Commutative Algebra

Alex Rutar*
University of Waterloo

Winter 2019†

*arutar@uwaterloo.ca
†Last updated: April 19, 2019

Contents

I. Modules

1 Basic Properties of Modules

In this course, all rings are assumed to be commutative and unitary unless explicitly stated otherwise. Essentially, modules are “vector spaces over arbitrary commutative rings”. Let’s see the definition:

Definition. Suppose A is a (commutative, unitary) ring. Then an A–**module** is an abelian group $(M,+,0)$ with a function $\mu : A\times M \to M$ and, writing $ax := \mu(a,x)$, satisfies for $a,b\in A$, $x,y\in M$

1. $a(x+y)=ax+ay$
2. $(a+b)x=ax+bx$
3. $(ab)x=a(bx)$
4. $1x=x$

In fact, one can re-interpret the axioms as follows.

Axiom 1 says that for fixed $a\in A$, the function $M\to M$ given by $x\mapsto ax$ is a group endomorphism. In this sense, let $\alpha : A\to \mathrm{End}(M)$ be the map taking a to multiplication by a on M: for $x\in M$, $\alpha(x)=\{x\mapsto ax\}$.

Since A is a ring, $\mathrm{End}(M)$ is also a ring under the operations $(f+g)(x)=f(x)+g(x)$ and $(fg)(x)=f(g(x))$ for all $f,g\in\mathrm{End}(M)$, $x\in M$. Naturally, this ring is not necessarily commutative (function composition composition is usually not commutative).

1.1 Proposition. *Let A be an A–module over a group M, and let $\alpha : A\to\mathrm{End}(M)$ be given by $\alpha(x)=ax$. Then α is a unitary ring homomorphism. Furthermore, if $\alpha : A\to\mathrm{End}(M)$ is any unitary ring homomorphism, then α induces a natural A–module structure*

Proof α must respect addition, multiplication, and take units to units. This follows directly from Axioms 2,3,4:

$$\begin{aligned}\alpha(a+b)&=\{x\mapsto(a+b)x\}=\{x\mapsto ax+bx\}=\alpha(a)+\alpha(b)\\ \alpha(ab)&=\{x\mapsto(ab)x\}=\{x\mapsto a(bx)\}=\alpha(a)\circ\alpha(b)\\ \alpha(1)&=\{x\mapsto 1x\}=\{x\mapsto x\}=\mathrm{id}\end{aligned}$$

so α is a unitary ring homomorphism.

Conversely, we can define $\mu : A\times M\to M$ by $ax=\mu(a,x)=\alpha(a)(x)$. But then $a(x+y)=\alpha(a)(x+y)=\alpha(a)(x)+\alpha(a)(y)$ since $\alpha(a)\in\mathrm{End}(M)$. Furthermore, Axioms 2,3,4 follow in the same way as above since α is a unitary ring homomorphism. ■

In this sense, A–modules are precisely given by ring homomorphisms $\alpha : A\to\mathrm{End}(M)$ defining $ax=\alpha(a)(x)$. Thus we have the following natural consequences of the definition of A–modules:

1.2 Proposition. *In any A–module,*

- $a0=0$

- $a(-x) = -(ax)$
- $(-1)x = -x$

Proof This follows directly since α is a unitary ring homomorphism (or can be proven directly from the axioms). ■

Common Examples of Modules

Modules are a general construction, and contain many common algebraic objects as examples.

1. If $A = k$ is a field, then A–modules are k–vector spaces.

2. $A = \mathbb{Z}$, then A–modules are abelian groups with $nx = x + \cdots + x$ for $n \geq 0$. That is to say that the class of $\mathbb{Z}$–modules are the abelian groups.

3. Let A be any ring, $I \subseteq A$ an ideal. Then I is a commutative group (closure under addition) and absorbs A–multiplication, so I is an A–module under A–multiplication. In particular, A is an A–module itself.

4. Suppose k is a field, V is a k–vector space, and $T : V \to V$ is a linear transformation. Let $A = k[x]$ by the polynomial ring in 1 variable over k. Then V (as an additive group) inherits a natural A–module structure.

   Let $p(x) \in k[x]$; then $p(T)$ defined in the natural way is a linear transformation. Then for any $v \in V$, we define $\mu(p, v) = pv = p(T)(v)$. Let's see that this makes V into a $k[x]$–module by verifying the axioms: for $p, q \in k[x]$, $x, y \in V$

   a) $p(x + y) = p(T)(x + y) = p(T)(x) + p(T)(y)$ since $p(T)$ is linear.
   b) $(p + q)(x) = (p(T) + q(T))(x) = p(T)(x) + q(T)(x)$ since p is a polynomial function.
   c) $(pq)(x) = (pq)(T)(x) = (p(T)q(T))(x)$ since $k[x]$ are polynomials over a field (which is a commutative ring).
   d) $1x = \mathrm{id}(T)(x) = \mathrm{id}(x) = x$

   so the axioms are satisfied.

Morphisms, Submodules, Quotients

Definition. If M, N are A–modules, a function $f : M \to N$ is A–**linear** or is an A–**module homomorphism** if it is a group homomorphism commuting with the action of A. That is, for all $x, y \in M$, $a \in A$,

- $f(x + y) = f(x) + f(y)$
- $f(ax) = af(x)$

As usual, f is an **isomorphism** if it is bijective, and write $M \cong N$.

Equivalently, f is an isomorphism of groups that is A–linear (respects the action of A on x).

1. If $A = k$ is a field, then an A–module homomorphism are just the regular linear transformations
2. If $A = \mathbb{Z}$, then A–module homomorphisms are exactly group homomorphisms.

Consider the collection of all A–linear maps $f : M \to N$. This set is itself an A–Module given the following structure: for $f, g \in \mathrm{Hom}_A(M, N)$, then $(f + g)(x) = f(x) + g(x)$, and if $a \in A$, then $(af)(x) = af(x)$.

Definition. The set $\mathrm{Hom}_A(M,N)$ is A–module of all A–linear maps $f : M \to N$.

Here's a basic proposition about this A–module:

1.3 Proposition. *Let M be an A–module and $x \in A$ an arbitrary element. Then $\alpha_x : \mathrm{Hom}_A(A,M) \to M$ given by $\alpha_x(f) = f(x)$ is A–linear. In particular, α_1 is an A–module isomorphism.*

Proof It is straightforward to show that α_x this is A–linear:

$$\begin{aligned} \alpha_x(f+g) &= (f+g)(x) = f(x) + g(x) = \alpha(f) + \alpha(g) \\ \alpha(af) &= (af)(x) = af(x) = a\alpha(f) \end{aligned}$$

Now, set $\alpha = \alpha_1$. To see injectivity, if $\alpha(f) = 0$, then $f(1) = 0$. Then for any $a \in A$,

$$f(a) = f(a \cdot 1) = af(1) = a0 = 0$$

and f is the zero homomorphism. To see surjectivity, let $x \in M$ be arbitrary, and define $f : A \to M$ by $f(a) := ax$. Then $f(a+b) = (a+b)x = ax+bx = f(a)+f(b)$, and $f(ab) = (ab)x = a(bx) = af(b)$, so $f \in \mathrm{Hom}_A(A,M)$. Then $\alpha(f) = f(1) = 1x = x$. ■

Definition. A subgroup $N \leq M$ of an A–module is a **submodule** if for all $a \in A$, $x \in N$, $ax \in N$. These are subgroups closed under the action of A.

Since M is an abelian group, $N \leq M$ is automatically a normal subgroup of M.

As in group thoery, such submodules occur naturally. If $f : M \to N$ is A–linear, then $\ker(f) = \{x \in M : f(x) = 0\}$ is a submodule of M, and $\mathrm{im}(f) = \{f(x) : x \in M\}$ is a submodule of N. Recall that $\mathrm{coker}(f) := N/\mathrm{im}(f)$.

1.4 Proposition. *If $N \leq M$, the **quotient module** $M/N = \{x+N : x \in M\}$ is an A–module over the quotient group with action $a(x+N) = ax+N$. The **quotient map** $\pi : M \to M/N$ given by $x \mapsto x+N$ is A–linear and $\ker(\pi) = N$.*

Proof Let's show that the action is well-defined. Suppose $x+N = y+N$ are the same coset with different representative. Then $x - y \in N$, so $a(x-y) \in N$, so $ax - ay \in N$. Thus $ax + N = ay + N$, so the map is well-defined.

As well, $\pi(x+y) = (x+y)+N = (x+N)+(y+N)$ (from the group structure), and $\pi(ax) = ax+N = a(x+N) = a\pi(x)$, so π is A–linear. Finally, $x \in \ker(\pi)$ iff $\pi(x) = N$ iff $x + N = N$ iff $x \in N$. ■

1.5 Theorem. (Correspondence) *Let N be a submodule of M. There is a bijective correspondence from submodules $M' \subseteq M$ containing N and submodules of M/N given by $M' \mapsto \pi(M')$ and $\tilde{M} \leq M/N \mapsto \pi^{-1}(\tilde{M})$ (the preimage/pullback).*

Proof From the Correspondence Theorem for groups, π and π^{-1} preserve subgroups: it suffices to show they are also closed under the action of A. Since π is A–linear, for any $\pi(x) = x+N \in M'$, since $x \in M'$, $ax \in M'$ and $\pi(ax) = a(x+N) \in M'$ as well. Conversely, for any $x \in \pi^{-1}(\tilde{M})$, $\pi(x) \in \tilde{M}$, so $\pi(ax) = a\pi(x) \in \tilde{M}$ and $ax \in \pi^{-1}(\tilde{M})$. ■

1.6 Proposition. (Universal Property of Quotients) *Suppose $F : M \to N$ is an A–module homomorphism and $M' \leq M$ submodule. If $M' \leq \ker(f)$, then there is a unique A–linear map $\overline{f} : M/M' \to N$ by $x + M' \mapsto f(x)$ such that $\ker(\overline{f}) = \ker(f)/M'$, $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$.*

Proof Since f is also a group homomorphism on an abelian group, M' is automatically a normal subgroup of M. Thus by the universal property of quotients for groups, there is a unique group homomorphism $\overline{f} : M/M' \to N$ defined by $\overline{f}(x+M') = f(x)$. It suffices to show that $\overline{f}$ is A–linear. Since $\overline{f}$ is a group homomorphism, $\overline{f}((x+M')+(y+M')) = \overline{f}(x+M') + \overline{f}(y+M')$, so let $a \in A$ and $x \in M$ be arbitrary. Then

$$\overline{f}(a(x+M')) = \overline{f}(ax+M') = f(ax) = af(x) = a\overline{f}(x+M')$$

since f is A–linear. ■

1.7 Corollary. (First Isomorphism Theorem) *If $f : M \to N$ is an A–linear map, then $M/\ker(f) \cong \operatorname{im}(f)$.*

Proof By the universal property of quotients to $M' = \ker(f)$, get $\overline{f} : M/\ker(f) \to N$, with $\ker(\overline{f}) = 0$ and $\operatorname{im}(\overline{f}) = \operatorname{im}(f)$. Thus $\overline{f}$ is injective with image $\operatorname{im}(f)$, and thus bijective. ■

1.8 Proposition. *The lattice of submodules is a complete lattice.*

Proof Let M be an A–module, N_1, N_2 submodule. One can verify that the subgroup $N_1 + N_2 = \{x + y : x \in N_1, y \in N_2\}$ is the smallest submodule containing both N_1 and N_2. Similarly, $N_1 \cap N_2$ is the largest submodule of M contained in both N_1 and N_2. ■

2 Operations on Modules

Sums, Products

Definition. Let $(N_i : i \in I)$ be a set of submodules of M. We define the **(internal) sum** of $(N_i : i \in I)$ to be

$$\sum_{i\in I} N_i := \left\{ \sum_{i\in I} a_i : a_i \in N_i, \text{ all but finitely many } a_i = 0 \right\}$$

Note that this is the smallest submodule containing all the N_i. The sum can also be defined externally:

Definition. Suppose $(M_i : i \in I)$ is a sequence of A–modules. The **direct sum** of $(M_i : i \in I)$

$$\bigoplus_{i\in I} M_i := \{(x_i : i \in I) : x_i \in M_i \text{ and for all but finitely many } i, x_i = 0\}$$

The **direct product** of $(M_i : i \in I)$ is

$$\prod_{i\in I} M_i = \{(x_i : i \in I), x_i \in M_i\}$$

The A–module structure on $\prod_{i\in I} M_i$ and $\bigoplus_{i\in I} M_i$ is given by corordinate-wise addition and scalar multiplication.

It is worth noting that $\bigoplus_{i\in I} M_i$ a submodule of $\prod_{i\in I} M_i$.

Remark. Fix $j \in I$ and let $\widetilde{M}_j := \{(x_i : i \in I) : x_i = 0 \text{ if } i \neq j, x_j \in M_j\}$. Then the map $M_j \to \widetilde{M}_j$ given by $x \mapsto (0, \ldots, 0, x, 0, \ldots)$ is an isomorphism, and $\widetilde{M}_j \leq \bigoplus_{i \in I} M_i$ is a submodule. It is clear that $M \cong \sum_{i \in I} \widetilde{M}_i$.

Remark. If X is an A–module, Y, Z submodules, then we write $X = Y \oplus Z$ if

- $Y + Z = X$
- $Y \cap Z = (0)$

In this case, each element $x \in X$ can be written uniquely as $x = y + z$ where $y \in Y$, $z \in Z$, and $\phi : X \to Y \oplus Z$ given by $x \mapsto (y, z)$ is an isomorphism.

Definition. Composing the above map, one has the **projection** map, which is denoted $\text{proj}_j : \oplus_{i \in I} M_i \to M_j$.

Definition. Fix an A–module M and an index set I. Then $M^I := \bigoplus_{i \in I} M$.

If $n < \omega$, then $M^n := \bigoplus_{i=1}^n M$.

Definition. An A–module is **free** if it is isomorphic to A^I for some set I. If $M \cong A^n$ for some $n < \omega$, then we say M is free of **rank** n.

Finitely Generated Modules

Definition. Let M be an A–module, $X \subseteq M$ a subset. The **submodule generated by** X is

$$(X) := \left\{ \sum_{i=1}^n a_i x_i, a_i \in A, x_i \in X \right\}$$

This is the smallest submodule of M that contains the set X. We say that M is **generated** by X if $M = (X)$. Then M is **finitely generated** if $M = (X)$ for some finite $X \subseteq M$.

2.1 Proposition. *M is finitely generated if and only if $M \cong A^n/N$ for some submodule $N \leq A^n$.*

Proof ($\Leftarrow$) $\{(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$ generates A^n as an A–module. Thus $\{(1, 0, \ldots, 0) + N, (0, 1, 0, \ldots, 0) + N, \ldots, (0, \ldots, 0, 1) + N\}$ generates A^n/N.

($\Rightarrow$) Suppose $X = \{x_1, \ldots, x_n\}$ generates M. Consider the map $\phi : A^n \to M$ given by $(a_1, \ldots, a_n) \mapsto a_1 x_1 + \cdots + a_n x_n$. This map is A–linear, and is surjective since (x_i) is a generator for M. Then by the First Isomorphism Theorem, $A^n/\ker(\phi) \cong M$. ∎

Nakayama's Lemma

Before we can prove Nakayama's Lemma, we need a bit of groundwork.

Definition. If M is an A–module and $I \subseteq A$ is an ideal, we say

$$IM = \left\{ \sum_{i=1}^n a_i x_i : n < \omega, a_1, \ldots, a_n \in I, x_1, \ldots, x_n \in M \right\}$$

2.2 Proposition. *Suppose M is a finitely generated A–module, $I \subseteq A$ an ideal, $\phi : M \to M$ A–linear such that $\phi(M) \subseteq IM$. Then there exists $n < \omega$, and $a_1, \ldots, a_n \in I$ such that $\phi^n + a_1 \phi^{n-1} + \cdots + a_{n-1}\phi + a_n = 0$ in $\text{Hom}_A(M, M) = \text{End}_A(M)$.*

In particular, taking $I = A$, every endomorphism of a finitely generated module satisfies a nontrivial polynomial identity over A.

Proof Let $x_1,\dots,x_n$ generate M. Then $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$ for some $a_{ij} \in I$ since $\phi(M) \subseteq IM$. Thus for for each $i = 1,\dots,n$,

$$\sum_{j=1}^{n}\Big(\delta_{ij}\phi(x_j) - a_{ij}x_j\Big) = 0 \Longrightarrow \sum_{j=1}^{n}(\delta_{ij}\phi - a_{ij})(x_j) = 0$$

Let $P = (\delta_{ij}\phi - a_{ij}) \in M_{n\times n}(\mathrm{End}_A(M))$ act naturally on M^n. Then by the above observation,

$$P\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum\limits_{j=1}^{n}(\delta_{1j}\phi - a_{1j})(x_j) \\ \vdots \\ \sum\limits_{j=1}^{n}(\delta_{nj}\phi - a_{1j})(x_j) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

By the adjoint formulation of inverse,

$$(\det P)\begin{pmatrix} 1 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 1 \end{pmatrix} = P^{\mathrm{adj}}P\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

Thus, $\det P \in \mathrm{End}_A(M)$ vanishes on $x_1,\dots,x_n$, and since $x_1,\dots,x_n$ generate M, $\det P = 0$ in $\mathrm{End}_A(M)$. In particular, $\det(\delta_{ij}\phi - a_{ij}) = 0$, and since the determinant is a monic polynomial in ϕ with coefficients in I, we are done. ■

Definition. The **annhilator of** M is the ideal $\mathrm{Ann}(M) = \{a \in A : aM = 0\}$.

2.3 Corollary. *Let M be a finitely generated module with $I \subseteq A$ an ideal such that $IM = M$. Then there exists $a \in \mathrm{Ann}(M)$ with so $a \equiv 1 \pmod{I}$.*

Proof Since $IM = M$, Proposition 2.2 applies to every $\phi \in \mathrm{End}_A(M)$. In particular, take $\phi = \mathrm{id}$ and get $a_1,\dots,a_n \in I$ so $1 + a_1 + \dots + a_n = 0$ in $\mathrm{End}_A(M)$. Thus $a := 1 + a_1 + \dots + a_n$, then $a \in \mathrm{Ann}(M)$ and $a \equiv 1 \pmod{I}$. ■

Definition. The **Jacobson radical** of a ring is the intersection of all maximal ideals of the ring.

Definition. A ring is a **local ring** if it has exactly one maximal ideal.

2.4 Lemma. (Nakayama) *Let M be finitely generated module and $I \subseteq A$ an ideal such that $I \subseteq R$, where R is the Jacobson radical. If $IM = M$, then $M = 0$.*

Proof By Corollary 2.3, there is $a \in \mathrm{Ann}(M)$, $a \equiv 1 \pmod{I}$. Write $a = 1 - b$ for some $b \in I$. If a is not a unit in A, then (a) is proper, so a is contained in some maximal ideal $\mathfrak{m} \subseteq A$. But $b \in I \subseteq\subseteq R\mathfrak{m}$, so $1 = a + b \in \mathfrak{m}$, a contradiction. Thus a is a unit, so $aM = 0$ and $a^{-1}aM = 0$ so $M = 0$. ■

If A is a local ring, Nakayama's Lemma applies to any proper ideal in A.

2.5 Corollary. *Suppose M is finitely generated, I is contained in the Jacobson radical, and $x_1,\dots,x_n \in M$ are such that their images in M/IM generate M/IM as an A–module. Then $\{x_1,\dots,x_n\}$ generates M.*

Proof Let $N = (x_1,\dots,x_n)$ be the submodule of M generated by $x_1,\dots,x_m$. Note that $I\cdot(M/N) = (N+IM)/N$. Since $(x_1+IM,\dots,x_n+IM)$ generate M/IM, $N+IM = (x_1,\dots,x_n)+IM = M$. Thus $I\cdot(M/N) = N/M$, so apply Nakayama's Lemma to M/N. Thus $M/N = 0$, so $M = N$ and $M = (x_1,\dots,x_n)$. ■

Exact Sequences

Definition. Let $M_0, M_1,\dots,M_n$ be A–modules, with A–linear maps $f_i : M_i \to M_{i+1}$. Then we say that this sequence is **exact at** M_i for $i \in \{1,\dots,n-1\}$ if $\operatorname{im}(f_i) = \ker(f_{i+1})$. The sequence is **exact** if it is exact at all such i.

Remark. Suppose $f : M \to N$ is an a–Linear map.

1. Then f is injective if and only if $0 \to M \xrightarrow{f} N$ is exact.
2. f is surective if and only if $M \xrightarrow{f} N \to 0$ is exact.

In this sense, exactness of sequences generalizes injectivity and surjectivity.

Now consider the sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$. This is exact if and only if f is injective, g is surjective, and $\operatorname{im}(f) = \ker(g)$. In this case, we say M is an **extension of** M'' **by** M'. Note that by the First Isomorphism Theorem, $M'' \cong M/M'$ after identifying $M' \cong f(M') \le M$.

Example. Whenever $h : M \to N$ is an A–linear map, we have the associated short exact sequence:

$$0 \to \ker(h) \hookrightarrow M \xrightarrow{h} \operatorname{im}(h) \to 0$$

Example. Given M', M'' A–modules, we always have the short exact sequence

$$0 \to M' \xrightarrow{f} M' \oplus M'' \xrightarrow{g} M'' \to 0$$

where $f(x) = (x,0)$ and $g(x,y) = y$. In this sense, $M' \oplus M''$ is a "trivial" extension of M'' by M'.

Definition. Given a short exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, we say that it is **split** if there is an isomorphism $\alpha : M \to M' \oplus M''$ such that

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

commutes, where $u(x) = (x,0)$ and $v(x,y) = y$.

Example. Here's an exact sequence that is not split: set $A = \mathbb{Z}$ and fix $n > 0$. Then

$$0 \to n\mathbb{Z} \hookrightarrow \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$$

is an exact sequence, but $\mathbb{Z} \ncong nZ \oplus \mathbb{Z}/n\mathbb{Z}$ since $\mathbb{Z}$ is torsion free, but $(0,1)$ is torsion.

Remark. If you have a long exact sequence

$$0 \to M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \xrightarrow{\phi_3} \cdots$$

you get a corresponding collection of short exact sequences

$$0 \to M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} \mathrm{im}(\phi_2) \to 0$$
$$0 \to \mathrm{coker}(\phi_2) \xrightarrow{\phi_3} M_4 \xrightarrow{\phi_4} \mathrm{im}(\phi_4) \to 0$$
$$\vdots$$

and the long exact sequence is exact if and only if all the short exact sequences are.

II. Finitely Generated Modules over PIDs

3 Rank, Basis, Torsion

Definition. Let M be an A–module, $X \subseteq M$ a subset. X is A–**linearly independent** if whenever $x_1, \dots, x_n \in X$ are distinct and $a_1, \dots, a_n \in A$, if $a_1x_1 + \cdots + a_nx_n = 0$, then $a_1 = a_2 = \cdots = a_n = 0$. We say that X is a **basis** for M if X generates M and is A–linearly independent.

Unlike vector spaces, modules usually do not have bases. In fact, we have the following lemma:

3.1 Lemma. *M has a basis if and only if M is free.*

Proof (⇒) First suppose $X \subseteq M$ is a basis. Consider the map

$$\bigoplus_{x \in X} A \xrightarrow{f} M \text{ given by } (a_x : x \in X) \mapsto \sum_{x \in X} a_x x$$

Since a domain is a direct sum, this summation is finite. As well, the map is clearly A–Linear: f is surjective since $M = (X)$, and f is injective since X is A–linearly independent. Thus M is isomorphic to a direct sum over A, so M is free.

(⇐) Conversely, suppose M is free. Let $f : M \to \bigoplus_{i \in I} A$ be an isomorphism. For each $i \in I$, let

$$e_j = \{(a_i : i \in I) : a_i = 1 \text{ if } i = j, a_i = 0 \text{ otherwise}\}$$

Clearly, $\{e_j : j \in I\}$ is a basis for $\bigoplus_{i \in I} A$ (the **standard basis**), so one can verify that $\{f^{-1}(e_j) : j \in I\} \subseteq M$ is a basis for M. ■

Definition. Suppose A is an integral domain, M an A–module. Then the **rank of** M is the maximum size of an A–linearly independent subset of M. We say $\operatorname{rank}(M) \in \mathbb{N} \cup \{\infty\}$.

3.2 Proposition. *If $F : M \to N$ is A–linear, then* $\operatorname{rank}(f(M)) \leq \operatorname{rank}(M)$.

Proof Suppose $\operatorname{rank}(M) = m \in \mathbb{N}$. Let $y_1, \dots, y_{m+1} \in f(M)$ distinct, and get $y_i = f(x_i)$ for $x_i \in M$. Thus $\{x_1, \dots, x_{m+1}\}$ is A–linearly dependent, so there is $a_1, \dots, a_{m+1} \in A$, not all zero, so

$$a_1x_1 + \cdots + a_{m+1}x_{m+1} = 0$$

Then by applying f, $a_1y_1 + \cdots + a_{m+1}y_{m+1} = 0$, so $\{y_1, \dots, y_{m+1}\}$ is A–linearly dependent, and $\operatorname{rank}(f(M)) \leq m$. ■

3.3 Lemma. *Let A be an integral domain. Then* $\operatorname{rank}(A^m) = m$.

Proof Let $F = \mathrm{Frac}(A)$, so $A^m \subseteq F^m$ in a natural way. Certainly $\mathrm{rank}(A^m) \geq m$, taking the standard basis, so let $x_1, \ldots, x_{m+1} \in A^m$ be distinct. F^m is a vector space, so this collection is F–linearly dependent in F^m. Thus get f_i so that $f_1 x_1 + \cdots + f_{m+1} x_{m+1} = 0$, where $f_i = a_i/b_i$, $a_i, b_i \in A$. Then clearing denominators, since we are in an integral domain, we see that $\{x_1, \ldots, x_{m+1}\}$ are A–linearly dependent and $\mathrm{rank}(A^m) \leq m$. ■

Definition. Let A be an integral domain and M an A–module. We define the **torsion submodule** by $\mathrm{Tor}(M) = \{x \in M : \exists a \in A \setminus \{0\} \text{ s.t. } ax = 0\}$. We say:
1. $x \in M$ is **torsion** if $x \in \mathrm{Tor}(M)$
2. $N \leq M$ is **torsion free** if $\mathrm{Tor}(M) \cap N = \{0\}$
3. $N \leq M$ is **torsion** if $N \leq \mathrm{Tor}(M)$.

Remark. x is torsion if and only if $\{x\}$ is A–linearly dependent.

3.4 Lemma. *Let A be an integral domain. Then*
(i) M is torsion if and only if $\mathrm{rank}(M) = 0$.
(ii) Free modules are torsion-free.
(iii) If M and N are torsion, then $M \oplus N$ is torsion. In particular, $a_1, \ldots, a_n \in A$ be non-zero. Then $A/(a_1) \oplus A/(a_2) \oplus \cdots \oplus A/(a_n)$ is torsion.

Proof (i) This follows since

$$\begin{aligned} M \text{ is torsion} &\iff x \in M \text{ is torsion} \\ &\iff \{x\} \text{ is linearly dependent for all } x \in M \\ &\iff \mathrm{rank}(M) < 1 \\ &\iff \mathrm{rank}(M) = 0 \end{aligned}$$

(ii) It suffices to do this for $M = \bigoplus_{i \in I} A$. Let $x \in M$, $x \neq 0$. Write $x = (a_i : i \in I)$. Then $x \neq 0$ implies $a_{i_0} \neq 0$ for some $i_0 \in I$. If $a \in A$ and $ax = 0$, then $aa_{i_0} = 0$. Thus $a = 0$ since $a_{i_0} \neq 0$ and A is an integral domain, so x is not torsion.

(iii) Let $(x, y) \in M \oplus N$, and get a_1, a_2 so $a_1 x = a_2 y = 0$; then A is an integral domain so $a_1 a_2 \neq 0$ and $a_1 a_2 (x, y) = (0, 0)$. For the latter part, $A/(a_i)$ is torsion since $a_i(x + (a_i)) = 0 + (a_i)$, so their direct sum is also torsion. ■

4 Noetherian Rings

Let R be a commutative ring.

Definition. R is **Noetherian** if every ascending chain of ideals in R stabilizes.

We have the following fundamental property of Noetherian rings:

4.1 Proposition. *The following are equivalent:*
1. *R is Noetherian.*
2. *Every non-empty set S of ideals of R has a maximal element in S.*
3. *Every ideal of R is finitely generated.*

Proof $(1) \Rightarrow (2)$. Let S be a non-empty set of ideals with no maximal element. Since S is non-empty, get $I_1 \in S$. Then for any $I_k \in S$, I_k is not maximal and get $I_{k+1} \supsetneq I_k$. This is an infinite chain of ideal which does not stabilize.

(2) $\Rightarrow$ (1). Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals, and let $S = \{I_k : k \in \mathbb{N}\}$. By assumption, S has a maximal element, I_N; but then for any $n \geq N$, $I_n = I_N$ and the chain stabilizes.

(3) $\Rightarrow$ (1). Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals, and set $I = \bigcup_{i=1}^{\infty} I_n$. By assumption, $I = (x_1, \ldots, x_n)$. Since each $x_i \in I_j$ for some j, get k so that $x_1, \ldots, x_n \in I_k$; but then $I_k = I_n$ and the chain stabilizes.

(1) $\Rightarrow$ (3). Let I be an ideal of R not finitely generated. Then $I \neq (0)$, so get $a_1 \in I$. For any finite $a_1, \ldots, a_k \in I$, since I is not finitely generated, there exists $a_{k+1} \in I \setminus (a_1, \ldots, a_k)$. Thus by the axiom of choice, choose $a_i, i \in \mathbb{N}$ so that $\{(a_1, \ldots, a_i) : i \in \mathbb{N}\}$ does not stabilize, a contradiction. ∎

4.2 Corollary. *Every PID is Noetherian.*

Proof Every ideal of a PID is finitely generated (by one element). ∎

Remark. Suppose A is a PID. If $I \subseteq A$ is a non-zero ideal, then it is a free A–Module of rank 1. To see this, write $I = (a)$ for some $a \in A \setminus \{0\}$. Consider $A \to I$ by $b \mapsto ba$, which is surjective. If $bn = 0$, then $b = 0$ since $a \neq 0$ is injective. Thus, as A–modules, $I \cong A$.

Definition. An A–module is **noetherian** if there is no properly increasing infinite chain of submodules.

Remark. A is a noetherian ring if and only if it is noetherian as an A–module. An A–module M is noetherian iff every submodule is finitely generated.

4.3 Theorem. (Hilbert Basis) *If A is noetherian, then $A[x]$ is noetherian.*

5 Finitely Generated Modules over PIDs

Proof of the Fundamental Theorem

5.1 Proposition. *Suppose A is a PID, M is a free A–module of rank $m \in \mathbb{N}$, and $N \leq M$ a submodule.*

(i) N is free with rank at most m.

(ii) There exists a basis $y_1, \ldots, y_m$ for M and $a_1, \ldots, a_n \in A \setminus \{0\}$ for some $n \leq m$ such that $a_1 y_1, \ldots, a_n y_n$ is a basis for N and $a_1 | a_2 | \cdots | a_n$.

(iii) $r, n, (a_1), \ldots, (a_n)$ are unique.

Proof We may assume $M = A^m$. Consider

$$\Sigma := \{I \subseteq A : I \text{ is an ideal s.t. } I = \phi(N) \text{ for some } \phi \in \operatorname{Hom}_A(M, A)\}$$

Since A is a PID, set $\phi(N) = (a_\phi)$.

Claim 1: $\Sigma \supsetneq \{(0)\}$ and Σ has a maximal element. Since $M = A^m$, we have coordinate projections $\pi_i : M \to A$ for $i = 1, \ldots, m$. Since $N \neq (0)$, not all of $\pi_1(N), \ldots, \pi_n(N)$ can be zero. Now, since A is a PID (and thus Noetherian), the second claim follows by Proposition 4.1

Now, let $\eta \in \operatorname{Hom}_A(M, A)$ be such that $\eta(N)$ is maximal in Σ. Thus $\eta(N) = (a_1)$ for some $0 \neq a_1 \in A$ non-zero; let $y \in N$ be such that $a_1 = \eta(y)$. We'll hold this notation for the rest of the proof.

Claim 2: $a_1|\phi(y)$ for all $\phi \in \mathrm{Hom}_A(M,A)$. Let $d \in A$ be such that $(a_1, \phi(y)) = (d)$, so $d = r_1a_1 + r_2\phi(y)$ for some $r_1, r_2 \in A$. Consider $\psi := r_1\eta + r_2\phi$. Then

$$\psi(y) = r_1\eta(y) + r_2\phi(y) = r_1a_1 + r_2\phi(y) = d$$

so $d \in \psi(N)$. Thus $(a_1, \phi(y)) \subseteq \psi(N) \subseteq \eta(N) = (a_1)$ by maximality of $\eta(N)$. But then $(a_1) = (a_1, \phi(y))$ so $a_1|\phi(y)$.

Claim 3: There exists some $y_1 \in M$ such that

(i) $\eta(y_1) = 1$

(ii) $M = (y_1) \oplus \ker(\eta)$

(iii) $N = (a_1y_1) \oplus (N \cap \ker(\eta))$

Consider the standard basis $e_1, \dots, e_m$ of $M = A^m$, so that for any $x \in M$, $x = \pi_1(x)e_1 + \cdots + \pi_m(x)e_m$. By Claim 2, since $\pi_i \in \mathrm{Hom}_A(M,A)$, get b_i so that $\pi_i(y) = a_1b_i$. Thus we can set

$$y = \sum_{i=1}^m \pi_i(y)e_i = \sum_{i=1}^m a_1b_ie_i = a_1\left(\sum_{i=1}^m b_ie_i\right) =: a_1y_1$$

In particular, $a_1y_1 = y \in N$. Now we have

(i) $a_1\eta(y_1) = \eta(a_1y_1) = \eta(y) = a_1$ so $\eta(y_1) = 1$.

(ii) Let $x \in M$ be arbitrary. Then $\eta(x - \eta(x)y_1) = \eta(x) - \eta(x)\eta(y_1) = 0$, so $x - \eta(x)y_1 \in \ker(\eta)$. Thus $x = \eta(x)y_1 + z$ for some $z \in \ker(\eta)$, so $M = (y_1) + \ker(\eta)$. Suppose $x \in (y_1) \cap \ker(\eta)$. Then $x = ay_1$ for some $a \in A$ and $0 = \eta(x) = a\eta(y_1) = a$, so $x = 0$ and $M = (y_1) \oplus \ker(\eta)$.

(iii) Let $x \in N$, so $\eta(x) \in \eta(N) = (a_1)$. Thus $\eta(x) = ba_1$ for some $b \in A$. Then

$$\begin{aligned} x &= \eta(x)y_1 + (x - \eta(x)y_1) \\ &= ba_1y_1 + (x - ba_1y_1) \end{aligned}$$

Thus $N = (a_1y_1) + (\ker(\eta) \cap N)$. Furthermore, $(a_1y_1) \cap (\ker(\eta) \cap N) \subseteq (y_1) \cap \ker(\eta) = (0)$. Thus $N = (a_1y1) \oplus (N \cap \ker(\eta))$.

For the remainder of the proof, set $K = \ker(\eta)$.

Proof of (i). Certainly $\mathrm{rank}(N) \leq m$ since N is a submodule of M. Let's proceed by induction on the rank of N. If $\mathrm{rank}(N) = 0$, by Lemma 3.4, N is torsion. However, $N \subseteq M$ which is free and thus has no non-trivial torsion, so $N = (0)$ and hence free.

Now, suppose $\mathrm{rank}(N) > 0$, so N is non-trivial. Applying Claim 3, we have $M = (y_1) \oplus K$, $N = (a_1y_1) \oplus (N \cap K)$. Let's see that $\mathrm{rank}(N) \geq \mathrm{rank}(K \cap N) + 1$. Let $x_1, \dots, x_l \in K \cap N$ A–linearly independent. Suppose we have $b_1, \dots, b_l, c \in A$ such that $b_1x_1 + \cdots + b_lx_l + c(a_1y_1) = 0$, so $ca_1y_1 = -(b_1x_1 + \cdots + b_lx_l) \in K \cap N$ while $ca_1y_1 \in (a_1y_1)$, so $ca_1y_1 = 0$ and $ca_1 = 0$ since y_1 is not torsion. Thus $b_1x_1 + \cdots + b_lx_l = 0$, so $b_1 = b_2 = \cdots = b_l = 0$, and $\{x_1, \dots, x_l, a_1y_1\}$ is A–linearly independent.

Thus, $\mathrm{rank}(N) \geq \mathrm{rank}(K \cap N) + 1$, so $\mathrm{rank}(K \cap N) < \mathrm{rank}(N)$ and by induction, $K \cap N$ is free. Furthermore, (a_1y_1) is free: consider $A \to (a_1y_1)$ by $b \mapsto ba_1y_1$, which is A–linear and surjective. If $ba_1y = 0$, then since M has no nontrivial torsion, $ba_1 = 0$ so $b = 0$ since $a_1 \neq 0$ and A is an integral domain. Thus $A \cong (a_1y_1)$ and $N = (a_1y_1) \oplus K \cap N$ is free.

Note that in general, any submodule of a free module over a PID is free.

Proof of (ii). The proof proceeds by induction on $\mathrm{rank}(M)$. If $\mathrm{rank}(M) = 0$, then $M = (0)$ and the statement holds vacuously, so suppose M is non-trivial. Similarly, if N is trivial, take $n = 0$, so suppose N is non-trivial. Note that $K \leq M$, so we may apply (i) with K in place of N. In particular, K is free with $\mathrm{rank}(K) < \mathrm{rank}(M)$.

By induction, apply the claim with $K \cap N \leq K$. Get a basis $y_2, \ldots, y_m$ of K and $a_2, \ldots, a_n \in A$ so $a_2 | a_3 | \cdots | a_n$, $n \leq m$, such that $\{a_2 y_2, \ldots, a_n y_n\}$ is a basis for $K \cap N$. But now, since $M = (y_1) \oplus K$ and $N = (a_1 y_1) \oplus (K \cap N)$ by Claim 3, $\{y_1, y_2, \ldots, y_m\}$ is a basis for M and $\{a_1 y_1, \ldots, a_n y_n\}$ is a basis for N. It remains to show $a_1 | a_2$. Consider $\phi \in \mathrm{Hom}_A(M, A)$ by $y_1 \mapsto 1$, $y_2 \mapsto 1$, $y_i \mapsto 0$ for $i > 2$ (since M is free, $y_1, \ldots, y_n$ a basis, for any A–module and $z_1, \ldots, z_m \in A$, then there is a unique A–linear map from $M \to N$ such that $y_i \mapsto z_i$). Then $\phi(a_1 y_1) = a_1$. Since $a_1 y_1 \in N$, this shows $a_1 \in \phi(N)$ so that $(a_1) \subseteq \phi(N)$. However, $K = (a_1)$, so by maximality, $(a_1) = \phi(N)$. Finally, $\phi(a_2 y_2) = a_2 \phi(y_2) = a_2$, so $a_2 \in \phi(N) = (a_1)$, so $a_1 | a_2$. ■

5.2 Theorem. *Let A be a PID, M a finitely generated A–module. Then $M \cong A^r \oplus A/(a_1) \oplus \cdots \oplus A/(a_n)$ where $r \geq 0$, $a_1 | a_2 | \cdots | a_n$ are nonzero nonunits in A.*

Proof That $a_1, \ldots, a_n$ are non-zero non-units is free. Suppose M is generated by $x_1, \ldots, x_m$ with m minimal. Consider $\pi : A^m \to M$ by $e_i \mapsto x_i$, where $\{e_1, \ldots, e_m\}$ is the standard basis for A^m. This is a surjective A–linear map, so $M \cong A^m / \ker(\pi)$. Apply Proposition 5.1 to $\ker(\pi)$ and get a basis $y_1, \ldots, y_m$ of A^m and $a_1 | a_2 | \cdots | a_n$ in A such that $\{a_1 y_1, \ldots, a_n y_n\}$ is a basis for $\ker(\pi)$, where $n = \mathrm{rank}(\ker(\pi))$. Thus $M \cong A^m / (a_1 y_1) + (a_2 y_2) + \cdots + (a_n y_n)$. Consider $f : A^m \to A/(a_1) \oplus \cdots \oplus A/(a_n) \oplus A^{m-n}$ by

$$f(\alpha_1 y_1 + \cdots + \alpha_m y_m) = (\alpha_1 (\mathrm{mod}\, a_1), \ldots, \alpha_n (\mathrm{mod}\, a_n), \alpha_{n+1}, \cdots, \alpha_m)$$

Furthermore, $\ker(f) = (a_1 y_1) + (a_2 y_2) + \cdots + (a_n y_n)$. Thus

$$A/(a_1) \oplus \cdots \oplus A/(a_n) \oplus A^{m-n} \cong A^m / \ker(f) = A^m / (a_1 y_1) + \cdots + (a_n y_n) \cong M$$ ■

Properties of the Fundamental Theorem

Remark. Any quotient module $A/(a)$ is generated by the element $1 + (a)$. In particular, every finitely generated A–module is a direct sum of cyclic A–modules.

5.3 Corollary. *Let A, M be as in the Fundamental Theorem.*

1. $\mathrm{Tor}(M) = A/(a_1) \oplus \cdots \oplus A/(a_n)$
2. *M is free if and only if M is torsion-free*
3. $\mathrm{rank}(M) = r$

Proof

1. From Lemma 3.4, if $x \in A/(a_1) \oplus \cdots \oplus A/(a_n)$, then x is torsion. Conversely, if $x \in \mathrm{Tor}(M)$, $x = (b_1, \ldots, b_r, c_a + (a_1), \ldots, c_n + (a_n))$. If $0 \neq b \in A$ such that $bx = 0$, then $bb_i = 0$ for $i = 1, \ldots, r$. Since A is an integral domain, $b_i = 0$ and $x \in A/(a_1) \oplus \cdots \oplus A/(a_n)$.
2. This is immediate from part (1).
3. Note that $\mathrm{rank}(M) = \mathrm{rank}(A^r) + \mathrm{rank}(A/(a_1) \oplus \cdots \oplus A/(a_m))$ by HW2 Q3. From Part (1), the second module is torsion and thus has rank 0, so $\mathrm{rank}(M) = r$. ■

5.4 Lemma. (Chinese Remainder) *Let A be a ring, I, J ideals such that $I + J = A$. Then $A/I \cap J \cong A/I \oplus A/J$ as rings (and thus also as A–modules).*

Proof Let $f : A \to A/I \oplus A/J$ be given by $a \mapsto (a+I, a+J)$, so $\ker(f) = I \cap J$. It remains to show surjectivity: let $a, b \in A$. We want $c \in A$ such that $c + I = a + I$ and $c + J = b + J$. Since $I + J = A$, there is $x \in I$, $y \in J$ so $x + y = 1$. Let $c := bx + ay \in A$, so

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

and in the same way, $c + J = b + J$. Thus f is surjective, and the result holds by the First Isomorphism Theorem for rings. ■

5.5 Theorem. *Let A be a PID, M a finitely generated A–module. Then $M \cong A^r \oplus A/(p_1^{\alpha_1}) \oplus \cdots \oplus A/(p_t^{\alpha_t})$ for some $r \geq 0$, $\alpha_1, \ldots, \alpha_t > 0$, $p_1, \ldots, p_t$ (possibly associate) primes, where r, t are unique and $p_1, \ldots, p_t$ are unique up to associates.*

Proof For any $a \in A$, write $a = up_1^{\alpha_1} \cdots p_s^{\alpha_s}$ where the p_i are non-associate primes and u is a unit. For $i \neq j$, $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = (d)$ for some $d \in A$ since A is a PID. Then $d | p_i^{\alpha_i}$ and $d | p_j^{\alpha_j}$, so d is a unit and $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = A$. Thus by the generalized Chinese Remainder Theorem,

$$A/(p_1^{\alpha_1}) \cap \cdots \cap (p_s^{\alpha_s}) \cong A/(p_1^{\alpha_1}) \oplus \cdots \oplus A/(p_s^{\alpha_s})$$

so that $(a) = (p_1^{\alpha_1}) \cap \cdots \cap (p_s^{\alpha_s})$. Thus

$$A/(a) \cong A/(p_1^{\alpha_1}) \oplus \cdots \oplus A/(p_s^{\alpha_s})$$

Now, by the Fundamental Theorem, let $a_1 | a_2 | \cdots | a_n$ be such that $M \cong A^r \oplus A/(a_1) \oplus \cdots \oplus A/(a_n)$. The result follows by applying the above construction to a_i for each i. Uniqueness follows by unique factorization and the uniqueness of the representation in the Fundamental Theorem. ■

Example. (Finitely Generated Abelian Groups) Let $A = \mathbb{Z}$, so M is a finitely generated abelian group. Then $M \cong \mathbb{Z}^r \oplus \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_n}$ where $a_1 | a_2 | \cdots | a_n$. As before, we also have $M \cong \mathbb{Z}^r \oplus \mathbb{Z}_{p_1}^{\alpha_1} \oplus \cdots \oplus \mathbb{Z}_{p_t}^{\alpha_t}$ with uniqueness statements.

Jordan and Rational Canonical Forms

Let F be a field, $A = F[t]$ be a polynomial ring in t over F. Since A is a PID, FTFGMPID applies.

The first thing we need to understand are the quotients A/I. Since I is principal, $I = (p(t))$. We may assume I is non-trivial and proper, so we may choose $p(t)$ to be a monic polynomial with degree greater than 0. Write $p(t) = t^k + b_{k-1}t^{k-1} + \cdots + b_1 t + b_0$. Note that $M = A/I = F[t]/(p(t))$ is a finite dimension F–vector space with basis $B = \{1 + I, t + I, \ldots, t^{k-1} + I\}$. Let $T : M \to M$ be the F–linear transformation given by $T(v) = tv$. Then, the matrix of T with respect to B

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & \cdots & 0 & -b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -b_{k-1} \end{pmatrix} = C_{p(t)}$$

Suppose $p(t) = (t-\lambda)^k$ for some $\lambda \in F$. In this case, we have another natural basis for M over F, namely $B' = \{1+I, (t-\lambda)+I, \dots, (t-\lambda)^{k-1}+I\}$. Then the matrix of T with respect to B' is $T(1+I) = t+I = \lambda(1+I)+(t-\lambda)+I$. $T((t-\lambda)+I) = \lambda((t-\lambda)+I)+((t-\lambda)^2+I)$ so the matrix is given by

$$\begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \\ 0 & 0 & \cdots & \lambda \end{pmatrix}$$

Now, suppose V is a F–vector space of finite dimension and $T : V \to V$ is a linear transformation. We make V into an $F[t]$–module by

$$(a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0)(v) := a_n T^n(v) + a_{n-1} T^{n-1}(v) + \cdots + a_0 v$$

Then V is finitely generated as an F–module. Hence, a fortiori, finitely generated as an A–module. By FTFGMPID, as an A–module, $V = F[t]^r \oplus F[t]/(a_1(t)) \oplus \cdots \oplus F[t]/(a_n(t))$ where $a_1(t)|a_2(t)|\cdots|a_n(t)$. Since V is a finite dimensional F–vector space (and $F[t]$ is not), r must be 0. Let B be an F–basis for V obtained by taking the union of the nontrivial bases for each $F[t]/(a_i(t))$. The matrix of T with respect to these bases is block diagonal with $C_{a_i(t)}$, which is the rational canonical form of T.

Now, suppose $F = F^{\text{alg}}$ is an algebraically closed field. Apply the elementary divisor form to get

$$V \cong F[t]/p_1(t)^{\alpha_1} \oplus \cdots \oplus F[t]/p_l(t)^{\alpha_l}$$

where $p_1, \dots, p_l$ are irreducible polynomials. Thus, since F is algebraically closeda and we may assume p_i are monic, $p_i(t) = t - \lambda_i$. Thus

$$V \cong F[t]/(t-\lambda_1)^{\alpha_1} \oplus \cdots \oplus F[t]/(t-\lambda_l)^{\alpha_l}$$

Let B' be the union of the natural bases for each $F[t]/(t-\lambda_i)^{\alpha_i}$. The matrix of T with respect to B' is the Jordan canonical form.

III. Tensors and Algebras

6 Categories and Functors

Definition. A **category** $\mathcal{C}$ consists of:

- A class $\mathrm{Ob}(\mathcal{C})$ of **objects**.
- For each $X, Y \in \mathrm{Ob}(\mathcal{C})$, a set $\mathrm{Hom}_{\mathcal{C}}(X,Y)$ of **morphisms** $f : X \to Y$.
- A **composition of morphisms**: for every three objects X, Y, Z, a binary operation $\circ : \mathrm{Hom}_{\mathcal{C}}(X,Y) \times \mathrm{Hom}_{\mathcal{C}}(Y,Z) \to \mathrm{Hom}_{\mathcal{C}}(X,Z)$.

such that

1. $\circ$ is associative
2. For each $X \in \mathrm{Ob}(C)$, there exists $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X,X)$ such that for all $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(Y,X)$, $f \circ \mathrm{id}_X = f$ and $\mathrm{id}_X \circ g = g$.

When we talk about categories, it is natural to talk about maps between categories.

Definition. A **(covariant) functor** $F : \mathcal{C} \to \mathcal{C}'$ is a map $F : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}')$ such that for all $X, Y \in \mathcal{C}$, there is a map $F : \mathrm{Hom}_{\mathcal{C}}(X,Y)$ such that

$$F(\mathrm{id}_X) = \mathrm{id}_{F(x)}, \qquad F(f \circ g) = F(f) \circ F(g)$$

The functor is **contravariant** if instead $F(g \circ f) = F(f) \circ F(g)$.

Definition. Let F be a covariant functor in an abelian category. Then F is:

- **exact** if $0 \to A \to B \to C \to 0$ exact implies $0 \to F(A) \to F(B) \to F(C) \to 0$ exact.
- **left exact** if $0 \to A \to B \to C$ exact implies $0 \to F(A) \to F(B) \to F(C)$ exact.
- **right exact** if $A \to B \to C \to 0$ exact implies $F(A) \to F(B) \to F(C) \to 0$ exact.

Similar definitions hold for contravariant functors.

The Hom functor

In the case of A–modules, recall that $\mathrm{Hom}_A(M,N)$ is the set of A–linear maps from M to N which is itself is an A–module with

$$(f+g)(x) = f(x) + g(x), \qquad (af)(x) = af(x)$$

6.1 Proposition. *Let M be an A–module. Then $\mathrm{Hom}_A(M,\bullet)$ is a left exact covariant functor $N \mapsto \mathrm{Hom}_A(M,N)$.*

Proof To show that $\mathrm{Hom}_A(M,\bullet)$ is a covariant functor, given $\eta : N \to N'$, define the induced map $\overline{\eta} : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N')$ by $\overline{\eta}(g) = \eta \circ g$.

$$\begin{tikzcd}
N \arrow[r, "\eta"] & N' \\
M \arrow[u, "g"] \arrow[ur, "\overline{\eta}(g):=\eta\circ g"'] &
\end{tikzcd}$$

$\overline{\mathrm{id}} = \{f \mapsto f\}$ is the identity map and $\overline{f \circ g} = \{\alpha \mapsto f \circ g \circ \alpha\} = \{\alpha \mapsto f \circ \alpha\} \circ \{\alpha \mapsto g \circ \alpha\} = \overline{f} \circ \overline{g}$, so we have a covariant functor.

Now let's see left exactness: suppose we are given an exact sequence $0 \to N' \xrightarrow{\rho} N \xrightarrow{\eta} N''$. We need to show that

$$0 \to \mathrm{Hom}_A(M, N') \xrightarrow{\overline{\rho}} \mathrm{Hom}_A(M, N) \xrightarrow{\overline{\eta}} \mathrm{Hom}_A(M, N'')$$

is exact.

Let's first show that $\overline{\rho}$ is injective. Let $g \in \mathrm{Hom}_A(M, N)$ be such that $\overline{\rho}(g) = 0$. Suppse $0 \neq x \in \mathrm{im}(g)$; then $\overline{\rho}(g)(x) = \rho(g(x)) \neq 0$ since ρ is injective, so $\overline{\rho}(g)$ is not the zero map. Thus $\overline{\rho}$ is injective.

Now we need to show that $\ker \overline{\eta} = \mathrm{im}\,\overline{\rho}$. First suppose $h \in \mathrm{im}\,\overline{\rho}$, so $h = \overline{\rho}(g)$. Then the following diagram commutes:

$$\begin{tikzcd} N' \arrow[r, "\rho"] & N \arrow[r, "\eta"] & N' \\ & M \arrow[ul, "g"] \arrow[u, "h"] \arrow[ur, "\overline{\eta}(h)"'] & \end{tikzcd}$$

Since $\mathrm{im}(\rho) = \ker(\eta)$, $\overline{\eta}(h) = \eta \circ \rho \circ g = 0$, so $\overline{\eta}(h) \in \ker \overline{\eta}$ and $\mathrm{im}\,\overline{\rho} \subseteq \ker \overline{\eta}$.

Now suppose $h \in \ker \overline{\eta}$: we want to show that $h \in \mathrm{im}\,\overline{\rho}$. We want to find ϕ so that the following diagram commutes:

$$\begin{tikzcd} N' \arrow[r, "\rho"] & N \arrow[r, "\eta"] & N' \\ & M \arrow[ul, "\phi"] \arrow[u, "h"] \arrow[ur, "\overline{\eta}(h)=0"'] & \end{tikzcd}$$

Let $x \in M$; then $h(\eta(x)) = \overline{\eta}(h)(x) = 0$, so $h(x) \in \ker \eta = \mathrm{im}\,\rho$. Thus by injectivity of ρ, get a unique $y \in N'$ so that $\rho(y) = h(x)$. Set $\phi(x) = y$; then verifying A–linearity is straightforward. ■

Example. Let $A = \mathbb{Z}$ and $n > 1$ be arbitrary. Let π be the quotient map (a surjective homomorphism), and suppose we want the following diagram to commute:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\pi"] & \mathbb{Z}/n\mathbb{Z} \\ \mathbb{Z}/n\mathbb{Z} \arrow[u, dashed, "?"] \arrow[ur, "\mathrm{id}"] & \end{tikzcd}$$

However, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \{0\}$ since $\mathbb{Z}/n\mathbb{Z}$ has torsion but $\mathbb{Z}$ is torsion free: any homomorphism f must take torsion elements to torsion elements, so they must all be the zero map. But then

$$\overline{\pi} : \{0\} = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \neq \{0\}$$

since id is in the image, and $\overline{\pi}$ is not surjective.

> ***6.2 Proposition.*** *Let M be an A–module. Then $\mathrm{Hom}_A(\bullet, M)$ is a right exact contravariant functor.*

Proof The methods are similar to the previous proof. ∎

6.3 Lemma. *Suppose we are given A–linear maps $u : X' \to X$ and $v : X \to X''$. Suppose that for all A–modules P,*

$$0 \to \mathrm{Hom}(X'', P) \xrightarrow{\overline{v}} \mathrm{Hom}(X, P) \xrightarrow{\overline{u}} \mathrm{Hom}(X', P)$$

is exact. Then

$$X' \xrightarrow{u} X \xrightarrow{v} X'' \to 0$$

is exact.

Proof Let's first see that v is surjective. Take $P = \mathrm{coker}(v) = X''/\mathrm{im}(v)$ so we have

$$\begin{tikzcd} X \arrow[r, "v"] \arrow[dr, "\overline{v}(\pi)"'] & X'' \arrow[d, "\pi"] \\ & P \end{tikzcd}$$

Since $\overline{v}(\pi) = \pi \circ v = 0$, by injectivity of $\overline{v}$, $\pi = 0$ so v is surjective.

To see $\ker(v) \subseteq \mathrm{im}(u)$, take $P = \mathrm{coker}(u)$. As before, $\overline{u}(\pi) = 0$, so by exactness with P, $\overline{u}(\pi) = \overline{v}(f)$ for some $f : X'' \to P$. Then the following diagram commutes:

$$\begin{tikzcd} X' \arrow[r, "u"] \arrow[dr, "0=\overline{u}(\pi)"'] & X \arrow[r, "v"] \arrow[d, "\pi"] & X'' \arrow[dl, "f"] \\ & P & \end{tikzcd}$$

Thus let $x \in \ker(v)$, so $\pi(x) = f(v(x)) = 0$ and $x \in \mathrm{im}(u)$.

To see $\mathrm{im}(u) \subseteq \ker(v)$, take $P = X''$. Then the following diagram commutes:

$$\begin{tikzcd} X' \arrow[r, "u"] \arrow[drr, bend right, "0=\overline{u}(v)"'] & X \arrow[r, "v"] \arrow[dr, "\overline{v}(\mathrm{id})"] & X'' \arrow[d, "\mathrm{id}"] \\ & & P \end{tikzcd}$$

Thus $0 = \overline{u}(v) = v \circ u$, so if $x \in \mathrm{im}(u)$, $v(x) = 0$. ∎

7 Tensor Products

Definition. Let M, N, P be A–modules. Then an A-**bilinear** map $f : M \times N \to P$ is a function satisfying:

1. For each $x \in M$, $f(x, \cdot) : N \to P$ given by $y \mapsto f(x, y)$ is A–linear.
2. For each $y \in N$, $f(\cdot, y) : N \to P$ given by $x \mapsto f(x, y)$ is A–linear.

Remark. We are not considering $M \times N$ as an A–module - just as a set: in general, an A–bilinear map $f : M \times N \to P$ is not A–linear.

7.1 Proposition. (Universal Property of Tensors) *Let M, N be A–modules. Then there exists a pair (T, g) consisting of an A–module T and an A–bilinear map $G : M \times N \to T$ such that:*

(i) Given any A–module P and A–bilinear mapping $f : M \times N \to P$, there exists a unique A–linear mapping $f' : T \to P$ so that

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

commutes.

(ii) If (T, g) and (T', g') satisfy (i), then there exists a unique isomorphism $j : T \to T'$ so that $j \circ g = g'$.

Proof (i) Let C denote the free A–module $A^{(M,N)}$. Elements of C are formal sums of the form $\sum_{i=1}^{n} a_i \cdot (x_i, y_i)$ for $a_i \in A, x_i \in M, y_i \in N$. Let $D \leq C$ be generated by elements of the following types:

$$\begin{gathered} (x + x', y) - (x, y) - (x', y) \\ (x, y + y') - (x, y) - (x, y') \\ (ax, y) - a \cdot (x, y) \\ (x, ay) - a \cdot (x, y) \end{gathered}$$

Let $T = C/D$: for any $(x, y) \in C$, let $x \otimes y = (x, y) + D$ and set $g(x, y) = x \otimes y$. By definition of D, g is A–bilinear.

Now, define $\overline{f} : C \to P$ by $\overline{f}\left(\sum_{i=1}^{n} a_i(x_i, y_i)\right) = \sum_{i=1}^{n} a_i f(x_i, y_i)$. Since f is bilinear, $\overline{f}$ takes elements of D to 0 so $D \subseteq \ker(\overline{f})$. Thus by the universal property of quotients, there is a unique $f' : T \to P$ so that $f'(x \otimes y) = f(x, y)$.

(ii) Let (T', g') play the role of (P, f) and get a unique $j : T \to T'$ such that $g' = j \circ g$. Swapping T and T', get $j' : T' \to T$ so that $g = j' \circ g'$. Thus $j \circ j'$ and $j' \circ j$ are both identity maps, so j is the unique such isomorphim. ■

7.2 Lemma. *Given an A–module P and an A–linear map $f : M \to N$, there is a unique A–linear map*

$$f \otimes 1 : M \otimes_A P \to N \otimes_A P$$

such that $f \otimes 1(x \otimes y) = f(x) \otimes y$. In particular, $\bullet \otimes_A P$ is a covariant functor.

Proof Consider the map $M \times P \to N \otimes_A P$ given by $(x, y) \mapsto f(x) \otimes y$. It is straightforward to verify that this map is bilinear, so by the universal property of tensors, there is a unique map $f \otimes 1 : M \otimes_A P \to N \otimes_A P$ such that $f \otimes 1(x \otimes y) = f(x) \otimes y$. ■

7.3 Proposition. *If M is an A–module, then $A \otimes_A M \cong M$.*

Proof The map $\phi : A \times M \to M$ given by $(a, x) \mapsto ax$ is bilinear by module axioms. By the universal property, there is an A–linear map $A \otimes_A M \to M$ such that $f(a \otimes m) = am$. Take $a = 1$, and the map is clearly surjective.

To show bijectivity, let's provide an inverse function. Consider $g : M \to A \otimes_A M$ by $x \mapsto 1 \otimes x$, which is clearly A–linear. Furthermore, $f \circ g(x) = f(1 \otimes x) = x$, so $f \circ g = \mathrm{id}$. Similarly, $g \circ f(a \otimes x) = g(ax) = 1 \otimes ax = a \otimes x$: $g \circ f$ and id agree on tensors $a \otimes x$ of $A \otimes_A M$. Since such tensors generate $A \otimes_A M$, $g \circ f = \mathrm{id}$. Thus $g = f^{-1}$ so g is a bijection. ■

Example. Whether or not a tensor is zero is quite subtle. For example, in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, $2 \otimes 1 = 2(1 \otimes 1) = 1 \otimes 2 = 1 \otimes 0 = 0$. However, in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, $2 \otimes 1 \neq 0$.

In general, if (x_i) generate M and (y_i) generate N, then $(x_i \otimes y_j)$ generate $M \otimes_A N$. To see this, $x \in M$, $y \in N$, then $x = \sum a_i x_i$ and $y = \sum b_j y_j$ so that $x \otimes y = (\sum a_i x_i) \otimes (\sum_j b_j y_j) = \sum a_i b_j (x_i \otimes y_j)$. Since pure tensors generate $M \otimes_A N$, $(x_i \otimes y_j)$ generate $M \otimes_A N$.

Applying this to the example, since 2 generates $2\mathbb{Z}$ and 1 generates $\mathbb{Z}/2\mathbb{Z}$, $2 \otimes 1$ generates $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. Thus if $2 \otimes 1 = 0$, then $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ would be the zero module. However, $\mathbb{Z} \cong 2\mathbb{Z}$ via the map $x \mapsto 2x$. Thus $f \otimes 1 : \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \to 2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is an isomorphism, so that $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \neq 0$.

With similar methods as in the proof of Proposition 7.3, one can prove the following:

7.4 Proposition. *Let M, N, P be A–modules. Then*

1. $M \otimes N \cong N \otimes M$
2. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$
3. $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$

Proof

1. Take $x \otimes y \mapsto y \otimes x$.
2. Take $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$
3. Take $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$. One can use the inverse $(x \otimes z_1, y \otimes z_2) \mapsto (x, 0) \otimes z_1 + (0, y) \otimes z_2$. ■

Exactness Properties of Tensors

7.5 Proposition. (Adjointness of Tensors) $\mathrm{Hom}(M \otimes N, P) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, P))$.

Proof Given $f : M \otimes N \to P$, consider $\phi(f) : M \to \mathrm{Hom}(N, P)$ given by $x \mapsto \{y \mapsto f(x \otimes y)\}$. One can verify $\phi(f)(x) \in \mathrm{Hom}(N, P)$ so that $\phi(f) \in \mathrm{Hom}(M, \mathrm{Hom}(N, P))$.

Conversely, given $g : M \to \mathrm{Hom}(N, P)$, define $\psi(g) : M \otimes N \to P$ by $x \otimes y \mapsto g(x)(y)$. Again, one can verify that g is A–linear. We thus have

$$\phi(\psi(f))(x \otimes y) = \phi(f)(x)(y) = f(x \otimes y)$$

so that $\phi(\psi(f)) = f$. Similarly,

$$\psi(\phi(g))(x)(y) = \psi(g)(x \otimes y) = g(x)(y)$$

Thus for all $y \in N$, $\psi(\phi(g))(x) = g(x)$ so $\psi(\phi(g)) = g$. Thus $\phi = \psi^{-1}$ and ϕ is an isomorphism. ■

Remark. $\bullet \otimes P$ is not an exact functor. For example, $f : 2\mathbb{Z} \to \mathbb{Z}$ given by $f(2n) = 2n$ is injective, but $f \otimes 1 : 2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ given by $f \otimes 1(2x \otimes y) = 2x \otimes y$ is the zero map and has kernel $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \neq 0$ (from the previous example). In particular, we see that $\bullet \otimes P$ does not necessarily preserve injectivity. However, the following proposition does hold:

7.6 Proposition. *$N \otimes_A \bullet$ is right exact: i.e. if $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact, then $N \otimes M' \xrightarrow{1 \otimes f} N \otimes M \xrightarrow{1 \otimes g} N \otimes M'' \to 0$ is exact.*

Proof Let P be an arbitrary A–module. By right exactness of the $\mathrm{Hom}(\bullet,P)$, $0 \to \mathrm{Hom}(M',P) \to \mathrm{Hom}(M,P) \to \mathrm{Hom}(M'',P)$ is exact. By left exactness of $\mathrm{Hom}(N,\bullet)$, we have $0 \to \mathrm{Hom}(N,\mathrm{Hom}(M',P)) \to \mathrm{Hom}(N,\mathrm{Hom}(M,P)) \to \mathrm{Hom}(N,\mathrm{Hom}(M'',P))$ is exact. By adjointness, $0 \to \mathrm{Hom}(N \otimes M',P) \to \mathrm{Hom}(N \otimes M,P) \to \mathrm{Hom}(N \otimes M'',P)$ is exact. Since P was arbitrary, the proposition follows by Lemma 6.3. ∎

Definition. If $N \otimes_A \bullet$ is an exact functor, then we say that N is a **flat** A–module.

7.7 Proposition. *Let N be an A–module; then the following are equivalent:*
- *(i) N is flat*
- *(ii) $N \otimes \bullet$ preserves short exact sequences*
- *(iii) $N \otimes \bullet$ preserves injectivity*
- *(iv) For any finitely generated modules M' and M, if $f : M' \to M$ is injective, then $1 \otimes f : N \times M' \to N \otimes M$ is injective.*

Proof ($i \Leftrightarrow ii$) follows by splitting the long exact sequence into short exact sequences.
($ii \Leftrightarrow iii$) follows by right exactness (Proposition 7.6).
($iii \Rightarrow iv$) is obvious.
($iv \Rightarrow iii$). Let $f : M' \to M$ be injective and let $u = \sum x_i \otimes y_i \in \ker(f \otimes 1)$ so that $\sum f(x_i) \otimes y_i = 0$ in $M \otimes N$. TODO: prove this ∎

Example. Free modules are flat. To see this, suppose $f : M' \to M$ is injective and $F = \bigoplus_{i\in I} A$ a free A–module. We want to show $F \otimes M' \to F \otimes M$ is injective. Since tensors commute with direct sum, $F \otimes M' = \bigoplus_{i\in I}(A \otimes_A M') = \bigoplus_{i\in I} M'$, we have $1 \otimes f : \bigoplus_{i\in I} M' \to \bigoplus_{i\in I} M$. But then $1 \otimes f(x_i : i \in I) = (f(x_i) : i \in I)$.

8 Algebras

Definition. An **A-algebra** is a ring B equipped with a ring homomorphism $f : A \to B$.

This endows B with an A–module structure: if $a \in A$ and $b \in B$, then we define $ab := f(a)b$. In particular, $f : A \to B$ is a homomorphism of A–modules: if $a \in A$, $x \in A$, then $f(ax) = f(a)f(x) = af(x)$. This A–module structure on B satisfies compatibility with multiplication on B: $a(b_1 b_2) = (ab_1)b_2$.

8.1 Lemma. *Suppose B is a ring with an A–module structure such that $a(b_1 b_2) = (ab_1)b_2$. Then there is a unique ring homomorphism $f : A \to B$ inducing this module structure on B.*

Proof Define $f : A \to B$ by $f(a) = a1_B$. We just check multiplicativity:

$$f(a_1 a_2) = a_1 a_2 1_b = a_1(a_2 1_B) = a_1((1_B)(a_2 1_B)) = (a_1 1_B)(a_2 1_B) = f(a_1)f(a_2)$$ ∎

Thus A–algebras are given by A–modules which are also rings, with multiplication compatible with the module structure.

Example. Suppose $A = k$ is a field. Then a k–algebra is a ring extending k with its k–vector space structure. A ring homomorphism $f : k \to B$ is necessarily injective, so we may identify k with its image in B.

Example. If $A = \mathbb{Z}$, then every ring is canonically a $\mathbb{Z}$−algebra. Note the relationship to the module case $\mathbb{Z}$−modules to $\mathbb{Z}$−algebras as abelian groups are to (commutative, unitary) rings.

Example. For any ring A, $B = A[t_1,\dots,t_n]$, the polynomial ring over A in variables $t_1,\dots,t_n$, is naturally an A−algebra with the inclusion map.

Definition. If (B,f), (C,g) are A−algebras, then a **homomorphism of A−algebras** is a ring homomorphism $\phi : B \to C$ such that $\phi(f(a)) = g(a)$ for all $a \in A$. These are also called **A−linear (ring) homomorphisms**.

An **A−subalgebra** is a subring $C \subseteq B$ containing $f(A)$. Then an **A−subalgebra generated by x**, denoted by $A[x]$ is the smallest subalgebra of B containing x.

We say that (B,f) is a **finite A−algebra** if it is finitely generated as an A−module.

This is well-defined, we have $A[X] = \bigcap\{C \subseteq B : C \text{ subalgebra containing } X\}$. As well, $A[x] = \{p(b_1,\dots,b_n) : n \geq 0, p \in [t_1,\dots,t_n], b_i \in X\}$.

Example. $\mathbb{Q}[t]$, polynomial ring is f.g. as a $\mathbb{Q}$−algebra, but not as a $\mathbb{Q}$−vector space.

8.2 Proposition. *Finite algebras are finitely generated.*

Proof Suppose B is a finite A−algebra with algebra structure given by $f : A \to B$. Let $b_1,\dots,b_n \in B$ which generate B as an A−module. Consider $A[b_1,\dots,b_n] \subseteq B$. Then if $b \in B$ is arbitrary, $b = a_1b_1 + \cdots + a_nb_n$ for some $a_1,\dots,a_n \in A$. Each $a_ib_i \in A[b_1,\dots,b_n]$, so $b \in A[b_1,\dots,b_n]$ and $B = A[b_1,\dots,b_n]$. ■

Example. $\mathbb{Q}[t]/I$ where $I = (p(t))$ is any polynomial is a finite $\mathbb{Q}$−algebra by the division algorithm. In particular, $\mathbb{Q}[t]/I = \operatorname{span}_{\mathbb{Q}}(t^{n-1}+I,\dots,t+I,1+I)$ where $n = \deg p$.

Remark. If B is an A−algebra and $I \subseteq B$ an ideal, then B/I has a canonical A−algebra structure $\phi : A \xrightarrow{f} B \xrightarrow{\pi} B/I$.

Definition. If B is an A−algebra, $I \subseteq A$ an ideal, then the **extension ideal** IB is the ideal generated by $f(I)$ in B. If $J \subseteq B$ is an ideal, then the **contraction ideal** is $J \cap A := f^{-1}(J)$.

Remark. When $A \subseteq B$ and $\iota : A \to B$ is an A−algebra, the extension and contraction ideals are exactly what the notation suggests.

8.3 Lemma. *If (B,f) is a finitely generated A−algebra, then $B \cong A[t_1,\dots,t_n]/I$ where $t_1,\dots,t_n$ are indeterminants and $I \subseteq A[t_1,\dots,t_n]$ an ideal.*

Proof Let $b_1,\dots,b_n$ generate B. Define $\phi : A[t_1,\dots,t_n] \to B$ by $t_i \mapsto b_i$, $a \mapsto f(a)$. There is an A−algebra homomorphism

$$\begin{tikzcd} A[t_1,\dots,t_n] \arrow[r, "\phi"] & B \\ A \arrow[u, hook] \arrow[ur, "f"'] & \end{tikzcd}$$

Let $b \in B$, then $b = P(b_1,\dots,b_n)$ for some $P \in A[t_1,\dots,t_n]$. Since $b_1,\dots,b_n$ generate B as an A−algebra, $\phi(P(t_1,\dots,t_n)) = P(b_1,\dots,b_n)$, so ϕ is surjective. Let $I = \ker(\phi)$. By the first isomorphism theorem for rings, $A[t_1,\dots,t_n]/I \cong B$ as rings, the isomorphism $P(t_1,\dots,t_n)+I \mapsto P(b_1,\dots,b_n)$ is A−linear. ■

Extension and Restriction by Scalars

Let (B,f) be an A–algebra and M an A–module. Since (B,f) is also a module, we can consider $M_B = B \otimes_A M$ as an A–module. Then M_B has a natural B–module structure given by

$$b \cdot \left(\sum_i b_i \otimes x_i \right) := \sum_i b b_i \otimes x_i$$

This makes M_B a B–module which we call it the **extension by scalars** of M.

We can also go the other way: suppose N is a B–module. Then, it is naturally an A–module via $ax := f(a)x$. This A–module is called the **restriction of scalars** of N.

Tensor Products of Algebras

Let (B,f), (C,g) A–algebras. Then $B \otimes_A C$ is a B–module and a C–module. Thus we can define

$$b \cdot \left(\sum_i b_i \otimes c_i \right) = \sum_i b b_i \otimes c_i$$
$$c \cdot \left(\sum_i b_i \otimes c_i \right) = \sum_i b_i \otimes c c_i$$

In fact, $D := B \otimes_A C$ is a B–algebra and a C–algebra. Put a ring structure on D by

$$(b_1 \otimes c_1)(b_2 \otimes c_2) = b_1 b_2 \otimes c_1 c_2$$
$$\left(\sum_{i=1}^{n} b_i \otimes c_i \right) \left(\sum_{j=1}^{l} b'_j \otimes c'_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{l} b_i b'_j \otimes c_i c'_j$$

We need to check:
- well-definedness
- ring axioms
- $B \to B \otimes_A C$ by $b \mapsto b \otimes 1$ is a ring homomorphism
- $C \to B \otimes_A C$ by $c \mapsto 1 \otimes c$ is a ring homomorphism

Having verified these things, we note that $B \otimes_A C$ has an A–algebra structure with $A \to B \otimes_A C$ given by $a \mapsto f(a) \otimes 1 = 1 \otimes g(a)$. In other words, the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "g"'] & B \arrow[r] & B \otimes_A C \arrow[d, "\mathrm{id}"] \\ & C \arrow[r] & B \otimes_A C \end{tikzcd}$$

9 Rings of Fractions

Definition. Let A be a ring. Then we say $S \subseteq A$ is **multiplicatively closed** if $1 \in S$ and whenever $s, t \in S$, $st \in S$ as well.

On $A \times S$, we define an equivalence relation by $(a,s) \equiv (a',s')$ if $(s'a - sa')t = 0$ for some $t \in S$. It is easy to verify that this is reflexive and symmetric. To see transitivity, if $(a,s) \equiv (b,t)$ and $(b,t) \equiv (c,u)$, then $(at - bs)v = 0$, $(bu - ct)w = 0$ for some $v, w \in S$. Then $atvuw - bsvuw = 0$ and $buwsv - ctwsv = 0$, so $(av - sc)tvw = 0$ where $tvw \in S$, so $(a,s) \equiv (c,v)$. We denote the class (a,s) by $\frac{a}{s}$. We say that

$$S^{-1}A := A \times S \big/ \sim \; = \left\{ \frac{a}{s} : a \in A, s \in S \right\}$$

We make this into a ring by taking $0 = 0/1$ and $1 = 1/1$ and defining

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

One can verify that this is well-defined and defines a commutative unitary ring structure on $S^{-1}A$ such that the map $\alpha : A \to S^{-1}A$ given by $a \mapsto a/1$ is a ring homomorphism (not necessarily injective). We call this the **ring of fractions of A with respect to S**. In fact, $(S^{-1}A, \alpha)$ is an A–algebra.

Remark. If A is an integral domain and $0 \notin S$, then $\frac{a}{s} = \frac{b}{t}$ if and only if $at = bs$. If $S = A \setminus \{0\}$, which when A is an integral domain is multiplicatively closed, then $S^{-1}A = \mathrm{Frac}(A)$. In this case, α is indeed injective.

In general, $\ker(\alpha) = \{a \in A : \exists v \in S : av = 0\}$.

Remark. $0 \in S$ if and only if $S^{-1}A = (0)$. If $s \in S$, in $S^{-1}A$, $1/s$ is a unit since $\frac{1}{s} \cdot \frac{s}{1} = \frac{s}{s} = 1$.

9.1 Proposition. (Universal Property of Fractions) *Suppose $f : A \to B$ is a ring homomorphism such that $f(s) \in B^\times$ for all $s \in S$. Then there is a unique ring homomorphism $g : S^{-1}A \to B$ such that the following commutes:*

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "a \mapsto \frac{a}{1}"'] & B \\
S^{-1}A \arrow[ur, "g"'] &
\end{tikzcd}$$

Proof Define $g(a/s) := f(a) \cdot f(s)^{-1}$. One can verify that g is well-defined and a ring homomorphism. ■

9.2 Corollary. *α is an isomorphism if and only if $S \subseteq A^\times$.*

Localization

Note that $P \subseteq A$ is a prime ideal if and only if $S := A \setminus P$ is multiplicatively closed. We write $A_P := S^{-1}A$ and call it the **localisation of A at P**.

9.3 Proposition. *A_P is a local ring (it has a unique maximal ideal).*

Proof Consider the ideal in A_P generated by $\{a/1 : a \in P\} =: PA_P$. One can verify that

$$PA_P = \left\{ \frac{a}{s} : a \in P, s \notin P \right\}$$

If $\frac{a}{s} \in A_P \setminus PA_P$, then $a \notin P$ so $a \in S$ so that $\frac{s}{a} \in A_P$. Then $s/a = (a/s)^{-1}$, so $a/s \in (A_P)^\times$. If $I \subseteq A_P$ is an ideal and $I \not\subseteq PA_P$, then A must contain a unit and $I = A_P$. This means that every proper ideal of A_p is contained in PA_P so that A_P is a local ring with a unique maximal ideal PA_P. ■

Example. Consider $A = \mathbb{Z}$, p a prime number, $P = (p)$. Then

$$\mathbb{Z}_{(p)} = \left\{ \frac{r}{s} : r,s \in \mathbb{Z}, \gcd(r,s) = 1, p \nmid s \right\} \subseteq \mathbb{Q}$$

Given $f \in A \setminus \{0\}$ consider $S = \{1, f, f^2, \dots,\}$ and define $A_f := S^{-1}A$. This is the **localisation of A at f**. Note that A_f is not necessarily a local ring. If f is a unit, then f^n is a unit for all n and $A_f \cong A$ via α.

Modules of Fractions

Let A be a ring and $S \subseteq A$ a multiplicatively closed set. If M is an A–module, we can define an $S^{-1}A$–module structure on $S^{-1}M$ as follows.

On $M \times S$, define an equivalence relation $(x,s) \sim (x',s')$ if there exists $t \in S$ such that $t(s'x - sx') = 0$. Denote the equivalence class of (x,s) by x/s, and define $S^{-1}M := M \times S/\!\sim$ with operations

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st}, \qquad \frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}$$

Example. Recall that if A is an integral domain and $S = A \setminus \{0\}$, then $S^{-1}A = \mathrm{Frac}(A) = A_{(0)}$. Then M is an A–module and $S^{-1}M$ is a $\mathrm{Frac}(A)$–vector space.

9.4 Proposition. *S^{-1} is an exact covariant functor on A–modules.*

Proof S^{-1} acts on A–linear maps as follows. Let $f : M \to N$ be an A–module homomorphism. Then we define $S^{-1}f : S^{-1}M \to S^{-1}N$ by $\frac{x}{s} \mapsto \frac{f(x)}{s}$. One must check

1. $S^{-1}f$ is well-defined,
2. $S^{-1}f$ is $S^{-1}A$-linear, and
3. if $M \xrightarrow{f} N \xrightarrow{g} K$, then

$$S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f \qquad\qquad S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}K$$

To verify exactness, suppose $M \xrightarrow{f} N \xrightarrow{g} K$ is exact. Consider

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

Since $\mathrm{im}(f) \subseteq \ker(g)$, $g \circ f = 0$. Thus $0 = S^{-1}(g \circ f) = S^{-1}(g) \circ S^{-1}(f)$, so $\mathrm{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$.

Conversely, if $\frac{m}{s} \in \ker(S^{-1}g)$ with $m \in N$, then $0 = S^{-1}g\left(\frac{m}{s}\right) = \frac{g(m)}{s}$. Thus $tg(m) = 0$ for some $t \in S$, so $g(tm) = 0$. Thus $tm \in \ker(g) \subseteq \mathrm{im}(f)$ and $tm = f(x)$ for some $x \in M$. Then $\frac{m}{s} = \frac{tm}{ts} = \frac{f(x)}{ts} = S^{-1}f\left(\frac{x}{ts}\right)$ and $\frac{m}{s} \in \mathrm{im}(s^{-1}f)$. ■

9.5 Corollary.
1. *Let $N \subseteq M$ a submodule, and $\iota : N \to M$ the inclusion map. Then $S^{-1}\iota : S^{-1}N \to S^{-1}M$ is injective, so we may identify $S^{-1}N$ with its image so $S^{-1}N \subseteq S^{-1}M$ as submodules.*
2. *If $N \leq M$ is a submodule, then $S^{-1}\left(M/N\right) \cong S^{-1}M \big/ S^{-1}N$.*
3. *If N, P are submodules of M, then $S^{-1}(N+P) = S^{-1}N + S^{-1}P$.*

4. *If N, P submodules of M, $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.*

Proof 1. (No proof needed)
2. Since $0 \to N \to M \to M/N \to 0$ is exact, so is $0 \to S^{-1}M \to S^{-1}M \to S^{-1}(M/N) \to 0$. Then $S^{-1}(M/N) \cong S^{-1}M\big/S^{-1}N$.
3. Clearly $\frac{x+y}{s} \in S^{-1}(N+P)$ if and only if $\frac{x}{s} + \frac{y}{s} \in S^{-1}N + S^{-1}P$.
4. TODO: am I missing something? Immediate from definition? ∎

9.6 Proposition. *Let M be an A–module, $S \subseteq A$ multiplicatively closed. Then $S^{-1}M \cong M \otimes_A S^{-1}A$ as $S^{-1}A$–modules.*

Proof Let's first prove there exists an A–linear isomorphism. Consider the map $M \times S^{-1}A \to S^{-1}M$ by $(x, a/s) \mapsto (ax)/s$. This map is A–bilinear, so we get an A–linear homomorphism $f : M \otimes_A S^{-1}A \to S^{-1}M$ with $m \otimes \frac{a}{s} \mapsto \frac{ma}{s}$. Surjectivity is clear. To see injectivity, note that all elements of $M \otimes_A S^{-1}A$ are pure tensors:

$$\sum_{i=1}^{l}\left(x_i \otimes \frac{a_i}{s_i}\right) = \sum_{i=1}^{l}\left(x_i \otimes \frac{a_i t_i}{t}\right) = \sum_{i=1}^{l}\left(a_i t_i x_i \otimes \frac{1}{t}\right) = \left(\sum_{i=1}^{l} a_i t_i x_i\right) \otimes \frac{1}{t}$$

where $t = s_1 \cdots s_l$ and $t_i = t/s_i$. Now if $x \otimes \frac{a}{s} \in \ker(f)$, then $\frac{ax}{s} = 0$ so get r so $rax = 0$. Thus $x \otimes \frac{a}{s} = rax \otimes \frac{1}{rs} = 0$.

Thus f is an A–linear isomorphism and one can check that it is $S^{-1}A$–linear. ∎

9.7 Corollary. *$S^{-1}A$ is a flat A–algebra, i.e. $\otimes S^{-1}A$ is exact.*

Proof Suppose $M' \to M \to M''$ is exact; since S^{-1} is exact, the diagram

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

commutes. ∎

This gives many examples of flat and not free A–algebras.

Example. $\mathbb{Q}$ is a flat but not free $\mathbb{Z}$–algebra. If $\frac{r}{s} \in \mathbb{Q}$, then $s \cdot \frac{r}{s} - r \cdot 1 = 0$, so $\{r/s, 1\}$ is not $\mathbb{Z}$–linearly independent. However, $\mathbb{Q} \not\cong \mathbb{Z}$ as $\mathbb{Z}$–modules, so it cannot be free.

Remark. If $I \subseteq A$ is an ideal, recall that I is naturally an A–module. In particular, $IS^{-1}A = S^{-1}I = \{a/s : a \in I\}$. To see this, it is straightfoward to verify that $IS^{-1}A \cong I \otimes_A S^{-1}A$ via the map

$$\sum b_i \cdot \frac{a_i}{s_i} \mapsto \sum b_i \otimes_A \frac{a_i}{s_i}$$

9.8 Proposition. *Let $S \subseteq A$ be multiplicatively closed. Then*

(i) Every ideal of $S^{-1}A$ is an extension ideal.

(ii) If $I \subseteq A$ is an ideal, then $A \cap (S^{-1}I) = \bigcup_{s \in S}(I : s)$ where $(I : s) := \{x \in A : sx \in I\}$.

(iii) $I \subseteq A$ is a contraction ideal if and only if no element of S/I is a zero divisor in A/I. In particular, if $P \in \mathrm{Spec}(A)$, then P is a contraction if and only if $P \cap S \neq \emptyset$.

(iv) We have a bijective correspondence

$$\begin{aligned} \{P \in \operatorname{Spec}(A) : P \cap S = \emptyset\} &\longleftrightarrow \operatorname{Spec}(S^{-1}A) \\ P &\longmapsto S^{-1}P \\ Q \cap A &\longleftarrow\!\shortmid\; Q \end{aligned}$$

Proof (i) In fact, we show that if $J \subseteq S^{-1}A$, then $J = (J \cap A)S^{-1}A$. Suppose $\frac{x}{s} \in J$, so $\frac{x}{1} = s \cdot \frac{x}{s} \in J$ and $x \in J \cap A$, so $\frac{x}{s} \in S^{-1}(J \cap A)$. If $\frac{x}{s} \in S^{-1}(J \cap A)$, then $x \in J \cap A$ so $\frac{x}{1} \in J$, so $\frac{x}{s} = \frac{1}{s} \cdot \frac{x}{1} \in J$.

(ii) Let $x \in I \cap (S^{-1}I)$, so $\frac{x}{1} \in S^{-1}I$ and $\frac{x}{1} = \frac{a}{s}$. The $tsx = ta$ for some $t \in S$, so $tsx \in I$ and $x \in (I : ts)$. Thus $A \cap (S^{-1}I) \subseteq \bigcup_{s \in S}(I : s)$.

Conversely, suppose $x \in (I : s)$ for some $s \in S$. Then $sx \in I$, so $\frac{x}{1} = \frac{sx}{x} \in S^{-1}I$, so $x \in S^{-1}I \cap A$.

(iii) Suppose $I = J \cap A$ for some $J \subseteq S^{-1}A$ ideal. Then $S^{-1}I \subseteq J$, so $A \cap S^{-1}I \subseteq A \cap J = I$. Conversely, $I \subseteq A \cap S^{-1}I$. This proves the "in this case clause".

Now I is a contraction ideal iff $I = S^{-1}I \cap A$ iff $I = \bigcup_{s \in I}(I : s)$ iff for all $x \in A$ and $s \in S$, if $sx \in I$, then $x \in I$ iff $s + I$ is not a zero divisor in A/I for any $s \in S$. ■

IV. Zariski Topology

Let A be a ring and $X = \mathrm{Spec}(A)$ be the set of all prime ideals in A. For any $E \subsetneq A$ (not necessarily an ideal), we write $V(E) = \{P \in \mathrm{Spec}(A) : P \cap E = \emptyset\}$. If $f \in A$, we say $D_f = V(f)^c$.

9.9 Proposition. *(i) If $I = (E)$ is the ideal generated by E, then $V(E) = V(I) = V(\sqrt{I})$.*

(ii) $V(0) = \mathrm{Spec}(A)$, $V(1) = \emptyset$.

(iii) If $\{E_i\}_{i \in I}$ is a family of subsets in A, then

$$V\left(\bigcup_{i\in I} E_i\right) = V\left(\sum_{i\in I} E_i\right) = \bigcap_{i\in I} V(E_i)$$

(iv) $V(I \cap J) = V(IJ) = V(I) \cup V(J)$.

In particular, this means that the sets $V(E)$ satisfy the axioms of closed sets in a topological space. The resulting topology is called the **Zariski topology** and $\mathrm{Spec}(A)$ is a topological space.

9.10 Proposition. *(i) $\mathrm{Spec}(A)$ is generated by $\{D_f : f \in A\}$.*

(ii) $D_f \cap D_g = D_{fg}$

(iii) $D_f = \mathrm{Spec}(A)$ if and only if f is a unit.

(iv) $D_f \subseteq D_g$ if and only if $\sqrt{(f)} \subseteq \sqrt{(g)}$.

(v) D_f is compact (in particular, $\mathrm{Spec}(A)$ is compact).

(vi) $U \subseteq \mathrm{Spec}(A)$ is compact if and only if $U = \bigcup_{i=1}^n D_{f_i}$.

Proof Will do later. ■

9.11 Proposition. *$V(I)$ is homeomorphic to $\mathrm{Spec}(A/I)$. A_f is homemorphic to $V(A \setminus S)$ where $S = \{1, f, f^2, \ldots\}$.*

Zariski Topology

Let A be a ring, and $\mathrm{Spec}(A)$ is the set of all prime ideals of A. Put a topology on $\mathrm{Spec}(A)$: given $E \subseteq A$ a subset, let $V(E) := \{P \in \mathrm{Spec}(A) : P \supseteq E\} \subseteq \mathrm{Spec}(A)$. These are the **Zariski closed** sets. Then $V(0) = \mathrm{Spec}(A)$ is closed, $V(1) = \emptyset$ is closed, $\bigcap_{i\in I} V(E_i) = V(\bigcup_{i\in I} E_i)$. By primality,

$$\begin{aligned}
V(E) \cup V(F) &= V(E \cdot A) \cup V(F \cdot A) \\
&\supseteq V((E \cdot A) \cdot (F \cdot A)) \\
&\supseteq V((E \cdot A) \cap (F \cdot A)) \\
&\supseteq V(E) \cup V(F)
\end{aligned}$$

and equality holds. Thus this defines a topology on $\mathrm{Spec}(A)$, and these are called Affine schemes.

9.12 Proposition. *Let $P \in \operatorname{Spec}(A)$ and $f \notin P$, $Q \in \operatorname{Spec}(A_f)$.*

1. *PA_f is prime in A_f.*
2. *$\alpha^{-1}(PA_f) = P$.*
3. *$(\alpha^{-1}Q)A_f = Q$.*

Proof 1. Suppose $\frac{a}{f^n} \cdot \frac{b}{f^m} = \frac{c}{f^l}$ were $c \in P$. Then $f^{l+r}ab = f^{n+m+r}c$ for some r (in $S^{-1}A$, $\frac{a}{s} = \frac{b}{t}$ if and only if $atu = bsu$ for some $u \in S$). Since $f^{l+r}ab \in P$, $ab \in P$ so $a \in P$ or $b \in P$. Thus $\frac{a}{f^n}$ or $\frac{b}{f^m}$ is in PA_f.

2. $\alpha(P) \subseteq PA_f$, so $P \subseteq \alpha^{-1}(PA_f)$. Conversely, suppose $a \in \alpha^{-1}(PA_f)$. Then $\frac{a}{1} = \frac{b}{f^n}$ for $b \in P$, $n \geq 0$. Then $f^{n+r}a = f^r b$ for some $r \geq 0$, so $f^{n+r}a \in P$ so $a \in P$ since $f \notin P$.

3. Certainly $\alpha^{-1}(Q)A_f$ is the ideal in A_f generated by $\alpha(\alpha^{-1}(Q)) \subseteq Q$, so $\alpha^{-1}(Q)A_f \subseteq Q$. Conversely, let $\frac{a}{f^n} \in Q$. In A_f, Q is prime and $\frac{1}{f^n}$, so $\frac{1}{f^n} \notin Q$. Then since $\frac{a}{f^n} \in Q$, $\alpha(a) = \frac{a}{1} \in Q$ and $a \in \alpha^{-1}(Q)$. ■

Remark. If $f \in P$, then $PA_f = A_f$.

We have associations $\operatorname{Spec}(A)/V(f) \leftrightarrow \operatorname{Spec}(A_f)$ with $P \mapsto PA_f$, $\alpha^{-1}(Q) \leftarrow Q$. These are inverses to each other, so this is a bijective correspondence. This bijection is a homeomorphism with respect to the (induced) Zarisky topology (exercise). We identify $\operatorname{Spec}(A) \setminus V(f) = \operatorname{Spec}(A_f)$. For fixed prime p, $\bigcap_{f \in P} \operatorname{Spec}(A) \setminus V(f) = \bigcap_{f \notin P} \operatorname{Spec}(A_f) = \operatorname{Spec}(A_p)$. If $f, g \notin P$, then $fg \notin P$. $p \in \operatorname{Spec}(A_f) \cap \operatorname{Spec}(A_f)$.

$$\{\operatorname{Spec}(A_f) : f \notin P\}$$

is the set of all basic open sets containing P, and $\operatorname{Spec}(A_p)$ is the intersection of all these.

V. Primary Decomposition

10 Radicals and Ideal Quotients

Definition. Let $I, J \leq A$ be ideals. We define the **ideal quotient** $(I : J) = \{x \in A : xJ \subseteq I\}$. If $J = (a)$ is a principal ideal, then we write $(I : (a)) = (I : a)$.

Remark. Note that $\mathrm{Ann}_A(I) = (0 : I)$.

10.1 Proposition. *(i) If $K \subseteq I$, then $(K : J) \subseteq (I : J)$. If $K \subseteq J$, then $(I : K) \supseteq (I : J)$*
(ii) $(I : J) = \mathrm{Ann}_A((I + J)/I)$
(iii) $(I : J)J \subseteq I \subseteq (I : J)$
(iv) $((I : J) : K) = (I : JK) = ((I : K) : J)$
(v) $(\bigcap_i I_i : J) = \bigcap_i (I_i : J)$
(vi) $(I : \sum_i J_i) = \bigcap_i (I : J_i)$

Proof (i) Immediate.
(ii) If $x \in (I : J)$, then $xJ \subseteq I$ so that $x(I+J) = xI+xJ \subseteq I$ and $x \in \mathrm{Ann}_A((I+J)/I)$. Conversely, if $x \in \mathrm{Ann}_A((I + J)/I)$, then for any $y \in J$, $0 + y \in I + J$ so $x(0 + y) = xy \in I$.
(iii) Suppose $x \in (I : J)K$ so that $x = \sum_{i=1} rx_i y_i$ with $x_i \in (I : J)$ and $y_i \in J$. Then $x_i y_i \in I$, so $x \in I$. Then, $xJ \subseteq I$ since I is an ideal.
(iv) Let $x \in ((I : J) : K)$, so that $xK \subseteq (I : J)$. Equivalently, for any $y \in K$ and $z \in J$, $x(yz) \in I$. Then if $\sum_{i=1}^r y_i z_i \in JK$, $x \sum_{i=1}^r y_i z_i = \sum_{i=1}^r x(y_i z_i) \in I$, so $x \in (I : JK)$.
Conversely, if $x \in (I : JK)$, then for any $y \in J$ and $z \in K$, then $x(yz) \in I$, so that $xy \in (I : J)$
(v) Let $x \in (\bigcap_i I_i : J)$. Then for any $y \in J$, $xy \in I_i$ for any i, so $x \in (I_i : J)$ for all i.
Conversely, if $x \in (I_i : J)$ for all i, then $xJ \in \bigcap_i I_i$.
(vi) If $x \in (I : \sum_i J_i)$, then for any i and $y \in J_i$, $y \in \sum_i J_i$ so $xy \in I$. Thus $x \in (I : J_i)$ for any i.
Conversely, if $x \in (I : J_i)$ for any i, then for any $y = \sum_{i=1}^r y_i \in \sum_i J_i$, $xy = \sum_{i=1}^r xy_i$ and each $xy_i \in I$ so $xy \in I$. ■

Definition. We say an element $x \in A$ is **nilpotent** if there exists $n \in N$ such that $x^n = 0$. The **nilradical** $\mathrm{Nil}(A) \subseteq A$ is the set of all nilpotent elements. If $I \leq A$, then the **radical** of the ideal is $\sqrt{I} = \{x \in A : x^n \in I \text{ for some } n > 0\}$.

10.2 Proposition. *(i)* $\mathrm{Nil}(A)$ *is an ideal in A*
(ii) $A/\mathrm{Nil}(A)$ *has no non-zero nilpotent elements.*
(iii) $\mathrm{Nil}(A) = \bigcap_{P \in \mathrm{Spec}(A)} P$.

Proof (i) If $x \in \mathrm{Nil}(A)$, certainly $ax \in \mathrm{Nil}(A)$ for any $a \in A$. If $x, y \in \mathrm{Nil}(A)$, get n, m so that $x^n = y^m = 0$. Then $(x + y)^{m+n-1} = 0$ so $x + y \in \mathrm{Nil}(A)$, so $\mathrm{Nil}(A)$ is an ideal.
(ii) Let $x + \mathrm{Nil}(A) \in A/\mathrm{Nil}(A)$. Then $(x + \mathrm{Nil}(A))^n = 0$ implies $x^n \in \mathrm{Nil}(A)$ so that $x^{nm} = 0$ for some m. But then $x \in \mathrm{Nil}(A)$ so $x + \mathrm{Nil}(A) = 0$.

(iii) The forward direction is clear: for any $P \in \operatorname{Spec}(A)$, if $x \in \sqrt{I}$, then $x^n = 0 \in P$ so $x \in P$ by primality.
By contrapositive, suppose $x \in A \setminus \sqrt{(0)}$. Consider $A_x := S^{-1}A$ where $S = \{1, x, x^2, \ldots\}$. Since $x^n \neq 0$ for all $n \in \mathbb{N}$, we have $0 \notin S$ so that $A_x \neq \{0\}$. Now let $\alpha : A \to A_f$ be the canonical map and let $Q \in \operatorname{Spec}(A_f)$ be prime. Then $P := \alpha^{-1}(Q) \leq A$ is prime and disjoint from S and $x \in P$. ∎

10.3 Corollary. *Let $I \leq A$, and recall that $V(I) = \{P \in \operatorname{Spec}(A) : P \supset I\}$. Then $\sqrt{I} = \bigcap_{P \in V(I)} P$.*

Proof From (iii) above, $\sqrt{(0)} = \bigcap_{P \in \operatorname{Spec}(A/I)} P$. Now, note that $\sqrt{I} = \{x \in A : x^n \in I\} = \{x \in A : x + I \in \operatorname{Nil}(A/I)\}$. Thus if $x \in \sqrt{I}$, then $x + I \in \operatorname{Nil}(A/I)$. ∎

Remark. If $\pi : A \to A/I$ is the quotient map, then $\sqrt{I} = \pi^{-1}(\operatorname{Nil}(A/I))$.

10.4 Proposition. *(i) $\sqrt{I} \supseteq I$*
(ii) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
(iii) $\sqrt{I} = (1)$ iff $I = (1)$
(iv) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$
(v) If P is prime, then $\sqrt{P^n} = P$.

11 Temporary Result Summary

All results presented with $\mathbb{Z}$−analogue.

11.1 Proposition. *Powers of maximal ideals are primary.*

Proof Let $m \subseteq A$ be a maximal ideal. Let $n \geq 1$, and consider A/m^n Then A/m^N is local with maximal ideal m/m^n. To see this, note that $\sqrt{m^n} = m$ implies $\sqrt{0} = m + m^n$ and $m + m^n$ is maximal in A/m^n. But $\sqrt{0} = \cap \operatorname{Spec}(A/m^n)$. Thus $m + m^n$ is the only maximal ideal of A/m^n
If $x + m^n \in A/m^n$, either $x \in m$, so $(x + m^n)^n = 0$ is nilpotent, or $x \notin m$, so $x + m^n$ is a unit in A/m^n and so not a zero divisor. Thus in A/m^n, ever zero divisor is nilpotent, so m^n is primary. ∎

Remark. The proof shows that if $I \subseteq A$ with $\sqrt{I}$ maximal, then I is primary. Thus Q primary implies $\sqrt{Q}$ is prime, and $\sqrt{Q}$ maximal implies Q is primary.

Definition. If Q is primary, let $P = \sqrt{Q}$. We say Q is **P-primary**.

11.2 Lemma. *Suppose $Q_1, \ldots, Q_n$ are P−primary ideals. Then $Q_1 \cap \cdots \cap Q_n$ is P−primary.*

Proof $\sqrt{Q_1 \cap \cdots \cap Q_n} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_n} = P \cap \cdots \cap P = P$ Suppose $xy \in Q_1 \cap \cdots \cap Q_n$ with $x \notin \mathbb{Q}_1 \cap \cdots \cap Q_n$. Then for some i, $x \notin \mathbb{Q}_i$, so $y \in \sqrt{Q_i} = P = \sqrt{Q_1 \cap \cdots \cap Q_n}$. Thus $Q_1 \cap \cdots \cap Q_n$ is primary ∎

Definition. A **primary decomposition** of an ideal I is an expression of the form $I = Q_1 \cap \cdots \cap Q_n$, where each Q_i is primary.

Remark. We'll see later than in a noetherian ring, every ideal has a primary decomposition.

1. If $\sqrt{Q_i} = \sqrt{Q_j}$, then by the lemma, $Q_i \cap Q_j$ is primary with some radical. Thus by grouping these together, we can produce a primary decomposition of I where $\sqrt{Q_i} \neq \sqrt{Q_j}$ for all i, j.

2. If $Q_i \supseteq \bigcap_{j \neq i} Q_j$, then we can drop Q_i and still have a primary decomposition.

Definition. We say that $I = Q_1 \cap \cdots \cap Q_n$ is an **independent primary decomposition** if each Q_i is P_i-primary such that
1. $P_i \neq P_j$ for $i \neq k$
2. $Q_i \not\supseteq \bigcap_{j \neq i}$ for any i.

If I has a primary decomposition, then it has an irredundant primary decomposition.

11.3 Theorem. (First Uniqueness) *If $I = Q_1 \cap \cdots \cap Q_n$ is an irredundant primary decomposition, then $\{\sqrt{Q_1}, \sqrt{Q_2}, \dots, \sqrt{Q_n}\}$ is independent of the particular irreducible decompsition. Thus, the number of elements in an irreducible decomposition and the set of radicals is unique.*

11.4 Lemma. *Let Q be p–primary, $x \in A$. Then if $x \notin Q$, then $Q \subseteq (Q : x) \subseteq P$ and $(Q : x)$ is P–primary.*

Proof Note that $Q \subseteq (Q : x) \subseteq P$, where the second inclusion follows since if $xy \in Q$ since $x \notin Q$, then $y \in \sqrt{Q} = 0$ by P–primariness. Suppose $yz \in (Q : x)$ but $y \notin (Q_x)$. Thus $yzx \in Q$ but $yx \notin Q$, so $z \in \sqrt{Q} = 0 = \sqrt{(Q : x)}$. Thus $Q \subseteq P \subseteq A$

If $x \notin P$, then $(Q : x) = Q$. Suppose $y \in (Q : x)$. If $y \notin Q$, then $x \in \sqrt{Q} = P$, contradiction.■

Proof Let $I = Q_1 \cap \cdots Q_n$ be an irreducible primary decomposition, and let $P_i := \sqrt{Q_i}$. We show that $\{P_1, \dots, P_n\}$ is precisely the prime ideals that appear in $\{\sqrt{(I : x)} : x \in A\}$. For any $x \in A$,

$$(I : x) = \left(\bigcap_{i=1}^{n} Q : x \right) = \bigcap_{i=1}^{n} (Q_i : x)$$

so that

$$\begin{aligned}
\sqrt{(I : x)} &= \bigcap_{i=1}^{n} \sqrt{(Q_i : x)} \\
&= \bigcap_{\substack{i=1 \\ x \notin Q_i}}^{n} \sqrt{(Q_i : x)} \\
&= \bigcap_{\substack{i=1 \\ x \notin Q_i}} x \notin Q_i, i = 1^n \sqrt{P_i} \\
&= \bigcap_{\substack{i=1 \\ x \notin Q_i}}^{n} P_i \qquad (*)
\end{aligned}$$

If $\sqrt{(I:x)}$ is prime, then $\sqrt{(I:x)} = P_i$ for some i such that $x \notin Q_i$. Conversely for $j = 1, \dots, n$, let $x \in \bigcap_{i \neq j} Q_i \setminus Q_i$; by irreducibility, $\sqrt{(I:x)} =$) by (*). Thus $\{P_1, \dots, P_n\}$ is the set of prime ideals $\{\sqrt{(I:x)} : x \in A\}$ and does not depend on the particular decomposition. ■

Example. Consider $A = k[x,y]$ and $I = (x^2, xy)$. Then $I = (x) \cap (x^2, y)$ or $I = (x) \cap (x,y)^2$. But then $\sqrt{(x)} = (x)$, $\sqrt{(x^2,y)} = (x,y)$ and $\sqrt{(x,y)^2} = (x,y)$.

Definition. If I is decomposable and $I = Q_1 \cap \cdots \cap Q_n$ is an independent primary decomposition, then $\{\sqrt{Q_1}, \dots, \sqrt{Q_n}\}$ are called the **prime ideals associated to** I. If P is associated to I, then we say P is a **minimal prime ideal of** I if it is minimal among the associated primes. Otherwise, P is called an **embedded prime** of I.

Example. In $k[x,y]$, the prime ideals associated to (x^2, y) are (x), (x,y). Then (x) is a minimal prime and (x,y) is an embedded prime.

11.5 Proposition. *Suppose I is decomposable. Then P is a minimal prime if and only if P is minimal in $V(I) := \{P \text{ prime} : P \supseteq I\}$.*

Proof Let $I = Q_1 \cap \cdots Q_n$ be an irredundant primary decomposition. Let $P_i := \sqrt{Q_i}$. Then if $P \in V(I)$, $P \supseteq Q_1 \cap \cdots \cap Q_n$ so $P \supseteq P_1 \cap \cdots \cap P_n$. Thus $P \supseteq P_j$ for soe j, and $\{P_1, \dots, P_n\} \subseteq V(I)$ and every element of $V(I)$ contains an element of $\{P_1, \dots, P_n\}$ so the minimals are equal. ■

11.6 Corollary. *If I is decomposable, then $\sqrt{I} = \bigcap\{\text{minimal primes of } I\}$.*

Proof Write $I = Q_1 \cap \cdots \cap Q_n$ so $\sqrt{I} = P_1 \cap \cdots P_n$ are associated primes, and thus the set of minimal elements among $\{P_1, \dots, P_n\}$. ■

11.7 Corollary. *Suppose I is decomposable Then $\sqrt{I}$ has an irredundant prime decomposition unique up to reordering of the prime ideals.*

Proof Let $I = Q_1 \cap \cdots Q_n$ be an irredundant primary decomposition, and let $P_1, \dots, P_l$ be the minimal primes associated to I. Then $\sqrt{I} = P_1 \cap \cdots \cap P_l$. If $P_i \supseteq \bigcap_{j \neq i} P_j$, then $P_i \supseteq P_j$ for some $j \neq i$, contradicting minimality. If $\sqrt{I} = P_1' \cap \cdots P_m'$, then (*) and (**) are both irreducible primary decompositions of $\sqrt{I}$ so $\{\sqrt{P_1}, \dots, \sqrt{P_l}\} = \{\sqrt{P_1'}, \dots, \sqrt{P_m'}\}$ and the sets are the same. ■

Geometric Significance

A Zariski closed set in Spec(A) is **irreducible** if it is not the union of two proper Zariski closed subsets.

Remark. If $P \subseteq A$ is prime, then $V(P)$ is irreducible.

Proof Suppose $V(P) = V(I) \cup V(J)$; then $V(P) = V(I \cap J)$ so $I \cap J \subseteq P$. Thus $P \supseteq I$ or $P \supseteq J$, so $V(P) \subseteq V(I)$ or $V(P) \subseteq V(J)$ so one equality must hold. ■

Let $I \subseteq A$ be decomposable, then $\sqrt{I} = P_1 \cap \cdots \cap P_l$ be an irredundant prime decomposition. Then $V(I) = V(\sqrt{I}) = V(P_1) \cup \cdots V(P_l)$, so we have written $V(I)$ as a finite union of irreducible Zariski closed subsets. Since $P_1, \dots, P_n$ are irredundant, this decomposition is irreducible.

Remark. Let $I \subseteq A$ an ideal; then I is primary if and only if (0) is primary in A/I. I is decomposable if and only if (0) is decomposable in A/I.

11.8 Proposition. *Suppose* (0) *is decomposable in A; then, the set of zero divisors in A is the union of all the prime ideals associated to (0).*

Proof Let $(0) = Q_1 \cap \cdots \cap Q_n$ be an irreducible primary decomposition. Let $D_i := \sqrt{Q_i}$ be associated primes, and D the set of zero divisors in A. We want to show $D = P_1 \cup \cdots \cup P_n$. Fix $x \in A$, $x \neq 0$. Then

$$\begin{aligned} \mathrm{Ann}(x) = (0:x) &\subseteq \sqrt{(0:x)} \\ &= \bigcap_{i=1}^{n} \sqrt{(Q_i : x)} = \bigcap_{x \notin Q_i} P_i \subseteq P_J \end{aligned}$$

for some j as $x \neq 0$ so $x \notin \bigcap_i Q_i$. Conversely, write $D = \bigcup_{x \neq 0} \mathrm{Ann}(x)$ For the converse, recall from the proof of uniquenes of the associated primes, each P_i is of the form $\sqrt{(0:x)} = \sqrt{Ann(x)} \subseteq D$ for some $x \in A$. ■

Definition. An ideal $I \subseteq A$ is **irreducible** if whenever $I = J_1 \cap J_2$ then $I = J - 1$ or $I = J_2$.

11.9 Proposition. *If A is noetherian, then every ideal is an intersection of irreducible ideals.*

Proof Let S be the set of all counterexamples. Suppose $S \neq \emptyset$, and since A is Noetherian, S has a maximal element, I. I is not irreducible, so $I = J_1 \cap J_2$, and equality certainly does not hold so by maximality $J_1, J_2 \notin S$. But then J_1 and J_2 are intersections of irreducible ideals, so $I = J_1 \cap H_2$ is also an intersection of irreducible ideals. ■

11.10 Proposition. *In a noetherian ring, every irreducible is prime.*

Proof It suffices to prove that if (0) is irreducible, then (0) is primary (since A is noetherian, so is any quotient). Suppose $xy = 0$ and $y \neq 0$, and consider $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \cdots$. By Noetheranity, this chain stabilizes after finitely many sets, so for some $N \geq 1$, $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1})$. Let's show that $(x^n) \cap (y) = (0)$. If $x \in (x^n) \cap (y)$, then $a = cy$ so $ax = cyx = 0$. Thus $a = bx^n$ and $0 = ax = bx^n x = bx^{n+1}$ so $B \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$. Thus $bx^n = 0$ so $a = 0$. ■

11.11 Corollary. *If A is noetherian, every ideal is decomposable. In particular, in* $\mathrm{Spec}(A)$, *every Zariski closed set has a (unique irredundant) decomposition into irreducible closed sets.*

Example. $\mathbb{Z}$ is a PID. $\mathbb{Q}[x_1, x_2, \ldots,]$ is a UFD but not noetherian $\mathbb{Z} \oplus \mathbb{Z}$ is a noetherian $\mathbb{Z}$−module and a noetherian ring. $\mathbb{Z}[i]$ is a PID $\mathbb{C}[x,y]$ is Noetherian (hilbert basis theorem) $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is a Noetherian $\mathbb{R}$−module and ring $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{C}$ is noetherian $\mathbb{Q}(\pi) \otimes_{\mathbb{Q}} \mathbb{Q}(\pi)$ is noetherian

11.12 Proposition. *Suppose* $0 \to N \to M \to Q \to 0$ *is an exact sequence. Then M is noetherian if and only if N and Q are noetherian.*

Proof Assume $N \leq M$ and $Q = M/N$. If M is noetherian, then $N \leq M$ is certainly noetherian and M/N is also noetherian by the correspondence theorem.

Now suppose $N, M/N$ are noetherian; we want to show ACC for M. Let $P_1 \subseteq P_2 \subseteq \cdots$ be a chain in M. Get N_1 such that the chain $P_1 \cap N \subseteq P_2 \cap N \subseteq \cdots$ stabilizes, and N_2 such that the chain $P_1/(N \cap P_1) \subseteq P_2/(N \cap P_2) \subseteq \cdots$ stabilizes, and $N = \max\{N_1, N_2\}$. Let's show that $P_{N+1} \subseteq P_N$; let $x \in P_{N+1}$. In M/N, $\overline{x} \in \overline{P_{k+1}} = .$ ■

11.13 Corollary. *If M, N are noetherian, so is $M \oplus N$.*

11.14 Corollary. *If A is noetherian and M is finitely generated A–module, then M is noetherian.*

Proof Take $0 \to N \to M \oplus N \to M \to 0$ in the first, and $0 \to P \to A^n \to A^n/P \to 0$ in the second. ■

Which of the following constructions preserve noetherian?

1. If $A \subseteq B$? Take $A = \mathbb{C}[x_1, x_2, \ldots]$, but $A \subseteq \mathrm{Frac}(A)$.
2. submodules, quotients preserve noetherian
3. If A is noetherian, then $S^{-1}A$ is noetherian (non-zero prime ideal). Use the bijection between ideals of A in S^c and ideals of $S^{-1}A$.
4. direct sums: also true
5. tensor products? not necessarily, $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{C}$ is not noetherian. Take a tower of fields $\mathbb{Q} \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subseteq \mathbb{C}$, possible since $\mathbb{C}$ has infinite transcendence degree over $\mathbb{Q}$. Define $f_i : \mathbb{C} \otimes_{\mathbb{Q}} \mathbb{C} \to \mathbb{C} \otimes_{F_i} \mathbb{C}$. This is a ring homomorphism, which is not injective but is surjective. Then $I_i := \ker(f_i)$ is an infinite ascending chain of ideals.
   If K/F is finitely generated as an F–algebra, then K/F is finite dimensional. When we say finitely generated field extension, we mean $K = F(\alpha_1, \ldots, \alpha_n)$ for (possible transcendental) α_i. Finitely generated as an F–algebra is saying $K = F[\alpha_1, \ldots, \alpha_n]$.
   We have K/F is a finitely generated field extension if and only if $K \otimes_F K$ is noetherian.

11.15 Theorem. *If A is noetherian, then so is $A[x]$.*

Proof Let $I \subseteq A[x]$ an ideal, and $J \subseteq A$ the ideal of leading coefficients of polynomials in I (exercise). Then A is noetherian implies $J = (a_1, \ldots, a_n)$ for some $a_i \in A$. For each $i = 1, \ldots, n$, let $f_i \in I$ be $f_i(x) = a_i x^{r_i} +$ (lower degree terms). Let $I' = (f_1, \ldots, f_n)$ and $R = \max\{r_1, \ldots, r_n\}$. We claim that if $f \in I$, then $f = g + h$ where $\deg g < r$ and $h \in I'$. This follows by induction on $\deg f$. If $\deg f < r$, take $h = 0$. Otherwise, suppose $\deg f \geq r$. Write $f = ax^m +$ (lower degree ters), $m \geq r = \max\{r_1, \ldots, r_n\}$. Since $a \in J$, $a = \sum_{i=1}^n b_i a_i$ for some $b_i \in A$. Fix I, so

$$\begin{aligned} b_i x^{m-r_i} f_i &= b_i x^{m-r_i}(a_i x^{r_i} + \text{(lower degree terms)} \\ &= b_i a_i x^m + \text{(lower degree terms)} \\ &= ax^m + \text{(lower degree terms)} \end{aligned}$$

so $f - \sum_{i=1}^n b_i x^{m-r_i} f_i$ has degree $< m$. By induction, $f = g + h$ whre $\deg g < r$, $h \in I'$. Thus $f = g + (h + \sum_{i=1}^n b_i x^{m-r_i} f_i)$.

Rephrased, the claim says $I = I' + I \cap A[x]_{<r}$. This is an A–submodule of $A[x]$, so $I \cap A[x]_{<r}$ is an A–submodule of $A[x]_{<r}$. Since $A[x]_{<r}$ is a finitely generated A–module, A is noetherian implies $A[x]_{<r}$ is a noetherian A–module. Thus $I \cap A[x]_{<r}$ is finitely generated as an $A[x]_{<r}$ submodule, say $g_1, \ldots, g_l \in I \cap A[x]_{<r}$. Then $I = (f_1, \ldots, f_n, g_1, \ldots, g_l)$. ■

11.16 Corollary. *If A is noetherian, every finitely generated A–algebra is noetherian.*

Proof Every finitely generated A–algebra is of the form $A[x_1,\dots,x_n]/I$. Apply HBT repeatedly to see that $A[x_1,\dots,x_n]$ is noetherian. ■

11.17 Proposition. *In a noetherian ring, if $J = \sqrt{I}$, then $J^n \subseteq I$ for some $n \geq 1$. In particular, the nilradical is nilpotent.*

Proof Set $J = (a_1,\dots,a_k)$ finitely generated as an A–module is noetherian. For each i, $a_i^{n_i} \in I$. Choose m such that $r_1 + \cdots + r_l = m$, so $r_i \geq n_i$ for each $i = 1,\dots,l$. Then J^m is the ideal generated by $b_1,\dots,b_m$ as $b_i \in J$ vary, so that

$$J^m = \left(\{a_1^{r_1} \cdots a_l^{r_l} : r_1 + \cdots + r_l = m\}\right) \subseteq I$$ ■

11.18 Corollary. *If A is noetherian, $\mathfrak{m} \subseteq A$ maximal, and $Q \subseteq A$ an ideal, TFAE:*
(i) $\mathfrak{m} = \sqrt{Q}$
(ii) *Q is $\mathfrak{m}$–primary*
(iii) *$m^n \subseteq Q \subseteq m$ for some $n > 0$.*

Proof $(i \Rightarrow ii)$ is done in general.
$(ii \Rightarrow iii)$: $\sqrt{Q} = \mathfrak{m}$ so by noetherianity, $m^n \subseteq Q$ for some $n \geq 1$.
$(iii \Rightarrow 1)$: $\sqrt{m} = \sqrt{m^n} \subseteq\subseteq \sqrt{m}$ ■

Suppose A is a ring, B is an A–algebra. hen B has various structures:
- B is a ring
- B is an A–module
- B is a B–module, and B submodules are ideals of B.

When we say B is noetherian, we mean as a B–module. That is, there is no infinite proper increasing chain of ideals.

Integrality is preserved by quotients and localising.
- If $A \subseteq B$ is an integral extension, $J \subseteq B$ is an ideal, then B/J is an integral extension with $A/J \cap A$.

  To see this, consider $A/J \cap A \hookrightarrow B/J$ from $A \xrightarrow{f} B \to B/J$. An element of B/J is of the form $\overline{b} := b + J$, with $b \in B$. By integrality, we have $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ for some $n \geq 1$, $a_i \in A$. Thus $\overline{b}^n = \overline{a_1}\overline{b}^{n-1} + \cdots + \overline{a_n} = 0$, so $\overline{a_i} \in A/J \cap A$.
- $A \subseteq B$ is integral, $S \subseteq A$ is multiplatively closed. Then $S^{-1}A \subseteq S^{-1}B$ is integral. Suppose $\frac{b}{s} \in S^{-1}B$, so $b^n + a_{n-1}b^{n-1} + \cdots + a_n = 0$ for some $n \geq 1$, $a_1,\dots,a_n \in A$. Multiplying both sides by $\frac{1}{s^n}$ in $S^{-1}B$ to get

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \frac{a_{n-2}}{s^2}\left(\frac{b}{s}\right)^{n-2} + \cdots + \frac{a_n}{s^n}$$

11.19 Proposition. *Suppose B is an integral domain and $A \subseteq B$ is integral. Then A is a field if and only if B is a field.*

Proof First suppose B is a field. Let $a \in A$, $a \neq 0$, so $a^{-1} \in B$. We want $a^{-1} \in A$. Let $b^n + a_1 b^{n-1} + \cdots + a_n - 0$ for some $n \geq 1$. Divide by b^{n-1} go get

$$b = -a_1 - \frac{a_2}{b} - \cdots - \frac{a_n}{b^{n-1}} = -a_1 - aa_2 - \cdots - a^{n-1}a_n \in A$$

Suppose A is a field, and let $b \in B$. Then $b^n + a_1 b^{n-1} + \cdots + a_n = 0$. Let's see that $a_n \neq 0$. Otherwise, $b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) = 0$, and since B ns ain integral domain $b = 0$.

Thus, divide by a_n, so that

$$b \cdot \left(-\frac{b^{n-1}}{a_n} - \frac{a_1 b^{n-2}}{a_n} - \cdots - \frac{a_{n-1}}{a_n} \right) = 1$$

so B is a field. ∎

Definition. A ring extension $A \subseteq B$, $P \in \operatorname{Spec}(A)$, $Q \in \operatorname{Spec}(B)$.

Example. $\mathbb{Q}[x]/(x^2) \supseteq \mathbb{Q}$ is integral, which is a finite $\mathbb{Q}-$vector space but not a field. We say that Q **lies above** P if $Q \cap A = P$.

11.20 Corollary. *Suppose $A \subseteq B$ is an integral extension, $P \in \operatorname{Spec}(A)$, $Q \in \operatorname{Spec}(B)$, with $Q \cap A = P$. Then P is maximal if and only if Q is maximal.*

Proof We have $A/P \hookrightarrow B/Q$ since A is integral in B. Then P is maximal iff A/P is a field iff B/Q is a field iff Q is maximal. ∎

11.21 Theorem. *Suppose $A \subseteq B$ is integral, $P \in \operatorname{Spec}(A)$. Then there exists $Q \in \operatorname{Spec}(B)$ such that $Q \cap A = P$.*

Proof Let $S = A \setminus P$. Then

$$\begin{tikzcd} A \arrow[r, "\subseteq"] \arrow[d, "S^{-1}"] & B \arrow[d, "S^{-1}"] \\ A_P \arrow[r, "\phi"] & B_P \end{tikzcd}$$

commutes, where ϕ is injective since localisation is exact. $B_P \neq 0$ since $0 \notin A \setminus P$. Let $\mathfrak{m} \subseteq B_P$ be a maximal ideal, and let $Q := \mathfrak{m} \cap B$. Then Q is disjoint for $A \setminus P$, and $Q \in \operatorname{Spec}(B)$ so $Q \cap A$ is also disjoint for $A \setminus P$ so $Q \cap A \subseteq P$.

Now, $Q \cap A = (\mathfrak{m} \cap A_P) \cap A$. Since $\mathfrak{m}$ is maximal in $B_P \supseteq A_P$, by the previous corollary, $\mathfrak{m} \cap A_P$ is maximal. But A_P is local, so $\mathfrak{m} \cap A_P = PA_P$ and $(m \cap A_P) \cap A = PA_P \cap A = P$, so $Q \cap A = P$. ∎

Remark. Consider the map $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ given by $Q \mapsto Q \cap A$ is continuous in the Zariski topology. The theorem says that if B is integral over A, then this map is surjective.

If $A \subseteq B$, then we get an induced homomorphism $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ by $Q \mapsto Q \cap A$. We say that Q **lies above** P if $Q \cap A = P$; i.e. if $f(Q) = P$. Last time, we proved that if B is integral over A, then $f : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective.

11.22 Proposition. *Let B be integral over A, $P \in \operatorname{Spec}(A)$. Suppose $Q \subseteq Q'$ are prime ideals in B lying above P. Then $Q = Q'$.*

If you fix a point in the image and look at the fibres (the preimage), then points are closed. This says that the points in the fibres at $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ points are closed. Essentially, this says that the previous proposition gives rise to all primes lying over P.

Proof As before, consider

$$\begin{array}{ccc} P \subseteq A & \xrightarrow{\subseteq} & B \supseteq Q' \supseteq Q \\ \downarrow{\scriptstyle S^{-1}} & & \downarrow{\scriptstyle S^{-1}} \\ A_P & \xrightarrow{\phi} & B_P = S^{-1}B \end{array}$$

Let's see that $QB_P \cap A_P = PA_P$. To see this, $0 \to P \to A \to B/Q$ is an exact sequence of A–modules since $Q \cap A = P$. Hence $0 \longrightarrow S^{-1}P \longrightarrow S^{-1}A \longrightarrow S^{-1}(B/Q)$ is exact since S^{-1} is exact. Thus $0 \longrightarrow PA_P \longrightarrow A_P \longrightarrow B_P/QB_P = S^{-1}(B/Q)$ is exact.

Thus QB_P in B_P lies above PA_P. But B_P is integral over A_P and PA_P is maximal in A_P, so QB_P is maximal in B_P. Similarly for $Q' \supseteq Q$, $QB_P = Q'B_P$. Since $S = A \setminus P$, $Q \cap A = P$ and $Q' \cap A = P$, so Q, Q' are disjoint from S so $Q = Q'$. ■

Suppose Q lies above P in B an integral extension of A. Given $P' \supseteq P$ a prime ideal in A¡ can we find $Q' \in \mathrm{Spec}(B)$ lying above P', and $Q' \supseteq Q$. That is, is $f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ closed?

Yes: consider $A/P \hookrightarrow B/Q$ is integral, so there exists I prime ideal in B/Q that lies above P'/P. Thus $I = Q'/Q$ for some $Q' \in \mathrm{Spec}(B)$. Then $Q'/Q \cap A/P = P'/P$, so $Q' \cap A = P'$.

11.23 Theorem. *Let B be an integral extension of A, $P \in \mathrm{Spec}(A)$, $Q \in \mathrm{Spec}(B)$, $Q \cap A = P$. If $P \subseteq P_1 \subseteq \cdots \subseteq P_l$ is a chain of prime ideals in A¡ then there is a corresponding chain of prime ideals $Q \subseteq Q_1 \subseteq \cdots \subseteq Q_l$ in B such that $Q_i \cap A = P_i$.*

Remark. By corollary 5.9, $Q \subsetneq Q_{i+1}$ if and only if $P_i \subsetneq P_{i+1}$. This can be used to prove $f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is a closed map.

11.24 Corollary. *If B is noetherian and integral over A, $P \in \mathrm{Spec}(A)$. There are only finitely many $Q \in \mathrm{Spec}(B)$ such that $Q \cap A = P$.*

Proof Let $Q \in \mathrm{Spec}(B)$ lie above P. Note that $Q \supseteq PB$. If $Q \supseteq Q' \supseteq PB$ and $Q' \in \mathrm{Spec}(B)$, then $P = Q \cap A \supseteq Q' \cap A \supseteq PB \cap A = P$. Thus $Q' \cap P$, so by the above corollary, $Q = Q'$, i.e. Q is a minimal prime containing PB. Thus Q is minimal amount the prime ideals associated to $PB \subseteq B$. Thus Q is an associated prime of PB, of which there are only finitely many. ■

11.25 Lemma. (Noether Normalisation) *Let k be an infinite field and A a finitely generated k–algebra. Then there exists algebraically independent elements $a_1, \ldots, a_r \in A$ over k such that A is integral over $k[a_1, \ldots, a_r]$.*

Remark. $a_1, \ldots, a_r$ algebraically independent over K meaus that if $f \in k[a_1, \ldots, a_r]$ and $f(a_1, \ldots, a_r) = 0$, then $f = 0$. Equivalently, $k[a_1, \ldots, a_r] \cong k[x_1, \ldots, x_r]$ as k–algebras (via $a_i \mapsto x_i$).

Proof If A is finitely generated, then $A = k[a_1, \ldots, a_n]$ for some $a_1, \ldots, a_n \in A$. We do induction on n.

If $n=1$, then $A=k[a]$. Then a ia algebraic over k and since k is a field, integral over k. Hence A is integral over K and the lemma holds with $r=0$. If a is not algebraic over k, then $\{a\}$ is algebraically independent over k. As A is integral over $A=k[a]$, we are done.

If $n>1$, $\{a_1,\dots,a_n\}$ are algebraically independent over k, then we are done, so we may assume not. Thus get $0\neq f\in k[x_1,\dots,x_n]$ such that $f(a_1,\dots,a_n)=0$. For each $0\leq l\leq d=\deg f$, let $f_l(x_1,\dots,x_n)$ be the sum of all degree L monomials of f. Then $f=f_d+f_{d-1}+\cdots+f_0$.

Claim: there exist $\lambda_1,\dots,\lambda_{n-1}\in k$ such that $f(\lambda_1,\dots,\lambda_{n-1},1)\neq 0$. If not, then for any $\gamma_1,\dots,\gamma_n\in k$, $\gamma_n\neq 0$, $f(\gamma_1,\dots,\gamma_n)=f_d(\gamma_n\frac{\gamma_1}{\gamma_n},\gamma_n\frac{\gamma_2}{\gamma_n},\dots,\gamma_n)=\gamma_n^d f_d\left(\frac{\gamma_1}{\gamma_n},\dots,\frac{\gamma_{n-1}}{\gamma_n},1\right)=0$. Also, $f_d(0,\dots,0)=0$. Thus f_d vanishes on all of k^n.

In general, if k is an infinite field and $F\in k[x_1,\dots,x_n]$ vanishes in k^n, then $F=0$. By induction on n: if $n=0$, this is clear. If $n>0$, then $F=\sum_{i=0}^D g_i(x_1,\dots,x_{n-1})x_n^i$ where $g_0,\dots,g_d\in k[x_1,\dots,x_{n-1}]$. Let $b_1,\dots,b_{n-1}\in k$, so $F(b_1,\dots,b_{n-1},x_n)\sum_{i=1}^D g_i(b_1,\dots,b_{n-1})x_n^i$ vanishes on all of k. But a single variable non-trivial polynomial has only finitely many roots. Thus $F(b_1,\dots,b_{n-1})=0$ in $k[x_n]$; that is, $g_i(b_1,\dots,b_{n-1})=0$ for all $i=0,\dots,D$. By induction, as $b_1,\dots,b_{n-1}$ was arbitrary, this implies each $g_i=0$, so $F=0$.

Thus, $f_d=0$, a contradiction for $d=\deg f$ and $f\neq 0$.

Let $\lambda_1,\dots,\lambda_{n-1}$ be as in the claim. For each $i=1,\dots,n-1$, let $b_i:=a_i-\lambda_i a_n$. Then

$$\begin{aligned}
0=f(a_1,\dots,a_n)&=f(b_1+\lambda_1a_n,\dots,b_{n-1}+\lambda_{n-1}a_n,a_n)\\
&=f_d(b_1+\lambda_1a_n,\dots,b_{n-1}\lambda_{n-1}a_n,a_n)+f_{d-1}(b_1+\lambda_1a_n,\dots,b_{n-1}\lambda_{n-1}a_n,a_n)+\cdots+f_0\\
&=f_d(\lambda_1a_n,\dots,\lambda_{n-1}a_n,a_n)+\text{lower degree terms}\\
&=a_n^d f_d(\lambda_1,\dots,\lambda_{n-1},1)+\text{lower degree } a_n \text{ terms}
\end{aligned}$$

Dividing by $f_x(\lambda_1,\dots,\lambda_{n-1},1)$, we see that a_n is integral over $k[b_1,\dots,b_{n-1}]$. By the inductive hypothesis applied to $k[b_1,\dots,b_{n-1}]$, we have $u_1,\dots,u_r\in k[b_1,\dots,b_r]$ algebraically independent over k such that $k[b_1,\dots,b_{n-1}]$ is integral over $k[u_1,\dots,u_r]$. Thus A is integral over $k[u_1,\dots,u_r]$. Thus if $i<n$, $a_i=b_i+\lambda_ia_n$, so $a_1,\dots,a_n$ areall integral over $k[u_1,\dots,u_r]$. Thus $A=k[a_1,\dots,a_n]$ is integral over $k[u_1,\dots,u_r]$. ■

Remark. Given A, we have found $k[u_1,\dots,u_r]\subseteq A$ so A is an integral extension. Last lecture, we saw that noetherian integral extensions are very nice. The first is a polynomial ring over k, and are, for example, a UFD.

Thus means $\mathrm{Spec}(A)\to\mathrm{Spec}(k[x_1,\dots,x_n])$ is a surjective, finite-to-one, continuous

Remark. If A is a finitely generated k–algebra, $A=k[y_1,\dots,y_l]/I$. This induces a continuous injective $\mathrm{Spec}(A)\hookrightarrow\mathrm{Spec}(k[y_1,\dots,y_l])=:\mathbb{A}_k^l$, bijection with $V(I)$. Why do we consider $\mathrm{Spec}(k[x_1,\dots,x_r])$ an affine space? In fact, when k is algebraically closed, k^r "is" of closed points in $\mathrm{Spec}(k[x_1,\dots,x_r])$ (the "is" statement is the weak nullstellensatz)

11.26 Proposition. *If k is an infinite field and A is a finitely generated k–algebra, $m\subseteq A$ a maximal ideal,. Then A/m is a finite algebraic extension of k.*

PROOF $k\hookrightarrow A\to A/m$. Note tht $m\cap k=(0)$ (intersection is proper ideal of k and hence (0)). Thus get an induced embedding $k\hookrightarrow A/m$. This is a field extension. The proposition claims that it is a finite algebraic extension. Since A is a finitely generated k–algebra, so is A/m. By Noether's Normalization Lemma, there is a polynomial subring $k\subseteq k[x_1,\dots,x_n]\subseteq A/m$. Since A/m is a field, $k[x_1,\dots,x_n]$ is a field, so $r=0$. Thus $k\subseteq A/m$ is integral and hence finite algebraic. ■

Remark. In particular, if k is algebraically closed and A is a finitely generated k–algebra and $m \subseteq A$ maximal, then $A/m = k$.

11.27 Corollary. (Weak Nullstellensatz) *If k is an algebraically closed field, $I \subseteq k[x_1,\dots,x_r]$ is an ideal. Then I ms maximal if and only if $I = (x - a_1,\dots,x - a_r)$ where $a_1,\dots,a_r \in k$.*

Proof ($\Leftarrow$) $k \subseteq k[x_1,\dots,x_r] \xrightarrow{\pi} k[x_1,\dots,x_r]\big/(x_1 - a_1,\dots,x_r - a_r)$. Then $\overline{x_i} = \pi(x_i)$ in k, but $\overline{x}_i = a_i$ since $\pi(x_i - a_i) = 0$. Thus $k[x_1,\dots,x_r]\big/(x_1 - a_1,\dots,x_r - a_r) = k$ a field. Then $(x_1 - a_1,\dots,x_r - a_r)$ is maximal.

($\Rightarrow$) Conversely, suppose $I \subseteq k[x_1,\dots,x_r]$ is a maximal ideal. By the proposition applied to I and $A = k[x_1,\dots,x_r]$, we have $k[x_1,\dots,x_r]/I = k$. Consider

$$k[x_1,\dots,x_n] \xrightarrow{\pi} k[x_1,\dots,x_r]\big/I = k$$

Let $a_i = \pi(x_i) \in k$ for $i = 1,\dots,r$. Then $\pi(x_i - a_i) = \pi(x_i) - a_i = 0$ (since π is a k–algbra homomorphism). Thus $(x_1 - a_1,\dots,x_r - a_r) \subseteq \ker(\pi) = I$. But as before, $(x_1 - a_1,\dots,x_r - a_r)$ is maximal, forcing equality. ■

Remark. Geometric interpretation. A point $p \in T$ is **closed** in a topological space T if $\{p\}$ is closed. The closed points of $\mathrm{Spec}(A)$ are precisely the maximal ideals. If $V(m) = \{m\}$. Conversely, suppose $P \in \mathrm{Spec}(A)$ is a closed point. Then $\{P\} = V(I)$ for some ideal $I \subseteq A$. So if $Q \supseteq P$, then $Q \supseteq I$ implies $Q \in V(I)$ implies $Q = P$ so P is maximal.

We get a bijectie correspondence

$$\text{closed points of } \mathrm{Spec}(k[x_1,\dots,x_r]) \leftrightarrow k^r$$

when k is algebraically closed, given by $(a_1,\dots,a_r) \mapsto (x_1 - a_1,\dots,x_r - a_r)$. Surjective weak nullstellensatz injective: if $(x_1 - a_1,\dots,x_r - a_r) = (x_1 - b_1,\dots,x_r - b_r)$, then in $k[x_1,\dots,x_r]/m$, $\overline{x}_i = a_i$, $\overline{x}_i = b_i$. Thus $a_i = b_i$ for $i = 1,\dots,r$.

Another formulation of WN

11.28 Corollary. *If k is an algebraically closed field, $I \subseteq k[x_1,\dots,x_r]$ an ideal. Let $Z(I) := \{(a_1,\dots,a_r) \in k^n : f(a_1,\dots,a_r) = 0 \text{ for all } f \in I\}$. Then $Z(I) \neq 0$ if and only if I is a proper ideal.*

Note that to compute $Z(I)$, we equivalently just need to compute a finite set of zeros of the generators of I, since $k[x_1,\dots,x_r]$ is noetherian.

Proof ($\Rightarrow$) If $I = k[x_1,\dots,x_n]$, then $1 \in I$ and $1 = 0$ has no solutions.

($\Leftarrow$) If I is properl, then there exists maximal $m \supseteq I$. By WN, $m = (x_1 - a_1,\dots,x_r - a_r)$ for some $a_1,\dots,a_r \in k$. If $f \in I \subseteq m$, then $f = g_1(x_1 - a_1) + \cdots + g_r(x_r - a_r)$ with $g_1,\dots,g_r \in k[x_1,\dots,x_r]$. Then $f(a_1,\dots,a_r) = 0$, i.e. $(a_1,\dots,a_r) \in Z(I)$. ■

Let $P \supseteq I$ prime, $P = (f_1,\dots,f_l)$. Want to solve $f_i(x_1,\dots,x_r) = 0$ for $i = 1,\dots,l$. Then

$$k \subseteq k[x_1,\dots,x_r] \to k[x_1,\dots,x_r]/P \subseteq \mathrm{Frac}(k[x_1,\dots,x_r]/P) = L \subseteq L^{alg}$$

In L^{alg}, this has a trivial solution. Note that the system of equations is a sentence with parameters only in k, so if it holds in L^{alg}, then it also holds in k.

Definition. Suppose K is a field. An **algebraic subset** of k^n is a set of the form

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

where $I \subseteq k[x_1,\dots,x_n]$.

Remark. This makes sense for arbitrary $x \subseteq k[x_1,\dots,x_n]$, by $Z(x) = Z((X))$. These form the closed sets of a topology on k^n, which we also call the Zariski topology. We have

$$\operatorname{Spec}(k[x_1,\dots,x_n]) \supseteq \max\operatorname{Spec}(k[x_1,\dots,x_n]) \leftrightarrow k^n affineschemesinV(I)algebraicsetsZ(I)$$

$I \mapsto Z(I)$ is a containment reversing correspondence between ideals if $k[x_1,\dots,x_n]$ and algebraic subsets of k^n.

Definition. If $X \subseteq k^n$, then

$$I(X) := \{f \in k[x_1,\dots,x_n] : f(a_1,\dots,a_n) = 0\frac{forall}{(}a_1,\dots,a_n) \in X\}$$

This is an ideal of $k[x_1,\dots,x_n]$.

Are these inverse operations? $I \subseteq I(Z(I))$ by definition, but is $I(Z(I)) \subseteq I$? No: consider $f \in \sqrt{I} \setminus I$. Then $f^l \in I$ for some $l > 0$, $(a_1,\dots,a_n) \in Z(I)$, so $f^l(a_1,\dots,a_n) = 0$. Thus $f(a_1,\dots,a_n) = 0$, so $f \in I(Z(I)) \setminus I$.

11.29 Theorem. (Hilbert's Nullstellensatz) *If k is algebraically closed, and $I \subseteq k[x_1,\dots,x_n]$ is an ideal, then $I(Z(I)) = \sqrt{I}$.*

Remark. We recover the weak Nullstellensats: if I is propert, then so is $\sqrt{I} = I(Z(I))$. If I is proper, then so is $\sqrt{I} = I(Z(I))$ so $Z(I) \neq \emptyset$.

Proof $\supseteq$ was proven above. For the converse, suppose $f \notin \sqrt{I}$ and show that $f \in I(Z(I))$. Let $P \in \operatorname{Spec}(k[x_1,\dots,x_n])$ such that $f \notin P$ and $P \supseteq I$. Consider

$$k[x_1,\dots,x_n] \longrightarrow k[x_1,\dots,x_n]/P \xrightarrow{\subseteq} \left(k[x_1,\dots,x_n]\big/P\right)_{\overline{f}} = k\left[\overline{x}_1,\dots,\overline{x}_n,\frac{1}{\overline{f}}\right] = A_{\overline{f}} \to A_{\overline{f}}\big/m = k$$

Let $\overline{f}$ be the image of $f \in k[x_1,\dots,x_m]/P$, so $\overline{f} \neq 0$. Let $\overline{x}_i$ be the image of x_i in $k[x_1,\dots,x_n]/P$. Let $A := k[x_1,\dots,x_n]/P$. Let $m \subseteq A_{\overline{f}}$ be a maximal ideal. Since $A_{\overline{f}}$ is a finitely generated k–algebra, $A_{\overline{f}}/m$ is a finite algebraic extension of k, so $A_{\overline{f}}/m = k$. Thus $\pi : k[x_1,\dots,x_n] \to k$ is a k–algebra homomorphism. Let $a_i := \pi(x_i)$, so $f(a_1,\dots,a_n) = f(\pi(x_1),\dots,\pi(x_n)) = \pi(f(x_1,\dots,x_n)) \neq 0$. On the other hand, if $g \in I \subseteq P$, then $g(a_1,\dots,a_n) = \pi(g(x_1,ldots,x_n)) = 0$, so $(a_1,\dots,a_n) \in Z(I)$. But then $f(a_1,\dots,a_n) \neq 0$, so $f \notin I(Z(I))$. ■

11.30 Corollary. $Z(I) = Z(\sqrt{I})$.

Proof $\supseteq$ is clear. For $\subseteq$, $I(Z(I)) = \sqrt{I}$, so $Z(I(Z(I))) = Z(\sqrt{I})$. Then $X \subseteq Z(I(X))$. Apply it to $X = Z(I)$ so $Z(I) \subseteq Z(I(Z(I)))$. ■

If k is an algebraically closed field, $A = k[x_1,\dots,x_n]$ a polynomia ring. Then the radical ideals of A correspond to the algebraic subsets of k^n via $I \mapsto Z(I)$ and $Z \mapsto I(Z)$.

11.31 Theorem. *The map Φ is a bijective correspondence.*

Proof If $I \subseteq k[x_1, \dots, x_n]$ is an ideal, then $I(Z(I)) = \sqrt{I} = I$ by Hilbert's Nullstellensatz. Conversely, if $Z \subseteq k^n$ an agebraic setm then $Z = Z(J)$ where $J \subseteq k[x_1, \dots, x_n]$ is an ideal. Then $Z(I(Z)) = Z(I(Z(J))) = Z(\sqrt{J}) = Z(J) = Z$. ■

there is also an association between Zariski closed subsets of $\mathrm{Spec}(A)$ and radical ideals of A via $I \mapsto V(I)$ and $V \mapsto I(V)$, where $I(V) = \bigcap_{P \in V} P$.

Proof We have $I(V(I)) = \bigcap_{P \supseteq I} P = \sqrt{I} = I$. Conversely, if $V \subseteq \mathrm{Spec}(A)$, then $V = V(J)$ for some $J \subseteq A$ ideal. Then $I(V) = I(V(J)) = \bigcap_{P \supseteq J} P = \sqrt{J}$ and $V(I(V)) = V(\sqrt{J}) = V(J) = V$. ■

Functional interpretation of the "modern" algebro-geometric convention. How do we view elements of A as functions on $\mathrm{Spec}\, A$? In such a way that $V(I)$ becomes the "vanishing locus" of I?

Given $f \in A$ and $P \in \mathrm{Spec}\, A$, what should $f(P)$ be? Recall that

$$A \longrightarrow A_p \longrightarrow A_P \big/ PA_p =: k(P)$$

and we say $f(P)$ is the image of f in $k(P)$. There is no natural codomain to this function; i.e. $f(P) \in k(P)$ which depends on P! When is $f(P) = 0$? If and only if $f \in PA_P$ if and only if $f \in P$, second iff since $PA_P \cap A = P$. Thus $V(I) = \{P \in \mathrm{Spec}(A) : P \supseteq I\} = \{P \in \mathrm{Spec}\, A : f(P) = 0 \forall f \in I\}$. In the special case $A = k[x_1, \dots, x_n]$, then $A_P/PA_P = k$ by Noether normalization lemma and image of f is $f(a_1, \dots, a_n)$.