All rings are assumed commutative in the below. Let A be a commutative ring. For any prime $\mathfrak{p} \subset A$, let $\kappa(\mathfrak{p})$ denote the field $K(A/\mathfrak{p}) = (A/\mathfrak{p})_{(0)} = A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$. A local ring is a ring with exactly one maximal ideal. The following lemma, stated in restricted form, is known as Nakayama's lemma, and is used below.

Lemma. *Let A be a local ring with maximal ideal $\mathfrak{m}$ and M a finitely-generated A-module. Then if $m_1, \ldots, m_n$ are elements of M whose images in $M \otimes \kappa(\mathfrak{m}) = M/\mathfrak{m}M$ generate it as a $\kappa(\mathfrak{m})$-vector space, then $m_1, \ldots, m_n$ generate M as an A-module.*

(1) Let A be a ring. Prove that a sequence of A-modules

$$0 \longrightarrow M \longrightarrow N \longrightarrow Q \longrightarrow 0 \qquad (*)$$

is exact if and only if the localized sequence

$$0 \longrightarrow M_\mathfrak{m} \longrightarrow N_\mathfrak{m} \longrightarrow Q_\mathfrak{m} \longrightarrow 0$$

is exact for every maximal ideal $\mathfrak{m} \subset A$ ($\Leftrightarrow$ for every prime ideal $\mathfrak{m}$).

Proof. One direction follows since localization is flat. The other direction follows from the following statements. (1) $M = 0$ iff $M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$. (2) A homomorphism $M \to N$ is a monomorphism (resp. epimorphism) iff $M_\mathfrak{m} \to N_\mathfrak{m}$ is for all maximal ideals $\mathfrak{m}$. (3) Arguing from the sequence (*), we see that from (1) it must be a complex. (2) gives us that the ends of the sequence are exact, so it suffices to see that the cohomology in the middle is zero; this is clear since the morphism $\operatorname{im}(M \to N) \to \ker(N \to Q)$ becomes an isomorphism at each $\mathfrak{m}$; now use flatness of localization and (2) to conclude.

The proof of (1) is as follows. Suppose $M \neq 0$. Then there exists an $x \in M$ such that $\operatorname{ann} x = \{f \in A : fx = 0\}$ is a proper ideal in A. By Zorn's lemma it is contained in a maximal ideal $\mathfrak{m}$. Then the map $M \to M_\mathfrak{m}$ does not annihilate x, hence $M_\mathfrak{m} \neq 0$.

The proof of (2) is as follows. $\Rightarrow$ is always true for epimorphisms since $- \otimes_A M$ is a right exact functor for any A-module M, and is true for monomorphisms in this case since localization is flat. $\Leftarrow$: $\alpha : M \to N$ is a monomorphism (resp. epimorphism) iff $\ker \alpha = 0$ (resp. $\operatorname{coker} \alpha = 0$). It is always true for any module L that $(\operatorname{coker} \alpha) \otimes_A L = \operatorname{coker}(\alpha \otimes_A 1_L)$, but the same statement is not true in general for ker unless M is flat. $A_\mathfrak{m}$ is a flat A-module, so we have $(\ker \alpha)_\mathfrak{m} = \ker(\alpha_\mathfrak{m})$ and $(\operatorname{coker} \alpha)_\mathfrak{m} = \operatorname{coker}(\alpha_\mathfrak{m})$; now apply (1) to conclude. □

(2) There is a tendency for ideals maximal with respect to a certain property to be prime. Case in point: prove that if $U \subset A$ is a multiplicatively closed subset, and $I \subset A$ is an ideal maximal among those not meeting U, then I is prime. Use this result to prove the formula

$$\{f \in A : f^n \in J \text{ for some } n\} =: \operatorname{rad} J = \bigcap_{J \subset \mathfrak{p}} \mathfrak{p}$$

for any ideal $J \subset A$, where the intersection is over all primes containing J.

Proof. For the first statement, if $f, g \in A$ are not in I, then by maximality of I, both $I + (f)$ and $I + (g)$ meet U. So there are elements of the form $af + i$ and $bg + j$ in U with i, j in I. If fg were in I¡ then the product of

$af + i$ and $bg + j$ would be in I, contradicting the fact tahtthat I doesn't meet U.

For the formula for the radical, the inclusion $\subset$ is clear. Conversely, if $f \notin \operatorname{rad} J$, then an ideal maximal among those containing J and disjoint from $\{f^n : n \geq 1\}$ is prime, so f is not contained in the right hand side. $\square$

(3) An A-module P is called projective if it satisfies any number of equivalent properties: it is a direct summand of a free module, or the functor $\operatorname{Hom}(P, -)$ is exact, or every short exact sequence of the form

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

splits. In particular if A is local noetherian, prove that the first characterization of a projective module as a direct summand of a free module actually implies that every finitely-generated projective A-module is free, using Nakayama's lemma.

As a corollary of this, one finds that a finitely-generated module M over a noetherian ring A is projective only if it is locally free, i.e. $M_{\mathfrak{p}}$ is free for all primes (equivalently, for all maximal ideals) $\mathfrak{p} \subset A$. In fact the 'only if' is an if and only if. (Such modules are the vector bundles over the scheme $\operatorname{Spec} A$.)

Proof. Let $m_1, \ldots, m_n$ be a vector space basis of $P \otimes \kappa(\mathfrak{m})$, where $\mathfrak{m}$ is the maximal ideal of A. Then these generators lift to n elements of P which generate it by Nakayama's lemma, hence providing a surjection $A^n \twoheadrightarrow P$. This surjection splits since P is projective; now $A^n = P \oplus N$. But reduction mod $\mathfrak{m}$ and a comparison of dimension shows that $N/\mathfrak{m}N = 0$. By Nakayama, $N = 0$. $\square$

(4) An A-module M is called faithfully flat if the functor $A\text{-mod} \to A\text{-mod}$ $- \otimes_A M$ is exact and faithful; equivalently if it is flat and reflects zero objects (an A-module F has $F \otimes M = 0$ if and only if $F = 0$);[1] equivalently if it is flat and whenever one has a complex of A-modules

$$N \longrightarrow P \longrightarrow Q \tag{*}$$

such that the tensored complex

$$N \otimes M \longrightarrow P \otimes M \longrightarrow Q \otimes M$$

is exact, then the complex (*) is exact. Prove that a flat module M over a ring A is faithfully flat if and only if it has nonempty fibers; i.e. if $M \otimes \kappa(\mathfrak{p}) \neq 0$ for every prime $\mathfrak{p}$ (as usual it suffices to check only the maximal ones). (Hint: For $\Rightarrow$, use that $A \to \kappa(\mathfrak{p})$ is nonzero. For $\Leftarrow$, study the cohomology $H = \ker(P \to Q)/\operatorname{im}(N \to P)$ of the complex (*).) Using this criterion, for $\mathfrak{p} \subset A$ prime, when is the flat A-module $A_{\mathfrak{p}}$ faithfully flat?

Proof. $\Rightarrow$: Let $R \to \kappa(\mathfrak{p})$ be denoted by α; then α is nonzero, so we have that $\operatorname{im} \alpha \neq 0$ in the exact sequence $0 \to \ker \alpha \to R \xrightarrow{\alpha} \operatorname{im} \alpha \to 0$; therefore as $-\otimes M$ is faithful and hence reflects zero objects, $M \otimes \kappa(\mathfrak{p}) \cong \operatorname{im}(1_M \otimes \alpha) \neq 0$.

[1] An exact functor T between abelian categories is faithful if and only if it reflects zero objects. Proof: First assume T faithful. An object o in an abelian category is called a zero object if the identity morphism 1_o is the zero morphism; as T is faithful, T reflects zero objects. For the converse, let $\alpha : X \to Y$ be a nonzero morphism, and factor α as $X \twoheadrightarrow \operatorname{im} \alpha \hookrightarrow Y$. As T is exact, $T\alpha$ factors as $X \twoheadrightarrow \operatorname{im} \alpha \hookrightarrow Y$. Since $\operatorname{im} \alpha \neq 0$, by hypothesis $T(\operatorname{im} \alpha) \neq 0$, so $T\alpha$ is nonzero. $\square$

$\Leftarrow$: Assume that M is flat and for every maximal ideal $\mathfrak{m}$, $M \otimes \kappa(\mathfrak{m}) = M/\mathfrak{m}M \neq 0$. Let H be as in the hint; by flatness we find $H \otimes_A M = 0$. Take $x \in H$ and let $I := \operatorname{ann} x$ be its annihilator. Since $A/I \hookrightarrow H$ by the map taking A to x, we find $M/IM \hookrightarrow H \otimes_A M = 0$ by flatness of M. If $I \neq 0$ we may choose a maximal ideal $I \subset \mathfrak{m} \subset A$, producing a contradiction, as $M/IM \twoheadrightarrow M/\mathfrak{m}M$ surjects.

By the criterion, the flat A-module $A_{\mathfrak{p}}$ is faithfully flat if and only if every fiber of the natural homomorphism is nonempty; by the ideal theory of localization, this is true if and only if A is local with maximal ideal $\mathfrak{p}$; i.e. if and only if $A \cong A_{\mathfrak{p}}$. □

(5) An artinian ring is a ring with finitely many prime ideals, all of which are maximal. It is a theorem that if a ring has a finite composition series (is 'of finite length') as a module over itself; i.e. $A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n = 0$ with quotients A_i/A_{i+1} which are simple modules (no nonzero submodules; i.e. isomorphic to $A/\mathfrak{m}$ for $\mathfrak{m}$ maximal), then A is artinian and noetherian. A finite morphism of rings $A \to B$ is one which makes B into a finite A-module; this is equivalent to B being generated over A by finitely many integral elements (elements which satisfy a monic polynomial with coefficients in A). Prove that a finite morphism is quasi-finite; i.e. for every prime $\mathfrak{p} \subset A$ the fibers $B \otimes_A \kappa(\mathfrak{p})$ are rings with only finitely many primes.

Proof. The fiber $B \otimes_A \kappa(\mathfrak{p})$ is a finite-dimensional vector space over the field $\kappa(\mathfrak{p})$, hence has finite length as a module over itself. □

The next two questions concern the relationship between ideals in polynomial rings and their vanishing in affine space. Let k denote an algebraically closed field. Given a subset $I \subset k[x_1, \ldots, x_n]$, we define an algebraic subset of $\mathbf{A}^n(k)$, considered as simply k^n, by

$$Z(I) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \quad \text{for all } f \in I\}.$$

Given a set $X \subset \mathbf{A}^n(k)$, define

$$I(X) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \quad \text{for all } (a_1, \ldots, a_n) \in X\}.$$

Then the classical Nullstellensatz states that if I as above is an ideal, then

$$I(Z(I)) = \operatorname{rad} I,$$

where $\operatorname{rad} I$ is defined in a previous problem. Thus, the correspondences $I \mapsto Z(I)$ and $X \mapsto I(X)$ induce a bijection between the collection of algebraic subsets of $\mathbf{A}^n(k)$ (subsets of the form $Z(I)$ for I as above; we may assume I is moreover an ideal) and radical ideals of $k[x_1, \ldots, x_n]$ (ideals which equal their own radical). The next two problems obtain this result as a corollary of a result about Jacobson rings.

Preserve all the notation above. It is easy to see that for each $p = (a_1, \ldots, a_n) \in \mathbf{A}^n(k)$, the ideal $\mathfrak{m}_p := (x_1 - a_1, \ldots, x_n - a_n) \subset k[x_1, \ldots, x_n]$ is a maximal ideal, even if k is not algebraically closed (continue to assume that it is); simply quotient by $\mathfrak{m}_p$ to see this.

A Jacobson ring is a ring in which every prime ideal is an intersection of maximal ideals. Grant the following theorem (general version of the Nullstellensatz).

Theorem. *Let R be a Jacobson ring and S be an R-algebra of finite type (finitely generated as an* algebra*). Then S is a Jacobson ring. Moreover, let $\mathfrak{n} \subset S$ be* *a maximal ideal. Then its restriction* $\mathfrak{m} := \mathfrak{n} \cap R$ *is maximal, and moreover the extension of residue fields* $\kappa(\mathfrak{m}) \subset \kappa(\mathfrak{n})$ *is finite.*

(6) Let $X \subset \mathbf{A}^n(k)$ be an algebraic set $X = Z(I)$. Then every maximal ideal of $A(X) := k[x_1, \ldots, x_n]/I$ is of the form $\mathfrak{m}_p/I$ for some $p \in X$. In particular, the points of X are in bijection with the maximal ideals of $A(X)$. (Hint: use the general form of the Nullstellensatz to show that every maximal ideal in the ring $k[x_1, \ldots, x_n]$ is of the form $\mathfrak{m}_p$ for some p.)

Proof. The natural map $k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/\mathfrak{m}_p = k$ may be described as evaluation at p; thus $\mathfrak{m}_p \supset I$ iff $p \in X$. Since the maximal ideals of $A(X)$ are the maximal ideals of $S := k[x_1, \ldots, x_n]$ taken modulo I, it only remains to show that every maximal ideal of S has the form $\mathfrak{m}_p$ for some p.

Suppose $\mathfrak{n}$ is a maximal ideal of S. The general form of the Nullstellensatz applied with $R = k$ shows us that $S/\mathfrak{n}$ is algebraic over $k/(\mathfrak{n} \cap k) = k$, but as k is algebraically closed we find $S/\mathfrak{n} = k$. Let a_i be the image of x_i under the map $S \to S/\mathfrak{n} = k$, and let $p = (a_1, \ldots, a_n)$. It follows that $\mathfrak{m}_p \subset \mathfrak{n}$, and as $\mathfrak{m}_p$ is maximal, the two ideals are actually equal. □

(7) Prove the classical Nullstellensatz from the general version, using the formula for the radical in the second problem.

Proof. The previous problem shows that the points of $Z(I)$ are in bijection with the maximal ideals of $k[x_1, \ldots, x_n]$ containing I. Thus $I(Z(I))$ is the intersection of all the maximal ideals containing I. By the general form of the Nullstellensatz, S (in the notation of the previous problem) is a Jacobson ring, so every prime ideal of S is an intersection of maximal ideals. Hence $I(Z(I))$ is equal to the intersection of all prime ideals containing I. By Problem 2, this is equal to $\operatorname{rad} I$, and we are done. (The equality $Z(I(X)) = X$ follows directly from the definition of an algebraic set.) □

E-mail address: barrett@math.uchicago.edu