1.

Additive identity: $(0,0)$. Multiplicative identity: $(0,1)$.

Suppose that λ is not a perfect square, and $(a,b)\odot(c,d)=(0,0)$, that is, $ad+bc=0$ and $bd+\lambda ac=0$. But then, $a(bd+\lambda ac)-b(ad+bc)=0$, that is, $(\lambda a^2-b^2)c=0$. Since λ is not a perfect square, we cannot have $\lambda a^2-b^2=0$ or $\lambda=(b/a)^2$. Therefore we must have $c=0$. This in turn implies $ad=0$ and $bd=0$. If $d=0$, we have $c=d=0$, whereas if $d\neq 0$, we have $a=b=0$. That is, A does not contain non-zero zero divisors.

Conversely, let $\lambda=\alpha^2$. As derived above, we see that $\lambda a^2-b^2=0$ is a necessary condition for the existence of non-zero zero divisors. We need to show that this condition is also sufficient. Taking $a=1$ and $b=\alpha$ satisfies the condition. We should also have $ad+bc=0$, that is, $\frac{a}{b}=-\frac{c}{d}$, that is, we can take $c=1$ and $d=-\alpha$. But then, $bd+\lambda ac=-\alpha^2+\lambda=0$. Since $(1,\alpha)$ and $(1,-\alpha)$ are non-zero elements of A, and $(1,\alpha)\odot(1,-\alpha)=(0,0)$, A is not an integral domain.

2. Let a, b ∈ S, such that a ∈ T1 and a ∉ T2, b ∈ T2 and b ∉ T1. Since a, b ∈ S, a + b ∈ S. Since S ⊆ T1 ∪T2, a + b ∈ T1 ∪T2, which means a+b must be either in T1 or T2 or both.
Let a + b ∈ T1. Then, since T1 is a subring, (a+b) - a = (b+a) - a = b ∈ T1, contradiction.
Let a + b ∈ T2. Then, since T2 is a subring, (a+b) - b = a ∈ T2, contradiction.
Thus, S ⊆ T1 or S ⊆ T2.

3.

Proof. Fix $a,b\in G$. Then $(ab)(ab)(ab)(ab)(ab)=(ab)^5=a^5b^5$ and cancelation of the end-terms, or multiplication by inverses, implies that $(ba)^4=b(ab)(ab)(ab)a=a^4b^4$. Likewise, $(ab)(ab)(ab)=(ab)^3=a^3b^3$ which implies that

$$(ba)^2=a^2b^2 \tag{1}$$

again by cancelation. But $(ba)^4=(ba)^2(ba)^2=a^2b^2a^2b^2$ so that $a^4b^4=a^2b^2a^2b^2$. Cancelation again implies $a^2b^2=b^2a^2$ which is certainly getting us closer. Now, using Equation 1, but switching the roles of a and b, we have $(ab)^2=b^2a^2$, so that $a^2b^2=b^2a^2=(ab)^2=(ab)(ab)$. Cancelation of the end-terms one last time yields $ab=ba$ which proves that G is Abelian. □

4.

[If] Let $h,h_1,h_2\in H$ and $k,k_1,k_2\in K$. We have $(h_1k_1)(h_2k_2)=h_1(k_1h_2)k_2$. Since $KH=HK$, $k_1h_2=h_3k_3$ for some $h_3\in H$ and $k_3\in K$. Therefore $(h_1k_1)(h_2k_2)=h_1(h_3k_3)k_2=(h_1h_3)(k_3k_2)\in HK$. Next, consider $(hk)^{-1}=k^{-1}h^{-1}$. Since $KH=HK$, we have $k^{-1}h^{-1}=h_4k_4$ for some $h_4\in H$ and $k_4\in K$, so $(hk)^{-1}=h_4k_4\in HK$.

[Only if] Take $hk\in HK$. Since HK is a subgroup, we have $(hk)^{-1}\in HK$, that is, there exist $h_1\in H$ and $k_1\in K$ such that $(hk)^{-1}=h_1k_1$. But then, $hk=(h_1k_1)^{-1}=k_1^{-1}h_1^{-1}\in KH$. That is, $HK\subseteq KH$.

Conversely, take $kh\in KH$. We have $h^{-1}\in H$ and $k^{-1}\in K$, so $h^{-1}k^{-1}\in HK$. Since HK is a subgroup, we have $(h^{-1}k^{-1})^{-1}=kh\in HK$. Therefore $KH\subseteq HK$.

Practice Problems

5. Proof: To show that H is a subgroup, it is sufficient to show closure property and the existence of inverse of all elements.

Closure: Let $p \in H$, $q \in H$. Then $p \circ g = g \circ p$, $q \circ g = g \circ q$ for all g in G. Then
$(p \circ q) \circ g = p \circ (q \circ g) = p \circ (g \circ q) = (p \circ g) \circ q = (g \circ p) \circ q = g \circ (p \circ q)$, which shows that $p \circ q \in H$.

Inverse: Let $p \in H$. Then $p \circ g = g \circ p$ for all g in G.
$\Rightarrow p^{-1} \circ (p \circ g) \circ p^{-1} = p^{-1} \circ (g \circ p) \circ p^{-1}$
$\Rightarrow g \circ p^{-1} = p^{-1} \circ g$ for all g in G.
Thus, $p^{-1} \in H$.

Hence, H is a subgroup.

6.

Reflexivity Let $x \in G$; we want to show that $x \; R \; x$, that is, $xx^{-1} \in H$. This is true, because $xx^{-1} = 1 \in H$.

Simmetry Let $x, y \in G$ and suppose $x \; R \; y$. We want to show that $y \; R \; x$, that is, $yx^{-1} \in H$. By hypothesis, $xy^{-1} \in H$, so, by the properties of a subgroup, $(xy^{-1})^{-1} \in H$; but, by general rule, $(xy^{-1})^{-1} = yx^{-1}$, so we are done.

Transitivity Let $x, y, z \in G$ and suppose $x \; R \; y$ and $y \; R \; z$. We want to show that $x \; R \; z$, that is $xz^{-1} \in H$. We know that $xy^{-1} \in H$ and $yz^{-1} \in H$, so $(xy^{-1})(yz^{-1}) \in H$. But $(xy^{-1})(yz^{-1}) = xz^{-1}$, so we are done.

7. **Associativity:** Let (g_1, h_1), (g_2, h_2) and $(g_3, h_3) \in G \times H$. Then $((g_1, h_1).(g_2, h_2)).(g_3, h_3) = (g_1 o\, g_2, h_1 {*} h_2).(g_3, h_3) = ((g_1 o\, g_2) o\, g_3, (h_1 {*} h_2) {*} h_3) = (g_1 o\, (g_2 o\, g_3), h_1 {*} (h_2 {*} h_3))$.

$(g_1, h_1).((g_2, h_2).(g_3, h_3)) = (g_1, h_1).(g_2 o\, g_3, h_2 {*} h_3) = (g_1 o\, (g_2 o\, g_3), h_1 {*} (h_2 {*} h_3))$.

Hence, $(G \times H, .)$ is associative.

Identity: Let e_G be the identity element of G and e_H be the identity element of H. Then, $(g, h).(e_G, e_H) = (g \text{ o } e_G, h {*} e_H) = (g, h)$ and $(e_G, e_H).(g, h) = (e_G \text{ o } g, e_H {*} h) = (g, h)$ for all $(g, h) \in G \times H$. Therefore, (e_G, e_H) is the identity element of $(G \times H, .)$.

Inverse: Let g^{-1} be the inverse of g in G and h^{-1} be the inverse of h in H. Then,

$(g, h).(g^{-1}, h^{-1}) = (g \text{ o } g^{-1}, h {*} h^{-1}) = (e_G, e_H)$ and $(g^{-1}, h^{-1}).(g, h) = (g^{-1} \text{ o } g, h^{-1} {*} h) = (e_G, e_H)$.

Therefore, (g^{-1}, h^{-1}) is the inverse of (g, h) in $(G \times H, .)$.

8. For R to be a ring, distributive property of **.** over + must hold. We show that it does not hold.

   Consider $f(n) = n + 1$, $g(n) = 1$, $h(n) = 1$ for all $n \in Z$. Then $(f.(g + h))(n) = f(g(n) + h(n)) = f(1+1) = f(2) = 3$.

   $f(g(n)) + f(h(n)) = f(1) + f(1) = 2+2 = 4$.

   Thus, R is not a ring.

9. b. [⇒] Take non-zero elements a, b ∈ R. Then a and b are non-zero (constant) polynomials. Since R[x] is an integral domain, ab is not the zero polynomial. But ab is again a constant polynomial. It follows that ab 6 = 0.
[⇐] Suppose that there exist A(x), B(x) ∈ R[x] such that A(x)B(x) = 0, A(x) 6 = 0, and B(x) 6 = 0. Write A(x) = a0 + a1x + a2x2 + · · · + ad xd with ad 6 = 0 and d > 0, and B(x) = b0 + b1x + b2x2 + · · · + bexe with be 6 = 0 and e > 0. Since A(x)B(x) = 0, we must be = 0. This implies that R is not an integral domain.

10. a.

Since $\mathbb{A}$ is a subset of the ring of 2×2 matrices with real entries, it suffices to show closure under addition, multiplication, and additive inverse in order to prove that $\mathbb{A}$ is a ring.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} (a+c) & (b+d) \\ -(b+d) & (a+c) \end{pmatrix}.$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{pmatrix}.$$

$$-\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} (-a) & (-b) \\ -(-b) & (-a) \end{pmatrix}.$$

For commutativity, note that

$$\begin{aligned} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} &= \begin{pmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{pmatrix} \\ &= \begin{pmatrix} (ca-db) & (da+cb) \\ -(da+cb) & (ca-db) \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}. \end{aligned}$$

Finally, the 2×2 identity matrix is in $\mathbb{A}$.

b.

Define the map $f : \mathbb{A} \to \mathbb{C}$ as

$$f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a + \mathrm{i}b.$$

We have

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= f\left(\begin{pmatrix} (a+c) & (b+d) \\ -(b+d) & (a+c) \end{pmatrix}\right) = (a+c) + \mathrm{i}(b+d) \\ &= (a+\mathrm{i}b) + (c+\mathrm{i}d) = f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right), \end{aligned}$$

and

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= f\left(\begin{pmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{pmatrix}\right) = (ac-bd) + \mathrm{i}(ad+bc) \\ &= (a+\mathrm{i}b)(c+\mathrm{i}d) = f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right). \end{aligned}$$

Therefore f is a ring homomorphism. Clearly, f is surjective. Finally,

$$f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right)$$

implies that $a + \mathrm{i}b = c + \mathrm{i}d$, that is, $a = c$ and $b = d$, that is,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}.$$

So f is injective too.

11.

$(G, *)$ is a group, because it satisfies the following properties of a group.

Closure: For any $p, q \in G$, $p * q = p \circ c \circ q \in G$, since $c \in G$ and G is closed under the operation $\circ$.

Associativity: For any $p, q, r \in G$, since G is associative under the operation $\circ$, we get:

$$(p * q) * r = (p \circ c \circ q) \circ c \circ r = p \circ c \circ (q \circ c \circ r) = p * (q * r)$$

Identity: c^{-1} is the identity element. For any element $p \in G$, we get:

$$p * c^{-1} = p \circ c \circ c^{-1} = p \circ e_G = p \quad \text{and} \quad c^{-1} * p = c^{-1} \circ c \circ p = e_G \circ p = p$$

where, $e_G \in G$ is the identity element with respect to the group $(G, \circ)$.

Inverse: For any element $p \in G$, let $p' \in G$ be its inverse with respect to $*$. Now, by definition we should get $p * p' = c^{-1} = p' * p$.

$$\therefore p \circ c \circ p' = c^{-1} \quad \text{or} \quad p' \circ c \circ p = c^{-1} \quad \Rightarrow \quad p' = c^{-1} \circ p^{-1} \circ c^{-1}$$

where, p^{-1} is the inverse of p with respect to the operation $\circ$.