Algebra 557: Weeks 3 and 4

1 Expansion and Contraction of Ideals, Primary ideals.

Suppose $f: A \to B$ is a ring homomorphism and $I \subset A$, $J \subset B$ are ideals. Then A can be thought of as a subring of B. We denote by I^e (expansion of I) the ideal $IB = f(I)B$ of B, and by J^c (contraction of J) the ideal $J \cap A = f^{-1}(J) \subset A$. The following are easy to verify:

$$\begin{aligned} I &\subset I^{ec}, \\ J^{ce} &\subset J, \\ I^{ece} &= I^e, \\ J^{cec} &= J^c. \end{aligned}$$

Since a subring of an integral domain is also an integral domain, and for any prime ideal $\mathfrak{p} \subset B$, $A/\mathfrak{p}^c$ can be seen as a subring of $B/\mathfrak{p}$ we have that

Theorem 1. *The contraction of a prime ideal is a prime ideal.*

Remark 2. The expansion of a prime ideal need not be prime. For example, consider the extension $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-1}]$. Then, the expansion of the prime ideal (5) is not prime in $\mathbb{Z}[\sqrt{-1}]$, since 5 factors as $(2+i)(2-i)$ in $\mathbb{Z}[\sqrt{-1}]$.

Definition 3. *An ideal $P \subset A$ is called primary if its satisfies the property that for all $x, y \in A$, $xy \in P, x \notin P$, implies that $y^n \in P$, for some $n \geq 0$.*

Remark 4. An ideal $P \subset A$ is primary if and only if all zero divisors of the ring A/P are nilpotent. Since thsi propert is stable under passing to sub-rings we have as before that the contraction of a primary ideal remains primary. Moreover, it is immediate that

Theorem 5. *If $P \subset A$ is a primary ideal, then $\sqrt{P}$ is a prime ideal.*

2 Spectrum of a ring A and the Zariski topology.

Definition 6. *The spectrum of A (denoted $\operatorname{Spec} A$) is the set of prime ideals of A. It is endowed with a topology (the Zariski topology) in which the closed sets are $V(I) = \{\mathfrak{p} \in \operatorname{Spec} A \mid I \subset \mathfrak{p}\}$ for some ideal $I \subset A$. The max-spectrum (denoted $\operatorname{mSpec} A$) of A is the set of maximal ideals of A.*

Lemma 7. *We have that*

$$\bigcap_{j \in J} V(I_j) = V(\sum_{j \in J} I_j),$$

and

$$V(I) \cup V(J) = V(I \cap J).$$

Definition 8. *A closed subset of X is called irreducible if it cannot be written as the union of two strictly smaller closed subsets.*

Theorem 9. *Any irreducible closed subset of* $\operatorname{Spec} A$ *is of the form* $V(\mathfrak{p})$ *for some* $\mathfrak{p} \in \operatorname{Spec} A$.

Proof. Let $\mathfrak{p} \in \operatorname{Spec} A$ and suppose that $V(\mathfrak{p}) = V(I) \cup V(J)$ with $V(I) \subsetneq V(\mathfrak{p})$ and $V(J) \subsetneq V(\mathfrak{p})$. Since $\mathfrak{p} \in V(\mathfrak{p})$ we have that $\mathfrak{p}$ is in one of $V(I)$ or $V(J)$ (say $V(I)$). Then, $\mathfrak{p} \supset I$ which implies that $V(I) \supset V(\mathfrak{p})$ which implies that $V(I) = V(\mathfrak{p})$.

Conversely, suppose that $V(I)$ is irreducible. Let Σ be the set of minimal prime ideals containing I. Then clearly

$$V(I) = \bigcup_{\mathfrak{p} \in \Sigma} V(\mathfrak{p}).$$

Since $V(I)$ is irreducible we must have that $V(I) = V(\mathfrak{p})$ for some $\mathfrak{p} \in \Sigma$. □

Definition 10. *A topological space X is said to be Noetherian if its closed sets satisfy the d.c.c.*

Theorem 11. *If the ring A is Noetherian then* $\operatorname{Spec} A$ *is a Noetherian topological space.*

Proof. Clear. □

3 Localization

Recall from Week 1 the definition of a multiplicative subset. Let $S \subset A$ be a multiplicative subset. The localization of the ring A at S (denoted A_S or $S^{-1}A$) is defined by the following universal property.

Definition 12. *There is a ring homomorphism $f: A \rightarrow A_S$ having the property that for each $s \in S$, $f(S)$ is invertible; and for any ring homomorphism $g: A \rightarrow B$ such that $g(s)$ is invertible for each $s \in S$, there exists a unique homomorphism h: $A_S \rightarrow B$ with $g = h \circ f$.*

We show that the localization exists by constructing it as follows:

Definition 13. *For any (a, s), $(b, s') \in A \times S$, we define $(a, s) \sim (b, s')$ if there exists $t \in S$, such that $t(a s' - b s) = 0$. We define A_S to be $A \times S / \sim$ (with sums and products defined in the obvious way thinking of the equivalence class of the pair (a, s) as a fraction $\frac{a}{s}$).*

Notation 14. *If $\mathfrak{p} \subset A$ is a prime ideal, then $A - \mathfrak{p}$ is a multiplicative subset, and we denote by $A_{\mathfrak{p}}$ the ring $A_{A-\mathfrak{p}}$.*

Some important properties of localization.

Theorem 15. *Every ideal of A_S is of the form IA_S, where I is an ideal of A. The prime ideals of A_S are of the form $\mathfrak{p} A_S$ where $\mathfrak{p}$ is a prime ideal of A with $\mathfrak{p} \cap S = \emptyset$. Conversely, if $\mathfrak{p}$ is a prime ideal of A disjoint from S, then $\mathfrak{p} A_S$ is a prime ideal of A_S. The same holds for primary ideals.*

Proof. Let $J \subset A_S$ be an ideal and let $I = J \cap A = J^c$. If $\frac{a}{s} \in J$, then $\frac{s}{1} \cdot \frac{a}{s} = \frac{a}{1}$ is also in J. Hence, clearly $J = IA_S$.

Now suppose that that $\mathfrak{p} \subset A$ is a prime ideal disjoint from S. Then, $\mathfrak{p} A_{\mathfrak{p}} \cap A = \mathfrak{p}$ as above. Now suppose that $\frac{a}{s}\frac{b}{t} \in \mathfrak{p} A_S$, and $\frac{a}{s} \notin \mathfrak{p} A_S$. Then, we have that $ab \in \mathfrak{p}$, $a \notin \mathfrak{p}$, implying that $b \in \mathfrak{p}$, and thus $\frac{b}{t} \in \mathfrak{p}$. Moreover, since $\mathfrak{p} \cap S = \emptyset$, we have that $1 \notin \mathfrak{p} A_S$. Hence, $\mathfrak{p} A_S$ is a prime ideal. Conversely, if $P \subset A_S$ is a prime ideal then, $\mathfrak{p} = P^c = P \cap A$ is prime (since the contraction of a prime ideal is always prime). Moreover, since $S \cap P = \emptyset$, we have that $\mathfrak{p} \cap S = \emptyset$, and $P = \mathfrak{p} A_S$. □

In particular, if $\mathfrak{p} \subset A$ is a prime ideal we have

Theorem 16. *$A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p} A_{\mathfrak{p}}$.*

Proof. The prime ideals of $A_{\mathfrak{p}}$ are in bijection with the prime ideals of A disjoint from the multiplicative subset $A - \mathfrak{p}$ (that is those prime ideals of A contained in $\mathfrak{p}$). This also shows that the ideal $\mathfrak{p} A_{\mathfrak{p}}$ is maximal and is the only maximal ideal in $A_{\mathfrak{p}}$. □

Notation 17. *The residue field, $A_{\mathfrak{p}} / \mathfrak{p} A_{\mathfrak{p}}$, will be denoted by $\kappa(\mathfrak{p})$.*

Corollary 18. *If A is Noetherian (resp. Artinian) so is A_S.*

Localization commutes with taking quotients. More precisely,

Theorem 19. *If $I \subset A$ is an ideal and S a multiplicatively closed subset of A, then*

$$A_S / IA_S \cong (A/I)_{\bar{S}},$$

where $\bar{S}$ is the image of S under the canonical homomorphism.

Definition 20. *If M is an A-module and S a multiplicatively closed subset, we define M_S to be the A_S-module in a natural way. M_S consists of equivalence classes of pairs $\frac{m}{s}$, $m \in M$, $s \in S$, where $\frac{m}{s} \sim \frac{m'}{s'}$ if there exists $t \in S$, such that $t(s'm - sm') = 0$ in M. If $\mathfrak{p} \subset A$ is a prime ideal, we denote by $M_{\mathfrak{p}}$ the $A_{\mathfrak{p}}$-module $M_{A-\mathfrak{p}}$. The support of M, denoted* $\mathrm{Supp}(M)$, *is the set $\{\mathfrak{p} \in \operatorname{Spec} A \mid M_{\mathfrak{p}} \neq 0\}$.*

Theorem 21. *If M is f.g. then* $\operatorname{Supp}(M) = V(\operatorname{ann}(M))$*. In particular,* $\operatorname{Supp}(M)$ *is a closed subset of* $\operatorname{Spec} A$*.*

Proof. Let $M = A\omega_1 + \cdots + A\omega_n$. Then for $\mathfrak{p} \in \operatorname{Spec} A$, if $M_{\mathfrak{p}} \neq 0$, then there exists i, such that $\omega_i \neq 0$ in $M_{\mathfrak{p}}$, which is the same as saying that $\operatorname{ann}(\omega_i) \subset \mathfrak{p}$ (since the invertible elements in $A_{\mathfrak{p}} \cap A$ are precisely $A - \mathfrak{p}$. Thus,

$$\operatorname{ann}(M) = \bigcap_{1 \leq i \leq n} \operatorname{ann}(\omega_i) \subset \mathfrak{p}.$$

Conversely, if the above holds then

$$\prod_{1 \leq i \leq n} \operatorname{ann}(\omega_i) \subset \bigcap_{1 \leq i \leq n} \operatorname{ann}(\omega_i) \subset \mathfrak{p},$$

implying that $\operatorname{ann}(\omega_i) \subset \mathfrak{p}$ for some i since $\mathfrak{p}$ is prime, and hence $M_{\mathfrak{p}} \neq 0$. Hence, $M_{\mathfrak{p}} \neq 0$ if and only if $\operatorname{ann}(M) \subset \mathfrak{p}$, and thus the support of M is the closed subset $V(\operatorname{ann}(M))$ of $\operatorname{Spec} A$. □

We also have the following local-to-global principle.

Theorem 22. *Let M be an A-module. Then $M = 0$ if and only if $M_{\mathfrak{p}} = 0$* for each *$\mathfrak{p} \in \operatorname{mSpec} A$.*

Proof. One direction is clear. In the other direction suppose that $M_{\mathfrak{p}} = 0$ for each maximal ideal $\mathfrak{p}$ of A. Then for $m \in M$, $\operatorname{ann}(m) \not\subset \mathfrak{p}$ for each maximal ideal $\mathfrak{p}$. But if $m \neq 0$, then $1 \notin \operatorname{ann}(m)$, and thus there must exist a maximal ideal containing $\operatorname{ann}(m)$. Thus, $m = 0$ and hence $M = 0$. □

4 Dimension and heights

Definition 23. *For a topological space X we let* $\dim X$ *denote the maximum length of a strictly ascending or descending sequence of irreducible closed subspaces.*

Definition 24. *We define the (Krull dimension) of A to be the length of the longest increasing sequence of prime ideals of A.*

Remark 25. Notice that $\dim A$ coincides with the combinatorial dimension of $\operatorname{Spec} A$.

Definition 26. *For a prime ideal $\mathfrak{p}$ we denote by* $\operatorname{ht} \mathfrak{p}$ *the supremum the lengths of all strictly descending sequence of prime ideals starting at $\mathfrak{p}$. In other words*

$$\operatorname{ht} \mathfrak{p} = \sup \{ r \mid \exists \mathfrak{p}_0 = \mathfrak{p} \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_r \}.$$

Definition 27. *For a prime ideal $\mathfrak{p}$ we denote by* $\operatorname{coht} \mathfrak{p}$ *the supremum the lengths of all strictly ascending sequence of prime ideals starting at $\mathfrak{p}$. In other words*

$$\operatorname{coht} \mathfrak{p} = \sup \{ r \mid \exists \mathfrak{p}_0 = \mathfrak{p} \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r \}.$$

It is easy to verify the following:

$$\operatorname{ht}\mathfrak{p} = \dim A_{\mathfrak{p}}$$

$$\operatorname{coht}\mathfrak{p} = \dim A/\mathfrak{p}$$

$$\operatorname{ht}\mathfrak{p} + \operatorname{coht}\mathfrak{p} \le \dim A$$

5 Nullstellensatz and dimension of affine rings

Theorem 28. *Let k be a field and $A = k[\alpha_1, \ldots, \alpha_n]$. If A is algebraic over k, then*

1. *$k[\alpha_1, \ldots, \alpha_n]$ is a field, and*
2. *there exists $f_i \in k[X_1, \ldots, X_i]$ such that $A = k[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$.*

Proof. Let L be an algebraic extension of k containing α_1, ..., α_n. Let ϕ_1: $k[X_1] \longrightarrow k[\alpha_1]$ be the surjective homomorphism sending X to α_1, and let $f_1 \in k[X_1]$ be a monic polynomials which generates ker ϕ_1. Then f_1 is irreducible and hence (f_1) is prime and hence maximal and thus $k[\alpha_1] \cong k[X_1]/(f_1)$ is a field. Continuing we obtain $f_2 \in k[X_1, X_2]$ such that $f_2(\alpha_1, X_2)$ is monic and generates $\ker \phi_2$ and so on. Let ϕ: $k[X_1, \ldots, X_n] \longrightarrow A$ be the surjective homomorphism sending each $X_i \longmapsto \alpha_i$, and let $P \in \ker \phi$. Treating P as a polynomial in X_n, and dividing by the polynomial f_n (which is *monic* in X_n) we obtain $P = Q_n\, f_n + R_{n-1}$, where $R_{n-1} \in k[X_1, \ldots, X_n]$ and $R_{n-1}(\alpha_1, \ldots, \alpha_{n-1}, X_n) = 0$. Now treating R_{n-1} as a polynomial in X_{n-1} and dividing by f_{n-1} we obtain $R_{n-1} = Q_{n-1}\, f_{n-1} + R_{n-2}$ with $R_{n-2}(\alpha_1, \ldots, \alpha_{n-2}, X_{n-1}, X_n) = 0$ (since f_{n-1} divides any polynomial in $k(\alpha_1, \ldots, \alpha_{n-2}, X_n)[X_{n-1}]$ which vanishes at α_{n-1}). Continuing this ay we finally obtain that $P \in (f_1, \ldots, f_n)$. Since its clear that $f_1, \ldots, f_n \in \ker \phi$ we obtain that $\ker \phi = (f_1, \ldots, f_n)$. ☐

Theorem 29. *Let k be a field and $A = k[\alpha_1, \ldots, \alpha_n]$ an integral domain. If* $\operatorname{tr.deg}_k A > 0$ *then A is not a field.*

Proof. Suppose that $\operatorname{tr.deg}_k A = r > 0$. Without loss of generality let $\alpha_1, \ldots, \alpha_r$ be a transcendence basis of A over k. Then, α_{r+1}, ..., α_n are algebraic over $K = k(\alpha_1, \ldots, \alpha_r)$ and by previous theorem there exists $f_{r+1}, \ldots, f_n \in K[X_{r+1}, \ldots, X_n]$ such that $K[\alpha_{r+1}, \ldots, \alpha_n] \cong K[X_{r+1}, \ldots, X_n]/(f_{r+1}, \ldots, f_n)$ and each $f_{r+i} \in K[X_{r+1}, \ldots, X_{r+i}]$ and monic in X_{r+i} of degree d_{r+i} (say). Since the finite number coefficients of the various f_{r+i} are in $k(\alpha_1, \ldots, \alpha_r)$ there exists $g \in k[\alpha_1, \ldots, \alpha_r]$ such that $f_{r+1}, \ldots, f_n \in k[\alpha_1, \ldots, \alpha_r, \frac{1}{g}] = B$. Now the fraction field of A is a K-vector space of dimension $d_{r+1} \cdots d_n$. From this it follows that the set of elements $\mathcal{B} = \{\alpha_{r+1}^{e_{r+1}} \cdots \alpha_n^{e_n} \mid 0 \le e_{r+1} < d_{r+1}, \ldots, 0 \le e_n < d_n\} \subset A$, form a basis of $A[\frac{1}{g}]$ as a *free* B-module. It is easy to see that B admits non-zero proper ideals. Hence, so does $A[\frac{1}{g}]$. Thus, $A[\frac{1}{g}]$ is not a field, implying that A is not a field. ☐

Theorem 30. *(Nullstellensatz) If k is a field, and $\mathfrak{m}$ a maximal ideal of $A = k[X_1, \ldots, X_n]$, then $A/\mathfrak{m}$ is algebraic over k.*

Corollary 31. *If an ideal $I \subset k[X_1, \ldots, X_n]$ has no common zero in $\bar{k}^n$, then $1 \in I$.*

6 Associated Primes and Primary Decomposition

Definition 32. *Let M be an A-module. The associated primes of M is defined by*

$$\mathrm{Ass}(M) = \{\mathfrak{p} \in \mathrm{Spec}\, A \mid \exists x \in M, x \neq 0, \text{ with } \mathfrak{p} = \mathrm{ann}(x)\}.$$

Remark 33. It is easy to see that $\mathfrak{p} \in \mathrm{Ass}(M)$ if and only if M has a submodule isomorphic to $A/\mathfrak{p}$ (namely the submodules Ax with $\mathfrak{p} = \mathrm{ann}(x)$).

Proposition 34. *Let $(M_i)_{i \in I}$ be a family of submodules of M with $M = \cup_{i \in I} M_i$. Then*

$$\mathrm{Ass}(M) = \bigcup_{i \in I} \mathrm{Ass}(M_i).$$

Proof. Clear. □

Proposition 35. *For every $\mathfrak{p} \in \mathrm{Spec}\, A$, and submodules M of $A/\mathfrak{p}, M \neq 0$,*

$$\mathrm{Ass}(M) = \{\mathfrak{p}\}.$$

Proof. Clear. □

Proposition 36. *Maximal elements of the set of ideals $(\mathrm{ann}(x))_{x \in M, x \neq 0}$ belong to $\mathrm{Ass}(M)$.*

Proof. It suffices to prove that if $\mathrm{ann}(x)$ is a maximal element then it is a prime ideal. Suppose that $a \notin \mathrm{ann}(x)$, $ab \in \mathrm{ann}(x)$. We have that $a \in \mathrm{ann}(bx) \supset \mathrm{ann}(x)$. But this contradicts the maximality of $\mathrm{ann}(x)$ unless $bx = 0$. Hence, $b \in \mathrm{ann}(x)$ proving that $\mathrm{ann}(x)$ is prime. □

Corollary 37. *If A is Noetherian and M an A-module with $M \neq 0$, then $\mathrm{Ass}(M) \neq 0$.*

Proof. If $x \in M, x \neq 0$ then $\mathrm{ann}(x) \neq A$. This shows that the set $(\mathrm{ann}(x))_{x \in M, x \neq 0}$ is not empty and by the maximal property of Noetherian rings there exists a maximal element in the set. Now apply previous proposition. □

Corollary 38. *If A is Noetherian and M an A-module, then for any $a \in A$ the homothety by a on M is injective if and only if $a \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Ass}(M)$.*

Proof. One direction is clear. In the other direction suppose that $a \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Ass}(M)$. If $ax = 0$ with $x \neq 0$, then $a \in \mathrm{ann}(x)$. Consider the submodule $Ax \subset M$. Then there exists $\mathfrak{p} \in \mathrm{Ass}(Ax)$. Then $\mathfrak{p} = \mathrm{ann}(bx)$. But then $a \in \mathrm{ann}(x) \subset \mathrm{ann}(bx) = \mathfrak{p}$. □

Corollary 39. *The set of divisors of zero in a Noetherian ring is the union of its associated primes.*

Proof. Clear from the above as the homothety by $0 \neq a \in A$ is an injection if and only if a is not a divisor of zero. □

Proposition 40. *Let M be an A-module and $N \subset M$ a sub-module. Then*

$$\mathrm{Ass}(N) \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N).$$

Proof. The first inclusion is clear. Now suppose $\mathfrak{p} \in \mathrm{Ass}(M)$. Then M contains a submodule E isomorphic to $A/\mathfrak{p}$. Let $F = E \cap N$. If $F \neq 0$, then by Proposition 35 we have that $\mathfrak{p} \in \mathrm{Ass}(F) \subset \mathrm{Ass}(N)$. Otherwise, $F = 0$ and E descends to an isomorphic submodule of M/N, and we have that $\mathfrak{p} \in \mathrm{Ass}\, M/N)$. □

Corollary 41. *If M is the direct sum of the family $(M_i)_{i \in I}$ then*

$$\mathrm{Ass}(M) = \bigcup_{i \in I} \mathrm{Ass}(M_i).$$

Proof. Firstly it can be reduced to the case when I is finite using Proposition 34, since M is the union of the direct sums of the finite subsets of the family $(M_i)_{i \in I}$. Now apply induction and the previous proposition. □

Proposition 42. *Let M be an A-module and Φ a subset of* $\mathrm{Ass}(M)$*. Then there exists a sub-module $N \subset M$, such that* $\mathrm{Ass}(N) = \mathrm{Ass}(M) - \Phi$*, and* $\mathrm{Ass}(M/N) = \Phi$*.*

Proof. Let $\mathfrak{C}$ be the set of sub-modules P of M such that $\mathrm{Ass}(P) \subset \mathrm{Ass}(M) - \Phi$. Then $\mathfrak{C}$ is not empty since $\mathrm{Ass}(0) = \emptyset \subset \mathrm{Ass}(M) - \Phi$, and $\mathfrak{C}$ is inductively ordered by inclusion. Let N be a maximal element of $\mathfrak{C}$. We now prove that $\mathrm{Ass}(M/N) \subset \Phi$, which will imply the proposition (using Proposition 40). Suppose $\mathfrak{p} \in \mathrm{Ass}(M/N)$. Then M/N contains a submodule F/N isomorphic to A/$\mathfrak{p}$. Then, $\mathrm{Ass}(F) \subset \mathrm{Ass}(N) \cup \{\mathfrak{p}\}$. By maximality of N, $\mathfrak{p} \notin \mathrm{Ass}(M) - \Phi$ and $\mathfrak{p} \in \mathrm{Ass}(F) \subset \mathrm{Ass}(M)$. Thus, $\mathfrak{p} \in \Phi$, and $\mathrm{Ass}(M/N) \subset \Phi$. □

Remark 43. Notice that no Noetherian assumption was needed in the previous proposition.