Hungerford: Algebra

III.2. Ideals

1. The set of all nilpotent elements in a commutative ring forms an ideal.

Proof: Let $R$ be a commutative ring and let $N$ denote the set of all nilpotent elements in $R$. Then

$$I = \{a \in R : \text{ for some } n \in \mathbb{Z}, r^n = 0\}.$$ 

As $0 \in I$, $I \neq \emptyset$. By Exercise III-1.12, $N$ is an abelian subgroup of the additive group of $R$. For any $a \in I$, there exists an integer $n \in \mathbb{Z}$ such that $a^n = 0$. And for any $r \in R$, since $R$ is commutative, $(ra)^n = r^n a^n = r^n \cdot 0 = 0$, and so $ra \in I$. This proves that $I$ is an ideal of $R$.

2. Let $I$ be an ideal in a commutative ring $R$ and let $\text{Rad} I = \{r \in R : r^n \in I \text{ for some integer } n \in \mathbb{Z}\}$. Show that $\text{Rad} I$ is an ideal.

Proof: Let $a, b \in \text{Rad} I$. Then for some integers $m, n$, we have $a^m \in I$ and $b^n \in I$. Since $R$ is commutative,

$$(a + b)^{m+n} = \sum_{k=1}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}.$$ 

Since $I$ is an ideal and since $a^m, b^n \in I$, it follows that for each $k$ with $0 \leq k \leq m+n$, $a^k b^{m+n-k} \in I$, and so $a + b \in \text{Rad} I$.

Now let $a \in \text{Rad} I$ and $r \in R$. As $a^m \in I$ and as $I$ is an ideal, $(ra)^n = r^m a^m \in I$, and so $ra \in \text{Rad} I$, which implies that $\text{Rad} I$ is an ideal.

3. If $R$ is a ring and $a \in R$, then $J = \{r \in R : ra = 0\}$ is a left ideal and $K = \{r \in R : ar = 0\}$ is a right ideal in $R$.

Proof: Let $r, r' \in J$. Then $ra = r'a = 0$, and so $(r+r')a = ra + r'a = 0$, which implies $r + r' \in RJ$. For any $x \in R$ and $r \in J$, $(xr)a = x(ra) = x \cdot 0 = 0$, and so $xr \in J$ also. Therefore, $J$ is a left ideal in $R$. The proof for $JK$ is similar.

4. If $I$ is a left ideal of $R$, then $A(I) = \{r \in R : rx = 0 \text{ for every } x \in I\}$ is an ideal in $R$.

Proof: Let $a, b \in A(I)$. Then $\forall x \in I$, $ax = bx = 0$, and so $(a+b)x = ax + bx = 0$. Thus $a + b \in A(I)$.

For any $r \in R$ and $a \in A(I)$, $\forall x \in I$, since $ax = 0$, we have $(ra)x = r(ax) = r \cdot 0 = 0$; and since $I$ is an ideal, $rx = x' \in I$ and so $(ar)x = a(rx) = ax' = 0$. It follows that both $ar \in A(I)$ and $ra \in A(I)$, and so $A(I)$ is an ideal.

5. If $I$ is an ideal in a ring $R$, let $[R : I] = \{r \in R : xr \in I \text{ for every } x \in R\}$. Prove that $[R : I]$ is an ideal of $R$ which contains $I$. 

1
Proof: Let $a, b \in [R : I]$. Then $\forall x \in R$, $xa = xb = 0$, and so $x(a + b) = xa + xb = 0$, implying that $a + b \in [R : I]$.

For any $r, x \in R$ and $a \in [R : I]$, $x(ra) = (xr)a = 0$, and so $[R : I]$ is an ideal in $R$.

6. (a) The center of the ring $S$ of all $2 \times 2$ matrices over a division ring $F$ consists of all matrices of the form 
\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\]
(b) The center of the ring of $S$ is not an ideal in $S$.
(c) What is the center of the ring of all $n \times n$ matrices over a division ring?

Proof: (a) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C(S)$. Let $B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, and $C = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$.

Since $AB = BA$, we have
\[
\begin{pmatrix} a + b & 0 \\ c + d & 0 \end{pmatrix} = AB = BA = \begin{pmatrix} a & b \\ a & b \end{pmatrix}.
\]

Therefore, $b = 0$. Now from $AC = CA$, we have
\[
\begin{pmatrix} 0 & a \\ 0 & d \end{pmatrix} = AC = CA = \begin{pmatrix} c & d \\ c & d \end{pmatrix}.
\]

Therefore, $a = d$ and $c = 0$. Hence if $A \in C(S)$, then there must be an element $a \in S$ such that $A = aI$.

On the other hand, for any matrix $M \in S$, $M(aI) = a(MI) = aM = (aI)M$, and $(aI)M = a(IM) = aM = M(aI)$. Therefore, any matrix in the form $aI$ is in $C(S)$.

Combine the above to conclude
\[C(S) = \{aI : a \in F\}.\]

(b) Let $B$ be defined as in (a). Then by (a), $BA \notin C(S)$, and so $C(S)$ is not an ideal in $S$.

(c) This is similar to (a). We did not assume that $F$ is a field in (a) and so when $F$ is a division ring, we still have
\[C(S) = \{aI : a \in F\}.\]

7. (a) A ring $R$ with identity is a division ring if and only if $R$ has no proper left ideals.
(b) If $S$ is a ring (possibly without identity) with no proper left ideal, then either $S^2 = 0$ or $S$ is a division ring.

Proof: (a) Suppose that $S$ is a division ring and $I$ is a proper left ideal in $S$. Since $I$ is proper,
\[ \exists a \in I - \{0\}. \] Since \( R \) is a division ring, \( a^{-1} \in R \). Therefore, as \( I \) is an ideal, \( 1_R = a^{-1}a \in I \). It follows that \( R \subseteq I \), and so \( I \) is not a proper ideal.

Now assume that \( R \) does not have proper left ideals. It suffices to show that every \( a \in R - \{0\} \) is a unit. Let \((a)\) be the principal left ideal generated by \( a \). Since \( R \) does not have proper left ideals, we have \((a) = R \), and in particular, \( 1_R \in (a) \). Thus \( \exists b \in (a) \) such that \( ba = 1_R \). Note that \( b \in R - \{0\} \), by the same reason, \( \exists c \in R \) such that \( cb = 1_R \). Multiply \( a \) from the right of \( cb = 1_R \) to get \( c = c1_R = c(ba) = (cb)a = 1_Ra = a \). Thus we have both \( ab = ba = 1_R \) and so \( a \) is a unit.

(b) We suppose that \( S^2 \neq 0 \) and try to prove that \( S \) is a division ring.

(7b.1) For any \( a \in S - \{0\} \),
\[ I_a = \{ s \in S : sa = 0 \} \]
is a left ideal in \( S \). In fact, if \( s, s' \in I_a \), then \( (s + s')a = sa + s'a = 0 + 0 = 0 \), and so \( s + s' \in I_a \).
For any \( r \in S \), \( (rs)a = r(sa) = 0 \). This \( I_a \) is a left ideal in \( S \).

(7b.2) Let \( I = \{ a \in S : Sa = 0 \} \). Then \( I \) is an ideal in \( S \); and \( I = \{0\} \).

Let \( a, a' \in I \). Then \( S(a + a') = Sa + Sa' = 0 + 0 = 0 \), and so \( a + a' \in I \). For any \( r \in S \), \( S(ra) = (Sr)a \subseteq Sa = 0 \) and \( S(ar) = (Sa)r = 0 \cdot r = 0 \), and so \( I \) is an ideal. Since \( S \) does not have proper left ideals and since \( d \not\in I \), we conclude that \( I = \{0\} \).

(7b.3) \( S \) does not have zero divisors.

Suppose that \( S \) has zero divisors. Then there exist \( u, v \in S - \{0\} \) such that \( uv = 0 \). But then \( u \in I_v \). By (7b.2), there must be an \( x \in S \) such that \( xv \neq 0 \). Therefore, \( x \in S - I_v \). By (7b.1), \( I_v \)
is a left ideal and since \( S \) does not have a proper left ideal, we must have \( I_v = \{0\} \), and so \( u = 0 \), a contradiction.

(7b.4) For any \( a \in S - \{0\} \), let \( (a) = \{ sa : s \in S \} \). Then \((a)\) is a left ideal. (The straight forward verification of this claim is omitted).

Since \( S^2 \neq 0 \), there must be some \( c, d \in S \) such that \( cd \neq 0 \), and so \( (d) \neq 0 \). Since \( S \) does not have a proper left ideal, we must have \((d) = S \). As \( d \in S = (d) \), there must be an element \( e \in S \) such that \( ed = d \).

(7b.5) \( e \) is in fact a two side identity.

First, from \( ed = d \), we have \( ded = d^2 \) and so \( (de - d)d = 0 \). By (7b.3), \( de = d \).

Now let \( a \in S - \{0\} \). Multiplying \( a \) from the left of both sides of \( ed = d \) to get \( aed = ad \). It follows that \( (ae - a)d = 0 \), and so by (7b.3), \( ae = a \). Multiplying \( a \) from the right of both sides of \( de = d \) to get \( dea = da \). It follows that \( d(ea - a) = 0 \), and so by (7b.3), \( ea = a \). Therefore, \( e \) is a two side identity of \( S \).

(7b.6) Every element \( a \in S - \{0\} \) is a unit.
By (7b.3), a is not a zero divisor, and so \( a \neq 0 \). By (7b.4) and since \( S \) does not have proper left ideals, we must have \( (a) = S \). Therefore, since \( e \in S = (a) \), there must be some \( b, c \in S \) such that \( ba = ac = e \). But \( b = be = b(ac) = (ba)c = ec = c \), and so \( a \) is a unit.

By (7b.5) and (7b.6), \( S \) is a division ring.

10. (a) Show that \( \mathbb{Z} \) is a principal ideal ring.
(b) Every homomorphic image of a principal ideal ring is also a principal ideal ring.
(c) \( \mathbb{Z}_m \) is a principal ideal ring for every \( m > 0 \).

**Proof:** (a) Let \( I \subseteq \mathbb{Z} \) be an ideal of \( \mathbb{Z} \). Since \( \mathbb{Z} = (1) \), and \( \{0\} = (0) \), we may assume that \( I \) is proper. Then since \( I \) is a proper ideal, \( I \) contains at least one positive integer. Pick \( a \in I \) be the smallest positive integer in \( I \), and we claim that \( I = (a) \).

Since \( a \in I \), it suffices to show that \( I \subseteq (a) \). Let \( x \in I - \{0\} \). By division algorithm, we can find integers \( q \) and \( r \) such that \( x = qa + r \) and such that \( 0 \leq r < a \). Since \( a \in I \) and since \( I \) is an ideal, \( qa \in I \) and so \( r = x - qa \in I \). It follows by the choice of \( a \) that \( r = 0 \). Hence \( \forall x \in I, x = qa \) for some \( q \in \mathbb{Z} \). Thus \( I \subseteq (a) \).

(b) Let \( R, R' \) be rings, such that \( R \) is a principal ideal ring, and \( f : R \rightarrow R' \) be a ring homomorphism such that \( R' = f(R) \). We want to show that \( R' \) is also a principal ideal ring.

Let \( I' \) be an ideal of \( R' \). Then \( I = f^{-1}(I') \) is an ideal of \( R \), and so \( \exists a \in R \) such that \( I = (a) \).

Note that (by Theorem 2.5(i)),

\[
I = (a) = \{ ra + as + na + \sum_{i=1}^{m} r_i a s_i : r, r_i, s_i \in R; \text{ and } m, n \in \mathbb{Z} \}.
\]

Let \( a' = f(a) \in R' \). Since \( f(R) = R' \), when \( r \) takes all the values of \( R \), \( f(r) \) takes all the values of \( R' \). Thus

\[
I' = f(I) = \{ f(r) a' + a' f(s) + na' + \sum_{i=1}^{m} f(r_i) a' f(s_i) : r, s, r_i, s_i \in R; \text{ and } m, n \in \mathbb{Z} \} = \{ r' a' + a' s' + na' + \sum_{i=1}^{m} r'_i a' s'_i : r', s', r'_i, s'_i \in R'; \text{ and } m, n \in \mathbb{Z} \} = (a').
\]

(c) Since \( \mathbb{Z} \) is a principal ideal ring and since the map \( f(n) = \overline{n} \in \mathbb{Z}_m \) is a ring epimorphism, it follows from (b) that \( \mathbb{Z}_m \) is a principal ideal ring.

11. If \( N \) is the ideal of all nilpotent elements in a commutative ring, then \( R/N \) is a ring with no nonzero nilpotent elements.

**Proof:** Let \( R' = R/N \) and suppose that \( a' \in R' \) is a nilpotent element. Then \( \exists a \in R \) such that \( a' = a + N \), for some positive integer \( n \), \( (a + N)^n = N \). Since \( N \) is an ideal, \( a^n \in N \), and so \( a^n \) is a nilpotent element. Thus for some positive integer \( m > 0 \), \( a^{mn} = (a^n)^m = 0 \). It follows that \( a \in N \) and so \( a' = a + N = N \) is the zero element in \( R' \). Therefore, \( R' \) does not have non zero nilpotent elements.
12. Let \( R \) be a ring without identity and with no zero divisors. Let \( S \) be the ring whose additive group is \( R \times \mathbb{Z} \) (with multiplication defined by \((r_1, k_1)(r_2, k_2) = (r_1r_2 + k_2r_1, k_1r_2, k_1k_2)\), for any \( r_1, r_2 \in R \) and \( k_1, k_2 \in \mathbb{Z} \). Let \( A = \{(r, n) : rx + nx = 0, \forall x \in R\}\).

(a) \( A \) is an idea in \( S \).
(b) \( S/A \) has an identity and contains a subring isomorphic to \( R \).
(c) \( S/A \) has no zero divisor.

**Proof:** (a) Let \((r', n') \in S \) and \((r, n) \in A\). Then \((r', n')(r, n) = (r'r + n'r + nr', n'n)\). For any \( x \in R \), \((r'r + n'r + nr')x + n'nx = r'(rx + nx) + n'(rx + nx) = 0\), and so \((r', n')(r, n) \in A\).

Similarly, \((r, n)(r', n') = (rr' + n'r + nr', n'n)\). For any \( x \in R \), \((rr' + n'r + nr')x + n'nx = r(r'x) + n(r'x) + n'(rx + nx) = 0\), and so \((r, n)(r', n') \in A\).

(b) Note that for any \((r, n) \in S\), \((0, 1)(r, n) = (r, n)(0, 1)\) and so \((0, 1)\) is the identity of \( S \), and so the element \((0, 1) + A\) is the identity of \( S/A \).

Define \( f : R \to S \) by \( f(r) = (r, 0) + A \) can be routinely verified to be a ring homomorphism. It suffices to show that \( \text{Ker}(f) = \{0\} \). Suppose that for some \( r, r' \in R \), \( f(r) = f(r') \). Then \( f(r - r') \in A \), and so \( \forall x \in R \), \( (r - r')x = 0 \). Since \( R \) does not have zero divisors, we must have \( r - r' = 0 \) and so \( r = r' \). This implies that \( f \) is a monomorphism.

(c) Let \((a, m) + A \) and \((b, n) + A \) be two non zero elements in \( S/A \). We assume that \((a, m)(b, n) + A = ((a, m) + B)((b, n) + A) = A \) or \((a, m)(b, n) \in A\) to derive a contradiction. Since \( a + A \) and \( b + A \) are nonzero elements in \( S/A \), \((a, m), (b, n) \not\in A\). Now suppose

\[
(ab + mb + na, mn) = (a, m)(b, n) \in A.
\]

Then \( \forall x \in R \), \((ab + mb + na)x + mnx = 0 \). Thus \( a(bx + nx) + m(bx + nx) = 0 \). Since \( R \) has no zero divisor and since \( a \neq 0 \), \( \forall x \in R \), we must have \( bx + nx = 0 \), and so \((b, n) \in A\), contrary to the assumption that \((b, n) \not\in A\).

14. If \( P \) is a proper ideal in a not necessarily commutative ring \( R \), then the following conditions are equivalent,

(a) \( P \) is a prime ideal.
(b) If \( r, s \in R \) are such that \( rRs \subseteq P \), then \( r \in P \) or \( s \in P \).
(c) If \( (r) \) and \( (s) \) are principal ideals of \( R \) such that \((r)(s) \subseteq P \), then \( r \in P \) or \( s \in P \).
(d) If \( U \) and \( V \) are right ideals in \( R \) such that \( UV \subseteq P \), then \( U \subseteq P \) or \( V \subseteq P \).
(e) If \( U \) and \( V \) are left ideals in \( R \) such that \( UV \subseteq P \), then \( U \subseteq P \) or \( V \subseteq P \).

**Proof:** (a) \( \Rightarrow \) (b). Suppose that for fixed \( r, s \in R \), \( rRs \subseteq P \). Since \( P \) is an ideal, \( RrR = R(rRs)R \subseteq P \). Similarly, \( RsR = R(rRs)R \subseteq P \). Again since \( P \) is an ideal, we have \((Rr)(RsR) \subseteq P \). However, both \( RrR \) and \( RsR \) are ideals (Firstly, apply Theorem III-2.2 to show that \( Rr \) is a left ideal: \( \forall x, y \in R \), \( xr - yr = (x - y)r \in Rr \) and \( \forall z \in R \), \( z(xr) = (zx)r \in Rr \). Then as \( R \) itself is also a left ideal, by Theorem III-2.6(1), \( RrR = (Rr)R \) is also a left ideal. Similarly, \( RrR \) is a right ideal, and so \( RrR \) is an ideal of \( R \)), and since \( P \) is a prime ideal, by Definition III-2.14 (definition of
prime ideal), either $RrR \subseteq P$ or $RsR \subseteq P$. Assume that $RsR \subseteq P$. Let $A = (s)$. Then $A$, $A^2$ and $A^3$ are ideals in $R$ (Theorem III-2.6). Since $A^3 \subseteq RsR \subseteq P$, by Definition III-2.14 again (repeated application if needed), we must have $(s) = A \subseteq P$, and so $s \in P$.

(b) $\implies$ (c). By the definition of an ideal, $rR \subseteq (r)$ and so $rRs = (rR)s \subseteq (r)(s) \subseteq P$. It follows by (b) that $r \in P$ or $s \in P$.

(c) $\implies$ (a). Apply Theorem III-2.15.

(b) $\implies$ (d). Suppose that we have $r \in U - P \neq \emptyset$. Since $U$ is a right ideal, $rR \subseteq U$. For any $s \in V$, we have $rRs \subseteq UV \subseteq P$. By (b) and since $r \notin P$, we must have $s \in P$, and so $V \subseteq P$. (Applying Theorem 2.15 to argue (b) $\implies$ (d) may not work, as $R$ may not be commutative.)

(d) $\implies$ (a). For any ideals $A, B$ such that $AB \subseteq P$, as any ideals are right ideals, by (d), $A \subseteq P$ or $B \subseteq P$, and so $P$ is prime by Definition III-2.14.

The proofs for (b) $\implies$ (c) $\implies$ (a) are similar and so are omitted.

19. The ring of even integers contains a maximal ideal $M$ such that $E/M$ is not a field.

**Proof:** Note that $E = (2)$ is a principal ideal in $\mathbb{Z}$. Let $p > 0$ be a prime and let $M = (2p)$. Then $M$ is a principal ideal of $E$. Let $I$ be an ideal in $E$. Then $\exists a \in E$ with $a > 0$ such that $I = (2a)$ (One can imitate the proof that $\mathbb{Z}$ is a principal ideal to show that $E$ is also a principal ideal ring). If $M \subseteq I$, then $2a|2p$ or $a|p$. Hence either $a = p$ or $a = 1$, and so $M$ is a maximal ideal.

To see that $E/M$ is no an integral domain, we observe that $E/M = \{0, 2, \ldots, 2p-2\}$. Hence $\forall a, b \in E/M - \{0\}, ab \neq a$ and $ab \neq b$. Therefore $E/M$ does not have an identity and so $E/M$ cannot be a field.