1. *Let U be a nonempty set and let R be the set of all subsets of U (i.e. the power set of U). For the two given proposed definitions of "addition" and "multiplication", determine whether R is a ring or not; if it is not a ring, explain why, and if it is a ring, identify its identity elements.*

   (a) *$A + B = A \cup B$ and $A \cdot B = A \cap B$.*

   This is not a ring, because there is no inverse under addition. To determine an identity, we note that $A + 0 = A \cup 0 = A$ is only universally true if $0 = \emptyset$; however, then since for nonempty A, there is no set $(-A)$ such that $A + (-A) = A \cup (-A) = \emptyset$.

   (b) *$A + B = (A \cup B) - (A \cap B)$ (also known as the "symmetric difference") and $A \cdot B = A \cap B$.*

   This is in fact a ring: closure is easily demonstrated, and associativity is a bit tedious but straightforward ($A + B + C$ consists of those elements lying in exactly 1 or 3 of the sets A, B, and C). The distributeive law may be derived from noting that $[(A \cup B) - (A \cap B)] \cap C = [(A \cap C) \cup (B \cap C)] - (A \cap B \cap C)$ The additive identity is $\emptyset$, and every element of R is its own additive inverse. There is also a multiplicative identity, U itself.

2. *Prove that for a commutative ring R and $x \in R$, x is a unit of R if and only if x divides every element of R.*

   First, let us note that the statement is vacuously true if R lacks a multiplicative identity, as *neither* of the conditions can be met. Clearly, x can be a unit only if $xy = 1$ for some $x, y \in R$, which would require that $1 \in R$. Similarly, if x divides every element of R, then in particular x divides x, so $x = kx$ for some $k \in R$; now, for any $r \in R$, there is an $\ell \in R$ such that $r = \ell x$, and so $r = \ell x = \ell k x = k(\ell x) = kr$, making k a multiplicative identity. Henceforth, we may thus assume that R has a multiplicative identity.

   Let us suppose that x is a unit, so that there is a $y \in R$ such that $xy = 1$. Then for any $r \in R$, $(xy)r = 1r = r$, so $r = x(yr)$. Thus x divides r.

   Conversely, if we suppose that x divides every element of R, then, in particular, x divides 1, so there is a $k \in R$ such that $xk = 1$; since k is definitionally the inverse of x, x is a unit.

3. *Prove the following two statements:*

   (a) *For any ring R and a (not necessarily finite) collection $\mathcal{R}$ of subrings of R, their intersection*

   $$\bigcap_{S \in \mathcal{R}} S$$

   is also a subring of R. (Hint: you may find it easier to warm up by addressing just an intersection of two subrings of R)

   Let $T = \bigcap_{S \in \mathcal{R}} S$ for brevity. Then if $a, b \in T$, it follows that $a, b \in S$ for every single ring $S \in \mathcal{R}$. Since each S is a ring, ab and $a + b$ are in S for every $S \in \mathcal{R}$, and thus ab and $a + b$ are in T, demonstrating closure of T under addition and multiplication.

   Likewise, since each S is a ring, $-a \in S$ for every $S \in \mathcal{R}$, and so $-a \in T$, demonstrating closure under additive inversion.

   Finally, since every S is a ring, $0 \in S$ and thus $0 \in T$.

   (b) *For a ring R and a subset S of R, there is a unique* smallest *subring $\langle S \rangle$ of R which contains all the elements of S (hint: choose an appropriate collection $\mathcal{R}$ for the above statement).*

   Let $\mathcal{R}$ contain every ring which is a superset of S and a subring of R. By the previous part, $T = \bigcap_{X \in \mathcal{R}} X$ is a subring of R, and for every ring X which is a superset of S and a subring of R, $X \subseteq T$, we may assert that T, as it contains S and is contained in every ring containing S, is the smallest such ring.

4. *Address the two following questions about subrings:*

   (a) *Let $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ denote the smallest subring of $\mathbb{R}$ which contains every rational number, the irrational number $\sqrt{2}$, and the irrational number $\sqrt{3}$. Let $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ denote the smallest subring of $\mathbb{R}$ which contains every rational number and the irrational number $\sqrt{2}+\sqrt{3}$ (note that the previous question guarantees that these structures are well-defined). Prove that $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$.*

   It suffices to show that $\sqrt{2}$ and $\sqrt{3}$ are elements of $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ to prove that $\mathbb{Q}[\sqrt{2},\sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2}+\sqrt{3}]$; likewise, if we show that $\sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$, then $\mathbb{Q}[\sqrt{2}+\sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2},\sqrt{3}]$, collectively showing the desired equality.

   The second of these is trivial: $\sqrt{2} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$ and $\sqrt{3} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$, so by closure of addition, $\sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$.

   The first membership, however, is more difficult. Since $(\sqrt{2}+\sqrt{3}) \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$, we may use closure of multiplication to find that its square $5+2\sqrt{6}$ is also in $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$. -5 and $\frac{1}{2}$ are rational, and can be added and multiplied in turn to the above to find that $\sqrt{6} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$. Finally, we multiply $\sqrt{6}$ by $(\sqrt{2}+\sqrt{3})$ once more to find that $2\sqrt{3}+3\sqrt{2}$ is in $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$, and subtracting twice and thrice $(\sqrt{2}+\sqrt{3})$ demonstrates that $\sqrt{2}$ and $-\sqrt{3}$ respectively are in $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

   (b) *Let $\mathbb{Z}[\sqrt{2},\sqrt{3}]$ and $\mathbb{Z}[\sqrt{2}+\sqrt{3}]$ be defined as in the previous part except with "rational number" replaced by "integer" in the definition. Demonstrate that $\mathbb{Z}[\sqrt{2},\sqrt{3}] \neq \mathbb{Z}[\sqrt{2}+\sqrt{3}]$.*

   The same argument as above can be used to show that $\mathbb{Z}[\sqrt{2}+\sqrt{3}] \subseteq \mathbb{Z}[\sqrt{2},\sqrt{3}]$; however, our argument for the reverse containment will not work as designed because we cannot multiply by $\frac{1}{2}$. It is, however, easy to follow the above argument without the division to guarantee that $2\sqrt{2}$, $2\sqrt{3}$, and $2\sqrt{6}$ are all elements of $\mathbb{Z}[\sqrt{2}+\sqrt{3}]$. However, half of each of these values is *not* in the ring: note that the set

   $$\{a+2b\sqrt{2}+2c\sqrt{6}+d(\sqrt{2}+\sqrt{3}) : a,b,c,d \in \mathbb{Z}\}$$

   is a ring containing $\mathbb{Z}$ and $\sqrt{2}+\sqrt{3}$ but not $\sqrt{2}$ or $\sqrt{3}$.

5. *Prove that if the additive group of a ring R is cyclic, then R is commutative.*

   Let g be a generator of the additive group. Thus, for any $a,b \in R$, either a or $-a$ may be written as $\underbrace{g+g+\cdots+g}_{k \text{ times}}$ for some nonnegative integer k; likewise b or $-b$ may be written as $\underbrace{g+g+\cdots+g}_{\ell \text{ times}}$ for some non-negative integer ℓ. Using the distributive law, the product ab can be written as $\pm\underbrace{g+g+\cdots+g}_{k\ell \text{ times}}$; however, likewise ba could be written as $\pm\underbrace{g+g+\cdots+g}_{\ell k \text{ times}}$; since k and ℓ are ordinary integers, the number of addends is the same in both expressions, so $ab=ba$.