Commutative Algebra

Runi Malladi

April 14, 2023

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.

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

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. $\square$

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.

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. $\square$ 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. $\square$

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 ref
in this ring correspond to ideals in $\mathbb{Z}$ containing (p^k) by , the ideals in this ring have ref
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).

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 ref
$\mathfrak{m} \subset A$ be maximal. But $\mathfrak{m} \subset A - A^\times$, so $\mathfrak{m} = A - A^\times$. □

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

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

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 $x \notin \mathrm{Nil}(A)$ then $x \notin \bigcap \mathrm{Spec}(A)$. So suppose $x \notin \mathrm{Nil}(A)$. 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 $x \notin \bigcap \mathrm{Spec}(A)$. □

Since $\mathrm{Nil}(A)$ 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

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

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

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

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

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. $\operatorname{Nil}(A) = \sqrt{0}$.

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

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

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, $\sqrt{a} = \pi^{-1}(\operatorname{Nil}(A/\mathfrak{a}))$. By (Proposition 1.21),

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

By Propositions 1.42 and 1.40,

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

□

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

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

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 $(\mathfrak{a} : x) = \text{Ann}(\bar{x} \in A/\mathfrak{a})$ 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

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

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

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

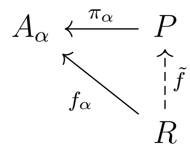
1.8 products

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:



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

$$\phi : A \longrightarrow (e) \times A/(e)$$

$$a \mapsto (ae, [a])$$

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 $\sum_n c_nd_n$ 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]i.e. $I + J = A$

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 $J(A)$.

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 $\{x_1, \dots, x_n\}$ 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 $x_1, \dots, x_n$. □

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

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

generates M if and only if its image in the quotient

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

generates M/IM.

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

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

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

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

(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

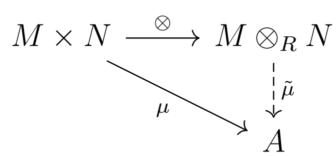
- (biadditive)

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

- (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:



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

$$\begin{gathered} e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)} \\ e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')} \\ e_{(mr,n)} - e_{(m,rn)}. \end{gathered}$$

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

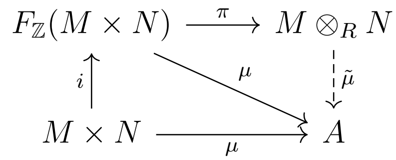
$$\begin{gathered} \otimes : M \times N \to F_{\mathbb{Z}}(M \times N) \to F_{\mathbb{Z}}(M \times N)/J = M \otimes_R N \\ (m, n) \mapsto e_{(m,n)} \mapsto [e_{(m,n)}] = m \otimes n \end{gathered}$$

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:



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

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

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

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

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:

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

□

Corollary 2.12.

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

Corollary 2.13.

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

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

$$\tilde{\mu_p} : M \otimes_R N \to M \otimes_R (N \otimes_S P)$$

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

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

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:

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

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

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

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

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

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

$$f(m + m', (n_\alpha)_\alpha) = ((m + m') \otimes n_\alpha)_\alpha = (m \otimes n_\alpha + m' \otimes n_\alpha)_\alpha = f(m, (n_\alpha)_\alpha) + f(m', (n_\alpha)_\alpha),$$
$$f(m, ((n_\alpha + n'_\alpha)_\alpha) = (m \otimes n_\alpha + m \otimes n'_\alpha)_\alpha = f(m, (n_\alpha)_\alpha) + f(m, (n'_\alpha)_\alpha).$$

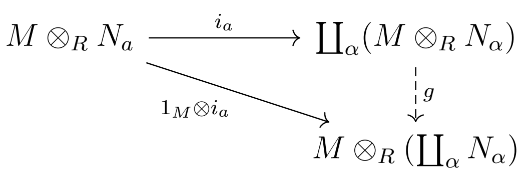
To see it is balanced:

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

Hence we have an induced map

$$M \otimes (\coprod_\alpha N_\alpha) \to \coprod_\alpha (M \otimes_R N_\alpha)$$
$$(m, (n_\alpha)_\alpha) \mapsto (m \otimes n_\alpha)_\alpha.$$

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



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

$$\begin{aligned} A \times B \times A \times B &\to A \otimes_k B \\ (a, b, a', b') &\mapsto aa' \otimes bb'. \end{aligned}$$

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

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

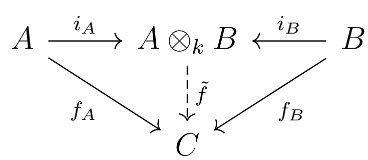
Since this should agree with our original map, we have

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

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:



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

$$A \times B \to C$$
$$(a, b) \mapsto f_A(a)f_B(b).$$

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: