Commutative Algebra

Runi Malladi

May 1, 2023

Contents

1 rings and ideals

1.1 operations on ideals

Let $\mathfrak{a}, \mathfrak{b} \subset A$ be ideals.

1.1.1 sum

The sum of two ideals is an ideal, and is the set

$$\mathfrak{a} + \mathfrak{b} = \{a + b\}.$$

The sum of finitely many ideals is the set

$$\sum_{i=1}^{n} \mathfrak{a}_i = \{\sum_{i=1}^{n} a_i\}.$$

The sum of infinitely many ideals is the set of all sums finite sums.

Note that the sum is the smallest ideal containing each of its summands.

1.1.2 intersection

The setwise intersection of arbitrary many ideals is naturally an ideal:

$$\bigcap_{i \in I} \mathfrak{a}_i$$

Proposition 1.1. If $\mathfrak{b} \subset \mathfrak{a}$ or $\mathfrak{c} \subset \mathfrak{a}$, then

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}.$$

1.1.3 product

The product of two ideals is an ideal, which is

$$\mathfrak{a}\mathfrak{b} = \{xy\}.$$

The product of finitely many ideals is likewise

$$\prod_{i=1}^{n} \mathfrak{a}_i = \{\prod_{i=1}^{n} a_i\}.$$

Proposition 1.2. $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c}$.

1.1.4 quotient

The quotient of two ideals $I \subset J \subset A$ is the abelian group formed by taking the quotient of abelian groups J/I. This is in general not an ideal of A. However, it is an A/I-module and, in fact, an ideal in the ring A/I:

Proposition 1.3. The abelian group J/I is A-module isomorphic to the extension (Definition 1.36) of J in A/I, under the natural quotient map $A \to A/I$.

Proof. Given ideals $I \subset J \subset A$, the extension of J to the ring A/I consists of finite sums of the form

$$\sum_{k=1}^{n}(j_k+I)(a_k+I) = (\sum_{k=1}^{n} j_k a_k) + I = j + I,$$

where j ranges over all of J. This is nothing but the quotient J/I as abelian groups. □

We have to be a bit careful though when there is no assumption on inclusions of I and J with respect to each other, since then the quotient of abelian groups doesn't make sense.

Corollary 1.4. $I(A/J) = (I+J)/J$.

Proof. $(I+J)/J$ is the extension of the ideal $I+J$ to the ring A/J under the natural quotient. But in this quotient, elements of J are killed, so this it is equivalently the extension of I to A/J. □

1.2 prime ideals

Proposition 1.5 (Krull)**.** Let $S \subset A$ be a multiplicatively closed not containing 0. Consider the set

$$\Sigma = \{\mathfrak{a} \subset A : \mathfrak{a} \cap S = \emptyset\}$$

of ideals avoiding S. Then any maximal element[1] of Σ is prime.

Proof. Let $\mathfrak{y} \in \Sigma$ be a maximal element. It suffices to show that for $a, b \in A$, if $ab \in \mathfrak{y}$ then $a \in \mathfrak{y}$ or $b \in \mathfrak{y}$. Suppose neither is in $\mathfrak{y}$. Then the ideals $\mathfrak{y}+(a)$ and $\mathfrak{y}+(b)$ strictly contain $\mathfrak{y}$, so there must exist $s \in (\mathfrak{y}+(a)) \cap S$, and $s' \in (\mathfrak{y}+(b)) \cap S$. We can write $s = y + ca$ and $s' = y' + c'a$ for $y, y' \in \mathfrak{y}$ and $c, c' \in A$. Then

$$ss' = pp' + cap' + pc'b + cc'ab,$$

which is in $\mathfrak{y}$ since $pp' + cap' + pc'b \in \mathfrak{y}$ and $ab \in \mathfrak{y}$. But this contradicts the fact that S is multiplicatively closed. □

Example 1.6. Take $S = A^\times$. Ideals avoiding S are all proper ideals, hence the above proposition is just saying that maximal ideals are prime.

[1] i.e. an ideal avoiding S which is not strictly contained in any other ideal avoiding S

Definition 1.7. Consider a multiplicatively closed set $S \subset A$, and let $s \in S$ and $a \in A$. We say that S is *saturated* if $as \in S$ implies $x \in S$.

Proposition 1.8. Let $\mathfrak{p}$ be prime, and consider the (multiplicatively closed) set $S = A - \mathfrak{p}$. Then S is saturated.

Proof. □ prove

The following tells us the this is almost the dual notion of "prime", but not exactly:

Proposition 1.9. The following are equivalent:

1. S is saturated.
2. $A - S$ is a union of prime ideals.

Proof. $(2 \Rightarrow 1)$ Suppose $A - S = \bigcup_\alpha \mathfrak{p}_\alpha$, where each $\mathfrak{p}_\alpha$ is prime. Then

$$S = A - \bigcup_\alpha \mathfrak{p}_\alpha = \bigcap_\alpha (A - \mathfrak{p}_\alpha).$$

First we will show S is multiplicatively closed. Let $s, s' \in S$. Then $s, s' \notin \mathfrak{p}_\alpha$ for all α. Since $\mathfrak{p}_\alpha$ is prime, we know $ss' \notin \mathfrak{p}_\alpha$ for all α. But this means that $ss' \in S$. Now to see that it is saturated, suppose to the contrary that $xs \in S$ with $x \notin S$ and $s \in S$. Then $x \in \mathfrak{p}_\beta$ for some β. But then $xs \in \mathfrak{p}_\beta$, contradicting that $xs \in S$.

$(1 \Rightarrow 2)$ Suppose S is saturated. Let $x \in A - S$. Then $(x) \cap S = \emptyset$, i.e. (x) avoids S. Define

$$\Sigma_x = \{\mathfrak{a} \subset A : (x) \subset \mathfrak{a}, \mathfrak{a} \cap S = \emptyset\}$$

to be the set of ideals avoiding S and containing (x). Let $\mathfrak{p}_x$ be a maximal element of Σ_x. By (a modified version of) Proposition 1.5, we have that $\mathfrak{p}_x$ is prime. In particular it contains x, and so

$$A - S = \bigcup_{x \in A - S} \{x\} \subset \bigcup_{x \in A - S} \mathfrak{p}_x \subset A - S$$

and the result follows. □

Corollary 1.10. $A - A^\times$ is the union of all maximal ideals.

Proof. Let $S = A^\times$. One checks this is saturated, and then applies Proposition 1.9. □

Corollary 1.11. The set of zero divisors is a union of prime ideals.

Proof. Take S to be the set of elements which are not zero divisors. One checks this is saturated, and then applies Proposition 1.9. □

Theorem 1.12 (prime avoidance)**.** Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals in A, and let $\mathfrak{a} \subset A$ be any ideal contained in their union. Then $\mathfrak{a} \subset \mathfrak{p}_i$ for some i.

Proof. We essentially need to contradict the fact that all of the $\mathfrak{p}_i$ are needed. We proceed by induction:

If $n = 1$, then the statement is trivial. For $n = 2$, suppose to the contrary that $\mathfrak{a}$ is not in $\mathfrak{p}_1$ or $\mathfrak{p}_2$. Then there exists $x_2 \in \mathfrak{a} - \mathfrak{p}_1$ and $x_1 \in \mathfrak{a} - \mathfrak{p}_2$. Note then that $x_1 \in \mathfrak{p}_1$ and $x_2 \in \mathfrak{p}_2$. Consider the element $x_1 + x_2 \in \mathfrak{a}$. Then $x \notin \mathfrak{p}_1$, for otherwise $x_2 = x - x_1$ would be. Likewise $x \notin \mathfrak{p}_2$. This is a contradiction.

Now for $n > 2$. By the induction step, if

$$\mathfrak{a} \subset \bigcup_{i \neq j} \mathfrak{p}_i$$

then we are done (the union is taken over all $1 \leq i \leq n$ with the exception of some $1 \leq j \leq n$). So we may assume $\mathfrak{a}$ is not in the above union for any j. Then for all j there exists $x_j \in \mathfrak{a}$ such that $x_j \in \mathfrak{p}_j$ and $x_j \notin x_i$ for all $i \neq j$. Let $x = \sum_j x_j \in \mathfrak{a}$.

We claim $x \notin \mathfrak{p}_j$ for any j. Suppose otherwise. Then $\sum_{i \neq j} x_j = x - x_1 \in \mathfrak{p}_j \in \mathfrak{p}_j$. But this is impossible, since by construction none of the x_i for $i \neq j$ are in $\mathfrak{p}_j$.

But this shows that $x \in \mathfrak{a} - \bigcup_i \mathfrak{p}_i$, which is an empty set. This is a contradiction. □

Definition 1.13. Let $\mathfrak{a} \subset A$ be proper. A *minimal prime* of (or above) $\mathfrak{a}$ is a prime ideal minimal in the set $V(A)$ of prime ideals containing $\mathfrak{a}$.

Proposition 1.14. Minimals primes exist.

Proof. Zorn's lemma backwards, comp hw □ prove

1.3 local rings

Definition 1.15. A is *local* if it has a unique maximal ideal.

Example 1.16.

1. The ring $\mathbb{C}\{z\}$ of convergent power series at the origin. The unique maximal ideal is (z).
2. The ring $\mathbb{Z}/p^k\mathbb{Z}$, where p is prime. Since every ideal of $\mathbb{Z}$ is principal (), and the ideals in this ring correspond to ideals in $\mathbb{Z}$ containing (p^k) by , the ideals in this ring have the form (a) where $a \mid p^k$. But this means $a = p^l$ for some $l \leq k$. In particular, all such (a) are contained in (p), hence the corresponding (now unique) maximal ideal in $\mathbb{Z}/p^k\mathbb{Z}$ is the ideal corresponding to (p). ref ref
3. $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Z} : p \nmid b\}$. Here every element is invertible except those with numerator dividing p. All such numbers are in the ideal (p).

Proposition 1.17. A is local if and only if $A - A^\times$ is an ideal.

Proof. Say A is local, with maximal ideal $\mathfrak{m}$. Then $A - A^\times$ is the union of maximal ideal (Proposition), hence $A - A^\times = \mathfrak{m}$ which is an ideal. Conversely, if $A - A^\times$ is an ideal, let $\mathfrak{m} \subset A$ be maximal. But $\mathfrak{m} \subset A - A^\times$, so $\mathfrak{m} = A - A^\times$. □

ref

1.4 nilpotents

Definition 1.18. An element $a \in A$ is called *nilpotent* if $a^k = 0$ for some k. We write the set of all nilpotent elements as $\mathrm{Nil}(A)$.

Proposition 1.19. $\mathrm{Nil}(A)$ is an ideal.

Proof. If $x \in \mathrm{Nil}(A)$, then $ax \in \mathrm{Nil}(A)$ for all $a \in A$, since $(ax)^k = a^k x^k = 0$. It remains to show $\mathrm{Nil}(A)$ is additively closed. Let $x, y \in \mathrm{Nil}(A)$ such that $x^N = 0 = y^N$. Then

$$(x+y)^{N+M} = \sum_{0 \le k < N} \binom{N+M}{k} x^k y^{N+M-k} + \sum_{N \le k \le N+M} \binom{N+M}{k} x^k y^{N+M-k}.$$

Notice that in the first summand, $N + M - k \geq M$, hence $y^{N+M-k} = 0$ there and the summand vanishes. Likewise, in the second summand $k \geq N$ and so $x^k = 0$ there and the summand vanishes. So in total $(x+y)^{N+M} = 0$ as desired. □

Proposition 1.20. $A/\mathrm{Nil}(A)$ is reduced, i.e. it has no nonzero nilpotents.

Proof. If $\overline{0} = \overline{a}^N = \overline{a^N}$, then $a^n \in \mathrm{Nil}(A)$ so there exists some $m > 0$ such that $a^{nm} = 0$. But then a is nilpotent, so $\overline{a} = 0$. □

Proposition 1.21. $\mathrm{Nil}(A) = \bigcap\{\text{prime ideals}\}$.

Proof 1. For the forward inclusion, let $x \in \mathrm{Nil}(A)$. Then $x^N = 0$ for some N. But 0 is an element of every prime ideal. Hence x^N is in every prime ideal, hence x is.

For the reverse direction, consider the inclusions

$$A \longrightarrow A[x] \longrightarrow A[[x]].$$

By Proposition 1.40, if we have prime ideal $\mathfrak{q} \subset A[X]$, then its pullback in A, which is $A \cap \mathfrak{q}$, is prime in A. Now suppose $a \in \bigcap \mathrm{Spec}(A)$. Then in particular a is in all prime ideals of the form $A \cap \mathfrak{q}$, so $a \in \mathfrak{q}$ for any prime ideal $\mathfrak{q} \subset A[X]$. So then $1 - aX$ is in no prime ideal of $A[X]$, for otherwise $1 - aX + aX = 1$ would be. Since maximal ideals are prime, $1 - ax$ is in no maximal ideal, hence $1 - ax$ is invertible in $A[X]$. We know what $(1-ax)^{-1}$ is mapped to in $A[[X]]$, since the inverse there is the formal power series $1 + aX + a^2X^2 + \cdots$. Since inverses are unique, and homomorphisms (which in our case is an inclusion) map inverses to inverses, it must be that this formal power series is in $A[X]$. But that is only possible if $a^N = 0$ for some N, i.e. the power series terminates at some finite degree. Hence $a \in \mathrm{Nil}(A)$. □

Proof 2. For the forward inclusion, do the same as the previous proof. For the reverse inclusion, we will prove the contrapositive, i.e. that if $x \notin \operatorname{Nil}(A)$ then $x \notin \bigcap \operatorname{Spec}(A)$. So suppose $x \notin \operatorname{Nil}(A)$. Then the set $S = \{1, x, x^2, \dots\}$ doesn't contain 0. Let Σ be the set of ideals in A avoiding S. This set is nonempty since $0 \in \Sigma$. Hence by Proposition 1.5, there is a prime ideal $\mathfrak{p}$ avoiding S. In particular, $x \notin \mathfrak{p}$, so $x \notin \bigcap \operatorname{Spec}(A)$. □

Since $\operatorname{Nil}(A)$ is the intersection of all prime ideals, we are led to the following similar definition:

Definition 1.22. The *Jacobson radical* of A is the set

$$J(A) \coloneqq \bigcap \operatorname{Spec}_m(A),$$

i.e. the intersection of all maximal ideals of A.

Corollary 1.23. $\operatorname{Nil}(A) \subset J(A)$.

Proof. Every maximal ideal is prime, so $J(A)$ is an intersection of a possibly smaller collection of prime ideals than $\operatorname{Nil}(A)$, hence contains $\operatorname{Nil}(A)$. □

Proposition 1.24. $x \in J(A)$ if and only if $1 - ax \in A^\times$ for all $a \in A$.

Proof. For the forard direction, let $x \in J(A)$. Then $ax \in J(A)$ for all $a \in A$, which means that ax is in every maximal ideal of A. But then $1 - ax$ is in no maximal ideal, for otherwise $1 - ax + ax = 1$ would be in that maximal ideal. This means that $1 - ax$ is invertible.

Conversely, suppose $1 - ax \in A^\times$ for all $a \in A$. Suppose to the contrary that $x \notin J(A)$. Then there exists a maximal ideal $\mathfrak{m}$ which doesn't contain x. By maximality, this must mean $\mathfrak{m} + (x) = A$, so $1 = m + ax$ for some $m \in \mathfrak{m}$, $a \in A$. But then $1 - ax = m \in \mathfrak{m}$, contradicting that $1 - ax$ is invertible. □

1.5 radicals

Nilpotent elements were ones whose powers were "eventually" 0. We can generalize this notion as follows:

Definition 1.25. Let $\mathfrak{a} \subset A$ be an ideal. The *radical* of $\mathfrak{a}$ is the ideal

$$\sqrt{\mathfrak{a}} \coloneqq \{x \in A : x^n \in \mathfrak{a} \text{ for some } n\}.$$

Corollary 1.26. $\sqrt{\mathfrak{a}}$ is indeed an ideal.

Proof. Consider the natural projection $\pi : A \to A/\mathfrak{a}$. Then $x^n \in \mathfrak{a}$ if and only if $\bar{x}^n = \bar{0}$, where the bar denotes the image in the quotient. But this is true if and only if $\bar{x} \in \operatorname{Nil}(A/\mathfrak{a})$, which we know is an ideal (Proposition 1.19). Thus $\sqrt{\mathfrak{a}}$ is the preimage of an ideal, hence an ideal (Proposition 1.39). □

Corollary 1.27. For a proper ideal $\mathfrak{a}$,

$$\sqrt{\mathfrak{a}} = \bigcap \{\mathfrak{p} \in V(\mathfrak{a}) : \mathfrak{p} \text{ is minimal over } \mathfrak{a}\}.$$

Example 1.28. $\mathrm{Nil}(A) = \sqrt{0}$.

For an ideal $\mathfrak{a} \subset A$, we will write

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supset \mathfrak{a}\},$$

i.e. $V(\mathfrak{a})$ is the set of prime ideals containing $\mathfrak{a}$.

Proposition 1.29. For an ideal $\mathfrak{a} \subset A$,

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}.$$

Proof. By the proof above, $\sqrt{a} = \pi^{-1}(\mathrm{Nil}(A/\mathfrak{a}))$. By (Proposition 1.21),

$$\pi^{-1}(\mathrm{Nil}(A/\mathfrak{a})) = \pi^{-1}(\bigcap \mathrm{Spec}(A/\mathfrak{a})).$$

By Propositions 1.42 and 1.40,

$$\pi^{-1}(\bigcap \mathrm{Spec}(A/\mathfrak{a})) = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}.$$

□

Proposition 1.30. Let $\mathfrak{a}, \mathfrak{b} \subset A$ be ideals.

1. (closure-like) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.
2. $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$.
3. $\sqrt{\mathfrak{a}} = A$ if and only if $\mathfrak{a} = A$.
4. $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$.
5. if $\mathfrak{p}$ is prime, then $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$.

Proof.

1. If $x \in \sqrt{\sqrt{\mathfrak{a}}}$, then $x^n = y$ for some $y \in \sqrt{\mathfrak{a}}$ and some n. But since $y \in \sqrt{\mathfrak{a}}$ there exists m such that $y^m \in \mathfrak{a}$. Then $x^{nm} \in \mathfrak{a}$, so $x \in \sqrt{\mathfrak{a}}$. Conversely, let $x \in \sqrt{\mathfrak{a}}$. Certainly $x^1 \in \sqrt{a}$, so $x \in \sqrt{\sqrt{\mathfrak{a}}}$.
2. t
3. t
4. prove

□

Corollary 1.31. Let $\mathfrak{a}, \mathfrak{b}$ be such that $\sqrt{\mathfrak{a}}, \sqrt{\mathfrak{b}}$ are coprime. Then $\mathfrak{a}$ and $\mathfrak{b}$ are coprime.

Proof. □ prove

1.6 quotient ideals

Definition 1.32. Let $\mathfrak{a} \subset A$ be an ideal, and $E \subset \mathfrak{a}$ a subset. Define

$$(\mathfrak{a} : E) \coloneqq \{a \in A : aE \subset \mathfrak{a}\}.$$

If $E = \{x\}$, we will use the shorthand $(\mathfrak{a} : x)$.

Corollary 1.33. $(\mathfrak{a} : E) \subset A$ is an ideal.

Proof. First consider the case $E = \{x\}$. Then $(\mathfrak{a} : x) = \mathrm{Ann}(\bar{x} \in A/\mathfrak{a})$ as an A-module, and since annihilators are ideal () it follows that $(\mathfrak{a} : x)$ is an ideal. For the general case, just observe ref

$$(\mathfrak{a} : E) = \bigcap_{x \in E} (\mathfrak{a} : x).$$

□

Example 1.34. The set of zero divisors on A is just

$$\bigcup_{x \neq 0} (0 : x).$$

1.7 extension and contraction

In what follows, let $f : A \to B$ be a ring homomorphism. Let $\mathfrak{a} \subset A$ be an ideal.

Example 1.35. $f(\mathfrak{a})$ is not always an ideal in B. For instance, consider the inclusion $f : \mathbb{Z} \to \mathbb{Q}$ and let $\mathfrak{a} \subset \mathbb{Z}$ be any nonzero ideal. Then for any $q \in \mathbb{Q} - \mathbb{Z}$, we have that $q\mathfrak{a} \not\subset \mathfrak{a}$.

As this example demonstrates, we need to "extend" the set $f(\mathfrak{a})$ if we want to obtain an ideal in B generally.

Definition 1.36. The *extension* of $\mathfrak{a}$, denoted $\mathfrak{a}^e$ or $Bf(a)$, is the ideal in B generated by $f(\mathfrak{a})$. Explicitly, it is the collection of finite sums $\sum_i y_i f(x_i)$, where $x_i \in \mathfrak{a}$ and $y_i \in B$.

Example 1.37. The extension of an ideal $I \subset A$ to A under the identity $A \to A$ is just I itself, since its elements are of the form

$$\sum_{k=1}^{n} i_k a_k$$

which is just all of I.

By Proposition 1.3, given ideals $I \subset J \subset A$, the extension of J to the ring A/I is equivalent to the quotient of abelian groups J/I (as A/I-modules).

Given an A-module M, the extension of an ideal $I \subset A$ to M, denoted IM, is the extension under the natural injection $A \to M$ sending $a \mapsto a \cdot 1$. It elements are thus of the form

$$\sum_{k=1}^{n} i_k m_k.$$

This is nothing but the abelian group generated by the product IM. We will often use the notation IM to represent this abelian group.

On the other hand, for an ideal $\mathfrak{b} \subset B$, it is always true that $f^{-1}(\mathfrak{a})$ is an ideal of A. In other words, the ideal structure on $\mathfrak{b}$ induces an ideal structure on $f^{-1}(\mathfrak{a})$. This is essentially because $f : A \to B$ is a homomorphism. Note however that f need not be surjective. In particular, it may be that for a proper inclusion of ideals $\mathfrak{b}_1 \subset \mathfrak{b}_2$ we have $f^{-1}(\mathfrak{b}_1) = f^{-1}(\mathfrak{b}_2)$. So in some sense we are potentially losing some information about $\mathfrak{b}$ by doing this operation (unless f is surjective onto $\mathfrak{b}$).

Definition 1.38. The *contraction* of $\mathfrak{b}$, denoted $\mathfrak{b}^c$, is the preimage $f^{-1}(\mathfrak{b})$.

Proposition 1.39. $\mathfrak{b}^c \subset A$ is an ideal.

Proof. Let $a_1, a_2 \in f^{-1}(\mathfrak{b})$. Then $f(a_1), f(a_2) \in \mathfrak{b}$ so $f(a_1) + f(a_2) = f(a_1 + a_2) \in \mathfrak{b}$, so $a_1 + a_2 \in f^{-1}(\mathfrak{b})$. Now let $a \in A$ and $a' \in f^{-1}(\mathfrak{b})$. Then $f(aa') = f(a)f(a') \in \mathfrak{b}$, so $aa' \in \mathfrak{b}$. □

Proposition 1.40. If $\mathfrak{b}$ is prime, then so is $\mathfrak{b}^c$.

Proof. Let $a_1, a_2 \in A$ and suppose $a_1 a_2 \in \mathfrak{b}^c$. Then $f(a_1 a_2) = f(a_1)f(a_2) \in \mathfrak{b}$, so either $f(a_1)$ or $f(a_2)$ is in $\mathfrak{b}$. Then either a_1 or a_2 is in $\mathfrak{b}^c = f^{-1}(\mathfrak{b})$. □

Example 1.41. If $\mathfrak{a} \subset A$ is prime, then $\mathfrak{a}^e \subset B$ need not be. Consider again the inclusion $f : \mathbb{Z} \to \mathbb{Q}$, and let $\mathfrak{a}$ be a nonzero ideal. Then $\mathfrak{a}^e = \mathbb{Q}$, which is not prime in $\mathbb{Q}$.

Now consider the following factorization of f:

$$A \xrightarrow{p} f(A) \xrightarrow{j} B.$$

We want to know what happens to ideals under these maps. It turns out that we know what happens with p, but the case of j is in general very hard.

Proposition 1.42. Fix an ideal $\mathfrak{a} \subset A$. There is a one-to-one, order-preserving correspondence

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{ideals} \\ \mathfrak{a} \subset \mathfrak{b} \subset A \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{ideals} \\ \overline{\mathfrak{b}} \subset A/\mathfrak{a} \end{array} \right\} \\ & \overline{\mathfrak{b}}^c \leftarrow \overline{\mathfrak{b}}. & \end{array}$$

Proof. We first claim $\mathfrak{a} \subset \overline{\mathfrak{b}}^c$. Let $a \in \mathfrak{a}$. Then $\pi(a) = 0 \in \overline{\mathfrak{b}}$, where π is the canonical projection onto the quotient.

Now we show injectivity. Suppose $\overline{\mathfrak{b}_1} \neq \overline{\mathfrak{b}_2}$. Then there exists $b \in \overline{\mathfrak{b}_1}$ which is not in $\overline{\mathfrak{b}_2}$. Let $a \in \pi^{-1}(b)$, which exists since π is surjective. Then also $a \in \overline{\mathfrak{b}_1}^c$, but $a \notin \overline{\mathfrak{b}_2}^c$.

Now we show surjectivity. Let $\mathfrak{a} \subset \mathfrak{b} \subset A$. It suffices to show $\pi(\mathfrak{b})$ is an ideal of $A/\mathfrak{a}$. Indeed, for $b_1 \in \pi(\mathfrak{b})$ and $b_2 \in A/\mathfrak{a}$, there exists $a_1 \in \mathfrak{b}$ and $a_2 \in A$ such that $\pi(a_1) = b_1$ and $\pi_(a_2) = b_2$. Then $a_1 a_2 \in \mathfrak{b}$, so $\pi(a_1 a_2) = \pi(a_1)\pi(a_2) = b_1 b_2 \in \pi(\mathfrak{b})$. It is also closed under addition. □

Returning to the factorization of f above, this proposition tells use exactly what happens to the ideals under p, for we can regard $f(A) \cong A/\ker(f)$.

Proposition 1.43.

1. $\mathfrak{a} \subset \mathfrak{a}^{ec}$ and $\mathfrak{b} \supset \mathfrak{b}^{ce}$.
2. $\mathfrak{a}^e = \mathfrak{a}^{ece}$ and $\mathfrak{b}^c = \mathfrak{b}^{cec}$.

Corollary 1.44. Extension and contraction form a (monotone?) Galois connection ().

ref

Corollary 1.45. There is a bijection

$$\left\{ \begin{matrix} \text{contracted} \\ \text{ideals in } A \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{extended} \\ \text{ideals in } B \end{matrix} \right\}$$
$$\mathfrak{a} \to \mathfrak{a}^e$$
$$\mathfrak{b}^c \leftarrow \mathfrak{b}.$$

1.8 products

We write out what a categorical product in the category of rings means explicitly:

Definition 1.46. The *product* of a family of rings $\{A_\alpha\}_\alpha$ is a ring P equipped with ring maps

$$\{\pi_\alpha : P \to A_\alpha\}_\alpha$$

called *projections* which is universal, i.e. given any ring R and any family of ring maps $\{f_\alpha : R \to A_\alpha\}_\alpha$, there exists a unique ring map $\tilde{f} : R \to P$ such that for all α the following diagram commutes:

$$\begin{tikzcd}
A_\alpha & P \arrow[l, "\pi_\alpha"'] \\
 & R \arrow[ul, "f_\alpha"] \arrow[u, dashed, "\tilde{f}"']
\end{tikzcd}$$

Note that the ring P is unique up to unique isomorphism, and so we can say an explicit construction of it is the usual product $\prod_\alpha A_\alpha$ with component-wise operations and projections.

A related question is whether we can determine a given ring is a product. Given a product ring $R = A_1 \times A_2$, consider the elements $e_1 = (1, 0)$ and $e_2 = (0, 1)$. These satisfy:

- (idempotent) $e_1^2 = e_1$ and $e_2^2 = e_2$
- (central) e_1, e_2 commute with all elements of R
- (orthogonal) $e_1 e_2 = 0$
- (complete) $e_1 + e_2 = 1$

Proposition 1.47. Let R be a (possibly noncommutative) ring. Let $\{e_1, e_2\}$ be a complete set of orthogonal central idempotents. Then $R \cong A_1 \times A_2$, where $A_i = Re_i$.

Proof. First we claim Re_1 and Re_2 are rings. We will work with Re_1, and the other case is analagous. First note that $e_1 \in Re_1$ acts as the unit. It contains the same 0 from R as well. It is closed under addition since $r_1e_1 + r_2e_1 = (r_1 + r_2)e_1$, and closed under multiplication since $r_1e_1 \cdot r_2e_1 = r_1r_2e_1^2 = r_1r_2e_1$, where we have used the fact that e_1 is central.

The map will be

$$\begin{aligned} R &\to Re_1 \times Re_2 \\ r &\mapsto (re_1, re_2). \end{aligned}$$

To see it is injective, suppose $(re_1, re_2) = (r'e_1, r'e_2)$. Then $re_1 = r'e_1$ and $re_2 = r'e_2$. So $(r-r')e_1 = 0$ and $(r-r')e_2 = 0$. Adding these together, $(r-r')(e_1+e_2) = 0$. But $e_1+e_2 = 1$ by assumption, and so $r = r'$.

To see it is surjective, consider an arbitrary element (r_1e_1, r_2e_2). Then it is the image of $r_1e_1 + r_2e_2$. □

Remark 1.48. Unlike above, neither A_i is a subring of R.

Proposition 1.49. If a commutative ring A has a nontrivial idempotent element (an element e other than 0 or 1 satisfying $e^2 = e$), then A decomposes as a product $A \cong A_1 \times A_2$ of two nontrivial rings.

The idea is to think of the idempotent element as a sort of projection, and in a sense decompose every element in A into its projected component and remainder.

Proof. We claim the map

$$\begin{aligned} \phi : A &\longrightarrow (e) \times A/(e) \\ a &\mapsto (ae, [a]) \end{aligned}$$

is a ring isomorphism, where $[a]$ is the class of a in the quotient.

We first show that it is unital. Under this map, $1_A \mapsto (e, [1])$. We claim this is a unit for $(e) \times A/(e)$. Indeed, any element in the product can be expressed as $(ae, [a'])$ for some $a, a' \in A$. Then

$$(e, [1]) \cdot (ae, [a']) = (ae^2, [a']) = (ae, [a']).$$

Now we will show it is a homomorphism:

$$\phi(a_1+a_2) = ((a_1+a_2)e, [a_1+a_2]) = (a_1e+a_2e, [a_1]+[a_2]) = \phi(a_1)+\phi(a_2).$$
$$\phi(a_1a_2) = (a_1a_2e, [a_1a_2]) = (a_1a_2e^2, [a_1]\cdot[a_2]) = (a_1e, [a_1])\cdot(a_2e, [a_2]) = \phi(a_1)\phi(a_2).$$

To see that it is injective, suppose $\phi(a) = (0,0)$. On the one hand, it must be $ae = 0$, so a is a zero divisor of e. On the other hand, it must be that $a \in (e)$, and so $a = a'e$ for some $a' \in A$. But then $ae = 0 = a'e^2 = a'e$, and so a' is also a zero divisor for e. Hence $a = a'e = 0$. This shows $\ker(\phi)$ is trivial, and so ϕ is injective.

To see that it is surjective, consider an arbitrary element $(ae, [a']) \in (e) \times A/(e)$. Then

$$\phi(ae - a' + a'e) = (ae - a'e + a'e^2, [ae - a' + a'e]) = (ae, [a'])$$

as desired. □

Theorem 1.50 (Chinese remainder theorem)**.** Let $I, J \subset A$ be coprime ideals[2]. Then $IJ = I \cap J$ and

$$A/IJ \cong A/I \times A/J.$$

Proof. First we will show $IJ = I \cap J$. Since elements of IJ are finite sums of the form $\sum_n c_n d_n$ for $c_n \in I$ and $d_n \in J$, we see that $IJ \subset I \cap J$. For the other direction, let $x \in I \cap J$. Since I and J are coprime, there exist $c \in I$ and $d \in J$ such that $c + d = 1$. Then $x = x(c+d) = cx + dx \in IJ$.

Now we will demonstrate the isomorphism. Consider the map

$$A \to A/I \times A/J$$
$$a \mapsto (\bar{a}, \bar{a})$$

sending a to its image in the respective quotients. Then the kernel of this map is the set of a such that $a = 0$ in both A/I and A/J. By definition of the quotient this only happens if $a \in I$ and $a \in J$ respectively, i.e. $a \in I \cap J = IJ$. If we can show that the map is also surjective, then we are done by the first isomorphism theorem. Since I and J are coprime, an arbitrary element in A/I can be expressed as $[d_1] = d_1 + c_1$ and an arbitrary element in A/J can be expressed as $[c_2] = c_2 + d_2$ for some $c_1, c_2 \in I$ and $d_1, d_2 \in J$. Then $c_2 + d_1 \mapsto ([d_1], [c_1])$ as desired. □

2 modules

The following theorem and its corollaries will be collectively referred to as "Nakayama's lemma"[3]. The base assumption for these will be that M is a finitely generated A-module, and $I \subset A$ is an ideal contained in $J(A)$.

[2] i.e. $I + J = A$

[3] apparently Nakayama himself wasn't fond of this name!

Theorem 2.1 (Nakayama's lemma)**.** Let $I \subset A$ be an ideal contained in $J(A)$. Let M be a finitely generated A-module. If $IM = M$, then $M = 0$.

Proof. Suppose $M \neq 0$. Let $\{x_1, \ldots, x_n\}$ be a minimal generating set for M. Then $x_n \in M = IM$, so

$$x_n = a_1x_1 + \cdots + a_nx_n$$

for some $a_i \in I \subset J(A)$. Subtracting a_nx_n, we get that

$$(1 - a_n)x_n = a_1x_2 + \cdots a_{n-1}x_{n-1}.$$

But since $a_n \in J(A)$, by Proposition 1.24 we know $1 - a_n \in A^\times$, so

$$x_n = (1 - a_n)^{-1}a_1x_1 + \cdots + (1 - a_n)^{-1}a_{n-1}x_{n-1},$$

violating the minimality of the generators $x_1, \ldots, x_n$. □

Corollary 2.2. Let M be a finitely generated A-module, $M' \subset M$ a submodule, and $I \subset A$ an ideal contained in $J(A)$. If $M' + IM = M$, then $M' = M$.

Proof. Note that $I(M/M') = (IM)/M' = (IM + M')/M' = M/M'$, where the last equality is our hypothesis. M/M' is finitely generated since M is, and so by Nakayama's lemma $M/M' = 0$, i.e. $M = M'$. □

Corollary 2.3. Let M be a finitely generated A-module, and let $I \subset A$ be an ideal contained in $J(A)$. Then a subset

$$\{x_1, \ldots x_n\} \subset M$$

generates M if and only if its image in the quotient

$$\{\bar{x_1}, \ldots, \bar{x_n}\} \subset M/IM$$

generates M/IM.

Proof. The forward direction is always true (). ref

For the reverse direction, suppose $\{\bar{x_1}, \ldots, \bar{x_n}\}$ generates M/IM. Consider the submodule

$$M' = Ax_1 + \cdots + Ax_n \subset M$$

(choosing x_i to be some representative in M of the class $\bar{x_i}$). It suffices to show that $M' = M$. By hypothesis, the composite map

$$M' \longrightarrow M \longrightarrow M/IM$$

is surjective, where the first map is the natural inclusion and the second is the natural projection. It's image is $(M' + IM)/IM$, and since it is surjective we have that $(M' + IM)/IM = M/IM$, i.e. $M' + IM = M$. Then Nakayama's lemma (Corollary 2.2) says $M = M'$. □

Remark 2.4. This result tells us that a (finite) generating set on a submodule pulls back to a generating set on the whole module *provided we know beforehand* that the whole module is finitely generated.

2.1 tensor product

Let M be a right R-module and N be a left R-module, over a not-necessarily-commutative ring R. Let A be an abelian group.

The tensor product can be thought of as the "universal multiplication", in the sense that any map $M \times N \to A$ which behaves like multiplication uniquely factors through the tensor product. In particular, the map $M \times N \to M \otimes_R N$ is itself multiplication map, and the induced map is linear.

First let's be precise about what a "multiplication map" should look like. One might propose the following:

Definition 2.5. A map $M \times N \to A$ is called *R-bilinear* if it is

- (biadditive)

$$\begin{aligned} \mu(m+m',n) =&\mu(m,n)+\mu(m',n) \\ \mu(m,n+n') =&\mu(m,n)+\mu(m,n') \end{aligned}$$

- (R-balanced)

$$\mu(mr,n)=\mu(m,rn)$$

We will construct an abelian group $M \otimes_R N$, the tensor product, equipped with an R-bilinear map $M \times N \to M \otimes_R N$, which is universal in the following sense: Given any abelian group A and any R-bilinear map $\mu : M \times N \to A$, there exists a unique abelian group map (i.e. linear map) $\tilde{\mu} : M \otimes_R N \to A$ such that the following diagram commutes:

$$\begin{tikzcd} M \times N \arrow[r, "\otimes"] \arrow[rd, "\mu"'] & M \otimes_R N \arrow[d, dashed, "\tilde{\mu}"] \\ & A \end{tikzcd}$$

2.1.1 construction

We will now construct the tensor product $M \otimes_R N$. This is occassionally useful, but it's main utility is to show that the tensor product actually exists. As will become apparant, $M \otimes_R N$ is a quotient of an unwieldy group under an unwieldy collection of relations.

Consider the free abelian group generated by $M \times N$, denoted $F_{\mathbb{Z}}(M \times N)$. This is the direct sum of copies of $\mathbb{Z}$, one for each element in $M \times N$:

$$F_{\mathbb{Z}}(M \times N) = \bigoplus_{\alpha \in M \times N} \mathbb{Z}.$$

This abelian group is generated by elements of the form $e_{(m,n)}$, which is the tuple with 0's in all coordinates except the one corresponding the $\alpha = (m, n)$.

At the moment the natural map

$$M \times N \to F_{\mathbb{Z}}(M \times N)(m,n) \mapsto e_{(m,n)}$$

is not R-bilinear. We can essentially force it to become R-bilinear by considering the subgroup J generated by elements of the form

$$e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}$$
$$e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}$$
$$e_{(mr,n)} - e_{(m,rn)}.$$

We call the quotient $F_{\mathbb{Z}}(M \times N)/J$ as the tensor product, and write it as $M \otimes_R N$. The induced map

$$\otimes : M \times N \to F_{\mathbb{Z}}(M \times N) \to F_{\mathbb{Z}}(M \times N)/J = M \otimes_R N$$
$$(m,n) \mapsto e_{(m,n)} \mapsto [e_{(m,n)}] = m \otimes n$$

is then R-bilinear.

Corollary 2.6. Elements of the form $m \otimes n$ generate $M \otimes_R N$. Such elements are called *elementary tensors.*

Corollary 2.7. $m \otimes 0 = 0 \otimes n = 0$.

Let us check that $(M \otimes_R N, \otimes)$ is universal. Let $\mu : M \times N \to A$ be an R-bilinear map into an abelian group. Consider the following diagram:

$$\begin{tikzcd}
F_{\mathbb{Z}}(M \times N) \arrow[r, "\pi"] \arrow[dr, "\mu"] & M \otimes_R N \arrow[d, dashed, "\tilde{\mu}"] \\
M \times N \arrow[u, "i"] \arrow[r, "\mu"'] & A
\end{tikzcd}$$

finish

It is not true in general that a element which is zero in a tensor product of modules descends to 0 in a tensor product of their submodules. However, there will always exist *some* pair of submodules to which the element descends to 0 in their tensor product. Explicitly:

Example 2.8. Let $A = \mathbb{Z}$, and consider the A-modules $M = \mathbb{Z}$ and $N = \mathbb{Z}/2\mathbb{Z}$, with their respective submodules $M' = 2\mathbb{Z}$ and $N' = N$. Then the element $2 \otimes 1$ is zero in $M \otimes N$, since $2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0$. However it is not zero in $M' \otimes N'$. First of all, we can't factor out the two since $1 \notin M'$. In fact, $2 \otimes 1$ generates $M' \otimes N'$, since any elementary tensor in it has the form $(2k, x)$. If $x = 1$, then $(2k, x) = k(2 \otimes x)$. If $x = 0$, then $(2k, x) = 2k(2 \otimes x)$.

Corollary 2.9. If $x_i \in M$, $y_i \in N$ are such that $\sum x_i \otimes y_i = 0$ in $M \otimes N$, then there exist finitely generated submodules M_0, N_0 such that $\sum x_i \otimes y_i = 0$ in $M_0 \otimes N_0$.

Proof. based on construction of tensor product □ it

Lemma 2.10 (functoriality)**.** Given a map $f : M \to M'$ between R-modules, there is an induced map

$$f \otimes 1_N : M \otimes N \to M' \otimes N$$

$$m \otimes n \mapsto f(m) \otimes n.$$

In the other direction too:

$$1_N \otimes f : N \otimes M \to N \otimes M'$$
$$n \otimes m \mapsto n \otimes f(m).$$

(we need to be careful about left/right modules if R is not commutative.)

Proof. It suffices to show that the map

$$\phi : M \times N \to M' \times N$$
$$(m, n) \mapsto f(m) \otimes n$$

is R-bilinear. To see it is biadditive:

$$\phi(m + m', n) = f(m + m') \otimes n = (f(m) + f(m')) \otimes n = \phi(m, n) + \phi(m', n),$$
$$\phi(m, n + n') = f(m) \otimes (n + n') = f(m) \otimes n + f(m) \otimes n' = \phi(m, n) + \phi(m, n').$$

To see it is balanced:

$$\phi(mr, n) = f(m)r \otimes n = f(m) \otimes rn = \phi(m, rn).$$

Hence the induced map is well-defined.

The other direction is analagous. □

2.1.2 useful identities

Proposition 2.11. Let R be a not-necessarily-commutative ring, let $I \subset R$ be a two-sided ideal, and let M be a left R-module. Then

$$R/I \otimes_R M \cong M/IM$$
$$\bar{r} \otimes m \mapsto \overline{rm}$$

Proof. Let us first check that the forward map $R/I \otimes_R M \to M/IM$ is well-defined. Based on the construction of the tensor product, it suffices to show that the map

$$\mu : R/I \times M \to M/IM(\bar{r}, m) \mapsto \overline{rm}$$

is R-bilinear.

First we will check that this is well-defined and additive in $\bar{r}$. So fix m, and consider the map

$$f_m : R \to M/IMr \mapsto \overline{rm}.$$

If $r \in I$, then $\overline{rm} = 0$ since then $rm \in IM$. So $f_m|_I = 0$, so we get a well-defined map on the quotient $\bar{f_m} : R/I \to M/IM$. No let us see that this map is additive. Indeed,

$$\overline{r_1 + r_2} \mapsto \overline{(r_1 + r_2)m} = \overline{r_1 m + r_2 m} = \overline{r_1 m} + \overline{r_2 m},$$

since taking equivalence classes is a homomorphism.

Now we will check that this is well-defined and additive in m. For well-defined, fix $\bar{r}$. Then if $\overline{rm_1} \neq \overline{rm_2}$ in M/IM then $rm_1 \neq rm_2 \in M$, and so $m_1 \neq m_2$. For additivity, the same argument as above works on m instead of r.

Thus the map is biadditive. It remains to show that it is R-balanced. Calling the map ϕ, we calculate

$$\phi(\bar{r}r' \otimes m) = \phi(\bar{rr}' \otimes m) = \overline{rr'm} = \phi(\bar{r}, r'm).$$

We thus have an induced map of abelian groups

$$\begin{gathered} f : R/I \otimes_R M \to M/IM \\ \bar{r} \otimes m \mapsto \overline{rm} \end{gathered}$$

In order to show this is an isomorphism, we can construct an inverse map. Consider the map

$$\begin{gathered} g : M \mapsto R/I \otimes_R M \\ m \mapsto \bar{1} \otimes m. \end{gathered}$$

To see this is well defined, suppose $\bar{1} \otimes m_1 \neq \bar{1} \otimes m_2$. Then $g(m_1 - m_2) = \bar{1} \otimes (m_1 - m_2) \neq 0$. Then $m_1 \neq m_2$, for otherwise $g(m_1 - m_2) = g(0) = \bar{1} \otimes 0 = 0$. Additivity follows by the bilinearity of the tensor product. Now note that if $m \in IM$, then we may write $m = im'$ adn then $\bar{1} \otimes m = i(\bar{1} \otimes m') = 0 \otimes m' = 0$, hence g vanishes on IM. Thus we get an induced map

$$\bar{g} : M/IM \to R/I \otimes_R M \bar{m} \mapsto \bar{1} \otimes m.$$

We check our constructed maps are inverses:

$$\begin{gathered} g(f(\bar{r} \otimes m)) = g(\overline{rm}) = \bar{1} \otimes rm = \bar{r} \otimes m, \\ f(g(\bar{m})) = f(\bar{1} \otimes m) = \overline{1 \cdot m} = \bar{m}. \end{gathered}$$

□

Corollary 2.12.

$$\begin{gathered} M \otimes N \xrightarrow{\sim} N \otimes M \\ m \otimes n \mapsto n \otimes m \end{gathered}$$

Corollary 2.13.

$$\begin{gathered} R \otimes_R R \xrightarrow{\sim} R \\ r_1 \otimes r_2 \mapsto r_1 r_2 \end{gathered}$$

Corollary 2.14. $R/I \otimes R/J \cong \frac{R}{I+J}$.

Proof. We know $R/I \otimes R/J \cong (R/J)/(I(R/J))$. By Corollary 1.4, $I(R/J) = (I+J)/J$. Hence

$$R/I \otimes R/J \cong \frac{R/J}{I(R/J)} \cong \frac{R/J}{(I+J)/J} \cong \frac{R}{I+J},$$

where the last isomorphism is the third(?) isomorphism theorem. □

Proposition 2.15. Let M be a right R-module, let N be an (R,S)-bimodule[4], and let P be a left S-module. The there is a natural isomorphism

$$(M \otimes_R N) \otimes_S P \xrightarrow{\sim} M \otimes_R (N \otimes_S P)$$
$$(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p).$$

Proof. We are done if we can find an S-bilinear map $(M \otimes_R N) \times P \to M \otimes_R (N \otimes_S P)$ and show it is an isomorphism. However we should always be weary of trying to define maps directly out of a tensor product, since it is hard to show they are well-defined. Instead we would like for such maps to be induced:

Fixing P, consider the map

$$\mu_p : M \times N \to M \otimes_R (N \otimes_S P)$$
$$(m,n) \mapsto m \otimes (n \otimes p).$$

Let us check this is R-bilinear. Indeed,

$$\mu_p(m+m',n) = (m+m') \otimes (n \otimes p) = m \otimes (n \otimes p) + m' \otimes (n \otimes p) = \mu_p(m,n) + \mu_p(m',n),$$
$$\mu_p(m,n+n') = m \otimes ((n+n') \otimes p) = m \otimes (n \otimes p + n' \otimes p) = \mu_p(m,n) + \mu_p(m,n')$$

so it is biadditive. To see it is balanced:

$$\mu_p(mr,n) = mr \otimes (n \otimes p) = m \otimes r(n \otimes p) = m \otimes (rn \otimes p) = \mu_p(m,rn).$$

Thus μ_p is R-bilinear, and so we get an induced map

$$\tilde{\mu_p} : M \otimes_R N \to M \otimes_R (N \otimes_S P)$$
$$m \otimes n \mapsto m \otimes (n \otimes p).$$

Now define a map

$$\phi : (M \otimes_R N) \times P \to M \otimes_R (N \otimes_S P)$$
$$(\xi, p) \mapsto \tilde{\mu_p}(\xi).$$

Let's check this is S-bilinear. To check it is biadditive:

$$\phi(\xi + \xi', p) = \tilde{\mu_p}(\xi + \xi') = \tilde{\mu_p}(\xi) + \tilde{\mu_p}(\xi') = \phi(\xi,p) + \phi(\xi',p),$$

[4] i.e. a left R-module and right S-module such that the two multiplications are compatible: $(rn)s = r(ns)$

$$\phi(\xi, p+p') = \tilde{\mu_{p+p'}}(\xi) = \sum_{k=1}^{n} m_k \otimes (n_k \otimes (p+p')) = \phi(\xi, p) + \phi(\xi, p').$$

To check it is balanced:

$$\phi(\xi s, p) = \tilde{\mu_p}(\xi s) = \sum_{k=1}^{n} m_k \otimes (n_k s \otimes p) = \tilde{\mu_{sp}}(\xi) = \phi(\xi, sp).$$

Hence it is S-bilinear, and the map

$$\begin{gathered}\tilde{\phi} : (M \otimes_R N) \otimes_S P \to M \otimes_R (N \otimes_S P) \\ (m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)\end{gathered}$$

is well-defined.

It remains to show $\tilde{\phi}$ is an isomorphism. To do so, one may analagously construct a map going in the other direction, and repeat the above procedure to show it is well-defined and sends $m \otimes (n \otimes p) \mapsto (m \otimes n) \otimes p$. Since such elements generate, this will suffice. □

Proposition 2.16.

$$M \otimes_R (\coprod_\alpha N_\alpha) \cong \coprod_\alpha (M \otimes_R N_\alpha).$$

Proof. There are the universal properties at play here: that of the tensor product and that of the coproduct. We will need one to define the forward map and one to define the reverse map.

First we will define the forward map. Consider the map

$$\begin{gathered}f : M \times (\coprod_\alpha N_\alpha) \cong \coprod_\alpha (M \otimes_R N_\alpha) \\ (m, (n_\alpha)_\alpha) \mapsto (m \otimes n_\alpha)_\alpha.\end{gathered}$$

Let us check this is R-bilinear. To see it is biadditive:

$$\begin{gathered}f(m+m', (n_\alpha)_\alpha) = ((m+m') \otimes n_\alpha)_\alpha = (m \otimes n_\alpha + m' \otimes n_\alpha)_\alpha = f(m, (n_\alpha)_\alpha) + f(m', (n_\alpha)_\alpha), \\ f(m, ((n_\alpha + n'_\alpha)_\alpha) = (m \otimes n_\alpha + m \otimes n'_\alpha)_\alpha = f(m, (n_\alpha)_\alpha) + f(m, (n'_\alpha)_\alpha).\end{gathered}$$

To see it is balanced:

$$f(mr, (n_\alpha)_\alpha) = (mr \otimes n_\alpha)_\alpha = (m \otimes rn_\alpha)_\alpha = f(m, (rn_\alpha)_\alpha).$$

Hence we have an induced map

$$\begin{gathered}M \otimes (\coprod_\alpha N_\alpha) \to \coprod_\alpha (M \otimes_R N_\alpha) \\ (m, (n_\alpha)_\alpha) \mapsto (m \otimes n_\alpha)_\alpha.\end{gathered}$$

For the other direction, the natural inclusion maps $1_M \otimes i_a : M \otimes_R N_a \to M \otimes_R (\coprod_\alpha N_\alpha)$, which are well-defined by the functoriality of the tensor product (Lemma 2.10), induce a unique map g

$$\begin{tikzcd}
M \otimes_R N_a \arrow[r, "i_a"] \arrow[dr, "1_M \otimes i_a"'] & \coprod_\alpha (M \otimes_R N_\alpha) \arrow[d, dashed, "g"] \\
 & M \otimes_R (\coprod_\alpha N_\alpha)
\end{tikzcd}$$

which evidently sends $(m \otimes n_\alpha)_\alpha \mapsto (m \otimes (n_\alpha)_\alpha)$ as desired. □

Proposition 2.17. Let M, N, P be A-modules. Then there are the following unique isomorphisms:

1. $$M \otimes N \xrightarrow{\sim} N \otimes M$$ $$m \otimes n \mapsto n \otimes m$$

2. $$(M \otimes N) \otimes P \xrightarrow{\sim} M \otimes N \otimes P \xrightarrow{\sim} M \otimes (N \otimes P)$$ $$(m \otimes n) \otimes p \mapsto m \otimes n \otimes p \mapsto m \otimes (n \otimes p)$$

3. $$(M \oplus N) \otimes P \xrightarrow{\sim} (M \otimes P) \oplus (N \otimes P)$$ $$(m \otimes n) \otimes p \mapsto (m \otimes p, n \otimes p)$$

4. $$A \otimes M \xrightarrow{\sim} M$$ $$a \otimes m \mapsto am$$

Proof. Use universal property... □ this

2.1.3 of algebras

Proposition 2.18. If A and B are k-algebras, then $A \otimes_k B$ is a k-algebra with respect to the multiplication

$$a \otimes b \cdot a' \otimes b' = aa' \otimes bb'.$$

Proof. The tricky part, as is always the case when defining maps out of a tensor product, is whether multiplication as defined above is well defined. We see this as follows: Consider the map

$$A \times B \times A \times B \to A \otimes_k B$$

$$(a, b, a', b') \mapsto aa' \otimes bb'.$$

One checks this is k-multilinear, hence there is an induced map

$$A \otimes_k B \otimes_k A \otimes_k B = (A \otimes_k B) \otimes_k (A \otimes_k B) \to A \otimes_k B.$$

By the universal property in the other direction, this must correspond to a k-bilinear map

$$\mu : (A \otimes_k B) \times (A \otimes_k B) \to A \otimes_k B.$$

Since this should agree with our original map, we have

$$\mu(a \otimes b, a' \otimes b') = aa' \otimes bb'$$

as desired. □

Corollary 2.19. The natural embeddings $A \to A \otimes_k B$ and $B \to A \otimes_k B$ are k-algebra maps.

Theorem 2.20. If A, B are k-algebras, then $A \otimes_k B$ satisfies the following universal property: given any algebra homomorphisms $f_A : A \to C$ and $f_B : A \to C$ such that the images of f_A and f_B commute in C, there exists a unique algebra homomorphism $\tilde{f} : A \otimes_k B \to C$ making the following diagram commute:

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[dr, "f_A"'] & A \otimes_k B \arrow[d, dashed, "\tilde{f}"] & B \arrow[l, "i_B"'] \arrow[dl, "f_B"] \\
& C &
\end{tikzcd}$$

Proof. We employ the typical strategy in proving universal properties: first uniqueness, then existence (because uniqueness will often tell us how to define the map).

Let us show the uniqueness of $\tilde{f}$. So suppose it exists. Then

$$\begin{aligned}
\tilde{f}(a \otimes b) =& \tilde{f}(a \otimes 1 \cdot 1 \otimes b) = \tilde{f}(a \otimes 1)\tilde{f}(1 \otimes b) \\
=& \tilde{f}(i_A(a))\tilde{f}(i_B(b)) = f_A(a)f_B(b).
\end{aligned}$$

So any map in place of $\tilde{f}$ making the diagram commute must be precisely $f_A(a)f_B(b)$, which shows uniqueness.

Now let us show existence. Consider the map

$$\begin{gathered}
A \times B \to C \\
(a, b) \mapsto f_A(a)f_B(b).
\end{gathered}$$

One checks this is k-bilinear. Thus there exists a k-module map $\tilde{f} : A \otimes_k B \to C$ sending $a \otimes b \mapsto f_A(a)f_B(b)$. It remains to check this is an algebra map:

$$\begin{aligned}
\tilde{f}(a \otimes b \cdot a' \otimes b') =& \tilde{f}(aa' \otimes bb') = f_A(aa')f_B(bb') \\
=& f_A(a)f_A(a')f_B(b)f_B(b') = f_A(a)f_B(b)f_A(a')f_B(b') \\
=& \tilde{f}(a \otimes b)\tilde{f}(a' \otimes b'),
\end{aligned}$$

where we have used the fact that the images of f_A and f_B commute. □

Remark 2.21. This implies that $A \otimes_k B$ is the coproduct in the category of commutative k-algebras.

Remark 2.22. If we are trying to get an algebra map out of the tensor product, we don't need to get a bilinear map or show there is a module map first: we can just directly check the universal property. In this sense getting an algebra map is perhaps easier than getting a module one (assuming now that we are working with modules instead of algebras, so that the algebra map doesn't exist and hence can't just descend to a module map).

2.1.4 adjointness

Let k be a commutative ring.

By the universal property, k-linear maps $V \otimes_k W \to X$ correspond to bilinear maps $V \times W \to X$. By Currying, these may be regarded as linear maps $V \to \mathrm{Hom}_k(W, X)$. Hence:

$$\mathrm{Hom}_k(V \otimes_k W, X) \cong \mathrm{Hom}_k(V, \mathrm{Hom}_k(W, X)).$$

More generally, given a not-neccessarily-commutative rings R, S, and given a right R-module N, a left S-module P, and an (R, S)-bimodule M we have

$$\mathrm{Hom}_S(N \otimes_R M, P) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_S(M, P)).$$

2.1.5 base change

Given a map $\phi : A \to B$ of rings, any B-module N becomes can be regarded as an A module via pullback along ϕ: for any $a \in A$, define $aN = \phi(a)N$. This defines a functor

$$\mathrm{res} : B\mathrm{Mod} \to A\mathrm{Mod}$$

called *restriction of scalars*, perhaps inspired by the special case when ϕ is an inclusion map.

We might ask if, given an A-module M, we can somehow push it forward to a B-module, and in such a way that is compatible with restricting scalars. Indeed we can, be sending $M \mapsto B \otimes_A M$, which we call *extension of scalars.*

Proposition 2.23. Let M be a left A-module. Then the map

$$\begin{aligned} \mathrm{ex} : M &\to B \otimes_A M \\ m &\mapsto 1 \otimes m \end{aligned}$$

is the universal map of M to a B-module: given any B-module N (viewed as an A module via restriction of scalars) and any A-module map $f : M \to N$, there exists a unique map $\tilde{f} : B \otimes_A M \to N$ making the following diagram commute:

$$\begin{tikzcd} & B \otimes_A M \arrow[dd, dashed, "\tilde{f}"] \\ M \arrow[ur, "i"] \arrow[dr, "f"'] & \\ & N \end{tikzcd}$$

2.2 misc

Definition 2.24. The *annihilator* of an A-module M, denoted $\mathrm{Ann}_A(M)$, is the set of elements $a \in A$ such that $am = 0$ for all $m \in M$.

Definition 2.25. A module is called *faithful* if it's annihilator is just 0, i.e. it has no nontrivial annihilators.

Proposition 2.26. Let $A \subset B$ be a ring extension. If N is finitely generated as a B-module, say by $\{x_1, \dots, x_r\}$, and B is finitely-generated as an A-module, say by $\{b_1, \dots, b_k\}$, then N is finitely-generated as an A-module, by $\{b_i x_j\}$.

$$\begin{tikzcd} N \arrow[d, dash, "<\infty"'] \arrow[dd, dash, bend left, "<\infty"] \\ B \arrow[d, dash, "<\infty"'] \\ A \end{tikzcd}$$

3 localization

3.1 of rings

3.1. This construction is a generalization of taking the field of fractions of a domain. We recall it here. Let A be a domain, and let $F = \mathrm{Frac}(A)$. We may explicitly construct F as follows:

Let $S = A - \{0\}$. Define an equivalence relation on $A \times S$ by

$$(a, s) \sim (a', s') \text{ if } s'a = sa'.$$

We write $\frac{a}{s}$ for the equivalence class of (a, s) in $A \times S/\sim$. Ring operations are defined in the natural way:

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'},$$
$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'},$$
$$1_F = \frac{1}{1}.$$

Of course, this only is well-defined if $\sim$ is actually an equivalence relation. The subtlety, and indeed where we use the fact that A is a domain, is in showing transitivity:

$$(a, s) \sim (a', s') \Rightarrow s'a = sa' \Rightarrow s''s'a = s''sa',$$
$$(a', s') \sim (a'', s'') \Rightarrow s''a' = s'a'' \Rightarrow ss''a' = ss'a''.$$

The last terms above are equal:

$$s''s'a = s''sa' = ss''a' = ss'a''.$$

But to show $(a,s) \sim (a'',s'')$, we need to somehow cancel the s' terms on the ends of the equality. We can do this because we are in an integral domain (). Thus $s''a = sa''$ and $(a,s) \sim (a'',s'')$ as desired.

ref

This might suggest the generalization: we should weaken $\sim$ so that $(a,s) \sim (a'',s'')$ if there exists another element $s' \in S$ such that $s'(s''a) = s'(sa'')$.

3.2. The field of fractions $F = \mathrm{Frac}(A)$ also satisfies a certain universal property: given any ring B and any ring homomorphism $f : A \to B$ such that $f(S) \subset B^\times$, there exists a unique $\tilde{f} : F \to B$ making the following diagram commute:

$$\begin{tikzcd}
A \arrow[r, "\iota"] \arrow[dr, "f"'] & \mathrm{Frac}(A) \arrow[d, dashed, "\tilde{f}"] \\
 & B
\end{tikzcd}$$

So F is the universal construction which makes the elements in S invertible.

3.3. The idea now is the following. Let A be a (commutative) ring, and $S \subset A$ a multiplicative set. If S does not have 1, we may just include it since it doesn't change anything else about S. We want to construct a ring $S^{-1}A$ and a ring map $\iota : A \to S^{-1}A$ that has the above universal property. The following construction, attributed to Uzkov, achieves this:

Define an equivalence relation $\sim$ on $A \times S$ as follows:

$$(a,s) \sim (a',s') \text{ if there exists } t \in S \text{ such that } ts'a = tsa'.$$

One checks properties as in the field of fractions case, and we will cover the case of transitivity now. Suppose $(a,s) \sim (a',s')$ and $(a',s') \sim (a'',s'')$. Then there exist $t,u \in S$ such that

$$\begin{gathered}
ts'a = tsa' \Rightarrow s''(ts'a) = s''(tsa') \Rightarrow u(s''ts'a) = u(s''tsa'), \\
us''a' = us'a'' \Rightarrow s(us''a') = s(us'a'') \Rightarrow t(sus''a') = t(sus'a'').
\end{gathered}$$

So

$$\begin{gathered}
us''ts'a = us''tsa' = tsus''a' = tsus'a'', \\
(uts')(s''a) = (uts')(sa'').
\end{gathered}$$

Since $uts' \in S$, this shows $(s,a) \sim (s'',a'')$ as desired.

We have thus defined a map

$$\begin{aligned}
\iota : A &\to S^{-1}A \\
a &\mapsto \frac{a}{1}
\end{aligned}$$

where $S^{-1}A$ is the above construction $A \times S/\sim$.

Definition 3.4. The ring $S^{-1}(A)$ is called the *localization* of the ring A.

Remark 3.5.

- If S contains nilpotents, then $S^{-1}A = 0$ since if we let x be a nilpotent then $\frac{0}{1} = \frac{x}{1} = \frac{1}{1}$.
- If S has zero divisors then $A \to S^{-1}A$ won't be injective. In fact we can write the kernel explicitly:

$$\begin{aligned}\ker(\iota) =& \{a \in A : \frac{a}{1} = \frac{0}{1}\} = \{a \in A : sa = 0 \text{ for some } s \in S\} \\ =& \bigcup_{s\in S}(0 : s) = \bigcup_{s \in S} \mathrm{Ann}(s).\end{aligned}$$

Proposition 3.6. The map

$$\begin{aligned}\iota : A &\to S^{-1}A \\ a &\mapsto \frac{a}{1}\end{aligned}$$

is universal in the sense of (3.2): given any ring B and any ring homomorphism $f : A \to B$ such that $f(S) \subset B^\times$, there exists a unique $\tilde{f} : S^{-1}A \to B$ making the following diagram commute:

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[dr, "f"'] & S^{-1}A \arrow[d, dashed, "\tilde{f}"] \\ & B \end{tikzcd}$$

Proof. We begin as usual with uniqueness:

$$\begin{aligned}\tilde{f}(\frac{a}{s}) =& \tilde{f}(\frac{a}{1} \cdot (\frac{s}{1})^{-1}) = \tilde{f}(\frac{a}{1})\tilde{f}(\frac{s}{1})^{-1} \\ =& \tilde{f}(\iota(a))\tilde{f}(\iota(s))^{-1} = f(a)f(s)^{-1}.\end{aligned}$$

For existence, define $\tilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$. We check this is well-defined. Suppose $\frac{a}{s} = \frac{a'}{s'}$. Then there exists $t \in S$ such that

$$ts'a = tsa' \Rightarrow f(t)f(s')f(a) = f(t)f(s)f(a') \Rightarrow f(s')f(a) = f(s)f(a'),$$

since $f(t) \in B^\times$ by assumption. But also $f(s), f(s') \in B^\times$, so $f(a)f(s)^{-1} = f(a')f(s')^{-1}$. Thus $\tilde{f}(\frac{a}{s}) = \tilde{f}(\frac{a'}{s'})$ as desired.

The remaining properties are verified by the reader. □

Example 3.7.

1. Let A be a ring, $f \in A$ nonzero, and $S = \{1, f, f^2, \dots\}$. Then

$$S^{-1}A = \frac{A[X]}{(Xf - 1)}.$$

Note the quotient ideal is the relation $Xf = 1$, i.e. $X^n f^n = 1$, so we are forcing X^n to be the inverse of f^n. In this case, we will write

$$S^{-1}A = A[\frac{1}{f}] = A_f.$$

2. Let A be a ring, let $\mathfrak{p} \in \operatorname{Spec}(A)$, and let $S = A - \mathfrak{p}$. In this case we will write
$$S^{-1}A = A_{\mathfrak{p}}.$$
This notation leads to the somewhat confusing terminology: localization "at" the prime $\mathfrak{p}$ actually means localizing with respect to the *complement* of $\mathfrak{p}$.

Proposition 3.8. Let $\mathfrak{a} \subset A$ be an ideal. Then
$$S^{-1}\mathfrak{p} := \{\frac{a}{s} : a \in \mathfrak{p}, s \in S\} = \mathfrak{p}^e.$$
In particular, this implies the $S^{-1}\mathfrak{p}$ is an ideal.

Proof. To prove $(\subset)$, note that for $\frac{a}{s} \in S^{-1}\mathfrak{a}$ we have
$$\frac{a}{s} = \frac{1}{s} \cdot \frac{a}{1} = \frac{1}{s} \cdot \iota(a) \in \mathfrak{a}^e$$
since elements of $\mathfrak{a}^e$ are finite sums of elements in $\iota(\mathfrak{a})$.

To see $(\supset)$, observe that an arbitrary element of $\mathfrak{a}^e$ looks like
$$\begin{aligned}\mathfrak{a} =& \sum_{i=1}^{n} \frac{a_i}{s_i}\iota(p_i) = \sum_{i=1}^{n} \frac{a_i p_i}{s_i} \\ =& \sum_{i=1}^{n} \frac{s_1 \cdots \hat{s_i} \cdots s_n \cdot a_i p_i}{s_1 \cdots s_n} \in S^{-1}\mathfrak{a},\end{aligned}$$
since the numerator is in $\mathfrak{a}$ and the denominator is in S. This proves this claim. □

Proposition 3.9. $A_{\mathfrak{p}}$ is a local ring whose maximal ideal is $S^{-1}\mathfrak{p}$.

Proof. Recall that a ring is local if its set of nonunits forms an ideal (this ideal is then the unique maximal ideal). We claim that the set of nonunits in $A_{\mathfrak{p}}$ is precisely $S^{-1}\mathfrak{p}$ (which is an ideal).

To see $(\subset)$, note that if $\frac{a}{s}$ is a nonunit then $a \in \mathfrak{p}$, since otherwise if $a \in S$ then $\frac{a}{s}$ would have inverse sa and thus be a unit.

To see $(\supset)$, let $a \in \mathfrak{p}$. We want to show $\frac{a}{s}$ is a nonunit. If it were, there there would exist an inverse $\frac{a'}{s'}$. Then $\frac{aa'}{ss'} = \frac{1}{1}$, so there exists $t \in S$ such that $taa' = tss'$. Note the left hand is in $\mathfrak{p}$ while the right hand side is in S. This is a contradiction. □

Proposition 3.10. Localization commutes with quotients: given an ideal $\mathfrak{a} \subset A$ and a multiplicative set S, consider the natural quotient map $\pi : A \to A/\mathfrak{a}$. Then
$$\pi(S)^{-1}(A/\mathfrak{a}) = S^{-1}A/S^{-1}\mathfrak{a}.$$

Proof. We will first construct the forward map. Consider the compose

$$A \to S^{-1}A \to S^{-1}A/S^{-1}\mathfrak{a}$$
$$a \mapsto \frac{a}{1} \mapsto [\frac{a}{1}].$$

Evidently $\mathfrak{a}$ vanishes under this composition, hence there is an induced map

$$g : A/\mathfrak{a} \to S^{-1}A/S^{-1}\mathfrak{a}$$
$$[a] \mapsto [\frac{a}{1}].$$

We claim the image of $\pi(S)$ lies in the units. Indeed, $g([s]) = [\frac{s}{1}]$, which is a unit. Thus we satisfy the universal property conditions and there is an induced map ϕ as follows:

$$\begin{tikzcd}
A/\mathfrak{a} \arrow[r] \arrow[dr, "g"'] & \pi(S)^{-1}(A/\mathfrak{a}) \arrow[d, dashed, "\phi"] \\
 & S^{-1}A/S^{-1}\mathfrak{a}
\end{tikzcd}$$

Since this diagram commutes, we know in particular that

$$\phi(\frac{[a]}{[s]}) = [\frac{a}{s}].$$

Now let's get a map in the other direction. Consider the composite

$$A \to A/\mathfrak{a} \to \pi(S)^{-1}(A/\mathfrak{a})$$
$$a \mapsto [a] \mapsto \frac{[a]}{[1]}.$$

It sends S to units: for any $s \in S$, the image is $\frac{[s]}{[1]}$ which is a unit. So there is likewise by the universal property an induced map

$$\psi : S^{-1}A \to \pi(S)^{-1}(A/\mathfrak{a})$$
$$\frac{a}{s} \mapsto \frac{[a]}{[s]}$$

This vanishes on $S^{-1}\mathfrak{a}$, so there is an induced map $\overline{\psi}$ out of $S^{-1}A/S^{-1}\mathfrak{a}$.

One just checks ϕ and $\overline{\psi}$ are inverses. □

Example 3.11. Recall that $A_\mathfrak{p}$, and that it's maximal ideal is $S^{-1}\mathfrak{p}$. It's residue field is then

$$A_\mathfrak{p}/S^{-1}\mathfrak{p} = S^{-1}A/S^{-1}\mathfrak{p} = \pi(S)^{-1}(A/\mathfrak{p}) = \mathrm{Frac}(A/\mathfrak{p}),$$

since $\pi(S)$ is precisely the nonzero elements of $A/\mathfrak{p}$ and $A/\mathfrak{p}$ is a domain.

Proposition 3.12. Let A be a ring, let $S, T \subset A$ be multiplicative subsets. Let $\hat{T}$ be the image of T under $A \xrightarrow{\iota} S^{-1}A$. Then $\hat{T}$ is a multiplicative subset of $S^{-1}A$, $ST \subset A$ is multiplicative, and

$$\hat{T}^{-1}(S^{-1}A) = (ST)^{-1}A.$$

Proof. prove □ todo

3.2 of modules

3.13. Localization depends on a multiplicative set, so what could we mean by the localization of a module? Given an A-module M and a multiplicative set $S \subset A$, we may wonder whether there is an induced $S^{-1}A-module$ corresponding to M under localization. We already know a method to extend a module to a larger ring: extension of scalars. So we might guess that $S^{-1}A \otimes_A M$ is the module we are looking for.

3.14. Let us construct this directly. As in the ring case, we want to put an equivalence relation on $M \times S$. Let's say that $(m, s) \sim (m', s')$ if there exists $t \in S$ such that $ts'm = tsm'$. Write

$$\frac{m}{s} := [(m, s)].$$

Let us see that this defined a module over $S^{-1}A$:

$$\frac{m}{s} + \frac{m'}{s'} = \frac{ms' + m's}{ss'},$$
$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}.$$

We thus get a map

$$\begin{aligned} \iota : M &\to S^{-1}M \\ m &\mapsto \frac{m}{1}. \end{aligned}$$

Proposition 3.15. The above construction of $S^{-1}M$ satisfies the universal property: for any $S^{-1}A$-module N and any A-module map $f : M \to N$ (regarding N as an A-module by restriction of scalars), there exists a unique $S^{-1}A$-module map $\tilde{f} : S^{-1}M \to N$ such that the following diagram commutes:

$$\begin{tikzcd} M \arrow[r, "\iota"] \arrow[dr, "f"'] & S^{-1}M \arrow[d, dashed, "\tilde{f}"] \\ & N \end{tikzcd}$$

Proof. As always we will start with uniqueness. If the map $\tilde{f}$ exists, then

$$\begin{aligned} \tilde{f}(\frac{m}{s}) =& \tilde{f}(\frac{1}{s})\tilde{f}(\frac{m}{1}) \\ =& \frac{1}{s}\tilde{f}(\frac{m}{1}) = \frac{1}{s}\tilde{f}(\iota(M)) \\ =& \frac{1}{s}f(m). \end{aligned}$$

For existence we check that this map is well-defined. □ check

Corollary 3.16. $S^{-1}M \cong S^{-1}A \otimes_A M$.

Proof. By the universal mapping properties, there are unique isomorphisms sending

$$\frac{m}{s} \mapsto \frac{1}{s} \otimes m,$$
$$\frac{a}{s} \otimes m \mapsto \frac{am}{s}.$$

d □ how

Proposition 3.17. Localization of modules

$$S^{-1}(-) : A\text{Mod} \to S^{-1}A\text{Mod}$$

defines a functor, i.e. a map $M \to M'$ of A-modules induces a map $S^{-1}f : S^{-1}M \to S^{-1}M'$ such that $S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$ and $S^{-1}(1_M) = 1_{S^{-1}M}$.

Proof. Consider the following diagrams:

$$\begin{tikzcd}
M \arrow[r, "\iota_M"] \arrow[d, "f"'] & S^{-1}M \arrow[d, dashed] \\
M' \arrow[r, "\iota_M"'] & S^{-1}M'
\end{tikzcd}
\qquad
\begin{tikzcd}
m \arrow[r, mapsto] \arrow[d, mapsto] & \frac{m}{1} \arrow[d, mapsto, dashed] \\
f(m) \arrow[r, mapsto] & \frac{f(m)}{1}
\end{tikzcd}$$

f □ finish

Proposition 3.18. $S^{-1}(-)$ is an exact functor, i.e. given an exact sequence of A-modules

$$M' \xrightarrow{u} M \xrightarrow{v} M'',$$

there is an induced exact sequence

$$S^{-1}M' \xrightarrow{S^{-1}u} S^{-1}M \xrightarrow{S^{-1}v} S^{-1}M''.$$

Proof. We need to show that $\ker(S^{-1}v) = \operatorname{im}(S^{-1}u)$. The $(\supset)$ direction is straightforward: if $v \circ u = 0$ then $S^{-1}(v \circ u) = 0 = S^{-1}v \circ S^{-1}u$.

For the $(\subset)$ direction, let $\frac{m}{s} \in \ker(S^{-1}v)$. Then $\frac{0}{1} = (S^{-1}v)(\frac{m}{s}) = \frac{v(m)}{s}$, so there exists $t \in S$ such that $v(tm) = tv(m) = 0$, i.e. $tm \in \ker(v) = \operatorname{im}(u)$, so there exists $m' \in M'$ such that $u(m') = tm$. Then $S^{-1}u(\frac{m'}{ts}) = \frac{u(m')}{ts} = \frac{tm}{ts} = \frac{m}{s}$. So $\frac{m}{s} \in \operatorname{im}(S^{-1}u)$ as desired. □

Corollary 3.19. $S^{-1}A$ is a flat A-module.

Example 3.20. We show that the rank of a finitely-generated $\mathbb{Z}$-module is well-defined. Let M be a finitely-generated $\mathbb{Z}$-module. Then

$$M \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^r$$

where $d_1 \mid d_2 \mid \cdots \mid d_k$. We call r the rank of M.

Why is this well-defined? Here is an alternative definition:

$$\mathrm{rank}(M) = \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} M).$$

We calculate that

$$\begin{aligned}\mathbb{Q} \otimes_{\mathbb{Z}} M =& \mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^r) \\ =& (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/d_k\mathbb{Z}) \oplus (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z})^r \\ =& \mathbb{Q}^r\end{aligned}$$

since each $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/d_i\mathbb{Z} = \mathbb{Q}/d_i\mathbb{Q} = 0$. Recall () that $\mathrm{rank}(M_1 + M_2) = \mathrm{rank}(M_1) + \mathrm{rank}(M_2)$. ref Then given an exact sequence of finitely generated $\mathbb{Z}$-modules

$$0 \to M' \to M \to M'' \to 0$$

we have by flatness that, since $\mathbb{Q}$ is a localization of $\mathbb{Z}$ (it is it's field of fractions), there is an exact sequence

$$0 \to \mathbb{Q} \otimes_{\mathbb{Z}} M' \to \mathbb{Q} \otimes_{\mathbb{Z}} M \to \mathbb{Q} \otimes_{\mathbb{Z}} M'' \to 0.$$

Note that these are vector spaces. we have $\mathrm{rank}(M) = \mathrm{rank}(M') + \mathrm{rank}(M'')$. fix

3.21. Similarly to the case for rings, given an A-module M and a multiplicative subset $\{1, f, f^2, \dots\}$ for some $f \in A$, we write $S^{-1}M$ as $M[\frac{1}{f}]$. If $S = A - \mathfrak{p}$ for some prime ideal $\mathfrak{p}$, then we write $S^{-1}M$ as $M_{\mathfrak{p}}$.

3.22. If $N \subset M$ is a submodule, then the inclusion $N \hookrightarrow M$ is injective and by the exactness result so is $S^{-1}N \overset{S^{-1}i}{\to} S^{-1}M$. By identifying $S^{-1}N$ with its image, we may regard it as a submodule of $S^{-1}M$.

Proposition 3.23. Let $S \subset A$ be a multiplicative set, M an A-module. Then

1. For submodules $N, P \subset M$, we have $S^{-1}(N + P) = S^{-1}N + S^{-1}P$.
2. For a submodule $N \subset M$, we have $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.
3. For $N, P \subset M$, we have $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.

Proof. 1. "easy" this

2. Consider the exact sequence

$$0 \to N \to M \to M/N \to 0,$$

which induces an exact sequence

$$0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0.$$

This shows $S^{-1}(M/N) \cong S^{-1}M/\mathrm{im}(S^{-1}i) = S^{-1}M/S^{-1}N$.

3. Consider the exact sequence

$$0 \to N \cap P \to M \to \frac{M}{N} \times \frac{M}{P} \to 0,$$

which induces an exact sequence

$$0 \to S^{-1}(N \cap P) \to S^{-1}M \to S^{-1}(\frac{M}{N} \times \frac{M}{P}) \to 0.$$

By functoriality, also

$$S^{-1}(\frac{M}{N} \times \frac{M}{P}) \cong S^{-1}(\frac{M}{N}) \times S^{-1}(\frac{M}{P}) \cong \frac{S^{-1}M}{S^{-1}N} \times \frac{S^{-1}M}{S^{-1}P}.$$

The kernel of the composite

$$S^{-1}M \to \frac{S^{-1}M}{S^{-1}N} \times \frac{S^{-1}M}{S^{-1}P}$$

has kernel $S^{-1}N \cap S^{-1}P$, which shows the result.

□

3.3 correspondence results

3.24. Let A be a ring, $S \subset A$ a multiplicative set. Recall that for an ideal $\mathfrak{a} \subset A$, we identified $\mathfrak{a}^e = S^{-1}\mathfrak{a} = \{\frac{a}{s} : a \in \mathfrak{a}\}$.

Proposition 3.25. All ideals of $S^{-1}A$ are extended ideals.

Proof. Let $\mathfrak{b} \subset S^{-1}A$ be an ideal. It suffices to show $\mathfrak{b} = \mathfrak{b}^{ce}$. Note we always have $\mathfrak{b} \supset \mathfrak{b}^{ce}$. So for the other direction, let $\frac{x}{s} \in \mathfrak{b}$. Then $\iota(x) = \frac{x}{1} = \frac{s}{1} \cdot \frac{x}{s} \in \mathfrak{b}$, i.e. $x \in \iota^{-1}(\mathfrak{b}) = \mathfrak{b}^c$. Then $\frac{x}{s} = \frac{1}{s} \cdot \frac{x}{1} = \frac{1}{s}\iota(x) \in \mathfrak{b}^{ce}$ as desired. □

Proposition 3.26. For an ideal $\mathfrak{a} \subset A$,

$$\mathfrak{a}^{ec} = \bigcup_{s \in S} (\mathfrak{a} : s).$$

Proof. ($\supset$) Let $x \in \bigcup_{s \in S}(\mathfrak{a} : s)$. Then there exists $s \in S$ such that $sx \in \mathfrak{a}$. then

$$\iota(x) = \frac{x}{1} \cdot \frac{sx}{1} = \frac{1}{s} \cdot \iota(sx) \in \mathfrak{a}^e,$$

i.e. $x \in \mathfrak{a}^{ec}$.

($\subset$) Let $x \in \mathfrak{a}^{ec}$, which is on the left above. Then $\frac{x}{1} \in \mathfrak{a}^e = S^{-1}A$, so there exists $a \in \mathfrak{a}$, $s, \in S$ such that $\frac{x}{1} = \frac{a}{s}$. So there exists $t \in S$ such that $txs = ta$. $ta \in \mathfrak{a}$, so $x(st) \in \mathfrak{a}$ so $x \in (a : st)$. □

Remark 3.27. This generalizes the case when $\mathfrak{a} = 0$ in . ref

Proposition 3.28. For an ideal $\mathfrak{a} \subset A$, we have $\mathfrak{a}^e = S^{-1}A$ if and only if $\mathfrak{a} \cap S \neq \emptyset$.

Proof. We have an exact sequence

$$0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0,$$

hence an induced exact sequence

$$0 \to S^{-1}\mathfrak{a} = \mathfrak{a}^e \to S^{-1}A \to S^{-1}(A/\mathfrak{a}) \to 0.$$

Hence

$$\begin{aligned} \mathfrak{a}^e = S^{-1}A \Leftrightarrow & S^{-1}(A/\mathfrak{a}) = 0 \\ \Leftrightarrow & \frac{[1]}{1} = \frac{[0]}{1} \text{ in } S^{-1}(A/\mathfrak{a}) \\ \Leftrightarrow & \exists s \in S : s[1] = s[0] \Leftrightarrow [s] = [0] \\ \Leftrightarrow & \exists s \in S : s \in \mathfrak{a} \Leftrightarrow S \cap \mathfrak{a} \neq \emptyset. \end{aligned}$$

□

Proposition 3.29. Let $\mathfrak{a} \subset A$ be an ideal. Then $\mathfrak{a}$ is contracted if and only if no element of S is a zero divisor on $A/\mathfrak{a}$.

Proof. $\mathfrak{a}$ is contracted means $\mathfrak{a} = \mathfrak{b}^c$ for some ideal $\mathfrak{b}$. Proposition tells us $\mathfrak{b}^c = \mathfrak{b}^{cec}$, so in ref particular $\mathfrak{a} = \mathfrak{a}^{ec}$. Thus $\mathfrak{a}$ is contracted if and only if

$$\mathfrak{a} = \mathfrak{a}^{ec} = \bigcup_{s \in S} (\mathfrak{a} : s).$$

But this is true if and only if: for all $x \in A$, if there exists $s \in S$ such that $xs \in \mathfrak{a}$, then $x \in \mathfrak{a}$. But this is true if and only if: for all $\bar{x} \in A/\mathfrak{a}$ if there exists $s \in S$ such that $s\bar{x} = \bar{0}$ then $\bar{x} = \bar{0}$. But this is true if and only if s is a zero divisor on $A/\mathfrak{a}$. □

3.30. The following tells us when a prime ideal in A extends to a prime ideal in its localization.

Proposition 3.31. If $\mathfrak{p} \in \operatorname{Spec}(A)$ is such that $\mathfrak{p} \cap S = \emptyset$, then $\mathfrak{p}^e = S^{-1}\mathfrak{p} \in \operatorname{Spec}(S^{-1}A)$.

Proof. Suppose $\frac{a}{s} \cdot \frac{a'}{s'} \in \mathfrak{p}^e = S^{-1}\mathfrak{p}$. Then there exists $p \in \mathfrak{p}$ and $t \in S$ such that $\frac{aa'}{ss'} = \frac{p}{t}$, i.e there exists $u \in S$ such that $uaa't = upss'$. Now the right hand side is in $\mathfrak{p}$, so on the left hand side either $ut \in \mathfrak{p}$ or $aa' \in \mathfrak{p}$. But $ut \in S$ and $S \cap \mathfrak{p} = \emptyset$ by assumption, so $aa' \in \mathfrak{p}$. So $a \in \mathfrak{p}$ or $a' \in \mathfrak{p}$, so either $\frac{a}{s} \in \mathfrak{p}^e$ or $\frac{a'}{s'} \in \mathfrak{p}^e$. □

Proposition 3.32. Extension and contraction define inverse bijections

$$\left\{ \begin{matrix} \text{ideals } \mathfrak{a} \subset A \text{ such that} \\ \forall s \in S \text{ if } sx \in \mathfrak{a} \text{ then } x \in \mathfrak{a} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{ideals of} \\ S^{-1}A \end{matrix} \right\}$$

Proof. By the Galois connections result, we have bijections between contracted ideals of A and extended ideals of $S^{-1}A$. But by (), contracted ideals of A are in this case as described in the proposition, and by () the extended ideals are as described. □

ref

ref

Proposition 3.33. Extension and contraction define inverse bijections

$$\left\{ \begin{array}{c} \mathfrak{p} \in \mathrm{Spec}(A) \text{ such} \\ \text{that } \mathfrak{p} \cap S = \emptyset \end{array} \right\} \longleftrightarrow \mathrm{Spec}(S^{-1}A)$$

Proof. If $\mathfrak{p} \cap S = \emptyset$, then, for all $s \in S$, if $sx \in \mathfrak{p}$ then $x \in \mathfrak{p}$. Thus $\mathfrak{p}$ satisfies the conditions of Proposition (), hence $\mathfrak{p} = \mathfrak{p}^{ec}$. By , $\mathfrak{p}^e \in \mathrm{Spec}(S^{-1}A)$. So extension followed by contraction is the identity on the set on the left hand side. But also contraction followed by contraction is the identity on the right hand side by (). □

ref

ref

ref

Corollary 3.34. If A is Noetherian, then so is $S^{-1}A$.

Proof. Follows from 6 . □

ref

Example 3.35. Let's consider the special case where $\mathfrak{p} \in \mathrm{Spec}(A)$ and $S = A - \mathfrak{p}$. Remember that we write $S^{-1}A = A_\mathfrak{p}$. By Proposition (), we have a bijection

ref

$$\left\{ \begin{array}{c} \mathfrak{p} \in \mathrm{Spec}(A) \text{ such} \\ \text{that } \mathfrak{p} \cap S = \emptyset \end{array} \right\} \longleftrightarrow \mathrm{Spec}(A_\mathfrak{p})$$

But in this case the left hand side is just the set of prime ideals contained in $\mathfrak{p}$. Then $\mathfrak{p}$ is the maximal element on the left hand side, and since we have a bijection it must be that $\mathfrak{p}^e$ is actually the (unique) maximal ideal in $A_\mathfrak{p}$. Thus we recover the fact that $A_\mathfrak{p}$ is local.

3.4 local properties

3.36. Roughly speaking, a local property of a ring A is a property which holds in A if and only if it holds in every localization of A at a prime/maximal ideal.

Proposition 3.37. Being zero is a local property of an A-module M, i.e. the following are equivalent:

1. $M = 0$
2. for all $\mathfrak{p} \in \mathrm{Spec}(A)$ we have $M_\mathfrak{p} = 0$
3. for all $\mathfrak{m} \in \mathrm{Spec}_m(A)$ we have $M_\mathfrak{m} = 0$

Proof. ($3 \Rightarrow 1$) Suppose $M_\mathfrak{m} = 0$ for all $\mathfrak{m} \in \mathrm{Spec}_m(A)$. We want to show $M = 0$. Let $x \in M$. If $x \neq 0$, then $\mathrm{Ann}(x)$ is a proper ideal, so there exists a maximal ideal $\mathfrak{m}$ containing it. Consider $\frac{x}{1} \in M_\mathfrak{m} = 0$. Then $\frac{x}{1} = \frac{0}{1}$ in $M_\mathfrak{m}$. Thus there exists $s \in A - \mathfrak{m}$ such that $sx = 0$. So $s \in \mathrm{Ann}(x) \subset \mathfrak{m}$, which is a contradiction. So $x = 0$ and so $M = 0$. □

Proposition 3.38. For a map $f : M \to N$ of A-modules, the following are equivalent:

1. f is injective (respectively, surjective)
2. for all $\mathfrak{p} \in \operatorname{Spec}(A)$, we have $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective (respectively, surjective)
3. for all $\mathfrak{m} \in \operatorname{Spec}_m(A)$, we have $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (respectively, surjective)

Proof. We will prove the injective proposition, and surjective is analagous if one works with cokernels instead of kernels.

($3 \Rightarrow 1$) We have an exact sequence

$$0 \to \ker(f) \to M \xrightarrow{f} N \to 0,$$

hence an exact sequence

$$0 \to (\ker(f))_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \to 0.$$

So for all $\mathfrak{m} \in \operatorname{Spec}_m(A)$ we have $(\ker(f))_{\mathfrak{m}} = \ker(f_{\mathfrak{m}}) = 0$, where the last equality is our assumption. This implies that for all $\mathfrak{m} \in \operatorname{Spec}_m(A)$ we have $(\ker(f))_{\mathfrak{m}} = 0$. By the previous proposition this implies $\ker(f) = 0$, so f is injective. □

Proposition 3.39. Flatness is a local property of an A-module M, i.e. the following are equivalent:

1. M is flat
2. for all $\mathfrak{p} \in \operatorname{Spec}(A)$ we have that $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module
3. for all $\mathfrak{m} \in \operatorname{Spec}_m(A)$ we have that $M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module

Proof. ($1 \Rightarrow 2$) Suppose M is flat. We want to show that $M_{\mathfrak{p}}$ is flat for all $\mathfrak{p} \in \operatorname{Spec}(A)$, i.e. that the functor $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} (-)$ is exact. But for any $A_{\mathfrak{p}}$-module M,

$$M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N = (M \otimes_A A_{\mathfrak{p}}) \otimes_{A_p} N \cong M \otimes_A (A_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N) \cong M \otimes_A N,$$

i.e. $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} (-) = M \otimes_A (-)$, which is exact by assumption that M is a flat A-module. So $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module.

($2 \Rightarrow 3$) "clear"

($3 \Rightarrow 1$) Suppose that $M_{\mathfrak{m}}$ is flat for all $\mathfrak{m} \in \operatorname{Spec}_m(A)$. We want to show that M is flat, i.e. that $M \otimes_A (-)$ is exact. Since $M \otimes_A (-)$ is always right exact, it suffices to show that if $N' \overset{u}{\to} N$ is an injective A-module map, then $M \otimes_A N' \overset{1\otimes u}{\to} M \otimes_A N$ is injective. By the previous proposition, being injective is a local property, so it suffices to show that for all $\mathfrak{m} \in \operatorname{Spec}_m(A)$ it is the case that

$$\begin{tikzcd}
(M \otimes_A N')_{\mathfrak{m}} \arrow[r, "(1\otimes u)_{\mathfrak{m}}"] \arrow[d, equal, "\sim"'] & (M \otimes_A N)_{\mathfrak{m}} \arrow[d, equal, "\sim"] \\
M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N'_{\mathfrak{m}} & M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N_{\mathfrak{m}}
\end{tikzcd}$$

But $N' \to N$ is injective, so by $N'_{\mathfrak{m}} \xrightarrow{u_{\mathfrak{m}}} N_{\mathfrak{m}}$ is injective, so since $M_{\mathfrak{m}}$ is flat, ref

$$M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N'_{\mathfrak{m}} \xrightarrow{1 \otimes u_{\mathfrak{m}}} M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N_{\mathfrak{m}}$$

is injective. □

3.4.1 applications

Proposition 3.40. Let $\phi : A \to B$ be a ring map. Then $\mathfrak{p} \in \operatorname{Spec}(A)$ is the contraction of a prime ideal $\mathfrak{q} \in \operatorname{Spec}(B)$ if and only if $\mathfrak{p} = \mathfrak{p}^{ec}$.

Remark 3.41. Note that the reverse direction is nontrivial: just because $\mathfrak{p} = \mathfrak{p}^{ec}$ does not necessarily mean $\mathfrak{p}$ is the contraction of a prime ideal, since $\mathfrak{p}^e$ need not be prime.

Proof. ($\Rightarrow$) Say $\mathfrak{p} = \mathfrak{q}^c$ for some $\mathfrak{q} \in \operatorname{Spec}(B)$. Then $\mathfrak{p}^{ec} = (\mathfrak{q}^c)^{ec} = \mathfrak{q}^c = \mathfrak{p}$.

($\Leftarrow$) Say $\mathfrak{p} = \mathfrak{q}^{ec}$. Let $S = A - \mathfrak{p}$. Then $\phi(S) \subset B$ is multiplicative. Note $\mathfrak{p}^e \cap \phi(S) = \emptyset$, for if there exists $s \in S$ such that $\phi(s) \in \mathfrak{p}^e$ then $s \in \mathfrak{p}^{ec} = \mathfrak{p} = A - S$, which is a contradiction. Consider now the localization $B \to \phi(S)^{-1}B$.

Since $\mathfrak{p}^e \subset B$ doesn't meet $\phi(S)$, there is an ideal $\mathfrak{q} \subset B$ containing $\mathfrak{p}^e$, maximal with respect to exclusion of $\phi(S)$. To see this, recall that prime ideals avoiding $\phi(S)$ are in one-to-one correspondence with prime ideals in the localization (). Consider the corresponding ideal in ref the localization. It is contained in a unique maximal ideal. Using the correspondence in the other direction, we get a prime ideal in B containing $\mathfrak{p}^e$. This ideal must be maximal with respect to ideals avoiding $\phi(S)$, since it corresponds to a maximal ideal in the localization under an order preservering () one-to-one correspondence. ref

By (3.6,3.8,Krull), $\mathfrak{q}$ is prime. Then $\mathfrak{q} \supset \mathfrak{p}^e$ and $\mathfrak{q} \cap \phi(S) = \emptyset$. The first condition implies $\mathfrak{q}^c \subset$ ref $\mathfrak{p}^{ec} = \mathfrak{p}$, where the last equality is our assumption. The second condition that $\mathfrak{q} \cap \phi(S) = \emptyset$ implies $\mathfrak{q}^c \cap S = \emptyset$, i.e. $\mathfrak{q}^c \subset \mathfrak{p}$, so $\mathfrak{q}^c = \mathfrak{p}$. □

4 integrality

4.1. Let's recall an example for motivation. Let B be a k-algebra, where k is a field. Then $b \in B$ is algebraic over k if there exists a nonzero $f \in k[X]$ such that $f(b) = 0$. Say

$$f = c_n X^n + \cdots + c_1 X + c_0.$$

Then, because our coefficients are a field, we can make this a monic polynomial so that

$$0 = b^n + \frac{c_{n-1}}{c_n} b^{n-1} + \cdots + \frac{c_0}{c_n}.$$

Crucially, this means $b^n \in \operatorname{span}\{1, b, \ldots, b^{n-1}\}$, and by extension higher powers of b are in this same span. This was important because now $\deg_k(k[b]) = [k[b] : k] < \infty$.

The step that made this all possible was that we could make f monic. This meant that it sufficed to find any f such that $f(b) = 0$. In the case that we are not a field though, we shouldn't expect to be able to do this. One wonders how much of the theory can be recovered by appropriately adjusting the theory in the situation where k is a ring.

An example of where the theory becomes weird if we don't restrict to monic polynomials is the following: regard $\mathbb{Q}$ as a $\mathbb{Z}$-algebra. Then $b = \frac{1}{2}$ satisfies the polynomial $2X - 1 \in \mathbb{Z}[X]$, but $\mathbb{Z}[\frac{1}{2}]$ is not aa finitely-generated $\mathbb{Z}$-module, much less of dimension 1 as we might expect in the case of fields.

Definition 4.2. Let $A \subset B$ be rings (so that we may regard B as an A-algebra). We say that $b \in B$ is *integral* over A if b is a root of a monic polynomial $f \in A[X]$.

4.3. The following example may elucidate the nomenclature. If $x \in \mathbb{Q}$ is integral over $\mathbb{Z}$, then we claim $x \in \mathbb{Z}$ (x is an integer!). To see this, write $x = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ are coprime. Since x is integral, there exist $c_i \in \mathbb{Z}$ such that

$$0 = \left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_0.$$

We can clearn denominators to get

$$a^n = -b^n - b(\cdots),$$

but then a prime divisor of the right hand side would also be a prime divisor of the left hand side. In particular a prime divisor of a is a prime divisor of b. Hence it must be the case that $b = 1$, i.e. $x = a$ is an integer.

Proposition 4.4. Let $A \subset B$ be a ring extension, $b \in B$. The following are equivalent:

1. b is integral over A
2. $A[b]$ is a finitely-generated A-module
3. there exists a subring B' with $A[b] \subset B' \subset B$ such that B' is finitely-generated as an A-module.
4. there exists a faithful $A[b]$-module F that is finitely-generated as an A-module.

Remark 4.5. Condition (3) addresses the issue with modules that a submodule of a finitely-generated module need not be finitely-generated.

Proof. ($1 \Rightarrow 2$) Say b is integral over A. Then b satisfies a monic polynomial

$$0 = b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n$$

so

$$b^n \in A + Ab + \cdots + Ab^{n-1}.$$

Inductively, $b^N \in \operatorname{span}\{1, b, \ldots, b^{n-1}\}$ for $N \geq n$. So

$$A[b] = \operatorname{span}_A\{1, b, b^2, \ldots\} = \operatorname{span}_A\{1, b, \ldots, b^{n-1}\}$$

which shows that $A[b]$ is a finitely-generated A-module.

($2 \Rightarrow 3$) Suppose $A[b]$ is finitely-generated as an A-module. Take $B' = A[b]$.

($3 \Rightarrow 4$) Suppose B' is a subring with $A[b] \subset B' \subset B$, and B' is finitely-generated as an A-module. Take $F = B'$.

($4 \Rightarrow 1$) Say F is a faitful $A[b]$-module, finitely generated as an A-module. Consider the left multiplication map

$$\begin{aligned} \lambda_b : F &\to F \\ x &\mapsto bx. \end{aligned}$$

By the Cayley-Hamilton trick (9.3) with $\mathfrak{a} = A$, we get that λ_b satisfies a monic polynomial ref $f \in A[X]$, i.e. $0 = f(\lambda_b)$. But for any $x \in F$, we then have $0 = f(\lambda_b)(x) = f(b)x$, so $f(b)F = 0$. Since F is faithful, it must be that $f(b) = 0$, i.e. b satisfies a monic polynomial in $A[X]$. □

Definition 4.6. Let $A \subset B$ be a ring extension. We say that B is *integral over* A if every $b \in B$ is integral over A.

Corollary 4.7. Let $A \subset B$ be a ring extension. Let $b_1, \ldots, b_n \in B$ be integral over A. Then $A[b_1, \ldots, b_n]$ if finitely-generated as an A-module.

Proof. We induct on n. The base case $n = 1$ is the above proposition. Now let $n > 1$. Let $A' = A[b_1, \ldots, b_{n-1}]$, which is finitely-generated by hypothesis. By ref, it suffices to show that $A'[b_n]$ is finitely-generated as an A'-module. To do that, it suffices to show that b_n is integral over A'. Since b_n is integral over A it satisfies a monic polynomial with coefficients in A. Since $A \subset A'$, it satisfies a monic polynomial with coefficients in A', and we are done.

$$\begin{tikzcd}
A'[b_n] = A[b_1, \ldots, b_n] \arrow[d, dash] \\
A' = A[b_1, \ldots, b_{n-1}] \arrow[d, dash] \\
A
\end{tikzcd}$$

□

Definition 4.8. Let $A \subset B$ be a ring extension. The subring

$$\overline{A} \coloneqq \{b \in B : b \text{ is integral over } A\}$$

is called the *integral closure of* A in B. If $\overline{A} = A$ we say that A is *integrally closed in* B. Sometimes we make no reference to B. This is done in the specific case where A is a domain and B is its field of fractions, we just say that A is *integrally closed* to implicitly mean that it is integrally closed in its field of fractions. Similarly we talk about the *integral closure* of A.

Proposition 4.9. Let $A \subset B$ be a ring extension. Let $\overline{A}$ be the integral closure of A in B. Then $\overline{A} \subset B$ is a subring, i.e. $\alpha, \beta \in \overline{A}$ implies $\alpha + \beta, \alpha\beta \in \overline{A}$.

Proof. Let $\alpha, \beta \in \overline{A}$. Let $B' = A[\alpha, \beta]$. By (9.4), B' is a finitely-generated A-module. By (9.2, $3 \Rightarrow 1$) we get that $\alpha + \beta$ is integral over A, i.e. $\alpha + \beta \in \overline{A}$. Similarly one shows $\alpha\beta$ is integral over A.

$$\begin{tikzcd}
B \arrow[d, dash] \\
B' = A[\alpha, \beta] \arrow[d, dash] \\
A[\alpha + \beta] \arrow[d, dash] \\
A
\end{tikzcd}$$

□

Proposition 4.10 (transitivity of integral dependence)**.** Let $A \subset B$ and $B \subset C$ be integral ring extensions. Then $A \subset C$ is integral.

Proof. Let $\gamma \in C$. We want to show that γ is integral over A. Now γ is integral over B by assumption, so there exists $b_1, \ldots, b_n \in B$ such that

$$\gamma^n + b_1\gamma^{n-1} + \cdots + b_n = 0.$$

Let $A' = A[b_1, \ldots, b_n]$. Then γ is integral over A', i.e. $A'[\gamma]$ is finitely-generated as an A'-module. Then by ref, $A'[\gamma]$ is finitely-generated as an A-module.

Now let $C' = A'[\gamma]$. Then C' is a subring of C (check) such that

1. $A[\gamma] \subset C' \subset C$
2. C' is finitely-generated as an A-module

But then by (9.2, $3 \Rightarrow 1$) it follows that γ is integral over A.

$$\begin{tikzcd}
 & & C \arrow[dl, dash] \arrow[dddd, dash, dashed] & \\
 & C' = A'[\gamma] \arrow[drr, dash] \arrow[ddl, dash] & & \\
 & & & A[\gamma] \arrow[ddl, dash] \\
A' = A[b_1, \ldots, b_n] \arrow[drr, dash] & & & \\
 & & A &
\end{tikzcd}$$

□

Corollary 4.11. Any $b \in B$ that is integral over $\overline{A}$ lies in $\overline{A}$.

4.12. The following generalizes the earlier example with $\mathbb{Z}$ and $\mathbb{Q}$.

Proposition 4.13. Let A be a factorial domain (UFD). Then A is integrally closed.

Proof. Let $x = \frac{b}{c} \in K = \text{Frac}(A)$ be integral over A. Since we are in a UFD, we can assume that $b, c \in A$ have no common non-unit factors. For some monic $f \in A[X]$, say $f = X^n + a_1 X^{n-1} + \cdots + a_n$, we have

$$0 = f(x) = \left(\frac{b}{c}\right)^n + a_1 \left(\frac{b}{c}\right)^{n-1} + \cdots + a_n.$$

If $c \in A^\times$ then we are done: $\frac{1}{c} \in A$ so f is already a monic polynomial in A. Otherwise, multiply through by c^n:

$$0 = b^n + a_1 c b^{n-1} + \cdots + a_{n-1} c^{n-1} b_1 + a_n c^n.$$

So

$$-b^n = c(a_1 b^{n-1} + \cdots + a_n c^{n-1}).$$

Let p be a prime divisor of c, i.e. $c \in (p)$. Then it is also a prime divisor of b^n, and since p is prime it must be that p is a divisor of b. But then p is a common divisor of b, c which is a contradiction. □

Example 4.14. Let K be an algebraic number field, i.e. a finite field extension of $\mathbb{Q}$. We call the integral closure of $\mathbb{Z}$ in K as the algebraic integers in K, denoted $\mathcal{O}_K$.

$$\begin{tikzcd}
K \arrow[dr, dash] \arrow[dd, dash] & \\
 & \mathcal{O}_K \arrow[dd, dash] \\
\mathbb{Q} \arrow[dr, dash] & \\
 & \mathbb{Z}
\end{tikzcd}$$

4.15. Given a ring extension $A \subset B$, it may be the case that B is finitely-generated as an A-algebra but not as an A-module (consider the polynomial ring in countably infinite variables). However, we have shown that if B is finitely-generated as an A algebra (of "finite type") as well as integral over A, then B will be finitely generated as an A-module (a "finite" module). This is because, in such a situation, $B = \overline{A}$?

Proposition 4.16. Let $A \subset B$ be an integral extension. Then $A^\times A \cap B^\times$.

Proof. A unit of A is a unit of B since $A \subset B$, hence $A^\times \subset A \cap B^\times$.

On the other hand, if $a \in A \cap B^\times$, then a has an inverse $a^{-1} \in B$. We want to show $a^{-1} \in A$. Now a^{-1} is integral over A, so we can write

$$(a^{-1})^n + c_1(a^{-1})^{n-1} + \cdots + c_n = 0$$

for some $c_i \in A$. Multiplying through by a^n gives

$$1 + c_1 a + \cdots + c_{n-1}a^{n-1} + c_n a^n = 0,$$

i.e.

$$-1 = a(c_1 + \cdots + c_n a^{n-1}).$$

This demonstrates an inverse of a which is computed as the finite sum of products of elements in A, hence $a^{-1} \in A$. □

Proposition 4.17. Let $A \subset B$ be an integral extension, where B is a domain. Then B is a field if and only if A is a field.

Proof. ($\Rightarrow$) If B is a field, then by (9.10) $A^\times = A \cap B^\times = A - \{0\}$, so A is a field.

($\Leftarrow$) SUppose A is a field. Let $0 \neq b \in B$. We want to show $b \in B^\times$. Since b is integral over A, we can write

$$0 = f(b) = b^n + a_1 b^{n-1} + \cdots + a_{n-1}b + a_n$$

where f is of minimal degree. Then $a_n \neq 0$, since otherwise we could factor out a b from f where either $b = 0$ or the lower degree polynomial at b is 0 (these are the only possibilities since we are in a domain).

We divide the above by $a_n \in A^\times$:

$$0 = \frac{1}{a_n}b^n + \cdots + \frac{a_{n-1}}{a_n}b + 1,$$

i.e.

$$1 = b\left(\frac{-1}{a_n}b^{n-1} - \cdots - \frac{a_{n-1}}{a_n}\right)$$

so $b \in B^\times$. □

Corollary 4.18. Let $A \subset B$ be an integral extension. Let $\mathfrak{q} \in \operatorname{Spec}(B)$. Then $\mathfrak{q}$ is a maximal ideal in B if and only if $\mathfrak{p} = A \cap \mathfrak{q}$ is a maximal ideal in A.

Proof. The extension $A/\mathfrak{p} \subset B/\mathfrak{q}$ is integral, and $B/\mathfrak{q}$ is a domain since $\mathfrak{q}$ is prime, so $\mathfrak{q}$ is maximal if and only if $B/\mathfrak{q}$ is a field. By 9.10', this is the case if and only if $A/\mathfrak{p}$ is a field, i.e. if and only if $\mathfrak{p} \subset A$ is maximal. □

5 Noether normalization

5.1. Noether normalization tells us that any finitely-generated k-algebra over a field can be "factored" as a polynomial extension followed by an integral extension.

$$\begin{tikzcd}
B \arrow[d, dash, "\text{integral}"'] \\
k[b_1, \dots, b_d] \cong k[T_1, \dots, T_d] \arrow[d, dash, "\text{polynomial}"'] \\
k
\end{tikzcd}$$

Theorem 5.2 (Noether)**.** Let k be a field, let B be a finitely-generated k-algebra. Then there exists $b_1, \dots, b_d \in B$ such that

1. $\{b_1, \dots, b_d\}$ is algebraically independent over k, i.e. the k-algebra map
$$\begin{aligned} k[X_1, \dots, X_d] &\to k[b_1, \dots, b_d] \\ f &\mapsto f(b_1, \dots, b_d) \end{aligned}$$
is an isomorphism.
2. B is integral over $A = k[b_1, \dots, b_d]$.

Lemma 5.3 (Nagata)**.** Let k be a field, let $f \in k[X_1, \dots, X_n]$ be a nonconstant polynomial. Then there exists a k-algebra automorphism ϕ of $k[X_1, \dots, X_n]$ such that $\phi(f)$ looks like

$$\phi(f) = cX_n^d + \sum_{i=0}^{d-1} g_i(X_1, \dots, X_{n-1})X_n^i$$

for some $g_1, \dots, g_{d-1} \in k[X_1, \dots, X_{n-1}]$ and $0 \neq c \in k$.

Remark 5.4. In other words, $\phi(f) = c\hat{f}$ is a k-multiple of a polynomial $\hat{f} \in k[X_1, \dots, X_{n-1}][X_n]$ that is monic in X_n. So we can think of $\phi(f)$ as "almost monic" in X_n.

Proof. Define

$$\begin{aligned} \phi : k[X_1, \dots, X_n] &\to k[X_1, \dots, X_n] \\ X_{i<n} &\mapsto X_i + X_n^{r_i} \\ X_n &\mapsto X_n \end{aligned}$$

where $r_1, \dots, r_{n-1}$ will be chosen below. Note that this indeed a k-algebra automorphism, as we can write down its inverse explicitly:

$$\begin{aligned} X_{i<n} &\mapsto X_i - X_n^{r_i} \\ X_n &\mapsto X_n. \end{aligned}$$

Now write

$$f = \sum_{\alpha \in I} c_\alpha X^\alpha,$$

where I is a finite set of multi-indices $\alpha = (\alpha_1, \dots, \alpha_n)$ and $X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ and each $c_\alpha \neq 0$. Then

$$\begin{aligned} \phi(f) =& \sum_{\alpha \in I} c_\alpha (X_1 + X_n^{r_1})^{\alpha_1} \cdots (X_{n-1} + X_n^{r_{n-1}})^{\alpha_{n-1}} X_n^{\alpha_n} \\ =& \sum_{\alpha \in I} c_\alpha (p_\alpha + X_n^{d(\alpha)}), \end{aligned}$$

where p_α is a polynomial of lower degere in X_n and $d(\alpha) = a_n + \alpha_1 r_1 + \cdots + \alpha_{n-1} r^{n-1}$ is a function $I \to \mathbb{N}$. Now the unique summand of highest degree in X_n in the α-summand of f is $c_\alpha X_n^{d(\alpha)}$.

We claim that $r_1, \dots, r_{n-1}$ can be chosen such that $d : I \to \mathbb{N}$ is injective. If the claim holds, then let γ be the unique multiindex in I where d attains maximal value. Then in $\phi(f)$ the unique summand of highest degree in X_n is $c_\gamma X_n^{d(\gamma)}$. This would complete the proof.

Now we prove the claim. Let $e > \max_{\alpha \in I}\{\alpha_1, \dots, \alpha_n\}$. Then define $r_i = e^i$ for $i = 1, \dots, n-1$. Then

$$d(\alpha) = \alpha_n + \alpha_1 e + \alpha_2 e^2 + \cdots + \alpha_{n-1} e^{n-1},$$

i.e. the e-ary expansion of $d(\alpha) \in \mathbb{N}$. These are unique. □

Proof of Noether normalization. Let $B = k[x_1, \dots, x_n]$ be a finitely-generated k-algebra, where $x_1, \dots, x_n$ are a collection of generators. We proceed by induction on n. In the case of $n = 0$ there is nothing to show. In the case of $n = 1$ then $B = k[x_1]$. There are two cases:

- x_1 is transcendental over k. Then let $A = k[x_1] \cong k[T]$. The integral extension is trivial.
- x_1 is algebraic. Then let $A = k$. The polynomial extension is trivial.

For $n > 1$, consider the map

$$\begin{aligned} k[X_1, \dots, X_n] \xrightarrow{\epsilon} B = k[x_1, \dots, x_n] \\ X_i \mapsto x_i \end{aligned}$$

so that $B \cong k[X_1, \dots, X_n]/I$ where $I = \ker(\epsilon)$. If $I = 0$ we are done: the integral extension is trivial. Suppose that $I \neq 0$, and let $f \in I$. Let ϕ the k-algebra automorphism of $k[X_1, \dots, X_n]$ as in Nagata's lemma. Then we can replace X_i by $X_i' = \phi(X_i)$ and x_i by $x_i' = \epsilon(X_i')$. By Nagata's lemma, we can assume f is "almost monic" in X^n, i.e.

$$f = cX_n^d + \sum_{i=0}^{d-1} g_i(X_1, \dots, X_{n-1}) X_n^i.$$

In B,

$$0 = \bar{f} = cx_n^d + \sum_{i=0}^{d-1} g_i(x_1, \ldots, x_{n-1})x_n^i.$$

By dividing through by $0 \neq c \in k$ we get that x_n satisfies a monic polynomial in $k[x_1, \ldots, x_{n-1}][X_n]$. Write $B' = k[x_1, \ldots, x_{n-1}]$. This shows that B is integral over B'. By induction, since B' has finitely many generators and strictly fewer generators than B, there exists $b_1, \ldots, b_d \in B'$ such that

- $\{b_1, \ldots, b_d\}$ are algebraically independent
- B' is integral over $A = k[b_1, \ldots, b_d]$.

By transitivity we are done:

$$\begin{tikzcd}
B = B'[x_n] \arrow[d, dash, "\text{integral}"'] \\
B' = k[x_1, \ldots, x_{n-1}] \arrow[d, dash, "\text{integral}"'] \\
k[b_1, \ldots, b_d] \cong k[T_1, \ldots, T_d] \arrow[d, dash, "\text{polynomial}"'] \\
k
\end{tikzcd}$$

□

Lemma 5.5 (Zariski's lemma)**.** Let k be a field, K a finitely-generated k-algebra that is a field. Then K is a finite algebraic extension of k.

Proof. By Noether normalization there exist $b_1, \ldots, b_d \in K$ such that

- $\{b_1, \ldots, b_d\}$ is algebraically independent over k
- K is integral over $k[b_1, \ldots, b_d]$

Since K is a field, by (prop/cor) we have that $k[b_1, \ldots, b_d]$ is a field. But this is only possible if $d = 0$, since k itself is a field. So K is integral over k, i.e. is a finite algebraic extension. □

6 Cohen-Seidenberg theorems

Proposition 6.1. Let $A \subset B$ be an integral extension, let $\mathfrak{b} \subset B$ be an ideal. Then

$$\frac{A}{\mathfrak{b} \cap A} \to B/\mathfrak{b}$$

is an integral extension.

Proposition 6.2. Let $A \subset B$ be an integral extension, let $S \subset A$ be a multiplicative set. Then $S^{-1}A \to S^{-1}B$ is an integral extension.

Proof. Let $\frac{b}{s} \in S^{-1}B$. Now b is integral over A, so there exists $a_1, \ldots, a_n \in A$ such that

$$b^n + a_1 b^n + \cdots + a_{n-1} b + a_n = 0.$$

In $S^{-1}A$,

$$\left(\frac{b}{1}\right)^n + \left(\frac{a_1}{1}\right)\left(\frac{b}{1}\right)^{n-1} + \cdots + \left(\frac{a_{n-1}}{1}\right)\left(\frac{b}{1}\right) + \left(\frac{a_n}{1}\right) = \frac{0}{1}.$$

Multiplying through by $\frac{1}{s^n}$:

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_1}{s}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_{n-1}}{s^{n-1}}\right)\left(\frac{b}{s}\right) + \left(\frac{a_n}{s^n}\right) = \frac{0}{1}.$$

Therefore $\frac{b}{s}$ satisfies a monic polynomial over $S^{-1}A$ so the extension is integral. □

Theorem 6.3 (lying over)**.** Let $j : A \hookrightarrow B$ be an integral extension. Then $j^\sharp : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective: for all $\mathfrak{p} \in \operatorname{Spec}(A)$ there exists $\mathfrak{q} \in \operatorname{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{p}$.

Proof. Suppose first that A is local, with $\mathfrak{p}$ its unique maximal ideal. Let $\mathfrak{M} \subset B$ be any maximal ideal, so $\mathfrak{M} \cap A \in \operatorname{Spec}(A)$. By Corollary 4.18 the fact that $\mathfrak{M}$ is maximal implies $\mathfrak{M} \cap A$ is maximal, hence it must be equal to the unique maximal ideal $\mathfrak{p} \subset A$.

We can drop the assumption that A is local now, but the idea is to pass to the local ring $A_{\mathfrak{p}}$. By Proposition 6.2, $A_{\mathfrak{p}} \subset B_{\mathfrak{p}}$ is integral with $A_{\mathfrak{p}}$ local. By our remarks in the first paragraph, there exists $\mathfrak{q}' \in \operatorname{Spec}(B)$ such that $\mathfrak{q}' \cap A_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}$. Then under the composite $A \to A_{\mathfrak{p}} \to B_{\mathfrak{p}}$, we have that $\mathfrak{q}'$ contracts to $\mathfrak{p}$. Let $\mathfrak{q}$ be the contraction of $\mathfrak{q}'$ under $B \to B_{\mathfrak{p}}$. By commutativity (see diagram below), $\mathfrak{q}$ contracts under $j : A \hookrightarrow B$ to $\mathfrak{p}$, i.e. $\mathfrak{q} \cap A = \mathfrak{p}$.

$$\begin{tikzcd}
& & & \mathfrak{q}' \arrow[dlll, bend right, mapsto] \arrow[ddd, mapsto] \\
\mathfrak{q} \arrow[dddd, dashed, mapsto] & & B_{\mathfrak{p}} & \\
& B \arrow[ur, "\iota_B"] & A_{\mathfrak{p}} \arrow[u, hook, "j_{\mathfrak{p}}"'] & \\
& A \arrow[u, hook, "j"] \arrow[ur, "\iota_{\mathfrak{p}}"'] & & \mathfrak{p}_{\mathfrak{p}} \arrow[dlll, bend left, mapsto] \\
\mathfrak{p} & & &
\end{tikzcd}$$

□

Theorem 6.4 (incomparability)**.** Let $A \subset B$ be an integral extension. Let $\mathfrak{q}_1, \mathfrak{q}_2 \in \operatorname{Spec}(B)$ be such that $\mathfrak{q}_1^c = \mathfrak{q}_2^c := \mathfrak{p} \in \operatorname{Spec}(A)$ and $\mathfrak{q}_1 \subset \mathfrak{q}_2$. Then $\mathfrak{q}_1 = \mathfrak{q}_2$.

Remark 6.5. This is not saying that only one ideal in $\operatorname{Spec}(B)$ contracts to an ideal in $\operatorname{Spec}(A)$, but that that there are no nontrivial relationships among the fibers:

$$\begin{tikzcd}
\mathfrak{q}_1' \arrow[d, equal] & & \mathfrak{q}_2' \arrow[d, equal] \\
\mathfrak{q}_1 \arrow[dr] & & \mathfrak{q}_2 \arrow[dl] \\
& \mathfrak{p} &
\end{tikzcd}$$

Proof. Let $\mathfrak{q} \in \operatorname{Spec}(B)$ be any prime that contracts to an ideal $\mathfrak{p} \in \operatorname{Spec}(A)$. Consider $S^{-1}B$, where $S = A - \mathfrak{p}$. Then $\mathfrak{q} \cap A = \mathfrak{p} = A - S$, hence $\mathfrak{q} \cap S = \emptyset$. Thus $S^{-1}\mathfrak{q}$ is a proper prime ideal of $S^{-1}B$, by (8.18). Now $S^{-1}\mathfrak{q}$ contracts under $S^{-1}A \to S^{-1}B$ to

$$S^{-1}A \cap S^{-1}\mathfrak{q} = S^{-1}(A \cap \mathfrak{q}) = S^{-1}\mathfrak{p} = \mathfrak{p}_{\mathfrak{p}},$$

which is maximal in $S^{-1}A = A_{\mathfrak{p}}$. By Proposition 6.1, $A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ is an integral extension, so by Corollary 4.18, $S^{-1}\mathfrak{q}$ is maximal in $S^{-1}B$.

Apply this procedure to $\mathfrak{q}_1$ and $\mathfrak{q}_2$ where $\mathfrak{q}_1^c = \mathfrak{q}_2^c$ and $\mathfrak{q}_1 \subset \mathfrak{q}_2$. Then $S^{-1}\mathfrak{q}_1$ and $S^{-1}\mathfrak{q}_2$ are both maximal in $S^{-1}B$, and $S^{-1}\mathfrak{q}_1 \subset S^{-1}\mathfrak{q}_2$, so it must be that $S^{-1}\mathfrak{q}_1 = S^{-1}\mathfrak{q}_2$. But by Proposition 3.33 there is a bijection

$$\{\mathfrak{q} \in \operatorname{Spec}(B) : \mathfrak{q} \cap S = \emptyset\} \leftrightarrow \operatorname{Spec}(S^{-1}B).$$

So the fact that $S^{-1}\mathfrak{q}_1 = S^{-1}\mathfrak{q}_2$ implies $\mathfrak{q}_1 = \mathfrak{q}_2$. □

Theorem 6.6 (going up)**.** Let $A \subset B$ be an integral extension. Let

$$\mathfrak{p}_1 \subset \cdots \mathfrak{p}_n$$
$$\mathfrak{q}_1 \subset \cdots \mathfrak{q}_m$$

be chains of primes in A and B, respectively, where $m < n$ and $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $i = 1, \ldots, m$. Then we can "complete the chain" in the sense that we can construct $\mathfrak{q}_{m+1} \subset \cdots \subset \mathfrak{q}_n$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathfrak{q}_1 \arrow[d, mapsto] & \subset & \cdots & \subset & \mathfrak{q}_m \arrow[d, mapsto] & \subset & \mathfrak{q}_{m+1} \arrow[d, mapsto, dashed] & \subset & \cdots & \subset & \mathfrak{q}_n \arrow[d, mapsto, dashed] \\
\mathfrak{p}_1 & \subset & \cdots & \subset & \mathfrak{p}_m & \subset & \mathfrak{p}_{m+1} & \subset & \cdots & \subset & \mathfrak{p}_n
\end{tikzcd}$$

(The maps above are contractions.)

Proof. By induction, it suffices to assume $n = 2$ and $m = 1$. Let $\overline{A} = A/\mathfrak{p}_1$ and $\overline{B} = B/\mathfrak{q}_1$. By Proposition 6.1, $\overline{A} = A/\mathfrak{p}_1 \hookrightarrow B/\mathfrak{q}_1$ is an integral extension. Now consider $\overline{\mathfrak{p}_2} = \mathfrak{p}_2/\mathfrak{p}_1 \in \operatorname{Spec}(\overline{A})$. By the lying over theorem applied to $\overline{A} \hookrightarrow \overline{B}$, there exists $\overline{\mathfrak{q}_2} \in \operatorname{Spec}(\overline{B})$ such that $\overline{\mathfrak{q}_2}$ contracts to $\overline{\mathfrak{p}_2}$ under $\overline{A} \hookrightarrow \overline{B}$. Like any prime ideal of $\overline{B} = B/\mathfrak{q}_1$, $\overline{\mathfrak{q}_2}$ has the form $\overline{q}_2 = \mathfrak{q}_2/\mathfrak{q}_1$ for som prime ideal $\mathfrak{q}_2 \in \operatorname{Spec}(B)$ with $\mathfrak{q}_2 \supset \mathfrak{q}_1$. Then $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ by the correspondence theorem. □

Proposition 6.7. Let $A \subset B$ be an integral extension, let $S \subset A$ multiplicatively closed. Write $\overline{A}$ for the integral closure of A in B. Then $S^{-1}\overline{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Remark 6.8. A cool way to write this is that $S^{-1}\overline{A} = \overline{S^{-1}A}$, but one should be careful to note the shifting notation here: $\overline{(-)}$ is representing integral closure in two different rings.

Proof. ($\subset$) Since $A \subset \overline{A}$ is integral by construction, by Proposition 6.2 we have that $S^{-1}A \subset S^{-1}\overline{A}$ is integral. But $\overline{S^{-1}A}$ consists of all elements of $S^{-1}B$ which are integral over $S^{-1}A$, and $S^{-1}\overline{A} \subset S^{-1}B$, so it must be the case that $S^{-1}\overline{A} \subset \overline{S^{-1}A}$.

($\supset$) Let $\frac{b}{s} \in \overline{S^{-1}A}$, so $\frac{b}{s}$ is integral over $S^{-1}A$. Then there exists an integral dependence relation

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s_1}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_{n-1}}{s_{n-1}}\left(\frac{b}{s}\right) + \frac{a_n}{s_n} = \frac{0}{1}$$

in $S^{-1}B$ for some $\frac{a_1}{s_1}, \ldots, \frac{a_n}{s_n} \in S^{-1}A$. Multiply by $\frac{s^n}{1}$:

$$\left(\frac{b}{1}\right)^n + \frac{a_1 s}{s_1}\left(\frac{b}{1}\right)^{n-1} + \cdots + \frac{a_{n-1}s^{n-1}}{s_{n-1}}\left(\frac{b}{1}\right) + \frac{a_n s^n}{s_n} = \frac{0}{1}$$

Let $t = s_1 \cdots s_n$ and multiply through by $\frac{t^n}{1}$:

$$\left(\frac{tb}{1}\right)^n + \frac{a_1 st}{s_1}\left(\frac{tb}{1}\right)^{n-1} + \cdots + \frac{a_{n-1}s^{n-1}t^{n-1}}{s_{n-1}}\left(\frac{tb}{1}\right) + \frac{a_n s^n t^n}{s_n} = \frac{0}{1},$$

i.e.

$$\frac{(tb)^n + a_1'(tb)^{n-1} + \cdots + a_{n-1}'(tb) + a_n'}{1} = \frac{0}{1}$$

in $S^{-1}B$. Thus there exists $u \in S$ such that

$$0 = u\big((tb)^n + a_1'(tb)^{n-1} + \cdots + a_{n-1}'(tb) + a_n'\big),$$

so

$$\begin{aligned} 0 =& u^n\big((tb)^n + a_1'(tb)^{n-1} + \cdots + a_{n-1}'(tb) + a_n'\big) \\ =& (utb)^n + a_1'u(utb)^{n-1} + \cdots + a_{n-1}'u^{n-1}(utb) + a_n'u^n, \end{aligned}$$

so utb is integral over A, i.e. $utb \in \overline{A}$. Then $\frac{b}{s} = \frac{utb}{uts} \in S^{-1}\overline{A}$, so $\overline{S^{-1}A} \subset S^{-1}\overline{A}$. □

Proposition 6.9. Let A be a domain, let $K = \mathrm{Frac}(A)$ be its field of fractions. Then being integrally closed is a local property, i.e. the following are equivalent:

1. A is integrally closed.
2. $A_{\mathfrak{p}}$ is integrally closed for all $\mathfrak{p} \in \mathrm{Spec}(A)$.
3. $A_{\mathfrak{m}}$ is integrally closed for all $\mathfrak{m} \in \mathrm{Spec}_m(A)$.

Remark 6.10. Saying A is integrally closed means integrally closed in its field of fractions. Saying $A_{\mathfrak{p}}$ is integrally closed means integrally closed in $S^{-1}K = K$, where $S^{-1} = A - \mathfrak{p}$. Likewise for $A_{\mathfrak{m}}$.

Proof. Let $\overline{(-)}$ denote integral closure. By Proposition 6.7, $(\overline{A})_{\mathfrak{p}} = (A_{\mathfrak{p}})^{-}$.

($1 \Rightarrow 2$) If A is integrally closed, then $A = \overline{A}$ so $A_{\mathfrak{p}} = (\overline{A})_{\mathfrak{p}} = (A_{\mathfrak{p}})^{-}$, so $A_{\mathfrak{p}}$ is its own integral closure, i.e. is integrally closed.

($2 \Rightarrow 3$) Immediate, since every maximal ideal is prime.

($3 \Rightarrow 1$) Suppose $A_{\mathfrak{m}}$ is integrally closed for all $\mathfrak{m} \in \mathrm{Spec}_m(A)$. Consider $A \hookrightarrow \overline{A}$. Now for all $\mathfrak{m} \in \mathrm{Spec}_m(A)$, we have that $A_{\mathfrak{m}} \to (\overline{A})_{\mathfrak{m}} = (A_{\mathfrak{m}})^{-}$ is surjective by hypothesis. But being surjective is a localy property (Proposition 3.38), so $A \hookrightarrow \overline{A}$ is surjective, hence $A = \overline{A}$. □

7 flat and projective modules

Definition 7.1. An A-module Q is *flat* if the functor

$$Q \otimes_A (-) : A\mathrm{Mod} \to \mathrm{Ab}$$

is exact.

Remark 7.2. Note tensoring is always right exact, so the only content here is that tensoring is now also left exact.

8 linear algebra

Definition 8.1. Given $M \in M_n(A)$, the (i,j)*-minor* of M, denoted $M(i,j)$, is element of A equal to the determinant of the matrix equal to M but with each entry in its ith row and jth column set to 0.

Definition 8.2. The *adjugate* of $M \in M_n(A)$ is the matrix defined as

$$(M^{\natural})_{i,j} = (-1)^{i+j} M(j,i).$$

Corollary 8.3. The determinant of the matrix equal to M but with it's ith column replaced by e_k is $(M^{\natural})_{ik}$.

Corollary 8.4. $(M^{\natural} M) = (\det(M)) \cdot I$.

Lemma 8.5 (Cayley-Hamilton trick)**.** Let M be a finitely-generated R-module. Let $\mathfrak{a} \subset R$ be an ideal. Let $\phi : M \to M$ be an R-module endomorphism such that $\phi(M) \subset \mathfrak{a}M$. Then ϕ satisfies a monic polynomial

$$0 = \phi^n + c_1\phi^{n-1} + \cdots + c_{n-1}\phi + c_n$$

with $c_i \in \mathfrak{a}^i$.

Proof. Let $\{m_1, \ldots, m_n\}$ be a generating set for M as an R-module. $\phi(M) \subset \mathfrak{a}M$ by assumption, so for $j = 1, \ldots, n$ we have that $\phi(m_j) = \sum_i a_{ij}m_i$ for some $a_{ij} \in \mathfrak{a}$. Now view M as an $R[X]$-module via the action induced from ϕ:

$$f \cdot m = f(\phi)(m), \quad f \in R[X], m \in M.$$

Under this action, for all j we have that $Xm_j = \phi(m_j) = \sum_i a_{ij}m_i$, i.e. for all j

$$\sum_i (X\delta_{ij} - a_{ij})(m_i) = Xm_j - \sum_i a_{ij}m_i = 0.$$

Since this is true for all j, we can express it as a matrix:

$$(XI - A)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

where $A_{i,j} = a_{ij}$. Multiplying both sides by $(XI - A)^\natural$ gives

$$\det(XI - A)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

Note $XI - A \in M_n(R[X])$, hence the determinant is in $R[X]$. Write $f = \det(XI - A)$. Then this shows that $f \in \mathrm{Ann}_{R[X]}(M)$. But for any $m \in M$ we also have $f \cdot m = f(\phi)(m) = 0$, so in particular $f(\phi) = 0$ in $\mathrm{End}(M)$. It remains to show that f is a monic polynomial.

Using an alternative definition of the determinant,

$$\begin{aligned} f = \det(XI - A) = &\sum_{\sigma \in S_n} (-1)^{\mathrm{sgn}(\sigma)}(XI - A)_{\sigma(1),1} \cdots (XI - A)_{\sigma(n),n} \\ =&X^n + \cdots \end{aligned}$$

which is a monic polynomial, where we have just observed that the top-degree term is only derived from the product of n copies of XI. But also the coefficient of the X^i term is the sum of products which look like the i-fold product of X multiplied by the $(n-i)$-fold product of some a_k which are entries in A. □