Solutions to Assignment 5

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 $\{\mathfrak{a}_\alpha\}$ of elements of $\mathcal{F}$, it is easily seen that $\bigcup_\alpha \mathfrak{a}_\alpha$ is an ideal as well. Since each element of this ideal is a zerodivisor, it follows that $\bigcup_\alpha \mathfrak{a}_\alpha \in \mathcal{F}$. By Zorn's Lemma, the set $\mathcal{F}$ has maximal elements.

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

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

2. Let $\mathfrak{a}$ be an ideal of A. Prove that radical($\mathfrak{a}$) is the intersection of all prime ideals of A containing $\mathfrak{a}$. **Solution:** Consider the quotient ring $A/\mathfrak{a}$. By Theorem porved in class, the nilradical of $A/\mathfrak{a}$ is the intersections of all prime ideals of $A/\mathfrak{a}$. The prime ideals of $A/\mathfrak{a}$ are in 1-1 correspondence of the prime ideals of A containing $\mathfrak{a}$ under the canonical homomorphism, and the nilradical of $A/\mathfrak{a}$ corresponds to the radical($\mathfrak{a}$) under the same correspondence.

3. Recall that a commutative ring A is Noetherian iff every ideal of A is finitely generated. Prove that A is Noetherian if every *prime* ideal is finitely generated. (Hint. Consider the set of ideals of A which are not finitely generated and use Zorn's lemma to find a maximal element.)

4. 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 $1 - e = 0$.

5. 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 exits 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,

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

   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 $e \equiv a^{2n-1} \mod \mathfrak{N} \equiv \mathfrak{a} \mod \mathfrak{N}$.

   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 $a = b$.

6. Prove that the subring of $\mathbb{Z}[i]$ of $\mathbb{C}$ is principal.
   Solution: We show that the ring $\mathbb{Z}[i]$ is Euclidean under the Euclidean norm $d(a+bi) = a^2 + b^2$ and then it follows that the ring $\mathbb{Z}[i]$ is factorial.

   In order to check that the map d satisfies the axioms of being a Euclidean norm, we need to check that for each $x, y \in \mathbb{Z}[i], y \neq 0$, there exists $q, r \in \mathbb{Z}[i]$ such that $x = qy + r$ and either $r = 0$ or $d(r) < d(y)$.

   First consider the case when $y = n \in \mathbb{Z}$. Let $x = u + iv, u, v \in \mathbb{Z}$. Let $u = an + b, v = cn + d$ and we can assume that $|c|, |d| \leq n/2$. Then, $x = an + b + (cn + d)i = (a + ic)n + (b + id)$. Letting $r = b + id$, notice that $d(r) = b^2 + d^2 \leq n^2/4 < n^2$.

   More generally, let $y\bar{y} = n$ and apply the previous part to obtain $x\bar{y} = qn + r$ wit $r = 0$ or $d(r) < n^2$. Then $\bar{y}(x - qy) = r$ and since $d(r) = |r|^2 < n^2$, and $|\bar{y}| = |y| = n$ we have that $|x - qy| < n/2 < n$.

7. Prove that the ring $\mathbb{R}[X, Y, Z]/(X^2 + Y^2 + Z^2)$ is factorial. What about the ring $\mathbb{C}[X, Y, Z]/(X^2 + Y^2 + Z^2)$?

   Solution: Discussed in class.

8. (Five lemma) Consider the following commutative diagram of A-modules and homomorphisms where each row is exact.

$$\begin{tikzcd} M_1 \arrow[r] \arrow[d, "a"'] & M_2 \arrow[r] \arrow[d, "b"'] & M_3 \arrow[r] \arrow[d, "c"'] & M_4 \arrow[r] \arrow[d, "d"'] & M_5 \arrow[d, "e"'] \\ N_1 \arrow[r] & N_2 \arrow[r] & N_3 \arrow[r] & N_4 \arrow[r] & N_5 \end{tikzcd}$$

Prove (by diagram chasing) that if a, b, d, e are isomorphisms then so is c. (extra credit: Can you reduce further the hypothesis on a, b, d, e ?)

Solution:

Let ϕ_i (resp. ψ_i) for $1 \leq i \leq 4$ be the horizontal homomorphisms $M_i \to M_{i+1}$ (resp. $N_i \to N_{i+1}$).

We first show that c is injective. Let $c(x_3) = 0$ for some $x_3 \in M_3$. Then $d\phi(x_3) = 0 \Rightarrow \phi_3(x_3) =$, because d is an isomorphism. Hence, $x_3 \in ker(\phi_3) = Im(\phi_2)$. Let $x_2 \in M_2$ be such that $x_3 = \phi_2(x_2)$. But then, $\psi_2 b(x_2) = 0 \Rightarrow b(x_2) \in ker(\psi_2) = Im(\psi_1)$. Let $y_1 \in N_1$ be such that $\psi_1(y_1) = b(x_2)$. Since a is an isomorphism there exists $x_1 \in M_1$ such that $y_1 = a(x_1)$ and $\psi_1 a(x_1) = b(x_2) = b\phi_1(x_1)$. Since b is an isomorphism this implies that $x_2 = \phi_1(x_1)$, and thus $x_3 = \phi_2\phi_1(x_1) = 0$.

Next we show that c is surjective. Let $y_3 \in N_3$. Since d is surjective there exists $x_4 \in M_4$ such that $\psi_3(y_3) = d(x_4)$. Now, $\psi_4\psi_3(y_3) = 0 = e\phi_4(x_4)$. Since e is injective this implies that $x_4 \in ker(\phi_4) = Im(\phi_3)$. Let $x_3 \in M_3$ be such that $x_4 = \phi_3(x_3)$. Then, $d\phi_3(x_3) = \psi_3 c(x_3) = \psi_3(y_3)$. Hence, $c(x_3) - y_3 \in ker(\psi_3) = Im(\psi_2)$. Let $y_2 \in N_2$ be such that $\psi_2(y_2) = c(x_3) - y_3$. There exists $x_2 \in M_2$ such that $\psi_2 b(x_2) = c(x_3) - y_3 = c\phi_2(x_2)$. But then, $c(x_3 - \phi_2(x_2)) = y_3$ showing that c is surjective.

9. Let k be a field. The ring $k[x, y]$ can be viewed as a k-module, as a $k[x]$-module, as a $k[y]$-module, or as a $k[x, y]$-module. Illustrate the differences between these structures by providing non-trivial examples of maps from $k[x, y]$ to itself which are:
   (a) k-module homomorphism but not a $k[x], k[y], k[x, y]$-module homomorphisms; **Solution:** Example: the homomorphism that sends $f(x, y)$ to the polynomial $f(y, x)$ is an example of such a homomorphism.
   (b) a $k[x]$-module homomorphism but not a $k[y], k[x, y]$-module homomorphisms; **Solution:** Example: the homomorphism that send $f(x, y)$ to the polynomial $f(x, y^2)$.
   (c) a ring homomorphism but not a $k[x, y]$-module homomorphism. **Solution:** The example in part (a).

10. Let A be a ring and let $X = \operatorname{Spec} A$. Recall that for each subset E of A, we defined $V(E) = \{\mathfrak{p} \in X \mid E \subseteq \mathfrak{p}\}$, 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 radical(f) = radical(g);

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

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

(c) $X_f = \emptyset \iff V(f) = X \iff f$ 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

$$\text{radical}(f) = \bigcap_{\mathfrak{p} \mid f \in \mathfrak{p}} \mathfrak{p} = \bigcap_{\mathfrak{p} \mid g \in \mathfrak{p}} \mathfrak{p} = \text{radical}(g).$$

Conversely, suppose that radical(f) = radical(g). If $\mathfrak{p} \in X_f$ then radical$(f) \nsubseteq \mathfrak{p}$, and so $g \notin \mathfrak{p}$. This implies that $\mathfrak{p} \in X_g$, and so we have $X_f \subseteq X_g$. By symmetry we conclude that $X_f = X_g$.

11. Prove that $X = \operatorname{Spec} A$ 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

    $$X = \bigcup_{\alpha \in \Lambda} X \setminus V(f_\alpha) = X \setminus \big(\bigcap_{\alpha \in \Lambda} V(f_\alpha)\big) = X \setminus V(f_\alpha \mid \alpha \in \Lambda),$$

    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 $X = X_{f_{\alpha_1}} \cup \cdots \cup X_{f_{\alpha_n}}$.

12. 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 $\mathfrak{a}_1 \times \mathfrak{a}_2$ for ideals $\mathfrak{a}_i \in A_i$. Given an ideal $\mathfrak{a}$ of $A_1 \times A_2$, let $\mathfrak{a}_i \subset A_i$ be the ideal which is the image of $\mathfrak{a}$ under the projection homomorphism $A_1 \times A_2 \longrightarrow A_i$. It is easily seen that $\mathfrak{a} \subseteq \mathfrak{a}_1 \times \mathfrak{a}_2$. Conversely, if $x \in \mathfrak{a}_1$ and $y \in \mathfrak{a}_2$, then $(x, \beta) \in \mathfrak{a}$ and $(\alpha, y) \in \mathfrak{a}$ for some $\alpha \in A_1$ and $\beta \in A_2$. But then

    $$(x, y) = (x, \beta)(1, 0) + (\alpha, y)(0, 1) \in \mathfrak{a}.$$

An ideal $\mathfrak{a}_1 \times \mathfrak{a}_2$ is prime if and only if

$$(A_1 \times A_2)/(\mathfrak{a}_1 \times \mathfrak{a}_2) \approx A_1/\mathfrak{a}_1 \times A_2/\mathfrak{a}_2$$

is a domain. But this can only happen if one of the rings $A_i/\mathfrak{a}_i$ 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 $A_1 \times \mathfrak{p}_2$ and $\mathfrak{p}_1 \times A_2$ where $\mathfrak{p}_i$ is a prime ideal of A_i.

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

    (a) $X = \operatorname{Spec} A$ 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 $X = V(\mathfrak{a}) \cup V(\mathfrak{b})$ be a disjoint union of nonempty closed (equivalently, open) sets. Then $\mathfrak{a} + \mathfrak{b} = A$, and so there exists $a \in \mathfrak{a}$ with $1 - a \in \mathfrak{b}$. Also, $\mathfrak{a}\mathfrak{b}$ is contained in every prime ideal, so $a(1-a) \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{N}$. This implies that $a + \mathfrak{N} \in A/\mathfrak{N}$ is an idempotent. By Problem 6, there exists an idempotent $e \in A$ with $e - a \in \mathfrak{N}$. If e is a unit, then so is a, but this is not possible since $\mathfrak{a} \neq A$. 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 φ is surjective. The kernel is $(e) \cap (1-e) = 0$, and therefore φ 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.

14. Let $L_1, \ldots, L_m$ be finite dimensional vector spaces over a field k and let $t \in L_1 \otimes \cdots L_m$. By the rank of t we mean the smallest number r such that t can be expressed as $t = \sum_{1 \le i \le r} v_1^i \otimes \cdots \otimes v_m^i$, where $v_j^i \in L_j$.

    (a) Let $t \in L_1^* \otimes L_2 = Hom(L_1, L_2)$. Prove that the rank of t is equal to $dim(im(t)), t : L_1 \to L_2$.

    Solution: Suppose $t = v^* \otimes w$ for $v^* \in L_1^*, w \in L_2$. Then writing in terms of a basis, it is clear that the matrix corresponding to t (as a linear transformation from L_1 to L_2) has rank at most one or that $dim(im(t)) \le 1$. Now, if

    $$t = \sum_{1 \le i \le r} v_i^* \otimes w_i,$$

with $v_i^* \in L_1, w_i \in L_2$ then the matrix corresponding to t is the sum of r rank one matrices and must have rank $\leq r$. This shows that $rank(t) \leq r \leq dim(im(t))$.

Conversely, we know that a matrix of rank r can be written as the sum of at most r rank one matrix. Hence, $rank(t) = dim(im(t))$.

(b) (extra credit) Let $L = \oplus_{1 \leq i,j \leq 2} \mathbb{C} a_{ij}$ be the space of complex 2×2 matrices. Prove that,

$$rank(\sum_{1 \leq i,j,k \leq 2} a_{ij} \otimes a_{jk} \otimes a_{ki}) \leq 7.$$

Solution: The given expression for the tensor $t = \sum_{1 \leq i,j,k \leq 2} a_{ij} \otimes a_{jk} \otimes a_{ki}$ shows that the $rank(t) \leq 8$. We can rewrite t as follows (please check) which will show that the rank is at most 7 .

$$\begin{aligned}
t &= (a_{11} - a_{22}) \otimes (a_{11} - a_{22}) \otimes (a_{11} + a_{22}) \\
&+ (a_{12} - a_{22}) \otimes (-a_{21} - a_{22}) \otimes (-a_{11}) \\
&+ (-a_{22}) \otimes (a_{11} + a_{21}) \otimes (-a_{11} - a_{21}) \\
&+ (a_{11} - a_{12}) \otimes (-a_{22}) \otimes (-a_{11} + a_{12}) \\
&+ a_{11} \otimes (-a_{22} - a_{12}) \otimes (-a_{12} - a_{22}) \\
&+ (-a_{22} + a_{21}) \otimes a_{11} \otimes (a_{11} - a_{22}) \\
&+ (a_{11} - a_{21}) \otimes (a_{11} + a_{12}) \otimes (-a_{22}).
\end{aligned}$$