III.1. Rings and Homomorphisms

1. (a) Let $G$ be an (additive) abelian group. Define an operation of multiplication in $G$ by $ab = 0, \forall a, b \in G$. Then $G$ is a ring.

(b) Let $S$ be the set of all subsets of some fixed set $U$. For $A, B \in S$, define $A + B = (A - B) \cup (B - A)$ and $AB = A \cap B$. Then $S$ is a ring. Is $S$ commutative? Does $S$ have an identity?

Proof: (a) For any $a, b, c \in G$, $(ab)c = 0 = a(bc)$, and $a(b + c) = 0 + 0 = ab + ac$. Therefore, $G$ is a ring. Note that $ab = 0 = ba$, $G$ is also commutative.

(b) Firstly, for any $A, B, C \in S$, $A + B = (A - B) \cup (B - A) = (B - A) \cup (A - B) \in S$, $(A + B) + C = (A - B) \cup (B - A) + C = ((A - B) \cup (B - A) - C) \cup (C - (A - B) \cup (B - A)) = (A - (B \cup C)) \cup (B - (A \cup C)) \cup (C - (A \cup B)) \cup (A \cap B \cap C) = A + (B + C)$, $A + \emptyset = A$, and $A + A = \emptyset$. Thus $S$ with addition is an abelian group with additive identity $\emptyset$.

Secondly, as $(AB)C = (A \cap B) \cap C = A \cap (B \cap C) = A(BC)$, and $A(B + C) = A \cap ((B - C) \cup (C - B)) = (A \cap (B - C)) \cup (A \cap (C - B)) = ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B)) = AB + AC$, $S$ is a ring. Furthermore, since $AB = A \cap B = B \cap A = BA$, $S$ is commutative; since $AU = UA = A \cap U = A$, $U$ is the multiplicative identity of $S$.

2. Let $\{R_i : i \in I\}$ be a family of rings with identity. Make the direct sum of abelian groups $\sum_{i \in I} R_i$ into a ring by defining multiplication coordinatewise. Does $\sum_{i \in I} R_i$ have an identity?

Answer: As a group, each element in $\{R_i : i \in I\}$ is a map $f : I \mapsto \cup_{i \in I} R_i$ such that for each $i$, $f(i) \in R_i$ and such that for all but finitely many $i \in I$, $f(i) = 0_i$, the additive identity of $R_i$.

Suppose that $\{R_i : i \in I\}$ has an identity $\epsilon : I \mapsto \cup_{i \in I} R_i$. Then there is a finite subset $I_0 \subseteq I$, such that $\epsilon(i) = 0_i$ for all $i \in I - I_0$. For an arbitrary $f \in \{R_i : i \in I\}$, since $\epsilon$ is an identity, we must have

$$f(i)\epsilon(i) = f(i), \forall i \in I.$$ 

Since $f$ is arbitrary, this holds if and only is for all $i \in I - I_0$, $R_i = \{0_i\}$. Therefore, $\{R_i : i \in I\}$ has an identity if and only if for all $i \in I - I_0$, $R_i = \{0_i\}$.
3. A ring $R$ such that $\forall a \in R, a^2 = a$ is called a **Boolean ring**. Prove that every Boolean ring is commutative and $a + a = 0, \forall a \in R$.

**Proof** Let $R$ be a Boolean ring, and $a, b \in R$. Since $R$ is Boolean,
\[
a + b = (a + b)^2 = a^2 + 2ab + b^2 = a + ba + b,
\]
and so $ab + ba = 0$, implying $ab = -ba$. Since $a, b$ are arbitrary, setting $b = a$, we have $a = a^2 = -a^2 = -a$. Therefore, for any $a \in R$, $a + a = 0$, and for any $a, b \in R$, $ab = -ba = b(-a) = ba$.

4. Let $R$ be a ring and $S$ a nonemptyset. Define
\[
M(S, R) = \{ f : S \mapsto R \}.
\]
Define addition in $M(S, R)$ as follows: $(f + g) : S \mapsto R$ is given by $(f + g)(s) = f(s) + g(s), \forall s \in S$; and multiplication in $M(S, R)$ as follows: $(fg) : S \mapsto R$ is given by $(fg)(s) = f(s)g(s), \forall s \in S$. Then $M(S, R)$ is a ring.

**Proof** Since addition and multiplication are associative in $R$, the addition and multiplication is also associative in $M(S, R)$. Since addition is commutative in $R$, addition is also commutative in $M(S, R)$.

Let $0 \in M(S, R)$ denote the map which sends every element in $S$ into $0 \in R$, the additive identity of $R$. Then by the definition of addition in $M(S, R)$, $0$ is the additive identity of $M(S, R)$; and for any $f \in M(S, R)$, then map $-f$ given by $s \mapsto -f(s)$ is the additive inverse of $f$. Therefore, $M(S, R)$ with addition is an abelian group.

To show that $M(S, R)$ is a ring, it remains to show that multiplication to addition is distributive. Since $R$ is a ring, $\forall f, g, h \in M(S, R)$ and $\forall s \in S$, $(f(g + h))(s) = f(s)(g + h)(s) = f(s)(g(s) + h(s)) = f(s)g(s) + f(s)h(s) = (fg)(s) + (fh)(s)$, and so $f(g + h) = fg + fh$. Thus $M(S, R)$ is a ring.

5. If $A = \mathbb{Z} \oplus \mathbb{Z}$ is a group, then $\text{End}(A)$, the set of all endomorphisms of $A$ (with addition $f + g$ given by $a \mapsto f(a) + g(a)$ and multiplication $fg$ given by $a \mapsto f(g(a))$) is a noncommutative ring.

**Proof:** It is routine to verify that $\text{End}(A)$ is an abelian group (see solution of Problem 4 above), and so the details for the verification is omitted.
Since compositions of functions are associative, the multiplication of $\text{End}(A)$ is associative. For any $f, g, h \in \text{End}(A)$, and $\forall a \in A$, since $f$ is a homomorphism,

$$f(g + h)(a) = f(g(a) + h(a)) = f(g(a)) + f(h(a)),$$

and so $f(g + h) = fg + fh$. Therefore, $\text{End}(A)$ is a ring.

**Remark** So far, we have shown that for any abelian group $A$, $\text{End}(A)$ is a ring, without turning to the structure of $A = \mathbb{Z} \oplus \mathbb{Z}$.

To see that $\text{End}(A)$ is noncommutative, we need to find two particular $f, g \in \text{End}(A)$ such that $fg \neq gf$. Since $A$ is generated by $e_1 = (1, 0)$ and $e_2 = (0, 1)$, define $f(e_1) = (1, 1) = e_1 + e_2$ and $f(e_2) = e_2$, $g(e_1) = e_1$ and $g(e_2) = (1, 1) = e_1 + e_2$. Linearly expand $f$ and $g$ to homomorphisms in $\text{End}(A)$. Then $g(1, 1) = g(e_1) + g(e_2) = (2, 1)$, and so $fg(1, 1) = f(2, 1) = 2f(e_1) + f(e_2) = (2, 2) + (0, 1) = (2, 3)$. On the other hand, $f(1, 1) = (1, 2)$ and $gf(1, 1) = g(1, 2) = g(e_1) + 2g(e_2) = (1, 0) + (2, 2) = (3, 2)$. Therefore, $fg \neq gf$.

6. A finite ring with more than one element and no zero divisors is a division ring.

**Proof** Let $R$ be such a ring. It suffices to show that $R$ has a multiplicative identity (unity) and that every nonzero element of $R$ has a multiplicative inverse.

Since $R$ is finite, denote $R^* := R - \{0\} = \{r_1, r_2, \ldots, r_n\}$. Since $R$ has no zero divisor, $r_1R^* = R^* = R^*r_1$. Therefore, there must be some $i$, such that $r_1r_i = r_1$.

Fix $i$. For any $1 \leq x \leq n$, $r_1r_ix = r_1r_x$. Since $R$ has no zero divisor, $r_1r_x = r_x$.

Since $R$ has no zero divisor, for any $1 \leq x \leq n$, $r_xr_i \in R^*$, and $R^*r_x = R^*$. Therefore, there must be a $j$ with $1 \leq j \leq n$, such that $r_xr_i = r_jr_x$. Multiply $r_x$ both sides from right, and apply $r_xr_i = r_x$ to get $r_x^2 = r_jr_x^2$. It follows that $r_xr_i = r_x = r_jr_x = r_xr_i$. Hence, $r_i$ is the multiplicative identity of $R$. We denote $r_i = 1$.

Now pick an arbitrary $r_x \in R^*$. By $r_xR^* = R^*$, there must be a $r_y \in R^*$ such that $r_xr_y = r_i = 1$. Let $r_t = r_yr_x$. Then as $r_xr_y = 1$, $r_x = (r_xr_y)r_x = r_x(r_yr_x) = r_xr_t$. Since $R$ has no zero divisor, and since $R$ has 1, we have $r_t = 1$, and so $r_yr_x = 1 = r_xr_y$. Thus every $r_x \in R^*$ has an inverse.

7 Let $R$ be a ring with more than one element such that for each $a \in R^* = R - \{0\}$, there is a unique $b \in R$ such that $aba = a$. Prove:

(a) $R$ has no zero divisor.

(b) $bab = b$. 

3
$R$ has an identity.

(d) $R$ is a divisor ring.

**Proof** (a) Suppose that $R$ has a zero divisor $a \in R^*$. Then there must be an $a'$ such that $aa' = 0$. By assumption, there is a unique $b \in R$ such that $aba = a$. Let $b' = b + a'$. Since $a' \in R^*$, $b \neq b'$. However, $ab'a = a(b + a')a = aba + aa'a = aba + 0 = a$, contrary to the uniqueness of $b$. Therefore, $R$ cannot have a zero divisor.

(b) Since $aba = a$, we have $abab = ab$, and so $a(bab - b) = 0$. Since $a \neq 0$, and by Part(a), we must have $bab = b$.

(c) Fix $a \in R^*$. Then there is a unique $b \in R$ such that $aba = a$. Pick an arbitrary $x \in R^*$. Since $bx = babx$ and $xa = xaba$, and by Part(a), we have $x = (ab)x$ and $x = x(ab)$. Therefore, $ab$ is an identity of $R$.

(d) Let $1$ denote the identity of $R$. For any $a \in R^*$, there exists $b \in R$ such that $aba = a$. by Part(a), $ab = 1 = ba$, and so $R$ is a divisor ring.

10. Let $k, n$ be integers such that $0 \leq k \leq n$, and \( \binom{n}{k} \) the binomial coefficient $\frac{n!}{(n-k)!k!}$, where $0! = 1$, and for $n > 0$, $n! = n(n-1)(n-2) \cdots 2 \cdot 1$.

(a) $\binom{n}{k} = \binom{n}{n-k}$.

(b) $\binom{n}{k} < \binom{n}{k+1}$, for $2(k+1) \leq n$.

(c) $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

(d) $\binom{n}{k}$ is an integer.

(e) If $p$ is a prime and $1 \leq k \leq p^n - 1$, then $\binom{p^n}{k}$ is divisible by $p$.

**Proof:** (a) $\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n!}{(n-(n-k))!(n-k)!} = \binom{n}{n-k}$. 

4
(b) When \(2(k + 1) \leq n\), \(\frac{(n - k - 1)!(k + 1)!}{(n - k)!k!} = \frac{k + 1}{n - k} < 1\), and so \(\binom{n}{k} = \frac{n!}{(n - k)!k!} < \) 

\[ \frac{n!}{(n - k - 1)!(k + 1)!} = \binom{n}{k + 1}. \]

(c) \(\binom{n}{k} + \binom{n}{k + 1} = \frac{n!}{(n - k)!k!} + \frac{n!}{(n - k - 1)!(k + 1)!} = \frac{n!}{(n - k)!(k + 1)!}(k + 1) + (n - k) = \frac{(n + 1)!}{(n - k)!(k + 1)!} = \binom{n + 1}{k + 1}. \)

(d) Note that by Part(c), if \(\binom{n - 1}{k - 1}\) and \(\binom{n - 1}{k}\) are integers, then \(\binom{n}{k}\) is also an integer. As induction basis, we verify by definition that \(\binom{m}{0} = 1, \binom{m}{m} = 1\) and \(\binom{m}{1} = m\), for all \(0 \leq m \leq n\).

11. Let \(R\) be a commutative ring with identity of prime characteristic \(p\). If \(a, b \in R\), then \((a \pm b)^p^n = a^{p^n} \pm b^{p^n}\).

**Proof:** Since \(R\) is commutative,

\[ (a \pm b)^p^n = \sum_{k=0}^{p^n} (\pm)^k \binom{p^n}{k} a^{p^n-k}b^k. \]

By Part(e) of Exercise III-1.10, and since \(R\) has a unity of prime characteristic \(p\), when \(k \neq 0\) and \(k \neq p^n\), \((\pm)^k \binom{p^n}{k} a^{p^n-k}b^k = 0\), and so \((a \pm b)^p^n = a^{p^n} \pm b^{p^n}\).

12. An element \(a\) in a ring is **nilpotent** if \(a^n = 0\) for some integer \(n > 0\). Prove that in a commutative ring \(R\), \(a + b\) is nilpotent if \(a\) and \(b\) are. Show that this result may be false if \(R\) is not commutative.

**Proof** Suppose that \(a^n = 0\) and \(b^m = 0\). Since \(R\) is commutative,

\[ (a + b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^{m+n-k}b^k. \]
Note that for each \( k \), either \( m + n - k \geq n \) or \( k \geq m \), and so \((a + b)^{m+n} = 0\).

**Example:** Let \( R \) be the ring of all 2 by 2 real matrices with matrix addition and matrix multiplication. Let

\[
a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.
\]

Then \( a^2 = 0 = b^2 \), but \( a + b \) is a nonsingular matrix which is not nilpotent.

13. In a ring \( R \), the following conditions are equivalent.
(a) \( R \) has no nonzero nilpotent elements.
(b) If \( a \in R \) and \( a^2 = 0 \), then \( a = 0 \).

**Proof:** Assume (a). Suppose that for some \( a \in R \), \( a^2 = 0 \). Then \( a \) is nilpotent. By (a), \( a = 0 \).

Assume (b). Suppose that for some \( b \in R^* \), and integer \( n > 0 \), \( b^n = 0 \). We may assume that for fixed \( b \), \( n \) is smallest, and we will show that \( n = 1 \). Suppose that for some integer \( t \), \( n = 2t > 1 \). Then \((a^t)^2 = a^n = 0\). By (b), \( a^t = 0 \), contrary to the choice of \( n \). Hence for some integer \( t > 0 \), \( n = 2t + 1 \). Then \((a^{t+1})^2 = a^{n+1} = a^n a = 0 \cdot a = 0 \), and so by (b), \( a^{t+1} = 0 \), contrary to the choice of \( n \).