Math 210B: Homework 3 Solutions

Recall that if $\mathfrak{a}$ is an ideal of A the *radical* of $\mathfrak{a}$ is

$$r(\mathfrak{a}) = \{f \in A | f^n \in \mathfrak{a} \text{ for some } n > 0\}.$$

This is an ideal containing $\mathfrak{a}$, and it is easy to see that $r(r(\mathfrak{a})) = r(\mathfrak{a})$. The ideal $\mathfrak{a}$ is called *radical* if $\mathfrak{a} = r(\mathfrak{a})$.

Let k be a field, which we assume to be algebraically closed. Let $\mathbb{A}^n(k)$ be *affine n-space* k^n. If S is a subset of the polynomial ring $k[X] = k[X_1, \cdots, X_n]$ then

$$V(S) = \{a = (a_1, \cdots, a_n) \in \mathbb{A}^n(k) | f(a) = 0 \text{ for all } f \in S\}.$$

If $\mathfrak{a}$ is the ideal generated by S and $r(\mathfrak{a})$ is the radical of $\mathfrak{a}$ then $V(S) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$. Also if X is a subset of $\mathbb{A}^n(k)$ let

$$I(X) = \{f \in k[X] | f(a) = 0 \text{ for all } a \in \mathfrak{a}\}.$$

It is an ideal. By the Nullstellensatz $I(V(\mathfrak{a})) = r(\mathfrak{a})$.

The sets $V(S)$ are called *algebraic sets* and last week you proved they form the closed sets in a topology, called the *Zariski topology* on $\mathbb{A}^n(k)$. The essential content of the Nullstellensatz is that $\mathfrak{a} \mapsto V(\mathfrak{a})$ is a bijection between radical ideals and Zariski closed sets.

A closed (i.e. algebraic) subset X of $\mathbb{A}^n(k)$ is called *reducible* if there exist proper closed subsets Y, Z of X such that $X = Y \cup Z$. If it is not reducible it is called *irreducible*. I will call an irreducible closed set a *variety* though this terminology is not universally adopted: often a variety is not required to be irreducible.

Problem 1. Prove that $V(\mathfrak{a})$ is irreducible if and only if $r(\mathfrak{a})$ is prime.

Solution. Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are radical ideals. Then it is clear from the defintions that if $\mathfrak{a} \subseteq \mathfrak{b}$ then $V(\mathfrak{a}) \supseteq V(\mathfrak{b})$. We also note that if $V(\mathfrak{a}) = V(\mathfrak{b})$ then $\mathfrak{a} = \mathfrak{b}$. This is because by the Nullstellensatz $I(V(\mathfrak{a})) = r(\mathfrak{a}) = \mathfrak{a}$ and similarly $I(V(\mathfrak{b})) = \mathfrak{b}$.

Suppose X is reducible, so $X = Y \cup Z$ with Y, Z proper subsets of X. Let $\mathfrak{b} = I(Y)$ and $\mathfrak{c} = I(Z)$. By the above discussion $\mathfrak{a}$ is a strictly proper subideal of $\mathfrak{b}$ and similarly of $\mathfrak{c}$. So let $f \in \mathfrak{b} \backslash \mathfrak{a}$ and $g \in \mathfrak{c} \backslash \mathfrak{a}$. Then f vanishes on Y while g vanishes on Z so fg vanishes on X, that is $fg \in \mathfrak{a}$. This shows that $\mathfrak{a}$ is not a prime ideal.

Conversely if $\mathfrak{a}$ is not prime let $f, g \notin \mathfrak{a}$ such that $fg \in \mathfrak{a}$. Then consider $\mathfrak{b} = \mathfrak{a} + (f)$ and $c = \mathfrak{a} + (g)$. Then $Y = V(\mathfrak{b})$ and $Z = V(\mathfrak{c})$ are strictly smaller Zariski closed subsets of X. But $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}$ so $X \subseteq Y \cup Z$. The other inclusion is also clear so $X = Y \cup Z$ and thus X is reducible.

Problem 2. (a) Let $A \subset F$ where F is a field, and let B be the integral closure of A in F. Let $S \subseteq A$ be a multiplicative set. Show that $S^{-1}B$ is the integral closure of $S^{-1}A$ in F.

(b) Let A be an integral domain. We recall that we say A is *integrally closed* if it is integrally closed in its field of fractions F. Show that A is integrally closed if and only if $A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$ of A.

Hint for (b): Let C be the integral closure of A in F. Let $x \in C$. Suppose that $x \notin A$. Let $\mathfrak{a} = \{f \in A | fx \in A\}$. Let $\mathfrak{m}$ be a maximal ideal of A containing $\mathfrak{a}$. Then ...

Solution. (a) Since $S^{-1}B$ is generated by $S^{-1}A$ and B it is integral over $S^{-1}A$. Conversely, suppose that $x \in F$ is integral over $S^{-1}A$. This means that we have a relation

$$x^n + \frac{a_{n-1}}{s_{n-1}} x^{n-1} + \cdots + \frac{a_0}{s_0} = 0.$$

Let $t = s_0 \cdots s_{n-1}$. Then

$$(tx)^n + \left(\frac{a_{n-1}t}{s_{n-1}} \right) (tx)^{n-1} + \cdots + \frac{a_0 t^n}{s_0} = 0.$$

The coefficients here are in A, so tx is integral over A, that is, $tx \in B$. Thus $x \in S^{-1}B$. We have shown that $S^{-1}B$ consists of precisely the elements of F that are integral over A.

(b) It follows from (a) that if A is integrally closed then so is $A_{\mathfrak{m}}$. For the converse, assume that $A_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m}$. Let C be the integral closure of A in F; we want to show that $C = A$. If not, let $x \in C\backslash A$. Let $\mathfrak{a} = \{f \in A | fx \in A\}$. Then this is a proper ideal of A. Let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{a}$. Then x is integral over A, *a fortiori* over $A_{\mathfrak{m}}$. Since $A_{\mathfrak{m}}$ is integrally closed, $x \in A_{\mathfrak{m}}$ and we may thus write $x = y/s$ where $y \in A$ and $s \in A - \mathfrak{m}$. But then $sx \in A$, so $s \in \mathfrak{a}$. This is a contradiction since $s \notin \mathfrak{m}$.

We recall the *Extension Theorem for valuations* that was proved in Week 2. If F is a field, a *valuation ring of* F is a subring R such that if $x \in F$ then either $x \in R$ or $x^{-1} \in R$. A valuation ring is R a local ring. Its maximal ideal $\mathfrak{p}$ may be characterized as $\{x \in R | x^{-1} \notin R\}$ since in a local ring, the nonunits comprise the unique maximal ideal.

Theorem 1. *Let F be a field and A a subring of F. Let $\phi : A \longrightarrow \Omega$ be a homomorphism of A into an algebraically closed field Ω. Then ϕ may be extended to a homomorphism $\Phi : R \longrightarrow \Omega$ where R is a valuation ring of F.*

This is Corollary 3.3 in Section VII.3 of Lang's *Algebra*. It was also proved in class and used to prove the Nullstellensatz. Use it in the next Exercise.

Problem 3. Let F be a field and A a subring of F. Show that the integral closure of A in F is the intersection of all valuation rings of F containing A.

Hint: To prove that if $x \in F$ is not integral over A then there is a valuation ring R of F such that $x \notin R$, show that $x^{-1}A[x^{-1}]$ is contained in a maximal ideal of $A[x^{-1}]$, then find a way to use the Extension Theorem.

Solution. First suppose that $x \in A$ is integral over A; we show that x is in every valuation ring R of F containing A. Indeed, write

$$x^n + a_{n-1}x + \ldots + a_0, \qquad a_i \in A.$$

If $x \notin R$ then x^{-1} is in the maximal ideal $\mathfrak{p}$ of R so $1 = -a_{n-1}x^{-1} - \ldots - x^{-n} \in \mathfrak{p}$ which is a contradiction.

For the other direction (using the Hint) assume that x is *not* integral over A. We claim that x^{-1} generates a proper ideal of $A[x^{-1}]$. Indeed, if $1 \in x^{-1}A[x^{-1}]$ then we may write

$$1 = a_1 x^{-1} + \ldots + a_m x^{-m}$$

for some $a_i \in A$ and then $x^m - a_1 x^{m-1} - \ldots - a_m = 0$ contradicting our assumption that x is not integral.

Now let $\mathfrak{p}$ be a maximal ideal of $A[x^{-1}]$ containing $x^{-1}A[x^{-1}]$. Let Ω be the algebraic closure of $A[x^{-1}]/\mathfrak{p}$. We have a homomorphism of $\varphi : x^{-1}A[x^{-1}] \longrightarrow \Omega$ such that $x^{-1} \mapsto 0$. By the Extension Theorem we may extend this map to a valuation ring R. Since x^{-1} maps to 0, x is not in R.

Problem 4. Let F be a field and let R be the polynomial ring $F[X,Y]$ in two variables. Give examples of prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ such that the local ring $R_\mathfrak{p}$ is a valuation ring but the local ring $R_\mathfrak{q}$ is not.

Solution. Let $\mathfrak{p} = (X)$, the principal ideal generated by X. We may write any element f of F as $X^k\phi/\psi$ where $k \in \mathfrak{Z}$ and ϕ, ψ are polynomials not divisible by X. Then $f \in R_\mathfrak{p}$ if and only if $k \geqslant 0$. From this description it is clear that either $f \in R_\mathfrak{p}$ or $f^{-1} \in R_\mathfrak{p}$, so $R_\mathfrak{p}$ is a valuation ring.

On the other hand let $\mathfrak{q}$ be the maximal ideal generated by X and Y. Then neither X/Y nor Y/X is in $R_\mathfrak{q}$, so it is not a valuation ring.

Problem 5. Let A be an integrally closed integral domain. This means that it is integrally closed in its field of fractions K. Let L/K be a finite separable extension and let B be the integral closure of A in L. Suppose that A is Noetherian. Prove that B is a finitely-generated A-module and deduce that B is also Noetherian.

Hint: This is Problem 3 in the exercises to Chapter VII of Lang (page 353). See Lang for the hint.

Solution: Let $\omega_1, \cdots, \omega_n$ be a basis of L over K. Using Proposition VII.1.1 we may multiply ω_i be a constant c_i such that it is integral over A. Therefore without loss of generality we may assume $\omega_i \in A$.

Now we make use of the trace bilinear form $\beta(x,y) = \mathrm{tr}(xy)$ on L which is nondegenerate since E/F is separable; see Theorem VI.5.2 and its Corollary 5.3 on page 286 of Lang. Let ω_i' be the dual basis of L so $\mathrm{tr}(\omega_i\omega_j') = \delta_{ij}$.

We claim that $B \subseteq A\omega_1' \oplus \cdots \oplus A\omega_n'$. Indeed, if $b \in B$ we may write $b = \sum c_i\omega_i'$ with $c_i \in L$. Now $c_i = \mathrm{tr}(b\omega_i)$ which is in A since the trace map takes B into A by Corollary VII.1.6. Hence $b \in A\omega_1' \oplus \cdots \oplus A\omega_n'$. Thus B is a submodule of a finitely generated A-module. Since A is Noetherian, B is finitely generated Noetherian (as an A-module, *a fortiori* as a ring) by Propositions 1.4 and 1.2 of Lang, Chapter X.

A commutative ring R is called a *Dedekind domain* if it is integrally closed in its field of fractions, Noetherian and every nonzero prime ideal is maximal. For example a principal ideal domain is a Dedekind domain. The class of Dedekind domains is important because many important rings are Dedekind domains. For example the integral closure of $\mathbb{Z}$ in a finite extension E of $\mathbb{Q}$ is called the *ring of algebraic integers* in E and it is a Dedekind domain. The affine algebra (coordinate ring) of a nonsingular affine curve is a Dedekind domain.

The next exercise is part of Exercise VII.7 in Lang's *Algebra.* We'll return to this Exercise in Homework 4.

Problem 6. Let $\mathfrak{o}$ be a Dedekind domain. Let K be its field of fractions. Given a nonzero ideal $\mathfrak{a}$ of $\mathfrak{o}$ prove that there exists a product of maximal ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$.

Solution. Suppose there are ideals $\mathfrak{a}$ that do not contain products of nonzero prime ideals. Since $\mathfrak{o}$ is Noetherian, there is a maximal counterexample $\mathfrak{a}$. Clearly $\mathfrak{a}$ cannot be prime, so there exist elements x, y of $\mathfrak{o}$ such that $x, y \notin \mathfrak{a}$ and $xy \in \mathfrak{a}$. Now consider the ideals $(x) + \mathfrak{a}$ and $(y) + \mathfrak{a}$. These are strictly larger than $\mathfrak{a}$, so there exist primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ and $\mathfrak{p}'_1, \cdots, \mathfrak{p}'_s$ such that $(x) + \mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ and $(y) + \mathfrak{a} \supseteq \mathfrak{p}'_1 \cdots \mathfrak{p}'_s$. Now observe that

$$\mathfrak{a} \supseteq ((x) + \mathfrak{a})((y) + \mathfrak{a}) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}'_1 \cdots \mathfrak{p}'_s.$$

This is a contradiction.