1. (DF7.1.13) An element x in R is called *nilpotent* if $x^m = 0$ for some $m \in \mathbb{Z}^+$.

   (a) Show that if $n = a^k b$ for some integers a and b then $\overline{ab}$ is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.

   Proof. Suppose that $n = a^k b$ for some integers a and b. Then in the commutative ring $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/a^k b\mathbb{Z}$, the element $\overline{ab}$ is nilpotent if there exists a positive integer m such that $\overline{ab}^m = \overline{a^m b^m} = \overline{0}$, which is equivalent to requiring that $a^m b^m \equiv 0 \pmod{a^k b}$. Then we should have that $a^k b \mid a^m b^m$, and of course we can choose $m \geq k$ so that $a^k b \mid a^m b^m$. Since a suitable m does exist such that $(\overline{ab})^m = \overline{0}$, $\overline{ab}$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$. $\square$

   (b) If $a \in \mathbb{Z}$ is an integer, show that the element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.

   Proof. Let a, n be integers, and let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ be the prime factorization of n for primes p_i.
   Suppose that every prime divisor of n is also a divisor of a. Observe that $p_1 p_2 \cdots p_s \mid a$, and let $\alpha = \max\{\alpha_i \mid 1 \leq i \leq s\}$. Then $p_1^\alpha p_2^\alpha \cdots p_s^\alpha \mid a^\alpha$, but due to our choice of α, $n \mid p_1^\alpha p_2^\alpha \cdots p_s^\alpha$. It follows that $n \mid a^\alpha$, so that $\overline{a^\alpha} = \overline{0}$, meaning that $\overline{a}$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$.
   Conversely, suppose that $\overline{a}$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$; that is, there exists a positive integer α such that $\overline{a^\alpha} = \overline{0}$ so that $n \mid a^\alpha$. Since $a \in \mathbb{Z}$ and $p_i \mid n$, we must have that $p_i \mid a$, for $1 \leq i \leq s$. (If $p_i \nmid a$, then we arrive at a contradiction with the fact that $n \mid a^\alpha$ by taking $\alpha = \max\{\alpha_i \mid 1 \leq i \leq s\}$ and observing that $n \mid p_1^\alpha p_2^\alpha \cdots p_s^\alpha$ but $p_1^\alpha p_2^\alpha \cdots p_s^\alpha \nmid a^\alpha$.)
   Hence $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a. $\square$

   In $\mathbb{Z}/72\mathbb{Z} = \mathbb{Z}/2^3 3^2\mathbb{Z}$ it follows that every nilpotent element is of the form $\overline{2^i 3^j a}$ for positive integers i, j, a, since 2 and 3 divide $2^i 3^j$. Explicitly, these are the elements whose integer representative is even and divisible by three:

   $$\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48}, \overline{54}, \overline{60}, \overline{66}$$

   (c) Let R be the ring of functions from a nonempty set X to a field F. Prove that R contains no nonzero nilpotent elements.

   Proof. Let R be the ring of functions from a nonempty set X to a field F as given. Suppose by way of contradiction that R contains a nonzero nilpotent element g.
   Because g is a nilpotent element of R, there exists a positive integer k such that g^k is the zero function $0_R \colon X \to F$ with $0_R(x) = 0_F$ for all $x \in X$.
   We have that g is not the zero function 0_R, so that there exists $y \in X$ such that $g(y) \neq 0_F$. Then $g^k(y) = [g(y)]^k = 0_F$. But $g(y) \neq 0_F$ so that F contains a nonzero zero divisor, which is a contradiction.
   Hence R does not contain a nonzero nilpotent element g. $\square$

2. (DF7.1.21) Let X be any nonempty set and let $\mathcal{P}(X)$ be the set of all subsets of X (the *power set* of X). Define addition and multiplication on $\mathcal{P}(X)$ by

   $$A + B = (A - B) \cup (B - A) \quad \text{and} \quad A \times B = A \cap B$$

i.e., addition is symmetric difference and multiplication is intersection.

(a) Prove that $\mathcal{P}(X)$ is a ring under these operations ($\mathcal{P}(X)$ and its subrings are often referred to as *rings of sets*).

Proof. Let X be a nonempty set and let $\mathcal{P}(X)$ be the power set of X as given with the operations of addition and multiplication as given above. Observe that the symmetric difference and intersection of subsets of X return subsets of X, so they are valid choices of binary operations.

Under the addition (symmetric difference) operation, $\mathcal{P}(X)$ is an abelian group. The additive identity is the empty set $\emptyset$: For any subset A of X,

$$\emptyset + A = (\emptyset - A) \cup (A - \emptyset) = \emptyset \cup A = A = A \cup \emptyset = (A - \emptyset) \cup (\emptyset - A) = A + \emptyset.$$

Addition is also associative: For any subsets A, B, C of X we have by lots of set algebra (writing S^c to mean the complement of S in X) that

$$\begin{aligned}
A + (B + C) &= A + ((B - C) \cup (C - B)) \\
&= [A - ((B - C) \cup (C - B))] \cup [((B - C) \cup (C - B)) - A] \\
&= [(A \cap B^c \cap C^c) \cup (A \cap B \cap C)] \cup [(A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C)] \\
&= [(A^c \cap B \cap C^c) \cup (A \cap B^c \cap C^c)] \cup [(A^c \cap B^c \cap C) \cup (A \cap B \cap C)] \\
&= [((A - B) \cup (B - A)) - C] \cup [C - ((A - B) \cup (B - A))] \\
&= ((A - B) \cup (B - A)) + C \\
&= (A + B) + C.
\end{aligned}$$

Each subset of X is its own additive inverse: For any subset A of X,

$$A + A = (A - A) \cup (A - A) = \emptyset.$$

Addition is also commutative: For any subsets A, B of X,

$$A + B = (A - B) \cup (B - A) = (B - A) \cup (A - B) = B + A.$$

With the power set of X being an abelian group under addition, the remaining ring axioms are checked for the multiplication given by intersection. Associativity of multiplication is immediate since set intersection is already associative; that is, for any subsets A, B, C of X, we have $(A \times B) \times C = (A \cap B) \cap C = A \cap (B \cap C) = A \times (B \times C)$.

The distributive laws hold: For any subsets A, B, C of X, we have

$$\begin{aligned}
(A+B) \times C &= [(A-B) \cup (B-A)] \times C \\
&= (A \cap B^c \cap C) \cup (B \cap A^c \cap C) \\
&= [(A \cap C \cap B^c) \cup (A \cap C \cap C^c)] \cup [(B \cap C \cap A^c) \cup (B \cap C \cap C^c)] \\
&= [(A \cap C) \cap (B \cap C)^c] \cup [(B \cap C) \cap (A \cap C)^c] \\
&= (A \cap C - B \cap C) \cup (B \cap C - A \cap C) \\
&= (A \times C) + (B \times C)
\end{aligned}$$

and

$$\begin{aligned}
A \times (B+C) &= A \times [(B-C) \cup (C-B)] \\
&= (A \cap B \cap C^c) \cup (A \cap C \cap B^c) \\
&= [(A \cap B \cap C^c) \cup (A \cap B \cap A^c)] \cup [(A \cap C \cap B^c) \cup (A \cap C \cap A^c)] \\
&= [(A \cap B) \cap (A \cap C)^c] \cup [(A \cap C) \cap (A \cap B)^c] \\
&= (A \cap B - A \cap C) \cup (A \cap C - A \cap B) \\
&= (A \times B) + (A \times C).
\end{aligned}$$

Hence $\mathcal{P}(X)$ is a ring under the operations of addition and multiplication given above. □

(b) Prove that this ring is commutative, has an identity and is a Boolean ring.

Proof. The ring $\mathcal{P}(X)$ is commutative because set intersection is commutative; that is, $A \times B = A \cap B = B \cap A = B \times A$ for any subsets A, B of X.

The multiplicative identity in this ring is the subset X, since for any subset A of X, we have $A \times X = A \cap X = A = X \cap A = X \times A$.

Then for any subset A of X, we have $A^2 = A \times A = A$, from which it follows that $\mathcal{P}(X)$ is a Boolean ring. □

3. (DF7.1.23)

4. (DF7.1.25)