Throughout, $A$ is a commutative ring with $0 \neq 1$.

1. We say that $a \in A$ is a zerodivisor if there exists $b \neq 0$ in $A$ such that $ab = 0$. (This differs from Lang’s definition only to the extent that $0$ will be called a zerodivisor.)

Let $\mathcal{F}$ be the set of all ideals of $A$ in which every element is a zerodivisor.

(a) Prove that $\mathcal{F}$ has maximal elements.

(b) Prove that every maximal element of $\mathcal{F}$ is a prime ideal.

(c) Conclude that the set of zerodivisors is a union of prime ideals.

**Solution:** (a) Since $(0) \in \mathcal{F}$, the set $\mathcal{F}$ is nonempty. Given a chain $\{a_\alpha\}$ of elements of $\mathcal{F}$, it is easily seen that $\bigcup_\alpha a_\alpha$ is an ideal as well. Since each element of this ideal is a zerodivisor, it follows that $\bigcup_\alpha a_\alpha \in \mathcal{F}$. By Zorn’s Lemma, the set $\mathcal{F}$ has maximal elements.

(b) Let $p \in \mathcal{F}$ be a maximal element. If $x \notin p$ and $y \notin p$, then the ideals $p + (x)$ and $p + (y)$ are strictly bigger than $p$, and hence there exist nonzerodivisors $a \in p + (x)$ and $b \in p + (y)$. But then $ab \in p + (xy)$ is a nonzero divisor, and so $xy \notin p$. Consequently $p$ is a prime ideal.

(c) If $x \in A$ is a zerodivisor, then every element of the ideal $(x)$ is a zerodivisor. Hence $(x) \in \mathcal{F}$, and so $(x) \subseteq p$ for some prime ideal $p \in \mathcal{F}$. It follows that

$$\{x \mid x \in A \text{ is a zerodivisor}\} = \bigcup_{p \in \mathcal{F}} p.$$

2. Let $a$ be a nilpotent element of $A$. Prove that $1 + a$ is a unit of $A$. Deduce that the sum of a nilpotent element and a unit is a unit.

**Solution:** If $a$ is nilpotent, then $a^n = 0$ for some $n > 0$. But then

$$(1 + a)(1 - a + a^2 - a^3 + \cdots + (-1)^{n-1}a^{n-1}) = 1,$$

and so $1 + a$ is a unit.

If $u$ is a unit and $a$ is nilpotent, then $u^{-1}a$ is nilpotent. By the above argument $1 + u^{-1}a$ is a unit, and so $u(1 + u^{-1}a) = u + a$ is a unit as well.

3. Let $A[x]$ be the ring of polynomials in an indeterminate $x$ with coefficients in a ring $A$. Let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ where $a_i \in A$.

(a) Prove that $f$ is a unit in $A[x]$ if and only if $a_0$ is a unit in $A$ and $a_1, \ldots, a_n$ are nilpotent.

(Hint: If $b_0 + b_1x + \cdots + b_nx^n$ is the inverse of $f$, prove by induction on $r$ that $a_n^{r+1}b_{n-r} = 0$.)

(b) Prove that $f$ is nilpotent if and only if $a_0, a_1, \ldots, a_n$ are nilpotent.

**Solution:** First note that if $a_1, \ldots, a_n$ are nilpotent, then $a_1x, a_2x^2, \ldots, a_nx^n$ are nilpotent as well. If $a$ is a unit, it follows from the previous problem that $f = a_0 + a_1x + \cdots + a_nx^n$ is a unit. For the converse, assume that $f$ is a unit, and so there exists $g = b_0 + b_1x + \cdots + b_nx^n \in A$ with $fg = 1$. Comparing the constant terms, we see that $a_0b_0 = 1$, so $a_0, b_0 \in A$ are units. If $n = 0$, there is nothing more to be proved, so assume $n \geq 1$. We prove inductively that $a_n^{r+1}b_{n-r} = 0$
Solutions to Assignment 5

for all $0 \leq r \leq m$. Comparing coefficients of $x^{m+n}$ in the equation $fg = 1$, we see that $a_nb_m = 0$, so the result is true for $r = 0$. Comparing the coefficients of $x^{m+n-r-1}$ for some $r < m$, we get

$$a_nb_{m-r-1} + a_{n-1}b_{m-r} + \cdots + a_{n-r-1}b_m = 0.$$  

Multiplying this equation by $a_n^{r+1}$ and using the induction hypothesis, we get $a_n^{r+2}b_{m-r-1} = 0$, which completes the induction. Consequently $a_n^{m+1}b_0 = 0$, but then $a_n^{m+1} = 0$ since $b_0$ is a unit. This shows that $a_n$ is nilpotent. Now $f - a_nx^n = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ is a unit, and an inductive argument shows that $a_{n-1}, \ldots, a_1$ are nilpotent.

4. Let $A$ be a ring and $\mathfrak{N}$ its nilradical. Prove that the following are equivalent:

(a) $A$ has exactly one prime ideal;
(b) every element of $A$ is either a unit or is nilpotent;
(c) $A/\mathfrak{N}$ is a field.

**Solution:** (a) $\implies$ (b) Since $\mathfrak{N}$ is the intersection of all prime ideals, (a) implies that $\mathfrak{N}$ is the unique prime ideal of $A$, in particular, $\mathfrak{N}$ is a maximal ideal. If $x \in A$ is not a unit, i.e., $(x) \neq A$, then $(x) \subseteq \mathfrak{N}$, and so $x$ is nilpotent.

(b) $\implies$ (c) If $x + \mathfrak{N}$ is nonzero in $A/\mathfrak{N}$ then $x \notin \mathfrak{N}$, and so $x$ is a unit in $A$. But then $x + \mathfrak{N}$ is a unit in $A/\mathfrak{N}$.

(c) $\implies$ (a) Since $A/\mathfrak{N}$ is a field, $\mathfrak{N}$ is a maximal ideal. But $\mathfrak{N}$ is the intersection of all prime ideals of $A$, so it must be the only prime ideal.

5. An element $e \in A$ is an **idempotent** if $e^2 = e$. Prove that the only idempotent elements in a local ring are 0 and 1.

**Solution:** Let $\mathfrak{m}$ be the unique maximal ideal of $A$. Then $e(1 - e) = 0 \in \mathfrak{m}$ and since $\mathfrak{m}$ is prime, $e \in \mathfrak{m}$ or $1 - e \in \mathfrak{m}$. Note that $e$ and $1 - e$ cannot both be elements of $\mathfrak{m}$ since this would imply $1 = e + (1 - e) \in \mathfrak{m}$.

If $e \in \mathfrak{m}$, then $1 - e \notin \mathfrak{m}$, and so $1 - e$ is a unit. But then $e = 0$. Similarly, if $1 - e \in \mathfrak{m}$, then $e$ is a unit and so $1 - e = 0$.

6. Let $\mathfrak{N}$ be the nilradical of a ring $A$. If $a + \mathfrak{N}$ is an idempotent element of $A/\mathfrak{N}$, prove that there exists a unique idempotent $e \in A$ with $e - a \in \mathfrak{N}$.

**Solution:** Since $a(1 - a) = a - a^2 \in \mathfrak{N}$, there exists $n > 0$ with $a^n(1 - a)^n = 0$. Taking the binomial expansion,

$$1 = (a + (1 - a))^{2n-1} = a^{2n-1} + \binom{2n-1}{1}a^{2n-2}(1-a) + \cdots + \binom{2n-1}{n-1}a^{n}(1-a)^{n-1} + \binom{2n-1}{n}a^{n-1}(1-a)^n + \cdots + (1-a)^{2n-1}.$$

Let $e = a^n\alpha$ be the sum of the first $n$ terms, and $1 - e = (1-a)^n\beta$ be the sum of the remaining $n$ terms. Then $e(1-e) = a^n(1-a)^n\alpha\beta = 0$, so $e \in A$ is an idempotent. Since $a(1-a) \in \mathfrak{N}$, we see that $e \equiv a^{2n-1} \mod \mathfrak{N} \equiv a \mod \mathfrak{N}$.

We next prove the uniqueness: If $a, b \in A$ are idempotents with $a - b \in \mathfrak{N}$, then $a(a-b) = a - ab = a(1-b) \in \mathfrak{N}$. Therefore there exists $n > 0$ with $a^n(1-b)^n = 0$. But $1 - b$ is an idempotent as well, so $a^n(1-b)^n = a(1-b) = 0$, i.e., $a = ab$. Similarly, $b = ab$, and so $a = b$.  

2
Solutions to Assignment 5

7. Let \( A \) be a ring and let \( X = \text{Spec} \ A \). Recall that for each subset \( E \) of \( A \), we defined \( V(E) = \{ p \in X \mid E \subseteq p \} \), and that these are precisely the closed sets for the Zariski topology on \( X \). For each \( f \in A \), let \( X_f \) be the complement of \( V(f) \) in \( X \). The sets \( X_f \) are open in the Zariski topology. Prove that

(a) the sets \( X_f \) form a basis of open sets, i.e., every open set in \( X \) is a union of sets of the form \( X_f \);
(b) \( X_f \cap X_g = X_{fg} \);
(c) \( X_f = \emptyset \) if and only if \( f \) is nilpotent;
(d) \( X_f = X \) if and only if \( f \) is a unit;
(e) \( X_f = X_g \) if and only if \( \text{radical}(f) = \text{radical}(g) \);

**Solution:**

(a) Given an open set \( X \setminus V(E) \) and a point \( p \in X \setminus V(E) \), there exists \( f \in E \setminus p \). But then \( p \in X_f \subseteq X \setminus V(E) \). Consequently \( X \setminus V(E) \) is a union of open sets of the form \( X_f \).

(b) \( X_f \cap X_g = (X \setminus V(f)) \cap (X \setminus V(g)) = X \setminus (V(f) \cup V(g)) = X \setminus V(fg) = X_{fg} \).

(c) \( X_f = \emptyset \iff \forall f(\alpha) = X \iff f \) belongs to every prime ideal of \( A \iff f \) is nilpotent.

(d) \( X_f = X \iff V(f) = \emptyset \iff f \) is a unit of \( A \).

(e) If \( X_f = X_g \), then \( f \) and \( g \) are contained in precisely the same set of prime ideals. Consequently

\[
\text{radical}(f) = \bigcap_{p \mid f \notin p} p = \bigcap_{p \mid g \notin p} p = \text{radical}(g).
\]

Conversely, suppose that \( \text{radical}(f) = \text{radical}(g) \). If \( p \in X_f \) then \( \text{radical}(f) \not\owns p \), and so \( g \notin p \). This implies that \( p \in X_g \), and so we have \( X_f \subseteq X_g \). By symmetry we conclude that \( X_f = X_g \).

8. Prove that \( X = \text{Spec} \ A \) is a compact topological space, i.e., every open cover of \( X \) has a finite subcover.

(Hint: It is enough to consider a cover of \( X \) by basic open sets \( X_{f_i} \).)

**Solution:** Suppose that \( X = \bigcup_{\alpha \in \Lambda} X_{f_\alpha} \). Then

\[
X = \bigcup_{\alpha \in \Lambda} X \setminus V(f_\alpha) = X \setminus \left( \bigcap_{\alpha \in \Lambda} V(f_\alpha) \right) = X \setminus V(f_\alpha \mid \alpha \in \Lambda),
\]

and so \( V(f_\alpha \mid \alpha \in \Lambda) = \emptyset \). But then \( (f_\alpha \mid \alpha \in \Lambda) \) is the unit ideal, and so there exist \( \alpha_i \in \Lambda \) and \( g_i \in A \) such that

\[
f_{\alpha_1}g_1 + \cdots + f_{\alpha_n}g_n = 1.
\]

It follows that \( X = X_{f_{\alpha_1}} \cup \cdots \cup X_{f_{\alpha_n}} \).

9. Let \( A_1, A_2 \) be rings, and \( A_1 \times A_2 \) their direct product. What are the prime ideals of the ring \( A_1 \times A_2 \)?

**Solution:** We first claim that all ideals of \( A_1 \times A_2 \) are of the form \( a_1 \times a_2 \) for ideals \( a_i \in A_i \). Given an ideal \( a \) of \( A_1 \times A_2 \), let \( a_1 \subseteq A_1 \) be the ideal which is the image of \( a \) under the projection homomorphism \( A_1 \times A_2 \to A_i \). It is easily seen that \( a \subseteq a_1 \times a_2 \). Conversely, if \( x \in a_1 \) and \( y \in a_2 \), then \((x,\beta) \in a \) and \((\alpha, y) \in a \) for some \( \alpha \in A_1 \) and \( \beta \in A_2 \). But then

\[
(x, y) = (x, \beta)(1, 0) + (\alpha, y)(0, 1) \in a.
\]
An ideal $a_1 \times a_2$ is prime if and only if
\[
(A_1 \times A_2)/(a_1 \times a_2) \approx A_1/a_1 \times A_2/a_2
\]
is a domain. But this can only happen if one of the rings $A_i/a_i$ is the zero ring, and the other
is a domain. Consequently the prime ideals of the ring $A_1 \times A_2$ are precisely those which are of
the form $A_1 \times p_2$ and $p_1 \times A_2$ where $p_i$ is a prime ideal of $A_i$.

10. Let $A$ be a ring. Prove that the following are equivalent:

(a) $X = \text{Spec } A$ is disconnected, i.e., $X$ is the disjoint union of two open sets;
(b) $A \approx A_1 \times A_2$ for rings $A_1, A_2$, neither of which is the zero ring;
(c) $A$ contains an idempotent other than 0 and 1.

**Solution:** (a) $\implies$ (b) Let $X = V(a) \cup V(b)$ be a disjoint union of nonempty closed (equivalently, open) sets. Then $a + b = A$, and so there exists $a \in a$ with $1 - a \in b$. Also, $ab$ is contained in every prime ideal, so $a(1 - a) \in ab \subseteq R$. This implies that $a + R \in A/R$ is an idempotent. By Problem 6, there exists an idempotent $e \in A$ with $e - a \in R$. If $e$ is a unit, then so is $a$, but this is not possible since $a \neq A$. A similar argument shows that $1 - e$ is not a unit. Consider the homomorphism

$$A \xrightarrow{\varphi} A/(e) \times A/(1 - e) \quad \text{where} \quad \varphi(x) = (x + (e), x + (1 - e)).$$

The Chinese remainder theorem implies that $\varphi$ is surjective. The kernel is $(e) \cap (1 - e) = 0$, and therefore $\varphi$ is an isomorphism.

(b) $\implies$ (c) The element $(1, 0) \in A_1 \times A_2$ is a nonzero idempotent.

(c) $\implies$ (a) If $e \in A$ is an idempotent other than 0 and 1, we claim $X = V(e) \cup V(1 - e)$ where
$V(e)$ and $V(1 - e)$ are disjoint closed sets. Since $e(1 - e) = 0$, every prime contains either $e$ or
$1 - e$, and no prime can contain both. If $V(e) = \emptyset$, then $e$ is a unit, but then $e = 1$. Similarly
$V(1 - e)$ is nonempty as well.