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; i.e., a multiple of 6:

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

   (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 $A^2 = A\times A = A\cap A = A$, from which it follows that $\mathcal{P}(X)$ is a Boolean ring. □

3. (DF7.1.23) Let D be a squarefree integer, and let $\mathcal{O}$ be the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{D})$. For any positive integer f prove that the set $\mathcal{O}_f = \mathbb{Z}[f\omega] = \{a + bf\omega \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathcal{O}$ containing the identity. Prove that $[\mathcal{O}\colon \mathcal{O}_f] = f$ (index as additive abelian groups). Prove conversely that a subring of $\mathcal{O}$ containing the identity and having finite index f in $\mathcal{O}$ (as additive abelian groups) is equal to $\mathcal{O}_f$. (The ring $\mathcal{O}_f$ is called the *order of conductor* f in the field $\mathbb{Q}(\sqrt{D})$. The ring of integers $\mathcal{O}$ is called the *maximal order* in $\mathbb{Q}(\sqrt{D})$.)

Proof. Let $\mathcal{O}_f$ be as given. It is clear that $\mathcal{O}_f$ is a nonempty subset of $\mathcal{O}$ because f is an integer. We check that this subset is closed under subtraction and multiplication:

For integers a, b, c, d we have $(a + bf\omega) - (c + df\omega) = (a - c) + (b - d)f\omega$, which is clearly an element of $\mathcal{O}_f$. Similarly, $(a + bf\omega)(c + df\omega) = ac + (ad + bc)f\omega + bdf^2\omega^2$, where

$$\omega^2 = \begin{cases} D & \text{if } D \not\equiv 1 \pmod 4 \\ \left(\frac{D-1}{4}\right) + \omega & \text{if } D \equiv 1 \pmod 4, \end{cases}$$

and in either case we have an element of $\mathcal{O}_f$ (when $D \equiv 1 \pmod 4$ the product is the element $(ac+bdf^2(D-1)/4) + (ad + bc + bdf)f\omega)$.

Hence $\mathcal{O}_f$ is a subring of $\mathcal{O}$, and it also inherits the same $1 = 1 + 0f\omega$ from $\mathcal{O}$ which behaves the same way: $1(a + bf\omega) = (a + bf\omega)1 = a + bf\omega$.

To show that the index of $\mathcal{O}_f$ in $\mathcal{O}$ is f, we use the group homomorphism given by projection onto $\mathbb{Z}/f\mathbb{Z}$ which maps $a + bf\omega$ to $\overline{b}$. Since b was an arbitary integer, this map is surjective. We check that this map is a group homomorphism: For integers a, b, c, d we have

$$(a + bf\omega) + (c + df\omega) = (a + c) + (b + d)f\omega \mapsto \overline{(b + d)} = \overline{b} + \overline{d},$$

where in the last equality the addition inside of the parenthesis is the addition in $\mathbb{Z}$ and the addition on the right hand side is the addition in $\mathbb{Z}/f\mathbb{Z}$. The kernel of this homomorphism is $\mathcal{O}_f$ (it is clear that elements of $\mathcal{O}_f$ are mapped to $\overline{0}$): For integers a, b, asserting the element $a + b\omega$ is in the kernel is equivalent to saying that f divides b, meaning $a + b\omega = a + b'f\omega$ where b' is the quotient b/f. Since b was arbitrary, b' is also arbitrary.

Thus by the first isomorphism theorem for groups we have

$$[\mathcal{O} \colon \mathcal{O}_f] = |\mathbb{Z}/f\mathbb{Z}| = f.$$

Suppose that we are given a subring $\mathcal{O}'$ of $\mathcal{O}$ of index f, containing 1. Since $\mathcal{O}'$ is closed under addition, $\mathbb{Z}$ is contained in $\mathcal{O}'$, so that for any integer a, the quantity $(f - 1)a$ is an element of $\mathcal{O}'$.

We have that the quotient group $\mathcal{O}/\mathcal{O}'$ has order f, so that for any element $a+b\omega$ of $\mathcal{O}$, the coset $f(a+b\omega)+\mathcal{O}'$ (where $f(a + b\omega)$ denotes the f-fold sum given by $af + bf\omega$) is equivalent to the coset $\mathcal{O}'$. Furthermore, since $(f - 1)a \in \mathcal{O}'$, it follows that $(af + bf\omega) + \mathcal{O}' = ((f - 1)a + 0f\omega) + \mathcal{O}'$, which is equivalent to saying that

$$(af + bf\omega) - ((f - 1)a + 0f\omega) = a + bf\omega \in \mathcal{O}'^n.$$

Since a, b were arbitrary, it follows that $\mathcal{O}_f$ is contained in $\mathcal{O}'$. Then

$$f = [\mathcal{O} \colon \mathcal{O}'] = [\mathcal{O} \colon \mathcal{O}_f][\mathcal{O}_f \colon \mathcal{O}'] = f[\mathcal{O}_f \colon \mathcal{O}'],$$

so that $[\mathcal{O}_f \colon \mathcal{O}'] = 1$ and so $\mathcal{O}' = \mathcal{O}_f$. Hence any subring of $\mathcal{O}$ containing the identity and having finite index f in $\mathcal{O}$ is equal to $\mathcal{O}_f$. □

4. (DF7.1.25) Let I be the ring of integral Hamilton Quaternions and define

$$N\colon I \to \mathbb{Z} \quad \text{by} \quad N(a+bi+cj+dk) = a^2+b^2+c^2+d^2$$

(the map N is called a *norm*).

(a) Prove that $N(\alpha) = \alpha\overline{\alpha}$ for all $\alpha \in I$, where if $\alpha = a+bi+cj+dk$ then $\overline{\alpha} = a-bi-cj-dk$.

(b) Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in I$.

(c) Prove that an element of I is a unit if and only if it has norm $+1$. Show that $I^\times$ is isomorphic to the quaternion group of order 8. [The inverse in the ring of rational quaternions of a nonzero element α is $\overline{\alpha}/N(\alpha)$.]

Proof. Let I be the ring of integral Hamilton Quaternions as given and define $N\colon I \to \mathbb{Z}$ as above. Then for any integral quaternion $\alpha = a+bi+cj+dk$, we have

$$\begin{aligned}
\alpha\overline{\alpha} = (a+bi+cj+dk)(a-bi-cj-dk) &= (a^2+b^2+c^2+d^2) \\
&\quad + (-ab+ab-cd+cd)i \\
&\quad + (-ac+ac-bd+bd)j \\
&\quad + (-ad+ad-bc+bc)k \\
&= a^2+b^2+c^2+d^2 \\
&= N(\alpha).
\end{aligned}$$

The function N is also multiplicative. Given any two integral quaternions $\alpha = a+bi+cj+dk$ and $\beta = e+fi+gj+hk$, we have $\alpha\beta = (ae-bf-cg-dh)+(af+be+ch-dg)i+(ag+ce+df-bh)j+(ah+de+bg-cf)k$. Then (with many cancellations between the first equality and the second equality), we have

$$\begin{aligned}
N(\alpha\beta) &= (ae-bf-cg-dh)^2 \\
&\quad + (af+be+ch-dg)^2 \\
&\quad + (ag+ce+df-bh)^2 \\
&\quad + (ah+de+bg-cf)^2 \\
&= a^2e^2+b^2f^2+c^2g^2+d^2h^2 \\
&\quad + a^2f^2+b^2e^2+c^2h^2+d^2g^2 \\
&\quad + a^2g^2+c^2e^2+d^2f^2+b^2h^2 \\
&\quad + a^2h^2+d^2e^2+b^2g^2+c^2f^2 \\
&= (a^2+b^2+c^2+d^2)(e^2+f^2+g^2+f^2) \\
&= N(\alpha)N(\beta).
\end{aligned}$$

An integral quaternion is a unit if and only if its norm is 1. If a quaternion α is a unit then it has an inverse α^{-1} with $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$. Then $N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1})$, so that $N(\alpha) = N\alpha^{-1} = \pm 1$ (they both need to have the same sign). But $N(\alpha)$ and $N(\alpha^{-1})$ are sums of squared integers, meaning that their values are necessarily positive. This forces $N(\alpha) = N(\alpha^{-1}) = 1$, which means that units have a norm of 1.

If an integral quaternion $\alpha = a + bi + cj + dk$ has a norm of 1, we have that $a^2 + b^2 + c^2 + d^2 = 1$. In the integers, there are only eight solutions, which we write as tuples (a, b, c, d):

$$(\pm 1, 0, 0, 0), (0, \pm 1, 0, 0), (0, 0, \pm 1, 0), (0, 0, 0, \pm 1).$$

Any other combination of integers will not satisfy the equality $a^2 + b^2 + c^2 + d^2 = 1$. The corresponding integral quaternions (suppressing the zero-coefficient terms in each one) which have a norm of 1 are

$$\pm 1, \pm i, \pm j, \pm k,$$

and these are units (observe that we multiply by the conjugate to obtain a multiplicative inverse):

$$1 = (1)(1) = i(-i) = (-i)i = j(-j) = (-j)j = k(-k) = (-k)k.$$

Hence the units of the integral quaternions are those with norm 1.

It follows that these eight units form a group under multiplication, $I^\times$, which is isomorphic to Q_8. The isomorphism needed is just the relabeling

$$\begin{aligned} \pm 1 + 0i + 0j + 0k &\mapsto \pm 1 \\ 0 + \pm i + 0j + 0k &\mapsto \pm i \\ 0 + 0i + \pm j + 0k &\mapsto \pm j \\ 0 + 0i + 0j + \pm k &\mapsto \pm k, \end{aligned}$$

which is an isomorphism because these units as a group obey the same multiplication rule as Q_8 due to the multiplication on the integral Hamilton Quaternions being defined in the same manner (meaning the multiplication tables are identical under the relabeling given above). $\square$