b be arbitrary elements of G. Then, by hypothesis $(ab)^2 = a^2b^2$. Expanding this, the left had side is $(ab)^2 = abab$ while the right hand side is $a^2b^2 = aabb$. Thus $(ab)^2 = a^2b^2$ means that $abab = aabb$. Multiply this on the left by a^{-1} to get $a^{-1}(abab) = a^{-1}(aabb)$, which by associativity gives $(a^{-1}a)(bab) = (a^{-1}a)(abb)$. Since $a^{-1}a = e$ this gives $e(bab) = e(abb)$ so that $bab = abb$. Now multiply this last expression on the right by b^{-1} to get $(bab)b^{-1} = (abb)b^{-1}$. By associativity again, this gives $(ba)(bb^{-1}) = (ab)(bb^{-1})$ and since $bb^{-1} = e$, we conclude that $ba = ab$. Since a and b are arbitrary elements of G, it follows that G is abelian. □

40. Let G consist of the 2×2 matrices of the form

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},$$

where $\theta \in \mathbb{R}$. Prove that G is a subgroup of $\mathrm{SL}_2(\mathbb{R})$.

Proof. First note that if $A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$, then $\det A = \cos^2\theta + \sin^2\theta = 1$ so $A \in \mathrm{SL}_2(\mathbb{R})$. Hence, G is a subset of $\mathrm{SL}_2(\mathbb{R})$. To check that it is a subgroup, verify the three properties in Proposition 3.30.

- The identity of $SL_2(\mathbb{R})$ is the identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Since,

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

  for $\theta = 0$, it follows that $I \in G$.

- Suppose that $A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ and $B = \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix}$ are elements of G, where θ and ϕ are in $\mathbb{R}$. Then,

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

  Since $\theta + \phi \in \mathbb{R}$ it follows that $AB \in G$.

- Suppose that $A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ is an element of G, where $\theta \in \mathbb{R}$. Since $\det A = 1$, the inverse of the matrix A is (see Example 3.26)

$$A^{-1} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{bmatrix} \in G$$

  since $-\theta \in \mathbb{R}$.

Thus, G satisfies the three conditions of Proposition 3.30, and hence G is a subgroup of $\mathrm{SL}_2(\mathbb{R})$. □

43. Prove or disprove: $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup of $SL_2(\mathbb{R})$.

▶ **Solution.** We will prove that this is a true statement. That is, $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup of $\mathrm{SL}_2(\mathbb{R})$. To do this, check the 3 conditions of Proposition 3.30.

- First, the identity of $\mathrm{SL}_2(\mathbb{R})$ is the identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Since this matrix has integer entries and has determinant 1, it follows that $I \in SL_2(\mathbb{Z})$.

- Now assume that $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ are elements of $\mathrm{SL}_2(\mathbb{Z})$. This means that $\det A = \det B = 1$ and all of the entries of the two matrices are integers. Then $\det(AB) = \det A \det B = 1 \cdot 1 = 1$ and

$$AB = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + c_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

  Therefore all of the entries of AB are sums of products of integers and hence are integers. Hence $AB \in \mathrm{SL}_2(\mathbb{Z})$.

- If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then a, b, c, and d are integers and $\det A = ad - bc = 1$. Therefore, $A^{-1} = \frac{1}{1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Thus, the entries of A^{-1} are integers and $\det A^{-1} = da - (-b)(-c) = ad - bc = \det A = 1$. Hence A^{-1} is in $\mathrm{SL}_2(\mathbb{Z})$.

Therefore, $\mathrm{SL}_2(\mathbb{Z})$ satisfies the 3 conditions of Proposition 3.30 and hence is a subgroup of $\mathrm{SL}(\mathbb{R})$. ◀

46. Prove or disprove: If H and K are subgroups of a group G, then the subset $H \cup K$ is a subgroup of G.

► **Solution.** We will show that this is false by giving a counterexample. Let $G = U(8)$, the group of units of $\mathbb{Z}_8$. See Table 3.12 for the multiplication table for $U(8)$. Let $H = \{1, 3\}$ and $K = \{1, 5\}$. Then the multiplication tables for H and K:

$\cdot$	1	3
1	1	3
3	3	1

$\cdot$	1	3
1	1	5
5	5	1

show that each is closed under multiplication modulo 8, contains 1, and each element is its own inverse. This shows that H and K are subgroups of $U(8)$. Then $H \cup K = \{1, 3, 5\}$ and this is not a subgroup of $U(8)$ since $3 \cdot 5 = 7$ which is not in $H \cup K$. Thus $H \cup K$ fails condition 2 of Propostion 3.30, and hence it is not a subgroup of $U(8)$. ◀