Course notes for PMATH 646

Christa Hawthorne

Lectures by Rahim N. Moosa, Winter 2016

Contents

1 Preliminaries

My thanks to Mitchell Haslehurst for the use of his notes when I was absent.

Assignments and final; no midterm. Marks will probably be 35% assignments, 5 or 6 assignments, 65% final.

Office hours will be Mondays 13:30-14:30+ and 2016-01-20 13:30-14:30; can always come by and see if he's in.

Do not collaborate on assignments.

Rings are unital, commutative, and non-trivial. Prime ideals are proper. Maximal ideals are proper.

1.1 Ring theory

Definition 1.1.1. We say an ideal P of R is *prime* if $ab \in P$ implies $a \in P$ or $b \in P$.

Remark 1.1.2. Equivalently, if $a_1, \ldots, a_n \in P$ implies $a_i \in P$ for some i. Equivalently, if R/P is an integral domain.

Example 1.1.3. In $\mathbb{C}[x]$, let $I = x^2\mathbb{C}[x]$. Then $x \cdot x \in I$, but $x \notin I$. So I is not prime.

Definition 1.1.4. We say $e \in R$ is *idempotent* if $e^2 = e$.

Definition 1.1.5. We say an ideal M of R is *maximal* if there does not exist an ideal J of R with $M \subsetneqq J$.

Theorem 1.1.6 (Correspondence theorem)**.** *There is an inclusion-preserving bijection between ideals of R/I and ideals of R that contain I.*

In particular, we send an ideal $\overline{J}$ of R/I to $\pi^{-1}(\overline{J}) \subseteq R$; we send an ideal J of R to $\pi(J) \subseteq R/I$.

Corollary 1.1.7. *An ideal M of R is maximal if and only if R/M is a field.*

Proof. Note that M is maximal if and only if the only ideals of R that contain M are $\{ M, R \}$; by the correspondence theorem, this is equivalent to $F = R/M$ having exactly two ideals (namely (0) and F).

Now, if $a \in F \setminus \{ 0 \}$, then Fa is a non-zero ideal of F; so $Fa = F$ and $1 \in Fa$, and there is $b \in F$ such that $ba = 1$. So F is a field.

Conversely, if F is a field, then (0) and F are its only ideals. □ Corollary 1.1.7

Corollary 1.1.8. *Maximal ideals are prime.*

Theorem 1.1.9 (Zorn's lemma)**.** *Suppose $(P, \leq)$ is a partially ordered set (e.g. ideals of a ring ordered by set inclusion). If every chain in P has an upper bound, then P has a maximal element.*

(A *chain* is $(x_\gamma : \gamma \in \Gamma)$ where Γ is totally ordered and if $\gamma_1 \leq \gamma_2$ then $x_{\gamma_1} \leq x_{\gamma_2}$. An *upper bound* is an x such that $x \geq x_\gamma$ for all $\gamma \in \Gamma$.)

Remark 1.1.10. One needs to prove this for arbitrary Γ; it does *not* suffice to check the case $\Gamma = \mathbb{N}$.

Example 1.1.11. Let P be the collection of countable subsets of $\mathbb{R}$ ordered by set inclusion. Then if $S_1 \subseteq S_2 \subseteq S_3 \subseteq \dots$ is a chain in P, we have

$$\bigcup_{i=1}^{\infty} S_i$$

is an upper bound. But P has no maximal element, since if $S \in P$ is maximal, then we may pick $x \in \mathbb{R} \setminus S$; then $S \cup \{ x \} \supsetneqq S$ and $S \cup \{ x \}$ is countable.

Corollary 1.1.12. *Let R be a ring. Then R has a maximal ideal. In fact, if I is an ideal of R, then there is a maximal ideal containing I.*

Proof. Suppose I is an ideal of R. Let $S = \{ J : J \supseteq I, J \text{ is an ideal of } R \}$ be ordered by $\subseteq$. Note that S is non-empty since $I \in S$. Further note that a maximal element of S is a maximal ideal that contains I.

Let Γ be a totally ordered set; let $(J_\gamma : \gamma \in \Gamma)$ be a chain in S.

Claim 1.1.13.

$$\bigcup_{\gamma \in \Gamma} J_\gamma \in S$$

Proof. Well, $1 \notin J_\gamma$ for any $\gamma \in \Gamma$ since J_γ is a proper ideal. So

$$1 \notin \bigcup_{\gamma \in \Gamma} J_\gamma$$

Furthermore, it holds in general that the union of a chain of ideals is an ideal. □ Claim 1.1.13

So this is an upper bound. So Zorn's lemma gives us that S has a maximal element. □ Corollary 1.1.12

Remark 1.1.14. For rings without identity, there might not be any maximal ideals.

Example 1.1.15. Let $R = \{ w \in \mathbb{C} : \exists j \geq 1 \text{ such that } w^{2^j} = 1 \}$.

Fact 1.1.16. *Any proper subgrape of R is finite, and is $R_n = \{ w : w^{2^n} = 1 \}$ for some $n \in \mathbb{N}$.*

Define a ring structure on R by $r \oplus s = rs$ and $r \otimes s = 1$. Note then that 1 is the additive identity, and the ring axioms are satisfied. Then ideals in $(R, \oplus, \otimes)$ are exactly subgrapes of $(R, \cdot)$. Then

$$R_1 \subsetneqq R_2 \subsetneqq R_3 \subsetneqq \dots \subsetneqq R$$

So R has no maximal ideals.

1.2 Modules

Definition 1.2.1. Suppose R is a ring. Then an *R-module* is an abelian grape $(M, +)$ with a map $R \times M \to M$ (written $(r, m) \mapsto r \cdot m$) such that the following hold for all $r, s \in R$ and all $m, m_1, m_2 \in M$:

- $r \cdot (s \cdot m) = (r \cdot s) \cdot m$.
- $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.
- $(r + s) \cdot m = r \cdot m + s \cdot m$.
- $1_R \cdot m = m$.

Remark 1.2.2. We then have that $r \cdot 0_M = 0_M$ for all $r \in R$.

Example 1.2.3.

1. Suppose $R = F$ is a field and V is a vector space over F. Then V is an F-module.
2. Suppose $R = \mathbb{Z}$ and $(A, +)$ is an abelian grape. Then A is a $\mathbb{Z}$-module under

$$n \cdot a = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ times}} & n \geq 0 \\ \underbrace{(-a) + \cdots + (-a)}_{|n| \text{ times}} & n < 0 \end{cases}$$

3. Suppose $R = \mathbb{R}[x]$ and $M = (\mathbb{C}, +)$. Define $p(x) \cdot \alpha = p(i)\alpha$; then M is an R-module under this multiplication.

Definition 1.2.4. Suppose R is a ring and M is an R-module. Given $S \subseteq M$, we define the *annihilator* of S to be

$$\mathrm{Ann}_R(S) = \{\, r \in R : rs = 0 \text{ for all } s \in S \,\}$$

Remark 1.2.5. If $S = \{\, m \,\}$ for some $m \in M$, we have $\mathrm{Ann}_R(m) = \mathrm{Ann}_R(\{\, m \,\}) = \{\, r \in R : rm = 0 \,\}$. If $S = M$, then $\mathrm{Ann}_R(M) = \{\, r \in R : rm = 0 \text{ for all } m \in M \,\}$.

Remark 1.2.6. $\mathrm{Ann}_R(S)$ is an ideal of R.

Definition 1.2.7. We say that M is a *faithful* R-module if $\mathrm{Ann}_R(M) = (0)$.

Example 1.2.8.

1. Consider $M = \mathbb{Z}/15\mathbb{Z}$ as a $\mathbb{Z}$-module. Then $\mathrm{Ann}_{\mathbb{Z}}(M) = 15\mathbb{Z}$.
2. Consider $M = (\mathbb{C}, +)$ as an $\mathbb{R}[x]$-module as in Example 1.2.3. Then $\mathrm{Ann}_{\mathbb{R}[x]}(M) = (x^2 + 1)\mathbb{R}[x]$.

Definition 1.2.9. An R-module M is *finitely generated* if there is a finite subset $\{\, m_1, \ldots, m_d \,\} \subseteq M$ such that

$$M = Rm_1 + Rm_2 + \cdots + Rm_d = \{\, r_1 m_1 + r_2 m_2 + \cdots + r_d m_d : r_1, \ldots, r_d \in R \,\}$$

Example 1.2.10. $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module. To see this, note that if

$$\mathbb{Q} = \mathbb{Z}\frac{m_1}{n_1} + \cdots + \mathbb{Z}\frac{m_d}{n_d}$$

where each $m_i, n_i \in \mathbb{Z}$ and each $n_i > 0$, then $\mathbb{Q} \subseteq \mathbb{Z}\frac{1}{N}$ where $N = n_1 n_2 \ldots n_d$, a contradiction.

Definition 1.2.11. Suppose M is an R-module. A *submodule* of M is an abelian subgrape $(N, +) \subseteq (M, +)$ that is closed under multiplication by R; i.e. if $r \in R$ and $n \in N$ then $r \cdot n \in N$.

Example 1.2.12. If I is an ideal of R then I is a submodule of R (where we regard R as a module over itself).

Definition 1.2.13. Suppose $N \subseteq M$ is a submodule. We define the module $M/N = \{ m + N : m \in M \}$ to be the quotient as an abelian grape together with the multiplication $r \cdot (m + N) = r \cdot m + N$.

Remark 1.2.14. This is well-defined: if $m_1 + N = m_2 + N$, then $m_1 - m_2 = n \in N$, and $rm_1 - rm_2 = r(m_1 - m_2) = rn \in N$; so $rm_1 + N = rm_2 + N$.

Definition 1.2.15. Suppose R be a ring; suppose M and N are R-modules. A map $f\colon M \to N$ is an *R-module homomorphism* or *R-homomorphism* if it satisfies the following

- $f(m_1 + m_2) = f(m_1) + f(m_2)$ for all $m_1, m_2 \in M$
- $f(r \cdot m) = r \cdot f(m)$ for all $r \in R$ and $m \in M$.

Example 1.2.16. Linear transformations, homomorphisms of abelian grapes.

Notation 1.2.17. We let $\hom_R(M, N)$ be the set of R-module homomorphisms $M \to N$.

Remark 1.2.18. If $f, g \in \hom_R(M, N)$ then $(f + g)(m) = f(m) + g(m)$ and $(-f)(m) = -(f(m))$ are also R-module homomorphisms. If $f \in \hom_R(M, N)$ and $r \in R$, then $(rf)(m) = r(f(m)) = f(rm)$ is also an R-module homomorphism. So we can make $\hom_R(M, N)$ into an R-module in a natural way.

Notation 1.2.19. If $f\colon M \to N$ is an R-module homomorphism then we set $\ker(f) = \{ m \in M : f(m) = 0 \}$; then this is a submodule of M since if $m_1, m_2 \in \ker(f)$ and $r \in R$ then $f(m_1 + m_2) = f(m_1) + f(m_2) = 0$ and $f(rm_1) = rf(m_1) = 0$, so $m_1 + m_2, rm_1 \in \ker(f)$.

We also set $\operatorname{im}(f) = \{ f(m) : m \in M \} \subseteq N$; then $\operatorname{im}(f)$ is a submodule of N.

Exercise 1.2.20 (First isomorphism theorem for R-modules). $M/\ker(f) \cong \operatorname{im}(f)$.

Definition 1.2.21. Suppose R is a ring. Suppose $(M_\alpha : \alpha \in I)$ is a collection of R-modules. We define the *direct sum* of the M_α to be

$$\bigoplus_{\alpha \in I} M_\alpha = \{ (m_\alpha : \alpha \in I) : m_\alpha \in M_\alpha \text{ for all } \alpha \in I, m_\alpha = 0 \text{ for all but finitely many } \alpha \in I \}$$

We make this into an R-module by

$$\begin{aligned} (m_\alpha : \alpha \in I) + (m'_\alpha : \alpha \in I) &= (m_\alpha + m'_\alpha : \alpha \in I) \\ r \cdot (m_\alpha : \alpha \in I) &= (r \cdot m_\alpha : \alpha \in I) \end{aligned}$$

We also define

$$\prod_{\alpha \in I} M_\alpha = \{ (m_\alpha : \alpha \in I) : m_\alpha \in M_\alpha \text{ for all } \alpha \in I \}$$

with coordinate-wise addition and multiplication by R as above; this too is an R-module.

Remark 1.2.22. If $|I| < \infty$ then

$$\bigoplus_{\alpha \in I} M_\alpha \cong \prod_{\alpha \in I} M_\alpha$$

Question 1.2.23. Let $R = \mathbb{Z}$, $I = \mathbb{N}$, and $M_\alpha = \mathbb{Z}$ for all $\alpha \in I$. Does it hold that

$$\bigoplus_{i \in I} \mathbb{Z} \cong \prod_{i \in I} \mathbb{Z}$$

as $\mathbb{Z}$-modules?

No, because

$$\left| \bigoplus_{i \in I} \mathbb{Z} \right| = \aleph_0 < 2^{\aleph_0} = \left| \prod_{i \in I} \mathbb{Z} \right|$$

Definition 1.2.24. An R-module M has a *basis* if there is $S \subseteq M$ such that every $m \in M$ has a unique expression

$$m = \sum_{s \in S} r_s \cdot s$$

where $r_s = 0$ for all but finitely many $s \in S$. In this case we say M is a *free R-module*.

Remark 1.2.25. This is equivalent to saying that

$$M \cong \bigoplus_{s \in S} R$$

where the isomorphism is

$$\begin{aligned} f\colon \qquad \bigoplus_{s \in S} R &\to M \\ (r_s : s \in S) &\mapsto \sum_{s \in S} r_s \cdot s \end{aligned}$$

Question 1.2.26 (Hard). Does

$$\prod_{i \in I} \mathbb{Z}$$

have a basis? (It does not.)

1.3 Jacobson radical

Definition 1.3.1. Suppose R is a ring with unity. We define the *Jacobson radical* of R to be

$$J(R) = \bigcap_{M \text{ a maximal ideal of } R} M$$

Remark 1.3.2. As noted before, since R has unity, we have at least one maximal ideal of R; so the intersection is non-empty.

One can often study $R/J(R)$, which is typically nicer, and lift results to R.

Example 1.3.3.

1. Consider $R = \mathbb{Z}$. What is $J(\mathbb{Z})$? Well, in $\mathbb{Z}$ prime ideals are maximal. So

   $$J(\mathbb{Z}) = \bigcap_{p \text{ prime}} p\mathbb{Z}$$

   So if $n \in J(\mathbb{Z})$, then $p \mid n$ for all primes p. So $n = 0$. So $J(\mathbb{Z}) = (0)$.

2. Let

   $$R = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \notin 2\mathbb{Z} \right\}$$

   First note that $\frac{a}{b} \in R$ is a unit exactly when a is odd. What are the maximal ideals of R? Well, if I is an ideal of R, then I cannot contain units; so $I \subseteq 2R$. But $2R$ is an ideal. So $2R$ is the unique maximal ideal. So $J(R) = 2R$.

3. Let $R = \mathbb{C}[x]$. What are the maximal ideals of $\mathbb{C}[x]$? Well, if I is a non-zero ideal of R then $I = (p(x)) \subseteq (x - \lambda_1)$ where $p(x)$ is monic; say $p(x) = (x - \lambda_1) \dots (x - \lambda_d)$ where $\lambda_1, \dots, \lambda_d \in \mathbb{C}$. So every proper ideal of R is contained in an ideal $(x - \lambda)$ for some $\lambda \in \mathbb{C}$.

   On the other hand, if $(x - \lambda) \subseteq (p(x))$, then $p \mid x - \lambda$; so p is either a unit, in which case $(p(x)) = \mathbb{C}[x]$, or p has degree 1, in which case $(p(x)) = (x - \lambda)$.

   (Alternatively, consider $\psi\colon \mathbb{C}[x] \to \mathbb{C}$ given by $f \mapsto f(\lambda)$. Then ψ is a surjective homomorphism with $\ker(\psi) = (x - \lambda)$. So, by the first isomorphism theorem, we have $\mathbb{C}[x]/(x - \lambda) \cong \mathbb{C}$ is a field. So $(x - \lambda)$ is maximal.)

Proposition 1.3.4. *If $x \in J(R)$ then for all $a \in R$ we have $1 - ax$ is a unit in R.*

Proof. Suppose for contradiction that $1 - ax$ is not a unit. Then $R(1 - ax) \subsetneq R$; so there is a maximal ideal M such that $R(1 - ax) \subseteq M$, and in particular we have $1 - ax \in M$. But $x \in J(R) \subseteq M$; so $1 = ax + (1 - ax) \in M$, a contradiction. □ Proposition 1.3.4

Theorem 1.3.5 (Nakayama's lemma)**.** *Suppose R is a ring and M is a finitely generated R-module. Suppose $J(R)M = M$. Then $M = (0)$.*

Proof. Suppose for contradiction that $M \neq (0)$. Pick a generating set $\{ m_1, \dots, m_d \}$ for M with d minimal. (So

$$M = Rm_1 + \cdots + Rm_d$$

and no set of size $< d$ works.) Since $M \neq (0)$, we have $d \geq 1$. Since $J(R)M = M$, we have $m_d \in J(R)M$; so there are $j_1, j_2, j_3, \dots, j_d \in J(R)$ such that

$$m_d = j_1 m_1 + j_2 m_2 + \cdots + j_d m_d$$

so

$$(1 - j_d) m_d = j_1 m_1 + j_2 m_2 + \cdots + j_{d-1} m_{d-1}$$

But $1 - j_d$ is a unit by the previous proposition. So

$$m_d = (1 - j_d)^{-1} j_1 m_1 + \cdots + (1 - j_d)^{-1} j_{d-1} m_{d-1} \in Rm_1 + \cdots + Rm_{d-1}$$

So $\{ m_1, \dots, m_{d-1} \}$ generates M, contradicting the minimality of d. So $M = (0)$. □ Theorem 1.3.5

Proposition 1.3.6. *Suppose $x \in R$ has the property that $1 - ax$ is a unit for all $a \in R$. Then $x \in J(R)$.*

Proof. Suppose $x \notin J(R)$. Then there is a maximal ideal M such that $x \notin M$. Let $F = R/M$; then F is a field. Let $\overline{x} = x + M \in F$ be the image of x in F; then $\overline{x} \neq 0$ since $x \notin M$. Since F is a field, there is $a \in R$ such that $\overline{ax} = 1$ in F. Then $\overline{1 - ax} = 0$; so $1 - ax \in M$, and $1 - ax$ is not a unit. □ Proposition 1.3.6

Corollary 1.3.7. *$x \in J(R)$ if and only if $1 - ax$ is a unit for all $a \in R$.*

Question 1.3.8. In Nakayama's lemma, is the requirement that M be finitely generated necessary? Yes: consider

$$R = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \notin 2\mathbb{Z} \right\}$$

Notice that $\mathbb{Q}$ is an R-module by

$$\frac{a}{b} \frac{c}{d} = \frac{ab}{cd}$$

Well, $J(R)\mathbb{Q} = (2R)(\frac{1}{2}\mathbb{Q}) = R\mathbb{Q} = \mathbb{Q}$. So $J(R)\mathbb{Q} = \mathbb{Q}$ but $\mathbb{Q} \neq (0)$. (This shows that $\mathbb{Q}$ is not finitely generated as an R-module.)

Question 1.3.9. Let $R = \mathbb{Z}/720\mathbb{Z}$. What is $J(R)$? Well, $720 = 2^4 \cdot 3^2 \cdot 5$. The maximal ideals are $2R, 3R, 5R$; so their intersection is $30R$.

2 Chapter 2

We begin to follow Atiyah and Macdonald.

2.1 Exact sequences

Fix a ring A; suppose $M_0, \dots, M_n$ are A-modules and $f_i \colon M_i \to M_{i+1}$ are A-module homomorphisms; we write this as

$$M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-2}} M_{n-1} \xrightarrow{f_{n-1}} M_n$$

Definition 2.1.1. We say this sequence is *exact* at M_i for $i \in \{1, \dots, n-1\}$ if $\operatorname{im}(f_{i-1}) = \ker(f_i)$. We say the sequence is *exact* if it isexact at each $M_1, \dots, M_{n-1}$.

Remark 2.1.2. Suppose $f \colon M' \to M$ is a homomorphism of A-modules. Then f is injective if and only if $0 \to M' \xrightarrow{f} M$ is exact.

(Here 0 denotes the trivial A-module, and the unnamed homomorphism $0 \to M'$ is the zero homomorphism. (In general, the *zero homomorphism* $0 \colon N \to P$ is the A-homomorphism that sends everything to 0_P.))

Proof. Well, $\operatorname{im}(0) = \{0\}$; so exactness is equivalent to $\ker(f) = \{0\}$, which is equivalent to f being injective. $\square$ Remark 2.1.2

Remark 2.1.3. $f \colon M \to M''$ is surjective if and only if $M \xrightarrow{f} M'' \to 0$ is exact.

Proof. The homomorphism $M'' \to 0$ is again the zero homomorphism whose kernel is M''; so exactness at M'' is equivalent to $\operatorname{im}(f) = M''$, which is equivalent to f being surjective. $\square$ Remark 2.1.3

Remark 2.1.4. A sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact if and only if

1. f is injective
2. g is surjective
3. $\operatorname{im}(f) = \ker(g)$

This follows from the previous remarks and the definition of exactness.

Definition 2.1.5. A *short exact sequence* is an exact sequence of the form $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$. If M fits into such an exact sequence (in the middle position) then we say that M is an *extension* of M'' by M'.

Example 2.1.6. Given A-modules M'' and M', let $M = M' \oplus M''$. Then we have an injective A-homomorphism $\iota_1 \colon M' \to M$ given by $x \mapsto (x, 0_{M''})$; we also have a surjective A-homomorphism $\pi_2 \colon M \to M''$ given by $(x, y) \mapsto y$. Furthermore, we have $\operatorname{im}(\iota_1) = \ker(\pi_2)$. So $0 \to M' \xrightarrow{\iota_1} M' \oplus M'' \xrightarrow{\pi_2} M'' \to 0$ is exact.

Definition 2.1.7. A short exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is *split* if there is an A-isomorphism $\alpha \colon M \to M' \oplus M''$ such that the following diagram commutes:

$$\begin{tikzcd}
M' \arrow[r, "f"] \arrow[dr, "\iota_1"'] & M \arrow[r, "g"] \arrow[d, "\alpha"] & M'' \\
 & M' \oplus M'' \arrow[ur, "\pi_2"'] &
\end{tikzcd}$$

Example 2.1.8 (A non-split short exact sequence). Let $A = \mathbb{Z}$; fix $n > 1$. Then $0 \to n\mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$ is exact. However, $\mathbb{Z}$ is torsion-free (i.e. it has no non-zero elements of finite order), and $n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ has torsion: $n(0, 1 + n\mathbb{Z}) = (n0, n(1 + n\mathbb{Z})) = (0, n + n\mathbb{Z}) = (0, 0 + n\mathbb{Z}) = 0_{\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}}$. So $\mathbb{Z} \ncong n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$; so the short exact sequence is not split.

Remark 2.1.9.

1. If $f \colon M' \to M$ is injective then the exact sequence $0 \to M' \xrightarrow{f} M$ extends to a short exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M/M' \to 0$ (where g is the quotient map and M' is identified with $\operatorname{im}(f)$).
2. If $g \colon M \to M''$ is surjective then $0 \to \ker(g) \xrightarrow{\subseteq} M \xrightarrow{g} M'' \to 0$ is a short exact sequence.

3. More generally, given any A-homomorphism $f\colon M \to N$ we get a short exact sequence

$$0 \to \ker(f) \xrightarrow{\subseteq} M \xrightarrow{f} \operatorname{im}(f) \to 0$$

How can we tell if a short exact sequence splits? (Note that the following answer is not in the text.)

Lemma 2.1.10 (Splitting lemma)**.** *Suppose $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is a short exact sequence. Then the following are equivalent:*

1. *The sequence splits.*
2. *There is A-linear $\widehat{g}\colon M'' \to M$ such that $g \circ \widehat{g} = \mathrm{id}_{M''}$.*
3. *There is A-linear $\widehat{f}\colon M \to M'$ such that $\widehat{f} \circ f = \mathrm{id}_{M'}$.*

Proof.

(1) $\implies$ (2) Suppose we have an isomorphism $\alpha\colon M \to M' \oplus M''$ such that the following diagram commutes:

$$\begin{tikzcd} M' \arrow[r, "f"] \arrow[dr, "\iota_1"'] & M \arrow[r, "g"] \arrow[d, "\alpha"] & M'' \\ & M' \oplus M'' \arrow[ur, "\pi_2"'] & \end{tikzcd}$$

Let $\iota_2\colon M'' \to M' \oplus M''$ be the injection pointed out above. Let $\widehat{g} = \alpha^{-1} \circ \iota_2$; then

$$g \circ \widehat{g} = \pi_2 \circ \alpha \circ \alpha^{-1} \circ \iota_2 = \pi_2 \circ \iota_2 = \mathrm{id}_{M''}$$

(2) $\implies$ (3) Given $x \in M$ consider $\widehat{g}(g(x)) \in M$. Then $g(x - \widehat{g}(g(x))) = g(x) - g(\widehat{g}(g(x))) = g(x) - g(x) = 0$; so $x - \widehat{g}(x) \in \ker(g) = \operatorname{im}(f)$. So $x - \widehat{g}(g(x)) = f(y)$ for some $y \in M'$; by injectivity of f, we have that y is unique. We define $\widehat{f}(x)$ to be this y. One then checks that $\widehat{f}$ is A-linear (i.e. a homomorphism of A-modules).

Now, suppose $y \in M'$; then $\widehat{f}(f(y))$ is the unique $z \in M'$ such that $f(y) - \widehat{g}(g(f(y))) = f(z)$. But $g(f(y)) = 0$; so $\widehat{f}(f(y))$ is the unique $z \in M'$ such that $f(y) = f(z)$; so $z = y$.

(3) $\implies$ (1) Define $\alpha\colon M \to M' \oplus M''$ by $x \mapsto (\widehat{f}(x), g(x))$. Then α is A-linear since $\widehat{f}$ and g are.

For injectivity of α, note that if $\alpha(x) = 0$ then $\widehat{f}(x) = 0$ and $g(x) = 0$. Then $x \in \ker(g) = \operatorname{im}(f)$, and $x = f(y)$ for some $y \in M'$; so $0 = \widehat{f}(x) = \widehat{f}(f(y)) = y$, and $f(y) = 0$.

For surjectivity of α, suppose $(y, z) \in M' \oplus M''$. By surjectivity of g we have some $x \in M$ such that $g(x) = z$; however, there is no reason to expect that $\widehat{f}(x) = y$. Consider instead $u = f(y - \widehat{f}(x)) + x \in M$; then

$$g(u) = g(f(y - \widehat{f}(x))) + g(x) = g(x) = z$$

and

$$\widehat{f}(u) = \widehat{f}(f(y - \widehat{f}(x))) + \widehat{f}(x) = y - \widehat{f}(x) + \widehat{f}(x) = y$$

So $\alpha(u) = (y, z)$, and α is surjective.

We now check that the following diagram commutes:

$$\begin{tikzcd} & M \arrow[dd, "\alpha"] \\ M' \arrow[ur, "f"] \arrow[dr, "\iota_1"'] & \\ & M' \oplus M'' \end{tikzcd}$$

Note that if $y \in M'$ then

$$\alpha(f(y)) = (\widehat{f}(f(y)), g(f(y))) = (y, 0) = \iota_1(y)$$

One also checks that the following diagram commutes:

$$\begin{tikzcd}
M \arrow[d, "\alpha"] \arrow[dr, "g"] & \\
& M' \\
M' \oplus M'' \arrow[ur, "\pi_2"] &
\end{tikzcd}$$

□ Lemma 2.1.10

Example 2.1.11.

1. This gives another proof that $0 \to n\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$ (over $A = \mathbb{Z}$) does not split: there can be no non-trivial maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ since the former has torsion and the latter does not, so there is no right inverse of the map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

2. Consider $A = k$ a field; then A-modules are exactly k-vector spaces.

   Proposition 2.1.12. *Every short exact sequence* $0 \to V' \xrightarrow{f} V \xrightarrow{g} V'' \to 0$ *splits.*

   Proof. Let $B \subseteq V'$ be a k-basis (possibly infinite). Identifying V' with $f(V') \subseteq V$; we may then expand B to a k-basis $B \sqcup C$ of V. Define $\widehat{f}\colon V \to V'$ by $\widehat{f}(b) = b$ for all $b \in B$ and $\widehat{f}(c) = 0$ for all $c \in C$. Then $\widehat{f} \circ f = \mathrm{id}_{V'}$ as $\widehat{f} \circ f$ fixes B pointwise; so, by the splitting lemma, we have that the exact sequence splits. □ Proposition 2.1.12

Recall that if M, N are A-modules then $\hom_A(M, N)$ is the set of A-linear maps $f\colon M \to N$ with the natural A-module structure.

Remark 2.1.13.

1. Fix M an A-module. Then $\hom_A(M, -)$ is a covariant functor; i.e. given an A-linear map $v\colon N \to N'$ we have an induced A-linear map $\overline{v}\colon \hom(M, N) \to \hom(M, N')$ given by $f \mapsto v \circ f$.

2. Fix N an A-module. Then $\hom_A(-, N)$ is a contravariant functor; i.e. given an A-linear $v\colon M \to M'$ we have an induced A-linear map $\overline{v}\colon \hom(M', N) \to \hom(M, N)$ given by $g \mapsto g \circ v$.

Proposition 2.1.14 (2.9 (i))**.** *Fix M an A-module. Then $\hom(M, -)$ is left-exact; i.e. given an exact sequence* $0 \to N' \xrightarrow{u} N \xrightarrow{v} N''$, *we have*

$$0 = \hom(M, 0) \to \hom(M, N') \xrightarrow{\overline{u}} \hom(M, N) \xrightarrow{\overline{v}} \hom(M, N'')$$

is exact.

Proof. We first check that $\overline{u}$ is injective. Suppose $g \in \hom(M, N')$ has $u \circ g = \overline{u}(g) = 0$; then $g = 0$ since u is injective.

We then check that $\ker(\overline{v}) = \mathrm{im}(\overline{u})$. Suppose $h \in \mathrm{im}(\overline{u})$; say $h = u \circ f$ where $f \in \hom(M, N')$. Then $\overline{v}(h) = v \circ h = v \circ u \circ f = 0$ since $v \circ u = 0$ by exactness of the original exact sequence at N. So $\mathrm{im}(\overline{u}) \subseteq \ker(\overline{v})$. Conversely, suppose $h \in \ker(\overline{v})$. Define $f\colon M \to N'$ by noting that for $x \in M$, we have $h(x) \in \ker(v) = \mathrm{im}(u)$; then by injectivity of u there is a unique $y \in N'$ such that $u(y) = h(x)$, and we set $f(x)$ to be this y. One then checks that f is A-linear and that $\overline{u}(f) = h$. So $\mathrm{im}(\overline{u}) = \ker(\overline{v})$, and

$$0 = \hom(M, 0) \to \hom(M, N') \xrightarrow{\overline{u}} \hom(M, N) \xrightarrow{\overline{v}} \hom(M, N'')$$

is exact. □ Proposition 2.1.14

It is *not* generally the case that if $v\colon N \to N''$ is surjective then $\hom(M,N) \xrightarrow{\overline{v}} \hom(M,N'')$.

Example 2.1.15. Consider the quotient map $v\colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$; then $\overline{v}\colon \hom(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}) = 0 \to \hom(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/n\mathbb{Z})$ is *not* surjective.

Proposition 2.1.16 (2.9 (ii))**.** *Fix N an A-module. Then given an exact sequence $M' \xrightarrow{u} M \xrightarrow{v} M' \to 0$, we have*

$$0 = \hom(0,N) \to \hom(M'',N) \xrightarrow{\overline{v}} \hom(M,N) \xrightarrow{\overline{u}} \hom(M',N)$$

is exact. (Recall that $\hom(-,N)$ *is contravariant.)*

Exercise 2.1.17. Prove the above proposition, and prove it doesn't preserve full short exact sequences.

Exercise 2.1.18. $\hom_A(A,N) \cong N$.

2.2 Tensor products

Definition 2.2.1. Suppose M,N,P are A-modules. A set map $f\colon M \times N \to P$ is *A-bilinear* if for all $x \in M$ we have $f(x,-)\colon N \to P$ is A-linear and for all $y \in N$ we have $f(-,y)\colon M \to P$ is A-linear. i.e. for all $x,x' \in M$, all $y,y' \in N$ and all $a \in A$, we have

$$\begin{aligned} f(x,y+y') &= f(x,y) + f(x,y') \\ f(x+x',y) &= f(x,y) + f(x',y) \\ f(ax,y) &= af(x,y) \\ &= f(x,ay) \end{aligned}$$

We will define an A-module $M \otimes_A N$ with the property that A-bilinear maps $M \times N \to P$ are in bijection with A-linear maps $M \otimes_A N \to P$.

Let C be the free A-module on generators $M \times N$; i.e.

$$C = \bigoplus_{(x,y)\in M\times N} A \cdot (x,y)$$

is the set of formal finite A-linear combinations

$$\sum_{i=1}^{n} a_i(x_i,y_i)$$

where each $x_i \in M$, $y_i \in N$, and $a_i \in A$. Let $D \subseteq C$ be the submodule generated by elements of the form

- $(x+x',y) - (x,y) - (x',y)$
- $(x,y+y') - (x,y) - (x,y')$
- $(ax,y) - a(x,y)$
- $(x,ay) - a(x,y)$

for $x,x' \in M$, $y,y' \in N$, and $a \in A$.

Definition 2.2.2. We set $M \otimes_A N = C/D$. Given $x \in M$ and $y \in N$ we let $x \otimes y$ be the image in C/D of (x,y) (i.e. $(x,y) + D \in M \otimes_A N$); such elements are called *tensors*.

Remark 2.2.3. From the construction we see that

1. $M \otimes_A N$ is generated by tensors.

Proof. If $c \in C$, then

$$c = \sum_{i=1}^{n} a_i(x_i, y_i)$$

so

$$\pi(c) = \sum_{i=1}^{n} a_i \pi(x_i, y_i) = \sum_{i=1}^{n} a_i(x_i \otimes_A y_i)$$

where $\pi \colon C \to C/D$ is the quotient map. □

Note that the tensors do not *freely* generate $M \otimes_A N$; there is no uniqueness in writing elements of $M \otimes_A N$ as a linear combination of tensors.

2. $\otimes$ behaves bilinearly:

$$\begin{aligned} x \otimes (y + y') &= x \otimes y + x \otimes y' \\ (x + x') \otimes y &= x \otimes y + x' \otimes y \\ (ax) \otimes y &= x \otimes (ay) \\ &= a(x \otimes y) \end{aligned}$$

Example 2.2.4. With $A = \mathbb{Z}$, consider $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. Then $2 \otimes 1 \in \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$; in fact

$$\begin{aligned} 2 \otimes 1 &= 2(1 \otimes 1) \\ &= 1 \otimes 2 \\ &= 1 \otimes 0 \\ &= 1 \otimes (0 \cdot 1) \\ &= 0(1 \otimes 1) \\ &= 0 \end{aligned}$$

Example 2.2.5. Again with $A = \mathbb{Z}$, consider $2 \otimes 1 \in 2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. Then $2 \otimes 1 \neq 0$. Why?

Lemma 2.2.6. *In general if M is generated by $\{ x_1, \ldots, x_n \}$ and N is generated by $\{ y_1, \ldots, y_m \}$, then $M \otimes_A N$ is generated by $\{ x_i \otimes y_j : i \in \{ 1, \ldots, n \}, j \in \{ 1, \ldots, m \} \}$.*

Proof. $M \otimes_A N$ is generated by tensors $x \otimes y$ but

$$\begin{aligned} x &= \sum a_i x_i \\ y &= \sum b_j y_j \\ x \otimes y &= \left(\sum a_i x_i\right) \otimes \left(\sum b_j y_j\right) \\ &= \sum a_i b_j x_i \otimes y_j \end{aligned}$$

□ Lemma 2.2.6

So $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is generated as an A-module by $2 \otimes 1$. So if $2 \otimes 1 = 0$ then $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = 0$.

Lemma 2.2.7. *If $f \colon M \to N$ is A-linear and P is another A-module then there is an A-linear map $f \otimes \mathrm{id} \colon M \otimes_A P \to N \otimes_A P$ such that $(f \otimes \mathrm{id})(m \otimes p) = f(m) \otimes p$. If f is an isomorphism then so is $f \otimes \mathrm{id}$.*

Note that this is not completely trivial since not every element of the tensor product is a tensor, and representations as an A-linear combination of tensors are not unique. Thus

$$(2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{f \otimes \mathrm{id}} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \neq 0$$

(In general $A \otimes_A M \cong M$.) So $2 \otimes 1 \neq 0$ in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.

Moral: $2 \otimes 1 = 0$ in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ but $2 \otimes 1 \neq 0$ in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.

Going back to the converse of 2.9(i):

Theorem 2.2.8. *Suppose we have a (not necessarily exact) sequence*

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0 \tag{1}$$

such that for every A-module N we have

$$0 \to \hom(M'', N) \xrightarrow{\overline{v}} \hom(M, N) \xrightarrow{\overline{u}} \hom(M', N)$$

is exact. Then (1) is exact.

Proof. We first check surjectivity of v. Taking $N = \operatorname{coker}(v) = M''/\operatorname{im}(v)$, we have a projection $\pi \in \hom(M'', N)$; then $\overline{v}(\pi) = \pi \circ v = 0$, so by injectivity of $\overline{v}$ we have $\pi = 0$ and $\operatorname{coker}(v) = 0$. So v is surjective.

We now check that $\operatorname{im}(u) \subseteq \ker(v)$. Letting $N = M''$, we have that $0 = \overline{u}(\overline{v}(\mathrm{id}_{M''})) = v \circ u$; so $\operatorname{im}(u) \subseteq \ker(v)$.

We finally verify that $\ker(v) \subseteq \operatorname{im}(u)$. Taking $N = \operatorname{coker}(u)$ with the projection $\pi \in \hom(M, N)$, we have $0 = \overline{u}(\pi)$; so $\pi \in \ker(\overline{v}) \subseteq \operatorname{im}(\overline{v})$. So there is $f\colon M'' \to N$ such that $\pi = \overline{v}(f)$. But then for $x \in \ker(v)$, we have

$$\pi(x) = \overline{v}(f)(x) = f(v(x)) = 0$$

So $x \in \ker(\pi) = \operatorname{im}(u)$. □ Theorem 2.2.8

Theorem 2.2.9 (2.12—Universal property of tensor products)**.** *Suppose M, N are A-modules. Given any A-module P and any A-bilinear function $f\colon M \times N \to P$, there is a unique A-linear map $f'\colon M \otimes_A N \to P$ such that the following diagram commutes:*

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "\otimes"] & P \\ M \otimes_A N \arrow[ur, "f'"'] & \end{tikzcd}$$

i.e. every bilinear map on $M \times N$ factors through $M \otimes_A N$.

Proof. Let C be the free module on generators $M \times N$. Extend f to an A-linear map $\overline{f}\colon C \to P$ by

$$\overline{f}\left(\sum_i a_i(x_i, y_i)\right) = \sum_i a_i f(x_i, y_i)$$

Recall the submodule D generated by

- $(x + x', y) - (x, y) - (x', y)$
- $(x, y + y') - (x, y) - (x, y')$
- $(ax, y) - a(x, y)$
- $(x, ay) - a(x, y)$

for $x, x' \in M$, $y, y' \in N$, and $a \in A$. Since f is bilinear, we have $D \subseteq \ker(\overline{f})$. So by the universal property of quotients we get a uniquely determined A-linear map $f'\colon C/D = M \otimes_A N \to D$ such that the following diagram commutes:

$$\begin{tikzcd} C \arrow[r, "\overline{f}"] \arrow[d, "\pi"] & P \\ C/D \arrow[ur, dashed, "f'"'] & \end{tikzcd}$$

So, restricting to $M \times N$, we find the following diagram commutes:

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "\otimes"] & P \\ M \otimes_A \arrow[ur, "f'"] & \end{tikzcd}$$

as desired. For uniqueness, suppose f'' were another such map. Then for any $m \in M$ and $n \in N$ we have $f'(m \otimes n) = f(m, n) = f''(m \otimes n)$; so f' and f'' agree on all tensors. But the tensors generate $M \otimes N$; so $f' = f''$. $\square$ Theorem 2.2.9

Remark 2.2.10. $M \otimes_A N$ is the unique A-module with this universal property.

Lemma 2.2.11. *Suppose $f \colon M \to N$ is A-linear and P is an A-module. Then there is a unique A-linear map $f \otimes 1 \colon M \otimes P \to N \otimes P$ such that $(f \otimes 1)(x \otimes y) = f(x) \otimes y$.*

Proof. Consider $g \colon M \times P \to N \otimes P$ given by $(x, y) \mapsto f(x) \otimes y$. Then this is bilinear since f is A-linear and $\otimes$ is bilinear. So the universal property gives us a uniquely determined A-linear map $g' \colon M \otimes P \to N \otimes P$ such that $x \otimes y \mapsto g(x, y) = f(x) \otimes y$. So we can set $f \otimes 1$ to be this g'. $\square$ Lemma 2.2.11

Remark 2.2.12. We then have that $- \otimes_A P$ is a covariant functor.

Proposition 2.2.13 (2.14 (iv))**.** *Suppose M is an A-module. Then $A \otimes_A M \cong M$.*

Proof. Consider $f \colon A \times M \to M$ given by $(a, m) \mapsto am$. The A-module axioms tell us that f is A-bilinear. So the universal property of tensor products gives us $f' \colon A \otimes_A M \to M$ such that the following diagram commutes:

$$\begin{tikzcd} A \times M \arrow[r, "f"] \arrow[d, "\otimes"] & M \\ A \otimes_A M \arrow[ur, dashed, "f'"'] & \end{tikzcd}$$

so $f'(a \otimes m) = am$. Let $g \colon M \to A \otimes_A M$ be $m \mapsto 1_A \otimes m$; then g is A-linear, and

$$\begin{aligned} (f' \circ g)(m) &= f'(1 \otimes m) \\ &= m \\ (g \circ f')(a \otimes m) &= g(am) \\ &= 1 \otimes (am) \\ &= a(1 \otimes m) \\ &= a \otimes m \end{aligned}$$

for all $a \in A$, $m \in M$. In particular, $f' \circ g = \mathrm{id}_M$, and $g \circ f'$ agrees with $\mathrm{id}_{A \otimes M}$ on tensors, and thus $g \circ f' = \mathrm{id}_{A \otimes M}$. So f' is an isomorphism $A \otimes_A M \to M$. $\square$ Proposition 2.2.13

One similarly verifies the following:

Proposition 2.2.14 (2.14)**.**

1. *$(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P)$ with isomorphism given on tensors by $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$.*
2. *$M \otimes_A N \cong N \otimes_A M$ with isomorphism given on tensors by $x \otimes y \mapsto y \otimes x$.*
3. *$(M \oplus N) \otimes_A P \cong (M \otimes_A P) \oplus (N \otimes_A P)$ with isomorphism given on tensors by $(m, n) \otimes p \mapsto (m \otimes p, n \otimes p)$.*

Hom and tensor products are related: they are *adjoints*.

Proposition 2.2.15. *Suppose M, N, P are A-modules. There is a canonical isomorphism of A-modules*

$$\hom(M \otimes N, P) \cong \hom(M, \hom(N, P))$$

Remark 2.2.16. Fix an A-module N. Let T be the functor $M \mapsto M \otimes N$; let U be the functor $M \mapsto \hom(N, M)$. Then the proposition says that $\hom(T(M), P) \cong \hom(M, U(P))$.

Proof of Proposition 2.2.15. Given $M \otimes N \xrightarrow{f} P$ we define $M \xrightarrow{\hat{f}} \hom(N, P)$ given by $m \mapsto (n \mapsto f(m \otimes n))$. Conversely, given $M \xrightarrow{g} \hom(N, P)$, we define $M \otimes N \xrightarrow{\underline{g}} P$ by $(m \otimes n) \mapsto g(m)(n)$. One checks that $\hat{\cdot}$ and $\underline{\cdot}$ are A-linear and mutually inverse. □ Proposition 2.2.15

Intuitively, these are both isomorphic to the set of A-bilinear maps $M \times N \to P$.

We can use this to get exactness properties of $\otimes$:

Proposition 2.2.17 (2.18)**.** *Suppose $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact. Then for any A-module N we have*

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0$$

Proof. Suppose P be an A-module. Then

$$0 \to \hom(M'', P) \xrightarrow{\overline{g}} \hom(M, P) \xrightarrow{\overline{f}} \hom(M', P)$$

is exact by Proposition 2.1.14; so

$$0 \to \hom(N, \hom(M'', P)) \to \hom(N, \hom(M, P)) \to \hom(N, \hom(M', P))$$

is exact by Proposition 2.1.16. Applying the previous proposition we get that this is isomorphic to

$$0 \to \hom(M'' \otimes N, P) \xrightarrow{\overline{g \otimes 1}} \hom(M \otimes N, P) \xrightarrow{\overline{f \otimes 1}} \hom(M' \otimes N, P)$$

which is then exact. (One checks that the arrows are indeed $\overline{g \otimes 1}$ and $\overline{f \otimes 1}$.) By Theorem 2.2.8, since P was arbitrary, we have that

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0$$

is exact. □ Proposition 2.2.17

Note that $\otimes$ is *not* exact:

Example 2.2.18. Consider $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z}$ given by $x \mapsto 2x$; then $0 \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{f \otimes 1} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ has $1 \otimes 1 \mapsto 2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0$ but $1 \otimes 1 \neq 0$, and $f \otimes 1$ is not injective.

We can also express this by saying that $2\mathbb{Z}$ is a submodule of $\mathbb{Z}$ but $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is *not* a submodule $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$; i.e. $\iota \colon 2\mathbb{Z} \to \mathbb{Z}$ has $\iota \otimes 1 \colon 2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is not injective.

The above can be expressed as saying that $\mathbb{Z}/2\mathbb{Z}$ is not a *flat* $\mathbb{Z}$-module.

Definition 2.2.19. An A-module N is *flat* if whenever $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact then $M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N$ is exact.

Proposition 2.2.20 (2.19)**.** *Suppose N is an A-module. Then the following are equivalent:*

1. *N is flat.*
2. *Whenever*
$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$
is exact we have
$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$
is exact.
3. *Whenever $f \colon M' \to M$ is injective we have $f \otimes 1 \colon M' \otimes N \to M \otimes N$ is injective.*
4. *Whenever M and M' are finitely generated and $f \colon M' \to M$ is injective we have $f \otimes 1 \colon M' \otimes N \to M \otimes N$ is injective.*

Proof.

(1) $\implies$ (2) Easy.

(2) $\implies$ (1) Suppose

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact. We want exactness of

$$M' \otimes N \xrightarrow{f\otimes 1} M \otimes N \xrightarrow{g\otimes 1} M'' \otimes N$$

We get two short exact sequences:

$$0 \to \mathrm{im}(f) \xrightarrow{\iota} M \xrightarrow{\widehat{g}} \mathrm{im}(g) \to 0$$

and

$$0 \to \mathrm{im}(g) \xrightarrow{\iota''} M'' \to \mathrm{coker}(g) \to 0$$

By hypothesis, we then have

$$0 \to \mathrm{im}(f) \otimes N \xrightarrow{\iota\otimes 1} M \otimes N \xrightarrow{\widehat{g}\otimes 1} \mathrm{im}(g) \otimes N \to 0$$

and

$$0 \to \mathrm{im}(g) \otimes N \xrightarrow{\iota''\otimes 1} M'' \otimes N \xrightarrow{\pi\otimes 1} \mathrm{coker}(g) \otimes N \to 0 \tag{2}$$

are exact. But then

$$\mathrm{im}(f\otimes 1) = (f(x') \otimes y : x' \in M', y \in N) = \mathrm{im}(\iota \otimes 1) = \ker(\widehat{g} \otimes 1)$$

Claim 2.2.21. $\ker(\widehat{g} \otimes 1) = \ker(g \otimes 1)$.

Proof. By definition of $\widehat{g}$ we have the following diagram commutes:

$$\begin{tikzcd} M \arrow[r, "g"] \arrow[d, "\widehat{g}"] & M'' \\ \mathrm{im}(g) \arrow[ur, "\iota''"] & \end{tikzcd}$$

Since $- \otimes N$ is a functor, we then get the following diagram commutes:

$$\begin{tikzcd} M \otimes N \arrow[r, "g\otimes 1"] \arrow[d, "\widehat{g}\otimes 1"] & M'' \otimes N \\ \mathrm{im}(g) \otimes N \arrow[ur, "\iota''\otimes 1"'] & \end{tikzcd}$$

But by exactness of (2) we have $\iota'' \otimes 1$ is injective. So $\ker(g \otimes 1) = \ker(\widehat{g} \otimes 1)$. $\square$ Claim 2.2.21

So $\mathrm{im}(f \otimes 1) = \ker(g \otimes 1)$, and we have that

$$M' \otimes N \xrightarrow{f\otimes 1} M \otimes N \xrightarrow{g\otimes 1} M'' \otimes N$$

is exact.

(3) $\iff$ (2) Proposition 2.2.17.

(4) $\implies$ (3) Suppose $M' \xrightarrow{f} M$ is injective. Suppose $u \in \ker(f \otimes 1)$; we wish to show $u = 0$. Write

$$u = \sum_{i=1}^{n} x_i \otimes y_i$$

where each $x_i \in M'$ and $y_i \in N$. Then

$$0 = (f \otimes 1)(u) = \sum_{i=1}^{n} f(x_i) \otimes y_i$$

in $M \otimes N = C_{M,N}/D_{M,N}$. So

$$\sum_{i=1}^{n} (f(x_i), y_i) \in D_{M,N}$$

and is thus a finite linear combination (*) of generators of $D_{M,N}$. Let M_0 be the submodule of M generated by $f(x_i)$ for $i \in \{1, \ldots, n\}$ and by the elements of M appearing in (*). Let $M'_0 = (x_1, \ldots, x_n)$ be the submodule of M' generated by $x_1, \ldots, x_n$. Then

$$\sum_{i=1}^{n} (f(x_i), y_i) \in D_{M_0,N} \leq C_{M_0,N}$$

by the same witness as (*). So

$$\sum_{i=1}^{n} f(x_i) \otimes y_i = 0$$

in $M_0 \otimes N = C_{M_0,N}/D_{M_0,N}$. Let $f_0 = f \restriction M'_0 \colon M'_0 \to M_0$; then f_0 is injective. By hypothesis we have $f_0 \otimes 1 \colon M'_0 \otimes N \to M_0 \otimes N$ is injective. Let

$$u_0 = \sum_{i=1}^{n} x_i \otimes y_i \in M'_0 \otimes N$$

But

$$(f_0 \otimes 1)(u_0) = \sum_{i=1}^{n} f(x_i) \otimes y_i = 0$$

in $M_0 \otimes N$. So $v_0 = 0$. So

$$\sum_{i=1}^{n} (x_i, y_i) \in D_{M'_0,N} \leq C_{M'_0,N} \leq C_{M',N}$$

(and in particular $D_{M'_0,N} \leq D_{M',N}$); so

$$\sum_{i=1}^{n} (x_i, y_i) \in D_{M',N}$$

and

$$u = \sum_{i=1}^{n} x_i \otimes y_i = 0$$

in $M' \otimes N$. $\square$ Proposition 2.2.20

Example 2.2.22. Free modules are flat. As an easy example, let $F = A \oplus A$. Suppose $f \colon M' \to M$ is injective. We then have

$$\begin{tikzcd}
M' \otimes (A \oplus A) \arrow[r, "f \otimes 1"] \arrow[d, "\cong"] & M \otimes (A \oplus A) \arrow[d, "\cong"] \\
(M' \otimes_A A) \oplus (M' \otimes_A A) \arrow[d, "\cong"] & (M \otimes_A A) \oplus (M \otimes_A A) \arrow[d, "\cong"] \\
M' \oplus M' \arrow[r, "\alpha"] & M \oplus M
\end{tikzcd}$$

Tracing through to find what α should be, we find that if $(x, y) \in M' \oplus M'$, we get

$$(x, y) \mapsto (x \otimes 1, y \otimes 1) \mapsto x \otimes (1, 0) + y \otimes (0, 1) \mapsto f(x) \otimes (1, 0) + f(y) \otimes (0, 1) \mapsto (f(x) \otimes 1, f(y) \otimes 1) \mapsto (f(x), f(y))$$

So $\alpha(x, y) = (f(x), f(y))$, and α is injective. So $f \otimes 1$ is injective. Since f was arbitrary, the previous proposition yields that $A \oplus A$ is flat.

2.3 Algebras

Definition 2.3.1. An A-*algebra* is a ring B with a ring homomorhpism $f \colon A \to B$.

Remark 2.3.2. f induces an A-module structure on B by $ab = f(a)b$ for $a \in A$, $b \in B$; this is indeed an A-module structure on B since f is a ring homomorphism. The A-module structure on B is compatible with the ring structure on B in the sense that

$$a \cdot (b_1 b_2) = f(a)(b_1 b_2) = (f(a) b_1) b_2 = (a \cdot b_1) b_2$$

Remark 2.3.3. Suppose B is a ring with an A-module structure satisfying $a \cdot (b_1 b_2) = (a \cdot b_1) b_2$. Then B is an A-algebra and the A-module structure is the induced one.

Proof. Define $f \colon A \to B$ by $a \mapsto a \cdot 1_B$. Then f is a homomorphism since

$$\begin{aligned} f(a_1 + a_2) &= (a_1 + a_2) \cdot 1_B \\ &= a_1 \cdot 1_B + a_2 \cdot 1_B \\ &= f(a_1) + f(a_2) \\ f(a_1 a_2) &= (a_1 a_2) \cdot 1_B \\ &= a_1 (a_2 \cdot 1_B) \\ &= (a_1 (1_B (a_2 \cdot 1_B)) \\ &= (a_1 \cdot 1_B)(a_2 \cdot 1_B) \\ &= f(a_1) f(a_2) \end{aligned}$$

☐ Remark 2.3.3

The point is that rings with an A-module structure satisfying $a \cdot (b_1 b_2) = (a \cdot b_1) b_2$ are exactly the rings with a homomorphism $f \colon A \to B$.

Example 2.3.4.

1. Suppose $A = k$ is a field. A k-algebra B is just a ring containing k as a subring. Indeed, every ring homomorphism on a field is injective, so we can identify k with its image $f \colon k \to B$.

2. Every ring is a $\mathbb{Z}$-algebra via the unique ring homomorphism $f \colon \mathbb{Z} \to B$; namely

$$n \mapsto \begin{cases} \underbrace{1_B + \cdots + 1_B}_{n \text{ times}} & n \geq 0 \\ -f(-n) & \text{else} \end{cases}$$

3. Suppose A is a ring. The polynomial ring $A[t_1, \ldots, t_n]$ is an A-algebra with respect to the inclusion $A \to A[t_1, \ldots, t_n]$.

Definition 2.3.5. Suppose $f \colon A \to B$ is an A-algebra. An A-*subalgebra* is a subring $f(A) \subseteq B' \subseteq B$; then the following diagram commutes:

$$\begin{tikzcd} B' \arrow[r, "\subseteq"] & B \\ A \arrow[u, "\hat{f}"] \arrow[ur, "f"'] & \end{tikzcd}$$

Definition 2.3.6. Suppose $f\colon A \to B$ is an A-algebra with $X \subseteq B$. We define the *A-subalgebra generated by X*, denoted $A[X]$, to be the smallest A-algebra containing X; i.e. the intersection of all subalgebras containing X.

Exercise 2.3.7. $A[X] = \{\, P(x_1, \dots, x_n) : P \in A[t_1, \dots, t_n], n \geq 0, x_1, \dots, x_n \in X \,\}$.

Definition 2.3.8. We say B is a *finitely generated A-algebra* if $B = A[X]$ for some finite $X \subseteq B$. We say B is a *finite A-algebra* if B is finitely generated as an A-module; i.e. there are $x_1, \dots, x_n \in B$ such that every element of B is of the form

$$\sum_{i=1}^{n} a_i x_i$$

where each $a_i \in A$.

Exercise 2.3.9. Every finite A-algebra is finitely generated.

Example 2.3.10.

1. Suppose $A = k$ is a field. Then a finite k-algebra is a finite dimensional k-vector space with a compatible ring structure.

   For example, consider $B = k[t]/(t^2)$ as a k-algebra. Suppose $b \in B$; then b takes the form $P(t) + (t^2)$ for some $P(t) = a_n t^n + \dots + a_0 \in k[t]$; then $b = a_1 t + a_0 + (t^2) = a_1(t + (t^2)) + a_0(1 + (t^2))$. So as a k-vector space B is spanned by $t + (t^2)$ and $1 + (t^2)$; so B is a finite k-algebra.

2. $B = k[t]$ is a finitely generated k-algebra generated by t. But $\{\, 1, t, t^2, \dots \,\}$ is a k-linearly independent set in B; so B is not a finite k-algebra.

Definition 2.3.11. Suppose $f_1\colon A \to B_1$ and $f_2\colon A \to B_2$ are A-algebras. An *A-algebra homomorphism* is $f\colon B_1 \to B_2$ is a ring homomorphism that is A-linear; i.e. such that the following diagram commutes:

$$\begin{tikzcd} B_1 \arrow[r, "f"] & B_2 \\ A \arrow[u, "f_1"] \arrow[ur, "f_2"] & \end{tikzcd}$$

Lemma 2.3.12. *Suppose $f\colon A \to B$ is a finitely generated A-algebra. Then $B \cong A[t_1, \dots, t_n]/I$ as A-algebras for some ideal $I \subseteq A[t_1, \dots, t_n]$.*

Proof. Suppose $x_1, \dots, x_n \in B$ generate B as an A-algebra. Define $F\colon A[t_1, \dots, t_n] \to B$ by $a \mapsto a \cdot 1 = f(a)$ for $a \in A$ and $t_i \mapsto x_i$ for $i \in \{\, 1, \dots, n \,\}$. This defines an A-algebra homomorphism, since it extends f. Also $\operatorname{im}(F)$ contains $x_1, \dots, x_n$ and is an A-subalgebra; so f is surjective. So, by the first isomorphism theorem for rings, we get an isomorphism $\overline{F}\colon A[t_1, \dots t_n]/\ker(F) \to B$; one checks that $\overline{F}$ is A-linear. $\square$ Lemma 2.3.12

Definition 2.3.13. Suppose $f\colon A \to B$ is an A-algebra and M is a B-module. We get a natural A-module structure on M via

$$a \cdot m = f(a)m$$

This A-module is called the *restriction of scalars* of M to A.

Proposition 2.3.14. *If B is a finite A-algebra and M is a finitely generated B-module, then the restriction of scalars of M to A is a finitely generated A-module.*

Proof. Say $b_1, \dots, b_n$ generate B as an A-module; say $m_1, \dots, m_\ell$ generate M as a B-module. Then

$$\{\, b_i m_j : i \in \{\, 1, \dots, n \,\}, j \in \{\, 1, \dots, \ell \,\} \,\}$$

generates M as an A-module. $\square$ Proposition 2.3.14

We can also go in the opposite direction:

Definition 2.3.15. Suppose N is an A-module. Then $B \otimes_A N$ has a B-module structure given by

$$b \cdot (b' \otimes n) = (bb') \otimes n$$

i.e.

$$b\left(\sum_{i=1}^{k} b_i \otimes n_i\right) = \sum_{i=1}^{k} (bb_i) \otimes n_i$$

(One checks that this is well-defined and satisfies the module axioms.) This construction is called *extension of scalars*.

Example 2.3.16. Consider $A = k$ a field; suppose B is a k-algebra. Suppose $A \subseteq B$ and

$$M = \bigoplus_{i=1}^{n} k \cdot m_i$$

is a finitely generated k-module (i.e. vector space over k). Then

$$B \otimes_k M = B \otimes_k \left(\bigoplus_{i=1}^{n} km_i\right) \cong B \otimes_k \left(\bigoplus_{i=1}^{n} k\right) \cong \bigoplus_{i=1}^{n} (B \otimes_k k) \cong \bigoplus_{i=1}^{n} B$$

is a free B-module with generators $1 \otimes m_1, \ldots, 1 \otimes m_n$.

In general we have:

Proposition 2.3.17. *Suppose M is generated as an A-module by $m_1, \ldots, m_n$. Then $B \otimes_A M$ is generated as a B-module by $1 \otimes m_1, \ldots, 1 \otimes m_n$.*

2.4 Tensor products of A-algebras

Suppose $f\colon A \to B$ and $g\colon A \to C$ are A-algebras. Consider $D = B \otimes_A C$. We wish to make D into an A-algebra.

Proposition 2.4.1. *There is an A-bilinear map $\mu\colon D \times D \to D$ such that*

$$\mu(b \otimes c, b' \otimes c') = (bb') \otimes (cc')$$

Proof. We want A-linear $\eta\colon D \to \hom_A(D, D)$; i.e. we want A-bilinear $\eta_1\colon B \times C \to \hom_A(D, D)$. Fix $b \in B$ and $c \in C$; we then define $\eta_1(b, c)\colon B \otimes C \to D$ to be the A-linear map corresponding to the A-bilinear map

$$\begin{aligned} B \times C &\to D \\ (b', c') &\mapsto (bb') \otimes (cc') \end{aligned}$$

One checks that everything involved is bilinear, and thus that we indeed get A-linear $\eta\colon D \to \hom_A(D, D)$; this then induces bilinear $\mu\colon D \times D \to D$ given by $(x, y) \mapsto \eta(x)(y)$. In particular, we have

$$\mu(b \otimes c, b' \otimes c') = \eta(b \otimes c)(b' \otimes c') = \eta_1(b, c)(b' \otimes c') = (bb') \otimes (cc')$$

□ Proposition 2.4.1

Exercise 2.4.2. Check that μ makes D into a ring; then by bilinearity we have $B \otimes_A C$ is an A-algebra.

Remark 2.4.3. The identity element of $B \otimes_A C$ is $1_B \otimes 1_C$. The ring homomorphism $A \to B \otimes_A C$ defining the algebra structure on $B \otimes_A C$ is given by $a \mapsto f(a) \otimes g(a)$. (Recall that $f\colon A \to B$ and $g\colon A \to C$ were the original algebra structures.) We also get canonical ring homomorphisms

$$\begin{aligned} B &\to B \otimes_A C \\ b &\mapsto b \otimes 1_C \end{aligned}$$

and

$$\begin{aligned} C &\to B \otimes_A C \\ c &\mapsto 1_B \otimes c \end{aligned}$$

Example 2.4.4. With $A = \mathbb{Q}$, we have $\mathbb{Q}[t] \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[t]$ as $\mathbb{R}$-algebras via the map

$$(a_n t^n + \cdots + a_0) \otimes r \mapsto r a_n t^n + \cdots + r a_0$$

Example 2.4.5. Again with $A = \mathbb{Q}$ we have $\mathbb{Q}[t_1] \otimes_{\mathbb{Q}} \mathbb{Q}[t_2] \cong \mathbb{Q}[t_1, t_2]$ is generated by $t_1^n \otimes t_2^m$ for $m, n \in \mathbb{N}$.

3 Interlude: Finitely generated modules over PIDs

We follow chapter 12 of Dummit and Foote.

Definition 3.0.1. Suppose M is an A-module and $X \subseteq M$. We say X is *linearly independent* if whenever

$$a_1 x_1 + \cdots + a_\ell x_\ell = 0$$

then

$$a_1 = \cdots = a_\ell = 0$$

(for $a_i \in A$, $x_i \in X$). A *basis* for M is a linearly independent generating set.

Lemma 3.0.2 (1)**.** *Suppose M is an A-module. Then M has a basis if and only if M is free.*

Proof.

($\implies$) Suppose $X \subseteq M$ is a basis. Consider the map

$$\bigoplus_{x \in X} Ax \to M$$

given by

$$(a_x x : x \in X) \mapsto \sum_{x \in X} a_x x$$

This is surjective since X generates M; it is injective since if

$$\sum_{x \in X} a_x x = 0$$

then $(a_x x : x \in X) = 0$. Composing with the canonical isomorphisms $Ax \to A$, we see

$$M \cong \bigoplus_{x \in X} A$$

and M is free.

($\impliedby$) Suppose

$$M \cong \bigoplus_{x \in I} A$$

Let $e_i = (0, \ldots, 0, 1, 0, \ldots)$ be the standard basis vectors of

$$\bigoplus_{x \in I} A$$

Then the images of the e_i form a basis for M. □ Lemma 3.0.2

Remark 3.0.3. When X is a basis for M, we get A-linear maps $\pi_x \colon M \to A$ for all $x \in X$ given by

$$\sum_{y \in X} a_y y \mapsto a_x$$

These satisfy

$$m = \sum_{x \in X} \pi_x(m) x$$

for all $m \in M$.

Even when M is not free, linearly independent sets may exist and be useful.

Definition 3.0.4. Suppose A is an integral domain; suppose M is an A-module. We say M is *of finite rank* if there is a maximal $m \in \mathbb{N}$ such that M has a linearly independent set of size m; in this case, m is called the *rank* of M. Otherwise we say M is *of infinite rank*.

Lemma 3.0.5 (2)**.** *Suppose A is an integral domain. Then the free module*

$$M = \bigoplus_{i=1}^{m} A$$

is of rank m.

Proof. Let F be the fraction field of A. Consider

$$F^m = \underbrace{F \oplus \ldots \oplus F}_{n \text{ times}}$$

as a vector space over F; then $M \subseteq F^m$. Suppose $x_1, \ldots, x_{m+1} \in X$; then $\{ x_1, \ldots, x_{m+1} \}$ is linearly dependent, and we have some $f_1, \ldots, f_{m+1} \in F$ such that

$$f_1 x_1 + \cdots + f_{m+1} x_{m+1} = 0$$

Multiplying by a common denominator, we may assume that each $f_i \in A$, and thus that $\{ x_1, \ldots, x_{m+1} \}$ is linearly dependent in M. So the rank of M is at most m. But we have an obvious linearly independent set of size m; so the rank of M is m. $\square$ Lemma 3.0.5

Remark 3.0.6. Suppose A is an integral domain.

1. By Lemma 3.0.2, we don't expect in the general finite rank case to get a basis.

2. If $N \leq M$ and $\operatorname{rank}(M) = n$ then $\operatorname{rank}(N) \leq n$.

Definition 3.0.7. Suppose A is an integral domain; suppose M is an A-module. A *torsion element of M* is $x \in M$ such that $ax = 0$ for some non-zero $a \in A$. We write

$$\operatorname{Tor}(M) = \{ x \in M : x \text{ is torsion} \}$$

Then $\operatorname{Tor}(M)$ is a submodule of M.

Lemma 3.0.8 (3)**.** *Suppose A is an integral domain. Then*

1. *M is torsion if and only if $\operatorname{rank}(M) = 0$.*

2. *Free modules are torsion-free.*

Proof.

1. Well

$$\begin{aligned} M \text{ is torsion} &\iff \text{for all } x \in M \text{ we have non-zero } a \in A \text{ such that } ax = 0 \\ &\iff \text{for all } x \in M \text{ we have that } \{ a \} \text{ is linearly dependent} \\ &\iff \operatorname{rank}(M) = 0 \end{aligned}$$

2. Say

$$M \cong \bigoplus_{i \in I} A$$

Suppose $x = (a_i : i \in I) \in M$; suppose we have non-zero $a \in A$ such that $ax = 0$. Then $aa_i = 0$ for all $i \in I$, and thus $a_i = 0$ for all $i \in I$; so $x = (a_i : i \in I) = 0$. So M is torsion-free. $\square$ Lemma 3.0.8

Proposition 3.0.9 (4)**.** *Suppose A is a PID and M is a free A-module of rank m. Suppose $0 \neq N \leq M$ is a submodule. Then*

1. *N is free of rank $n \leq m$.*
2. *There exists a basis $y_1, \dots, y_m$ of M and $a_1 \mid a_2 \mid \cdots \mid a_n$ such that $\{ a_1 y_1, \dots, a_n y_n \}$ is a basis for N.*

Proof. Consider $\hom_A(M, A)$. If $\varphi \colon M \to A$, then $\varphi(N) \subseteq A$ is an ideal; so, since A is a PID, we have $\varphi(N) = (a_N)$ for some $a_\varphi \in A$. Define

$$\Sigma = \{ \varphi(N) : \varphi \in \hom_A(M, A) \}$$

Claim 3.0.10. *Σ has a maximal element.*

Proof. We apply Zorn's lemma. We need to check that if $I_1 \subseteq I_2 \subseteq \dots$ is a chain in Σ then

$$\bigcup_i I_i \in \Sigma$$

Since A is a PID, we have

$$\bigcup_i I_i = (a)$$

for some $a \in A$. So $a \in I_{i_0}$ for some i_0; so

$$\bigcup_i I_i = I_{i_0} \in \Sigma$$

□ Claim 3.0.10

Claim 3.0.11. $\Sigma \neq \{ 0 \}$.

Proof. Well, we are guaranteed some basis $\{ x_1, \dots, x_m \}$ for M; we then get projections $\pi_i \colon M \to A$ such that

$$x = \sum_{i=1}^{m} \pi_i(x) x_i$$

for all $x \in M$. But $N \neq 0$; so there is $x \in N$ such that $x \neq 0$. Then

$$0 \neq x = \sum_{i=1}^{m} \pi_i(x) x_i$$

So, since $\{ x_1, \dots, x_n \}$ are a basis, we have some $i_0 \in \{ 1, \dots, m \}$ such that $\pi_{i_0}(x) \neq 0$. Then $0 \neq \pi_{i_0}(N) \in \Sigma$.

□ Claim 3.0.11

Let $\nu(N) \in \Sigma$ be maximal, where $\nu \in \hom_A(M, A)$. Let $\nu(N) = (a_1)$; pick $y \in N$ such that $\nu(y) = a_1$. Note that $a_1 \neq 0$ by the claim.

Claim 3.0.12. *$a_1 \mid \varphi(y)$ for all $\varphi \in \hom_A(M, A)$.*

Proof. Since A is a PID, we have $(a_1, \varphi(y)) = (d)$ for some $d \in A$; say $d = r_1 a_1 + r_2 \varphi(y)$ where $r_1, r_2 \in A$. Consider

$$\psi = r_1 \nu + r_2 \varphi \in \hom_A(M, A)$$

Then $\psi(N) \ni \psi(y) = r_1 \nu(y) + r_2 \varphi(y) = r_1 a_1 + r_2 \varphi(y) = d$. So $(a_1) \subseteq (d) \subseteq \psi(N) \in \Sigma$; so, by maximality of $\nu(N) = (a_1)$, we have $(d) = (a_1)$. So $\varphi(y) \in (a_1)$; so $a_1 \mid \varphi(y)$. □ Claim 3.0.12

Claim 3.0.13. *There exists $y_1 \in M$ such that*

1. *$\nu(y_1) = 1$*
2. *$A y_1 \cap \ker(\nu) = 0$ and $A y_1 + \ker(\nu) = M$. (One checks that this implies $M = A y_1 \oplus \ker(\nu)$.)*
3. *$A(a_1 y_1) \oplus (\ker(\nu) \cap N) = N$.*

Proof. Fix a basis $x_1, \dots, x_m$ for M; consider the projection $\pi_i \colon M \to A$. Then for the $y \in N$ that we previously defined (with $\nu(y) = a_1$) we have

$$y = \sum_{i=1}^{m} \pi_i(y) x_i$$

But by the previous claim we have $a_1 \mid \pi_i(y)$, so $\pi_i(y) = a_1 b_i$ for some $b_1, \dots, b_m \in A$. So

$$y = \sum_{i=1}^{m} a_1 b_i x_i = a_1 \sum_{i=1}^{m} b_i x_i = a_1 y_1$$

where

$$y_1 = \sum_{i=1}^{n} b_i x_i$$

We now check the desired properties.

1. Well, $\nu(a_1 y_1) = \nu(y)$; so $a_1 \nu(y_1) = a_1$ in A, and $\nu(y_1) = 1$.

2. Suppose $x \in M$. Then

   $$\nu(x - \nu(x) y_1) = \nu(x) - \nu(x)\nu(y_1) = \nu(x) - \nu(x) = 0$$

   since we previously showed that $\nu(y_1) = 1$. So $x = \nu(x) y_1 + (x - \nu(x) y_1) \in Ay_1 + \ker(\nu)$, and $M = Ay_1 + \ker(\nu)$.

   On the other hand, let $x \in Ay_1 \cap \ker(\nu)$. Then $x = a y_1$ for some $a \in A$. But then

   $$0 = \nu(x) = \nu(a y_1) = a \nu(y_1) = a$$

   So $x = 0$. So $Ay_1 \cap \ker(\nu) = 0$.

3. Note $a_1 y_1 = y \in N$; so $A(a_1 y_1) + (\ker(\nu \cap N) \subseteq N$. As before, given $x \in N$ we have

   $$x = \nu(x) y_1 + (x - \nu(x) y_1)$$

   where $x - \nu(x) y_1 \in \ker(v)$ as before. But $x \in N$, so $\nu(x) \in \nu(N)$; so $\nu(x) = b a_1$ for some $b \in A$. So

   $$x = b a_1 y_1 + (x - b a_1 y_1)$$

   where we still have that $x - b a_1 y_1 \in \ker(\nu)$; furthermore, $x - b a_1 y_1 \in N$ since $x \in N$ and $a_1 y_1 \in N$. So

   $$N = A(a_1 y_1) + (\ker(v) \cap N)$$

   Also $A(a_1 y_1) \cap (\ker(\nu) \cap N) \subseteq Ay_1 \cap \ker(\nu) = \emptyset$. □ Claim 3.0.13

We now prove the statements of the theorem.

1. Apply induction on $n = \operatorname{rank}(N) \leq \operatorname{rank}(M) = m$ (where the inequalities and equalities follow from previous lemmata).

   If $n = 0$, then by a previous lemma we have that N is torsion. But M is free and is thus torsion-free. So $N = 0$.

   Suppose $n > 0$.

   Exercise 3.0.14. If M', M'' are finite rank, then $\operatorname{rank}(M' \oplus M'') = \operatorname{rank}(M') + \operatorname{rank}(M'')$.

   By part (3) of the previous claim, we then get $\operatorname{rank}(\ker(\nu) \cap N) = n - 1$. So $\ker(\nu) \cap N$ is a submodule of the free module M of rank $n - 1$; so $\ker(\nu) \cap N$ is free of rank $n - 1$ by the induction hypothesis. So N is free of rank n.

2. Apply induction on m the rank of M. By part (1), we have $\ker(\nu)$ is free; by part (2) of the claim, we have $\operatorname{rank}(\ker(\nu)) = n-1$. By the induction hypothesis, we then get $y_2, \ldots, y_m$ a basis for $\ker(\nu)$ and $a_2 \mid a_3 \mid \cdots \mid a_n$ in A such that $\{ a_2 y_2, \ldots, a_n y_n \}$ is a basis for $\ker(\nu) \cap N$.

   Then by the claim we have $y_1, \ldots, y_m$ is a basis for M and $a_1 y_1, \ldots, a_n y_n$ is a basis for N; it remains to check that $a_1 \mid a_2$.

   Consider $\varphi \colon M \to A$ given by

$$
\begin{aligned}
y_1 &\mapsto 1 \\
y_2 &\mapsto 1 \\
y_i &\mapsto 0 \text{ for } i \notin \{ 1, 2 \}
\end{aligned}
$$

   Then $\varphi(a_1 y_1) = a_1 \varphi(y_1) = a_1$; thus $(a_1) \leq \varphi(N) \in \Sigma$ since $a_1 y_1 \in N$, and by maximality of (a_1) we have $(a_1) = \varphi(N)$. Also $\varphi(a_2 y_2) = a_2 \varphi(y_2) = a_2$; so $a_2 \in \varphi(N) = (a_1)$, and $a_1 \mid a_2$. ☐ Proposition 3.0.9

Theorem 3.0.15 (5: Fundamental theorem for finitely generated modules over PIDs, existence)**.** *Suppose A is a PID and M is a finitely generated A-module. Then $M \cong A^r \oplus A/(a_1) \oplus \ldots \oplus A/(a_m)$ for some $r \geq 0$ and $a_1 \mid a_2 \mid \cdots \mid a_m$ are non-zero non-units unit A.*

Remark 3.0.16.

1. All the factors on the RHS are cyclic A-modules, so in particular this says that every finitely generated A-module is a direct sum of cyclic submodules. (Note that any cyclic A-module is of the form A/I where if $N = (x)$ then $I = \operatorname{Ann}(x)$; in a PID, we have $I = (a)$.)

2. Each factor of the form A is free; each factor of the form $A/(a_i)$ is non-trivial torsion. This then splits M into a free part and a torsion part.

Corollary 3.0.17. *Suppose A is a PID and M is a finitely generated A-module.*

1. *In Theorem 3.0.15, we have*
$$\operatorname{Tor}(M) \cong A/(a_1) \oplus \ldots \oplus A/(a_m)$$

2. *M is free if and only if M is torsion-free.*

3. *In Theorem 3.0.15, we have $r = \operatorname{rank}(M)$. (In particular, the r in Theorem 3.0.15 is unique.)*

Proof.

1. We saw
$$A/(a_1) \oplus \ldots \oplus A/(a_m) \subseteq \operatorname{Tor}(M)$$
   Conversely if
$$\alpha = (x_1, \ldots, x_r, y_1, \ldots, y_m) \in A^r \oplus A/(a_1) \oplus \ldots A/(a_m)$$
   is torsion then there is $0 \neq b \in A$ such that
$$b\alpha = (bx_1, \ldots, bx_r, y_1, \ldots, y_m) = 0$$
   So $bx_i = 0$ for $i \in \{ 1, \ldots, m \}$; so $x_i = 0$ for $i \in \{ 1, \ldots, m \}$. So
$$\alpha = 9), 0, \ldots, 0, y_1, \ldots, y_m) \in A/(a_1) \oplus \ldots \oplus A/(a_m)$$

2. Follows from A.

3. By a previously given exercise we have
$$\operatorname{rank}(M) = \operatorname{rank}(A^r) + \operatorname{rank}(\operatorname{Tor}(M))$$
   which is then $r + 0 = r$ by Lemma 3.0.5 and Lemma 3.0.8. ☐ Corollary 3.0.17

Proof of Theorem 3.0.15. Note that we get the a_i non-zero and non-unit from the main statement since if $a_i = 0$ then $A/(a_i) = A$ can be absorbed into A^r, and if a_i is a unit then $A/(a_i) = 0$ can be thrown out.

Now, let $x_1, \ldots, x_n$ generate M as an A-module. Consider $\pi \colon A^n \to M$ given by $e_i \mapsto x_i$ (where $\{ e_1, \ldots, e_n \}$ is the standard basis for A). Then π is a surjective A-linear map. Thus we get an isomorphism

$$\overline{\pi} \colon A^n / \ker(\pi) \to M$$

Apply Proposition 3.0.9 to $\ker(\pi)$ to get a basis $y_1, \ldots, y_n$ for A^n and $a_1 \mid a_2 \mid \cdots \mid a_m$ in A such that $\{ a_1 y_1, \ldots, a_m y_m \}$ is a basis for $\ker(\pi)$, for some $m \leq n$. Then

$$M \cong (Ay_1 \oplus \ldots \oplus Ay_n)/(A(a_1 y_1) \oplus \ldots \oplus A(a_m y_m))$$

Consider

$$\begin{aligned} f \colon \quad Ay_1 \oplus \ldots Ay_n &\to A/(a_1) \oplus \ldots \oplus A/(a_m) \oplus A^{n-m} \\ (\alpha_1 y_1, \ldots, \alpha_n y_n) &\mapsto (\alpha_1 \bmod (a_1), \ldots, \alpha_m \bmod (a_m), \alpha_{m+1}, \ldots, \alpha_n) \end{aligned}$$

for $\alpha_i \in A$. Then f is an A-linear map and is surjective since f is the direct sum of quotient maps. Also

$$\ker(f) = A(a_1 y_1) \oplus \ldots \oplus A(a_m y_m)$$

So

$$M \cong A/(a_1) \oplus \ldots \oplus A/(a_m) \oplus A^{n-m}$$

□ Theorem 3.0.15

We can do better: we can decompose $A/(a_i)$ further. We will need:

Lemma 3.0.18 (7: Chinese remainder theorem)**.** *Suppose A is a ring and I and J are ideals of A such that $I + J = A$ (we say I and J are* comaximal*). Then*

$$A/(I \cap J) \cong A/I \oplus A/J$$

as rings (and in particular as A-modules).

Proof. Pick $x \in I$ and $y \in J$ such that $x + y = 1$. Consider

$$\begin{aligned} A &\to A/I \oplus A/J \\ a &\mapsto (a + I, a + J) \end{aligned}$$

We need to show that f is surjective: given $a, b \in A$ we need to find $c \in A$ such that

$$\begin{aligned} c + I &= a + I \\ c + J &= b + J \end{aligned}$$

i.e.

$$\begin{aligned} c &\equiv a \pmod{I} \\ c &\equiv b \pmod{J} c + J = b + J \end{aligned}$$

Let $c = bx + ay$. Then

$$\begin{aligned} c + I &= (bx + I) + (ay + I) \\ &= (b + I)(x + I) + (a + I)(y + I) \\ &= (a + I)(y + I) \\ &= (a + I)(1 - x + I) \\ &= (a + I)(1 + I) \\ &= a + I \end{aligned}$$

and similarly we get $c + J = b + J$. □ Lemma 3.0.18

By induction one can prove more generally that if $I_1, \ldots, I_\ell$ are ideals of a ring A with $I_i + I_j = A$ for all $i \neq j$ then

$$A/(I_1 \cap \cdots \cap I_\ell) \cong A/I_1 \oplus \ldots \oplus A/I_\ell$$

as rings.

Suppose now that A is a PID and $a \in A$ is a non-zero non-unit. Then A is a UFD, so we can write $a = up_1^{\alpha_1} \ldots p_s^{\alpha_s}$ where $u \in A^\times$, $p_1, \ldots, p_s$ are distinct primes in A, and $\alpha_1, \ldots, \alpha_s$ are positive integers. Then $(a) = (p_1^{\alpha_1}) \cap \cdots \cap (p_s^{\alpha_s})$ by prime factorization. If $i \neq j$ then $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = (d)$ for some $d \in A$; but then d is a common divisor of $p_i^{\alpha_i}$ and $p_j^{\alpha_j}$, so d is a unit in A and $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = A$. So the Chinese remainder theorem yields

$$A/(a) \cong A/(p_1^{\alpha_1}) \oplus \ldots \oplus A/(p_s^{a_s})$$

So Theorem 3.0.15 implies:

Theorem 3.0.19 (8, FTFGMPID, existence, elementary divisors form)**.** *Suppose A is a PID and M is a finitely generated A-module. Then*

$$M \cong A^r \oplus A/(p_1^{\alpha_1}) \oplus \ldots A/(p_t^{\alpha_t})$$

where $p_1, \ldots, p_t$ are (not necessarily distinct) primes in A and $\alpha_1, \ldots, \alpha_t$ are positive integers.

Exercise 3.0.20. Derive Theorem 3.0.15 from Theorem 3.0.19. The problem is to recover the $a_1 \mid \cdots \mid a_m$ condition; the solution is to use the Chinese remainder theorem to put the p_i back together properly.

Definition 3.0.21. We call $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ the *elementary divisors* of M; we call $a_1, \ldots, a_m$ that appeared in Theorem 3.0.15 the *invariant factors* of M. (Note that this implicitly assumes uniqueness, which we have yet to prove.)

Theorem 3.0.22 (9)**.** *These forms are unique; i.e.*

1. *If we also have*
$$M \cong A^{r'} \oplus A/(a_1') \oplus \ldots \oplus A/(a_{m'})$$
with $a_1' \mid \cdots \mid a_{m'}'$ non-zero and non-units then $r = r'$, $m = m'$, and $(a_i) = (a_i')$ for all $i \in \{1, \ldots, m\}$ (i.e. a_i is the product of a unit and a_i'; we then write $a_i \sim a_i'$ and say they are associates*).*

2. *If we also have*
$$M \cong A^{r'} \oplus A/((p_1')^{\alpha_1'}) \oplus \ldots \oplus A/((p_{t'}')^{\alpha_{t'}'})$$
with $p_1', \ldots, p_t'$ primes and $\alpha_1', \ldots, \alpha_{t'}'$ positive integers, then $r = r'$, $t = t'$, and after reordering we have $\alpha_i = \alpha_i'$ and $p_i \sim p_i'$ (and in particular that $(p_i^{\alpha_i}) = ((p_i')^{\alpha_i'})$).

We will need

Lemma 3.0.23 (10)**.** *Suppose A is a principal ideal domain, p is prime in A, and $F = A/(p)$ (so F is a field as (p) is prime and thus maximal). Suppose*

$$M = A/(a_1) \oplus \ldots \oplus A/(a_k)$$

with each a_i divisible by p. Then $M/pM \cong F^k$ as vector spaces over F.

(One should check that in general for $I \subseteq A$ an ideal we have that M/IM is naturally an A/I-module via $(a + I)(x + IM) = ax + IM$.)

Proof. Fix $i \in \{1, \ldots, k\}$. Consider the quotient map $\pi_i \colon A/(a_i) \to (A/(a_i))/p(A/(a_i))$. But

$$p(A/(a_i)) = \{ pa + (a_i) : a \in A \} = (p)/(a_i)$$

since $p \mid a_i$, and thus $(a_i) \subseteq (p)$. Thus

$$(A/(a_i))/p(A/(a_i)) = (A/(a_i))/((p)/(a_i)) \cong A/(p) = F$$

by the second isomorphism theorem. Consider then

$$\begin{aligned}\pi\colon M = A/(a_1) \oplus \dots A/(a_n) &\to F^k\\ (\alpha_1, \dots, \alpha_k) &\mapsto (\pi_1(\alpha_1, \dots, \pi_k(\alpha_k))\end{aligned}$$

Then π is a surjective A-linear map, and

$$\ker(\pi) = \{\, (\alpha_1, \dots, \alpha_k) : \text{each } \alpha_i \in p(A/(a_i)) \,\} = pM$$

Thus $M/pM \cong F^k$ as A-modules; one checks that the isomorphism is F-linear. $\square$ Lemma 3.0.23

Proof of Theorem 3.0.22. We have already seen that $r = \operatorname{rank}(M)$ and hence is uniquely determined in both forms of FTFGMPID. Considering M/A^r, we may assume M is torsion; i.e. that $r = 0$.

2. Fix a prime $p \in A$; consider

$$M[p] = \{\, x \in M : \text{ some power of } p \text{ annihilates x} \,\}$$

Then $M[p]$ is a submodules of M. Then

$$M[p] \cong \bigoplus_{\substack{i \in \{\,1,\dots,t\,\}\\ p_i \sim p}} A/(p_i^{\alpha_i})$$

since if $p_i \not\sim p$ and $a \in A$ has $p^\alpha a \in (p_i^{\alpha_i})$, then $p_i^{\alpha_i} \mid p^\alpha a$; so $p_i^{\alpha_i} \mid a$ by unique factorization, and $a \in (p_i^{\alpha_i})$. Also

$$M[p] \cong \bigoplus_{\substack{i \in \{\,1,\dots,t'\,\}\\ p_i' \sim p}} A/(p_i'^{\alpha_i'})$$

Working with one p at a time, we have reduced to the case when all p_i and p_i' are associates of p. Multiplying by a unit (which doesn't change the ideals), we may assume

$$p_1 = p_2 = \dots = p_t = p_1' = p_2' = \dots = p_{t'}' = p$$

So

$$A/(p^{\alpha_1}) \oplus \dots \oplus A/(p^{\alpha_t}) \cong M \cong A/(p^{\alpha_1'}) \oplus \dots \oplus A/(p^{\alpha_{t'}'})$$

As in Lemma 3.0.23, we have $M/pM \cong F^t$ and $M/pM \cong F^{t'}$ as vector spaces over F; so $t = t'$. We then get

$$A/(p^{\alpha_1}) \oplus \dots \oplus A/(p^{\alpha_t}) \cong M \cong A/(p^{\alpha_1'}) \oplus \dots \oplus A/(p^{\alpha_t'})$$

Re-order that

$$\alpha_1 = \alpha_2 = \dots = \alpha_m = 1 < \alpha_{m+1} \le \alpha_{m+2} \le \dots \le \alpha_t$$

and

$$\alpha_1' = \alpha_2' = \dots = \alpha_{m'}' = 1 < \alpha_{m'+1}' \le \alpha_{m+2}' \le \dots \le \alpha_t'$$

Note that $p^{\alpha_t}M = 0$ implies $\alpha_t' \le \alpha_t$; symmetrically we get $\alpha_t \le \alpha_t'$, and $\alpha_t = \alpha_t'$.

We proceed by inductino on α_t. If $\alpha_t = 0$, then $M = 0$, and there is nothing to do. Suppose then that $\alpha_t > 0$. Then

$$pM \cong pA/(p^{\alpha_{m+1}}) \oplus \dots \oplus pA/(p^{\alpha_t}) \cong A/(p^{a_{mn}-1}) \oplus \dots \oplus A/(p^{\alpha_t - 1})$$

since $A \to pA \to pA/(p^{\alpha_i})$ has kernel $(p^{\alpha_i - 1})$, so by the first isomorphism theorem we have

$$A/(p^{a_i - 1}) \cong pA/(p^{\alpha_i})$$

for $i \in \{\, m+1, \dots, t \,\}$. We similarly get

$$A/(p^{\alpha'_{m'+1}-1}) \oplus \dots \oplus A/(p^{\alpha_t'} - 1)$$

The induction hypothesis then applies to pM to get $t - m = t - m'$, and thus $m = m'$, and that $\alpha_{m+1} = \alpha_{m+1}', \dots, \alpha_t = \alpha_t'$.

1. We obtain the elementary divisors $p_1^{\alpha_1}, \dots, p_t^{\alpha_t}$ from the invariant factors $a_1, \dots, a_m$ by considering the prime factorization. Since $a_1 \mid \cdots \mid a_m$, it must be that a_n is the product of the largest powers of primes appearing in the elementary divisors; likewise a_{m-1} is the product of the largest powers of primes appearing in the elementary divisors after removing those appearing in a_m, and so on. Thus the a_i are determined by the $p_i^{\alpha_i}$; uniqueness of the invariant factors follows. □ Theorem 3.0.22

Example 3.0.24. Consider $A = \mathbb{Z}$; then FTFGMPID is exactly the fundamental theorem of finitely generated abelian grapes. i.e. That any finitely generated abelian grape is isomorphic to something of the form

$$\mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_m\mathbb{Z}$$

where $n_1 \mid \cdots \mid n_m$ are integers > 1. We also get that it is isomorphic to something of the form

$$\mathbb{Z}^r \oplus \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_t^{\alpha_t}\mathbb{Z}$$

where $p_1, \dots, p_t$ are positive prime numbers and $\alpha_1, \dots, \alpha_t$ are positive integers. Furthermore, both of these decompositions are unique.

Example 3.0.25. Consider $A = F[t]$ where F is a field; then A is a PID. Note that an $F[t]$-module is simply an F-vector space equipped with a linear transformation $T\colon V \to V$, where multiplication is

$$f(t)v = a_nT^n(v) + a_{n-1}T^{n-1}(v) + \cdots + a_1T(v) + a_0v = f(T)v$$

Consider the $F[t]$-module $V = F[t]/(a)$ where $a \in F[t]$ is monic and of non-zero degree; say

$$a(t) = t^k + b_{k-1}t^{k-1} + \cdots + b_1t + b_0$$

Let $\bar{t}$ denote the image of t in V. Then $\{1, \bar{t}, (\bar{t})^2, \dots, (\bar{t})^{k-1}\}$ is a basis for V as a vector space over F. The matrix of T with respect to this basis is

$$\mathcal{C}_a = \begin{pmatrix} 0 & 0 & \ldots & 0 & -b_0 \\ 1 & 0 & \ldots & 0 & -b_1 \\ 0 & 1 & \ldots & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -b_{k-1} \end{pmatrix}$$

since

$$T((\bar{t})^{k-1}) = (\bar{t})^k = -b_{k-1}(\bar{t})^{k-1} - \cdots - b_1\bar{t} - b_0$$

We call $\mathcal{C}_a$ the *companion matrix*.

Now, let V be any finite-dimensional F-vector space with $T\colon V \to V$; then V is an $F[t]$-module, and in particular is finitely generated as an $F[t]$-module. So, by FTFGMPID, we get

$$V \cong F[t]^r \oplus F[t]/(a_1) \oplus \ldots \oplus F[t]/(a_m)$$

where $a_1 \mid a_2 \mid \cdots \mid a_m$ are monic polynomials of non-zero degree. (Note that a_m is the minimal polynomial of T.) Since $F[t]$ is not finite-dimensional, we have that $r = 0$. So

$$V \cong F[t]/(a_1) \oplus \ldots \oplus F[t]/(a_m)$$

Choose basis for each cyclic factor as above; then their union B is an basis for V as a vector space over F. The matrix of T with respect to this basis is

$$\begin{pmatrix} \mathcal{C}_{a_1} & & & 0 \\ & \mathcal{C}_{a_2} & & \\ & & \ddots & \\ 0 & & & \mathcal{C}_{a_m} \end{pmatrix}$$

This is called the *rational canonical form* of T; its uniqueness follows from our previous results. So we have proven the rational canonical form theorem.

Now, consider $V = F[t]/(t-\lambda)^k$ for $\lambda \in F$ and $k > 0$. One checks that $\{ (\bar{t}-\lambda)^{k-1}, \ldots, (\bar{t}-\lambda), 1 \}$ is an F-basis for V. What is the matrix of T with respect to this basis? Well

$$T((\bar{t}-\lambda)^{k-1}) = \bar{t}(\bar{t}-\lambda)^{k-1} = (\bar{t}-\lambda)(\bar{t}-\lambda)^{k-1} + \lambda(\bar{t}-\lambda)^{k-1} = \lambda(\bar{t}-\lambda)^{k-1}$$

and

$$T((\bar{t}-\lambda)^{k-2}) = (\bar{t}-\lambda)^{k-1} + \lambda(\bar{t}-\lambda)^{k-2}$$

etc. So the matrix of T is

$$J_{\lambda,k} = \begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 & 0 \\ 0 & \lambda & 1 & \ldots & 0 & 0 \\ 0 & 0 & \lambda & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda & 1 \\ 0 & 0 & 0 & \ldots & 0 & \lambda \end{pmatrix}$$

a *Jordan matrix*.

Suppose now that V is a finite-dimensional vector space over F and $T\colon V \to V$; view this as an $F[t]$-module. So, by the elementary divisor form of FTFGMPID we have

$$V \cong F[t]^r \oplus F[t]/(p_i^{\alpha_i}) \oplus \ldots \oplus F[t]/(p_\ell^{\alpha_\ell})$$

where $p_1, \ldots, p_\ell$ are irreducible monic polynomials of non-zero degree. Again $r = 0$ since V is finite-dimensional.

Suppose now that F is algebraically closed; then each $p_i(t) = t - \lambda_i$ for some $\lambda_i \in F$. So

$$V \cong F[t]/((t-\lambda_1)_1^{\alpha}) \oplus \ldots \oplus F[t]/((t-\lambda_\ell)^{\alpha_\ell})$$

Choose bases for the factors as before; then their union B is a basis for V and the matrix of T with respect to B is

$$\begin{pmatrix} J_{\lambda_1,\alpha_1} & & & 0 \\ & J_{\lambda_2,\alpha_2} & & \\ & & \ddots & \\ 0 & & & J_{\lambda_\ell,\alpha_\ell} \end{pmatrix}$$

This is the *Jordan canonical form* of T; so we have proven the Jordan canonical form theorem.

4 Chapter 3: Rings and modules of fractions, localizations

We return to Atiyah and Macdonald.

We have seen the construction of the field of fractions of an integral domain; we generalize this.

Definition 4.0.1. Suppose A is a ring. A subset $S \subseteq A$ is called *multiplicatively closed* if

- $1 \in S$.
- If $u, v \in S$ then $uv \in S$.

Given a multiplicatively closed $S \subseteq A$, we define a binary relation $\equiv$ on $A \times S$ by $(a, s) \equiv (b, t)$ if $(at - bs)u = 0$ for some $u \in S$. Note that if $0 \notin S$ and A happens to be an integral domain then $(a, s) \equiv (b, t)$ if and only if $at - bs = 0$, and we recover the equivalence relation used to define the field of fractions.

It is clear that $\equiv$ is reflexive and symmetric.

Claim 4.0.2. $\equiv$ *is transitive.*

Proof. Suppose $(a,s) \equiv (b,t)$ and $(b,t) \equiv (c,u)$; then we have $v, w \in S$ such that $(at - bs)v = 0$ and $(vu - ct)w = 0$. So

$$\begin{aligned} atvuw - bsvuw &= 0 \\ buwsv - ctwsv &= 0 \\ \implies atvuw - ctwsv &= 0 \end{aligned}$$

So $(av - cs)tvw = 0$; but $t, v, w \in S$, so $tvw \in S$. So $(a,s) \equiv (c,u)$. □ Claim 4.0.2

Let $S^{-1}A = A[S^{-1}](A \times S)/\equiv$; let $\frac{a}{s}$ denote the equivalence class of (a,s). We view elements of $S^{-1}A$ as "fractions with denominators from S". Note that

$$\frac{a}{s} = \frac{a'}{s'} \iff (as' - a's)u = 0 \text{ for some } u \in S$$

We make $S^{-1}A$ a ring by

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &= \frac{at + bs}{ts} \\ \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st} \end{aligned}$$

Exercise 4.0.3.

1. Check that $+$ and $\cdot$ do not depend on the choice of representation for the fractions, and are thus well-defined.

2. Check that $(S^{-1}A, +, \cdot)$ is a commutative ring with $1 = \frac{1}{1}$ and $0 = \frac{0}{1}$. Moreover,

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

Note that f defined above is not in general injective (or surjective); indeed,

$$a \in \ker(f) \iff \frac{a}{1} = \frac{0}{1} \iff (a \cdot 1 - 0 \cdot 1)v = 0 \text{ for some } v \in S \iff av = 0 \text{ for some } v \in S$$

If A is an integral domain and $0 \notin S$ then f is injective. If A is an integral domain and $S = A \setminus \{0\}$ then $S^{-1}A = \mathrm{Frac}(A)$ and $f \colon A \hookrightarrow \mathrm{Frac}(A)$ is just the usual containment.

We generally assume $0 \notin S$. Indeed, if $0 \in S$ then $S^{-1}A = 0$.

Example 4.0.4.

1. Consider $A = \mathbb{Z}$ with $S = \{1, 2, 4, 8, \dots\}$. Then

$$S^{-1}A = A[S^{-1}] = \mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \frac{a}{2^\ell} : a \in \mathbb{Z}, \ell \geq 0 \right\}$$

   More generally, if A is any commutative ring and $s \in A$ then we define

$$A\left[\frac{1}{s}\right] = S^{-1}A$$

   where $S = \{1, s, s^2, \dots\}$.

2. Let $\operatorname{Spec} A$ be the set of prime ideals of A; i.e. the set of ideals $P \subsetneq A$ such that whenever $ab \in P$ we have $a \in P$ or $b \in P$. For $P \in \operatorname{Spec} A$, let $S = A \setminus P$. Then A_P is defined to be $S^{-1}A$, which we call the *localization* at P.

Consider $A = \mathcal{C}(X \to \mathbb{C})$ where X is a compact Hausdorff space. Fix a point $x_0 \in X$ and let

$$\mathfrak{m}_{x_0} = \{ f \in A : f(x_0) = 0 \}$$

Then $A/\mathfrak{m}_{x_0} \cong \mathbb{C}$; so $\mathfrak{m}_{x_0}$ is maximal, and in particular is prime. We can thus apply the above construction to $\mathfrak{m}_{x_0}$ to get

$$A_{\mathfrak{m}_{x_0}} = \left\{ \frac{f}{g} : f \in A, g(x_0) \neq 0 \right\}$$

3. Let $s \in A$ and consider $B = A[\frac{1}{s}]$ as before. What is $\operatorname{Spec} B$ in terms of $\operatorname{Spec} A$? Well, since B is an A-algebra, we have that ideals I of A generate ideals $I^e = BI$.

   Claim 4.0.5. *These are all the prime ideals of B.*

   Indeed,
   $$\operatorname{Spec}(A) \cong \operatorname{Spec}\left(A\left[\frac{1}{s}\right]\right) \sqcup \operatorname{Spec}(A/(s))$$
   (where the $\cong$ is a homeomorphism in the Zariski topology; to be defined later).

4.1 Universal property of $S^{-1}A$

There is a natural map $\varphi\colon A \to S^{-1}A$ given by $\varphi(a) = \frac{a}{1}$. Note, however, that φ is *not* in general injective. Indeed,

$$\ker(\varphi) = \left\{ a \in A : \frac{a}{1} = \frac{0}{1} \right\} = \{ a \in A : as = 0 \text{ for some } s \in S \}$$

So φ is injective if and only if S contains no zero divisors.

Notice φ is a ring homomorphism satisfying $\varphi(s) \in (S^{-1}A)^\times$ for all $s \in S$.

Proposition 4.1.1. *Suppose $\psi\colon A \to B$ is a ring homomorphism such that $\psi(s) \in B^\times$ for all $s \in S$. Then there is a unique ring homomorphism $\widetilde{\psi}\colon S^{-1}A \to B$ such that the following diagram commutes:*

$$\begin{tikzcd} A \arrow[r, "\psi"] \arrow[d, "\varphi"] & B \\ S^{-1}A \arrow[ur, dashed, "\widetilde{\psi}"'] & \end{tikzcd}$$

Proof. Define $\widetilde{\psi}$ by

$$\widetilde{\psi}\left(\frac{a}{s}\right) = \psi(a)\psi(s)^{-1}$$

Then $\widetilde{\psi}(\varphi(a)) = \widetilde{\psi}(\frac{a}{1}) = \psi(a)$, so the diagram does indeed commute. One then checks that this is the unique ring homomorphism making the diagram commute. □ Proposition 4.1.1

Corollary 4.1.2. *Let B be a ring with a map $\psi\colon A \to B$ satisfying*

1. *$\psi(s) \in B^\times$ for all $s \in S$.*
2. *$\ker(\psi) = \{ a \in A : as = 0$ for some $s \in S \}$. (Note that $\supseteq$ follows from the previous condition.)*
3. *Each $b \in B$ has the form $b = \psi(a)\psi(s)^{-1}$ for some $a \in A$ and some $s \in S$.*

Then there is a unique *isomorphism $\widetilde{\psi}\colon S^{-1}A \to B$ such that the following diagram commutes:*

$$\begin{tikzcd} A \arrow[r, "\psi"] \arrow[d, "\varphi"] & B \\ S^{-1}A \arrow[ur, dashed, "\widetilde{\psi}"'] & \end{tikzcd}$$

4.2 Localization of modules

Definition 4.2.1. Suppose M is an A-module; suppose $S \subseteq A$ is multiplicatively closed. We define

$$S^{-1}M = M \times S / \sim$$

where $(m, s) \sim (m', s')$ if $(s'm - m's)t = 0$ for some $t \in S$. One checks that this is an $(S^{-1}A)$-module via

$$\frac{a}{s}\frac{m}{t} = \frac{am}{st}$$
$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + m's}{ss'}$$

(where $\frac{m}{s}$ is the equivalence class of (m, s)). (One also checks that these are well-defined.)

Remark 4.2.2. If $f\colon M \to N$ is an A-module homomorphism, it induces an $(S^{-1}A)$-module homomorphism $S^{-1}f\colon S^{-1}M \to S^{-1}N$ such that the following diagram commutes:

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

where $S^{-1}f)(\frac{m}{s}) = \frac{f(m)}{s}$.

Claim 4.2.3. *$S^{-1}M \cong M \otimes_A S^{-1}A$.*

Proof. Define $\Phi\colon M \otimes_A S^{-1}A \to S^{-1}M$ by $m \otimes_A \frac{a}{s} \mapsto \frac{am}{s}$. One checks that Φ is an isomorphism of $(S^{-1}A)$-modules. □ Claim 4.2.3

If $P \subseteq A$ is a prime ideal, then we can also define the *localized module at P* to be $M_P = M \otimes_A A_P$.

Claim 4.2.4. *$M = 0$ if and only if $M_P = 0$ for all such P.*

Claim 4.2.5. *$f\colon M \to N$ is injective if and only if $f_P\colon M_P \to N_P$ is injective for all such P.*

Claim 4.2.6. *A module M is projective if and only if M_P is free A_P-module for all such P.*

Example 4.2.7.

1. Suppose $P \subseteq A$ a prime ideal; we define $A_P = S^{-1}A$ where $S = A \setminus P$. (Note that S is multiplicatively closed since P is prime.) We call this the *localization of A at P*.
2. For $f \in A \setminus \{0\}$, we define $A_f = S^{-1}A$ where $S = \{1, f, f^2, \dots\}$. We call this the *localization of A at f*.

Why are these examples related? The motivation is from algebraic geometry.

Given a ring A, we define $\mathrm{Spec}(A)$ to be the set of all prime ideals in A. We put a topology on $\mathrm{Spec}(A)$ called the *Zariski topology* by declaring the closed sets to be sets of the form $V(E)$ for some $E \subseteq A$, where $V(E) = \{P \in \mathrm{Spec}(A) : E \subseteq P\}$. One checks that

$$\begin{aligned} V(0) &= V(\{0\}) \\ &= \mathrm{Spec}(A) \\ V(1) &= V(\{1\}) \\ &= \emptyset \\ \bigcap_{i \in I} V(E_i) &= V\left(\bigcup_{i \in I} E_i\right) \end{aligned}$$

For unions, note that $V(E) = V((E)A)$; one then checks that

$$V(E) \cup V(f) = V((E)A) \cup V((F)A) = V((E) \cdot (F)) = V((E) \cap (F))$$

Exercise 4.2.8. $(E) \cdot (F) = (E) \cap (F)$ if and only if $(E) + (F) = A$.

What are the basic open sets? We get $\operatorname{Spec}(A) \setminus V(f)$ (where $V(f) = V(\{f\})$) since

$$V(E) = \bigcap_{f \in E} V(f)$$

Suppose $P \in \operatorname{Spec}(A)$. We define $P \cdot A_f$ to be the ideal in A_f generated by $\frac{a}{1}$ for $a \in P$. (Recall that the localization map $\alpha \colon A \to A_f$ is not necessarily an embedding.) We can also write $P \cdot A_f = \alpha(P) \cdot A_f$. (Note that this notion applies to arbitrary localizations.) In this particular case, we get

$$P \cdot A_f = \left\{ \frac{a}{f^n} : a \in P, n \geq 0 \right\}$$

since for $b_1, \ldots, b_\ell \in A_f$, $a_1, \ldots, a_\ell \in P$, and $n_1, \ldots, n_\ell \in \mathbb{N}$ we have

$$\frac{b_1 a_1}{f^{n_1}} + \cdots + \frac{b_\ell a_\ell}{f^{n_\ell}} = \frac{a}{f^N}$$

for some $a \in P$ and $N \geq 0$.

Claim 4.2.9. *Suppose $f \notin P$; then PA_f is prime in A_f.*

Proof. Suppose

$$\frac{a}{f^n} \cdot \frac{b}{f^m} = \frac{c}{f^\ell}$$

for some $c \in P$ and $a, b \in A$. Then we have $r \geq 0$ such that

$$f^r (f^\ell ab - f^{n+m} c) = 0$$

so $f^{\ell+r} ab = f^{n+m+r} c \in P$. But $f \notin P$. So $ab \in P$; so $a \in P$ or $b \in P$, and

$$\frac{a}{f^n} \in P \cdot A_f$$

or

$$\frac{b}{f^m} \in P \cdot A_f$$

□ Claim 4.2.9

Claim 4.2.10. *Suppose $Q \in \operatorname{Spec}(A_f)$; then $\alpha^{-1}(Q) \in \operatorname{Spec}(A) \setminus V(f)$.*

Proof. We generally have that the pullback of a prime ideal is a prime ideal; it remains to check that $f \notin \alpha^{-1}(Q)$. But if $f \in \alpha^{-1}(Q)$, we would have $\frac{f}{1} \in Q \subseteq A_f$; but $\frac{f}{1}$ is a unit in A_f, so $Q = A_f$, contradicting our assumption that Q is prime. □ Claim 4.2.10

Claim 4.2.11. *Suppose $f \notin P$; then $P = \alpha^{-1}(P \cdot A_F)$.*

Proof.

($\subseteq$) Generally true.

($\supseteq$) Suppose $a \in A$ has $\alpha(a) = \frac{a}{1} = \frac{b}{f^n} \in PA_f$ for some $b \in P$. Then

$$f^{n+r} a = f^r b \in P$$

So, since $f \notin P$, we have $a \in P$. □ Claim 4.2.11

We then get a bijective correspondence

$$\begin{aligned} \operatorname{Spec}(A_f) &\leftrightarrow \operatorname{Spec}(A) \setminus V(f) \\ P \cdot A_f &\leftarrow P \\ Q &\rightarrow \alpha^{-1}(Q) \end{aligned}$$

(One checks that $\alpha^{-1}(Q) \cdot A_f = Q$.)

Exercise 4.2.12. This correspondence is a homeomorphism.

So the basic open sets in $\mathrm{Spec}(A)$ are of the form $\mathrm{Spec}(A_f)$ for $f \in A \setminus \{0\}$.

Now, fix $P \in \mathrm{Spec}(A)$. If $f \notin P$ then $P \in \mathrm{Spec}(A) \setminus V(f)$, and $\mathrm{Spec}(A) \setminus V(f)$ is a basic open neighbourhood of P in $\mathrm{Spec}(A)$. But

$$\bigcap_{f \notin P} \mathrm{Spec}(A) \setminus V(f) = \bigcap_{f \notin P} \mathrm{Spec}(A_f) = \mathrm{Spec}(A_P)$$

(Note that the above equalities are not literally true; one needs to make some identifications.) We think of $\mathrm{Spec}(A_P)$ as capturing the local behaviour of $P \in \mathrm{Spec}(A)$. (Note that in A_P we have that $P \cdot A_P$ is the unique maximal ideal; so every $Q \in \mathrm{Spec}(A_P)$ is $Q \subseteq P \cdot A_P$.)

In particular, if A is an integral domain, then for any $f \in A \setminus \{0\}$ we have $A \subseteq A_f \subseteq \mathrm{Frac}(A)$. Then we have

$$A_P = \bigcap_{f \notin P} A_f$$

is literally true. This is in fact a *directed union*: given $f, g \notin P$, primality of P gives that $fg \notin P$, so $A_f \subseteq A_{fg}$ and $A_g \subseteq A_{fg}$. (While arbitrary unions of rings are not typically rings, directed unions are.)

In general (i.e. if A is not necessarily an integral domain), there is a natural map $A_f \to A_{fg}$ by $\frac{a}{f^n} \mapsto \frac{ag^n}{(fg)^n}$. (Though these will no longer be embeddings.) We then have that A_P is the directed limit of the A_f.

Example 4.2.13. Think about what the topologies $\mathrm{Spec}(\mathbb{Z})$ and $\mathrm{Spec}(\mathbb{C}[t])$ look like.

The final exam will be Monday April 11$^{\text{th}}$ 12:30–3:00pm.

Recall that given $S \subseteq A$ multiplicatively closed and M an A-module, we define $S^{-1}M = \{ \frac{m}{s} : s \in S \}$ as an $(S^{-1}A)$-module. In fact, given an A-linear map $f \colon M \to N$ we get an $S^{-1}A$-linear map $S^{-1}f \colon S^{-1}M \to S^{-1}N$ given by $\frac{m}{s} \mapsto \frac{f(m)}{s}$.

Proposition 4.2.14 (3.3)**.** *S^{-1} is an exact functor; i.e. if*

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact then so is

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

Proof. Since $\mathrm{im}(f) \subseteq \ker(g)$ we have $g \circ f = 0$; so $0 = S^{-1}(g \circ f) = S^{-1}(g) \circ S^{-1}(f)$. (One needs to check that S preserves composition.) So $\mathrm{im}(S^{-1}(f)) \subseteq \ker(S^{-1}(g))$.

Conversely, suppose $\frac{m}{s} \in \ker(S^{-1}(g))$. Then $S^{-1}(g)(\frac{m}{s}) = 0$; so $\frac{g(m)}{s} = 0$ in $S^{-1}M''$, and there is $t \in S$ such that $g(tm) = tg(m) = 0$ in M''. But then $tm \in \ker(g) \subseteq \mathrm{im}(f)$; so $tm = f(m')$ for some $m' \in M'$. But then

$$\frac{m}{s} = \frac{tm}{ts} = \frac{f(m')}{ts} = S^{-1}(f)\left(\frac{m'}{ts}\right) \in \mathrm{im}(S^{-1}(f))$$

□ Proposition 4.2.14

Corollary 4.2.15 (3.4)**.**

1. *Suppose $N \subseteq M$ is a submodule; let $\iota \colon N \to M$ be the containment map. Then $S^{-1}\iota \colon S^{-1}N \to S^{-1}M$ given by $\frac{n}{s} \mapsto \frac{n}{s}$ is injective. We thus identify $S^{-1}N$ with its image in $S^{-1}M$ and view $S^{-1}N \subseteq S^{-1}M$ as a submodule.*

2. *There is a natural isomorphism $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.*

3. *Suppose $P, N \subseteq M$ are submodules; then $S^{-1}(N + P) = S^{-1}N + S^{-1}P$ (as submodules of $S^{-1}M$).*

4. *$S^{-1}(P \cap N) = (S^{-1}N) \cap (S^{-1}P)$.*

Proof.

1. Well, $0 \to N \to M$ is exact; so by the previous proposition we get $0 \to S^{-1}N \xrightarrow{S^{-1}\iota} S^{-1}M$ is exact, and $S^{-1}\iota$ is injective.

2. Well,
$$0 \to N \to M \to M/N \to 0$$
is exact; so by the previous proposition we get
$$0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$$
is also exact. So $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

3. Note that
$$\frac{n+p}{s} = \frac{n}{s} + \frac{p}{s}$$

4. That $S^{-1}(P \cap N) \subseteq (S^{-1}N) \cap (S^{-1}P)$ is clear. Suppose now that
$$\alpha = \frac{n}{s} = \frac{p}{t} \in (S^{-1}N) \cap (S^{-1}P)$$
Then $utn = usp$ for some $u \in S$; let $x = utn$ for this u. Then $x \in N \cap P$. Then
$$\alpha = \frac{n}{s} = \frac{utn}{uts} = \frac{x}{uts} \in S^{-1}(N \cap P)$$

$\square$ Corollary 4.2.15

We view $S^{-1}A$ as an A-algebra via the canonical map $A \to S^{-1}A$ via $a \mapsto \frac{a}{1}$. Given an A-module M, we have two natural $(S^{-1}A)$-modules: $S^{-1}M$ and $S^{-1}A \otimes_A M$.

Proposition 4.2.16 (3.5)**.** *$S^{-1}A \otimes_A M \cong S^{-1}M$ as $(S^{-1}A)$-modules; in particular, there is an isomorphism $S^{-1}A \otimes_A M \to S^{-1}M$ such that*
$$\frac{a}{s} \otimes m \mapsto \frac{am}{s}$$

Proof. Consider the map $S^{-1}A \times M \to S^{-1}M$ given by $(\frac{a}{s}, m) \mapsto \frac{am}{s}$; this is A-bilinear. So, by the universal property for tensor products, we get an A-linear $f\colon S^{-1}A \otimes_A M \to S^{-1}M$ such that $\frac{a}{s} \otimes m \mapsto \frac{am}{s}$. But $\frac{m}{s} = f(\frac{1}{s} \otimes m)$; so f is surjective.

Claim 4.2.17. *Every element of $S^{-1}A \otimes_A M$ is a tensor.*

Proof. Suppose
$$\sum_i \frac{a_i}{s_i} \otimes m_i \in S^{-1}A \otimes_A M$$
Then
$$\begin{aligned}\sum_i \frac{a_i}{s_i} \otimes m_i &= \sum_i \frac{a_i \prod_{j \neq i} s_j}{\prod_j s_j} \otimes m_i \\ &= \sum_i \frac{1}{\prod_j s_j} \otimes a_i \prod_{j \neq i} s_j m_i \\ &= \frac{1}{\prod_j s_j} \otimes \left(\sum_i a_i \prod_{j \neq i} s_j m_i \right)\end{aligned}$$
Hence every element of $S^{-1}A \otimes_A M$ is indeed a tensor. $\square$ Claim 4.2.17

Claim 4.2.18. *f is injective.*

Proof. By the previous claim, it suffices to check tensors. Suppose

$$\frac{a}{s} \otimes m \in \ker(f)$$

Then

$$0 = f\left(\frac{a}{s} \otimes m\right) = \frac{am}{s}$$

So there is $t \in S$ such that $tam = 0$. But then

$$\frac{a}{s} \otimes m = \frac{ta}{ts} \otimes m = \frac{1}{ts} \otimes tam = \frac{1}{ts} \otimes 0 = 0$$

□ Claim 4.2.18

So f is an A-linear isomorphism. To see that f is $(S^{-1}A)$-linear, note that

$$f\left(\frac{a}{s}\left(\frac{b}{t} \otimes m\right)\right) = f\left(\frac{ab}{st} \otimes m\right) = \frac{abm}{st} = \frac{a}{s}\left(\frac{bm}{t}\right) = \frac{a}{s} f\left(\frac{b}{t} \otimes m\right)$$

So f is an $(S^{-1}A)$-linear isomorphism. □ Proposition 4.2.16

Corollary 4.2.19 (3.6)**.** *$S^{-1}A$ is a flat A-algebra (i.e. is a flat A-module).*

Proof. Suppose $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact. Then by Proposition 4.2.14 we have $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} M''$ is exact. By Proposition 4.2.16 we have that

$$S^{-1}M' \cong S^{-1}A \otimes_A M'$$
$$S^{-1}M \cong S^{-1}A \otimes_A M$$
$$S^{-1}M'' \cong S^{-1}A \otimes_A M''$$

Also, one notes that the following diagram commutes:

$$\begin{tikzcd}
S^{-1}M' \arrow[r, "S^{-1}f"] & S^{-1}M \arrow[d, "\cong"] \\
S^{-1}A \otimes_A M' \arrow[u, "\cong"] \arrow[r, "1\otimes f"] & S^{-1}A \otimes_A M
\end{tikzcd}$$

Since going one way we get

$$\frac{q}{s} \otimes m \mapsto \frac{am}{s} \mapsto \frac{f(am)}{s} = \frac{af(m)}{s} \mapsto \frac{q}{s} \otimes f(m)$$

and going the other way we get

$$\frac{q}{s} \otimes m \mapsto \frac{q}{s} \otimes f(m)$$

Likewise we get

$$\begin{tikzcd}
S^{-1}M \arrow[r, "S^{-1}g"] & S^{-1}M'' \arrow[d, "\cong"] \\
S^{-1}A \otimes_A M \arrow[u, "\cong"] \arrow[r, "1\otimes g"] & S^{-1}A \otimes_A M''
\end{tikzcd}$$

So the following diagram commutes:

$$\begin{tikzcd}
S^{-1}M' \arrow[r, "S^{-1}f"] \arrow[d, dash, "\cong"] & S^{-1}M \arrow[r, "S^{-1}g"] \arrow[d, dash, "\cong"] & S^{-1}M'' \arrow[d, dash, "\cong"] \\
S^{-1}A \otimes_A M' \arrow[r, "1\otimes f"] & S^{-1}A \otimes_A M \arrow[r, "1\otimes g"] & S^{-1}A \otimes_A M''
\end{tikzcd}$$

Then, since the top line is exact, we have that the bottom line is as well (exercise). So $S^{-1}A$ is a flat A-module. □ Corollary 4.2.19

In particular, the following are flat A-algebras:

- A_P where $P \subseteq A$ is a prime ideal.
- A_f where $f \in A \setminus \{0\}$.
- If A is an integral domain, then $\mathrm{Frac}(A)$ is a flat A-algebra.

Proposition 4.2.20 (3.7)**.** *Localization commutes with $\otimes$; i.e. given A-modules M, N and multiplicatively closed $S \subseteq A$, we have an isomorphism (of $(S^{-1}A)$-modules)*

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N)$$
$$\left(\frac{m}{s} \otimes \frac{n}{t}\right) \mapsto \frac{m \otimes n}{st}$$

Proof. Well, by Proposition 4.2.16, we have

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong (S^{-1}A \otimes_A M) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N)$$

We leave it as an exercise to then check that this is in turn isomorphic to

$$M \otimes_A (S^{-1}A \otimes_{S^{-1}A} (S^{-1}A \otimes_A N))$$

and that *this* is in turn isomorphic to

$$M \otimes_A (S^{-1}A \otimes_A N) \cong (M \otimes_A N) \otimes_A S^{-1}A \cong S^{-1}(M \otimes_A N)$$

(where the last isomorphism is again by Proposition 4.2.16).

Finally, we trace what happens to

$$\left(\frac{m}{s} \otimes \frac{n}{t}\right) \in S^{-1}M \otimes_{S^{-1}A} S^{-1}N$$

Well,

$$\begin{aligned}
\left(\frac{m}{s} \otimes \frac{n}{t}\right) &\mapsto \left(\frac{1}{s} \otimes_A m\right) \otimes_{S^{-1}A} \left(\frac{1}{t} \otimes_A n\right) \\
&\mapsto m \otimes_A \left(\frac{1}{s} \otimes_{S^{-1}A} \left(\frac{1}{t} \otimes_A n\right)\right) \\
&\mapsto m \otimes_A \frac{1}{s}\left(\frac{1}{t} \otimes_A n\right) \\
&= m \otimes_A \left(\frac{1}{st} \otimes_A n\right) \\
&\mapsto (m \otimes_A n) \otimes_A \frac{1}{st} \\
&\mapsto \frac{m \otimes_A n}{st}
\end{aligned}$$

☐ Proposition 4.2.20

Proposition 4.2.21 (3.8)**.** *Suppose M is an A-module. Then the following are equivalent:*

1. *$M = 0$.*
2. *$M_P = 0$ for all prime ideals $P \subseteq A$.*
3. *$M_m = 0$ for all maximal ideals $m \subseteq A$.*

Proof. It is clear that (1) $\implies$ (2) $\implies$ (3); it remains to check that (3) $\implies$ (1).

Suppose we have $x \in M \setminus \{0\}$; then $\mathrm{Ann}(x) = \{a \in A : ax = 0\} \subsetneq A$ is a proper ideal. Let $m \supseteq \mathrm{Ann}(x)$ be a maximal ideal. Then if we had $M_m = 0$, we would have $\frac{x}{1} = 0$ in M_m, and $sx = 0$ for some $s \in S = A \setminus m$. But then $s \in \mathrm{Ann}(x) \subseteq m$, a contradiction. So $M_m \neq 0$. ☐ Proposition 4.2.21

Definition 4.2.22. A property of modules R is *local* if M satisfies R exactly when M_P satisfies R for all primes $P \subseteq A$.

So Proposition 4.2.21 states that being zero is a local property.

Another example of a local property:

Proposition 4.2.23 (3.9)**.** *Injectivity and surjectivity of A-linear maps are local properties; i.e. given an A-linear map $\varphi\colon M \to N$, we have that the following are equivalent:*

1. *$\varphi\colon M \to N$ is injective (respectively, surjective).*
2. *$\varphi\colon M_P \to N_P$ is injective (respectively, surjective) for all prime ideals $P \subseteq A$. (Recall that $\varphi_P = S^{-1}\varphi\colon S^{-1}M \to S^{-1}N$ is given by $\frac{m}{s} \to \frac{\varphi(m)}{s}$ where $S = A \setminus P$.)*
3. *$\varphi_m\colon M_m \to N_m$ is injective (respectively, surjective) for all maximal ideals $m \subseteq A$.*

Proof.

(1) $\implies$ (2) Well, $0 \to M \xrightarrow{\varphi} N$ is exact, and by Proposition 4.2.14 we have that localization is exact. So $0 \to M_P \xrightarrow{\varphi_P} N_P$ is exact; so φ_P is injective. (For surjectivity, consider instead $M \xrightarrow{\varphi} N \to 0$.)

(2) $\implies$ (3) Trivial.

(3) $\implies$ (1) Suppose $\ker(\varphi) \neq 0$; then $\ker(\varphi)_m \neq 0$ for some maximal ideal $m \subseteq A$. Then $0 \to \ker(\varphi) \to M \xrightarrow{\varphi} N$ is exact; so, by Proposition 4.2.14, we get that $0 \to \ker(\varphi)_m \to M_m \xrightarrow{\varphi_m} N_m$ is exact. So $0 \neq \ker(\varphi)_m = \ker(\varphi_m)$. (For surjectivity, consider instead the exact sequence $M \xrightarrow{\varphi} N \to \operatorname{coker}(\varphi) \to 0$.) ☐ Proposition 4.2.23

Example 4.2.24. Being an integral domain is *not* a local property, as we see on the assignment.

Proposition 4.2.25 (3.10)**.** *Flatness is a local property; i.e. given an A-module M, we have that the following are equivalent:*

1. *M is a flat A-module.*
2. *M_P is a flat A_P-module for all $P \in \operatorname{Spec}(A)$.*
3. *M_m is a flat A_m-module for all maximal ideals $m \subseteq A$.*

Proof.

(1) $\implies$ (2) By Proposition 4.2.16 we have $M_p \cong M \otimes_A A_P$; by assignment 2 question 4(b), we have that if M is a flat A-module then $M \otimes_A B$ is a flat B module for any A-algebra $A \to B$. Applying this to $A \to A_P$ given by $a \mapsto \frac{a}{1}$, we get that M_P is a flat A_P-module.

(2) $\implies$ (3) Trivial.

(3) $\implies$ (1) It suffices to show that if $\varphi\colon N \to P$ is injective then so is $\varphi \otimes_A \mathrm{id}_M$. By Proposition 4.2.23 it suffices to show that for all maximal ideals $m \subseteq A$ we have that the map $(N \otimes_A M)_m \to (P \otimes_A M)_m$ is injective. But by Proposition 4.2.20 we have

$$(N \otimes_A M)_m \cong N_m \otimes_{A_m} M_m$$
$$(P \otimes_A M)_m \cong P_m \otimes_{A_m} M_m$$

It then suffices to check that the map $N_m \otimes_{A_m} M_m \to P_m \otimes_{A_m} M_m$ is injective for all maximal ideals $m \subseteq A$. But this is injective because $N_m \to P_m$ is injective by Proposition 4.2.23 and since M_m is a flat A_m-module by assumption.

So $N \otimes_A M \to P \otimes_A M$.

☐ Proposition 4.2.25

Definition 4.2.26. Suppose we have an A-algebra $A \xrightarrow{f} B$. Given an ideal $I \subseteq A$, we define $I \cdot B$ to be $f(I) \cdot B$, the ideal of B generated by $f(I)$; these are called the *extension ideals of* B. (Note that in general f will not be a containment, or even an embedding.) Given an ideal $J \subseteq B$, we define $J \cap A$ to be $f^{-1}(J)$, which is necessarily an ideal of A; these are called the *contraction ideals of* A.

Example 4.2.27. Consider $A \to S^{-1}A$ given by $a \mapsto \frac{a}{1}$, where $S \subseteq A$ is multiplicatively closed. What are the extension and contraction ideals?

Remark 4.2.28. Given $I \subseteq A$, we have

$$I \cdot S^{-1}A = S^{-1}I = \left\{ \frac{a}{s} : a \in I, s \in S \right\}$$

Proof.

($\supseteq$) Trivial.

($\subseteq$) Suppose

$$r = \frac{a_1}{1}\frac{b_1}{s_1} + \cdots + \frac{a_\ell}{1}\frac{b_\ell}{s_\ell} \in I \cdot S^{-1}A$$

where $a_1, \ldots, a_\ell \in I$, $b_1, \ldots, b_\ell \in A$, and $s_1, \ldots, s_\ell \in S$. Then

$$r = \frac{a_1 b_1 s_2 \ldots s_\ell + a_2 b_2 s_1 s_3 \ldots s_\ell + \cdots + a_\ell b_\ell s_1 s_2 \ldots s_{\ell-1}}{s_1 s_2 \ldots s_\ell} \in S^{-1}I$$

☐ Remark 4.2.28

Remark 4.2.29. Localizations commute with kernels and images; i.e. given $f\colon M \to N$ we have $\ker(f)_P = \ker(f_P)$ and $\operatorname{im}(f)_P = \operatorname{im}(f_P)$.

Proof. Well, $0 \to \ker(f) \to M \xrightarrow{f} N$ is exact. So $0 \to \ker(f)_P \to M_P \xrightarrow{f_P} N_P$ is exact, and $\ker(f)_P = \ker(f_P)$. Likewise, we have $M \xrightarrow{f} \operatorname{im}(f) \to 0$ is exact; so $M_P \xrightarrow{f_P} \operatorname{im}(f)_P \to 0$ is exact, and $\operatorname{im}(f_P) = \operatorname{im}(f)_P$.

☐ Remark 4.2.29

Is exactness local? Well, localization is exact, so localization preserves exactness. What of the converse? Does it hold that if $M'_P \xrightarrow{f_P} M_P \xrightarrow{g_P} M''_P$ is exact for all $P \in \operatorname{Spec}(A)$ then $M' \xrightarrow{f} M \xrightarrow{g} M''$?

Well, Proposition 4.2.23 says it holds for sequences $0 \to M \xrightarrow{f} M''$ and $M \xrightarrow{g} M'' \to 0$. In fact, the answer is yes in general.

Proposition 4.2.30. *Exactness is local.*

Proof. Suppose $M'_m \xrightarrow{f_m} M_m \xrightarrow{g_m} M''_m$ is exact for every maximal ideal m of A. Then for all maximal ideals m of A we have

$$\operatorname{im}(g \circ f)_m = \operatorname{im}((g \circ f)_m) = \operatorname{im}(g_m \circ f_m) = 0$$

By Proposition 4.2.21 we get that $\operatorname{im}(g \circ f) = 0$; so $\operatorname{im}(f) \subseteq \ker(g)$.

Now, for each maximal ideal ideal m of A, we have

$$(\ker(g)/\operatorname{im}(f))_m = \ker(g)_m/\operatorname{im}(f)_m = \ker(g_m)/\operatorname{im}(f_m) = 0$$

by Corollary 4.2.15 and exactness of $M'_m \xrightarrow{f_m} M_m \xrightarrow{g_m} M''_m$. So by Proposition 4.2.21 we get that $\operatorname{im}(f) = \ker(g)$.

☐ Proposition 4.2.30

Consider the A-algebra $f\colon A \to S^{-1}A$ given by $a \mapsto \frac{a}{1}$; suppose $S \subseteq A$ is multiplicatively closed. For an ideal I of A, consider $I(S^{-1}A) = f(I)(S^{-1}A) = S^{-1}I$; likewise for an ideal J of $S^{-1}A$, consider $J \cap A = f^{-1}(J)$.

Proposition 4.2.31. *1. Every ideal of $S^{-1}A$ is an extension ideal.*

2. *For every ideal I of A we have*

$$(I(S^{-1}A)) \cap A = \bigcup_{s \in S} \{ x \in A : sx \in I \}$$

As a notational convenience, we let $(I : s) = \{ x \in A : sx \in I \}$; rewriting the above, we get

$$(I(S^{-1}A)) \cap A = \bigcup_{s \in S} (I : s)$$

3. *For every ideal I of A we have that $I(S^{-1}A) = S^{-1}A$ if and only if $I \cap S \neq \emptyset$.*

4. *$I \subseteq A$ is a contraction ideal if and only if the image of S in A/I has no zero divisors.*

5. *There is a bijective correspondence*

$$\begin{aligned} \operatorname{Spec}(S^{-1}A) &\leftrightarrow \{ p \in \operatorname{Spec}(A) : p \cap S = \emptyset \} \\ P(S^{-1}A) &\xleftarrow{F} P \\ Q &\xrightarrow{G} Q \cap A \end{aligned}$$

Proof.

1. Suppose $J \subseteq S^{-1}A$ is an ideal. Then for $\frac{a}{s} \in J$, we have $\frac{a}{1} = s\frac{a}{s} \in J$; so $\frac{a}{1} \in (J \cap A)S^{-1}A$, and $\frac{a}{s} \in (J \cap A)S^{-1}A$. So $J \subseteq (J \cap A)S^{-1}A$. But it is clear that $J \supseteq (J \cap A)S^{-1}A$; so $J = (J \cap A)S^{-1}A$.

2. ($\subseteq$) Suppose $x \in (I(S^{-1}A)) \cap A$. Then $\frac{x}{1} \in I(S^{-1}A) = S^{-1}I$. So $\frac{x}{1} = \frac{a}{s}$ for some $a \in I$ and some $s \in S$. So $tsx = ta$ for some $t \in S$. But $ta \in I$ since $a \in I$; so $x \in (I : st)$.

   ($\supseteq$) Suppose $sx \in I$ for some $s \in S$. Then $\frac{x}{1} = \frac{sx}{s} \in S^{-1}I = I(S^{-1}A)$. So $(I : s) \subseteq I(S^{-1}A) \cap A$.

3. ($\implies$) Suppose $I(S^{-1}A) = S^{-1}A$. Then $I(S^{-1}A) \cap A = A$. So

$$A = \bigcup_{s \in S} (I : s)$$

   Then there is $s_0 \in S$ such that $s_0 1 \in I$; so $I \cap S \neq \emptyset$.

   ($\impliedby$) Suppose we have $s \in I \cap S$. Then $\frac{1}{1} = \frac{s}{1} \cdot \frac{1}{s} \in I(S^{-1}A)$ (since $\frac{s}{1} \in I(S^{-1}A)$). So $IS^{-1}A = S^{-1}A$.

4. Well,

$$\begin{aligned} I \text{ is a contraction ideal } &\iff I = J \cap A \text{ for some ideal } J \subseteq S^{-1}A \\ &\iff I = I(S^{-1}A) \cap A = f^{-1}(S^{-1}I) \end{aligned}$$

   The last reverse implication is clear; to see the forward implication, suppose $I = J \cap A$ for some ideal J of $S^{-1}A$. It is clear that $I \subseteq I(S^{-1}A) \cap A$. To see that $I \supseteq I(S^{-1}A) \cap A$, note that $f^{-1}(J) = I$; then $f(I) \subseteq J$, so $I(S^{-1}A) \subseteq J$, and $I(S^{-1}A) \cap A \subseteq J \cap A = I$.

   Continuing the chain of equivalences, we find

$$\begin{aligned} I \text{ is a contraction ideal } &\iff I = \bigcup_{s \in S} (I : s) \\ &\iff \text{for all } x \in A, s \in S \text{ such that } sx \in I \text{ we have } x \in I \\ &\iff \text{for all } x \in A, s \in S \text{ such that } sx + I = 0 + I \text{ we have } x + I = 0 + I \\ &\iff \text{for all } s \in S \text{ we have that } s \text{ is not a zero divisor in } A/I \end{aligned}$$

5. Suppose $P \in \operatorname{Spec}(A)$ has $P \cap S = \emptyset$. Then
$$S^{-1}A/P(S^{-1}A) = S^{-1}A/S^{-1}P \cong S^{-1}(A/P)$$
as A-modules; this is in turn isomorphic to $(\overline{S})^{-1}(A/P)$ as A-algebras, where $\overline{S}$ is the image of S in A/P. Since P is prime, we have that A/P is an integral domain. So $\overline{S} \subseteq A/P$ is multiplicatively closed and $0 \notin \overline{S}$ since $S \cap P = \emptyset$. So $A/P \subseteq (\overline{S})^{-1}(A/P) \subseteq \operatorname{Frac}(A/P)$; so $(\overline{S})^{-1}(A/P)$ is an integral domain. So $S^{-1}A/P(S^{-1}A)$ is an integral domain. So $P(S^{-1}A)$ is prime.

It remains to check that the maps are mutually inverse. That $F \circ G = \mathrm{id}$ is exactly an earlier point. Suppose now that $P \in \operatorname{Spec}(A)$ has $P \cap S = \emptyset$. Then A/P is an integral domain and $0 \notin \overline{S}$ since $P \cap S = \emptyset$. So, by the previous point, we have P is a contraction ideal. In fact, the second equivalence of the proof of the previous point shows that an ideal is a contraction ideal if and only if it is the contraction of its extension. So $P = (P(S^{-1}A)) \cap P$; So $G \circ F = \mathrm{id}$. □ Proposition 4.2.31

Example 4.2.32. The prime ideals of A_P are in bijective correspondence with prime ideals of A contained in P. The prime ideals of A_f are in bijective correspondence with the prime ideals of A not containing f.

Definition 4.2.33. Suppose A is a ring. We define the *nilradical of* A to be $\mathcal{R} = \{ f \in A : f^n = 0 \text{ for some } n \}$.

Proposition 4.2.34 (1.8)**.** *Suppose A is a ring. Then*
$$\mathcal{R} = \bigcap \{ P : P \text{ is a prime ideal} \}$$

Proof.

($\subseteq$) Clear: $P \in \operatorname{Spec}(A)$ and $f^n = 0$, then $f^n \in P$, and thus $f \in P$.

($\supseteq$) Suppose $f \in A \setminus \mathcal{R}$; we wish to find a prime ideal P with $f \notin P$. Well, $0 \notin S = \{1, f, f^2, \dots\}$; so the localization A_f is non-zero. But then if m is a maximal ideal in A_f, Proposition 4.2.31 gives us that $m \cap A$ is a prime ideal in A that doesn't contain f, as desired. □ Proposition 4.2.34

Proposition 4.2.35 (3.16)**.** *Suppose $f\colon A \to B$ is an A-algebra; suppose $P \subseteq A$ is prime. Then the following are equivalent:*

1. *P is the contraction of a prime ideal of B.*
2. *P is the contraction of an ideal of B.*
3. *$P = PB \cap A$.*

Proof.

(1) $\implies$ (2) Clear.

(2) $\implies$ (3) That $P \subseteq PB \cap A$ is clear. For the converse, note that by hypothesis we have $P = J \cap A$ for some ideal J of B; then $PB \cap A = ((J \cap A)B) \cap A \subseteq J \cap A = P$.

(3) $\implies$ (1) Suppose $PB \cap A = P$. Let $S = f(A \setminus P)$; then S is multiplicatively closed. Furthermore, if $x \in A \setminus P$ and $f(x) \in PB$, then $x \in f^{-1}(PB) = PB \cap A = P$, a contradiction; so $PB \cap S = \emptyset$. So, by Proposition 4.2.31, we have that $P \cdot S^{-1}B = PB \cdot S^{-1}B \subsetneq S^{-1}B$; so there is a maximal (and hence prime) ideal m of $S^{-1}B$ containing $P \cdot S^{-1}B$; by Proposition 4.2.31, we get that $m \cap S = \emptyset$. But
$$m \cap B \supseteq (P \cdot S^{-1}B) \cap B = (PB \cdot S^{-1}B) \cap B \supseteq PB$$
So
$$m \cap A = (m \cap B) \cap A \supseteq PB \cap A = P$$
Conversely, we have $m \cap S = \emptyset$; so
$$m \cap B \subseteq B \setminus S = B \setminus f(A \setminus P) \subseteq (B \setminus f(A)) \cup f(P)$$
So
$$m \cap A = f^{-1}(m \cap B) \subseteq f^{-1}((B \setminus f(A)) \cup f(P)) = f^{-1}(f(P)) \subseteq f^{-1}(f(P)B) = PB \cap A = P$$
So $P = m \cap A = (m \cap B) \cap A$. But m is a prime ideal of $S^{-1}B$, and hence is a prime ideal of B. So P is the contraction of a prime ideal of B. □ Proposition 4.2.35

5 Chapter 4: Primary decompositions

In a general context (i.e. Noetherian rings), we can uniquely factorize ideals into "primary" ideals.

Definition 5.0.1. An ideal Q of A is *primary* if $Q \neq A$ and whenever $xy \in Q$ we have $x \in Q$ or $y^n \in Q$ for some $n > 0$.

Remark 5.0.2. Q is primary if and only if $A/Q \neq 0$ and every zero divisor in A/Q is nilpotent.

Remark 5.0.3. Contractions of primary ideals are primary.

Proof. Consider the A-algebra $f\colon A \to B$; suppose Q is a prime ideal of B. Let $\pi\colon A \to B/Q$ be $x \mapsto f(x)+Q$. Then $\ker(\pi) = f^{-1}(Q)$; so, by the first isomorphism theorem, we get an isomorphism $A/f^{-1}(Q) \cong B/Q$. In particular, we get that every zero divisor of $A/f^{-1}(Q)$ is nilpotent; so $f^{-1}(Q)$ is primary. □ Remark 5.0.3

Definition 5.0.4. Suppose A is a ring; suppose I is an ideal of A. We define the *radical of* A to be $r(A) = \sqrt{A} = \{ f \in A : f^n \in Q \text{ for some } n \geq 0 \}$.

Proposition 5.0.5 (4.1)**.** *Suppose Q is a primary ideal of A. Then $r(Q)$ is the smallest prime ideal containing Q; i.e. $r(Q)$ is prime and given any prime ideal P containing Q we have $r(Q) \subseteq P$.*

Proof. It suffices to show that $r(Q)$ is prime. But if $xy \in r(Q)$, then $x^m y^m \in Q$ for some $m > 0$; so either $x^m \in Q$ or $y^{mn} \in Q$ for some $n > 0$, and in particular we get $x \in r(Q)$ or $y \in r(Q)$. □ Proposition 5.0.5

Definition 5.0.6. Suppose Q is primary; let $P = r(Q)$, so P is prime. We then say that Q is *P-primary*.

Example 5.0.7. Let $A = \mathbb{Z}$. The prime ideals are (0) and (p) for p prime; the primary ideals are (0) and (p^n) for p prime and $n > 0$.

In general it's not true that every primary ideal is a power of a prime ideal; nor is it true in general that a power of a prime ideal is primary.

Remark 5.0.8. If $P \in \operatorname{Spec}(A)$ then for any $n > 0$ we have $r(P^n) = P$.

Proof. It is clear that $P \subseteq r(P^n)$. For the converse, note that if $x \in r(P^n)$ then $x^m \in P^n \subseteq P$ for some $m > 0$. But P is prime; so $x \in P$. □ Remark 5.0.8

It was mentioned that in $\mathbb{Z}$ the primary ideals are (p^n) where p is prime and $n > 0$.

Remark 5.0.9.

1. Suppose A is a UFD, $p \in A$ is prime, and $n > 0$; then (p^n) is primary.
2. Suppose A is a PID and Q is a primary ideal of A. Then $Q = (p^n)$ for some prime $p \in A$ and some $n > 0$.

Proof.

1. Suppose $xy \in (p^n)$; then $p^n \mid xy$, and the prime factorization of xy is $xy = p^m q_1 q_2 \dots q_\ell$ for some $m \geq m$. If $x \notin (p^n)$, then p appears less than n-many times in the prime factorization of x; so p appears in the prime factorization of y. So $p \mid y$, and $p^n \mid y^n$; so $y^n \in (p^n)$.
2. Write $Q = (d)$; let $d = p_1^{n_1} \dots p_\ell^{n_\ell}$ be the prime factorization, and let $m = \max\{ n_1, \dots, n_\ell \}$. Then $(p_1 \dots p_\ell)^m \in (d)$. So $(p_1, \dots, p_\ell \in r(Q)$; so, by Proposition 5.0.5 since $r(Q)$ is prime we have that $p_i \in r(d)$ for some $i \in \{ 1, \dots, \ell \}$. So $p_i^n \in (d)$, and $d \mid p_i^n$; so p_i is the only prime in the prime factorization of d. So $\ell = 1$, and $Q = (p_i^n)$. □ Remark 5.0.9

Example 5.0.10. For k a field, consider $A = k[x, y]$ and $Q = (x, y^2)$.

Claim 5.0.11. *Q is primary.*

Proof. Well,

$$A/Q \cong k[y]/(y^2) = \{\, ay + b : a, b \in k \,\}$$

Suppose now that $ay + b$ is a zero divisor; say $0 = (ay + b)(a'y + b') = (ab' + ba')y + bb'$ with at least one of a', b' non-zero. In particular, we get

$$bb' = 0$$
$$ab' + ba' = 0$$

Well, since $bb' = 0$, we have $b = 0$ or $b' = 0$; but in the latter case the second equation yields $ba' = 0$ and $a' \neq 0$, so $b = 0$. So in either case we have $b = 0$. So zero divisors are of the form ay for some $a \in k$. But $(ay)^2 = 0$ in $k[y]/(y^2)$; so every zero divisor in A/Q is nilpotent. □ Claim 5.0.11

Claim 5.0.12. *$r(Q) = (x, y)$.*

Proof.

($\supseteq$) Easy.

($\subseteq$) Note that by Proposition 5.0.5 we have that $r(Q)$ is contained in every prime containing Q. But $Q \subseteq (x, y)$ and (x, y) is prime. So $r(Q) \subseteq (x, y)$. □ Claim 5.0.12

But now if we had $Q = P^n$ for some prime ideal P and some $n > 0$, then $(x, y) = r(Q) = r(P^n) = P$. So $Q = (x, y)^n$. But $x \notin (x, y)^n$ for any $n > 1$; so $n = 1$. So $(x, y^2) = Q) = (x, y)$, a contradiction since $y \notin (x, y^2)$.

So Q is a primary ideal of a UFD that is not a power of any prime ideal. (Note that given an ideal I we define I^n to be the ideal generated by $a_1 \dots a_n$ for $a_1, \dots, a_n \in I$.)

Example 5.0.13. Consider $A = k[x, y, z]/(xy - z^2)$; let $\overline{x}, \overline{z}$ be the images of x, z in A. Let $P = (\overline{x}, \overline{z})$. By the second isomorphism theorem, we then get that

$$A/P \cong k[x, y, z]/(x, z) \cong k[y]$$

is an integral domain; so P is prime. But in A we have $\overline{xy} = (\overline{z})^2 \in P^2$.

Claim 5.0.14. *$\overline{x} \notin P^2$.*

Proof. Well, if we had $\overline{x} \in P^2$, then we would have $x \in (x, z)^2 + (xy - z^2) \subseteq (x, y, z)^2$ in $k[x, y, z]$, a contradiction. □ Claim 5.0.14

Claim 5.0.15. *$\overline{y} \notin P$.*

Proof. If we had $\overline{y} \in P$ then we would have $A/P \cong k \ncong k[y]$, a contradiction. □ Claim 5.0.15

So $\overline{y} \notin r(P^2) = P$. So P^2 is not primary.

However, we do get

Proposition 5.0.16 (4.2)**.** *A power of a maximal ideal is primary.*

Proof. Suppose m is a maximal ideal of A; suppose $n > 0$. Then $m = r(m^n)$; so m/m^n is the nilradical of A/m^n; so, by Proposition 4.2.34 we have that m/m^n is the intersection of all prime ideals in A/m^n. But m/m^n is maximal in A/m^n. So m/m^n is the only prime ideal in A/m^n. So for every $\alpha \in A/m^n$ we have either $\alpha \in m/m^n$ or $(\alpha) = A/m^n$. But in the former case we get that $\alpha^n = 0$, and in the latter case we get that α is invertible in A/m^n. So every element of A/m^n is either nilpotent or invertible; in particular, we get that all zero divisors are nilpotent. □ Proposition 5.0.16

Remark 5.0.17. We only used that $r(m^n)$ is maximal. In particular, if I is any ideal whose radical is maximal, then I is primary.

Lemma 5.0.18 (4.3)**.** *Suppose $Q_1, \dots, Q_n$ are P-primary; i.e. each Q_i is primary and $r(Q_i) = P$. Then $Q_1 \cap \dots \cap Q_n$ is P-primary.*

Proof. Well, $r(Q_1 \cap \cdots \cap Q_n) = r(Q_1) \cap \cdots \cap r(Q_n) = P$. Suppose now that $xy \in Q_1 \cap \cdots \cap Q_n$ with $x \notin Q_1 \cap \cdots \cap Q_n$. Then for some i we have $x \notin Q_i$. But $xy \in Q_i$, and Q_i is primary; so $y \in r(Q_i) = P = r(Q_1 \cap \cdots \cap Q_n)$. So $Q_1 \cap \cdots \cap Q_n$ is primary. ☐ Lemma 5.0.18

Definition 5.0.19. A *primary decomposition* of an ideal I is an expression of the form $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ with each Q_i primary. We say I is *decomposable* if I has a primary decomposition.

Fact 5.0.20 (To prove later)**.** *In a Noetherian ring every ideal is decomposable.*

If in a primary decomposition

$$I = \bigcap_{i=1}^{n} Q_i$$

we have $r(Q_i) = r(Q_j)$ then $Q_i \cap Q_j$ is primary with the same radical; so we may replace Q_i and Q_j by $Q_i \cap Q_j$ in the decomposition. So, if I is decomposable, then there is a primary decomposition where the $r(Q_i)$ are distinct. Also if

$$Q_i \supseteq \bigcap_{j \neq i} Q_j$$

then we can drop Q_i from the intersection. So we get a decomposition where

$$Q_i \not\supseteq \bigcap_{j \neq i} Q_j$$

for any i.

Definition 5.0.21. A primary decomposition satisfying the above two properties is called an *irredundant decomposition*. (The book calls these *minimal decompositions*.)

Lemma 5.0.22 (4.4)**.** *Suppose Q is P-primary; suppose $x \in A$. Then*

1. *If $x \in Q$ then $\{ a \in A : xa \in Q \} = (Q : x) = A$.*
2. *If $x \notin P$ then $(Q : x) = Q$.*
3. *If $x \notin Q$ then $Q \subseteq (Q : x) \subseteq P$ and $(Q : x)$ is P-primary.*

Proof.

1. Generally true; doesn't require that Q be P-primary.
2. That $(Q : x) \supseteq Q$ is clear. For the converse, suppose $y \in (Q : x)$; i.e. suppose $xy \in Q$. If $y \notin Q$ then since Q is primary we have that $x \in r(Q) = P$, a contradiction.
3. Again, that $Q \subseteq (Q : x)$ is clear. Note also that if $xy \in Q$, then since $x \notin Q$ and Q is primary we have that $y \in r(Q)$; so $(Q : x) \subseteq P$. Then

   $$P = r(Q) \subseteq r(Q : x) \subseteq r(P) = P$$

   So $r(Q : x) = P$. Suppose now that $yz \in (Q : x)$; i.e. suppose $xyz \in Q$. If $y \notin (Q : x)$, then $xy \notin Q$; so $z \in r(Q) = P = r(Q : x)$ since Q is primary. So $(Q : x)$ is primary.

☐ Lemma 5.0.22

Theorem 5.0.23 (4.5: First uniqueness theorem of primary decompositions)**.** *Suppose*

$$I = \bigcap_{i=1}^{n} Q_i$$

is an irredundant primary decomposition. Let $P_i = r(Q_i)$. Then $\{ P_1, \ldots, P_n \}$ is independent of the particular irredundant decomposition. (In particular, so is n.)

Proof. We will show that the P_i are precisely the prime ideals appearing in $\{ r(I : x) : x \in A \}$; this will suffice. Note that for any $x \in A$ we have

$$(I : x) = \left(\bigcap_{i=1}^{n} Q_i : x \right) = \bigcap_{i=1}^{n} (Q_i : x) = \bigcap_{\substack{i \\ x \notin Q_i}} (Q_i : x)$$

by Lemma 5.0.22. So

$$r(I : x) = \bigcap_{\substack{i \\ x \notin Q_i}} r(Q_i : x) = \bigcap_{\substack{i \\ x \notin Q_i}} P_i$$

again by Lemma 5.0.22.

Claim 5.0.24. *In general if Q is prime and $Q \supseteq P_1 \cap \cdots \cap P_\ell$ then $Q \supseteq P_j$ for some j.*

Proof. If we had $Q \not\supseteq P_i$ for all i, we would have $b_i \in P_i \setminus Q$ for all i. Then

$$b_1 \dots b_\ell \in \bigcap_{i=1}^{\ell} P_i \subseteq Q$$

So, since Q is prime, we would have $b_j \in Q$ for some j, a contradiction. ☐ Claim 5.0.24

Hence if $r(I : x)$ is prime then $r(I : x) = P_j$ for some j.

Conversely, fix j; we show that $P_j = r(I : x)$ for some $x \in A$. Since the decomposition is irredundant, there is

$$x_j \in \bigcap_{i \neq j} Q_i \setminus Q_j$$

Then

$$r(I : x_j) = \bigcap_{\substack{i \\ x_j \notin Q_i}} P_i = P_j$$

☐ Theorem 5.0.23

Hence if I is a decomposable ideal then we can associate to it as invariants the radicals of the primary ideals appearing in any irredundant primary decomposition.

Definition 5.0.25. The prime ideals $P_1, \dots, P_n$ are said to *belong to* or to be *associated to* I.

The irredundant primary decomposition is *not* unique; only the associated primes are.

Example 5.0.26. Let $A = k[x, y]$, where k is a field; consider $I = (x^2, xy)$.

Claim 5.0.27. $I = (x) \cap (x^2, y)$.

Proof.

($\subseteq$) One simply notes that $x^2, xy \in (x) \cap (x^2, y)$.

($\supseteq$) Suppose $f \in (x) \cap (x^2, y)$; then $f = gx = h_1x^2 + h_2y$ for some $g, h_1, h_2 \in A$. But then $h_2y = gx - h_1x^2$; so $x \mid h_2y$. But x is prime in A, and $x \nmid y$; so $x \mid h_2$, and $h_2 = h_3x$ for some $h_3 \in A$. So

$$f = h_1x^2 + h_2y = h_1x^2 + h_3xy \in I$$

☐ Claim 5.0.27

Now, (x) is prime, and hence primary. Furthermore, (x^2, y) is primary since $k[x, y]/(x^2, y) \cong k[x]/(x^2)$ has zero divisors ax for $a \in k$, which are all nilpotent. Also, $r(x) = (x) \neq (x, y) = r(x^2, y)$; so $I = (x) \cap (x^2, y)$ is an irredundant primary decomposition.

Claim 5.0.28. $I = (x) \cap (x, y)^2$.

Proof.

($\subseteq$) Again, one notes that $x^2, xy \in (x) \cap (x,y)^2$.

($\supseteq$) Suppose $f \in (x) \cap (x,y)^2$. Then, since $f \in (x,y)^2$, we have that the monomials of f are all divisible by x^2, y^2, or xy. Since $f \in (x)$ we have that the monomials of f are all divisible by x. So the monomials of f are all divisible by x^2 or xy; so $f \in (x^2, xy) = I$. $\square$ Claim 5.0.28

Now, (x) is prime, and $(x,y)^2$ is primary by Proposition 5.0.16 since (x,y) is maximal in $k[x,y]$. Also $r(x) = (x) \neq r(x,y)^2 = (x,y)$, so $I = (x) \cap (x,y)^2$ is a second irredundant decomposition. Note also that the primes associated to I are (x) and (x,y), and $(x) \subseteq (x,y)$. So we can have non-trivial containments among the associated prime ideals.

Definition 5.0.29. Suppose I is a decomposable ideal. The minimal elements of the set of associated primes are called the *minimal primes* (or *isolated primes*) of I. i.e. a minimal prime of I is an associated prime of I that does not properly contain any other associated prime of I. The other associated primes are called *embedded primes*.

In the previous example, we saw that (x) is a minimal prime of (x^2, xy) while (x,y) is an embedded prime of (x^2, xy).

Proposition 5.0.30 (4.6)**.** *Suppose I is a decomposable ideal. Then the minimal primes of I are precisely the minimal elements of $\{ P \supseteq I : P \text{ prime} \}$.*

Proof. Let $I = Q_1 \cap \cdots \cap Q_n$ be an irredundant primary decomposition; let $P_i = r(Q_i)$ be the associated prime ideals of I. Suppose $P \supseteq I$ is prime; then $P \supseteq Q_1 \cap \cdots \cap Q_n$, and

$$P = r(P) \supseteq r(Q_1) \cap \cdots \cap r(Q_n) = P_1 \cap \cdots \cap P_n$$

So, by Claim 5.0.24, we have $P \supseteq P_j$ for some j. Hence every prime containing I contains an associated prime of I. But $\{ P_1, \ldots, P_n \} \subseteq \{ P \supseteq I : P \text{ prime} \}$, and every element of the latter contains an element of the former; so the minimal elements of $\{ P_1, \ldots, P_n \}$ are exactly the minimal elements of $\{ P \supseteq I : P \text{ prime} \}$. $\square$ Proposition 5.0.30

Remark 5.0.31. If I is decomposable then $r(I)$ is the intersection of the minimal primes of I.

Proof. Proposition 4.2.34 applied to A/I implies

$$\begin{aligned} r(I) &= \bigcap \{ P \in \operatorname{Spec}(A) : P \supseteq I \} \\ &= \bigcap \{ P \in \operatorname{Spec}(A) : P \supseteq I, P \text{ minimal such} \} \\ &= \bigcap \{ P \in \operatorname{Spec}(A) : P \text{ minimal associated prime ideal of } I \} \end{aligned}$$

by Proposition 5.0.30. Alternatively, if $I = Q_1 \cap \cdots \cap Q_m$ is the primary decomposition, then $r(I) = r(Q_1) \cap \cdots \cap r(Q_m)$ is the intersection of the minimal elements of $\{ r(Q_1), \ldots, r(Q_m) \}$. $\square$ Remark 5.0.31

Corollary 5.0.32. *Suppose I is a radical decomposable ideal. Then I has a* prime decomposition *$I = P_1 \cap \cdots \cap P_n$ where $P_1, \ldots, P_n$ are prime. Moreover, if this decomposition is* irredundant *(i.e.*

$$P_i \not\supseteq \bigcap_{j \neq i} P_j$$

for all $i \in \{ 1, \ldots, n \}$) then the decomposition is unique (up to reordering).

Proof. Write $I = Q_1 \cap \cdots \cap Q_m$ be the irredundant primary decomposition; then $I = r(I) = r(Q_1) \cap \cdots \cap r(Q_m)$. Let $P_i = r(Q_i)$. Reordering, we may assume that $P_1, \ldots, P_n$ are the minimal primes of I, where $n \leq m$. Then $I = P_1 \cap \cdots \cap P_n$ is an irredundant prime decomposition (since if

$$P_i \supseteq \bigcap_{j \neq i} P_j$$

then by primality of P_i we get that $P_i \supseteq P_j$ for some $j \neq i$, contradicting minimality.)

Suppose now that $I = P_1 \cap \cdots \cap P_n = P'_1 \cap \cdots \cap P'_{n'}$ are two irredundant prime decompositions. Then both are irredundant primary decompositions, so by Theorem 5.0.23, we get that $n' = n$ and

$$\{ P'_1, \ldots, P'_n \} = \{ r(P'_i), \ldots, r(P'_n) \} = \{ r(P_1), \ldots, r(P_n) \} = \{ P_1, \ldots, P_n \}$$

□ Corollary 5.0.32

Note that radical is necessary here since the intersection of prime ideals is always radical.

For a geometric interpretations, we work in the Zariski topology on $\mathrm{Spec}(A)$; recall that the closed sets are $V(I) = \{ P \in \mathrm{Spec}(A) : P \supseteq I \}$ for I an ideal of A.

Proposition 5.0.33. *$V(I) = V(J)$ if and only if $r(I) = r(J)$.*

Proof. We apply Proposition 4.2.34 to A/I and A/J to get that

$$\begin{aligned} r(I) = r(J) &\iff \bigcap \{ P \in \mathrm{Spec}(A) : P \supseteq I \} = \bigcap \{ P \in \mathrm{Spec}(A) : P \supseteq J \} \\ &\iff \{ P \in \mathrm{Spec}(A) : P \supseteq I \} = \{ P \in \mathrm{Spec}(A) : P \supseteq J \} \\ &\iff V(I) = V(J) \end{aligned}$$

since if $P \supseteq I$ then

$$P \supseteq \bigcap \{ Q \in \mathrm{Spec}(A) : Q \supseteq J \} \supseteq J$$

□ Proposition 5.0.33

Definition 5.0.34. A closed set is *irreducible* if it is not the union of two proper closed sets.

Suppose I is a decomposable ideal; let $r(I) = P_1 \cap \cdots \cap P_n$ be the irredundant prime decomposition. Then

$$V(I) = V(r(I)) = V(P_1) \cup \cdots \cup V(P_n)$$

and this decomposition is irredundant in the sense that

$$V(P_i) \not\subseteq \bigcup_{j \neq i} V(P_j)$$

As we will see on assignment 4, we get that each $V(P_i)$ is irreducible. Furthermore, the uniqueness of the prime decomposition of $r(I)$ will imply the uniqueness of the irredundant decomposition of $V(I)$ into irreducible closed sets.

Geometrically, we interpret this as saying that if I is decomposable, then $V(I)$ can be written uniquely as an irredundant union of irreducible closed sets. These $V(P_i)$ are called the *irreducible components of* $V(I)$.

If we write $I = Q_1 \cap \cdots \cap Q_m$ for $m \geq n$ with $P_i = r(Q_i)$, then $P_{n+1}, \ldots, P_m$ are the embedded primes. So if $j > n$ we have $V(P_j) \subseteq V(P_i)$ for some $i \leq n$; hence the term "embedded".

Returning to algebra, what can we say about the existence of decomposable ideals?

Definition 5.0.35. A ring is *Noetherian* if every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ is *stationary*; i.e. there is $n \geq 1$ such that $I_n = I_{n+1} = I_{n+2} = \cdots$.

A consequence of Noetherianity is that every non-empty set of ideals has a maximal element (with respect to $\subseteq$); this is simply by Zorn's lemma.

Definition 5.0.36. An ideal I of A is *irreducible* if whenever $I = J \cap J'$ then $I = J$ or $I = J'$.

Lemma 5.0.37 (7.13)**.** *If A is Noetherian then every ideal is a finite intersection of irreducible ideals.*

Proof. If not, let $\mathcal{S} \neq \emptyset$ be the set of counterexamples; let $I \in \mathcal{S}$ be maximal (which exists by Noetherianity). Then $I = J \cap J'$ with $J \supsetneq I$ and $J' \supsetneq I$. Then, by maximality of I, we have $J, J' \notin \mathcal{S}$. So

$$\begin{aligned} J &= J_1 \cap \cdots \cap J_\ell \\ J' &= J'_1 \cap \cdots \cap J'_{\ell'} \end{aligned}$$

with each J_i and each J_i' irreducible. But then

$$I = J \cap J' = J_1 \cap \cdots \cap J_\ell \cap J_1' \cap \cdots \cap J_{\ell'}'$$

So $I \notin \mathcal{S}$, a contradiction. ☐ Lemma 5.0.37

Lemma 5.0.38 (7.12)**.** *In a Noetherian ring, every irreducible ideal is primary.*

Proof. Suppose $I \subseteq A$ is an ideal. Then since A is Noetherian we get that A/I is Noetherian. Then I is irreducible if and only if (0) is irreducible in A/I, and I is primary if and only if (0) is primary in A/I; it thus suffices to check the case $I = (0)$. Suppose then that $xy = 0$ but $y \neq 0$; we wish to show that $x^n = 0$ for some n. Consider $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \ldots$. This is an ascending chain of ideals, so by Noetherianity we get than $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1}) = \ldots$ for some n.

Claim 5.0.39. $(x^n) \cap (y) = (0)$.

Proof. If $a \in (x^n) \cap (y)$, then $a = cy$ for some $c \in A$; so $ax = cyx = 0$. But $a \in (x^n)$ as well, so $a = bx^n$ for some $b \in A$; so $0 = ax = bx^{n+1}$, and $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$. So $bx^n = 0$, and $a = 0$. ☐ Claim 5.0.39

But (0) is irreducible, and by assumption we have that $(y) \neq (0)$; so $(x^n) = (0)$, and $x^n = 0$. ☐ Lemma 5.0.38

Corollary 5.0.40 (7.14)**.** *In a Noetherian ring every ideal is decomposable.*

5.1 Noetherian rings

We look more closely at Noetherian rings.

An important characterization of Noetherian rings is the following:

Proposition 5.1.1. *A is Noetherian if and only if every ideal is finitely generated.*

Proof.

($\Longrightarrow$) Suppose $I \subseteq A$ is not finitely generated. We inductively define a sequence of elements $a_i \in I$ by picking any $a_0 \in I$ and choosing $a_{i+1} \in I \setminus (a_0, \ldots, a_i)$; this is possible since $I \neq (a_0, \ldots, a_i)$ as I is not finitely generated.

($\Longleftarrow$) Suppose $I_1 \subseteq I_2 \subseteq \ldots$ is an ascending chain of ideals. Let

$$I = \bigcup_{i=1}^{\infty} I_i$$

Then I is an ideal of A, so I is finitely generated; say $I = (a_1, \ldots, a_\ell)$. Pick $N > 0$ such that $a_1, \ldots, a_\ell \in I_N$; then $I \subseteq I_N \subseteq I_{N+1} \subseteq \ldots \subseteq I$, and $I_N = I_{N+1} = \cdots = I$. ☐ Proposition 5.1.1

A natural generalization to modules:

Definition 5.1.2. Suppose A is a ring; suppose M is an A-module. We say M is *Noetherian* if every ascending chain of submodules is stationary.

Remark 5.1.3. A ring A is Noetherian as an A-module if and only if A is a Noetherian ring.

Just as in the ring case, we have:

Proposition 5.1.4. *M is Noetherian if and only if every submodule is finitely generated.*

Proposition 5.1.5 (6.3)**.** *Suppose $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is an exact sequence of A-modules. Then the following are equivalent:*

1. *M is Noetherian.*

2. *M' and M'' are Noetherian.*

Proof.

($\implies$) This is exactly saying that Noetherianity is preserved under submodules and quotients. But $f\colon M' \to \operatorname{im}(f)$ is an isomorphism; so any ascending chain of submodules in M' gets mapped isomorphically to an ascending chain of submodules in $\operatorname{im}(f) \subseteq M$, and is thus stationary. Furthermore, $M'' \cong M/\ker(g)$, so any ascending chain of submodules in M'' lifts to an ascending chain of submodules in M by the correspondence theorem, and is thus stationary. So M' and M'' are Noetherian.

($\impliedby$) Suppose $L_1 \subseteq L_2 \subseteq \cdots$ is an ascending chain of submodules in M. Choose n such that $g(L_n) = g(L_{n+1}) = \cdots$ and $f^{-1}(L_n) = f^{-1}(L_{n+1}) = \cdots$.

Claim 5.1.6. $L_n = L_{n+1} = \cdots$.

Proof. We check that $L_n = L_{n+1}$. Suppose $a \in L_{n+1}$. Then $g(a) \in g(L_{n+1}) = g(L_n)$; we may thus pick $b \in L_n$ such that $g(a) = g(b)$. So $a - b \in \ker(g) = \operatorname{im}(f)$; pick $c \in M'$ such that $a - b = f(c)$. Then $f(c) = a - b \in L_{n+1}$; so $c \in f^{-1}(L_{n+1}) = f^{-1}(L_n)$, and $a - b = f(c) \in L_n$. But $b \in L_n$; so $a \in L_n$. □ Claim 5.1.6

□ Proposition 5.1.5

Corollary 5.1.7 (6.4)**.** *If $M_1, \ldots, M_n$ are Noetherian A-modules then*

$$\bigoplus_{i=1}^{n} M_i$$

is Noetherian.

Proof. Well, $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ is exact; so $M_1 \oplus M_2$ is Noetherian by Proposition 5.1.5. Iterating, one obtains the desired conclusion. □ Corollary 5.1.7

Corollary 5.1.8 (6.5)**.** *If A is a Noetherian ring, then every finitely generated A-module is Noetherian.*

Proof. Suppose M is generated as an A-module by $x_1, \ldots, x_\ell$. We then get a surjective A-linear map

$$\begin{aligned} A^\ell &\to M \\ (0, \ldots, \underbrace{1}_{i^{\text{th}} \text{ spot}}, \ldots, 0) &\mapsto x_i \end{aligned}$$

But A is Noetherian, so by Corollary 5.1.7 we get that A^ℓ is Noetherian A-module, and then by Proposition 5.1.5 we get that M is a Noetherian A-module. □ Corollary 5.1.8

Corollary 5.1.9 (Proposition 7.2)**.** *If A is a Noetherian ring and B is a finite A-algebra, then B is a Noetherian ring.*

(Recall that a finite A-algebra is one that is finitely generated as an A-module.)

Proof. Well, B is a finitely generated A-module, so B is a Noetherian A-module. So every ideal of B is an A-submodule of B; so every ideal of B is finitely generated as an A-module, and hence as a B-submodule. So B is a Noetherian ring. □ Corollary 5.1.9

Theorem 5.1.10 (7.5: Hilbert's basis theorem)**.** *Suppose A is a Noetherian ring. Then $A[x]$ is a Noetherian ring.*

Proof. Suppose $I \subseteq A[x]$ is an ideal. Let $J \subseteq A$ be the set of leading coefficients of elements of I.

Claim 5.1.11. *J is an ideal.*

Proof. Suppose $a, b \in J$; take $f, g \in I$ with $f(x) = ax^n + \cdots$ and $g(x) = bx^m + \cdots$ (where the remaining terms are of lower order). Suppose without loss of generality that $n \geq m$. Then $x^{n-m}g = bx^n + \cdots \in I$; so

$$f + x^{n-m}g = (a+b)x^n + \cdots \in I$$

so $a + b \in J$. Also, if $c \in A$ then $cf = cax^n + \cdots \in I$; so $ca \in J$. So J is an ideal. ☐ Claim 5.1.11

But A is Noetherian; so $J = (a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in A$. For $i \in \{1, \ldots, n\}$, pick $f_i = a_i x^{r_i} + \cdots \in I$. Let $I' = (f_1, \ldots, f_n) \subseteq I$. Let $r = \max\{r_1, \ldots, r_n\}$.

Claim 5.1.12. *If $f \in I$ then $f = g + h$ where $\deg(g) < r$ and $h \in I'$.*

Proof. We apply induction on $\deg(f)$.

For the base case, note that if $\deg(f) < r$, then we can take $g = f$ and $h = 0$.

For the induction step, write $f = ax^m + \cdots$. Then since $a \in J$ we have

$$a = \sum_{i=1}^{n} u_i a_i$$

for some $u_1, \ldots, u_n \in A$. Then

$$h = \sum_{i=1}^{n} u_i x^{m-r_i} f_i = ax^m + \cdots \in I'$$

since $u_i x^{m-r_i} f_i$ has leading coefficient $u_i a_i$ and degree m. But then h and f have the same leading term, namely ax^m; so $\deg(f - h) < \deg(f)$. So, by the induction hypothesis, we get that $f - h = g + h_1$ where $\deg(g) < r$ and $h_1 \in I'$; so $f = g + (h + h_1)$, with $\deg(g) < r$ and $h + h_1 \in I'$. ☐ Claim 5.1.12

So $I = I' + I \cap \{g \in A[x] : \deg(g) < r\}$. But $M = \{g \in A[x] : \deg(g) < r\}$ is a finitely generated A-module (with generators $1, x, \ldots, x^{r-1}$), and A is Noetherian; so, by Corollary 5.1.8, we have that M is Noetherian. But $I \cap M$ is a submodule of M; hence by Noetherianity we have M is finitely generated as an A-module, say by generators $g_1, \ldots, g_\ell$. So if $f \in I$ then

$$f = h_1 f_1 + \cdots + h_n f_n + b_1 g_1 + \cdots + b_\ell g_\ell \in (f_1, \ldots, f_n, g_1, \ldots, g_\ell)$$

where $h_1, \ldots, h_n \in A[x]$ and $b_1, \ldots, b_\ell \in A$. So $I = (f_1, \ldots, f_n, g_1, \ldots, g_\ell)$, and I is finitely generated. ☐ Theorem 5.1.10

Corollary 5.1.13. *Suppose A is a Noetherian ring; suppose B is a finitely generated A-algebra. Then B is a Noetherian ring.*

Proof. Let $b_1, \ldots, b_\ell$ be generators for B. Then

$$\begin{aligned} A[x_1, \ldots, x_\ell] &\xrightarrow{\pi} B \\ P(x_1, \ldots, x_\ell) &\mapsto P(b_1, \ldots, b_\ell) \end{aligned}$$

is a surjective ring homomorphism. (Note that $P(b_1, \ldots, b_\ell) = P^f(b_1, \ldots, b_\ell)$ where $f\colon A \to B$ is the given ring homomorphism and P^f is the result of applying f to the coefficients of P.) So $B \cong A[x_1, \ldots, x_\ell]/\ker(\pi)$. But applying Hilbert's basis theorem ℓ times yields that $A[x_1, \ldots, x_\ell]$ is Noetherian; so B is a Noetherian ring. ☐ Corollary 5.1.13

Example 5.1.14. PIDs are Noetherian. So, by Hilbert's basis theorem, we have that every finitely generated ring (i.e. finitely generated $\mathbb{Z}$-algebra) is Noetherian. Likewise, every finitely generated k-algebra is Noetherian, where k is a field.

Proposition 5.1.15 (7.3)**.** *Noetherianity is preserved by localization.*

Proof. Suppose A is Noetherian and $S \subseteq A$ is multiplicatively closed; suppose $I \subseteq S^{-1}A$ is an ideal. Since every ideal is an extension ideal, we have some ideal J of A such that $I = S^{-1}J$. Then, since A is Noetherian, we have $J = (a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in A$; one checks that $I = \left(\frac{a_1}{1}, \ldots, \frac{a_n}{1}\right)$. ☐ Proposition 5.1.15

Besides primary decomposition, we get many nice properties of Noetherian rings.

Proposition 5.1.16 (7.14)**.** *In a Noetherian ring, every ideal contains a finite power of its radical.*

Proof. Suppose A is Noetherian; suppose $I \subseteq A$ is an ideal. Write $r(I) = (a_1, \ldots, a_n)$. Then for each $i \in \{1, \ldots, n\}$ there is some $r_i > 0$ such that $a_i^{r_i} \in I$. But for any $m > 0$, we have

$$r(I)^m = (a_1^{m_1} \cdots a_n^{m_n} : m_1 + \cdots + m_n = m)$$

Let $m = n \max\{r_1, \ldots, r_n\}$; then whenever $m_1 + \cdots + m_n = m$ we have $i \in \{1, \ldots, n\}$ such that $m_i \geq r_i$. Then $r(I)^m \subseteq I$. □ Proposition 5.1.16

Corollary 5.1.17 (7.15)**.** *In a Noetherian ring the nilradical is nilpotent.*

Proof. Applying Proposition 5.1.16 to $I = (0)$, we get that $\mathcal{R}^m = (0)$ for some m. □ Corollary 5.1.17

Corollary 5.1.18 (7.16)**.** *Suppose A is Noetherian, $m \subseteq A$ is a maximal ideal, and $Q \subseteq A$ is an ideal. Then the following are equivalent:*

1. *$r(Q) = m$.*
2. *Q is m-primary.*
3. *$m^n \subseteq Q \subseteq m$ for some $n > 0$.*

Proof.

(1) $\Longrightarrow$ (2) By Proposition 5.0.16 we have that Q is primary. So Q is m-primary.

(2) $\Longrightarrow$ (3) By Proposition 5.1.16 there is $n > 0$ such that $m^n = r(Q)^n \subseteq Q \subseteq m$.

(3) $\Longrightarrow$ (1) We are given that $m^n \subseteq Q \subseteq m$; taking radicals, we find that

$$m = r(m^n) \subseteq r(Q) \subseteq r(m) = m$$

and $r(Q) = m$. □ Corollary 5.1.18

Proposition 5.1.19 (7.17)**.** *Suppose A is Noetherian and $I \subsetneq A$ is a proper ideal. Then the associated primes of I are precisely the prime ideals appearing in $\{(I : x) : x \in A\}$.*

Remark 5.1.20. When we proved "uniqueness" of primary decompositions, we saw that the associated primes of any decomposable ideal are the primes that appear in $\{r(I : x) : x \in A\}$.

Proof of Proposition 5.1.19. Note that $(I : x)$ is the pullback of the annihilator of the image of x in A/I. So if $\pi \colon A \to A/I$ is the quotient, then we get $(I : x) = \pi^{-1}(\mathrm{Ann}(\pi(x)))$. But $\mathrm{Ann}(\pi(x)) = (0 : \pi(x))$ in A/I. So by the correspondence theorem we have that $(I : x)$ is prime if and only if $(0 : \pi(x)) = \mathrm{Ann}(\pi(x))$ is prime. So P is an associated prime of I if and only if $\pi(P)$ is an associated prime of (0). It then suffices to show that the associated primes of (0) are exactly the prime ideals which are annihilators.

Let

$$(0) = \bigcap_{i=1}^{n} Q_i$$

be an irredundant primary decomposition of (0). Fix $i \in \{1, \ldots, n\}$; consider $P_i = r(Q_i)$. By Theorem 5.0.23 we know that $P_i = r(\mathrm{Ann}(x))$ for some $x \in A$. But by the proof of Theorem 5.0.23, any $x \neq 0$ such that

$$x \in \bigcap_{j \neq i} Q_j$$

will do; so for any such x we get that $\mathrm{Ann}(x) \subseteq P_i$. Now, by Proposition 5.1.16, we have $P_i^m \subseteq Q_i$ for some m. So

$$\left(\bigcap_{j \neq i} Q_j\right) \cdot P_i^m \subseteq \bigcap_{j \neq i} Q_j \cap P_i^m \subseteq \bigcap_{j=1}^{n} Q_j = (0)$$

Let m be least such that

$$\left(\bigcap_{j\neq i} Q_j\right) \cdot P_i^m = (0)$$

Let $x \neq 0$ satisfy

$$x \in \left(\bigcap_{j\neq i} Q_j\right) \cdot P_i^{m-1} \neq (0)$$

Since

$$x \in \bigcap_{j\neq i} Q_j$$

we get that $\operatorname{Ann}(x) \subseteq P_i$; by choice of m we get that $P_i \subseteq \operatorname{Ann}(x)$.

The converse is left as an exercise. □ Proposition 5.1.19

6 Chapter 5: Integral dependence

Definition 6.0.1. Suppose $A \subseteq B$ is a subring and $b \in B$. We say b is *integral over* A if there is a non-zero monic $P \in A[x]$ such that $P(b) = 0$.

Remark 6.0.2.

1. If A is a field, then b is integral over A if and only if b is algebraic over A.

2. Every element of A is integral over A; if $a \in A$, we may take $P(x) = x - a$.

3. We can generalize the definition to any A-algebra $f\colon A \to B$. We have to make sense of $P(b)$ where $b \in B$ and $P \in A[x]$; as usual, we define $P(b) = P^f(b)$ where $P^f \in B[x]$ is obtained from P by applying f to the coefficients. Note that $P^f \in f(A)[x]$ is monic; one thus gets that

   Exercise 6.0.3. Suppose $f\colon A \to B$ is an A-algebra; suppose $b \in B$. Then b is integral over A if and only if b is integral over $f(A)$.

   Hence for the most part we can work in the setting of a true subring $A \subseteq B$.

Example 6.0.4. Suppose $q = \frac{r}{s} \in \mathbb{Q}$ where $\gcd(r, s) = 1$. If q is integral over $\mathbb{Z}$, then

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0$$

so

$$r^n + \underbrace{a_{n-1}sr^{n-1} + \cdots + a_0 s^n}_{\text{divisible by } s} = 0$$

So $s \mid r^n$. But $\gcd(r, s) = 1$; so $s = 1$, and $q = r \in \mathbb{Z}$. Hence the only rationals integral over $\mathbb{Z}$ are in fact integers.

Proposition 6.0.5 (5.1)**.** *Suppose $A \subseteq B$; suppose $b \in B$. Then the following are equivalent:*

1. *b is integral over A.*

2. *$A[b]$ (the sub-A-algebra generated by b) is a finite A-algebra; i.e. $A[b]$ is finitely generated as an A-module.*

3. *There exists a finite A-subalgebra $C \subseteq B$ (i.e. $A \subseteq C \subseteq B$ is a subring and C is a finitely generated A-module with $b \in C$.)*

Proof.

(1) $\implies$ (2) Suppose b is integral over A; then

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

for some $n > 0$ and some $a_0, \ldots, a_{n-1} \in A$. Let $M \subseteq B$ be the A-submodule generated by $1, b, \ldots, b^{n-1}$; then $M \subseteq A[b]$ since $1, b, \ldots, b^{n-1} \in A[b]$.

Claim 6.0.6. *$b^m \in M$ for all $m \geq 0$.*

Proof. We apply induction on m. If $m < n$, then this is by construction. If $m \geq n$ then

$$b^m = b^{m-n} \cdot b^n = b^{m-n}(-a_{n-1}b^{n-1} - \cdots - a_1 b - a_0) = -a_{n-1}b^{m-1} - a_{n-2}b^{m-2} - \cdots - a_0 b^{m-n}$$

and by the induction hypothesis we have $b^{m-1}, \ldots, b^{m-n} \in M$; so $b^m \in M$. $\square$ Claim 6.0.6

But every element of $A[b]$ is of the form

$$\sum_{j=1}^{\ell} c_i b^i$$

for some $c_i \in A$. Hence by the claim we have $A[b] = M$.

(2) $\implies$ (3) Clear.

(3) $\implies$ (1) Suppose we have such a C; let $c_1, \ldots, c_n$ generate C as an A-module. Note that for each $i \in \{ 1, \ldots, n \}$ we have $bc_i \in C$ since $b \in C$ and C is a subring; thus

$$bc_i = \sum_{j=1}^{n} a_{ij} c_j$$

for some $a_{ij} \in A$. So

$$(b - a_{ii})c_i - \sum_{\substack{j=1 \\ j \neq i}}^{n} -a_{ij} c_j = 0$$

We can write this system of linear equations in matrix form as follows:

$$\underbrace{\begin{pmatrix} b - a_{11} & -a_{12} & -a_{13} & \cdots & -a_{1n} \\ -a_{21} & b - a_{22} & -a_{23} & \cdots & -a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & -a_{n3} & \cdots & b - a_{nn} \end{pmatrix}}_{M \in M_{n \times n}(C)} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

Multiplying both sides on the left by the matrix of cofactors of M, we find

$$\begin{pmatrix} \det(M) & & 0 \\ & \ddots & \\ 0 & & \det(M) \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

and $\det(M) \in C$. So $\det(M) \cdot c_i = 0$ for all i. But the $c_1, \ldots, c_n$ generate C as an A-module, and multiplication by $\det(M)$ is an A-linear map $C \to C$. So $\det(M) \cdot x = 0$ for all $x \in C$. In particular, since $1 \in C$ we have $\det(M) = 0$. But

$$\det(M) = b^n + a'_{n-1}b^{n-1} + \cdots + a'_1 b + a_0$$

where the a'_i are sums of products of a_{ij}, and thus in A. (One checks this by induction.) So b is integral over A. $\square$ Proposition 6.0.5

Corollary 6.0.7 (5.2)**.** *Suppose $b_1, \dots, b_\ell \in B$ are integral over A. Then $A[b_1, \dots, b_\ell]$ is a finite A-algebra.*

Proof. By Proposition 6.0.5 we have

- $A[b_1]$ is a finite A-algebra since b_1 is integral over A.
- $A[b_1, b_2]$ is a finite $A[b_1]$-algebra since b_2 is integral over A, and hence over $A[b_1]$.
- Continuing, we find that $A[b_1, \dots, b_\ell]$ is a finite $A[b_1, \dots, b_{\ell-1}]$-algebra.

TODO 1. *Ref? 2.3.14?*

Hence, by **??**, we get that $A[b_1, \dots, b_\ell]$ is a finite A-algebra. ☐ Corollary 6.0.7

Corollary 6.0.8 (5.3)**.** *Suppose $A \subseteq B$. Let $C = \{ b \in B : b \text{ is integral over } A \}$. Then C is a subring of B.*

Proof. Suppose $b_1, b_2 \in C$. We wish to show that $b_1 + b_2, -b_1, b_1 b_2 \in C$. But $b_1 + b_2, -b_1, b_1 b_2 \in A[b_1, b_2]$ is a finite A-algebra by Corollary 6.0.7; so, by Proposition 6.0.5, we get that $b_1 + b_2$, $-b_1$, and $b_1 b_2$ are all integral over A. So C is a subring of B. ☐ Corollary 6.0.8

Definition 6.0.9. The subring C given in Corollary 6.0.8 is called the *integral closure* of A in B. If $C = B$ (i.e. every $b \in B$ is integral over A) then we say that B is *integral over A*. If $C = A$ then we say that A is *integrally closed in B*.

Example 6.0.10. $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Remark 6.0.11. Integrality explains the distinction between finitely generated A-algebras and finite A-algebras: if B is an A-algebra, then B is a finitely generated integral A-algebra if and only if B is a finite A-algebra.

Proof.

($\implies$) Suppose $B = A[b_1, \dots, b_\ell]$ is integral over A. Then each $b_1, \dots, b_\ell$ is integral over A; so, by Corollary 6.0.7, we have that B is a finitely generated A-module.

($\impliedby$) If $b \in B$ then by Proposition 6.0.5 we get that b is integral over A. So B is integral over A. ☐ Remark 6.0.11

Corollary 6.0.12 (5.4)**.** *Suppose $A \subseteq B \subseteq C$ are rings with B integral over A and C integral over B. Then C is integral over A.*

Proof. Suppose $c \in C$. Then c is integral over B, so

$$c^n + b_{n-1} c^{n-1} + \cdots + b_1 c + b_0 = 0$$

for some $n > 0$ and some $b_0, \dots, b_{n-1} \in B$. Then c is integral over $A[b_0, \dots, b_{n-1}]$, and $A[b_0, \dots, b_{n-1}, c]$ is a finite $A[b_0, \dots, b_{n-1}]$-algebra. But $A[b_0, \dots, b_{n-1}]$ is a finitely generated and integral extension of A; so $A[b_0, \dots, b_{n-1}]$ is a finite A-algebra, and $A[b_0, \dots, b_{n-1}, c]$ is a finite A-algebra. So c is integral over A. ☐ Corollary 6.0.12

Corollary 6.0.13 (5.5)**.** *Integral closures are integrally closed; i.e. if $A \subseteq B$ are rings and C is the integral closure of A in B (i.e. $C = \{ b \in B : b \text{ is integral over } A \}$), then C is integrally closed in B.*

Proof. Suppose $b \in B$ is integral over C. Then $C[b]$ is integral over C, and C is integral over A; hence, by Corollary 6.0.12, we get that $C[b]$ is integral over A. So b is integral over A; so $b \in C$. ☐ Corollary 6.0.13

Proposition 6.0.14 (5.6)**.** *Suppose B is an integral extension of A. Then:*

1. *Integrality is preserved by quotients; i.e. if $J \subseteq B$ is an ideal, then B/J is an integral extension of $A/J \cap A$.*
2. *Integrality is preserved by localization: if $S \subseteq A$ is a multiplicatively closed set, then $S^{-1}B$ is an integral extension of $S^{-1}A$.*

Proof.

1. Consider $\pi\colon A \to B/J$ the composition of $A \xrightarrow{\subseteq} B \to B/J$; then $\ker(\pi) = A \cap J$, so π induces an embedding $A/A \cap J \hookrightarrow B/J$. Suppose $\overline{b} \in B/J$, where $b \in B$. Then b is integral over A; so

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

for some $n > 0$ and some $a_0, \ldots, a_{n-1} \in A$. Thus

$$(\overline{b})^n + \overline{a_{n-1}}(\overline{b})^{n-1} + \cdots + \overline{a_1}\overline{b} + \overline{a_0} = 0$$

in B/J, and $\overline{a_i} \in A/J \cap I$. So $\overline{b}$ is integral over $A/J \cap I$.

2. Suppose $\frac{b}{s} \in S^{-1}B$. Then $b \in B$ is integral over A; so

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

for some $n > 0$ and some $a_0, \ldots, a_{n-1} \in A$. Multiplying by $s^{-n} \in S^{-1}A$, we find that

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \frac{a_{n-2}}{s^2}\left(\frac{b}{s}\right)^{n-2} + \cdots + \frac{a_0}{s^n} = 0$$

and each $\frac{a_{n-i}}{s^i} \in S^{-1}A$. So $\frac{b}{s}$ is integral over $S^{-1}A$. □ Proposition 6.0.14

Proposition 6.0.15 (5.8)**.** *Suppose B is integral over A. Suppose $Q \subseteq B$ is prime; let $P = Q \cap A \in \operatorname{Spec}(A)$. Then Q is maximal in B if and only if P is maximal in A.*

Proof. By Proposition 6.0.14, we have $A/P \hookrightarrow B/Q$ is an integral extension of integral domains. Replacing A by A/P and B by B/Q, it suffices to show the following:

Claim 6.0.16. *Suppose A, B are integral domains with B integral over A. Then B is a field if and only if A is a field.*

Proof.

($\Longrightarrow$) Suppose $a \in A$ is non-zero. Let $b = a^{-1} \in B$; then b is integral over A, so we may write

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

Then

$$b^n = -(a_{n-1}b^{n-1} + \cdots + a_1 b + a_0$$

Since B is a field, we may then divide by b^{n-1}; we then get

$$b = -\Big(a_{n-1} + \frac{a_{n-2}}{b} + \cdots + \frac{a_1}{b^{n-2}} + \frac{a_0}{b^{n-2}}\Big)$$

So

$$a^{-1} = b = -\big(a_{n-1} + a_{n-2}a + \cdots + a_1 a^{n-2} + a_0 a^{n-2}\big) \in A$$

So A is a field.

($\Longleftarrow$) Suppose $b \in B$ is non-zero. Then b is integral over A, so we may write

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

Without loss of generality, we may take n to be minimal. Since B is an integral domain, we get that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b = \underbrace{b}_{\neq 0}\underbrace{(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_2 b + a_1)}_{\neq 0 \text{ by minimality of } n} \neq 0$$

Then

$$a_0 = -(b^n + a_{n-1}b^{n-1} + \cdots + a_1) \neq 0$$

So

$$-\left(\frac{b^n}{a_0} + \frac{a_{n-1}}{a_0}b^{n-1} + \cdots + \frac{a_1}{a_0}b\right) = 1$$

and

$$-\left(\frac{b^{n-1}}{a_0} + \frac{a_{n-1}b^{n-2}}{a_0} + \cdots + \frac{a_1}{a_0}\right)b = 1$$

So b has a multiplicative inverse. So B is a field. □ Claim 6.0.16

Lifting, we find that Q is maximal in B if and only if P is maximal in A. □ Proposition 6.0.15

Given an extension $A \subseteq B$, in general we are interested in the question of whether a given prime $P \subseteq A$ is a contraction of a prime in B; i.e. is there a prime $Q \subseteq B$ such that $P = Q \cap A$. In this case we say Q *lies over* P.

Remark 6.0.17.

1. We saw in Proposition 4.2.35 that this has nothing much to do with primality of Q; in particular, we had that P is the contraction of a prime ideal of B if and only if P is the contraction of some ideal of B if and only if $P = PB \cap A$.

2. Such a Q may not exist for the extreme reason that $PB = B$. If $PB \neq B$, there will be always be a prime (indeed, a maximal) $Q \subseteq B$ such that $PB \subseteq Q$; but perhaps $P \subsetneq Q \cap A$.

Theorem 6.0.18 (5.10)**.** *Suppose B is integral over A and $P \subseteq A$ is prime. Then there is a prime $Q \subseteq B$ such that $P = Q \cap A$.*

Proof. Consider the commuting square:

$$\begin{tikzcd} A \arrow[r, hook, "\iota"] \arrow[d, "\alpha"] & B \arrow[d, "\beta"] \\ A_P \arrow[r, hook, "\iota_P"] & B_P \end{tikzcd}$$

where $B_P = S^{-1}B$ (with $S = A \setminus P$), and α and β are the localization maps. Then $B_P \neq 0$; so B_P has a maximal ideal $N \subseteq B_P$. So $Q = \beta^{-1}(N)$ is a prime ideal in B that does not meet S (by Proposition 4.2.31). So Q does not meet $A \setminus P$, and $Q \cap A \subseteq P$. (Note that we haven't used integrality so far. This result, however, is too weak to derive our conclusion; e.g. if $Q = (0)$.)

Now, by the commuting square, we have $Q \cap A = \alpha^{-1}(N \cap A_P)$. By Proposition 6.0.14, we get that B_P is integral over A_P; by Proposition 6.0.15, since $N \subseteq B_P$ is maximal, we get that $N \cap A_P \subseteq A_P$ is maximal. So $N \cap A_P = P \cdot A_P$, and $\alpha^{-1}(N \cap A_P) = P$. So $Q \cap A = P$, as desired. □ Theorem 6.0.18

Suppose now that $B \supseteq A$ an integral extension with a prime $P \subseteq A$ and a prime $Q \subseteq A$ such that $Q \cap A = P$. Suppose $P' \subseteq A$ is a prime with $P' \supseteq P$. Can we find prime $Q' \subseteq B$ with $Q' \cap A = P'$ and $Q' \supseteq Q$?

We can.

Proof. Work in $A/P \hookrightarrow B/Q$; note that this is an integral extension. Then P'/P is prime in A; so, by Theorem 6.0.18, we get a prime $\overline{Q}' \subseteq B/Q$ such that $\overline{Q}' \cap A/P = P'/P$. By the correspondence theorem, we have $\overline{Q}' = Q'/Q$ for some prime $Q' \subseteq Q$ containing Q. We get the following diagram:

$$\begin{tikzcd} A \arrow[r, hook, "\subseteq"] \arrow[d, two heads] & B \arrow[d, two heads] \\ A/P \arrow[r, hook] & B/Q \end{tikzcd}$$

TODO 2. *Relevance?*

Then $Q' \cap A = P'$ since $(Q'/Q) \cap A/P = P'/P$. □

Iterating, we get:

Theorem 6.0.19 (Going-up theorem)**.** *Suppose B is integral over A; suppose $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n \subseteq A$ are prime ideals and for some $m \leq n$ we have prime ideals $Q_1 \subseteq \cdots \subseteq Q_m$ of B with $Q_i \cap A = P_i$ for $i \in \{1, \dots, m\}$. Then there exist prime ideals $Q_{m+1} \subseteq \cdots \subseteq Q_n$ in B containing Q_m such that $Q_j \cap A = P_j$ for $j \in \{m+1, \dots, n\}$.*

Remark 6.0.20. Theorem 6.0.18 is not true if B is simply an integral A-algebra; i.e. if $f\colon A \to B$ is a ring homomorphism that is not necessarily injective. Indeed, we don't necessarily have that $f(P)$ is prime in $f(A)$ if P is prime in A, so we can't apply Theorem 6.0.18 to $f(A) \subseteq B$ to get the desired result. In particular, one notes that the primes that get mapped to a prime ideal in $f(A)$ are exactly those that contain the kernel. So we *do* have that every $P \subseteq A$ containing $\ker(f)$ is the pullback of a prime in Q.

We now turn to a geometric interpretation of Theorem 6.0.18. Suppose $f\colon A \to B$ is a (not necessarily integral) A-algebra. Define $f^*\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ by $Q \mapsto f^{-1}(Q)$.

Proposition 6.0.21. *f^* is continuous.*

Proof. It suffices to check that the preimage of a closed set is closed. Consider a closed set $V(I)$, where $I \subseteq A$ is an ideal; we wish to show that $(f^*)^{-1}(V(I))$ is closed. Let $J = I \cdot B$ be the ideal generated by $f(I)$ in B.

Claim 6.0.22. *$f^*(V(I)) = V(J)$.*

Proof.

($\subseteq$) Suppose $Q \in (f^*)^{-1}(V(I))$; then $f^*(Q) = f^{-1}(Q) \supseteq I$. So $Q \supseteq Q \cap f(A) = f(f^{-1}(A)) \supseteq f(I)$; so $Q \supseteq J$, and $Q \in V(J)$.

($\supseteq$) Suppose $Q \in \operatorname{Spec}(B)$ has $Q \supseteq J \supseteq f(I)$. Then $f^*(Q) = f^{-1}(Q) \supseteq I$; so $f^*(Q) \in V(I)$, and $Q \in (f^*)^{-1}(V(I))$. □ Claim 6.0.22

□ Proposition 6.0.21

Proposition 6.0.23. *If B is integral over A, then f^* is closed.*

Proof. Suppose $J \subseteq B$ is an ideal; we show that $f^*(V(J))$ is closed in $\operatorname{Spec}(A)$. Let $I = f^{-1}(J)$; then I is an ideal in A.

Claim 6.0.24. *$f^*(V(J)) = V(I)$.*

Proof.

($\subseteq$) Suppose $P \in f^*(V(J))$; say $P = f^*(Q) = f^{-1}(Q)$ for $Q \in V(J)$. Then $Q \supseteq J$, so $P = f^{-1}(Q) \supseteq f^{-1}(J) = I$, and $P \in V(I)$.

($\supseteq$) Suppose $P \in V(I)$; then $P \supseteq I = f^{-1}(J) \supseteq \ker(f)$. We have $f\colon A \to f(A) \cong A/\ker(f)$; so $f(P)$ is prime in $f(A)$ by the correspondence theorem. But B is integral over $f(A)$; so, by Theorem 6.0.18, we get that $f(P) = Q \cap f(A)$ for some $Q \in \operatorname{Spec}(B)$. Then $f^*(Q) = f^{-1}(Q) = f^{-1}(Q \cap f(A)) = f^{-1}(f(P)) = P$ since $P \supseteq \ker(f)$.

Exercise 6.0.25. Since $Q \supseteq J$, we have $Q \in V(J)$.

This is actually false; see homework 5.

So $P \in f^*(V(J))$. □ Claim 6.0.24

□ Proposition 6.0.23

Remark 6.0.26. If in addition we have that f is injective then f^* is surjective; this is precisely Theorem 6.0.18.

What of uniqueness in Theorem 6.0.18? i.e. given an integral extension B of A and a prime P of A, how many primes Q of B satisfy $Q \cap A = P$?

Proposition 6.0.27 (5.9)**.** *Suppose B is an integral extension of A; suppose Q, Q' are prime ideals in B with $Q \subseteq Q'$. If $Q \cap A = Q' \cap A$ then $Q = Q'$.*

Proof. Let $P = Q \cap A = Q' \cap A$. Consider two commuting diagrams:

$$\begin{tikzcd} A \arrow[r, "\iota", "\subseteq"'] \arrow[d, "\alpha"] & B \arrow[d, "\beta"] \\ A_P \arrow[r, "\iota_P", "\subseteq"'] & B_P \end{tikzcd}$$

and

$$\begin{tikzcd} B \arrow[rr, "\pi"] \arrow[d, "\beta"] & & B/Q \arrow[d] \\ B_P \arrow[r, "\pi_P"] & S^{-1}(B/Q) = S^{-1}B/S^{-1}Q = B_P/QB_P \end{tikzcd}$$

where $B_P = S^{-1}B$ with $S = A \setminus P$.

Claim 6.0.28. *$QB_P \cap A_P = PA_P$ (always, not assuming integrality).*

Proof. Consider the exact sequence of A-modules

$$0 \to P \to A \xrightarrow{\pi \circ \iota} B/Q$$

(This is exact because $\ker(\pi \circ \iota) = Q \cap A = P$.) Localizing, we find that

$$0 \to S^{-1}P \to S^{-1}A \to S^{-1}(B/Q)$$

is exact; i.e.

$$0 \to PA_P \to A_P \to B_P/QB_P$$

is exact. So

$$PA_P = \ker((\pi \circ \iota)_P) = \ker(\pi_P \circ \iota_P) = \ker(\pi_P) \cap A_P = QB_P \cap A_P$$

since ι_P is an embedding and since π_P is just the quotient map. $\square$ Claim 6.0.28

Since B is integral over A, Proposition 6.0.14 gives us that B_P is integral over A_P. Observe that PA_P is maximal in A_P. Further note that QB_P is prime in B_P since there is by Proposition 4.2.31 a bijective correspondence between primes in B_P and primes in B that don't meet S, and $Q \cap (A \setminus P) = \emptyset$ since $Q \cap A = P$. So Proposition 6.0.15 yields that QB_P is maximal in B_P. Similarly, we get that $Q'B_P$ is maximal. But $Q \subseteq Q'$, so $QB_P \subseteq Q'B_P$; so $QB_P = Q'B_P$. Since $Q \cap S = Q' \cap S = \emptyset$, Proposition 4.2.31 yields that $Q = Q'$. $\square$ Proposition 6.0.27

Corollary 6.0.29. *Suppose B is Noetherian and is an integral extension of A. Then every prime in A has finitely many primes in B lying above it.*

Proof. Suppose $P \subseteq A$ is a prime ideal; suppose $Q \subseteq B$ is a prime ideal with $Q \cap A = P$.

Claim 6.0.30. *Q is a minimal prime containing PB.*

Proof. If $Q \supseteq Q' \supseteq PB$ with Q' prime, then

$$P = Q \cap A \supseteq Q' \cap A \supseteq PB \cap A \supseteq P$$

So $Q \cap A = Q' \cap A = P$, and by Proposition 6.0.27 we get that $Q = Q'$. $\square$ Claim 6.0.30

Since B is Noetherian, we know that PB is decomposable. So the minimal prime ideals containing PB are the minimal associated prime ideals. (Recall that the associated primes are the radicals of the primary ideals appearing in the primary decomposition of PB.) But there are only finitely many associated prime ideals of PB. ☐ Corollary 6.0.29

Proposition 6.0.31. *Suppose $f\colon A \to B$ is an integral A-algebra and B is Noetherian. Then $f^*\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is a finite-to-one map.*

Proof. Suppose $P \in \operatorname{Spec}(A)$. If $P \not\supseteq \ker(f)$, then $P \notin \operatorname{im}(f^*)$. (Recall that if $P \in \operatorname{im}(f^*)$ then $P = f^*(Q)$, so $P = f^{-1}(Q)$, and $P \supseteq \ker(f)$.) So if $P \not\supseteq \ker(f)$ then $(f^*)^{-1}(P) = \emptyset$.

If on the other hand we have $P \supseteq \ker(f)$ then $f(P)$ is a prime ideal in $f(A)$; then

$$\begin{aligned} f^*(Q) = P &\iff f^{-1}(Q) = P \\ &\iff f^{-1}(Q \cap f(A)) = P \\ &\iff Q \cap f(A) = f(P) \text{ (since both sides contain } \ker(f)) \end{aligned}$$

Hence the points of $(f^*)^{-1}(P)$ are exactly the primes in B that lie above $f(P)$; by the previous corollary, we get that there are only finitely many such primes. ☐ Proposition 6.0.31

Lemma 6.0.32 (Noether's normalization lemma)**.** *Suppose k is an infinite field and A is a finitely generated k-algebra. Then there exist $u_1, \ldots, u_r \in A$ algebraically independent over k (i.e. if $p \in k[x_1, \ldots, x_r]$ has $p(u_1, \ldots, u_r) = 0$ then $p = 0$) such that A is integral over $k[u_1, \ldots, u_r]$.*

Note that $k[u_1, \ldots, u_r]$ is isomorphic to a polynomial ring over k as $u_1, \ldots, u_r$ are algebraically independent; the map will be $k[x_1, \ldots, x_r] \to k[u_1, \ldots, u_r]$ given by $x_i \mapsto u_i$.

Proof. Let $a_1, \ldots, a_n$ generate A as a k-algebra. If we have $a_1, \ldots, a_n$ are algebraically independent, then we're done. Suppose then that $f \in k[x_1, \ldots, x_n]$ is non-zero and satisfies $f(a_1, \ldots, a_n) = 0$; let $d = \deg(f)$ be the *total degree of f* (i.e. with $\deg(x_1^{r_1} \cdots x_n^{r_n}) = r_1 + \cdots + r_n$). Let $f_\ell(x_1, \ldots, x_n)$ be the sum of the monomials in f of degree ℓ; then

$$f = f_0 + f_1 + \cdots + f_d$$

Claim 6.0.33. *There exist $\lambda_1, \ldots, \lambda_{n-1} \in k$ such that $f_d(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$.*

Proof. Well, $f_d(x_1, \ldots, x_{n-1}, 1) \in k[x_1, \ldots, x_{n-1}]$ is non-zero since

$$f_d = \sum_{r_1+\cdots+r_n=d} \gamma_{(r_1,\ldots,r_n)} x_1^{r_1} \cdots x_n^{r_n}$$

and if $(r_1, \ldots, r_n) \neq (r'_1, \ldots, r'_n)$, then $(r_1, \ldots, r_{n-1}) \neq (r'_1, \ldots, r'_{n-1})$ since

$$r_n = d - r_1 - \cdots - r_{n-1}$$

Exercise 6.0.34. If k is an infinite field and $P \in k[x_1, \ldots, x_\ell]$ is non-zero, then P cannot vanish on all of k^ℓ.

So there are $\lambda_1, \ldots, \lambda_{n-1} \in k$ such that $f_d(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. ☐ Claim 6.0.33

For $i \in \{1, \ldots, n-1\}$, let $b_i = a_i - \lambda_i a_n \in A$; then $k[b_1, \ldots, b_{n-1}, a_n] = k[a_1, \ldots, a_n] = A$ since $a_i = b_i + \lambda_i a_n$. But

$$\begin{aligned} 0 &= f(a_1, \ldots, a_n) \\ &= f(b_1 + \lambda_1 a_n, b_2 + \lambda_2 a_n, \ldots, b_{n-1} + \lambda_{n-1} a_n, a_n) \\ &= f_d(b_1 + \lambda_1 a_n, \ldots, b_{n-1} + \lambda_{n-1} a_n, a_n) + f_{d-1}(\cdots) + \cdots \\ &= f_d(\lambda_1, \ldots, \lambda_{n-1}, 1) a_n^d + (\text{lower degree terms in } a_n \text{ with coefficients in } k[b_1, \ldots, b_{n-1}]) \end{aligned}$$

(where the last equality is an exercise). By the claim we have $f_d(\lambda_1, \ldots, \lambda_{n-1}, 1) \in k \setminus \{0\}$, so we may divide it out; hence a_n is integral over $k[b_1, \ldots, b_{n-1}]$. By an induction argument, we may assume $k[b_1, \ldots, b_{n-1}]$ is integral over some $k[u_1, \ldots, u_r]$ which are algebraically independent over k. So A is integral over $k[u_1, \ldots, u_r]$. ☐ Lemma 6.0.32

From Noether's normalization lemma, we get that every *affine scheme of finite type over a field* k (i.e. $\mathrm{Spec}(A)$ where A is a finitely generated k-algebra) si a finite cover of some *affine space* (i.e. the spectrum of a polynomial ring). i.e. we get a surjective, continuous, closed, finite-to-one map $\mathrm{Spec}(A) \to \mathrm{Spec}(k[x_1, \dots, x_r]) = \mathbb{A}^r_k$. Noether's normalization lemma gives us that $k[x_1, \dots, x_r] \subseteq A$ is an integral extension.

Why is $\mathbb{A}^r_k$ called "affine space"? Our intuition is that affine r-space over k is k^r. We will see that when k is algebraically closed, we have that the closed points of $\mathbb{A}^r_k$ form k^r.

Proposition 6.0.35 (7.10)**.** *Suppose k is a field, A is a finitely generated k-algebra, and $m \subseteq A$ is a maximal ideal. Then A/m is a finite algebraic field extension of k.*

Proof. We first note that A/m is an extension of k by π the composition $k \hookrightarrow A \to A/m$; then $\ker(\pi) = m \cap k = (0)$ since $k \setminus \{ 0 \}$ consists entirely of units, and $m \subsetneq A$. So $k \subseteq A/m$, and A/m is a field. Also A/m is a finitely generated k-algebra: if $A = k[a_1, \dots, a_n]$ for some generators $a_1, \dots, a_n \in A$, then $A/m = k[\overline{a_1}, \dots, \overline{a_m}]$, where $\bar{\cdot}$ denotes the image in A/m. So, by Noether's normalization lemma applied to A/m, we have algebraically independent $u_1, \dots, u_r \in A/m$ (where $r \geq 0$) such that $k[u_1, \dots, u_r] \subseteq A/m$ is an integral extension. By Proposition 6.0.15, since Am is a field and integral over $k[u_1, \dots, u_r]$, we get that maximality of (0) in A/m yields maximality of $(0) = (0) \cap k[u_1, \dots, u_r]$ in $k[u_1, \dots, u_r]$, and $k[u_1, \dots, u_r]$ is a field. But u_1 is not invertible in $k[u_1, \dots, u_r]$; so $r = 0$, and $k \subseteq A/m$ is integral, and hence algebraic. It is also a finite extension, since it is finitely generated as a k-algebra. (Recall by Proposition 6.0.5, Corollary 6.0.7 that finitely generated and integral extensions are finite.) ☐ Proposition 6.0.35

Corollary 6.0.36 (Weak Nullstellensatz)**.** *Suppose k is an algebraically closed field and $k[x_1, \dots, x_r]$ is a polynomial ring. Then the maximal ideals are of the form $(x_1 - a_1, x_2 - a_2, \dots, x_r - a_r)$ for some $a_1, \dots, a_r \in k$.*

Proof. First suppose $a_1, \dots, a_r \in k$; we show $(x_1 - a_1, \dots, x_r - a_r)$ is a maximal ideal. Consider the k-algebra homomorphism $\pi \colon k[x_1, \dots, x_r] \to k$ given by $x_i \mapsto a_i$ for $i \in \{ 1, \dots, r \}$. Then $1 \notin \ker(\pi)$ and $(x_1 - a_1, \dots, x_r - a_r) \subseteq \ker(\pi)$; so $1 \notin (x_1 - a_1, \dots, x_r - a_r)$, and $(x_1 - a_1, \dots, x_r - a_r)$ is proper. Using $\bar{\cdot}$ to denote image in $R = k[x_1, \dots, x_r]/(x_1 - a_1, \dots, x_r - a_r)$, we get that

$$\begin{gathered} \overline{x_1} = \overline{a_1} \\ \vdots \\ \overline{x_r} = \overline{a_r} \end{gathered}$$

So $R = k[\overline{x_1}, \dots, \overline{x_r}] = k[a_1, \dots, a_r] = k$ since $a_1, \dots, a_r \in k$. So $k[x_1, \dots, x_r]/(x_1 - a_1, \dots, x_r - a_r)$ is a field, and $(x_1 - a_1, \dots, x_r - a_r)$ is maximal. Note that this direction did not require algebraic closure.

Now, suppose $m \subseteq k[x_1, \dots, x_r]$ is maximal. Then $k \subseteq k[x_1, \dots, x_r]/m$ is a finite algebraic extension by Proposition 6.0.35. Since k is algebraically closed, we get that $k = k[x_1, \dots, x_r]/m$. Consider the k-algebra homomorphism $\pi \colon k[x_1, \dots, x_r] \to k[x_1, \dots, x_r]/m = k$. Let $a_i = \pi(x_i)$ for $i \in \{ 1, \dots, r \}$; then $a_1, \dots, a_r \in k$. Then

$$\pi(x_i - a_i) = \pi(x_i) - \pi(a_i) = \pi(x_i) - a_i = a_i - a_i = 0$$

So $(x_1 - a_1, \dots, x_r - a_r) \subseteq \ker(\pi) = m$. But $(x_1 - a_1, \dots, x_r - a_r)$ is maximal by the previous part of the proof. So $(x_1 - a_1, \dots, x_r - a_r) = m$. ☐ Corollary 6.0.36

Example 6.0.37. $(x^2 + 1)$ is maximal in $\mathbb{Q}[x]$ but is not of the above form.

We now give a geometric interpretation of the above.

Definition 6.0.38. A point p in a topological space T is *closed* if $\{ p \}$ is a closed set.

Remark 6.0.39. In $\mathrm{Spec}(A)$, the closed points are precisely the maximal ideals.

Proof. Suppose $m \subseteq A$ is maximal. Then $\{ m \} = V(m)$. Conversely, if $P \in \mathrm{Spec}(A)$ is closed, then $P = V(I)$ for some ideal I; so if $Q \supseteq P$ is prime, then $Q \in V(I) = \{ P \}$, and $Q = P$. So P is maximal. ☐ Remark 6.0.39

Corollary 6.0.40. *Suppose k is an algebraically closed field. Then there is a bijective correspondence between k^n and the set of closed points in* $\mathrm{Spec}(k[x_1, \dots, x_n]) = \mathbb{A}^n_k$

Proof. Given $(a_1, \ldots, a_n) \in k^n$, we get a maximal ideal $F(a_1, \ldots, a_n) = (x_1 - a_1, \ldots, x_n - a_n)$, which is then a closed point. By the weak Nullstellensatz we get that F is surjective. To see that F is injective, note that if $F(a_1, \ldots, a_n) = F(b_1, \ldots, b_n)$, then $(x_1 - a_1, \ldots, x_n - a_n) = m = (x_1 - b_1, \ldots, x_n - b_n)$. Then $\overline{x_i} = \overline{a_i} = a_i$ and $\overline{x_i} = \overline{b_i} = b_i$ (since k embeds into $k[x_1, \ldots, x_n]/m$); so $a_i = b_i$, and F is a bijection. □ Corollary 6.0.40

Another formulation of the weak Nullstellensatz, which justifies the name, is the following:

Corollary 6.0.41. *Suppose k is an algebraically closed field; suppose $I \subseteq k[x_1, \ldots, x_n]$ is an ideal. Let $Z(I) = \{ (a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0$ for all $f \in I \}$. Then $Z(I) \neq \emptyset$ if and only if I is proper.*

Proof.

($\Longrightarrow$) It is easily seen that if $1 \in I$ then $Z(I) = \emptyset$.

($\Longleftarrow$) Suppose I is proper; then there is a maximal ideal m containing I. Then by the weak Nullstellensatz, we get that $m = (x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in k$. But then $(a_1, \ldots, a_n) \in Z(m)$ since if $g = (x_1 - a_1)f_1 + \cdots + (x_n - a_n)f_n$ then

$$g(a_1, \ldots, a_n) = (a_1 - a_1)f_1(a_1, \ldots, a_n) + \cdots + (a_n - a_n)f_n(a_1, \ldots, a_n) = 0$$

But $I \subseteq m$; so $Z(m) \subseteq Z(I)$, and $(a_1, \ldots, a_n) \in Z(I)$. So $Z(I) \neq \emptyset$. □ Corollary 6.0.41

Definition 6.0.42. Suppose k is a field. An *algebraic subset of k^n* is a subset of the form $Z(I)$ for some ideal I of $k[x_1, \ldots, x_n]$.

Remark 6.0.43.

1. One can instead consider $Z(X)$ for any subset $X \subseteq k[x_1, \ldots, x_n]$; however, it is easily seen that $Z(X) = Z(I)$ where $I = (X)$. In particular, by Hilbert's basis theorem, we get that any algebraic set is of the form $Z(\{ f_1, \ldots, f_\ell \})$ for some $f_1, \ldots, f_\ell$; we simply take $f_1, \ldots, f_\ell$ to be the generators of $I = (X)$.

2. The algebraic subsets of k^n are the closed sets of a topology on k^n, called the *Zariski topology.*

3. We compare $V(I)$ and $Z(I)$. We have $V(I)$ is a Zariski-closed subset of $\mathrm{Spec}(k[x_1, \ldots, x_n])$; this approach is due to Grothendieck. On the other hand, we have $Z(I)$ is a Zariski-closed subset of k^n; this is the classical approach.

   We may regard $k^n \subseteq \mathrm{Spec}(k[x_1, \ldots, x_n])$; in fact, the Zariski topology on k^n is the induced topology from the Zariski topology on $\mathrm{Spec}(k[x_1, \ldots, x_n])$.

Note that $I \mapsto Z(I)$ is an inclusion-reversing map from ideals in the polynomial ring to algebraic sets. There is a natural map in the other direction: if $Z \subseteq k^n$ is an algebraic set, we define

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

It is easily seen that $I(Z)$ is an ideal of $k[x_1, \ldots, x_n]$. Are these maps mutually inverse? In particular, is $I(Z(I)) = I$ for all ideals I of $k[x_1, \ldots, x_n]$? Clearly we have $I \subseteq I(Z(I))$. Does it hold that $I(Z(I)) \subseteq I$ for all ideals I of $k[x_1, \ldots, x_n]$?

It does not. Suppose $f \in k[x_1, \ldots, x_n]$ has $f^\ell \in I$ for some $\ell > 0$. Then for each $(a_1, \ldots, a_n) \in Z(I)$, we have

$$0 = f^\ell(a_1, \ldots, a_n) = (f(a_1, \ldots, a_\ell))^\ell$$

But $f(a_1, \ldots, a_\ell) \in k$; so $f(a_1, \ldots, a_\ell) = 0$ for all $(a_1, \ldots, a_\ell) \in Z(I)$. So $f \in I$. In particular, we get

$$I \subseteq r(I) \subseteq I(Z(I))$$

So for I not radical, we get $I \subsetneqq r(I) \subseteq I(Z(I))$, and $I \neq I(Z(I))$.

The full Nullstellensatz says that this is the only obstacle.

Theorem 6.0.44 (Hilbert's Nullstellensatz)**.** *Suppose k is an algebraically closed field; suppose $I \subseteq k[x_1, \dots, x_n]$ is an ideal. Then $I(V(I)) = r(I)$.*

Remark 6.0.45. We can recover the corollary to weak Nullstellensatz from Hilbert's Nullstellensatz since if I is a proper ideal of $k[x_1, \dots, x_n]$ then so is $r(I)$; hence $I(Z(I)) = r(I) \neq k[x_1, \dots, x_n]$, and thus $Z(I) \neq \emptyset$. (Vacuously we get that $I(\emptyset) = k[x_1, \dots, x_n]$.)

Hence we get the classical algebro-geometric correspondence mapping an ideal $I \subseteq k[x_1, \dots, x_n]$ to $Z(I) = \{ (a_1, \dots, a_n) \in k^n : f(a_1, \dots, a_n) = 0 \text{ for all } f \in \}$.

Remark 6.0.46. $Z(I) = Z(r(I))$. (Recall that we had a similar fact about $V(I) \subseteq \operatorname{Spec}(A)$.)

Proof.

($\subseteq$) Last time we saw that $r(I) \subseteq I(Z(I))$; hence $Z(I) \subseteq Z(I(Z(I))) \subseteq Z(r(I))$.

($\supseteq$) Since $I \subseteq r(I)$, we get that $Z(r(I)) \subseteq Z(I)$. ☐ Remark 6.0.46

Proof of Theorem 6.0.44. We just saw that $r(I) \subseteq I(Z(r(I))) = I(Z(I))$. For the other direction, given $f \notin r(I)$, we wish to find a point in $Z(I)$ on which f does not vanish. Since $f \notin r(I)$, we get a prime ideal $P \supseteq I$ with $f \notin P$; let $\overline{f}$ denote the image of f in $A = k[x_1, \dots, x_n]/P$. Then since $f \notin P$ we get that $\overline{f} \neq 0$, and $A_{\overline{f}} \neq 0$; since A is an integral domain (as P is prime), we get that $A \subseteq A_{\overline{f}}$. (Recall $A_{\overline{f}} = S^{-1}A$ where $S = \{ 1, \overline{f}, (\overline{f})^2, \dots \}$.)

Note that $\frac{1}{\overline{f}} \in A_{\overline{f}}$; so $A\left[\frac{1}{\overline{f}}\right] \subseteq A_{\overline{f}}$. But every element of $A_{\overline{f}}$ is of the form $\frac{a}{(\overline{f})^\ell}$ for some $a \in A$ and $\ell \geq 0$. So $A\left[\frac{1}{\overline{f}}\right] = A_{\overline{f}}$, and $A_{\overline{f}} = k\left[\overline{x_1}, \dots, \overline{x_n}, \frac{1}{\overline{f}}\right]$ is a finitely generated k-algebra.

Now, let $m \subseteq A_{\overline{f}}$ be a maximal ideal; then by Proposition 6.0.35 we get that $A_{\overline{f}}/m$ is a finite algebraic extension of k. But k is algebraically closed; so $A_{\overline{f}}/m = k$. Let $\pi \colon k[x_1, \dots, x_n] \to k$ be the corresponding k-algebra homomorphism. Let $a_i = \pi(x_i)$ for $i \in \{ 1, \dots, n \}$; then $(a_1, \dots, a_n) \in k^n$.

Note that for $g \in I$ we have $g(a_1, \dots, a_n) = g(\pi(x_1), \dots, \pi(x_n)) = \pi(g(x_1, \dots, x_n)) = 0$ since $g \in I \subseteq P$ and π factors through $k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]/P$. So $(a_1, \dots, a_n) \in Z(I)$. We also get that

$$f(a_1, \dots, a_n) = f(\pi(x_1), \dots, \pi(x_n)) = \pi(f(x_1, \dots, x_n)) = \pi(f) \neq 0$$

Since $\overline{f}$ is invertible in $A_{\overline{f}}$, we have that $\overline{f} \notin m$; so $\pi(f) = \overline{f} + m \neq 0$ in $A_{\overline{f}}/m$. So f does not vanish on $Z(I)$. So $I(Z(I)) \subseteq r(I)$, and $I(Z(I)) = r(I)$. ☐ Theorem 6.0.44

Corollary 6.0.47. *Suppose k is an algebraically closed field. Then there is an inclusion-reversing bijective correspondence between radical ideals of $k[x_1, \dots, x_n]$ and algebraic subsets of k^n given by I and Z.*

Proof. Note that $I(Z)$ is radical: if f^ℓ vanishes on Z then so does f. So the codomains are correct. It is clear that the maps are inclusion-reversing. It remains to show that they are mutually inverse. By Hilbert's Nullstellensatz, we get that $I(Z(I)) = r(I) = I$ since I is radical. For the other direction, note that if $Z \subseteq k^n$ is algebraic, then $Z = Z(J)$ for some ideal $J \subseteq k[x_1, \dots, x_n]$; then by Hilbert's Nullstellensatz

$$Z(I(Z)) = Z(I(Z(J))) = Z(r(J)) = Z(J) = Z$$

So Z and I are mutually inverse. ☐ Corollary 6.0.47

7 Tidbits

7.1 Integrally closed domains (Chapter 5)

Definition 7.1.1. An integral domain A is *integrally closed* if it is integrally closed in $\operatorname{Frac}(A)$; i.e. if

$$\{ r \in \operatorname{Frac}(A) : r \text{ is integral over } A \} = A$$

Example 7.1.2. As previously noted, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$; so $\mathbb{Z}$ is an integrally closed domain. **Warning:** $\mathbb{Z}$ is *not* integrally closed in, for example, $\mathbb{C}$.

Example 7.1.3. As remarked in the homework, the proof that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$ shows that any UFD is integrally closed. In particular, $\mathbb{Z}[x_1, \ldots, x_n]$ and $k[x_1, \ldots, x_n]$ for k a field are integrally closed.

Proposition 7.1.4 (5.12). *Localization preserves integral closures. i.e. suppose $A \subseteq B$ are rings and C is the integral closure of A in B; suppose $S \subseteq A$ is multiplicatively closed. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. We saw in Proposition 6.0.14 that localization preserves integrality; hence since C is integral over A we get that $S^{-1}C$ is integral over $S^{-1}A$. Suppose now that $\frac{b}{s} \in S^{-1}B$ is integral over $S^{-1}A$. Then we have $n > 0$, $a_0, \ldots, a_{n-1} \in A$, and $s_0, \ldots, s_{n-1} \in S$ such that

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_1}{s_1}\frac{b}{s} + \frac{a_0}{s_0} = 0$$

Let $t = s_0 \cdots s_{n-1}$; multiplying both sides by $(st)^n$, we find that

$$(bt)^n + \frac{a_{n-1}st}{s_{n-1}}(bt)^{n-1} + \cdots + \frac{a_1 s^{n-1}t^{n-1}}{s_1}(bt) + \frac{a_0 s^n t^n}{s_0} = 0$$

But each $\frac{a_i s^{n-i} t^{n-i}}{s_i} \in A$ since $s_i \mid t$; so $bt \in B$ is integral over A. So $bt \in C$. So in $S^{-1}B$, we get that $\frac{b}{s} = \frac{1}{st}(bt) \in S^{-1}C$ (since $t \in S$).

So $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$. □ Proposition 7.1.4

Proposition 7.1.5 (5.13). *Being integrally closed is a local property; i.e. if A is an integral domain, then the following are equivalent:*

1. *A is integrally closed.*
2. *A_P is integrally closed for all primes $P \subseteq A$.*
3. *A_m is integrally closed for all maximal ideals $m \subseteq A$.*

Proof.

(1) $\Longrightarrow$ (2) In general if C is the integral closure of A in $k = \operatorname{Frac}(A)$ and $P \subseteq A$ is prime then $C_P = S^{-1}C$ (with $S = A \setminus P$); hence by Proposition 7.1.4 we get that C_P is the integral closure of A_P in $k_P = k = \operatorname{Frac}(A_P)$ (since $A \subseteq A_P \subseteq k = \operatorname{Frac}(A)$). By hypothesis we get that $A = C$, and thus $A_P = C_P$; hence A_P is integrally closed in $\operatorname{Frac}(A_P) = k$. So A_P is integrally closed.

(2) $\Longrightarrow$ (3) Clear. □ Proposition 7.1.5

(3) $\Longrightarrow$ (1) Let $K = \operatorname{Frac}(A)$; let C be the integral closure of A in K. Suppose $m \subseteq A$ is maximal; then $A_m \subseteq C_m \subseteq K_m = K$. By Proposition 7.1.4, we get that C_m is the integral closure of A_m in K. But A_m is integrally closed by hypothesis; so $A_m = C_m$. So for all maximal ideals m of A we have $\iota_m \colon A_m \to C_m$ is surjective. But by Proposition 4.2.23 we have that surjectivity is local; so $\iota \colon A \to C$ is surjective, and $A = C$ is integrally closed.

One important source of integrally closed domains is DVRs

Definition 7.1.6. Suppose k is a field. A *discrete valuation* on k is a surjective $v \colon k^* \to \mathbb{Z}$ satisfying

1. v is a grape homomorphism $(k^*, \cdot) \to (\mathbb{Z}, +)$.
2. $v(x + y) \geq \min\{\, v(x), v(y) \,\}$ for all $x, y \in k^*$ with $x + y \neq 0$.

(If we set $v(0) = \infty$ with the usual conventions for arithmetic on the extended reals, then the above two properties hold on all of k.) The *valuation ring* is $\mathcal{O}_v = \{\, a \in k : v(a) \geq 0 \,\}$; the *maximal ideal* is $m_v = \{\, a \in k : v(a) > 0 \,\}$.

Example 7.1.7. Let $k = \mathbb{Q}$; suppose p is prime. Consider $v\colon \mathbb{Q}^* \to \mathbb{Z}$ given by $p^\ell \frac{n}{m} \mapsto \ell$ (where $n, m \notin p\mathbb{Z}$); this is the *p-adic valuation*. Then

$$\mathcal{O}_v = \left\{ \frac{n}{m} : p \nmid m \right\} = \mathbb{Z}_{(p)}$$

and

$$m_v = \left\{ \frac{n}{m} : p \nmid m, p \mid n \right\} = p\mathbb{Z}_{(p)}$$

Example 7.1.8. Suppose k is a field; let $K = k(x) = \mathrm{Frac}(k[x])$. Fix an irreducible $f \in k[x]$; we then define $v\colon k(x)^* \to \mathbb{Z}$ by $f^\ell \frac{g}{h} \mapsto \ell$ as above. This is the *f-adic valuation*. We then get $\mathcal{O}_v = k[x]_{(f)}$ and $m_v = fk[x]_{(f)}$.

Proposition 7.1.9. *Suppose $v\colon K^* \to \mathbb{Z}$ is a discrete valuation.*

1. *If $x \in K^*$ then either $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$.*
2. *$\mathcal{O}_v$ is a local ring and m_v is its maximal ideal.*
3. *m_v is principal.*
4. *Every non-zero ideal of $\mathcal{O}_v$ is of the form m_v^k for some $k \geq 0$. In particular, we get that $\mathcal{O}_v$ is a PID.*
5. *$\mathcal{O}_v$ is integrally closed.*

Proof.

1. Note that
$$x \in \mathcal{O}_v \iff v(x) \geq 0 \iff v(x^{-1}) = -v(x) \leq 0 \iff x^{-1} \notin \mathcal{O}_v$$
2. To see that $\mathcal{O}_v$ is a ring, one notes that for $x, y \in \mathcal{O}_v$ we have
$$\begin{aligned} v(x+y) &\geq \min\{ v(x), v(y) \} \\ &\geq 0 \\ v(xy) &= v(x) + v(y) \\ &\geq 0 \\ v(1) &= 0 \\ &\geq 0 \\ v(-1) &= 0 \\ &\leq 0 \end{aligned}$$
A similar proof shows that m_v is an ideal. To check that m_v is maximal, one simply checks that $\mathcal{O}_v/m_v$ is a field.
3. Since $v\colon K^* \to \mathbb{Z}$ is surjective, there is $x \in K^*$ such that $v(x) = 1$. Suppose now that $y \in m_v$; then $\frac{y}{x} \in K$, and $v\left(\frac{y}{x}\right) = v(y) - v(x) = v(y) - 1 \geq 0$ since $v(y) > 0$. So $y = \frac{y}{x} \cdot x$, and $m_v = (x)$.
4. For $k \geq 0$ we let $m_k = \{ y \in \mathcal{O}_v : v(y) \geq k \}$.

   Claim 7.1.10. *The only non-zero ideals of $\mathcal{O}_v$ are the m_k.*

   Proof. Suppose I is a non-zero ideal of $\mathcal{O}_v$. Let $k \geq 0$ be minimal such that there is $a \in I$ with $v(a) = k$; then $a \neq 0$. By minimality of k, we have $I \subseteq m_k$. Conversely, suppose $y \in m_k$. Then $\frac{y}{a} \in K$, and $v\left(\frac{y}{a}\right) = v(y) - k \geq 0$; so $\frac{y}{a} \in \mathcal{O}_v$, and $y = \frac{y}{a} a \in I$. $\square$ Claim 7.1.10

   By the previous part, we get that $m_v = (x)$ where $v(x) = 1$.

   Claim 7.1.11. $m_k = m_v^k = (x^k)$.

   Proof.

(⊆) Suppose $y \in m_k$; then $\frac{y}{x^n} \in K$ has $v\left(\frac{y}{x^n}\right) = v(y) - k \geq 0$. So $\frac{y}{x^k} \in \mathcal{O}_v$, and $y \in (x^k)$.

(⊇) Clear since $v(x^k) = kv(x) = k$. ☐ Claim 7.1.11

The two claims yield the desired result.

5. Well, $\mathcal{O}_v$ is an integral domain as a subring of a field. By Item 1 we get that $\mathrm{Frac}(\mathcal{O}_v) = K$; it then suffices to show that $\mathcal{O}_v$ is integrally closed in K. Suppose $b \in K$ is integral over $\mathcal{O}_v$; say

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

for some $a_{n-1}, \ldots, a_0 \in \mathcal{O}_v$. If we had $b \notin \mathcal{O}_v$, then $b^{-1} \in \mathcal{O}_v$; so, multiplying by b^{1-n}, we get that

$$b + \underbrace{a_{n-1} + a_{n-2}b^{-1} + \cdots + a_0 b^{1-n}}_{\in \mathcal{O}_v} = 0$$

So $b \in \mathcal{O}_v$, a contradiction. So $b \in \mathcal{O}_v$. ☐ Proposition 7.1.9

Lemma 7.1.12 (Chapter 9)**.** *Suppose A is a local Noetherian integral domain in which every non-zero ideal is a power of the maximal ideal. Then A is a DVR or a field.*

Proof. Let $m \subseteq A$ be the maximal ideal; suppose A is not a field.

Claim 7.1.13. *$m^2 \neq m$.*

Proof. Suppose for contradiction that $m \cdot m = m$. But $m = J(A)$, and since A is Noetherian we have that m is finitely generated; so, by Nakayama's lemma, we get that $m = 0$, contradicting our assumption that A is not a field. ☐ Claim 7.1.13

We may thus let $x \in m \setminus m^2$. Then by hypothesis we have $(x) = m^k$ for some $k \geq 0$. But if $k \geq 2$ then $m^k \subseteq m^2$; thus, since $x \notin m^2$, we get that $(x) = m$. So each $m^k = (x^k)$. Define $v \colon A \setminus \{0\} \to \mathbb{Z}$ by sending a to the unique k such that $(a) = (x^k) = m^k$; we then extend v to $\mathrm{Frac}(A)^*$ by setting

$$v\left(\frac{a}{b}\right) \mapsto v(a) - v(b)$$

One checks that v is a discrete valuation with $A = \mathcal{O}_v$. So A is a discrete valuation ring. ☐ Lemma 7.1.12

In the study of Noetherian integral domains, the simplest case we come across are those of dimension 0: Noetherian integral domains A for which there do not exist prime ideals $P \subsetneqq Q$. Since (0) is prime, this is equivalent to A being a field.

The next case are those of dimension 1: Noetherian integral domains A such that there does not exist prime ideals $P_0 \subsetneqq P_1 \subsetneqq P_2$. Since (0) is prime, this is equivalent to requiring that every non-zero prime ideal is maximal. We focus on this case.

Lemma 7.1.14. *Suppose $A \subseteq B$ are integral domains. Suppose A is of dimension 1 and B is integral over A. Then B is of dimension 1.*

Proof. A is not a field; so, by Proposition 6.0.15 we get that B is not a field. Suppose $Q \subseteq B$ is a prime ideal.

Case 1. Suppose $Q \cap A = 0$. Then $(0) \subseteq Q$ are prime ideals in B, and both (0) and Q lie above (0) in A. So Proposition 6.0.27 yields that $(0) = Q$.

Case 2. Suppose $Q \cap A = P \neq (0)$. Since A is of dimension 1, we get that P is maximal; so, by Proposition 6.0.15, we get that Q is maximal.

So every non-zero prime ideal is maximal; so B is of dimension 1. ☐ Lemma 7.1.14

Example 7.1.15 (Plane curves). Suppose k is a field; suppose $f \in k[x, y]$ is non-zero and irreducible. Then $k[x, y]/(f)$ is a Noetherian integral domain of dimension 1.

Proof. Let $A = k[x, y]/(f)$; then A is a finitely-generated k-algebra, and is thus Noetherian, by Hilbert's basis theorem. Since (f) is prime, we get that A is an integral domain. Let $K = \mathrm{Frac}(A) = k(\overline{x}, \overline{y})$ where $\overline{x} = x + (f) \in A$ and $\overline{y} = y + (f) \in A$. Since $f(\overline{x}, \overline{y}) = \overline{f(x, y)} = 0$ in A, we have that $\{\,\overline{x}, \overline{y}\,\}$ is algebraically dependent; so $\mathrm{trdeg}(K/k) \leq 1$. One checks then that $\mathrm{trdeg}(K/k) = 1$. By Noether's normalization lemma, we get that A is integral over $k[a_1, \ldots, a_n]$ where $a_1, \ldots, a_n \in A$ are algebraically independent over k; by the above, we get that $n = 1$, and A is integral over a polynomial ring in one variable. But such rings are PIDs, and are thus of dimension 1; hence, by Lemma 7.1.14, we get that A is of dimension 1. ☐

Example 7.1.16 (Rings of integers). Suppose K is a finite algebraic extension of $\mathbb{Q}$. (Such fields are called *number fields*.) Let A be the integral closure of $\mathbb{Z}$ in K; this is called the *ring of integers in* K. Then A is a Noetherian integral domain of dimension 1.

Proof. That A is of dimension 1 follows by Lemma 7.1.14; that A is an integral follows as it is a subring of a field. To see that A is Noetherian needs work; this is 5.17 in the book. ☐

Theorem 7.1.17 (9.3)**.** *Suppose A is a Noetherian integral domain of dimension 1. Then the following are equivalent:*

1. *A is integrally closed.*
2. *For every non-zero $P \in \mathrm{Spec}(A)$ we have A_P is a DVR.*
3. *Every primary ideal of A is a power of a prime ideal.*

Proof.

(2) $\Longrightarrow$ (1) DVRs are integrally closed; so every localization at a non-zero prime is integrally closed. But being integrally closed is a local property; so A is integrally closed.

(Note that this direction only required that A be an integral domain.)

(2) $\Longrightarrow$ (3) Suppose $Q \subseteq A$ is P-primary, so $P = r(Q)$ is prime in A. We will show that Q is a power of P. If $Q = (0)$, we're done; assume then that $Q \neq 0$. So $P \neq 0$; so, since A is of dimension 1, we get that P is maximal. In the localization, we have $QA_P \subseteq PA_P$. But A_P is a DVR; so every ideal is a power of PA_P (the maximal ideal). So $QA_P = (PA_P)^k = P^k A_P$. (One checks this last equality; it essentially says that localization is compatible with taking powers of primes.) Note that in A, both Q and P^k are primary ideals in P (by hypothesis and since P is maximal, respectively). By question 4 on homework 4, we have that primary ideals in A_P correspond bijectively to primary ideals of A contained in P. So $QA_P = P^k A_P$ implies that $Q = P^k$.

(3) $\Longrightarrow$ (2) Suppose $P \subseteq A$ is a non-zero prime. Note that since A is of dimension 1 we get that A_P is as well; so PA_P is the only non-zero prime ideal. Suppose now that I is a proper, non-zero ideal of A_P; then $r(I)$ is a non-zero prime, and thus $r(I) = PA_P$. So, by Proposition 5.0.16, we get that A_P; by question 4 on homework 4, we get that $I \cap A$ is primary in A. So, since $I \cap A \subseteq P$, the hypothesis and dimension 1 yield that $I \cap A = P^k$ for some $k > 0$. So $I = P^k A_P = (PA_P)^k$.

So every non-zero ideal of A_P is a power of the maximal ideal. By Lemma 7.1.12, we get that A_P is a DVR.

(1) $\Longrightarrow$ (2) Suppose $P \subseteq A$ is a non-zero prime ideal; we show that A_P is a DVR. Let $R = A_P$; let $m = PA_P$. Since A is integrally closed, we get that R is as well. But R is of dimension 1; so m is the only non-zero prime ideal of R. Suppose $a \in m$ is non-zero; then

$$r((a)) = \bigcap V(a) = m$$

By Noetherianity and Proposition 5.1.16, we get that $m^k \subseteq (a)$ for some $k \geq 0$; choose a least such k, so $m^k \subseteq (a)$ but $m^{k-1} \not\subseteq (a)$. Suppose $b \in m^{k-1} \setminus (a)$; consider

$$\alpha = \frac{b}{a} \in K = \mathrm{Frac}(R)$$

Note that $\alpha m \subseteq R$: indeed, if $x \in m$ then $\alpha x = \frac{bx}{a}$ with $b \in m^{k-1}$; so $bx \in m^k \subseteq (a)$, so $a \mid bx$ in R, and $\frac{bx}{a} \in R$. We further note that αm is an ideal in R.

Claim 7.1.18. *$\alpha m = R$.*

Proof. If not, we would have $\alpha m \subseteq m$. Consider $\varphi\colon m \to m$ given by $x \mapsto \alpha x$. Then since m is a finitely-generated R-module (by Noetherianity) and φ is R-linear, generalized Cayley-Hamilton (i.e. linear algebra; see proof of Proposition 6.0.5) yields that α is integral over R. But R is integrally closed and $\alpha \in \mathrm{Frac}(R) = K$; so $\alpha \in R$. So $a \mid b$ in R, contradicting our assumption that $b \notin (a)$. □ Claim 7.1.18

Claim 7.1.19. *m is principal.*

Proof. By the previous claim, we get that $1 \in \alpha m = \frac{b}{a}m$; so $\alpha^{-1} = \frac{a}{b} \in m \subseteq R$. So $\left(\frac{a}{b}\right) \subseteq m$. Conversely, if $x \in m$ then

$$x = \alpha\alpha^{-1}x = \frac{a}{b}\underbrace{\alpha x}_{\in \alpha m \subseteq R} \in \left(\frac{a}{b}\right)$$

So $m = \left(\frac{a}{b}\right)$. □ Claim 7.1.19

Claim 7.1.20. *Every non-zero ideal of R is a power of m; hence R is a DVR.*

Proof. Suppose I is a non-zero ideal of R. Suppose I is proper; then $I \subseteq m$, and $r(I) = m$ since R is of dimension 1. By Noetherianity we get that $m^k \subseteq I$ for some k. If $I \subseteq m^k$, then $I = m^k$, and we're done. Suppose then that $I \not\subseteq m^k$; choose a least ℓ such that $I \not\subseteq m^\ell$. By the previous claim we may write $m = (x)$. Then $I \subseteq (x^{\ell-1})$ but $I \not\subseteq (x^\ell)$. So there is $y \in I$ such that $y \notin (x^\ell)$ but $y = ax^{\ell-1}$ for some $a \in R$. So $a \notin (x) = m$; so $a \in R^\times$, and $x^{\ell-1} = a^{-1}y \in I$. So $m^{\ell-1} = (x^{\ell-1}) \subseteq I$; so $I = (x^{\ell-1}) = m^{\ell-1}$. □ Claim 7.1.20

So R is a DVR. □ Theorem 7.1.17

Definition 7.1.21. A *Dedekind domain* is a Noetherian integral domain of dimension 1 such that any of the three conditions of Theorem 7.1.17 hold.

Corollary 7.1.22. *In a Dedekind domain A every proper ideal has a factorization as a product of prime ideals.*

Proof. Suppose I is a proper ideal. If $I = (0)$ then I is prime; assume then that $I \neq (0)$. Take an irredundant primary decomposition

$$I = Q_1 \cap \cdots \cap Q_\ell$$

where the Q_i are P_i-primary (with $P_i = r(Q_i)$) and $P_1, \ldots, P_\ell$ are distinct. By dimension 1 we get that $P_1, \ldots, P_\ell$ are maximal; hence if $i \neq j$ then $P_i + P_j = A$. So

$$r(Q_i + Q_j) = r(r(Q_i) + r(Q_j)) = r(P_i + P_j) = r(A) = A$$

So $Q_i + Q_j = A$. Recall in general that if $I + J = A$ then $I \cap J = IJ$. So

$$I = Q_1 \cdot \cdots \cdot Q_\ell = P_1^{r_1} \cdot P_2^{r_2} \cdot \cdots \cdot P_\ell^{r_\ell}$$

since Q_i is P_i-prime and A is a Dedekind domain implies $Q_i = P_i^k$. □ Corollary 7.1.22

In fact the factorization is unique.

Final exam: Monday April 11, 12:30-15:00, MC 4041. Office hours this week: MW 13:30-15:30, Friday 12:30-14:30, MC 5018. Will cover everything we covered in class except the final week (DVRs, dimension 1, Dedekind domains). The exam format will be content/synthesis (definitions, true or false, short answer, example and counterexample) and a couple of problem-solving questions (problems and proofs). Recall that the exam is 65% of the final grade and the assignments are 35%.