250B: Commutative Algebra

Nir Elber

Spring 2022

Contents

THEME 1: LOCALIZATION

Hold tight to your geometric motivation as you learn the formal structures which have proved to be so effective in studying fundamental questions.

—Ravi Vakil

1.1 February 1

Hopefully we finish localizing today.

1.1.1 A Little On Tensor Products

Let's start with some review exercises.

Proposition 1.1. Fix R a ring and M an R-module and $I \subseteq R$ an R-ideal. This gives the R-module R/I, and we claim that

$$(R/I) \otimes_R M \cong M/IM.$$

canonically.

Proof. We will use a few facts about the tensor product here. To start off, we use the short exact sequence

$$0 \to I \to R \to R/I \to 0$$

and then tensor by $\otimes_R M$. This gives the right-exact sequence

$$I \otimes_R M \to R \otimes_R M \to (R/I) \otimes_R M \to 0.$$

We know that $R \otimes_R M \cong M$ (canonically) by $r \otimes m \mapsto rm$, and then tracking the image of $I \otimes_R M$ through the isomorphism $R \otimes_R M \cong M$, we see that

$$I \otimes_R M \cong \{rm : r \in I \text{ and } m \in M\} = IM.$$

So we are promised the right-exact sequence

$$IM \to M \to (R/I) \otimes_R M \to 0,$$

which gives the desired isomorphism. ∎

Remark 1.2 (Nir)**.** As usual, this isomorphism is functorial in M.

Corollary 1.3. Fix R a ring and $I, J \subseteq R$ ideals. Then $(R/I) \otimes_R (R/J) \cong R/(I+J)$.

Proof. From the above we can conclude

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

This finishes. ∎

The above result could be used for fun and profit on the homework.

Remark 1.4. Professor Serganova does not care too much about noncommutative rings in this class.

We also have the following "change of constants" results.

Proposition 1.5. Fix S an R-algebra. Then, given S-modules A and B and C, we have

$$(A \otimes_R B) \otimes_S C \simeq A \otimes_R (B \otimes_S C).$$

Proof. The isomorphism is by $(a \otimes b) \otimes c \mapsto a \otimes (b \otimes c)$. ∎

Proposition 1.6. Fix S an R-algebra. Then, given R-modules M and N, we have

$$S \otimes_R (M \otimes_R N) \cong (S \otimes_R M) \otimes_S (S \otimes_R N),$$

where $S \otimes_R M$ is given an S-module structure by multiplying the left coordinate.

Proof. The trick is to use associativity in clever ways. Indeed,

$$\begin{aligned}(S \otimes_R M) \otimes_S (S \otimes_R N) &\cong (M \otimes_R S) \otimes_S (S \otimes_R N) \\ &\cong (M \otimes_R (S \otimes_S (S \otimes_R N))) \\ &\cong (M \otimes_R ((S \otimes_S S) \otimes_R N)) \\ &\cong (M \otimes_R (S \otimes_R N)),\end{aligned}$$

which becomes $S \otimes_R (M \otimes_R N)$ after more association. ∎

1.1.2 Artinian Rings

We have the following definition, dual to the ascending chain condition for Noetherian modules.

Artinian module

Definition 1.7 (Artinian module)**.** An R-module M is *Artinian* if and only if any descending chain of R-submodules

$$M \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

will stabilize.

Definition 1.8. The ring R is *Artinian* if and only if R is an Artinian as an R-module.

In other words, after recalling that R-submodules of R are ideals, we see that being an Artinian ring is the same as having the descending chain on ideals.

Example 1.9. Fix k a field and $p(x) \in k[x] \setminus \{0\}$. Then $k[x]/p(x)$ is a finite-dimensional k-vector space (in fact, of dimension $\deg p$), which means that it is both Noetherian and Artinian because a chain of k-subspaces can be measured to stabilize by dimension.

Example 1.10. More generally, any finite-dimensional k-algebra is an Artinian ring.

Example 1.11. The ring $\mathbb{Z}/n\mathbb{Z}$ is finite and hence Artinian (and Noetherian).

Observe that all of our examples of Artinian rings are in fact Noetherian. In fact, we will show that all Artinian rings are Noetherian; in the process, we will be able to describe all Artinian rings.

Here is a technical result which we will want to use later; it is dual to the Noetherian case in **??**.

Proposition 1.12. Fix a short exact sequence

$$0 \to A \to B \to C \to 0$$

of R-modules. Then B is Artinian if and only if A and C are Artinian.

Proof. We omit this proof; one can essentially copy the proof of the Noetherian case in **??**. ■

1.1.3 Composition Series

The main character in our story on Artinian rings will be the "module of finite length."

Composition series

Definition 1.13 (Composition series)**.** Fix an R-module M. Then a *composition series* (or *Jordan–Hölder series*) is a chain of distinct R-submodules

$$M := M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_N := \{0\}$$

such that each quotient M_i/M_{i+1} is a simple R-module. The M_i/M_{i+1} are the *composition factors*.

Lemma 1.14. If an R-module M is both Artinian and Noetherian, then it has a composition series.

Proof. Because M is Noetherian, the set of all proper ideals will have a maximal element, which we call M_1. Observe that M_1 will then be both Artinian and Noetherian (as a submodule of M), so we can repeat the process to get a maximal submodule $M_2 \subsetneq M_1$. Continuing, we get

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots.$$

But this process must stop eventually because M is Artinian, so we are done. ■

Non-Example 1.15. This process does not work when M is not Artinian. For example,

$$\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq 8\mathbb{Z} \supsetneq \cdots$$

creates an infinite descending chain.

Here is the main result on composition series.

Theorem 1.16 (Jordan–Hölder)**.** Fix M an R-module which has a composition series. Then all composition series of M have the same length and in fact the same multiset of composition factors.

Proof. Omitted. This is Eisenbud and in fact essentially the same as the proof for groups if one has seen the corresponding proof for groups. ■

1.1.4 Modules of Finite Length

Theorem 1.16 gives us the following definition.

Length

Definition 1.17 (Length)**.** An R-module M with a composition series is said to have *length* n if and only if all composition series have n factors.

Finite length

Definition 1.18 (Finite length)**.** An R-module M is *of finite length* if and only if M has a composition series.

Our work with Jordan–Hölder gives us the following quick, technical results.

Corollary 1.19. Fix M an R-module of finite length. Then M is both Artinian and Noetherian.

Proof. We will be brief; suppose M has a composition series with n composition factors. The point is that composition series are maximal among all chains of distinct submodules, so any chain of submodules can have at most $n+1$ distinct submodueles. In particular, any ascending or descending chain must stabilize. ■

Corollary 1.20. Fix a short exact sequence

$$0 \to A \to B \to C \to 0$$

of R-modules. Then B is of finite length if and only if A and C are of finite length.

Proof. An R-module M is of finite length if and only if it is Noetherian and Artinian. So combine **??** with Proposition 1.12 to finish. ■

Corollary 1.21. Fix a module M and a chain of submodules

$$M := M_0 \supseteq M_1 \supseteq \cdots \supseteq M_N := \{0\}.$$

If each quotient M_i/M_{i+1} is of finite length, then M is of finite length.

Proof. We induct on N. When $N = 1$, we have $M = M_1/M_0$, so there is nothing to say. Otherwise, by the induction, we may assume that M_1 is of finite length because of the chain of submodules

$$M_1 \supseteq \cdots \supseteq M_N := \{0\}$$

with M_i/M_{i+1} always simple. But now we see we have the short exact sequence

$$0 \to M_1 \to M \to M_0/M_1 \to 0,$$

so because M_1 and M_0/M_1 both have finite length, $M = M_0$ will have finite length. ■

Quickly, note that the support of M is particularly nice when M has a composition series, which essentially comes from various facts we've already proven.

Lemma 1.22. Fix M an R-module with a finite composition series

$$M := M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_0 := \{0\}.$$

Then $\operatorname{Supp} M$ is the composition factors.

Proof. The point is to turn the composition series into a whole bunch of short exact sequence, from which we can read off the support. Namely, we have the short exact sequences

$$0 \to M_i \to M_{i+1} \to M_{i+1}/M_i \to 0$$

from which we can read off the support inductively. ■

And here is a nice result which we get from this.

Theorem 1.23. Fix M a R-module of finite length. Then the following are true.

(a) We can glue the localization maps $M \to M_{\mathfrak{p}}$ together to form an R-module isomorphism

$$M \cong \bigoplus_{\mathfrak{p} \in \operatorname{Supp} M} M_{\mathfrak{p}}.$$

(b) The multiplicity of a simple module $R/\mathfrak{m}$ as a composition factor is the length of $M_{\mathfrak{p}}$ as an $R_{\mathfrak{p}}$-module.

Proof. We will be very brief. The details are in Eisenbud. Last time we showed that if a morphism $\varphi : M \to N$ induces isomorphisms $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ for each maximal ideal $\mathfrak{m} \subseteq R$, then φ is an isomorphism. Thus, it suffices to show the canonical map

$$\varphi : M \to \bigoplus_{\mathfrak{p} \in \operatorname{Supp} M} M_{\mathfrak{p}}$$

induces isomorphisms under localization. Namely, localizing by some maximal ideal $\mathfrak{m}$, we get a map

$$\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to \bigoplus_{\mathfrak{p} \in \operatorname{Supp} M} (M_{\mathfrak{p}})_{\mathfrak{m}}.$$

The main point, now, is to compute that

$$(R/\mathfrak{p})_{\mathfrak{q}} \cong \begin{cases} 0 & \mathfrak{p} \neq \mathfrak{q}, \\ R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} & \mathfrak{p} = \mathfrak{q}. \end{cases}$$

For (b), the point is to localize a composition series to get the result, again using the above computatin. ■

1.1.5 Artinian Grab-Bag

We are now able to give the following classification.

Theorem 1.24. Fix R a ring. Then R is Artinian if and only if R is Noetherian and all its primes are maximal.

We split the proof into two parts.

Proof of the backwards direction in Theorem 1.24. Suppose R is neither Artinian nor Noetherian. It will suffices to show that not all prime ideals of R are maximal.

Being neither Artinian nor Noetherian conspire to give us an ideal J maximal with respect to the property that R/J is not Artinian: because R is not Artinian, the collection

$$\mathcal{P} := \{\text{ideal } J \subseteq R : R/J \text{ is not Artinian}\}$$

is nonempty (for $(0) \in \mathcal{P}$), and because R is Noetherian, there will be a maximal element, which we call $\mathfrak{p}$. Observe that $\mathfrak{p}$ is not maximal, for then $R/\mathfrak{p}$ would be a field and hence be Artinian.

With this in mind, we claim that $\mathfrak{p}$ must be prime. This will finish because $\mathfrak{p}$ will be a prime which is not maximal. Well, suppose that $a \notin \mathfrak{p}$. Consider the short exact sequence of R-modules

$$0 \to \frac{\mathfrak{p}+(a)}{\mathfrak{p}} \to \frac{R}{\mathfrak{p}} \to \frac{R}{\mathfrak{p}+(a)} \to 0.$$

We are going to profit from studying this short exact sequence by using Proposition 1.12. In particular, $R/\mathfrak{p}$ is not Artinian, so we cannot have both R-modules on its left and right be Artinian.

Well, $\mathfrak{p} \subsetneq \mathfrak{p}+(a)$, so by maximality, $R/(\mathfrak{p}+(a))$ will have to be Artinian. So instead $(\mathfrak{p}+(a))/\mathfrak{p}$ cannot be Artinian. But now we observe that we have the following isomorphism of R-modules.

Lemma 1.25. Fix R a ring and $I \subseteq R$ an ideal and $a \in R$. Then we define $(I : a) := \{r \in R : ar \in I\}$, and we claim that $(I : a)$ is an ideal and

$$\frac{R}{(I:a)} \cong \frac{I+(a)}{I}.$$

Proof. Note that there is an R-module map $\varphi : R \to (a) + I$ by

$$\varphi : x \mapsto ax.$$

Indeed, $\varphi(r_1x_1 + r_2x_2) = ar_1x_1 + ar_2x_2 = r_1\varphi(x_1) + r_2\varphi(x_2)$. Now, modding out the image by $I \subseteq (a) + I$, we get a map

$$\widetilde{\varphi} : R \to \frac{(a)+I}{I}.$$

We note that this map is surjective because any coset $[x]_I$ with $x \in (a) + I$ can have $x = ar + p$ where $r \in R$ and $p \in I$, meaning that $\widetilde{\varphi}(r) = [ar]_I = [x]_I$. Further, we can compute the kernel of $\widetilde{\varphi}$ as

$$\{r \in R : ar \in I\} = (I : a).$$

Thus, $(I : a) = \ker \widetilde{\varphi}$ is an ideal, and $\widetilde{\varphi}$ induces an isomorphism $R/(I : a) \to (I + (a))/I$, finishing. ■

Now, because $(\mathfrak{p} + (a))/\mathfrak{p}$ is not Artinian, we see $R/(\mathfrak{p} : a)$ cannot be Artinian. But certainly $\mathfrak{p} \subseteq (\mathfrak{p} : a)$ because each $x \in \mathfrak{p}$ has $ax \in \mathfrak{p}$, so we must have

$$\mathfrak{p} = (\mathfrak{p} : a)$$

by the maximlity of $\mathfrak{p}$. We now finish the proof. Suppose now that $ab \in \mathfrak{p}$, and we claim that $b \in \mathfrak{p}$. Well, $ab \in \mathfrak{p}$ implies that $b \in (\mathfrak{p} : a) = \mathfrak{p}$. So we are done. ■

Proof of the forwards direction of Theorem 1.24. For the other direction, we note that we can show all primes are maximal without tears.

Lemma 1.26. Fix R an Artinian ring. Then any prime ideal $\mathfrak{p} \subseteq R$ is maximal.

Proof. We follow the argument given here. Well, given $\mathfrak{p}$ a prime so that $R/\mathfrak{p}$ is an integral domain, we show that $R/\mathfrak{p}$ is actually a field. Well, we can pick up $[x]_\mathfrak{p} \neq 0$ represented by some $x \notin \mathfrak{p}$, and we show that $[x]_\mathfrak{p}$ is a unit. Note that we have the descending chain

$$(x) \supseteq \left(x^2\right) \supseteq \left(x^3\right) \supseteq \cdots,$$

which must eventually stabilize, so there is some $n \in \mathbb{N}$ such that $(x^n) = \left(x^{n+1}\right)$, so there is $r \in R$ with $x^n = rx^{n+1}$. In particular,

$$x^n(1 - xr) = 0.$$

Working in $R/\mathfrak{p}$, we see that $[x]_\mathfrak{p} \neq 0$, so the fact that $R/\mathfrak{p}$ is an integral domain implies that

$$[x]_\mathfrak{p} \cdot [r]_\mathfrak{p} = 1,$$

so indeed, $[x]_\mathfrak{p}$ is a unit. ■

So it remains to show that R is Artinian implies that R is Noetherian. We introduce the following definition.

Jacobson radical

Definition 1.27 (Jacobson radical)**.** Fix R a ring. Then we define the *Jacobson radical* $J \subseteq R$ to be

$$J := \bigcap_{\mathfrak{m}} \mathfrak{m},$$

where $\mathfrak{m}$ ranges over all maximal ideals of R.

Note that the Jacobson radical is an ideal because ideals are closed under intersection. Alternatively, we can view J as the kernel of the map

$$R \to \prod_{\mathfrak{m}} R,$$

for any ring R, where the product is over maximal ideals $\mathfrak{m} \subseteq R$.

In fact, in the case where R is Artinian, the above map will be surjective. By the Chinese remainder theorem, it suffices to show that there are only finitely many maximal ideals of R.

Lemma 1.28. Fix R an Artinian ring. Then R has only finitely many maximal ideals.

Proof. We follow the argument from here because I think it is pretty close to what I understand Professor Serganova saying in class.

The point here is that infinitely many maximal ideals will induce an infinite composition series. Indeed, suppose that we have some infinite collection $\{\mathfrak{m}_k\}_{k=1}^{\infty}$ of maximal ideals, and we claim that the chain

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supseteq \cdots$$

is an infinite composition series; this will verify that R is not Artinian.

Indeed this chain is infinite, and to see that it is a composition series, we have to check that

$$\frac{\mathfrak{m}_1 \cap \cdots \mathfrak{m}_k}{\mathfrak{m}_1 \cap \cdots \mathfrak{m}_k \cap \mathfrak{m}_{k+1}}$$

is simple for each $k \geq 1$. Indeed, note that we have the following commutative diagram with exact rows, where the vertical morphisms are isomorphisms given by the Chinese remainder theorem.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}} & \longrightarrow & \dfrac{R}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}} & \longrightarrow & \dfrac{R}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n} & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & R/\mathfrak{m}_{n+1} & \longrightarrow & \bigoplus_{k=1}^{n+1} R/\mathfrak{m}_k & \longrightarrow & \bigoplus_{k=1}^{n} R/\mathfrak{m}_k & \longrightarrow & 0
\end{array}$$

In particular, the square commutes because $[r]_{\mathfrak{m}_1 \cap \cdots \mathfrak{m}_n \cap \mathfrak{m}_{n+1}}$ in the top-left will go to $([r]_{\mathfrak{m}_1}, \ldots, [r]_{\mathfrak{m}_n})$ in the bottom-right, no matter which we path we choose. Thus, there is an induced isomorphism

$$\frac{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}} \cong \frac{R}{\mathfrak{m}_{n+1}},$$

so indeed this R-module is simple, say by **??**. ∎

Remark 1.29. Intuitively, there can only be finitely many maximal ideals $\mathfrak{m}$ because each $R/\mathfrak{m}$ will induce a composition factor, of which there are only finitely many because R is Artinian. In the above proof, we have actually shown how to induce such a composition series using each of these composition factors.

Remark 1.30 (Nir)**.** In fact, an Artinian ring will have only finitely many prime ideals, which we can see directly because all primes are maximal.

We now proceed with the proof of Theorem 1.24. The payoff to Lemma 1.28 is that the Chinese remainder theorem gives us right-exactness of the short exact sequene

$$0 \to J \to R \to \prod_{\mathfrak{m}} R/\mathfrak{m} \to 0.$$

In particular,

$$R/J \cong \prod_{\mathfrak{m}} R/\mathfrak{m}$$

is a product of finitely many simple modules $R/\mathfrak{m}$, so R/J will be of finite length. (In particular, R/J has only finitely many ideals because each $R/\mathfrak{m}$ has only two ideals.) We would like to build use this result on R/J to tell us that R is of finite length, but we will need a smallness condition on J to make this work.

The key claim is as follows.

Lemma 1.31. Fix R an Artinian ring. Then the Jacobson radical J is nilpotent.

Proof. Observe that we have a descending chain

$$J \supseteq J^2 \supseteq J^3 \subseteq \cdots,$$

which stabilizes because R is Artinian. So suppose that $J^n = J^{n+1} = I$ for some $n \geq 1$, and we hope $I = (0)$. By the stabilization, we see $I^2 = J^{2n} = J^n = I$.

Now, if $I \neq (0)$, then we can find a minimal ideal $K \subseteq I$ such that $IK \neq (0)$ and $K \neq (0)$. (Note that $I = K$ would work—$I^2 = I \neq (0)$—but is perhaps not minimal; we need Zorn's lemma to get the minimal such ideal.) We start with some fact-collection on K. Note that $I(IK) = I^2K = IK \neq (0)$ and $IK \neq (0)$ while $IK \subseteq K$, so K's minimality forces

$$IK = K.$$

Furthermore, because $K \neq (0)$, there exists $a \in K \setminus \{(0)\}$ such that $aI \neq (0)$. So $(a)I \neq (0)$ while $(a) \neq 0$, so $(a) \subseteq K$ combined with K's minimality (again) forces

$$K = (a).$$

Combining the above two facts, we are granted $b \in I$ such that $ba = a$.

But here is the key trick: we can write $ba = a$ as

$$a(1-b) = 0.$$

However, $b \in I$ implies $b \in J$ implies $1-b \notin J$, so $(1-b)$ is not in any maximal ideal. So it follows $(1-b) = R$, so $1 - b \in R^\times$! Upon cancelling, we see $K = (a) = 0$, which is our contradiction. ∎

We now return to the proof. We claim that R is of finite length, which will imply that R is Noetherian. We work with the chain

$$R \supseteq J \supseteq J^2 \supseteq \cdots \supseteq J^n = (0).$$

By Corollary 1.21, it suffices to check that J^i/J^{i+1} is of finite length, for each i. But observe that we have the short exact sequences

$$0 \to \frac{J^i}{J^{i+1}} \to \frac{R}{J^{i+1}} \to \frac{R}{J^i} \to 0. \tag{$*$}$$

So by Corollary 1.20, it suffices to check that R/J^{i+1} is of finite length for each i.

We do this by induction. For $i = 0$, we have already shown that R/J is of finite length above. For the inductive step, take $i > 0$. We know that R/J^i is of finite length, but then Corollary 1.20 applied to $(*)$ tells us that that R/J^{i+1} will be of finite length as well. This finishes. ∎

1.1.6 Geometry of Artinian Rings

While we're here, we provide some more nice facts.

Proposition 1.32. Any Artinian ring is a product of local Artinian rings.

Proof. This essentially comes down to modules of finite length being products of localizations over their support. ■

We can even give a geometric view to what we are doing.

Proposition 1.33. Fix $I \subseteq k[x_1, \dots, x_n]$. Then the following are equivalent.

- The ring $R := k[x_1, \dots, x_n]/I$ is Artinian.
- The set $Z(I) \subseteq \mathbb{A}^n(k)$ is finite.
- The ring R is a finite-dimensional k-algebra.

Proof. Omitted. See Eisenbud. ■

1.1.7 The Radical, Returned

And we end our discussion with the following miscellaneous result.

Proposition 1.34. Fix an ideal $I \subseteq R$. Then

$$\operatorname{rad} I = \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p},$$

where $\mathfrak{p}$ ranges over all prime ideals.

Proof. The main point is the following lemma.

Lemma 1.35. Fix R a ring and $I \subseteq R$ an ideal and $U \subseteq R$ a multiplicatively closed subset such that $I \cap U = \varnothing$. Suppose $\mathfrak{p}$ is maximal in the set of ideals satisfying $\mathfrak{p} \cap U = \varnothing$ and $I \subseteq \mathfrak{p}$. Then $\mathfrak{p}$ is prime.

Before proving the lemma, we note that, under the hypotheses of the problem, such a maximal ideal $\mathfrak{p}$ will exist, which we can conjure by Zorn's lemma from the set of all ideals satisfying $\mathfrak{p} \cap U = \varnothing$ and $I \subseteq \mathfrak{p}$.[1]

Proof. Suppose that $a, b \notin \mathfrak{p}$, and it suffices to show that $ab \notin \mathfrak{p}$. Well, $(a) + \mathfrak{p}$ and $(b) + \mathfrak{p}$ are both strictly larger than $\mathfrak{p}$ while containing $I \subseteq \mathfrak{p}$, so they must intersect U. Suppose $u \in ((a)+\mathfrak{p}) \cap U$ and $v \in ((b)+\mathfrak{p}) \cap U$. Then

$$uv \in ((a) + \mathfrak{p})((b) + \mathfrak{p}) = (ab) + (a)\mathfrak{p} + (b)\mathfrak{p} + \mathfrak{p}^2 \subseteq (ab) + \mathfrak{p}.$$

Thus, $(ab)+\mathfrak{p}$ intersects U at $uv \in U$, so it follows $\mathfrak{p} \neq (ab)+\mathfrak{p}$ because $\mathfrak{p} \cap U = \varnothing$. Thus, $ab \notin \mathfrak{p}$, finishing. ■

We now attack the proposition directly. In one direction, suppose that $a \in \operatorname{rad} I$ so that $a^n \in I$ for some $n \in \mathbb{N}$. Then for any prime $\mathfrak{p}$ containing I, we have $a^n \in \mathfrak{p}$, so $a \in \mathfrak{p}$ by primality of $\mathfrak{p}$. It follows

$$\operatorname{rad} I \subseteq \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$

[1] This set is nonempty because $I \cap U = \varnothing$ and $I \subseteq I$. All ascening chains have an upper bound by taking the union along the chain.

The other inclusion requires the lemma. Suppose that $a \notin \operatorname{rad} I$, and we will find a prime $\mathfrak{p} \supseteq I$ such that $a \notin \mathfrak{p}$. Indeed, we pick up an ideal $\mathfrak{p}$ containing I which is maximal avoiding the set

$$\langle a \rangle := \{a^n : n \in \mathbb{N}\}.$$

Indeed, such an ideal $\mathfrak{p}$ by the discussino preceding the lemma, and it is prime by the lemma. But $a \notin \mathfrak{p}$ while $I \subseteq \mathfrak{p}$, so it follows that

$$a \notin \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p},$$

finishing. ■

Corollary 1.36. Fix R a ring. Then $r \in R$ is nilpotent if and only if $r \in \mathfrak{p}$ for each prime ideal $\mathfrak{p} \subseteq R$.

Proof. The set of nilpotent elements in R is

$$\operatorname{rad}(0) = \{r \in R : r^n = 0 \text{ for some } n \in \mathbb{N}\}.$$

By Proposition 1.34, this will be the intersection of all prime ideals of R. In other words, an element $r \in R$ is nilpotent if and only if $r \in \mathfrak{p}$ for all primes $\mathfrak{p}$, which is what we wanted. ■