COMMUTATIVE ALGEBRA HOMEWORK I

HOJIN LEE 2021–11045

I tend to use the conventions of Atiyah & Macdonald, since I have studied this first. Please bear with me.

Problem 1. *Compute the following:*

1. $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m))$ *and* $\mathrm{Hom}_{k[x]}(k[x]/(x^n), k[x]/(x^m))$.
2. $\mathbb{Z}/(n) \otimes_{\mathbb{Z}} \mathbb{Z}/(m)$ *and* $k[x]/(x^n) \otimes_{k[x]} k[x]/(x^m)$.
3. $k[x,y]/(y^2 - x^2(x+1)) \otimes_{k[x,y]} k[x,y]/(y)$.

Proof. 1. Consider the exact sequence

$$\mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/(n) \to 0$$

and apply $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/(m))$ to get

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/(m)) \xrightarrow{\times n} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/(m)).$$

Using the identity $\mathrm{Hom}_A(A, M) \cong M$, we conclude

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \cong \ker\left(\mathbb{Z}/(m) \xrightarrow{\times n} \mathbb{Z}/(m)\right).$$

For $\overline{k} \in \mathbb{Z}/(m)$ to be in the kernel, $kn = mz$ must hold for some integer z. Let $d = \gcd(m,n)$ and write $m = dm'$, $n = dn'$. Then $k = m'z/n'$. There are d possibilities of z, namely $0, n', \ldots, (d-1)n'$. It follows that the kernel is a subgroup of order d of $\mathbb{Z}/(m)$, which is isomorphic to $\mathbb{Z}/(d)$.

Similarly, consider the exact sequence

$$k[x] \xrightarrow{\times x^n} k[x] \to k[x]/(x^n) \to 0$$

and apply $\mathrm{Hom}_{k[x]}(-, k[x]/(x^m))$ to get

$$0 \to \mathrm{Hom}_{k[x]}(k[x]/(x^n), k[x]/(x^m)) \to k[x]/(x^m) \xrightarrow{\times x^n} k[x]/(x^m),$$

again using the identity $\mathrm{Hom}_A(A, M) \cong M$. In the case $n \geq m$, the kernel $\ker\left(k[x]/(x^m) \xrightarrow{\times x^n} k[x]/(x^m)\right)$ is just $k[x]/(x^m)$. If $n < m$, then for $f + (x^m) \in k[x]/(x^m)$ to be in the kernel, f must have degree $< m-n$ coefficients all zero. Denote as P the $k[x]$-module of all such $f + (x^m)$. Then the $k[x]$-module homomorphism $k[x]/(x^n) \xrightarrow{\times x^{m-n}} P$ is bijective, so $P \cong k[x]/(x^n)$. Therefore we may conclude

$$\mathrm{Hom}_{k[x]}(k[x]/(x^n), k[x]/(x^m)) \cong k[x]/(x^{\min(m,n)}).$$

□

Date: March 20, 2024.

Proof. 2. We first prove the identity

$$R/I \otimes_R R/J \cong R/(I+J).$$

Define $\varphi : R/I \times R/J \to R/(I+J)$ by $(r_1+I, r_2+J) \mapsto r_1r_2+I+J$. Suppose $r_1 - r_1' \in I$ and $r_2 - r_2' \in J$. Since $r_1r_2 - r_1'r_2' = r_2(r_1-r_1') + r_1'(r_2-r_2') \in I+J$, this map is well-defined. Also, this map is R-bilinear, which yields $\exists! \widetilde{\varphi} : (R/I) \otimes_R (R/J) \to R/(I+J)$ such that $(r_1+I) \otimes (r_2+J) \mapsto r_1r_2+I+J$. Note that $(r_1+I)\otimes(r_2+J) = r_1r_2(1+I)\otimes(1+J)$, so $\widetilde{\varphi}$ is bijective, hence an isomorphism.

Using this identity, we conclude $\mathbb{Z}/(n) \otimes_{\mathbb{Z}} \mathbb{Z}/(m) \cong \mathbb{Z}/((n)+(m))$, where $(n)+(m) = (\gcd(m,n))$. Write $d = \gcd(m,n)$, then this is $\mathbb{Z}/(d)$.

As above, we have

$$k[x]/(x^n) \otimes_{k[x]} k[x]/(x^m) \cong k[x]/((x^n)+(x^m)),$$

where $(x^n)+(x^m) = (x^{\min(m,n)})$. Hence this is $k[x]/(x^{\min(m,n)})$. ☐

Proof. 3. Using the identity proved in 2, this is isomorphic to $k[x,y]/(y, y^2 - x^2(x+1))$. I do not know how to further simplify this. ☐

Problem 2. *Let A be a ring, let $I_1, \ldots, I_n$ ideals of A s.t. $I_i + I_j = A$ for $i \neq j$. Show $A/(\bigcap_k I_k) \cong \prod_k A/I_k$.*

Proof. Define $\phi : A \to \prod_k A/I_k$ by $a \mapsto (a+I_1, \ldots, a+I_n)$. We claim this homomorphism is surjective. To show this, it is enough to find $x_k \in A$ such that $\phi(x_k) = (I_1, \ldots, 1+I_k, \ldots, I_n)$ for each $1 \leq k \leq n$. Since $I_k + I_j = A$ for all $j \neq k$, there exists $u_j \in I_j$ such that $u_k + u_j = 1$ for a fixed $u_k \in I_k$. Take $x_k = 1 - u_k$. Then for all j, we have $x_k = u_j$, so $(x_k+I_1, \ldots, x_k+I_k, \ldots, x_k+I_n) = (I_1, \ldots, 1+I_k, \ldots, I_n)$. Surjectivity follows obviously. Also, the kernel of ϕ is a such that $a \in I_k$ for all k, i.e. is $\bigcap_k I_k$. By the first isomorphism theorem we have $A/(\bigcap_k I_k) \cong \prod_k A/I_k$. ☐

Problem 3. *Prove the following are equivalent:*

1. *A contains a nontrivial idempotent*
2. *$A \cong A_1 \times A_2$ for some nonzero rings A_1 and A_2*

If $e \in A$ is a nontrivial idempotent, describe localization of A with respect to $\{e\}$.

Proof. ($\Rightarrow$) Suppose $e \in A$ such that $e^2 = e$, and $e \neq 0, 1$. Consider the ring homomorphism $A \to Ae \times A(1-e)$ given by $a \mapsto (ae, a(1-e))$, where $Ae = \{ae \mid a \in A\}$, and similarly for $A(1-e)$. Both have multiplicative identity e, $1-e$, respectively. If $ae = a(1-e) = 0$, then $ae + a - ae = a = 0$, so the map is injective. Also, for any $(ae, b(1-e))$ we have $ae + b(1-e) \mapsto (ae, b(1-e))$. Therefore $A \cong Ae \times A(1-e)$.

($\Leftarrow$) Take $(1,0) \in A_1 \times A_2$.

We now describe the localization of A with respect to $\{e\}$. We claim that $A_{\{e\}} \cong Ae$. Define a ring homomorphism $Ae \to A_{\{e\}}$ given by $ae \mapsto ae/e$. Since $a/e = ae/e$ for all $a \in A$, it follows that e/e is the multiplicative identity of $A_{\{e\}}$. Since $e \mapsto e/e$, this maps 1 to 1. Suppose $ae/e = 0$. Then $ae = 0$, so the kernel is trivial. Also, for any $a/e \in A_{\{e\}}$, if we send $ae \mapsto ae/e$, then $ae/e = a/e$, so this map is surjective. Therefore $A_{\{e\}} \cong Ae$. ☐

Problem 4. *Identify associated primes of a finitely generated abelian group, viewed as a $\mathbb{Z}$-module, in terms of the usual structure theory of finitely generated abelian groups.*

Proof. In the general case, the group is isomorphic to some $\mathbb{Z}^n \oplus \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k}\mathbb{Z}$, where p_i are prime numbers, not necessarily distinct. We first prove a preliminary result:

$$\operatorname{Ass}(M \oplus N) = \operatorname{Ass}(M) \cup \operatorname{Ass}(N) \text{ for } A\text{-modules } M \text{ and } N.$$

Suppose $\mathfrak{p} \in \operatorname{Ass}(M \oplus N)$. Then $\mathfrak{p} = \operatorname{Ann}(m, n)$ for some nonzero $(m, n) \in M \oplus N$. This means that elements of $\mathfrak{p}$ annihilate both m and n, so $\mathfrak{p} \subset \operatorname{Ann}(m) \cap \operatorname{Ann}(n)$. If $\mathfrak{p} = \operatorname{Ann}(m)$, then $\mathfrak{p} \in \operatorname{Ass}(M)$. Suppose $\mathfrak{p} \subsetneq \operatorname{Ann}(m)$. There exists some element $a \in \operatorname{Ann}(m)$ which is not in $\mathfrak{p}$. Then, $a(m, n) = (am, an) = (0, an) \neq 0$ since $a \notin \mathfrak{p} = \operatorname{Ann}(m, n)$. Hence $an \neq 0$, so $a \notin \operatorname{Ann}(n)$. From this, it follows that $\operatorname{Ann}(m) - \mathfrak{p} \subset \operatorname{Ann}(m) - \operatorname{Ann}(n)$, so $\operatorname{Ann}(m) \cap \operatorname{Ann}(n) \subset \mathfrak{p} \subset \operatorname{Ann}(m) \cap \operatorname{Ann}(n)$ which implies $\mathfrak{p} = \operatorname{Ann}(m) \cap \operatorname{Ann}(n)$. In this case, $\mathfrak{p}$ is either $\operatorname{Ann}(m)$ or $\operatorname{Ann}(n)$, but we assumed $\mathfrak{p} \subsetneq \operatorname{Ann}(m)$, so $\mathfrak{p} = \operatorname{Ann}(n)$. Hence $\mathfrak{p} \in \operatorname{Ass}(N)$. Therefore, $\operatorname{Ass}(M \oplus N) \subset \operatorname{Ass}(M) \cup \operatorname{Ass}(N)$. Conversely, if $\mathfrak{p}$ is either $\operatorname{Ann}(m)$ or $\operatorname{Ann}(n)$ for nonzero m, n, then it follows that $\mathfrak{p} = \operatorname{Ann}(m, 0)$ or $\operatorname{Ann}(0, n)$, which are both nonzero in $M \oplus N$. Thus the opposite inclusion holds, proving the result.

Using this, it suffices to find $\operatorname{Ass}(\mathbb{Z})$ and $\operatorname{Ass}(\mathbb{Z}/p^k\mathbb{Z})$. Since $\mathbb{Z}$ is torsion-free, the only associated prime of $\mathbb{Z}$ is (0). Now for $\mathbb{Z}/p^k\mathbb{Z}$, the prime ideals of $\mathbb{Z}$ that annihilates nonzero elements of $\mathbb{Z}/p^k\mathbb{Z}$ are (0) and (p).

Combining everything, the associated primes of $G \cong \mathbb{Z}^n \oplus \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k}\mathbb{Z}$ as a $\mathbb{Z}$-module are (0) and (p_i) for $1 \leq i \leq k$. Note that p_i may not be distinct. □

Problem 5. *Let A noetherian. Prove the total quotient ring $Q(A)$ has finitely many maximal ideals.*

Proof. Recall $Q(A) = A_{S(A)}$ where $S(A)$ is the set of A-regular elements of A, i.e. the non zerodivisors of A. The following lemmas consist the proof of the Lasker-Noether theorem, which is a copy of Atiyah & Macdonald, pp.82-83.

Lemma 7.11. Every ideal in a noetherian ring is a finite intersection of irreducible ideals.

Proof. Suppose not; then the set of ideals in A for which the lemma is false is not empty, hence has a maximal element $\mathfrak{a}$. Since $\mathfrak{a}$ is reducible, we have $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ where $\mathfrak{b} \supset \mathfrak{a}$ and $\mathfrak{c} \supset \mathfrak{a}$. Hence each of $\mathfrak{b}, \mathfrak{c}$ is a finite intersection of irreducible ideals and therefore so is $\mathfrak{a}$; contradiction. □

Lemma 7.12. In a noetherian ring, every irreducible ideal is primary.

Proof. Passing to quotient ring, ETS for zero ideal. Let $xy = 0$ with $y \neq 0$, and consider the chain of ideals $\operatorname{Ann}(x) \subset \operatorname{Ann}(x^2) \subset \cdots$. By ACC, this stabilizes at some n. It follows that $(x^n) \cap (y) = 0$, for if $a \in (y)$ then $ax = 0$, and if $a \in (x^n)$ then $a = bx^n$ so $bx^{n+1} = 0$, hence $b \in \operatorname{Ann}(x^{n+1}) = \operatorname{Ann}(x^n)$, so $bx^n = 0$. Thus $a = 0$. Since (0) is irreducible by hypothesis, and $(y) \neq 0$, we have $x^n = 0$, so (0) is primary. □

Therefore, every (proper) ideal of a noetherian ring has a primary decomposition. In particular, the ideal (0) has a minimal primary decomposition, say $(0) = \bigcap_{i=1}^n \mathfrak{q}_i$. Denote $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$. We claim that the set of zero divisors D of A is the union $\bigcup_{i=1}^n \mathfrak{p}_i$.

Suppose $x \in D$. Then, $xy = 0$ for some nonzero $y \in A$. Thus, $xy = 0 \in (0) = \bigcap_{i=1}^n \mathfrak{q}_i$, which implies $xy \in \mathfrak{q}_i$ for all i. By primary-ness, either $x \in \sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$ or $y \in \mathfrak{q}_i$. If x is not in $\mathfrak{p}_i$ for all i, then $y \in \mathfrak{q}_i$ for all i, thus $y \in \bigcap_{i=1}^n \mathfrak{q}_i = (0)$ so $y = 0$. This contradicts our assumption that $y \neq 0$. Therefore, x must be in at least one $\mathfrak{p}_i$, which implies $D \subset \bigcup_{i=1}^n \mathfrak{p}_i$.

Conversely, suppose $x \in \bigcup_{i=1}^n \mathfrak{p}_i$. WLOG, suppose $x \in \mathfrak{p}_1$. Since we assumed the decomposition is minimal, we must have $(0) \neq \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$, so there exists some nonzero $y \in \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$. Suppose $x^k \in \mathfrak{q}_1$. Since $x^k y \in \bigcap_{i=1}^n \mathfrak{q}_i$, it follows that $x^k y = 0$. Suppose k is the minimal k such that $x^k \in \mathfrak{q}_1$, i.e. $x^k y = 0$. If $k = 1$, then $x \in D$. If $k > 1$, then $x \cdot x^{k-1} y = 0$, and by minimality $x^{k-1} y \neq 0$, so $x \in D$. Thus $\bigcup_{i=1}^n \mathfrak{p}_i \subset D$, proving our desired result.

Therefore, $D = \bigcup_{i=1}^n \mathfrak{p}_i$, and every prime ideal $\mathfrak{p}$ contained in D is contained in some $\mathfrak{p}_i$ by prime avoidance. Since prime ideals of $Q(A)$ are of the form $S(A)^{-1}\mathfrak{p}$ for primes $\mathfrak{p}$ of A contained in D, it follows that every prime ideal of $Q(A)$ is contained in one of the $S(A)^{-1}\mathfrak{p}_i$, so the $S(A)^{-1}\mathfrak{p}_i$ are the only possible maximal prime ideals of $Q(A)$. (Note that not all $S(A)^{-1}\mathfrak{p}_i$ may be maximal.) Since maximal ideals are automatically prime, it follows that the maximal primes coincide with the maximal ideals. Hence there are finitely many (at most n) of them. □

Problem 6. *Give an example of a noetherian ring A and an ideal $I \subset A$ s.t. $\sqrt{I}$ is prime but I is not primary.*

Proof. Let $A = k[x, y]$ and $I = (x^2, xy)$ for k a field, as in Problem 7. A is noetherian by Hilbert's basis theorem. Then $\sqrt{I} = (x, xy) = (x)$, which is prime since x is obviously irreducible, and $k[x, y]$ is a UFD. But I itself is not primary since $xy \in I$, and $x \notin I$ but $y^n \notin I$ for all n. □

Problem 7. *Let $A = k[x, y]$ and $I = (x^2, xy) \subset A$.*

1. *Show (x^2, xy, y^2) and (x^2, y) are (x, y)-primary.*
2. *Prove $I = (x) \cap (x^2, xy, y^2)$ and $I = (x) \cap (x^2, y)$ are minimal primary decompositions of I.*

In particular, minimal primary decompositions need not be unique.

Proof. 1. We will use the following lemma:

Lemma. If $\sqrt{I}$ is maximal then I is ($\sqrt{I}$-)primary.

Proof. Let $\sqrt{I} = \mathfrak{m}$. The image of $\mathfrak{m}$ in A/I is the nilradical, which is the intersection of all prime ideals of A/I. But primes of A/I correspond to primes of A containing I, which automatically contain $\sqrt{I} = \mathfrak{m}$. Thus the image of $\mathfrak{m}$ in A/I is the only prime ideal $\mathfrak{p}$ of A/I. Suppose a is not in the unique prime ideal, i.e. is not nilpotent. Then since the quotient ring by this prime is a field, $a + \mathfrak{p}$ has an inverse, say $b + \mathfrak{p}$ s.t. $ab + \mathfrak{p} = 1 + \mathfrak{p}$, so $ab - 1 =: n$ is nilpotent. Since $ab = 1 + n$, a unit plus a nilpotent, ab is a unit. Therefore there exists some $c \in A$ such that $abc = 1 = a(bc)$, so a is a unit. Thus every element of A/I is either a unit or a nilpotent, so every zero divisor in A/I is not a unit, hence is a nilpotent. Hence I is primary. □

Using the lemma above, we show $\sqrt{I}$ is maximal. Since $x^2 \in (x^2, xy, y^2)$, x is in the radical. Same for y. Therefore $(x, y) \subset \sqrt{(x^2, xy, y^2)}$, but since the radical is a proper ideal we conclude that the radical must equal to (x, y), since (x, y) is maximal. To see this, check $k[x, y]/(x, y) \cong k$. Thus (x^2, xy, y^2) is (x, y)-primary.

Also, x and y are in the radical of (x^2, y), so $(x, y) = \sqrt{(x^2, y)}$ which implies (x^2, y) is (x, y)-primary. □

Proof. 2. First, we must check the identities actually hold. Since $(x) \cap (x^2, xy, y^2) = (x^2, xy, xy^2) = (x^2, xy)$, and $(x) \cap (x^2, y) = (x^2, xy)$, both equalities are valid.

Above we have checked that (x), (x^2, xy, y^2) and (x^2, y) are primary ideals, so both are indeed primary decompositions. To check minimality, we have to show the radicals are distinct prime ideals, and no primary ideal contains another.

Since $\sqrt{(x)} = (x)$, $\sqrt{(x^2, xy, y^2)} = (x, y)$, these are distinct. Also, $(x) \nsubseteq (x^2, xy, y^2)$ since $x \notin (x^2, xy, y^2)$. Conversely, $(x^2, xy, y^2) \nsubseteq (x)$ since $y^2 \notin (x)$.

Also, $\sqrt{(x)} = (x)$ and $\sqrt{(x^2, y)} = (x, y)$, and $(x) \nsubseteq (x^2, y)$ since $x \notin (x^2, y)$ and $(x^2, y) \nsubseteq (x)$ since $y \notin (x)$. As we can see, primary decompositions, even though minimal, may not be unique.

(In the sense of the lecture notes, the primary decompositions are minimal since I itself is not primary, and there are two primary ideals in each.) □

Problem 8. *Define* $\dim A = \dim \operatorname{Spec} A$*, the RHS being Krull dimension of a topological space. Is being of finite dimension a local property?*

Proof. We cite the example of Nagata: Let $A = k[x_1, x_2, \ldots]$ the polynomial ring over a field k with countably many indeterminates. Let $m_1, m_2, \ldots$ be an increasing sequence of positive integers such that $m_{i+1} - m_i > m_i - m_{i-1}$ for all $i > 1$. Let $\mathfrak{p}_i = (x_{m_i+1}, \ldots, x_{m_{i+1}})$ and let $S = A - \bigcup_i \mathfrak{p}_i$. This S is multiplicatively closed. Since each $S^{-1}\mathfrak{p}_i$ has height $m_{i+1} - m_i$, it follows that $\dim S^{-1}A = \infty$. It is known that this ring is noetherian; then since localization of noetherian rings are noetherian, and noetherian local rings have finite Krull dimension, this example serves as an example of an infinite dimensional ring, whose local rings are all finite dimensional. □