2010

Class Notes for Math 905: Commutative Algebra, Instructor Sylvia Wiegand

Laura Lynch
University of Nebraska-Lincoln, llynch@ccga.edu

Class Notes for Math 905: Commutative Algebra, Instructor Sylvia Wiegand

Topics include: Rings, ideals, algebraic sets and affine varieties, modules, localizations, tensor products, intersection multiplicities, primary decomposition, the Nullstellensatz

Prepared by Laura Lynch, University of Nebraska-Lincoln

August 2010

1. Atiyah MacDonald, Chapter 1: Rings and Ideals

All rings are commutative with 1. We let A denote an arbitrary such ring, unless otherwise stated.

Zorn's Lemma Let $S \neq \emptyset$ be a poset. If every chain in S has an upper bound in S, then S has a maximal element.

Proposition 1.1. For I an ideal of a ring A, the correspondence $J \to J/I$ is one-to-one and onto:
$\{\text{ideals } J \text{ of } A \mid J \supseteq I\} \to \{ \text{ ideals } \overline{J} \text{ of } \overline{A} = A/I\}$.

Proposition 1.2. Let A be a non-zero ring. These are equivalent:

(1) A is a field.
(2) A has exactly two ideals, (0) and (1).
(3) If $\varphi : A \to B$ is a ring homomorphism and $B \neq \{0\}$, then φ is one-to-one.

Remarks 1.2. For I an ideal of a ring A,

(1) I is prime $\iff$ A/I is an integral domain.
(2) I is maximal $\iff$ A/I is a field.
(3) I maximal $\implies$ I is prime.
(4) If $f : A \to B$ is a ring homomorphism and $P \in \operatorname{Spec} B := \{$ prime ideals of $B\}$, then $f^{-1}(P)$ is a prime ideal of A.
(5) If $f : A \to B$ is as in (4), then f^{-1} is an order-preserving set function: $\operatorname{Spec} B \to \operatorname{Spec} A$.

Theorems 1.3,1.4, 1.5. Let A be a non-zero ring. Then

(1) A has at least one maximal ideal.
(2) If I is an ideal of A and $I \neq A$, then I is contained in some maximal ideal.
(3) If x is a non-unit of A, then $x \in \mathbf{m}$, for some maximal ideal $\mathbf{m}$.

Proof. (Of 2.) Since $I \in S$, we have $S \neq \emptyset$. Also, its a poset with partial order $\subseteq$. Let $\{I_\alpha\}_{\alpha \in B}$ be a chain in S. Let $L = \bigcup_{\alpha \in B} I_\alpha$. Then L is an ideal (as $a, b \in L$ imply $a, b \in I_\alpha$ for some α.) Clearly L is an upperbound. So by Zorn's Lemma S has a maximal element. Therefore $\exists$ a maximal ideal containing I. □

Definition. A **local ring** is a ring with a unique maximal ideal.

Example. (1) If K is a field, then $K[[x]]$ (the ring of power series with coefficients from K) is a local ring.

- (x) is maximal as $K[[x]]/(x) \cong K$, which is a field.
- If $f(x) \notin (x)$, then $f(x) = a + x(\text{stuff})$ where $a \in K$ (and thus a is a unit) which implies f^{-1} exists (exercise 5(i)) and thus $(f(x)) = K[[x]]$.
- Thus (x) is the unique maximal ideal.

(2) Let $S = \{\text{odd integers}\}$. Then $S^{-1}\mathbb{Z} = \{\frac{a}{b} | b \in S\}$ is local.

- $\{\frac{a}{b} | a \in 2\mathbb{Z}\}$ is maximal.
- Any fraction in which the numerator and denominator are both odd has an inverse in $S^{-1}\mathbb{Z}$ and thus can not be maximal.

Definition. A **semilocal ring** has finitely many maximal ideals.

Example. Let $S = \mathbb{Z} - 2\mathbb{Z} - 3\mathbb{Z}$. Then $S^{-1}\mathbb{Z}$ has 2 maximal ideals: $2S^{-1}\mathbb{Z}$ and $3S^{-1}\mathbb{Z}$.

Proposition 1.6. Let $\mathbf{m}$ be a maximal ideal of A.

(1) If I is an ideal of A such that $I \neq A$ and every $x \in A - I$ is a unit in A, then A is a local ring and $I = \mathbf{m}$.
(2) If every element of $1 + \mathbf{m} = \{1 + x \mid x \in \mathbf{m}\}$ is a unit of A, then A is a local ring.

Proposition. If R is a PID, then every nonzero prime ideal is maximal.

Proof. Let $P \neq 0$ be a prime ideal of R. Then $P = (x)$, $x \neq 0$. Suppose $P \subsetneq Q$. Then $Q = (y)$ for some y. Then $x = yr$ for some $r \in R$ which implies either $y \in P$ or $r \in P$. By assumption, $y \notin P$. Thus $r \in P$ and therefore $r = xs$ for some s. This gives $x = yxs$, i.e., $0 = x(1 - ys)$. By assumption, $x \neq 0$ and since R is an integral domain $ys = 1$. Thus y is a unit and $Q = R$. □

Definition. Let A be a ring. Define $\mathcal{N} = \{\text{nilpotent elements of } A\}$ to be the **nilradical** of A and $\mathcal{R} = \cap\{m | m \text{ is maximal}\}$ to be the **Jacobson Radical** of A.

Examples.

(1) For $\mathbb{Z}$, $J = N = (0)$.
(2) For $S^{-1}\mathbb{Z}$, (the odd denominators), $J = 2S^{-1}\mathbb{Z}$ since it is the only maximal ideal.
(3) For $\mathbb{Z}/6\mathbb{Z}$, the maximal and prime ideals are both $2\mathbb{Z}/6\mathbb{Z}$ and $3\mathbb{Z}/6\mathbb{Z}$ and so $J = N = 2\mathbb{Z}/6\mathbb{Z} \bigcap 3\mathbb{Z}/6\mathbb{Z} = (0)$.
(4) For $\mathbb{Z}/48\mathbb{Z}$, we again have that both the maximal and prime ideals are $2\mathbb{Z}/48\mathbb{Z}$ and $3\mathbb{Z}/48\mathbb{Z}$ and so $J = N = 2\mathbb{Z}/48\mathbb{Z} \bigcap 3\mathbb{Z}/48\mathbb{Z} = 6\mathbb{Z}/48\mathbb{Z}$.
(5) For $K[[x]]$ where K is a field, $J = (x)$ and $N = (0)$ (which are the only two prime ideals).

Proposition 1.7. The set $\mathcal{N} := \{$ nilpotent elements of $A\}$ is an ideal and $A/\mathcal{N}$ has no non-zero nilpotents.

Proof. (1) $\mathcal{N} \neq \emptyset$ as $0 \in \mathcal{N}$. Let $x, y \in \mathcal{N}$ and $x^n = 1$ and $y^m = 1$. Then $(x - y)^{n-m} = 0$ by the binomial theorem. Clearly, if $x^n = 0$ then $(rx)^n = 0$. Thus $\mathcal{N}$ is an ideal.
(2) Clear □

Proposition 1.8. The nilradical $\mathcal{N}$ of A satisfies $\mathcal{N} = \bigcap\limits_{P \in \operatorname{Spec} A} P$, where $\operatorname{Spec} A = \{$ prime ideals of $A\}$.

Proof. $\subseteq$: If $f \in \mathcal{N}$ then $f^n = 0 \in P$ for all P. Then $f^{n-1}f = 0$ implies f^{n-1} or $f \in P$. Either way, we can see inductively that $f \in P$.

$\supseteq$: Let $f \in P$ for all P. Suppose $f^n \neq 0$ for all $n > 0$. Let $S = \{$ideals I such that $f^n \notin I \forall n\}$. Know $S \neq \emptyset$ as $(0) \in S$. Let $\{I_\alpha\}_{\alpha \in A}$ be a chain (with respect to inclusion) in S. Let $I = \bigcup I_\alpha \in S$. This is an upper bound. Thus by Zorn's Lemma, S has a maximal element, call it J. Then $f \notin J$ implies J is not prime. Also $J \neq R$ as $f \in R$. So there exists $x, y \in R$ such that $xy \in J$ but $x, y \notin J$. Then $J + Rx$ and $J + Ry$ are ideals strictly larger than J. By maximality of J, there exists n, m such that $f^n \in J + Rx$ and $f^m \in J + Ry$. Then $f^{n+m} \in (J + Rx)(J + Ry) \subseteq J$, a contradiction. □

Note. For ideals I_1 and I_2, $I_1 \cdot I_2 = \{\sum_0^n a_{1_i} a_{2_i} : n > 0, a_{1_i} \in I_1, a_{2_i} \in I_2\}$.

Proposition 1.9. Let $x \in A$ and $\mathcal{R}$ the Jacobson radical of A. ($\mathcal{R} := \cap \mathbf{m}$, $\mathbf{m}$ max $\in \operatorname{Spec} A$.) Then
$x \in \mathcal{R} \iff 1 - xy$ is a unit of A, $\forall y \in A$.

Definition. Let $I_1, ..., I_n$ be ideals of a ring R. Consider the homomorphism $\phi : R \to \prod_{i=1}^n R/I_i$. We say $\{I_1, ..., I_n\}$ are **coprime** if for all $i \neq j$ $I_i + I_j = R$.

Example. In $\mathbb{Z}$, the ideals $2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}$ are all pairwise coprime. Thus $\phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ defines a homomorphism.

Proposition 1.10. Let $I_1, \ldots, I_n$ be ideals of A and define a ring homomorphism
$$\varphi : A \to \prod_{i=1}^n (A/I_i) \text{ by } \varphi(x) = (x + I_1, \ldots, x + I_n).$$
(1) If $I_i + I_j = A$, for all i, j with $i \neq j$, then $\prod\limits_{i=1}^n I_i = \bigcap\limits_{i=1}^n I_i$.

(2) φ is surjective $\iff I_i + I_j = A$, for all i, j with $i \neq j$.
(3) φ is injective $\iff \bigcap_{i=1}^{n} I_i = (0)$.

Proof. (Of 1) By induction. Let $n = 2$. Say I, J are coprime ideals of R. We know $IJ = I \bigcap J$. Suppose $n > 2$ Let $J = I_1 I_2 \cdots I_{n-1} = \bigcap_{i=1}^{n-1} I_i$. We want to know $JI_n = J \bigcap I_n$. If J and I_n are coprime, we're done by the $n = 2$ case. We know there exists $x_i \in I_i$ and $y_i \in I_n$ such that $x_i + y_i = 1$. Then $1 = \prod(x_i + y_i) \in J + I_n$. Thus they are coprime and we are done. □

Proposition 1.11 expanded. Let $P, P_1, \ldots, P_n$ be prime ideals of A and let $I, J_1, J_2, I_1, \ldots, I_n$ be ideals of A. Then

(1) If $I \subseteq J_1 \cup J_2 \cup \bigcup_{i=1}^{n} P_i$, then $I \subseteq J_j$, for some j, or $I \subseteq P_i$, for some i.
(2) If $P \supseteq \bigcap_{i=1}^{n} I_i$, then $P \supseteq I_i$, for some i. $P = \bigcap_{i=1}^{n} I_i \implies P = I_i$, for some i.

Proof. We will induct on n. If $n = 1$, it's trivial. So assume true for $\leq n - 1$. Assume I is not contained in any of the $n - 1$ ideals. Then there exists $a_1 \in I\ (J_2 \bigcup P_3 \bigcup \cdots \bigcup P_n)$, $a_2 \in I\ (J_1 \bigcup P_3 \bigcup \cdots \bigcup P_n)$, $c_3 \in I\ (J_1 \bigcup J_2 \bigcup P_4 \bigcup \cdots \bigcup P_n), \ldots\ c_n \in I\ (J_1 \bigcup J_2 \bigcup P_3 \bigcup \cdots \bigcup P_{n-1})$. Then $a_1 \in J_1, a_2 \in J_2, c_3 \in P_3, \ldots$ Let $z_3 = c_3 + a_1 a_2 c_4 \cdots c_n$. Since P_3 is prime and $a_1, a_2, c_4, \ldots, c_n \notin P_3$, their product is not in P_3 which implies $z_3 \notin P_3$. Then $z_3 \in I$ but in no J_i or P_i. Then $I \not\subseteq J_1 \bigcup J_2 \bigcup P_3 \bigcup \cdots \bigcup P_n$, a contradiction. □

Definition. For ideals I, J of a ring R, we can define the **colon ideals**, or **ideal quotient**, of I and J the set $(I : J) = \{r \in R | rJ \subseteq I\}$.

Examples. In $\mathbb{Z}$ $(2\mathbb{Z} : 3\mathbb{Z}) = 2\mathbb{Z}$ and $(6\mathbb{Z} : 8\mathbb{Z}) = 3\mathbb{Z}$.

Later on, we will see that for an integral domain R inside a quotient field F we can define **fractional ideals** as a subset of F satisfying the properties of an ideal under R (that is, the sponge property with multiplication by R and subtraction). In this case, we can extend the colon ideal to $(I :_F J) = \{f \in F | fJ \subseteq I\}$. For example $(6\mathbb{Z} :_{\mathbb{Q}} 8\mathbb{Z}) = \frac{3}{4}\mathbb{Z}$.

Note. $((0) : I) = \{r \in R | rI = (0)\}$ is called the **Annihilator of** I. For example, in $\mathbb{Z}/48\mathbb{Z}, (0 : 4\mathbb{Z}) = 12\mathbb{Z}$. If $I \subseteq J$, then $Ann\ J \subseteq Ann\ I$.

Remarks 1.11b. Let I be an ideal of A. Then

(1) $\bigcup_{x \neq 0} \mathrm{Ann}(x) = \{$ zero-divisors of $A\}$.
(2) The *radical* of I, $r(I) := \{x \in A \mid x^n \in I$, for some $n > 0\}$, is an ideal.
(3) $r(I) = \pi^{-1}(\mathcal{N}_{A/I})$, where $\pi : A \to A/I$, is the natural projection.

Exercise 1.12. Let α and β be ideals of a ring A. Then

(1) $\alpha \subseteq (\alpha : \beta)$
(2) $(\alpha : \beta)\beta \subset \alpha$.
(3) $(\alpha : \beta) : \gamma) = (\alpha : \beta\gamma) = ((\alpha : \gamma) : \beta)$.
(4) $(\bigcap_i \alpha_i : \beta) = \bigcap_i (\alpha_i : \beta)$
(5) $(\alpha : \sum_i \beta_i) = \bigcap_i (\alpha : \beta_i)$.

Exercise 1.13. If I and J are ideals of a ring A and P is a prime ideal of A, then

1. $r(I) \supseteq I$
2. $r(r(I)) = r(I)$
3. $r(IJ) = r(I \cap J)$
4. $r(I) = 1$ if and only if $I = (1)$.
5. $r(I + J) = r(r(I) + r(J))$
6. $r(P^n) = P$ for all $n > 0$.

Proposition 1.14. Let A be a ring and I an ideal. The radical $r(I)$ of I satisfies $r(I) = \cap\{P | P \in Spec\ A$ and $I \subseteq P\}$.

Proposition 1.15. Let A be a ring. Then $\{\text{zero divisors of } A\} = \cup_{x\neq 0} r(Ann(x))$.

Proposition 1.16. Let A be a ring and I, J ideals of A. If $r(I)$ and $r(J)$ are coprime, then I and J are coprime.

Let $f : A \to B$ be a ring homomorphism. Then if I is an ideal A, it is NOT necessarily true that $f(I)$ is an ideal of B. However, if f is surjective, then $f(I)$ is an ideal of B. Also, it is always the case that $f(I)B$ is an ideal of B and we call this ideal an **extension** of I.

Example. Consider the identity homomomorphism $\mathbb{Z} \to \mathbb{Q}$. $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$ but not of $\mathbb{Q}$. However, $2\mathbb{Z}\mathbb{Q} = \mathbb{Q}$ is an (uninteresting) ideal of $\mathbb{Q}$.

Example. In Exercise 5, we showed if P was a prime ideal of A, then $P[x]$ was a prime ideal of $A[x]$. In this case, $P[x]$ is an extension of P.

We can also define a **contraction**. If J is an ideal of B, then $f^{-1}(B)$ is an ideal of A.

Proposition 1.17. Let A and B be rings with I an ideal of A and J an ideal of B. Let $f : A \to B$ be a ring homomorphism. Then

(1) $I \subseteq f^{-1}(f(I)B)$. $J \subseteq f(f^{-1}(J)$.
(2) $f^{-1}(J) \subseteq f^{-1}(f(f^{-1}(J)))$ etc.

2. Atiyah MacDonald, Chapter 2: Modules

Definition. Lat A be a commutative ring. An $A-$**module** is an abelian group M (written additively) on which A acts linearly, i.e., for all $a, b \in A, x, y \in M$

$$\begin{array}{rclcrcl} a(x+y) & = & ax+ay & \qquad & (a+b)x & = & ax+bx \\ (ab)x & = & a(bx) & & 1x & = & x \end{array}$$

Examples.

(1) An ideal α of A is an $A-$module and, in particular, A is an $A-$module.
(2) If A is a field k, then an $A-$module is a $k-$VS.
(3) Every $\mathbb{Z}-$module is an abelian group ($nx = x + ... + x$) and every abelian group is a $\mathbb{Z}-$module.
(4) If $A = k[x]$ for a field k, then an $A-$module is a $k-$VS with a linear transformation.
(5) If A is a ring, then $A[x], A[[x]], A[G] = \{\sum a_i g_i | a_a \in A, g_i \in G\}$ are all $A-$modules.

Definition. Let M, N be $A-$modules. A mapping $f : M \to N$ is an $A-$**module homomorphism** if $f(x + y) = f(x) + f(y)$ and $f(ax) = af(x)$ for all $a \in A, x, y \in M$. Define $\text{Hom}_A(M, N) = \{A - \text{module homomorphism } f : M \to N\}$.

Note. If A is a field then an $A-$module homomorphism is a linear transformation vector spaces.

Remarks 2.0. Let A be a ring and M, M', N, N' $A-$modules.

(1) $\text{Hom}_A(M, N)$ is an A-module. [We can define $f + g : M \to N$ to be $(f + g)(m) = f(m) + g(m)$.]
(2) If $u : M' \to M$ and $v : N \to N'$ are A-homomorphisms, then there exist A-homomorphisms $\widetilde{u} : \text{Hom}_A(M', N) \to \text{Hom}_A(M, N), \widetilde{v} : \text{Hom}_A(M, N) \to \text{Hom}_A(M, N')$ defined by $\widetilde{u}(f) = f \circ u, \widetilde{v}(f) = v \circ f$, $\forall f \in \text{Hom}_A(M, N)$.

$$\begin{array}{ccc} M' & & M \xrightarrow{f} N \\ {\scriptstyle u}\downarrow & & \qquad\quad {\scriptstyle v}\downarrow \\ M \xrightarrow{f} N & & \qquad\quad N' \end{array}$$

(3) $\text{Hom}_A(A, N) \cong N$, via $\varphi : \text{Hom}_A(A, N) \xrightarrow{\cong} N$; $\varphi(f) = f(1)$, $\forall f \in \text{Hom}_A(A, N)$.

Definition. A **submodule** M' of M is a subgroup of M which is closed under multiplication by A. The $A-$module M/M' is the **quotient** of m by M'.

Operations on Submodules

- $\sum M_i = \{\sum_{finite} x_i | x_i \in M_i\}$. This is the smallest submodule of M which contains all the M_i's.
- $\cap M_i$ is also a submodule.
- $\alpha M = \{\sum a_i x_i | a_i \in \alpha \text{ (an ideal) }, x_i \in M\}$. This is also a submodule.

Proposition 2.1. *The three isomorphism theorems.*

(1) ($1^{\text{st}} \cong$ Thm) Let $f : M \to N$ be a module homomorphism. Then
$M/\text{Ker } \varphi \cong \text{Im } \varphi$. Also, if $M' \subseteq \ker \varphi \subseteq M$, then $\exists \overline{f} : M/M' \to N$.

(2) ($2^{\text{nd}} \cong$ Thm) If M_1 and M_2 are submodules of M, then
$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$.

(3) ($3^{\text{rd}} \cong$ Thm) If $N \subseteq M \subseteq L$ are A-modules, then $(L/N)/(M/N) \cong L/M$.

Definition. If N, P are submodules of M, define $(N : P) = \{a \in A | aP \subseteq M\}$. This is an ideal of A. In particular, we have $(0 : M) = \{a \in A | aM = 0\}$. Call this the **annihilator** of M and denote it $Ann(M)$. An $A-$module is **faithful** if $Ann(M) = 0$. If $Ann(M) = a$, then M is faithful as an $A/a-$module.

Exercise 2.2. Let M, N, P be submodules of some bigger module. Then

(1) $\text{Ann}(M + N) = \text{Ann}(M) \cap \text{Ann}(N)$.

(2) $(N : P) = \text{Ann } ((N + P)/N)$.

Definition. If $(M_i)_{i \in I}$ is any family of $A-$modules, define the **direct sum** as

$$\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} | x_i \in M_i \text{ and only finitely many are nonzero}\}.$$

If we drop the finite restriction, then we have the **direct product** $\prod M_i$.

Remarks.

(1) $\bigoplus_{i \in I} M_i$ is an $A-$module. For the case of 2 modules, we see $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ and $a(x, y) = (ax, ay)$.

(2) If a ring $A = \prod_{i=1}^n A_i$, then the set of all elements $(0, ..., 0, a_i, 0, ..., 0)$ for $a_i \in A_i$ is an ideal $\alpha_i \in A$. In fact $A = \alpha_1 \oplus \cdots \oplus \alpha_n$. Conversely, if $A = \alpha_1 \oplus \cdots \oplus \alpha_n$, then $A \cong \prod_{i=1}^n A/b_i$ for $b_i = \bigoplus_{j \neq i} \alpha_j$.

Definition. A **free** module M is such that $M \cong \bigoplus_{i \in I} M_i$ where each $M_i \cong A$ as an $A-$module. Say $M = A^{(I)}$. A finitely generated free $A-$module is of the form $A \oplus \cdots \oplus A$ and is denoted A^n.

Proposition 2.3. Let M be an A-module. Then M is finitely generated $\iff$ $M \cong A^n/N$, for some integer $n \geq 0$ and some submodule $N \subseteq A^n$.

Proposition 2.4. Let M be a finitely generated A-module, let I be an ideal of A, and let φ be an A-module endomorphism of M such that $\varphi(M) \subseteq IM$. Then φ satisfies an equation of the form
$\varphi^n + a_1\varphi^{n-1} + \cdots + a_n = 0$, where the a_i are in I.

Proof. Say $M = Ax_1 + ... + Ax_n$, that is $x_1, ..., x_n$ generate M and let $phi : M \to M$. Then $\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j$ where $a_{ij} \in I$ since $\phi(M) \subseteq IM$. Then $0 = \phi(x_i) - a_{i1}x_1 - ... - a_{in}x_n$ for all i. Rewriting this, we see

$$\begin{aligned} 0 &= (\phi - a_{11})x_1 - a_{12}x_2 - ... - a_{1n}x_n \\ 0 &= a_{11}x_1 - (\phi - a_{22})x_2 - ... - a_{2n}x_n \\ &\vdots \\ 0 &= -a_{n1}x_1 - a_{n2}x_2 - ... - (\phi - a_{nn})x_n \end{aligned}$$

Of course, writing this in matrix form we have

$$0 = \begin{bmatrix} (\phi - a_{11}) & -a_{12} & \cdots & -a_{1n} \\ a_{11} & -(\phi - a_{22}) & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & -(\phi - a_{nn}) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = BX$$

Recall that $I(\det B) = (\text{Adj } B)B$ and note that this holds for matrices over commutative rings. So multiply our above equation by Adj B to get $0 = (\det B)X$. Since this is true for all X, we see that $(\det B)M = 0$. Thus $\det B$ is the $0-$homomorphism. Writing out what $\det B$ is, we get an equation of the form $\phi^n + c_1\phi^{n-1} + ... + c_n =$ for some $c_i \in I$ (since c_i are sums and products of $a_ij \in I$.) □

Corollary 2.5. Let M be a finitely generated A-module and let I be an ideal of A such that $IM = M$. Then there exists $x \in A$, $x \equiv 1 \pmod{I}$ such that $xM = 0$.

Proof. Let $\phi = 1_M$. By Proposition 2.4, there exists $a_1, ..., a_n \in I$ such that $phi^n + a_1\phi^{n-1} + ... + a_n = 0$. Thus $(1 + a_1 + ... + a_n)1_M = 0$. Let $x = 1 + a_1 + ... + a_n$. Then $x \equiv 1 \mod I$. and $xM = (1 + a_1 + ... + a_n)M = 0$. □

Proposition 2.6, 2.7. **Nakayama's Lemma**. Let M be a finitely generated A-module, let I be an ideal of A such that $I \subseteq \mathcal{R}$, the Jacobson radical of A and let N be a submodule of A. Then

(1) $IM = M \implies M = (0)$.
(2) $M = IM + N \implies M = N$.
(3) For A a local ring, J any proper ideal of A, $M = JM + N \implies M = N$.

Proof. (1) By Corollary 2.5, there exists $x \in A$ such that $x \equiv 1 \mod I$ and $xM = 0$. Since $x \equiv 1 \mod I$, there exists $r \in R$ such that $x = 1 + r$. Then, by Proposition 1.9, x is a unit. Thus $M = x^{-1}xM = x^{-1}0 = 0$.

(2) Consider M/N. Then we can show $I(M/N) = (IM + N)/N$. By assumption, $(IM + N)/N = M/N$. Then by *1*, $M/N = (0)$. So $M = N$.

□

Proposition 2.8. Let A be a local ring with maximal ideal $\mathbf{m}$, M an A-module. Then $A/\mathbf{m} = k$ is a field and

(1) $M/\mathbf{m}M$ is a k-module, that is, a vector space over k.
(2) If M is finitely generated as an A-module, then $M/\mathbf{m}M$ is a finite-dimensional vector space over k.
(3) If M is finitely generated as an A-module and $x_1, \ldots, x_n \in M$ are such that their images $\overline{x}_1, \ldots, \overline{x}_n \in M/\mathbf{m}M$ generate $M/\mathbf{m}M$ as a k-vector space, then $x_1, \ldots, x_n$ generate M as an A-module.

Combining *2* and *3*, we have that M is finitely generated if and only if M/mM is finite dimensional.

Proof. (of *3*) Say $M = Ax_1 + ... + Ax_n + mM$. By Nakayama, since $m \in \mathcal{R}$, $M = Ax_1 + ... + Ax_n$. □

Note. If A is a local ring with maximal ideal m and $A/m = k$, we often say (A, m, k) is a local ring.

Definition. A sequence of A-modules and $A-$homomorphisms $\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$ is said to be **exact** at M_i if $\text{im}(f_i) = \ker(f_{i+1})$. The sequence is exact if it is exact at each M_i.

Remarks.

(1) $0 \to M' \xrightarrow{f} M$ is exact if and only if f is injective (since $\{0\} = \text{im}(0) = \ker f$).

(2) $M \xrightarrow{g} M'' \to 0$ is exact if and only if g is surjective (since $\text{im}g = \ker(0)$).

(3) $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact if and only if f is injective, g is surjective, and f induces an isomorphism of $Coker f = M/f(M')$ onto M''. A sequence of this type is called a **short exact sequence**.

Examples. The following are short exact sequences.

- $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \to 0$ where $f(n) = 2m$ and $g(m) = \overline{m} = m + 2\mathbb{Z}$.
- $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z}[x] \xrightarrow{g} \mathbb{Z}[x]/(x) \to 0$ where $f(n) = n$ and g sends a polynomial to its constant term.
- $0 \to M \xrightarrow{f} M \oplus N \xrightarrow{g} N \to 0$ where $f(a) = (a, 0)$ and $g((c, d)) = d$.

Proposition 2.9. Let P be an A-module.

(1) A sequence (*) of A-modules and homomorphisms gives rise to another sequence (**), where
$$(*): \quad M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0 \qquad (**): \quad 0 \to \text{Hom}(M'', P) \xrightarrow{\tilde{v}} \text{Hom}(M, P) \xrightarrow{\tilde{u}} \text{Hom}(M', P).$$

(2) Furthermore (*) is exact $\iff$ (**) is exact for all P.

(3) A sequence (#) of A-modules and homomorphisms gives rise to another sequence (##), where
$$(\#): \quad 0 \to N' \xrightarrow{u} N \xrightarrow{v} N'' \qquad (\#\#): \quad 0 \to \text{Hom}(P, N') \xrightarrow{\tilde{u}} \text{Hom}(P, N) \xrightarrow{\tilde{v}} \text{Hom}(P, N'').$$

(4) Furthermore (#) is exact $\iff$ (##)) is exact for all P.

We can consider commutative diagrams to get a better understanding of this:

$$\begin{array}{ccccccc} M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & {\scriptstyle g}\downarrow & & {\scriptstyle f}\downarrow & & \\ & & N & & N & & \end{array} \qquad \text{and} \qquad \begin{array}{ccccccc} & & & & M & & M \\ & & & & {\scriptstyle f}\downarrow & & {\scriptstyle g}\downarrow \\ 0 & \longrightarrow & N' & \xrightarrow{u} & N & \xrightarrow{v} & N'' \end{array}$$

Proof. (1) $\Leftarrow$: In book.

(2) $\Rightarrow$: First, we will show $\text{im}0 = \ker \tilde{u}$. This is the same as showing $\tilde{u}$ is injective. Let $f : M \to N$ and $\tilde{u}(f) = 0$. Then $\tilde{u}(f)(m) = 0$ for all $m \in M$ which implies $u(f(m)) = 0$ for all $m \in M$. Of course, u is injective so $f(m) = 0$ for all $m \in M$ which implies $f = 0$. Now We will show $\text{im}\tilde{u} = \ker \tilde{v}$. To show $\subseteq$, we can just show $\tilde{v}(\tilde{u}) = 0$. Let $f : M \to N'$. Then $\tilde{v}(\tilde{u})(f) = \tilde{v}(u(f)) = v(u(f))$. Then for all $m \in M$ we see $v(u(f))(m) = 0$ as $\text{im}u \subseteq \ker v$, so $\text{im}\tilde{u} \subseteq \ker \tilde{v}$.

□

Proposition 2.10. For every commutative diagram of A-modules and A-homomorphisms with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & {\scriptstyle f'}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle f''}\downarrow & & \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0, \end{array}$$

there exists an exact sequence

$$0 \to \text{Ker}(f') \xrightarrow{\tilde{u}} \text{Ker}(f') \xrightarrow{\tilde{v}} \text{Ker}(f'') \xrightarrow{d} \text{Coker}(f') \xrightarrow{\tilde{u}'} \text{Coker}(f') \xrightarrow{\tilde{v}'} \text{Coker}(f'') \to \quad 0,$$

where, $\forall x'' \in Ker(f'') \subseteq M''$ and $x \in M$ such that $v(x) = x'', f(x) = u'(y)$, the mapping d is well-defined by $d(x'') = y' + Im(f') \in Coker(f')$.

Proof. We will explain where d comes from. Let $x'' \in \ker f'' \subseteq M''$. Since v is onto, there exists $x \in M$ such that $v(x) = x''$. Now, $v'f(x) = f''(v(x))$ by the commutative properties of the diagram. Of course, $v'f(x) = f''(v(x)) = f''(x'') = 0$. So $f(x) \in \ker v' = \text{im}u'$. Thus $f(x) = u'(y')$ for some $y' \in N'$. Since u' is injective, there exists only one such y'. Define $d(x'') = y' + \text{im}f' \in N'/\text{im}f'$. This shows that d is well-defined. □

Proposition 2.11. Suppose we have an exact sequence of A-modules and homomorphisms

$$0 \to M_0 \to M_1 \to \cdots \to M_n \to 0,$$

in which all the modules M_i and the kernels of all the homomorphisms belong to a class of A-modules $\mathcal{C}$. If λ is an additive function on $\mathcal{C}$, that is, $\lambda : \mathcal{C} \to \mathbb{Z}$ as defined p. 23, A & M, then $\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0$.

Let M, N be $A-$modules. The goal of a tensor product is to find some D such that $M \times N/D = M \otimes N$ where $a(x \otimes y) = ax \otimes y = x \otimes ay$ and $(x_1 + x_2) \otimes y = x_1 \otimes y + x_2 \otimes y$. Let $C = A^{(M \times N)} = \sum_{finite} A(x, y)$ where $x \in M, y \in N$. Now, let $D =$

$$< \{a(x,y) - (ax,y), a(x,y) - (x,ay), (x_1 + x_2, y) - (x_1, y) - (x_2, y), (x, y_1 + y_2) - (x, y_1) - (x, y_2) | a \in A\} > .$$

Then define $M \otimes N = C/D$. So we have $x \otimes y = (x, y) + D$ and

$$M \otimes N = \{ \sum_{finite} a_i(x_i \otimes y_i) | a_i \in A, x_i \in M, y_i \in N\}.$$

Definition. Let M, N, P be $A-$modules. Say $F : M \times N \to P$ is an $A-$**bilinear map** if for all $x, x_1, x_2 \in M, y, y_1, y_2 \in N, a \in A$, we have

$$\begin{aligned} f(x_1 + x_2, y) &= f(x_1, y) + f(x_2, y) \\ f(x, y_1 + y_2) &= f(x, y_1) + f(x, y_2) \\ f(ax, y) &= af(x, y) \\ f(x, ay) &= af(x, y) \end{aligned}$$

Proposition 2.12. Let M and N be A-modules. Then

(1) *Existence of tensor product.* There exists an A-module T, called $M \otimes_A N$, and an A-bilinear mapping $g : M \times N \to T$ with the property that, for every A-module P and every A-bilinear mapping $f : M \times N \to P$, there exists a unique A-linear mapping $f' : T \to P$ such that $f = f' \circ g$:

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & P \\ {\scriptstyle g}\downarrow & \overset{\exists! f'}{\nearrow} & \\ T & & \end{array} .$$

(2) *Uniqueness of tensor product.* If (T, g) and (T', g') are two pairs with the property (1) above, then there exists a unique isomorphism $j : T \to T'$ such that $j \circ g = g'$.

(3) Items (1) and (2) can be extended to a finite product of A-modules $M_1 \times \cdots \times M_r$ and multi-linear maps, to define $M_1 \otimes \cdots \otimes M_r$.

Proof. (1) Notice $T = M \otimes N$ and $\sum_{finite} a_i(x_i, y_i) \mapsto \sum_{finite} a_i(x_i \otimes y_i)$ by g satisfies 1. Clearly, T is an $A-$module. Also $g((x, y)) = x \otimes y = (x, y) + D$ is $A-$bilinear by the way we defined D. Now suppose we have another bilinear map $f : M \times N \to P$. Since f is bilinear, we see $f(D) = 0$. Then f extends to $T = C/D$. Call the extension f'. Then f' is well defined and $f' : T \to P$. Note that there is only one way to extend f, thus f' is unique.

(2) Consider the commutative diagram:

$$\begin{array}{ccc} & & T \\ & & {\scriptstyle \exists! j}\downarrow \\ M \times N & \xrightarrow{g'} & T' \\ & & {\scriptstyle \exists! i}\downarrow \\ & & T \end{array}$$

This tells us that $ij : T \to T$. Of course, we also have $1_T : T \to T$ and by uniqueness, we have $ij = 1_T$. Similarly, we see $ji = 1_{T'}$. Thus i and j are bijective. Thus j is an isomorphism.

□

Corollary 2.13. Let $x_i \in M, y_i \in N$ be such that $\sum(x_i \otimes y_i) = 0$ in $M \otimes N$. Then there exist finitely generated A-submodules M_0 of M and N_0 of N such that $\sum(x_i \otimes y_i) = 0$ in $M_0 \otimes N_0$.

Proposition 2.14. Let M, N, P be $A-$modules. Then there exist unique isomorphisms, described with $x \in M, y \in N, z \in P$, as follows

(1) $M \otimes N \to N \otimes M$, where $x \otimes y \to y \otimes x$.
(2) $(M \otimes N) \otimes P \to M \otimes (N \otimes P)$ where $(x \otimes y) \otimes z \to x \otimes (y \otimes z)$.
(3) $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$, where $(x, y) \otimes z \to (x \otimes z, y \otimes z)$.
(4) $A \otimes M \to M$ where $a \otimes x \to ax$.

Exercise 2.15. Let A, B be rings, let M be an A-module, P be an B-module, N be an A, B-bimodule. Then $M \otimes_A N$ is a natural B-module, $N \otimes_B P$ an A-module, and $(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$.

Remark 2.15. Let $f : M \to M'$, $f' : M' \to M'', g : N \to N', g' : N' \to N''$ be A-module homomorphisms. Define $h : M \times N \to M' \otimes N'$ by $h(x, y) = f(x) \otimes g(y)$ and $h' : M' \times N' \to M'' \otimes N''$ similarly. Then

(1) h, h' are A-bilinear and therefore induce $f \otimes g : M \otimes N \to M' \otimes N'$, via $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$ and similarly $f' \otimes g' : M' \otimes N' \to M'' \otimes N''$. (2) $(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$.

Propositions 2.16, 2.17. Let $f : A \to B$ be a ring homomorphism, M an A-module, N a B-module. Then

(1) N is an A-module (define $ax := f(a)x$, for all $a \in A, x \in N$).
(2) If N is finitely generated as a B-module and B is finitely generated as an A-module, then N is finitely generated as an A-module.
(3) With N an A-module as in (1), $M_B = B \otimes_A N$ is a B-module and $b(b' \otimes x) = bb' \otimes x$, for all $b, b' \in B, x \in M$.
(4) If M is finitely generated as an A-module, then M_B is finitely generated as a B-module.

Proof. For (1) and (2), say $N = By_1 + ... + By_n$ for $y_i \in N$ and $B = Ax_1 + ... + Ax_m$ for $x_i \in N$. Then $N = (Ax_1 + ... + Ax_m)y_1 + ... + (Ax_1 + ...Ax_m)y_n$. For (3) and (4), let $M = Ax_1 + ... + Ax_m$. Then M_B is generated by $\{1 \otimes x_i\}$. □

Proposition 2.18. Let M, M', M'', N be A-modules and let 1_N denote the identity mapping on N. Then

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \text{ exact } (A\text{-module homomorphisms}) \implies M' \otimes N \xrightarrow{f \otimes 1_N} M \otimes N \xrightarrow{g \otimes 1_N} M'' \otimes N \to 0$$

exact.

Remark. It is *not* true in general that, if $M' \to M \to M''$ is an exact sequence of $A-$modules and homomorphisms, the sequence $M' \otimes N \to M \otimes N \to M'' \otimes N$ obtained by tensoring with an arbitrary $A-$module N is exact.

Examples. Take $A = \mathbb{Z}$ and consider $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z}$ where $f(x) = 2x$ for all $x \in \mathbb{Z}$. Let $N = \mathbb{Z}/2\mathbb{Z}$. Then the sequence $0 \to \mathbb{Z} \otimes N \xrightarrow{f \otimes 1} \mathbb{Z} \otimes N$ is *not* exact as $f \otimes 1(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0$. Thus $f \otimes 1$ is the 0 mapping, but $\mathbb{Z} \otimes N \neq 0$.

Definition. Say the $A-$module N is flat provided for all exact sequences $(*) \to M_{i+1} \to M_i \to M_{i-1} \to \cdots$, we have that $* \otimes N$ is exact.

Remarks.

(1) A is flat.

Proof. We see that $*$ is equivalent to $* \otimes A$ as $M \otimes A \cong M$. So clearly, $*$ is exact if and only if $* \otimes A$ is exact. □

(2) $F = A^{(n)} = \otimes_n A$ is flat.

Proof. For F, note that $M_i \otimes F = M_i \otimes (\oplus A) = \oplus(M_i \otimes A) = \oplus M_i$. Thus $*$ is equivalent to $* \otimes F$ and thus $*$ is exact if and only if $* \otimes F$ is. □

Proposition 2.19. These are equivalent for N an A-module.

(1) N is flat.
(2) $0 \to M' \to M \to M'' \to 0$ exact $\implies 0 \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0$ exact.
(3) If $f : M' \to M$ is 1:1, so is $f \otimes 1_N : M' \otimes_A N \to M \otimes_A N$.
(4) If $f : M' \to M$ is 1:1 and M, M' are finitely generated, then $f \otimes 1_N : M' \otimes_A N \to M \otimes_A N$ is 1:1.

Introduction to chain complexes and Tor (from Rotman)

Let R be a commutative ring with 1.

Definition. R, p. 166. A *complex* A is a sequence of R-modules and maps:
$\mathbf{A}$ $\cdots \to A_{n+1} \stackrel{d_{n+1}}{\to} A_n \stackrel{d_n}{\to} A_{n-1} \to \cdots$, where $n \in \mathbb{Z}$ and $d_n d_{n+1} = 0$, for all n. The maps d_n are *differentiations*. Sometimes the complex is denoted by ($\mathbf{A}$, d).

Remarks. Rotman, page 60-61.

(1) $d_n d_{n+1} = 0 \iff \mathrm{Im}(d_{n+1}) \subseteq \mathrm{Ker}(d_n)$.
(2) Every exact sequence is a complex (because $\mathrm{Im}(d_{n+1}) = \mathrm{Ker}\, d_n$).
(3) If M is an R-module then there is an exact sequence and so a complex $\mathbf{F}$, called a *free resolution of* M, with free modules F_n of form
$\mathbf{F}$ $\cdots \to F_{n+1} \stackrel{d_{n+1}}{\to} F_n \stackrel{d_n}{\to} F_{n-1} \to \cdots F_0 \stackrel{d_0}{\to} M \to 0$.

Theorem. R, p. 60. Every module M has a free resolution.

Definition. R. p. 166. If ($\mathbf{A}$,d) is a complex, then the n^{th} *homology module* of ($\mathbf{A}$,d) is
$H_n(\mathbf{A}) = \mathrm{Ker}\, d_n / \mathrm{Im}\, d_{n+1}$.

Definition. R, p. 166. If
$\mathbf{F}$ $\cdots \to F_{n+1} \stackrel{d_{n+1}}{\to} F_n \stackrel{d_n}{\to} F_{n-1} \to \cdots F_0 \stackrel{d_0}{\to} M \to 0$
is a free resolution of M and N is another R-module, then
$\mathbf{F}\otimes_R N : \cdots \to F_{n+1} \otimes_R N \stackrel{d_{n+1}\otimes 1_N}{\to} F_n \otimes_R N \stackrel{d_n \otimes 1_N}{\to} F_{n-1} \otimes_R N \to \cdots F_0 \otimes_R N \stackrel{d_0 \otimes 1_N}{\to} 0$
is also a complex, and
$\mathrm{Tor}_n^R(M, N) = H_n(\ \mathbf{F}\otimes_R N) = \ker(d_n \otimes 1)/\ \mathrm{im}(d_{n+1} \otimes 1)$.
(Note that we drop the term $M \otimes_R N$ in this resolution!)

Theorem. Rotman, p. 220–223. For M, N, B, B', B'' modules over a ring R,

(1) $\mathrm{Tor}_n^R(M, N)$ is an R-module (for R a commutative ring).
(2) $\mathrm{Tor}_0^R(M, N) \cong M \otimes_R N$.
(3) $\mathrm{Tor}_n^R(M, N) \cong \mathrm{Tor}_n^R(N, M)$.
(4) If $0 \to B' \to B \to B'' \to 0$ is a short exact sequence, then there is a long exact sequence:
$$\cdots \to \mathrm{Tor}_2^R(M, B') \to \mathrm{Tor}_2^R(M, B) \to \mathrm{Tor}_2^R(M, B'') \to \mathrm{Tor}_1^R(M, B') \to \mathrm{Tor}_1^R(M, B) \to \mathrm{Tor}_1^R(M, B'')$$
$$\to M \otimes_R B' \to M \otimes_R B \to M \otimes_R B'' \to 0\ .$$

(5) If N is flat, $\mathrm{Tor}_n^R(M,N)=0$, for all $n\geq 1$.
(6) If $\mathrm{Tor}_1^R(M,N)=0$, for all M, then N is flat.

3. Atiyah MacDonald, Chapter 3: Localizations

Recall that $\mathbb{Z}$ is an integral domain and we can define its fraction field as

$$\mathbb{Q}=\frac{\{(a,b)|a\in\mathbb{Z},b\in\mathbb{Z}\setminus\{0\}\}}{\equiv},$$

where $\equiv$ represents the equivalence relation $(a,b)\equiv(c,d)$ if and only if $ad=bc$.

We can generalize this to any integral domain A, where we say

$$K=\frac{A\times(A\setminus\{0\})}{<\{(a,b)-(c,d)|ad=bc\}>}.$$

In fact, in general, if A is a ring and S a multiplicatively closed subset of A (that is, for $s,t\in S, st\in S$) with 1. Now, we define our relation $\equiv$ by $(a,s)\equiv(b,t)$ for $a,b\in A, s,t\in S$ if and only if there exists $s'\in S$ such that $s'(at-sb)=0$. We call this $S^{-1}A=\frac{A\times S}{(\equiv)}$. Note that $S^{-1}A$ is a ring where we identify the equivalence class $[(a,s)]$ with $\frac{a}{s}$. If A is an integral domain and $S=A\setminus\{0\}$, then $S^{-1}A$ is called the **field of fractions**.

Remark. There exists a homomorphism $A\xrightarrow{f}S^{-1}A$ defined by $a\mapsto\frac{a}{1}$.

Examples.

(1) $A=\mathbb{Z}/6\mathbb{Z}, S=\{1,3\}$. Then $S^{-1}A=\{\frac{0}{1},\frac{1}{1}\}$ as the equivalence relation gives that all of the fractions with even numerators are equivalent and all of the fractions with odd numerators are equivalent.
(2) $A=\mathbb{Z}/4\mathbb{Z}, S=\{1,3\}$. Here, S is made of units. Now $S^{-1}A=\{\frac{0}{1},\frac{1}{1},\frac{2}{1},\frac{3}{1}\}$.

Definition. For a prime ideal P of A, define $A_P=S^{-1}A$ where $S=A\setminus P$. This ring is very useful.

Examples.

(1) $A=\mathbb{Z}, P=2\mathbb{Z}$. Then $\mathbb{Z}_{(2)}=\{\text{fractions with odd denominator}\}$.
(2) $A=\mathbb{Z}[x], P=(2,x)$. Then $A_p=\{\text{fractions with denominators who have odd constant terms}\}$.

Remarks.

(1) A_p is a local ring with PA_P as the unique maximal ideal.
(2) If S contains no zero divisors (or 0), then $f:A\to S^{-1}A$ is injective.

Proof. If f is not injective, then there exists $a\neq 0$ such that $f(a)=0$. Then there exists $s\in S$ such that $0=s(a\cdot 1-0\cdot 1)=sa$. Thus a is a zero divisor. □

Note: For $S=A-p$, S is not necessarily disjoint from all the zero divisors. For example, $A=\mathbb{Z}/6\mathbb{Z}$ and $P=2\mathbb{Z}/6\mathbb{Z}$. Here $S=\{1,3,5\}$ and 3 is a zero divisor.

(3) If $a\in A\setminus\{0\}$ and $S=\{1,a,a^2,a^3,...\}$, then $S^{-1}A=A[\frac{1}{a}]=:A_a$.
Example: Let $A=k[x]$ where k is a field and x an indeterminant. Then $A_x=k[x,\frac{1}{x}]$ is called the Laurent polynomial ring.
(4) For A a commutative ring, $S=\{\text{non zerodivisors of } A\setminus\{0\}\}$. Say $S^{-1}A$ is the **total quotient ring of** A.

Proposition 3.1. Let $g:A\to B$ be a ring homomorphism. If $g(s)$ is a unit in B for every $s\in S$, then there exists a unique ring homomorphism $h:S^{-1}A\to B$ such that $g=h\circ f$.
(Here f is canonical, $f:A\to S^{-1}A$, via $a\to a/1$.)

$$\begin{array}{ccc} A & \xrightarrow{\quad g\quad} & B \\ {\scriptstyle f}\big\downarrow & \overset{\exists!\, h}{\nearrow} & \\ S^{-1}A & & \end{array}$$

Proof. **Uniqueness:** If h is as describe ave and $\frac{a}{s} \in S^{-1}A$, then

$$g(a) = h\left(\frac{a}{1}\right) = h\left(\frac{as}{s}\right) = h\left(\frac{a}{s} \cdot \frac{s}{1}\right) = h\left(\frac{a}{s}\right) h\left(\frac{s}{1}\right) = g\left(\frac{a}{s}\right) g(s).$$

So $h(\frac{a}{s}) = g(a)g(s)^{-1}$.

Existence: Check that $h(\frac{a}{s}) = g(a)g(s)^{-1}$ is a well-defined ring homomorphism. If $\frac{a}{s} = \frac{a'}{s'}$, then there exists t such that $t(as' - a's) = 0$. Then $g(t)(g(a)g(s') - g(a')g(s)) = 0$. Now, since $g(s)$ is a unit for all $s \in S$, we get $g(a)g(s)^{-1} = g(a')g(s')^{-1}$. Thus $h(\frac{a}{s}) = h(\frac{a'}{s'})$.

□

Remarks. The homomorphism $f : A \to S^{-1}A$ satisfies

(1) For all $s \in S$, $\frac{s}{1} = f(s)$ is a unit in $S^{-1}A$ as $\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1}$.
(2) If $f(a) = \frac{0}{1}$, then a is a zero divisor as there exists $s \in S$ such that $sa = 0$.
(3) For all $\frac{a}{s} \in S^{-1}A$, we see $\frac{a}{s} = f(a)f(s)^{-1} = \frac{a}{1}\frac{1}{s}$.

Corollary 3.2. If $A \xrightarrow{g} B$ is a ring homomorphisms and S is a multiplicatively closed subset of A, and

(1) $g(s)$ is a unit of B for all $s \in S$
(2) If $g(a) = 0$, then $as = 0$ for some $s \in S$
(3) Every element of B is of the form $\frac{g(a)}{g(s)}$ for $a \in A, s \in S$

Then $B \cong S^{-1}A$ such that the homomorphism h in the universal property is an isomorphism.

Let M be an $A-$module, S a multiplicatively closed subset of A. Then we can define $S^{-1}M = \frac{M \times S}{(\equiv)}$ in the same way.

Remarks.

(1) For $A-$modules M, N and $u : M \to N$ a homomorphisms, then there exists a homomorphism $S^{-1}u : S^{-1}M \to S^{-1}N$ defined by $\frac{m}{s} \mapsto \frac{u(m)}{s}$.
(2) If $M \xrightarrow{u} N \xrightarrow{v} P$ are homomorphisms, then $S^{-1}M \xrightarrow{S^{-1}u} S^{-1}N \xrightarrow{S^1 v} S^{-1}P$ satisfies $(S^{-1}v) \circ (S^{-1}u) = S^{-1}(v \circ u)$.

Proposition 3.3. For A-modules M, M', M'',
$M' \xrightarrow{f} M \xrightarrow{g} M''$ exact (with f, g A-module homomorphisms) $\implies S^{-1}M' \overset{S^{-1}f}{\to} S^{-1}M \overset{S^{-1}f}{\to} S^{-1}M''$ exact.

Proof. We want to show $\ker S^{-1}g = imS^{-1}f$.

$\supseteq$: $(S^{-1}g) \circ (S^{-1}f) = S^{-1}(g \circ f) = S^{-1}(0) = 0$ as $*$ is exact.

$\subseteq$: Let $\frac{m}{s} \in \ker S^{-1}g$. Then $S^{-1}g(\frac{m}{s}) = 0$, that is $\frac{g(m)}{s} = \frac{0}{1}$. Let $t \in S$ such that $tg(m) = 0$. Then $0 = g(tm)$ which implies $tm \in \ker g = imf$. Thus $tm = f(m')$ for some $m' \in M'$. Then $\frac{m}{1} = \frac{f(m')}{t}$ which implies $\frac{m}{s} = \frac{f(m')}{st}$. Thus $\frac{m}{S} \in imS^{-1}f$.

□

Corollary 3.4. If ${}_AN, {}_AP$ are submodules of ${}_AM$, then

(1) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$.
(2) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.
(3) $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$ as $S^{-1}A$-modules.

Proof. **(1) and (4):** Follow from the fact that $0 \to N \to M \to M/N \to 0$ is exact implies $0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$ is exact.

(2): Trivial

(3): Left to reader

□

Proposition 3.5. For every ${}_AM$, there exists a unique isomorphism $f : S^{-1}A \otimes_A M \to S^{-1}M$, so that $f(a/s) \otimes am/s = am/s$, for all $a \in A, m \in M, s \in S$.

Proof. Consider the following diagram: Clearly, h is bilinear. Then there exists a unique homomorphism f. We want to show that f is an isomorphism. Note that f is surjective as every element of $S^{-1}M = \frac{m}{s} = h(\frac{1}{s}, m) = f(\frac{1}{2} \otimes m)$.

Claim: For all $\alpha \in S^{-1}A \otimes M$, $\alpha = \frac{1}{s} \otimes m$ for some $s \in S$ and $m \in M$.
Proof: Let $\alpha \in \sum_{i=1}^{n} \frac{a_i}{s_i} \otimes m_i$. Let $s = \prod s_i$. Then $\frac{a_i}{s} = \frac{a_i t_i}{s_i}$ for $t_i \in S$. Then $\alpha = \sum \frac{a_i t_i}{s} \otimes m_i = \sum \frac{1}{s} \otimes a_i t_i m_i = \frac{1}{s} \otimes \sum a_i t_i m_i$. Let $m = \sum a_i t_i m_i$.

To show f is injective, suppose $f(\frac{1}{s} \otimes m) = 0$. Then $\frac{0}{1} = f(\frac{1}{s} \otimes m) = f(g(\frac{1}{s}, m)) = h(\frac{1}{s}, m) = \frac{m}{s}$. So there exists t such that $tm = 0$. Now $\frac{1}{s} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0$. Thus f is injective. □

Corollary 3.6. $S^{-1}A$ is a flat A-module.

Proof. For $M' \to M \to M''$ exact, we see $S^{-1}M' \to S^{-1}M \to S^{-1}M''$ is exact and thus $S^{-1}A \otimes M' \to S^{-1}A \otimes M \to S^{-1}A \otimes M''$ is exact. Thus $S^{-1}A$ is flat. □

Proposition 3.7. Given A-modules M and N, $\exists\ !\ \ f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes N)$, an $S^{-1}A$-module homomorphism; f is defined by $f((m/s) \otimes (n/t)) = (m \otimes n)/st$. For P a prime ideal, $M_P \otimes N_P \cong (M \otimes N)_P$ as A_P-modules.

Proof. **Claim** (**Exercise 2.15**): Let A, B be rings, M an $A-$module, P a $B-$module, and N a $(A, B) - bimodule$ (N is simultaneously an $A-$module and $B-$module such that $a(xb) = (ax)b$ for $a \in A, b \in B, x \in N$). Then

(1) $M \otimes_A N$ is a $B-$module and $N \otimes_B P$ is an $A-$module
(2) $(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$

Proof. (1) Consider multiplication as $(m \otimes n)b = m \otimes nb$ and $a(n \otimes p) = an \otimes p$.
(2) We will mimic the proof of exercise 2.14 by first showing that $(M \otimes_A N) \otimes_B P \cong M \otimes_A N \otimes_B P$. Note that once we show this we are finished as we can show $M \otimes_a (N \otimes_B P) \cong M \otimes_a N \otimes_B P$. So for all $z \in P$ define $h_z : M \times N \to M \otimes_A N \otimes_B P$ by $(m, n) \mapsto m \otimes n \otimes z$. This is bilinear. So there exists $f_z : M \otimes_A N \to M \otimes_A N \otimes_B P$.

We can use f_z to define $f : (M \otimes_A N) \otimes_B P \to M \otimes_A N \otimes_B P$.

To show f is an isomorphism, we will construct its inverse. So define $g_z : M \times N \times P \to (M \otimes_A N) \otimes_B P$ by $(m, n, z) \mapsto (m \otimes n) \otimes z$. This is linear in each variable, so there exists a unique homomorphism $g : M \otimes_A N \otimes_B P \to (M \otimes_A N) \otimes_B P$.

Clearly, f and g are inverses. Thus we see $(M \otimes_A N) \otimes_B P \cong M \otimes_A N \otimes_B P$.

□

Let A, B be rings with C an $A-$module, P a $B-$module, and D an $(A, B)-$bimodule. Then $(C \otimes_A D) \otimes_B P \cong C \otimes_A (D \otimes_B P)$. Let $B = S^{-1}A$ and recall $S^{-1}M = S^{-1}A \otimes M$. Then

$$\begin{aligned} S^{-1}M \otimes_{S^{-1}A} S^{-1}N &\cong (S^{-1}A \otimes_A M) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \\ &\cong (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \\ &\cong M \otimes_A (S^{-1}A \otimes_{S^{-1}A} (S^{-1}A \otimes_A N)) \\ &\cong M \otimes_A (S^{-1}A \otimes_A N) \\ &\cong M \otimes_A (N \otimes_A S^{-1}A) \\ &\cong (M \otimes_A N) \otimes_A S^{-1}A \cong S^{-1}(M \otimes_A N). \end{aligned}$$

□

Definition. We define a **local property** to be a property $\mathcal{P}$ such that A has $\mathcal{P}$ if and only if A_P has $\mathcal{P}$ for all $P \in SpecA$.

Proposition 3.8. Given an $A-$module M, TFAE

(1) $M = 0$
(2) $M_P = 0$ for all $P \in SpecA$
(3) $M_m = 0$ for all maximal ideals m.

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3)**:** Trivial

(3) $\Rightarrow$ (1)**:** Let $x \in M \setminus \{0\}$. Let $I = Annx \subsetneq A$. Then there exists a maximal ideal m such that $m \supseteq I$. Now $\frac{x}{1} \equiv \frac{0}{1}$ implies there exists $s \in A \setminus m$ such that $s(x \cdot 1 - 0 \cdot 1) = 0$. So $s \in I \subseteq m$, a contradiction. So $M = 0$.

□

Proposition 3.9. Let $\phi : M \to N$ be an $A-$module homomorphism. TFAE

(1) ϕ is injective
(2) $\phi_P : M_P \to N_P$ is injective for all $P \in SpecA$

(3) $\phi_m : M_m \to N_m$ is injective for all maximal m.

Also, the corresponding statements are equivalent when injective is replaced with surjective.

Proof. (1) $\Rightarrow$ (2)**:** Since $M_P = S^{-1}M$ for $S = A \setminus P$ and S^{-1} preserves exactness.

(2) $\Rightarrow$ (3)**:** Clear as every maximal ideal is prime.

(3) $\Rightarrow$ (1)**:** Let $M' = \ker \phi$. Then $0 \to M' \to M \xrightarrow{\phi} N$ is exact. Then $0 \to (M')_m \to M_m \xrightarrow{\phi_m} N_m$ is exact. But ϕ_m is 1-1. Then $\ker \phi_m = 0$ which implies $(M')_m = 0$ by exactness. Since this holds for all m, we see $M' = 0$ by Prop 3.8. Thus $\ker \phi = 0$ which implies ϕ is 1-1.

□

Proposition 3.10. Given an $A-$module M, TFAE

(1) M is flat as an $A-$module

(2) M_P is flat as an A_p-module for all $P \in SpecA$.

(3) M_m is flat for all maximal m.

Proof. **Claim (Exercise 2.20):** If $A \to B$ is a ring homomorphism and M is a flat $A-$module, then $B \otimes M = M_B$ is flat as a $B-$module.

Proof: Say $N'_B \xrightarrow{f} N_B$ is injective. We want to show $N'_B \otimes M_B \xrightarrow{f \otimes 1} N_B \otimes M_B$ is injective. Since $A \to B$ is a homomorphism, N'_B is also an $A-$module. Note that $N' \otimes_A M \to N \otimes_A M$ is injective as M is flat. But now (by Exercise 2.15), we see

$$N' \otimes_B M_B \cong N' \otimes_B (B \otimes_A M) \cong (N' \otimes_B B) \otimes_A M \cong N' \otimes_A M \xrightarrow{1-1} N \otimes_A M \cong (N \otimes_B B) \otimes_A M \cong N \otimes_B (B \otimes_A M) \cong N \otimes_B M_B$$

Thus $f \otimes 1$ is injective and M_B is flat.

(1) $\Rightarrow$ (2)**:** By claim. Let $B = A_P$ and recall $A_P \otimes M = M_P$ by Prop 3.5

(2) $\Rightarrow$ (3)**:** Clear, as every maximal ideal is prime.

(3) $\Rightarrow$ (1)**:** Let $N \to P$ be injective. Then $N_m \to P_m$ is injective by Prop 3.9, which says $N_m \otimes M_m \to P_m \otimes M_m$ is injective as M_m is flat. But then $(N \otimes M)_m \cong N_m \otimes M_m \xrightarrow{1-1} P_m \otimes M_m \cong (P \otimes M)_m$ is injective. Thus, by Prop 3.9, we see $N \otimes M \to P \otimes M$ is injective and therefore M is flat.

□

Let $f : A \to B$ be a ring homomorphism. In Chapter 1, we defined an extended ideal as $I^e := f(I)B$ for an ideal $I \subseteq A$ and a contracted ideal as $J^c := f^{-1}(J)$ for an ideal $J \subseteq B$. We can similarly define these ideals for localizations:

Definition. Let $f : A \to S^{-1}A$ be the ring homomorphism for which $a \mapsto \frac{a}{1}$. Then an **extended ideal** is defined to be $I^e = S^{-1}I = \{\frac{a}{1} | a \in I\}(S^{-1}A)$ for an ideal $I \subseteq A$ and a contracted ideal is defined to be $J^c = f^{-1}(J) = \{x | \frac{x}{1} \in J\}$ for an ideal $J \in= S^{-1}A$.

Note. $I \subseteq (I^e)^c$ and $J \subseteq (J^c)^e$ as $I \subseteq f^{-1}(S^{-1}I)$ and $J \subseteq S^{-1}(f^{-1}(J)$ for $I \subseteq A$ and $J \subseteq B$.

Proposition 3.11, (1) Every ideal in $S^{-1}A$ is an extended ideal.

(2) If I is an ideal of A, then $I^{ec} = \cup_{s \in S}(I : s)$. Hence $I^e = (1) \iff I \cap S \neq \emptyset$.

(3) An ideal I of A is a contracted ideal from $S^{-1}A \iff$ no element of S is (0 or) a zero-divisor in A/I.

(4) The correspondence $P \to S^{-1}P$ is one-to-one and onto: {prime ideals P of $A \mid P \cap S = \emptyset$} $\to$ { prime ideals of $S^{-1}A$}.

(5) The operation S^{-1} commutes with formation of finite sums, products, intersections and radicals.

Proof. **(1):** Let $I = f^{-1}(J)$. We want to show $J = S^{-1}I = S^{-1}f^{-1}(J)$. By the note, we need only show $J \supseteq S^{-1}(f^{-1}(J))$. Let $\frac{x}{s} \in S^{-1}f^{-1}(J)$. Then $x \in f^{-1}(J)$ which implies $\frac{x}{1} \in J$. Since $\frac{1}{s} \in S^{-1}A$, we see $(\frac{x}{1})(\frac{1}{s}) = \frac{x}{s} \in J$ as ideals are closed under multiplication from the ring.

(4): We need to check multiple things:

- P prime in A such that $P \cap S = \emptyset$ implies $S^{-1}P$ is prime.

  Proof. Let $\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}P$. Say $\frac{a}{s} \cdot \frac{b}{t} \equiv \frac{p}{u}$. Then there exists $v \in S$ such that $v(abu - stp) = 0$. Then $vabu = vstp \in P$. So $(ab)vu \in P$. Now $vu \in S$ and $S \cap P = \emptyset$. So we see $ab \in P$. Since P is prime, either a or $b \in P$. Thus either $\frac{a}{s}$ or $\frac{b}{t} \in S^{-1}P$. □

- Q prime in $S^{-1}A$ implies $f^{-1}(Q)$ is prime in A and $f^{-1}(Q) \cap S = \emptyset$.

  Proof. This follows from Problem #21 in Chapter 1. □

- Clearly, $f^{-1}f(P) = P$ and $ff^{-1}(Q) = Q$.

□

Corollary 3.12. $\mathcal{N}(S^{-1}A) = S^{-1}\mathcal{N}(A)$.

Proof. Let $\frac{x}{s} \in S^{-1}\mathcal{N}(A)$. Then $x \in \mathcal{N}(A)$ which implies $x^t = 0$ for some t. Then $(\frac{x}{s})^t = \frac{0}{s^t} = 0$. Thus $\frac{x}{s} \in \mathcal{N}(S^{-1}A)$. Now, let $\frac{x}{s} \in \mathcal{N}(S^{-1}A)$. Then there exists t such that $(\frac{x}{s})^t = 0$. Of course, $(\frac{x}{s})^t = \frac{x^t}{s^t}$. □

Corollary 3.13. If P is a prime ideal of A, then $\{$ prime ideals of $A_P\} \overset{1:1,\ \text{onto}}{\to} \{$ prime ideals Q of $A \mid Q \subseteq P\}$.

Proposition 3.14. Let M be a finitely generated A-module. Then $S^{-1}(\text{ Ann } M) = \text{Ann } (S^{-1}M)$.

Proof. Let $M = Ax_1 + ... + Ax_n$, for $x_i \in M$.

($\subseteq$)**:** Let $\frac{x}{S} \in S^{-1}AnnM$, that is, $x \in AnnM$ and $s \in S$. Then $\frac{x}{s} \in AnnS^{-1}M$ as $(\frac{x}{s})(\frac{m}{t}) = \frac{xm}{st} = \frac{0}{st} \equiv \frac{0}{1}$.

($\supseteq$)**:** Let $\frac{x}{s} \in AnnS^{-1}M$. Note $S^{-1}M = S^{-1}A\frac{x}{1} + \ldots + S^{-1}A\frac{x_n}{1}$. Then $\frac{x}{s} \cdots \frac{x_i}{1} = 0$ for all i. So there exists u_i such that $u_i(xx_i) = 0$. Let $u = u_1 \cdots u_n$. Then $uxx_i = 0$ for all i. Now consider $\frac{m}{1} \in S^{-1}M$. Then $m = a_1x_1 + \ldots + a_nx_n$. Then $uxm = ux(a_1x_1 + ... + a_nx_n) = a_1(uxx_1) + ... + a_n(uxx_n) = 0$. So $ux \in AnnM$. Then $\frac{x}{s} = \frac{ux}{us} \in S^{-1}AnnM$.

□

Example. Let $M = \bigoplus_{p\ prime} \mathbb{Z}/p\mathbb{Z}$. This is not finitely generated. Let $S = \mathbb{Z} \setminus \{0\}$. Then $M_{(0)} = 0$ as, for example, $\frac{(1 + 2\mathbb{Z}, 1 + 3\mathbb{Z}, 0, ..., 0)}{1} \equiv \frac{0}{1}$ as $6(1 + 2\mathbb{Z}, 1 + 3\mathbb{Z}, 0, ..., 0) = 0$. So $AnnM_{(0)} = AnnS^{-1}M = \mathbb{Q}$. However, $AnnM = \cap_1^\infty Ann(\mathbb{Z}/p_i\mathbb{Z}) = \cap p_i\mathbb{Z} = 0$. So $S^{-1}AnnM = 0$.

Corollary 3.15. If $N, P \subseteq M$ are $A-$modules and P is finitely generated, then $S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$.

Proof. Recall from Exercise 2.2 that $(N : P) = Ann((N + P)/N)$. Thus we want to show $S^{-1}Ann(N + P/N) = Ann(S^{-1}N + S^{-1}P/S^{-1}N)$. From Proposition 3.14, since $(N+P)/N$ is finitely generated (as $(N+P)/N \cong P/N \cap P$ where P is finitely generated), we know $S^{-1}Ann((N + P)/N) \cong AnnS^{-1}((N + P)/N$. Also, $S^{-1}((N + P)/N) \cong S^{-1}N + S^{-1}P/S^{-1}N$ since $0 \to N \to N+P \to (N+P)/N \to 0$ is exact, which implies $0 \to S^{-1}N \to S^{-1}(N+P) \to S^{-1}((N + P)/N) \to 0$ is exact. □

Proposition 3.16. Let : $A \to B$ be a ring homomorphism and $P \in$ Spec (A). Then

(1) $P = Q^c$, for some $Q \in$ Spec (B) $\iff$ (2) $P^{ec} = P$. Let $f : A \to B$ be a ring homomorphism and $P \in SpecA$. Then $P = Q^C$ for some $Q \in SpecB$ if and only if $P^{ec} = P$.

4. Atiyah MacDonald, Chapter 4: Primary Decomposition

Terminology: (p.50-53,) Let q, I be ideals of A

q is *primary* if $q \neq A$ and $xy \in q \implies x \in q$ or $\exists t > 0$ with $y^t \in q$.

Nilradical of q: $r(q) = \{x \in A \mid x^n \in q,\ \exists n \geq 0\}$. (Recall $r(q) = \cap\{p \mid p \supseteq q,\ p \text{ a prime ideal}\}$, Prop. 1.8, p. 5 A & M.)

q is *primary for* p (with p a prime ideal) or *p-primary* if $r(q) = p$.

Primary decomposition: An expression $I = \cap_{i=1}^n q_i$, where each q_i is primary.

Minimal primary decomposition: $I = \cap_{i=1}^n q_i \mid$ each q_i primary and (i) $i \neq j \implies r(q_i) \neq r(q_j)$, (ii) $\forall j, \quad q_j \not\supseteq \cap_{i=1, i\neq j}^n q_i$.

Associated primes of I (defined only if I has a minimal primary decomposition $\cap_{i=1}^n q_i$): The set $\{r(q_i)\}_{i=1}^n$.

Minimal associated primes or *isolated* primes of I (defined only for I having a primary decomposition): The set of minimal elements of $\{r(q_i)\}_{i=1}^n$ from above.

The *embedded* associated primes are the associated primes that are not minimal.

Remarks 4.0. For q, I ideals of a ring A,

(1) q is primary $\iff$ $A/q \neq 0$ and every zero-divisor in A/q is nilpotent.
(2) q prime $\implies$ q primary.
(3) If $f : A \to B$ is a ring homomorphism and q is primary for P in B, then $f^{-1}(q)$ is primary for $f^{-1}(P)$ in A.
(4) If I has a primary decomposition, then it has a minimal one.

Example. In $k[x, y]$ for a field k, $(x, y)^2$ is primary as $k[x, y]/(x, y)^2 = \{\overline{a_0 + a_1x + a_2y}\}$. If $a_0 \neq 0$, then $a_0 + a_1x + a_2y$ is not a zero divisor. If $a_0 = 0$, then $(a_1x + a_2y)^2 = 0$, that is it is nilpotent. Also, (x, y^2) is primary.

Propositions 4.1, 4.2. For q an ideal of a ring A,

(1) q primary $\implies$ $r(q)$ is prime and is the smallest prime ideal containing q.
(2) If $r(q)$ is a maximal ideal, then q is primary.
(3) If $\mathbf{m}$ is a maximal ideal, then $\mathbf{m}^n$ is primary, $\forall n \geq 0$.

Proof. Note that $r(q) \neq A$ as $1 \notin q$ implies $1 \notin r(q)$. Let $ab \in r(q)$ with $a \notin r(q)$. Then there exists n such that $(ab)^n \in q$ which implies $a^n b^n \in q$ but $a^n \notin q$. Thus there exists t such that $(b^n)^t \in q$ which implies $b \in r(q)$ and thus $r(q)$ is prime. □

Examples 4.1a. Let A be a non-zero ring.

(1) Not every primary ideal is a power of a prime ideal; e.g. $q = (x^2, y) \subseteq k[x, y]$, where k is a field.
(2) Not every power of a prime ideal is primary; e.g. $A = k[x, y, z]/(xy - z^2)$, $(\bar{x}, \bar{y})^2$ is not primary. Thus $r(q)$ prime does *not* imply q is primary.

Lemmas 4.3, 4.4. Let q, q_i, $1 \leq i \leq n$ be primary ideals for p, $x \in A$. Then

(1) $\cap_{i=1}^n q_i$ is p-primary.
(2) (i) If $x \in q$, then $(q : x) = (1)$; (ii) If $x \notin q$, then $(q : x)$ is p-primary, $r(q : x) = p$. (iii) If $x \notin p$, then $(q : x) = q$.

Recall: • Prop 1.11, p.8: If a prime ideal equals an intersection of ideals, it equals one of them.

• Prop 1.12, p.8, part (1v): For I_i, J ideals, $(\cap_{i\in\mathcal{I}} I_i : J) = \cap_{i\in\mathcal{I}}(I_i : J)$.

• The radical (r) of a finite intersection of ideals is the intersection of the radicals of the ideals.

Theorem 4.5.(and remarks), "First Uniqueness Theorem". Let I be an ideal of A with a minimal primary decomposition $I = \cap_{i=1}^n q_i$, where each q_i is primary. Let $p_i := r(q_i),\ \forall i$. Then

(1) $\{p_1, \ldots, p_n\} = \{r(a : x) \mid x \in A,\ r(a : x) \text{ is prime }\}$.

(2) The set $\{p_1, \ldots, p_n\}$ is independent of the choice of the decompositon of I.

(3) For every i with $1 \leq i \leq n$, the colon ideal $(I : x_i)$ is $r(q_i)$-primary, for some $x_i \in A$.

(4) The set $\{p_1, \ldots, p_n\} = \{\, r(\text{ Ann } (\bar{x})\,) \mid \bar{x} \in A/I, \text{ and } r(\text{Ann } (\bar{x})\,) \text{ is a prime ideal of } A\}$.

Proof of 4.5: Use the Lemmas. By 1.12, p. 8, and 4.2, $(I : x) = (\,(\cap_{i=1}^n q_i) : x) = \cap_{i=1}^n (q_i : x)$.
Hence, using 1.13, p. 9, $r(I : x) = \cap_{i=1}^n r(q_i : x) = \cap_{i=1, x \notin q_i}^n p_i$.
If $r(I : x)$ is a prime ideal, then by Prop. 1.11, p. 8, $r(I : x) = p_j$, for some j. Thus every prime ideal of the form $r(I : x)$ is in $\{p_1, \ldots, p_n\}$.

Now suppose that $p_j \in \{p_1, \ldots, p_n\}$. Then $\exists x \in \cap_{i=1, i \neq j}^n q_i - q_j$, by minimality of the decomposition, and $r(I : x) = p_j$.

Example 4.5a. For $I = (x^2, xy)$ in $A = k[x, y]$, $I = (x) \cap (x, y)^2$. Now $(x, y)^2$ is primary for (x, y) by Proposition 4.2 above. Thus the associated primes of I are (x) and (x, y).

Proposition 4.6. If an ideal I of A has a primary decomposition, then

(1) Every prime ideal P containing I contains a minimal prime ideal belonging to I and

(2) $\{P \mid P \text{ is prime ideal minimal with respect to } P \supseteq I\} = \{P \mid P \text{ is a minimal associated prime of } I\}$.

Proposition 4.7, Let I be an ideal of A with a minimal primary decomposition $I = \cap_{i=1}^n q_i$, where each q_i is primary. Let $p_i := r(q_i),\ \forall i$. Then $\cup_{i=1}^n p_i = \{x \in A \mid (I : x) \neq I\}$.

In particular, if (0) has a primary decomposition and $(0) = \cap_{i=1}^n q_i$ is a minimal primary decomposition of (0), then

$D := \{$ zero-divisors of $A\} = \cup_{i=1}^n p_i$, the union of all the prime ideals associated to (0).

5. Chapter 5: Integral independence and valuations–Nick

We interpret "$A \subseteq B$" as "A is a subring of B", unless otherwise noted.

Definition. Let B be a ring, with A a subring. An element $\alpha \in B$ is *integral* over A if there exist $a_i \in A$ such that $\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0$. Equivalently, there exists a monic polynomial $f(x) \in A[x]$ with $f(\alpha) = 0$. ($A[x]$ denotes the polynomial ring over A.)

Notes: (1) This is completely analogous to the concept of being algebraic over a field!

(2) Clearly, if $\alpha \in A, \alpha - \alpha = 0$, so every element of A is integral over A.

Examples 5.0.

(1) Let $B = \mathbb{R}, A = \mathbb{Z}$. The element $\alpha = \sqrt{2} \in B$ satisfies: $\alpha^2 - 2 = 0$, so α is integral over $\mathbb{Z}$. Similarly, n^{th}-roots, $\forall n > 0$.

(2) Let $B = \mathbb{Q}, A = \mathbb{Z}$. Suppose that $\alpha = r/s \in B$ is integral over A and $(r, s) = 1$. Then there exist $a_i \in \mathbb{Z}$ with $(r/s)^n + a_1(r/s)^{n-1} + a_2(r/s)^{n-2} + \cdots + a_n = 0$. Multiply both sides by s^n to get: $r^n + a_1 s r^{n-1} + \cdots + a^n s^n = 0$. Now s divides every term except possibly the first; therefore $s | r^n$. But $(s, r) = 1$, and so $s = 1$, so that $\alpha = r \in A$. Thus $\mathbb{Z}$ is the set of all integral elements in $\mathbb{Q}$ over $\mathbb{Z}$.

Proposition 5.1. Let $A \subseteq B$ and $\alpha \in B$. The following are equivalent:

(1) α is integral over A.

(2) $A[\alpha]$ is a finitely generated A-Module.

(3) There exists a subring $C \subseteq B$, with $A[\alpha] \subseteq C$, and C a finitely generated A-Module.

(4) There exists a faithful $A[\alpha]$-Module M, with M finitely generated as an A-Module.

proof: (1) $\implies$ (2): By assumption, there exist $a_i \in A$ with $\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0$. Rearranging, we get: $\alpha^n = -(a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n)$. Hence, $\alpha^r \in A\alpha^1 + A\alpha^2 + \cdots + A\alpha^{n-1}$, for every $r \geq 0$. Thus $A[\alpha]$ is a finitely generated A-Module. (2) $\implies$ (3): Take $C = A[\alpha]$. (3) $\implies$ (4): Take $M = C$. We need only show that M is faithful as an $A[\alpha]$-module. Let $\alpha \in \text{Ann}(M)$. Since C is a subring of B, $1 \in C$. Then $\alpha \cdot 1 = 0$, forcing $\alpha = 0$. (4) $\implies$ (1): Recall *Proposition 2.4*: Let M be a finitely generated A-module, let I be an ideal of A, and let φ be an A-module endomorphism of M with $\varphi(M) \subseteq IM$. Then there exist $a_i \in A$ such that $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. [That is, the right side is the 0-map.]

Define $\varphi : M \to M$ by $\varphi(y) = \alpha y$, and set $I = A$. Clearly $\varphi(M) = \alpha M \subseteq IM$, since M is an $A[\alpha]$-module. Thus we may apply (2.4) to get: $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. [That is, it is the 0-map]. Let $m \in M$. Then $0 = 0(m) = (\alpha^n + a_1\alpha^{n-1} + \cdots + a_n)(m) = \alpha^n(m) + a_1\alpha^{n-1}(m) + \cdots + a_n(m) = \alpha^n * m + a_1\alpha^{n-1} * m + a_2\alpha^{n-2} * m + \cdots + a_n * m = m*(\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n)$. But since M is faithful, $\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0$. □

Corollary 5.2. Let $A \subseteq B$ and let $\{\alpha_i\}_{i=1}^n \subseteq B$ be a finite set of integral elements over A. Then $A[\alpha_1, \alpha_2, \cdots, \alpha_n]$ is a finitely generated A-module.

Proof: Induct on n. For $n = 1$, this is the proposition. Suppose the claim holds for all k with $1 \leq k < n$. Set $A_r := A[\alpha_1, \alpha_2, \cdots, \alpha_r]$. Then $A_n = A_{n-1}[\alpha_n]$ is finitely generated as an A_{n-1} module. By induction, A_{n-1} is finitely generated as an A-module. So by (2.16), A_n is finitely generated as an A-module. [Finitely generated-ness is transitive.] □

Definition 5.2a, Let $A \subseteq B$. Denote $C_{A,B} = \{\alpha \in B \mid \alpha \text{ is integral over } A\}$, the *Integral Closure of A in B*. If $C_{A,B} = A$, then A is *Integrally Closed in B*. If $C_{A,B} = B$, then B is *Integral over A*. [Note: The subscripts are needed, as the integral closure can change depending on B. Refer back to the two examples.]

Corollary 5.4. Let $A \subseteq B \subseteq C$ be rings. B integral over A and C integral over $B \implies C$ integral over A.

Proof: Let $\alpha \in C$. Then there exist $b_i \in B$ such that $\alpha^n + b_1\alpha^{n-1} + b_2\alpha^{n-2} + \cdots + b_n = 0$. Set $B' = A[b_1, b_2, \ldots, b_n]$. Since B is integral over A, B' is finitely generated over A. Hence, $B'[\alpha]$ is finitely generated over A, so α is integral over A. □

Corollary 5.3, 5.5. Let $A \subseteq B$ be rings. Then $A \subseteq C_{A,B} \subseteq B$ and $C_{A,B}$ is an integrally closed subring of B.

Proof: The containments are obvious. Let $x, y \in C_{A,B}$. Then both are integral over A, so $A[x, y]$ is finitely generated. Since $A[x + y], A[x - y], A[xy] \subseteq A[x, y]$, by the proposition, we get $x + y$, $x - y$ and xy are integral over A. Hence, $C_{A,B}$ is a ring. To see that it is closed in B, let $\alpha \in B$ be integral over $C_{A,B}$. We have that $C_{A,B}[\alpha]$ is integral over $C_{A,B}$ which in turn is integral over A. Hence, α is integral over A, so $\alpha \in C_{A,B}$.

Proposition 5.6. Let $A \subseteq B$ be rings, with B integral over A.

(1) If J is an ideal of B, and $I = J^c = A \cap J$, an ideal of A, then B/J is integral over A/I.

Proof: Let $\alpha + J \in B/J$. Then there exist $a_i \in A$ such that $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. Then each $a_i + I \in A/I$, and $(\alpha + J)^n + (a_1 + I)(\alpha + J)^{n-1} + \cdots + (a_n + I)(1 + J) = (\alpha^n + J) + (a_1\alpha^{n-1} + J) + \cdots + (a_n + J) = (\alpha^n + a_1\alpha^{n-1} + \cdots + a_n) + J = 0 + J$. Hence, $\alpha + J$ is integral over A/I. □

(2) If S is a multiplicatively closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.

Proof: Let $\alpha/s \in S^{-1}B$. Then there exist $a_i \in A$ such that $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. Divide by s^n to get: $(\alpha/s)^n + (a_1/s) * (\alpha/s)^{n-1} + \cdots + (a_n/s^n) = 0$. Note that $a_i/s^i \in S^{-1}A$, so α/s is integral over $S^{-1}A$. □

Chapter 5 A & M : Integrally Closed Domains, The Going Up Theorem–David

Proposition 5.7. Let $A \subseteq B$ be integral domains, with B integral over A. Then B is a field $\iff$ A is a field.

Proof. ($\Leftarrow$)**:** Suppose A is a field. Let $y \in B \setminus \{0\}$. Then y is integral over A. Say $y^n \neq a_1 y^{n-1} + \ldots + a_n = 0$ for $a_i \in A$ has minimal degree. Since B is an integral domain, $a_n \neq 0$. So $y^{-1} = -a_n^{-1}(y^{n-1} + ... + a_{n-1}) \in B$.

($\Rightarrow$)**:** Let $x \in A \setminus \{0\}$. Then $x^{-1} \in B$ and x^{-1} is integral over A. So we get $x^{-m} + a_1 + a^{-m+1} + ... + a_m = 0$ for $a_i \in A$. Then $x^{-1} = (a_1 + a_2 x + ... + a_m x^{m-1})$.

□

Corollary 5.8. Let $A \subseteq B$ be rings, with B integral over A. Let Q be a prime ideal of B and let $P = Q^c = Q \cap A$. Then Q is maximal $\iff$ P is maximal.

Proof. By 5.6, B/q is integral over A/p and since p, q are prime, $B/q, A/p$ are integral domains. Thus B/q is a field if and only if A/p is field which implies q is maximal if and only if p is maximal. □

Corollary 5.9. Let $A \subseteq B$ be rings, with B integral over A. Let $Q \subseteq Q'$ be prime ideals of B and say that $Q \cap A = Q' \cap A$. Then $Q = Q'$.

Theorem 5.10. Let $A \subseteq B$ be rings, with B integral over A. Let $Q \subseteq Q'$ be prime ideals of B and say that $Q \cap A = Q' \cap A$. Then $Q = Q'$.

Proof. By 5.6, B_p is integral over A_p. We also have that the diagram below commutes.

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle\alpha}\downarrow & & {\scriptstyle\beta}\downarrow \\ A_p & \longrightarrow & B_p \end{array}$$

Let I be a maximal ideal of B_p. Then $J = I \cap A_p$ is maximal by Corollary 5.8. Since A_p is local, J is the unique maximal ideal. Let $q = \beta^{-1}(I)$. The q is prime and $q \cap A = \alpha^{-1}(J) = p$. □

Theorem 5.11,. *Going Up Theorem*: Let $A \subseteq B$ be rings, with B integral over A. Let $m < n$, and let $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n$ be prime ideals of A and $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m$ be prime ideals of B such that $Q_i \cap A = P_i, \forall i$ with $1 \leq i \leq m$. Then the chain of prime ideals of B can be extended to $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_n$ with $Q_i \cap A = P_i, \forall i$ with $1 \leq i \leq n$.

Proof. By induction, we may just consider $n = 1, 2$. Let $\overline{A} = A/p_1, \overline{B} = B/q_1$. Then $\overline{A} \subseteq \overline{B}$ and $\overline{B}$ is integral over $\overline{A}$ by 5.6. Hence, there exists a prime $\overline{q}_2 \in \overline{B}$ such that $\overline{q}_2 \cap \overline{A} = \overline{p}_2$. Lift $\overline{q}_2$ back to B from $\overline{B}$ to get a prime ideal q_2 such that $q_2 \cap A = p_2$. □

Chapter 5 A & M : Integrally Closed Domains, The Going Down Theorem–Ela

Proposition 5.12. Let $A \subseteq B$ be rings, C the integral closure of A in B. Let S be a multiplicatively closed subset of A. Then, $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Proof: By A & M 5.6 (ii), $S^{-1}C$ is integral over $S^{-1}A$. Now, if $b/s \in S^{-1}B$ is integral over $S^{-1}A$, then we have an equation of the form $(b/s)^n + (a_1/s_1)(b/s)^{n-1} + ... + (a_n/s_n) = 0$, where $a_i \in A$, $s_i \in S$ $(1 \leq i \leq n)$. If we let $t = s_1 ... s_n$ and multiply this equation by $(st)^n$, we find $(bt)^n + (a_1 s s_2 ... s_n)(bt)^{n-1} + ... + a_n s^n {s_1}^n ... {s_n}^{n-1} = 0$. This new equation shows that bt is integral over A. So, $bt \in C$. Therefore, $\dfrac{b}{s} = \dfrac{bt}{st} \in S^{-1}C$.

Definition: An integral domain is said to be *integrally closed* if it is integrally closed in its field of fractions.

Example: $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$ by Example 5.0.

Remarks: 1) Every unique factorization domain (UFD) is integrally closed. 2) For example, the polynomial ring $k[x_1, ..., x_n]$, for k a field, is integrally closed.

Proposition 5.13 Let A be an integral domain. Then TAE: (i) A is integrally closed; $\iff$ (ii) $A_{\mathfrak{p}}$ is integrally closed, for each prime ideal $\mathfrak{p}$ of A; $\iff$ (iii) $A_{\mathfrak{m}}$ is integrally closed, for each maximal ideal $\mathfrak{m}$ of A.

Proof: Let K be the field of fractions of A. Let C be the integral closure of A in K. Let $f : A \to C$ be the identity mapping of A into C. So,

A is integrally closed $\Leftrightarrow$ f is surjective and hence $A_{\mathfrak{p}}$ (resp. $A_{\mathfrak{m}}$) is integrally closed (by Proposition 5.12) $\Leftrightarrow$ $f_{\mathfrak{p}}$ (resp. $f_{\mathfrak{m}}$) is surjective $\Leftrightarrow$ f is surjective.

Definitions: Let $A \subseteq B$ be rings and let I be an ideal of A. An element $x \in B$ is *integral over* I if x satisfies an equation of the form $x^n + \alpha_1 x^{n-1} + ... + \alpha_n = 0$, where $\alpha_i \in I$ for all i. **Note**: This is not the standard modern definition; others require each $a_i \in I^i$.

The *integral closure of* I in B, C_I, is the set of all elements of B which are integral over I, i.e.,

$C_I = \{x \in B : \ x \text{ is integral over } I\}$.

Lemma 5.14.. Let C_A be the integral closure of A in B and let I be an ideal of A. Let I^e denote the extension of I in C_A. Then, $C_I = r(I^e)$ where $r(I^e)$ is the radical of the ideal I^e.

Proposition 5.15. Let $A \subseteq B$ be integral domains, A integrally closed and let $x \in B$ be integral over an ideal I of A. Then x is algebraic over the field of fractions K of A and its minimal polynomial over K has form $t^n + a_1 t^{n-1} + ... + a_n$, where $a_i \in r(I)$ for all i.

Lemma: Let A be a ring, S a multiplicatively closed subset of A and I an ideal of A. If $I \cap S = \emptyset$, then there exists a prime ideal $\mathfrak{p}$ in A such that $\mathfrak{p} \cap S = \emptyset$ and $I \subseteq \mathfrak{p}$.

Proof: Consider the natural map $f : A \to S^{-1}A$. Since $I \cap S = \emptyset$, we have $IS^{-1}A \neq S^{-1}A$ so that $\exists\ \mathfrak{q} \in Spec(S^{-1}A)$ such that $IS^{-1}A \subseteq \mathfrak{q}$. As $\mathfrak{q} \in S^{-1}A$, $\mathfrak{q} = \mathfrak{p}S^{-1}A$ for some $\mathfrak{p} \in Spec(A)$ such that $\mathfrak{p} \cap S = \emptyset$. Since $IS^{-1}A \subseteq \mathfrak{p}S^{-1}A$, we get $I \subseteq IS^{-1}A \subseteq \mathfrak{p}S^{-1}A \cap A = \mathfrak{p}$. This proves the lemma.

Proposition 5.16. *Going Down Theorem.* Let $A \subseteq B$ be integral domains, A integrally closed, B integral over A. Let $\mathfrak{p}_1 \supseteq ... \supseteq \mathfrak{p}_n$ be a chain of prime ideals of A, and let $\mathfrak{q}_1 \supseteq ... \supseteq \mathfrak{q}_m$ $(m < n)$ be a chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq m$.

Then the chain $\mathfrak{q}_1 \supseteq ... \supseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \supseteq ... \supseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.

Proof: It is enough to prove the case where $m = 1$, $n = 2$ since then we can complete the chain inductively. So, we have $\mathfrak{p}_2 \subseteq \mathfrak{p}_1$ primes in A and $\mathfrak{q}_1$ prime in B, such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.

Claim: $\mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A = \mathfrak{p}_2$ where $\mathfrak{p}_2 B_{\mathfrak{q}_1}$ is the extension of $\mathfrak{p}_2 \in Spec(A)$ in $B_{\mathfrak{q}_1}$.

Proof of the Claim: It is clear that $\mathfrak{p}_2 \subseteq \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A$. So, it is enough to prove $\mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A \subseteq \mathfrak{p}_2$. Let $0 \neq x \in \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A$. Then, $x \in A$ and $x = y/s$ for some $y \in \mathfrak{p}_2 B$ and $s \in B - \mathfrak{q}_1$. By Lemma 5.14, the integral closure of $\mathfrak{p}_2$ in B is $r(\mathfrak{p}_2 B)$. (Here $C_A = B$ since $A \subseteq B$ integral).

So, $y \in \mathfrak{p}_2 B \subseteq r(\mathfrak{p}_2 B) = \{z \in B : \text{z is integral over } \mathfrak{p}_2\}$ implies y is integral over $\mathfrak{p}_2$. By Proposition 5.15, y is algebraic over the field of fractions K of A. Let $f(t)$ be the minimal polynomial of y over K, say $f(t) = t^r + u_1 t^{r-1} + ... + u_r$. Then, again by Proposition 5.15, each $u_i \in r(\mathfrak{p}_2) = \mathfrak{p}_2$.

Note that $x^{-1} \in K$ since $0 \neq x \in A$.

¿From $x = \dfrac{y}{s}$, we have $sx = y$ and $g(t) := t^r + \left(\dfrac{u_1}{x}\right) t^{r-1} + ... + \left(\dfrac{u_r}{x^r}\right)$ is the minimal polynomial of s over K since $g(s) = 0$ and g is a monic irreducible polynomial over K. (Note that $f(tx) = x^r g(t)$ and $g(t)$ is irreducible over $K[t]$

since $f(t)$ and hence $f(tx)$ is irreducible over $K[t]$.)
Let $v_i := \frac{u_i}{x^i}$ for $1 \leq i \leq r$. Then, $x^i v_i = u_i$ for $1 \leq i \leq r$. Since $s \in B - \mathfrak{q}_1 \subseteq B$ and $A \subseteq B$ integral extension, s is integral over A. By Proposition 5.15, taking $\mathfrak{a} = A$, we get $v_i \in A = r(A)$ for $1 \leq i \leq r$. Now, suppose $x \notin \mathfrak{p}_2$. Then, $x^i v_i = u_i \in \mathfrak{p}_2$ implies $v_i \in \mathfrak{p}_2$ for $1 \leq i \leq r$. As $g(s) = 0$, we have $s^r + v_1 s^{r-1} + ... + v_r = 0$ and hence $s^r = -(v_1 s^{r-1} + ... + v_r) \in \mathfrak{p}_2 B$ since each $v_i \in \mathfrak{p}_2$ and $s^j \in B$. Since $q_1 \cap A = p_1$ we have $p_1 B \subseteq q_1$ and since $p_2 \subseteq p_1$ we have $\mathfrak{p}_2 B \subseteq \mathfrak{p}_1 B \subseteq \mathfrak{q}_1$. So, $s^r \in \mathfrak{p}_2 B$ implies $s^r \in \mathfrak{q}_1$ and hence $s \in q_1$ since $q_1 \in Spec(B)$. This contradicts $s \in B - \mathfrak{q}_1$. So, $x \in p_2$ and hence $\mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A \subseteq \mathfrak{p}_2$. This finishes the proof of the claim. ♦
Now let $I := \mathfrak{p}_2 B\mathfrak{q}_1$ and $S = A - \mathfrak{p}_2$. Then S is a multiplicatively closed subset of $B\mathfrak{q}_1$ since we have $A \hookrightarrow B\mathfrak{q}_1$. Then, by the lemma above, $\exists$ a prime ideal $\mathfrak{q}$ of $B\mathfrak{q}_1$ such that $I \subseteq \mathfrak{q}$ and $S \cap \mathfrak{q} = \emptyset$ since $I \cap S = (\mathfrak{p}_2 B\mathfrak{q}_1) \cap (A - \mathfrak{p}_2) = \emptyset$ (This follows from the claim as $\mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A = \mathfrak{p}_2$). Then $\mathfrak{q} = \mathfrak{q}_2 B\mathfrak{q}_1$ for some $\mathfrak{q}_2 \in Spec(B)$ with $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$. As $I = \mathfrak{p}_2 B\mathfrak{q}_1 \subseteq \mathfrak{q} = \mathfrak{q}_2 B\mathfrak{q}_1$, we get $\mathfrak{p}_2 = \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A \subseteq \mathfrak{q}_2 B_{\mathfrak{q}_1} \cap A$. As $\mathfrak{q} \cap S = (\mathfrak{q}_2 B\mathfrak{q}_1) \cap (A - \mathfrak{p}_2) = \emptyset$, we get $\mathfrak{q}_2 B\mathfrak{q}_1 \cap A \subseteq \mathfrak{p}_2$. So, $\mathfrak{q}_2 B\mathfrak{q}_1 \cap A = \mathfrak{p}_2$. Now, this implies $\mathfrak{q}_2 \cap A = (\mathfrak{q}_2 B\mathfrak{q}_1) \cap (B \cap A) = (\mathfrak{q}_2 B\mathfrak{q}_1 \cap A) \cap B = \mathfrak{p}_2 \cap B = \mathfrak{p}_2$. Therefore, $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. This finishes the proof of the theorem.■

Chapter 5 A & M : Integrally Closed Domains, Valuation Rings–Nate

Proposition 5.17. Let A be an integrally closed domain, K its quotient field, L a finite separable algebraic extension of K, and B the integral closure of A in L. Then there exists a basis $v_1, \dots v_n$ of L over K such that $B \subseteq \sum_{j=1}^{n} A v_j$.

Definition 5.17a. Let B be an integrally closed domain, K its quotient field. Then B is a *valuation ring of* K if, for each $x \in B$ with $x \neq 0$, either $x \in B$ or $x^{-1} \in B$.

Proposition 5.18. Let B be a valuation ring. Then:

(1) B is a local ring.
(2) For every ring B' such that $B \subseteq B' \subseteq K$, B' is also a valuation ring of K.
(3) B is integrally closed in K.

Proof. (1) Let $M = \{\text{non-units in } B\}$. Then $x \in M$ if $x = 0$ or $x^{-1} \in K \setminus B$.
Claim: M is an ideal.
Proof: If $a \in B, x \in M$, then $ax \in M$. Let $x, y \in M \setminus \{0\}$. Then either $x^{-1}y$ or $xy^{-1} \in B$. WLOG, assume $xy^{-1} \in B$. Then $x + y = (xy^{-1} + 1)y \in M$.
Since M is an ideal, we must have B is local.
(2) Easy
(3) Let $x \in K$ be integral over B. If $x \in B$, done. If $x \notin B$, then $x^{-1} \in B$. Since x is integral, we have $x^n + b_{n-1}x^{n-1} + ... + b_0 = 0$ for some $b_i \in B$. Now, multiply by $(x^{-1})^{n-1}$ to get $x = -(b_{n-1} + ... + b_0 x^{1-n}) \in B$.
□

Existence of valuation rings

Construction 5.18a. Let K be a field and Ω an algebraically closed field. Let $\Sigma = \{(A, f)$, where A is a subring of K and $f : A \to \Omega\}$. For $(A, f), (A, f') \in \Sigma$, we say
$(A, f) \leq (A, f') \iff A \subseteq A'$ and $f'|_A = f$. Note $\Sigma \neq 1\emptyset$ (either K and Ω contain $\mathbb{Z}$ or $\mathbb{Z}_p$ and just take f to be the identity). Then Σ contains maximal elements by Zorn's Lemma.

Lemma 5.19. Let B be a maximal element of Σ from (5.18a). Then B is a local ring and $\mathbf{m} = \ker g$ is the maximal ideal of B.

Proof. Note $g(B)$ is a subring of a field. So $g(B)$ is an integral domain which implies $\ker g$ is prime. So extend g to $\overline{g} : B_m \hookrightarrow \Omega$ where $\overline{g}(\frac{a}{b}) = \frac{g(a)}{g(b)}$. Now $B \subseteq B_m$ and $\overline{g}|_B = g$. Since B was maximal in Ω, we must have $B = B_m$. So B is a local ring and $m = \ker g$ is the maximal ideal. □

Lemma 5.20. With the setup of (5.18a), let $x \in K$, $x \neq 0$. Let $B[x]$ be the subring of K generated by x over B and let $\mathbf{m}[x]$ be the extension of $\mathbf{m}$ to $B[x]$. The either $\mathbf{m}[x] \neq B[x]$ or $\mathbf{m}[x^{-1}] \neq B[x^{-1}]$.

Proof. By contradiction. □

Theorem 5.21. Let B be a maximal element of Σ from (5.18a). Then B is a valuation ring of K.

Proof. Let $x \neq 0$ in K be given. WLOG, we may assume $m[x] \neq B[x]$ by the Lemma. Then there exists a maximal ideal m' of $B[x]$ such that $m' \supseteq m[x]$. Furthermore, $m' \cap B = m$.

$$\begin{array}{ccc} B & \xrightarrow{\ i\ } & B[x] =: B' \\ {\scriptstyle\pi}\downarrow & & {\scriptstyle\pi'}\downarrow \\ k := B/m & & k' := B'/m' \end{array}$$

Define $\overline{i} : k \to k'$ by $b + m \mapsto b + m'$. Then $\overline{i}$ is injective (as it is a nonzero field map) and the diagram commutes.

Claim: $k' = k[\overline{x}]$ for $\overline{x} = \pi'(x)$.

Proof: Every element of B'/m' is of the form $\overline{a_n}\overline{x}^n + ... + \overline{a_0}$. We will show $\overline{a_j} \in k$. Now $\overline{a_j} = \pi' \circ i(a_j) = \overline{i} \circ \pi(a_j)$ which implies $\overline{a_j} \in k$ as $\overline{i}$ is injective.

By Lemma 1.9 in Ueno (if an integral domain which is finitely generated over a field is a field, then every element of it is algebraic over the smaller field), we get $\overline{x}$ is algebraic over k. So k' is a finite algebraic extension of k. So consider $\overline{g} : k \to \Omega$. We can extend this to $\overline{g}' : k' \to \Omega$ so that $b' \xrightarrow{\pi'} k' \xrightarrow{\overline{g}'} \Omega$. Of course, B was maximal in Ω. Thus $B = B' = B[x]$ which implies $x \in B$. □

Corollary 5.22. Let A be a subring of a field K. Then the integral closure $\overline{A}$ of A in K satisfies
$\overline{A} = \cap\{V \mid V \text{ is a valuation ring of } K \text{ with } A \subseteq V\}$.

Corollary 5.23. Let $A \subseteq B$ be integral domains, with B finitely generated over A. Then there exists a $u \in A, u \neq 0$ such that Property (*) holds:

Property (*): For every homomorphism $f : A \to \Omega$, where Ω is an algebraically closed field, if $f(u) \neq 0$, then there exists a homomorphism $g : B \to \Omega$ such that $g(v) \neq 0$.

Corollary 5.24. Let k be a field and B a finitely generated k-algebra. If B is a field, then it is a finite algebraic extension of k.

6. Chapter 6: Chain Conditions—Lori

Let Σ be a set partially ordered by a relation $\leq$, which is reflexive and transitive and satisfies $a \leq b, b \leq a \implies a = b$.

Proposition 6.1. The following are equivalent:

(1) Every increasing sequence $x_1 \leq x_2 \leq \cdots$ in Σ is stationary (ie. $\exists n$ s.t. $x_n = x_{n+1} = \cdots$).

(2) Every non-empty subset of Σ has a maximal element.

Proof: (1)⇒(2): If (2) doesn't hold, then there exists $T \subseteq \Sigma$, nonempty with no maximal element. So, given $x_i \in T$, $\exists x_{i+1} \in T$ s.t. $x_i \leq x_{i+1}$. Use this to create a subsequence that is not stationary.

(2)⇒(1): For any sequence $(x_n)_{n=1}^{\infty}$, the set $T = \{x_n : n \geq 1\}$ has a maximal element, x_m. So $x_i = x_m$ for $i \geq m$.□

Definitions 6.1a. Let Σ be the set of submodules of a module M, ordered by $\subseteq$. Then (1) is the *ascending chain condition (acc)* on M and (2) is the *maximal condition.* An A-module M that satisfies (1) or (2) is called *Noetherian.*

A ring A is *Noetherian* if it is Noetherian as an $A-$module (i.e., if it satisfies acc on ideals).

For Σ the set of submodules of a module M, ordered by $\supseteq$, (1) is the *descending chain condition (dcc)* and (2) is the *minimal condition.* A module satisfying either one of these is *Artinian.*

Examples 6.1b. (1) Let $G = \{\overline{x} \in \mathbb{Q}/\mathbb{Z} \mid |\overline{x}| = p^n \text{ for some prime } p \text{ and some } n \geq 0\}$, a subgroup of $\mathbb{Q}/\mathbb{Z}$. Then, for each $n \geq 0,\ G$ has exactly one subgroup of order p^n, namely $G_n = \left\langle \frac{1}{p^n} + \mathbb{Z} \right\rangle$. Then $G_0 \subset G_1 \subset \cdots \subset G_n \subset \cdots$ (with strict inclusions), so that G does not satisfy the acc. However, G does satisfy the dcc, because the only proper subgroups of G are the G_n.

(2) Let X be a compact Hausdorff space and $C(X)$ the ring of real valued continuous functions on X. Then given a strictly decreasing sequence of closed sets $F_1 \supset F_2 \supset \cdots$ in X, let $I_n = \{f \in C(X) : f(F_n) = 0\}$. Then $(I_n)_{n \geq 1}$ forms a strictly increasing sequence of ideals in $C(X)$, so $C(X)$ is not Noetherian.

Proposition 6.2. M is a Noetherian $A-$module $\iff$ every submodule of M is finitely generated.

Proof ($\Rightarrow$) Suppose M is a Noetherian $A-$ module, and let N be a submodule of M. Let $\Sigma = \{K : K \text{ is a finitely generated submodule of } N\}$. Note $(0) \in \Sigma$ so $\Sigma \neq \emptyset$. So by Zorn's Lemma, Σ has a maximal element, N_0. If $N_0 \neq N$, choose $x \in N \backslash N_0$. Then the module $N_0 + Ax \subset N$ is finitely generated and properly contains N_0, contradicting the maximality of N_0. Thus, $N_0 = N$ and so N is finitely generated.

($\Leftarrow$) Suppose every submodule of M is finitely generated, and let $M_1 \subseteq M_2 \subseteq \cdots$ be an ascending chain in M. Then $N = \bigcup_{n=1}^{\infty} M_n$ is a submodule of M, hence finitely generated, by say $\{x_1, ..., x_n\}$. Then for each i, $x_i \in M_{n_i}$ for some n_i. Let $k = \max\{n_i : 1 \leq i \leq n\}$. Then $x_i \in M_k$ for any i. Hence, $M_j = M_k$ for any $j \geq k$.□

Proposition 6.3. Let $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ be an exact sequence of $A-$ modules. Then

(1) M is Noetherian $\iff$ M' and M'' are Noetherian.

(2) M is Artinian $\iff$ M' and M'' are Artinian.

Proof (1) ($\Rightarrow$) Suppose M is Noetherian. Then given any chain $M_1 \subseteq M_2 \subseteq \cdots$ in M', $\alpha(M_1) \subseteq \alpha(M_2) \subseteq \cdots$ in M must be stationary. Since α is injective, we have $M_1 \subseteq M_2 \subseteq \cdots$ is stationary in M'. Conversely, any ascending chain in M'' gives rise to an ascending chain in M, hence is stationary.

($\Leftarrow$) Now suppose both M' and M'' are Noetherian. Let $(M_n)_{n=1}^{\infty}$ be an ascending chain in M. Then $\left(\alpha^{-1}(M_n)\right)$ and $(\beta(M_n))$ are ascending chains in M' and M'', respectively, hence stationary. Choosing N large enough that both chains are stationary for $k \geq N$, we have that (M_n) is stationary.

The proof of (2) is similar.□

Corollary 6.4. If A-modules M_i are Noetherian (respectively, Artinian) $A-$modules, for all i with $1 \leq i \leq n$, then so is $\oplus_{i=1}^{n} M_i$.

Proof Induct on n :

If $n = 2$, then the sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ is exact, so by Prop. 6.3 $M_1 \oplus M_2$ is Noetherian.

If $n > 2$, consider the exact sequence $0 \to M_1 \to \oplus_{i=1}^{n} M_i \to \oplus_{i=2}^{n} M_i \to 0$. By induction, $\oplus_{i=2}^{n} M_i$ is Noetherian. Thus, by (6.3) we have $\oplus_{i=1}^{n} M_i$ is Noetherian.□

Proposition 6.5. Let A be a Noetherian (resp, Artinian) ring and M a finitely generated $A-$module. Then M is Noetherian (respectively, Artinian).

Proof Say $M = x_1A + \cdots x_nA$. Then M can be thought of as a quotient of A^n, say A^n/N. Then $0 \to N \to A^n \to A^n/N \to 0$ is an exact sequence. A^n is Noetherian by (6.4), so A^n/N is Noetherian by (6.3). Hence, M is Noetherian as $M \cong A^n/N$.□

Proposition 6.6. Let A be a Noetherian ring (resp, Artinian) and I an ideal of A. Then A/I is a Noetherian ring.

Proof: $0 \to I \to A \to A/I \to 0$ is an exact sequence of $A-$modules, so by (6.3) A/I is Noetherian as an $A-$module. Hence, A/I is Noetherian as an A/I module.□

Definitions 6.6a. A *chain* of submodules of a module M is a sequence $(M_i)_{i=0}^n$ of submodules such that

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0 \quad \text{(strict inclusions)}$$

The *length* of the chain is n.

A *composition series* of M is a maximal chain (ie one in which no extra submodules can be inserted).

Thus $(M_i)_{i=0}^n$ is a composition series $\iff$ M_i/M_{i+1} is simple, for each $0 \leq i \leq n-1$.

Proposition 6.7. Suppose M has a composition series of length n. Then every composition series of M has length n and every chain in M can be extended to a composition series.

Proof: Let $\ell(M)$=least length of a compostion series of M. (So $\ell(M) = \infty$ if M has no composition series.)

Claim 1: $N \subsetneq M \Rightarrow \ell(N) \lneq \ell(M)$.

Proof: Let $(M_i)_{i=1}^n$ be a composition series of M of minimal length and consider $N_i = N \cap M_i$, for each i. Since $N_{i-1}/N_i \subseteq M_{i-1}/M_i$, either $N_{i-1}/N_i = M_{i-1}/M_i$ or $N_{i-1}/N_i = 0$ (as M_{i-1}/M_i is simple). So, removing repeated terms we have a composition series of N. Therefore $\ell(N) \leq \ell(M)$.

If $\ell(N) = \ell(M) = n$ then $N_{i-1}/N_i = M_{i-1}/M_i$ for each i, so $M_{n-1} = N_{n-1}, M_{n-2} = N_{n-2}$, etc. Therefore, $M = N$.

Claim 2: Every chain in M has length $\leq \ell(M)$.

Pf. Let $M = M_0 \supset M_1 \supset \cdots \supset M_k = 0$ be a chain of length k. By claim 1, $\ell(M) > \ell(M_1) > \cdots > \ell(M_k) = 0$ Hence, $\ell(M) \geq k$.

Finally, consider any composition series of M. If it has length k, then $k \leq \ell(M)$ by claim 2. Hence, $k = \ell(M)$ by definition of $\ell(M)$. Hence, all composition series have the same length. Now, consider any chain. If its length is $\ell(M)$ it must be a composition series by claim 2. If its length is $< \ell(M)$, it is not a composition series, hence not maximal. Therefore, new terms may be inserted until the length is $\ell(M)$.□

Proposition 6.8. M has a composition series $\iff$ M satisfies both chain conditions.

Proof ($\Rightarrow$) All chains in M have finite length, hence both acc and dcc hold.

($\Leftarrow$) Now suppose acc and dcc hold for M. Construct a compostition series in the following way:

Since $M = M_0$ satisfies the maximum condition, there exists a maximal submodule $M_1 \subset M_0$. Similarly, M_1 has a maximal submodule $M_2 \subset M_1$. Continue in this way to get a strictly descending chain $M_0 \supset M_1 \supset \cdots$ By the dcc, this chain must be finite, and hence is a composition series of M.□

Homework notes from Chapter 6 A & M : (pp.78–70)

(1) Problem 4 (done by Laura, recommended by Lori): ${}_AM$ Noetherian, $I = \operatorname{Ann} M \implies A/I$ Noetherian. Not true for "Artinian".

7. Chapter 7: Noetherian Rings—Laura

Definition. A ring A is *Noetherian*, if it satisfies any of the following equivalent conditions:

- Every nonempty set of ideals in A has a maximal element
- Every ascending chain of ideals in A is stationary (i.e., there exists an n such that $I_n = I_{n+1} = I_{n+2} = \cdots$)

- Every ideal in A is finitely generated.

Proposition 7.1 If A is Noetherian and $\phi : A \to B$ is a surjective ring homomorphism, then B is Noetherian.

Proof. By the First Isomorphism Theorem, $B \cong A/\ker\phi$. Since $\ker\phi$ is an ideal, Proposition 6.6(p 76) tells us $A/\ker\phi$ (and therefore B) is Noetherian. □

Proposition 7.2 Let A be a subring of B, A be Noetherian, and B finitely generated as an $A-$module. Then B is a Noetherian ring.

Proof. By Proposition 6.5 (p 76), B is Noetherian as an $A-$module and therefore as a $B-$module. Thus B is Noetherian as a ring. □

Proposition 7.3 If A is Noetherian and S is a m.c.s of A, then $S^{-1}A$ is Noetherian.

Proof. By Proposition 3.11(i) (p 41), every ideal of $S^{-1}A$ is an extended ideal of A. So for a nonempty set of ideals of $S^{-1}A$, say $\mathcal{I}$, we have that $\mathcal{I} = \{S^{-1}I_\alpha\}$ where $\{I_\alpha\}$ are ideals of A. Since A is Noetherian, every nonempty set of ideals has a maximal element. Thus $\{I_\alpha\}$ has a maximal element, call it I. Of course, S^{-1} preserves inclusion so we must have $S^{-1}I$ is maximal in $\mathcal{I}$. Thus $S^{-1}A$ is Noetherian. □

Corollary 7.4 If A is Noetherian and p a prime ideal of A, then A_p is Noetherian.

Proof. Recall that $A_p = S^{-1}A$ where $S = A \setminus p$. By Proposition 7.3, done. □

Theorem 7.5 *Hilbert's Basis Theorem.* If A is Noetherian, then $A[x]$ is Noetherian.

Proof. Let α be an ideal in $A[x]$. We show α is finitely generated. Let I be the set of leading coefficients of polynomials in α.

Claim: I is an ideal.

Proof: If a_n is the leading coefficient of $f \in \alpha$, then $r\alpha_n$ is the leading coefficient of $rf \in \alpha$ and if b_m is the leading coefficient of $g \in \alpha$, then $x^{m-n}f + g$ (assuming $m > n$, if not flip it) has leading coefficient $a_n + b_m$.

Furthermore, since A is Noetherian, I is finitely generated. Say $I = (a_1, ..., a_n)$ where a_i is the leading coefficient of $f_i \in \alpha$. Let $r_i := \deg f_i$ and define $r := \max_{1\le i\le n} r_i$. Note that $\{f_i\}_1^n$ generate an ideal $\alpha' \subseteq \alpha$.

Let $f = ax^m +$(lower terms) $\in \alpha$. Then $a \in I$. If $m \ge r$, find $u_i \in A$ such that $a = \sum u_i a_i$. Then $f - \underbrace{\sum i_i f_i x^{m-r_i}}_{\in\alpha'} \in$ α and has $\deg < m$. Continue to get a polynomial $g \in \alpha$ such that $f = g + h$ where $h \in \alpha'$.

Let M be the $A-$module generated by $\{1, x, ..., x^{r-1}\}$. The above shows that $\alpha = (\alpha \cap M) + \alpha'$. Of course, M is finitely generated and thus is Noetherian (by Proposition 6.5 (p 76)). Thus $\alpha \cap M$, a submodule of M, is finitely generated by Proposition 6.2 (p 75). Say $\{g_1, ..., g_m\}$ generate $\alpha \cap M$. Then $\{g_1, ..., g_m, f_1, ..., f_n\}$ generate $(\alpha \cap M) + \alpha' = \alpha$. Thus we have shown α is finitely generated and thus $A[x]$ is Noetherian. □

Corollary 7.6 If A is Noetherian, so is $A[x_1, ..., x_n]$.

Proof. Induct on n. If $n = 1$, done by HBT. Let $n > 1$. Then A Noetherian implies $A[x_1, ..., x_{n-1}]$ is Noetherian by induction and $A[x_1, ..., x_{n-1}]$ Noetherian implies $A[x_1, ..., x_n]$ is Noetherian by the base case. □

Let $f : A \to B$ be a ring homomorphism where B is commutative. Recall that B is then considered to be an $A-$module with multiplication by a defined by $f(a)b$ and we say B is an $A-$**algebra**. If B is finitely generated as a ring over $f(A)$, then we say B is a finitely generated $A-$algebra.

Corollary 7.7 Let B be a finitely generated $A-$algebra. If A is Noetherian, then so is B. In particular, every finitely generated ring and every finitely generated algebra over a field is Noetherian.

Proof. Say that B is generated by $s_1, ..., s_n$. Then $B = A[s_1, ..., s_n]$. For B a commutative ring, we can consider B as being isomorphic to the polynomial ring $A[x_1, ..., x_n]$. Then, by the above Corollary, B is Noetherian. □

Proposition 7.8 Let $A \subseteq B \subseteq C$ be rings. Suppose A is Noetherian, C is finitely generated as an $A-$algebra and C is either

(1) finitely generated as a $B-$module, or
(2) integral over B.

Then B is finitely generated as an $A-$algebra.

Proof. First note that Proposition 5.1 and Corollary 5.2 (pp 59-60), show that (1) $\Leftrightarrow$ (2). Thus, we will assume C is a finitely generated $B-$module. Let $x_1, ..., x_m$ generate C and an $A-$algebra and $y_1, ..., y_n$ generate C as a $B-$module. Then

$$(*)x_i = \sum_j b_{ij} y_j \qquad \text{and} \qquad (**)y_i y_j = \sum_k b_{ijk} y_k \text{ for } b_{ij}, b_{ijk} \in B.$$

Let B_0 be the algebra generated over A by $\{b_{ij}\}$ and $\{b_{ijk}\}$. Then $A \subseteq B_0 \subseteq B$. By the above corollary, B_0 is Noetherian.

Now, every element of C is a polynomial in the x_i with coefficients in A. Replacing the x_i with $\sum_j b_{ij} y_j$ by $(*)$ and then repeatedly using $(**)$, we can show that each element of C is a linear combination of the y_j with coefficients in B_0. So C is finitely generated as a B_0-module. Since B_0 is Noetherian and $B \subseteq C$, Propositions 6.2 and 6.5 (p 76) tell us B is finitely generated as a B_0-module. Now B_0 a finitely generated $A-$algebra together and B a finitely generated B_0-module implies B is finitely generated as an $A-$algebra. □

Definition. Let A be a ring. Define the *degree* of $p(x) \in A[[x]]$ to be the smallest power of x such that the coefficient of the term in x^d is nonzero and the *leading coefficient* of $p(x) \in A[[x]]$, $\ell(p)$ to be the coefficient of the term with the smallest power of x.

Theorem 7.5′ *Hilbert Basis Theorem for Power Series.* Hungerford, pp. 392-393, modified. If A is Noetherian, then so is $A[[x]]$.

Proof. Let J be an ideal of $A[[x]]$. Define ideals of A as follows

$$\begin{aligned} h_0 &= \{\ell(p(x)) | p(x) \in J, \deg p(x) = 0\} \cup \{0\} \\ h_1 &= \{\ell(p(x)) | p(x) \in J, \deg p(x) = 1\} \cup \{0\} \\ &\vdots \\ h_i &= \{\ell(p(x)) | p(x) \in J, \deg p(x) = i\} \cup \{0\} \end{aligned}$$

Then h_i is an ideal for all i :

- Let $a \in h_i$, $r \in A$. Say $a = \ell(p(x))$ for $p(x) \in J$. Then $ra = \ell(rp(x))$ and $rp(x) \in J$.
- Let $a, b \in h_i$ such that $a = \ell(p(x))$ and $b = \ell(q(x))$ for $p(x), q(x) \in J$. Then if $a + b \neq 0$, then $a + b = \ell((p + q)(x))$ for $(p + q)(x) \in J$ and if $a + b = 0$ then $a + b \in h_i$.

Also $h_i \subseteq h_{i+1}$ for all i : If $a \in h_i$ is the leading coefficient of $p(x) \in J$ where $\deg p(x) = i$, then a is the leading coefficient of $xp(x) \in J$ where $\deg xp(x) = i + 1$. Thus we have the chain of ideals $h_0 \subseteq h_1 \subseteq h_2 \subseteq \cdots$. Since A is Noetherian, this chain is stationary, that is, there exists m such that $h_m = h_j$ for all $j \geq m$. Since A is Noetherian, each h_i is finitely generated. Let h_i be generated by $a_{i,1}, ..., a_{i,t_i}$ the leading coefficients for $p_{i,1}, ..., p_{i,i_t}$ for all $i \leq m$. Let P be the ideal generated by the $p_{i,j}$ for all $i \leq m, j \leq i_t$. We show $J \subseteq P$.

Claim 1: Suppose there exists $q \in J$ and $\deg q = i < m$. Then there exists a $g \in P$ such that $q - g \in J$ and $\deg q - g = \geq i + 1$.

Proof: If $\deg q = i < m$, then $\ell(q) \in h_i$, which implies there exist $\{u_k\}_{k=1}^{t_i}$ such that $\ell(q) = \sum_{k=1}^{t_i} u_k a_{i,k}$. Then $q - \sum_{k=1}^{t_i} u_k p_{i,k} \in J$ has degree $> i$.

Returning to the theorem, redefine $h_m :=< a_1, ..., a_t >$ where $a_i = \ell(p_i)$ for simplicity.

Claim 2: Let $q \in J$. There exists $\alpha_i \in A[[x]]$ such that $q - \sum \alpha_i p_i = 0$, that is, $q \in P$.

Proof: By Claim 1, we may assume $q = c_m x^m + q'$ for $q' \in A[[x]]$ such that $\deg q' > m$. Then, $c_m \in h_m$, which implies $c_m = \sum_{i=1}^{t} b_{i,0} a_i$ for some $b_{i,0} \in A$. Let ${}_0\alpha_i := b_{i,0}$. Then $q - \sum_{i=1}^{t} {}_0\alpha_i p_i$ has degree $> m$. Say $q - \sum_{i=1}^{t} {}_0\alpha_i p_i = c_{m+1} x^{m+1} + q''$ for $q'' \in A[[x]]$ such that $\deg q'' > m+1$. Then, $c_{m+1} \in h_{m+1} = h_m$, which implies $c_{m+1} = \sum_{i=1}^{t} b_{i,1} a_i$. Let ${}_1\alpha_i = b_{i,0} + b_{i,1} x$. Then $q - \sum_{i=1}^{t} {}_1\alpha_i p_i$ has degree $> m+1$. Now, continue to define ${}_n\alpha_i = \sum_{j=0}^{n} b_{i,j} x^j$ for all n such that $q - \sum_{i=1}^{t} {}_n\alpha_i p_i$ has degree $> m+n$. Then, let $\alpha_i := \sum_{j=0}^{\infty} b_{i,j} x^j \in A[[x]]$ and observe $q - \sum_{i=1}^{t} \alpha_i p_i = 0$.

Thus $J \subseteq P$. Since P is finitely generated, J is as well. Thus $A[[x]]$ is Noetherian. □

Chapter 7: Primary Decompositions of Ideals in Noetherian Rings—Silvia S.

Definition. An ideal $\mathfrak{q}$ in a ring A is *primary* if $\mathfrak{q} \neq A$ and

$$xy \in \mathfrak{q} \quad \Longrightarrow \quad \text{either } x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n > 0.$$

Equivalently, if $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$, then $y \in r(\mathfrak{q})$.

Note. An ideal $\mathfrak{q}$ of A is primary if and only if $A/\mathfrak{q} \neq 0$ and every zero-divisor in $A/\mathfrak{q}$ is nilpotent.

Definition. If $\mathfrak{q}$ is a primary ideal of a ring A, then $\mathfrak{q}$ is said to be $\mathfrak{p}$-*primary* (or *primary for* $\mathfrak{p}$) and the prime ideal $\mathfrak{p} = r(\mathfrak{q})$ is called the *associated prime* to $\mathfrak{q}$.

Definition. An ideal $\mathfrak{a}$ in a ring A has a *primary decomposition* if it may be written as a finite intersection of primary ideals, i.e.

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i \ ,$$

where $\mathfrak{q}_i$ is a primary ideal of A.

The primary decomposition above is said to be *minimal* (or *irredundant*) if

(1) no primary ideal contains the intersection of the remaining primary ideals, i.e. $\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$ for all i, and

(2) the associated prime ideals are all distinct: $r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ for $i \neq j$.

In this case, the $\mathfrak{q}_i$ are called the *primary components of* $\mathfrak{a}$ and the $\mathfrak{p}_i = r(\mathfrak{q}_i)$ are called the *associated prime ideals* of $\mathfrak{a}$.

If an associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$ does not contain any other associated prime ideal of $\mathfrak{a}$, then $\mathfrak{p}$ is called an *isolated prime ideal*. The remaining associated prime ideals of $\mathfrak{a}$ are called *embedded prime ideals*.

Definition. A proper ideal $\mathfrak{a}$ of a ring A is said to be *irreducible* if $\mathfrak{a}$ cannot be written nontrivially as the intersection of two other ideals, i.e.

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \quad \Longrightarrow \quad \mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c} \ .$$

Note. A prime ideal is irreducible. Primary ideals need not be irreducible (e.g., the ideal $(x, y)^2$ in $k[x, y]$ is a primary ideal, but is not irreducible since it is the intersection of the ideals (x, y^2) and (x^2, y)).

We now prove that in a Noetherian ring every proper ideal has a (minimal) primary decomposition.

Lemma 7.11.In a Noetherian ring A, every proper ideal is a finite intersection of irreducible ideals.

Proof. Let A be a Noetherian ring and let $\mathfrak{a}$ be an ideal of A. If $\mathfrak{a}$ is irreducible, then we are done. If not, then $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$ for some ideals $\mathfrak{a}_1, \mathfrak{a}_2$ of A with $\mathfrak{a} \subseteq \mathfrak{a}_i$, $i = 1, 2$. If both $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are irreducible, then we are done. Otherwise, assume $\mathfrak{a}_1$ is reducible and write $\mathfrak{a}_1 = \mathfrak{a}_1^{(1)} \cap \mathfrak{a}_2^{(1)}$. By repeating this process, we obtain an ascending chain of ideals of A,

$$\mathfrak{a} \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_1^{(1)} \subseteq \cdots .$$

Since A is Noetherian, this process must terminate, i.e. $\mathfrak{a}$ is a finite intersection of irreducible ideals.

Therefore every ideal in a Noetherian ring A is a finite intersection of irreducible ideals. □

Lemma 7.12. In a Noetherian ring A, every irreducible ideal is primary.

Proof. Suppose A is a Noetherian ring and $\mathfrak{a}$ is an irreducible ideal of A. Note that $\mathfrak{a} \neq A$.

Consider the quotient $\overline{A} = A/\mathfrak{a}$ and note that $\overline{A} \neq 0$ (since $\mathfrak{a} \neq A$). By Proposition (6.6), $\overline{A}$ is a Noetherian ring.

Suppose $\bar{x}$ is a zero divisor in $\overline{A}$. Then there is $\bar{y} \in \overline{A}, \bar{y} \neq \bar{0}$ such that $\bar{x}\bar{y} = \bar{0}$ in $\overline{A}$. Consider the ascending chain of ideals in A

$$\mathrm{Ann}(\bar{x}) \subseteq \mathrm{Ann}(\bar{x}^2) \subseteq \cdots .$$

Since $\overline{A}$ is Noetherian, the chain is stationary and hence there is $n \in \mathbb{N}$ such that $\mathrm{Ann}(\bar{x}^n) = \mathrm{Ann}(\bar{x}^{n+1}) = \cdots$.

If $\bar{a} \in (\bar{y}) \cap (\bar{x}^n)$, then $\bar{a} = \bar{b}\bar{y} = \bar{c}\bar{x}^n$ for some $\bar{b}, \bar{c} \in \overline{A}$. Thus

$$\bar{a}\bar{x} = \bar{b}\bar{y}\bar{x} = 0 \quad \Longrightarrow \quad \bar{c}\bar{x}^{n+1} = \bar{c}\bar{x}^n\bar{x} = \bar{a}\bar{x} = 0 .$$

So $\bar{c} \in \mathrm{Ann}(\bar{x}^{n+1}) = \mathrm{Ann}(\bar{x}^n)$. Hence $\bar{a} = \bar{c}\bar{x}^n = \bar{0}$. That is, $(\bar{y}) \cap (\bar{x}^n) = (\bar{0})$.

Since there is a bijective correspondence between ideals of $\overline{A}$ and ideals of A containing $\mathfrak{a}$ and since $\mathfrak{a}$ is irreducible, $(\bar{0})$ is irreducible. Hence $(\bar{y}) = (\bar{0})$ or $(\bar{x}^n) = (\bar{0})$. Since $\bar{y} \neq \bar{0}$, it follows that $\bar{x}^n = \bar{0}$. Thus, $\bar{x}$ is a nilpotent element of $\overline{A}$. Hence $\mathfrak{a}$ is a primary ideal of A by Remark 1.1(1) from Chapter 4.

Therefore every irreducible ideal in a Noetherian ring A is a primary ideal. □

Theorem 7.13. *(Primary Decomposition Theorem)* Let A be a Noetherian ring. Then every ideal $\mathfrak{a} \neq A$ has a minimal primary decomposition. If

$$\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i = \bigcap_{j=1}^{n} \mathfrak{q}'_j$$

are two minimal primary decompositions for $\mathfrak{a}$, then the sets of associated primes in the two decompositions are the same:

$$\{r(\mathfrak{q}_1), \ldots, r(\mathfrak{q}_m)\} = \{r(\mathfrak{q}'_1), \ldots, r(\mathfrak{q}'_n)\} .$$

Moreover, the primary components $\mathfrak{q}_i$ so that $r(\mathfrak{q}_i)$ are minimal elements in this set of associated primes are uniquely determined by $\mathfrak{a}$.

Proof. The fact that in a Noetherian ring every proper ideal has a primary decomposition follows from the previous Lemmas.

If any of the primary ideals in the decomposition contains the intersection of the remaining primary ideals, then we may simply remove this ideal since this will not change the intersection. Hence we may assume the decomposition satisfies (1) in the definition of a minimal primary decomposition. Since a finite intersection of $\mathfrak{p}$-primary ideals is again $\mathfrak{p}$-primary, replacing the primary ideals in the decomposition with the intersections of all those primary ideals belonging to the same prime, we may also assume the decomposition satisfies (2) in the definition of a minimal primary decomposition.

The proof of the uniqueness of the set of associated primes is a consequence of Proposition (7.17). Indeed, Proposition (7.17) shows that the associated primes for a minimal primary decomposition are precisely the collection

of prime ideals among the ideals $(\mathfrak{a} : x)$ for $x \in A$ and thus the associated primes for a minimal primary decomposition are uniquely determined by $\mathfrak{a}$ independent of the minimal primary decomposition. Hence

$$\{\mathfrak{p}_i = r(\mathfrak{q}_i) : i = 1, \ldots, m\} = \{\mathfrak{p} \in \mathrm{Spec}(A) | \mathfrak{p} = (\mathfrak{a} : x) \text{ for some } x \in A \ \} = \{\mathfrak{p}'_j = r(\mathfrak{q}'_j) : j = 1, \ldots, n\} \ .$$

By minimality, it follows that $m = n$.

The proof of the uniqueness of the primary components associated to the minimal primes can be found in [2, Corollary 44, page 717]. □

Remark. The primary decomposition of an ideal is not necessarily unique. For example, in $\mathbb{R}[x, y]$, $I = (x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$ are two distinct minimal primary decompositions. The associated primes for I are (x) and $r((x, y)^2) = r((x^2, y)) = (x, y)$. Thus I has two distinct minimal primary decompositions, but the set of associated primes in the two decompositions are the same. Moreover, $r((x)) = (x)$ is minimal and (x) appears in both the minimal primary decompositions for I.

Proposition 7.14. In a Noetherian ring A, every ideal $\mathfrak{a}$ contains a power of its radical.

Proof. Let $\mathfrak{a}$ be an ideal of A. Since A is Noetherian, $r(\mathfrak{a})$ is finitely generated, say $x_1, \ldots, x_k$ are generators of $r(\mathfrak{a})$. Then $x_i^{n_i} \in \mathfrak{a}$ for some n_i, $1 \leq i \leq k$.

Let $m = \sum_{i=1}^{k} (n_i - 1) + 1$. Then $r(\mathfrak{a})^m$ is generated by the products $x_1^{r_1} \cdots x_k^{r_k}$, where $\sum_{i=1}^{k} r_i = m$.

¿From the definition of m, we have $r_i \geq n_i$ for at least one index i. Hence each generator $x_1^{r_1} \cdots x_k^{r_k}$ of $r(\mathfrak{a})^m$ is in $\mathfrak{a}$.

Therefore $r(\mathfrak{a})^m \subseteq \mathfrak{a}$, i.e. every ideal $\mathfrak{a}$ of a Noetherian ring A contains a power of its radical. □

Corollary 7.15. In a Noetherian ring A, the nilradical $\mathcal{N} = r((0))$ is nilpotent.

Proof. Let $\mathfrak{N}$ denote the nilradical of A and note that $\mathfrak{N} = r(0)$. Apply the previous Proposition to the ideal (0) to get $\mathfrak{N}^n = r(0)^n \subseteq (0)$ for some integer n. Therefore $\mathfrak{N}^n = (0)$, i.e. the nilradical is nilpotent. □

Corollary 7.16. Let A be a Noetherian ring, $\mathfrak{m}$ a maximal ideal of A, $\mathfrak{q}$ any ideal of A. Then the following are equivalent:

(i) $\mathfrak{q}$ is $\mathfrak{m}$-primary;
(ii) $r(\mathfrak{q}) = \mathfrak{m}$;
(iii) $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ for some $n > 0$.

Proof. (i) $\iff$ (ii) By definition.

(ii) $\implies$ (iii) We have $\mathfrak{m}^n = r(\mathfrak{q})^n \subseteq \mathfrak{q}$ for some $n > 0$ by Proposition (7.14) and $\mathfrak{q} \subseteq r(\mathfrak{q}) = \mathfrak{m}$.

(iii) $\implies$ (ii) Since $\mathfrak{m}$ is prime, $r(\mathfrak{m}^n) = \mathfrak{m}$ for all $n > 0$. From $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ for some $n > 0$, it follows that $\mathfrak{m} = r(\mathfrak{m}^n) \subseteq r(\mathfrak{q}) \subseteq r(\mathfrak{m}) = \mathfrak{m}$, i.e. $r(\mathfrak{q}) = \mathfrak{m}$. □

Lemma 4.4 Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal, x an element of A. Then

(i) if $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = (1)$;
(ii) if $x \notin \mathfrak{q}$, then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary and hence $r(\mathfrak{q} : x) = \mathfrak{p}$;
(iii) if $x \notin \mathfrak{p}$, then $(\mathfrak{q} : x) = \mathfrak{q}$.

Proposition 7.17. Let A be a Noetherian ring and let $\mathfrak{a} \neq A$ be an ideal of A. Then the prime ideals which belong to $\mathfrak{a}$ are precisely the prime ideals which occur in the set of ideals $(\mathfrak{a} : x)$, $x \in A$.

Proof. Let $\mathfrak{a}$ be a proper ideal of a Noetherian ring A and let $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition for $\mathfrak{a}$. Define

$$\text{Assoc}(\mathfrak{a}) = \{\mathfrak{p}_i = r(\mathfrak{q}_i) : i = 1, \ldots, n\} \quad \text{and} \quad \mathcal{P} = \{\mathfrak{p} \in \text{Spec}(A) | \mathfrak{p} = (\mathfrak{a} : x) \text{ for some } x \in A \} .$$

($\supseteq$) Let $(\mathfrak{a} : x) \in \mathcal{P}$ be a prime ideal. Then

$$(\mathfrak{a} : x) = (\cap_{i=1}^{n} \mathfrak{q}_i : x) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : x) .$$

Since $(\mathfrak{a} : x)$ is prime, there is a j such that $(\mathfrak{a} : x) = (\mathfrak{q}_j : x)$ by 1.12. By Lemma (4.4), since $(\mathfrak{a} : x) \neq (1)$ (being a prime ideal), $x \notin \mathfrak{q}_j$ and so $(\mathfrak{q}_j : x)$ is $\mathfrak{p}_j$-primary and $r(\mathfrak{q}_j : x) = \mathfrak{p}_j$. Hence

$$(\mathfrak{a} : x) = r(\mathfrak{a} : x) = r(\mathfrak{q}_j : x) = \mathfrak{p}_j = r(\mathfrak{q}_j)$$

since $(\mathfrak{a} : x)$ is prime. Hence $(\mathfrak{a} : x) = r(\mathfrak{q}_j) \in \text{Assoc}(\mathfrak{a})$ and so $\mathcal{P} \subseteq \text{Assoc}(\mathfrak{a})$.

($\subseteq$) Let $\mathfrak{p}_j \in \text{Assoc}(\mathfrak{a})$. By Proposition (7.14), $\mathfrak{q}_j$ contains a power of its radical $\mathfrak{p}_j$, i.e. $\mathfrak{p}_j^t \subseteq \mathfrak{q}_j$ for some positive integer t. We have

$$(\cap_{i \neq j} \mathfrak{q}_i)\mathfrak{p}_j^0 = (\cap_{i \neq j} \mathfrak{q}_i) \not\subseteq \mathfrak{q}_j \quad \text{and} \quad (\cap_{i \neq j} \mathfrak{q}_i)\mathfrak{p}_j^t \subseteq (\cap_{i \neq j} \mathfrak{q}_i) \cap \mathfrak{p}_j^t \subseteq (\cap_{i \neq j} \mathfrak{q}_i) \cap \mathfrak{q}_j \subseteq \mathfrak{q}_j .$$

Choose $m > 0$ to be the smallest integer such that $(\cap_{i \neq j} \mathfrak{q}_i)\mathfrak{p}_j^m \subseteq \mathfrak{q}_j$. Then $(\cap_{i \neq j} \mathfrak{q}_i)\mathfrak{p}_j^{m-1} \not\subseteq \mathfrak{q}_j$.

Choose $y \in (\cap_{i \neq j} \mathfrak{q}_i)\mathfrak{p}_j^{m-1}$, $y \notin \mathfrak{q}_j$.

Then

$$y\mathfrak{p}_j \subseteq (\cap_{i \neq j} \mathfrak{q}_i)\mathfrak{p}_j^m \subseteq (\cap_{i \neq j} \mathfrak{q}_i) \cap \mathfrak{q}_j = \mathfrak{a} ,$$

i.e. $\mathfrak{p}_j \subseteq (\mathfrak{a} : y)$.

Also, since $(\cap_{i \neq j} \mathfrak{q}_i)\mathfrak{p}_j^{m-1} \subseteq (\cap_{i \neq j} \mathfrak{q}_i) \cap \mathfrak{p}_j^{m-1}$, $y \in \cap_{i \neq j} \mathfrak{q}_i$. Since $y \notin \mathfrak{q}_j$, by Lemma (4.4) $r(\mathfrak{q}_j : y) = \mathfrak{p}_j$. Noting that $r(\mathfrak{q}_i : y) = A$ for $i \neq j$ (since $y \in \mathfrak{q}_i$ for $i \neq j$), we have

$$\mathfrak{p}_j \subseteq (\mathfrak{a} : y) \subseteq r(\mathfrak{a} : y) = r(\cap_{i=1}^{n} \mathfrak{q}_i : y) = \bigcap_{i=1}^{n} r(\mathfrak{q}_i : y) = r(\mathfrak{q}_j : y) \cap (\cap_{i \neq j} r(\mathfrak{q}_i : y)) = r(\mathfrak{q}_j : y) = \mathfrak{p}_j .$$

Hence $\mathfrak{p}_j = (\mathfrak{a} : y)$, $y \in A$, and so $\text{Assoc}(\mathfrak{a}) \subseteq \mathcal{P}$.

Therefore $\text{Assoc}(\mathfrak{a}) = \mathcal{P}$. □

Problem 7.19 page 86 (worked by Silvia)
Let $\mathfrak{a}$ be an ideal in a Noetherian ring A. Let

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i = \bigcap_{j=1}^{s} \mathfrak{c}_j$$

be two minimal decompositions of $\mathfrak{a}$ as intersections of irreducible ideals. Prove that $r = s$ and that (possible after re-indexing the $\mathfrak{c}_j$) $r(\mathfrak{b}_i) = r(\mathfrak{c}_i)$ for all i.

Proof. Since in a Noetherian ring irreducible ideals are primary, the given decompositions are minimal primary decompositions of $\mathfrak{a}$. By Theorem (7.13), it follows that $r = s$ and (possible after re-indexing) $r(\mathfrak{b}_i) = r(\mathfrak{c}_i)$ for all i.
Problems worked by Laura:
8. If $A[x]$ is Noetherian, is A necessarily Noetherian?

Proof. I claim that A is necessarily Noetherian. Consider the map $\phi : A[x] \to A$ which sends a polynomial to its constant coefficient. This is a homomorphism as for $f, g \in A[x]$ with constant coefficients $a, b \in A$ respectively, we see the constant coefficient of $f + g$ is $a + b$ and the constant coefficient of fg is ab. Also, the identity maps to the identity. Now, this function is clearly surjective. Thus, by Proposition 7.1 (above), A is Noetherian. □

9. Let A be a ring such that for each maximal ideal m of A, the local ring A_m is Noetherian and for each $x \neq 0$ in A, the set of maximal ideals of A Show that A is Noetherian.

Proof. Let $I \neq 0$ be an ideal of A. Let $m_1, ..., m_r$ be the maximal ideals which contain I. Choose $x_0 \in I \setminus \{0\}$ and let $m_1, ..., m_{r+s}$ be the maximal ideals which contain x_0. Since $I \not\subseteq m_{r+j}$ for $j = 1, .., s$, there exists $x_j \in I$ such that $x_j \notin m_{r+j}$. Since A_{m_i} is Noetherian, $I_{m_i} \leq A_{m_i}$ (the extended image of I) is finitely generated for $1 \leq i \leq r$. Hence there exists $x_{s+1}, ..., x_t \in I$ whose images in A_{m_i} generate I_{m_i} for all $i = 1, .., r$. Let $I_0 = (x_0, ..., x_t)$. Then I_0 is finitely generated. We will show $I = I_0$.

- For $m \notin \{m_1, ..., m_r\}$ a maximal ideal, we know $I \not\subseteq m$. Thus there exists $x \in I$ such that $x \notin m$, that is, $x \in A - p$. So $1 \equiv \frac{x}{x} \in I_m$ which implies $I_m = A_m$. Similarly, since $I_0 \subseteq \{m_1, ..., m_r\}$ as well, $(I_0)_m = A_m$. Thus, for $(I_0)_m = I_m$.
- Now suppose $m \in \{m_1, ..., m_r\}$. Since $I_0 \subseteq I$, we know $(I_0)_m \subseteq I_m$. Of course, we also have $I_m = (x_{s+1}, ..., x_t)_m \subseteq (I_0)_m$. Thus $(I_0)_m = I_m$.

Thus we see $I_m = (I_0)_m$ for all maximal ideals m. So define $\phi : I_0 \to I$ by inclusion. Then we see $\phi_m : (I_0)_m \to I_m$ is both injective and surjective for all maximal ideals m and thus by Proposition 3.9 (p 40), we have that $\phi : I_0 \to I$ is an isomorphism. Since $I_0 \subseteq I$ we have $I_0 = I$. Therefore, since I_0 is finitely generated, I is finitely generated. Thus A is Noetherian. □

10. Let M be a Noetherian $A-$module. Show that $M[x]$ is a Noetherian $A[x]-$module.

Proof. This proof is almost exactly the same as that for the Hilbert Basis Theorem. I will go ahead and prove it-following a different proof for the Hilbert Basis Theorem than that which I presented above. Note that I will abuse the notation for an ideal by saying $(f_0, ..., f_k)$ is the submodule generated by $f_0, ..., f_k$. Recall Proposition 6.2 (p 75) which says M is a Noetherian $A-$module if and only if every submodule of M is finitely generated.

Let N be a submodule of $M[x]$. If N is finitely generated, then we are done. So let f_0 be a polynomial of least degree in N and inductively choose $f_{k+1} \in N \setminus (f_0, ..., f_k)$ of least degree. Let a_k be the leading coefficient of f_k and consider the submodule L generated by $\{a_i\}_{i=0}^{\infty}$. Since M is Noetherian, L is finitely generated. Say $L = (a_0, ..., a_n)$ for some n. Then $a_{n+1} = \sum_{i=0}^{n} u_i a_i$ for $u_i \in A$. Define $g(x) = \sum u_i x^{d_i} f_i$ where $d_i = \deg f_{n+1} - \deg f_i$. Then $\deg(f_{n+1} - g) < deg f_{n+1}$. Since f_{n+1} was chosen to have least degree, we see $f_{n+1} - g \in (f_0, ..., f_n)$. Of course, $g \in (f_0, ..., f_n)$ and since submodules are closed under addition, we see $f_{n+1} \in (f_0, ..., f_n)$. Contradiction- thus N is a finitely generated submodule. □

11. Let A be a ring such that each local ring A_p is Noetherian. Is A necessarily Noetherian?

Proof. I claim that A is NOT necessarily Noetherian. Consider the following counterexample. Let F be a field and $A = F \times F \times F \times \cdots$ an infinite product. Let p be a prime ideal and consider $\frac{a}{b} \in A_p$.

- If $a \notin p$, then $a \in A - p$ which says $\frac{b}{a} \in A_p$ and thus $\frac{a}{b}$ is a unit.
- If $a \in p$, then $a = (a_1, a_2, ...)$ is such that $a_i = 0$ for some i (otherwise, since A is an infinite product of fields, a is a unit- contradiction as a is contained in a prime ideal). So define $c = (c_1, c_2, ...)$ such that $c_i = 0$ if $a_i \neq 0$ and $c_i = 1$ if $a_i = 0$ for all i. Then $c \neq 0$ and $c \notin p$ (as otherwise $a + c \in p$ which implies p contains a unit). So $bc \in A \setminus p$ (since p is prime) and $\frac{a}{b} \equiv \frac{ac}{bc} \equiv \frac{0}{1}$.

Thus we have shown A_p is a field which implies it is Noetherian (fields have only two ideals which are both finitely generated). Of course, A is not Noetherian as it is an infinite product (the chain of ideals $((1, 0, 0, 0, ...)) \subseteq ((1, 1, 0, 0, ...)) \subseteq ((1, 1, 1, 0...)) \subseteq \cdots$ is not stationary). □

8. Atiyah McDonald, Chapter 10, completions—Micah

The goal of this presentation is to give the general construction for completions with a focus on I-adic completions of an R-module M where I is an ideal of R.

Remarks. Let G be a topological abelian group (written additively) such that the following mappings are continuous: $(a, b \in G) \quad \pi : G \times G \to G$, where $\pi(a, b) = a + b$ and $\text{inv} : G \to G$, where $\text{inv}(a) = -a$, and $\pi \circ (\text{id}, \text{inv})(a, b) = a - b$.

(1) Suppose G is T_1; then $(\pi \circ (\text{id}, \text{inv}))^{-1}(0)$, the *diagonal*, is closed in $G \times G \implies G$ is Hausdorff.

(2) $\forall a \in G$, $T_a(x) = x + a$ is a homeomorphism from G to G with inverse T_{-a}.

(3) Consequently there is a one two one correspondence between neighborhoods U of 0 and neighborhoods V of a given by $V = T_a(U) = U + a$.

Lemma 10.1: Let H be the intersection of all neighborhoods of 0 in a topological group G. Then
(i) H is a subgroup
(ii) $H = \overline{0}$
(iii) G/H is Hausdorff
(iv) G Hausdorff $\iff H = 0$.

Proof: First, for item (i): The mapping inv is a homeomorphism sending neighborhoods of 0 to neighborhoods of 0. Thus $a \in H \implies inv(a) = -a \in H$. Let $a, b \in H$. Let U be a neighborhood of 0. Then $-a \in U \implies 0 \in U + a$. Thus every neighborhood of 0 is a neighborhood of a and vice versa $\implies H = H + a$. Thus $a + b \in H + a + b = H + a = H$.

For item (ii): The closure of a set is the intersection of all open sets containing it.

For item (iii): G/H is again an abelian topological group. H is closed in G/H. Hence every point $H + x$ is closed in G/H. G/H is T_1. We have shown this implies G/H is Hausdorff.

For item (iv): $H = 0$ implies G is Hausdorff by (iii). Also G Hausdorff implies G is T_1 implies 0 is closed, which by (ii) implies $H = 0$.■

Definitions: *Completions using Cauchy sequences.* Assume that 0 in G has a countable basis of neighborhoods. That is, there exists a sequence of neighborhoods $\{U_n\}_{n\in\mathbb{N}}$ such that every neighborhood of 0 contains at least one of the U_n. Then a sequence $\{x_m\}_{m\in\mathbb{N}}$ in G is *Cauchy* provided that for every n there exist N such that $x_i - x_j \in U_n$ for all $i, j > N$.

Let $\sim$ be the equivalence relation on Cauchy sequences defined by $\{x_n\}_{n\in\mathbb{N}} \sim \{y_n\}_{n\in\mathbb{N}} \iff x_n - y_n \to 0$ as $n \to \infty$.

Define $\widehat{G}$, the *closure* of G, to be the set of all equivalence classes of Cauchy sequences in G.

Notes: (1) Addition of Cauchy sequences sends equivalence classes to equivalence classes.

(2) Let $\varphi : G \to \widehat{G}$ be the homomorphism sending x to the constant sequence $(x, x, \dots)$, i.e. each $x_n = x$. Then $\text{Ker}(\varphi) = \cap U_n = H$ from (10.1). Thus by (iv) φ is injective $\iff$ G is Hausdorff.

Definitions: *I-adic completion using Cauchy sequences.* Given an abelian group G and a nested sequence of subgroups $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots G_n \supseteq \cdots \supsetneq (0)$, we define a topology on G by specifying that $U \subseteq G$ is a *neighborhood* of $x \in G \iff U \supseteq G_n + x$, for some n.

If M is an R-module and I is an ideal of R, then $\widehat{M}$, the *I-adic completion of M*, is the set of all Cauchy equivalence classes of sequences, where $\{I^n M\}_{n\in\mathbb{N}}$ is the countable basis of neighborhoods of 0.

Examples: (1) If $M = R = \mathbb{Z}, I = p\mathbb{Z}$, then $\widehat{M}$ is the p-adic numbers.

(2) If $M = \mathbb{Q}$, $R = \mathbb{Z}$, $I = p\mathbb{Z}$, then $\widehat{M} \cong 0$.

(3) For S a commutative Noetherian ring, $M = R = S[x]$, and $I = (x)$, $\widehat{M} \cong S[[x]]$.

(4) If $M = R = \mathbb{Z}[x]$ and $I = (p, x)$ then $\widehat{M}$ is the ring of power series over the p-adic numbers. To see this, apply problem #5 chapter 10, page 114, to the previous examples.

Remarks: (1) If $f : G \to G'$ is a homomorphism of topological groups then f sends Cauchy sequences to Cauchy sequences inducing a map $\widehat{f} : \widehat{G} \to \widehat{G'}$.

(2) Let $\lambda_n : G \to G/G_n$ be the natural map. Then $\{x_v\}_{v\in\mathbb{N}}$ Cauchy implies each $\{\lambda_n(x_v)\}_{v\in\mathbb{N}}$ is eventually constant ϵ_n, and so $\lim_{v\to\infty} \lambda_n x_v = \epsilon_n$. Then, given that $\theta_{n+1} : G/G_{n+1} \to G/G_n$ is the natural map, we say that $\{\epsilon_n\}$ is a *coherent sequence* in the sense that $\theta_{n+1}(\epsilon_{n+1}) = \epsilon_n$.

(3) There is a one to one relationship between coherent sequences and equivalence classes of Cauchy sequences. So, given that we can uniquely determine the representatives of G/G_n for all n, we can produce unique representatives of equivalence classes of Cauchy sequences.

(4) Let $\{A_n\}_{n\in\mathbb{N}}$ be a sequence of groups and let $\{\theta_{n+1} : A_{n+1} \to A_n\}_{n\in\mathbb{N}}$ be ring homomorphisms. Then $\{A_n, \theta_{n+1}\}_{n\in\mathbb{N}}$ is called an *inverse system.* The set of all coherent sequences $\{(x_n)_{n\in\mathbb{N}} \mid x_n \in \mathbb{N}\}$ (where *coherence* is expanded to homomorphisms rather than only containments) is called the *inverse limit* and denoted $\varprojlim A_n$. Thus, for G an abelian group, the Cauchy sequence definition of $\widehat{G}$ from above is isomorphic to the inverse limit: $\widehat{G} \cong \varprojlim (G/G_n)$.

Definition: *I-adic completion definition using inverse limits.* For ${}_AM$ an R-module and I an ideal of R, define $\widehat{M} = \varprojlim (M/I^nM)$, where each $\theta_{n+1} : (M/I^{n+1}M) \to (M/I^nM)$ is the natural map.

In chapter 10, the proofs that taking completions respects exact sequences and the Noetherian property use this last definition of completion with inverse limits.

9. Ueno, Chapter 1

Let k be a field, usually algebraically closed. Let $\underline{x} = \{x_1, \ldots, x_n\}$ be variables over k and $\underline{a} = (a_1, \ldots, a_n)$ a point in k^n.

Before we begin, we will list some assumptions and facts necessary for the understanding of this section.

(1) Using degrees and the Euclidean Algorithm, we can show that $k[x]$ is a PID (and therefore also a UFD). If $P \neq (0)$ is a prime ideal in $k[x]$, then $P = (f)$ where f is irreducible (since k is algebraically closed, we know $f = ax + b$.) Similarly, in $k[x_1, ..., x_n]$, every ideal is finitely generated and is also a UFD.

(2) If k is a field, then there exists infinitely many irreducible polynomial in $k[x]$. (See Hungerford)

(3) If f is irreducible in $k[x]$, then (f) is prime and therefore maximal, which implies $kk[x]/(f)$ is a field. If k is algebraically closed, then the only irreducible polynomials have degree 1. Then $k[x]/(ax + b) \cong k$ by the map $\phi : k[x] \to k$ where $a \mapsto a$ and $x \mapsto -\frac{b}{a}$. Also $\ker\phi = (ax + b)$ and it is onto.

Section 1.1. Algebraic Sets

Definition.

(1) Let k be an algebraically closed field. Define the **affine $n-$space** over k to be the set of all $n-$tuples $(a_1, ..., a_n)$ where $a_i \in k$. We denote this space by k^n. Note: We'll see k^n is an $n-$dimensional vector space and an affine variety. When we regard it as an affine variety, we denote it $\mathbb{A}^n_k$.

(2) Define the **(affine) algebraic set** to be the set of all solutions in k of $f_\alpha(x_1, ..., x_n) = 0$ for $\alpha = 1, ..., \ell$ and denote it by $V(f_1, ..., f_\ell)$. Let J be an ideal in $k[x_1, ..., x_n]$. Define $V(j) = \{(b_1, ...b_n) \in k^n | g(b_1, ..., b_n) = 0 \text{ for all } g \in J\}$.

Lemma (1.1). Ueno, p. 2. If $I = (f_1, \ldots, f_\ell)$, then $V(I) = V(\{f_1, \ldots, f_\ell\})$.

Proof. First note that $V(I) = \{a \in k^n | g(a) = 0 \text{ for all } g \in I\}$ and $V(\{f_1, ..., f_\ell\}) = \{a | f_i(a) = 0 \text{ for all } j,\ 1 \le j \le \ell\}$. We will prove by double containment:
($\subseteq$:) Since f_j's are possible g's, if $g(a) = 0$ then $f_j(a) = 0$.
($\supseteq$:) Let $a \in V(\{f_1, ..., f_\ell\})$. Then $f_j(a) = 0$ for all j. Of course, $g = \sum_{i=1}^{\ell} h_i f_i$. Thus $g(a) = \sum_{i=1}^{\ell} h_i(a) f_i(a) = 0$. □

Note. $V((0)) = k^n, V(k[x_1, ..., x_n]) = \emptyset$.

Theorem (1.2). Ueno, p. 3, *Hilbert's basis theorem.* Any ideal in $k[x_1, ..., x_n]$ is finitely generated. That is, any ideal J is of the form $J = (g_1, ..., g_\ell)$ for $g_\alpha \in k[x_1, ..., x_n]$ and $\alpha = 1, ..., \ell$.

Problem 1 Any algebraic set in $\mathbb{A}^1_k$, except $\mathbb{A}^1_k$ itself, consists of finite points.

Proof. By Lemma 1.1, we know $V = V(I)$ for some $I \neq 0$ in $k[x]$. Since it is a PID, $I = (f)$ for some nonzero polynomial $f \in k[x]$. Then $V(I) = V(f)$ and since the number of roots is less than or equal to the degree, it is finite. □

Example (1.3). Ueno, p. 3. In $\mathbb{A}^2_k$, if $\text{char}(k) \neq 2$, then $V(x^2 + y^2 + 1) \sim V(x^2 + y^2 - 1)$, via $(a_1, a_2) \to (ia_1, ia_2)$ $(i = \sqrt{-1})$.

If $\text{char}(k) = 2$, then $V(x^2 + y^2 + 1) = V(x + y + 1)$.

Proposition (1.4). Ueno, p. 4. Let $I < J < I_\lambda$ be ideals of $k[\underline{x}]$, where $\lambda \in \Lambda$ (Λ may be an infinite set). Then:
(i) $V(I) \cup V(J) = V(I \cap J)$, (ii) $\cap_{\lambda \in \Lambda} V(I_\lambda) = V(\sum_{\lambda \in \Lambda} I_\lambda)$, (iii) $\sqrt{I} \subseteq \sqrt{J} \implies V(I) \supseteq V(J)$,
where $\sum_{\lambda \in \Lambda} I_\lambda$ is the ideal of $k[\underline{x}]$ generated by $\{I_\lambda \,|\, \lambda \in \Lambda\}$ and
$\sqrt{I} := r(I) = \{f \in k[\underline{x}] \,|\, f^m \in I, \text{ for some positive integer } m\}$, the *(nil)radical* of I.

Proof. (1) ($\subseteq$:) Since $I, J \supset I \cap J$, we see $V(I), V(J) \subset V(I \cap J)$. Thus $V(I) \cup V(J) \subset V(I \cap J)$.
($\supseteq$:) Let $a = (a_1, ..., a_n) \in V(I \cap J)$. If $a \notin V(I)$, there exists $f \in I$ such that $f(A) =\neq 0$. Then for $g \in J$, let $h = fg \in I \cap J$. Then $f(a)g(a) = h(a) = 0$ since $h \in I \cap J$. Since $f(a) \neq 0$, $g(a) = 0$ which implies $a \in V(J)$. So $V(I \cap J) \subseteq V(I) \cup V(J)$.

(2) ($\supseteq$:) We know $I_\lambda \subseteq \sum_{\lambda \in \Lambda} I_\lambda$ for all $\lambda \in \Lambda$. Thus $V(I_\lambda) \supseteq V(\sum I_\lambda)$ for all lambda. Therefore $\cap V(I_\lambda) \supseteq V(\sum I_\lambda)$.
($\subseteq$:) For all λ, $I_\lambda = (h_{\lambda_a}, ..., h_{\lambda_{m_\lambda}})$. For $a \in \cap V(I_\lambda)$, we know $h_{\lambda_j}(a) = 0$. But $\{h_{\lambda_j}\}_{\lambda \in \Lambda}$ generates $\sum I_\lambda$. Therefore $a \in V(\sum I_\lambda)$.

(3) **Claim:** $V(I) = V(\sqrt{I})$
Since $I \subseteq \sqrt{I}$, we know $V(I) \supseteq V(\sqrt{I})$. To show the other containment, let $a \in V(I), g \in \sqrt{I}$. Then $g^m \in I$ for some $m > 0$ which implies $g^m(a) = 0$. Since k is a field, this says $g(a) = 0$, that is $a \in V(\sqrt{I})$.
Now, $\sqrt{I} \subseteq \sqrt{J}$ implies $V(I) = V(\sqrt{I}) \supseteq V(\sqrt{J}) = V(J)$.

□

Note. Ueno, (iii), p. 5. $V(\sqrt{I}) = V(I)$.

Corollary (1.5). Ueno, p. 5. Let $I_1, \ldots, I_s$ be finitely many ideals of $k[\underline{x}]$. Then $\cup_{j=1}^{s} V(I_j) = V(\cap_{j=1}^{s} I_j)$.

Note that this is not true for infinitely many ideals. Consider the following example (1.6 in Ueno):

Example. Let $\{c_i\}_{i\in A}$ be a countably infinite collection of distinct elements in a field k. Let $I_j = (x - c_j)$ be ideals in $k[x]$. Then $\cup_{j=1}^{\infty} V(I_j) = \{c_i\}_{i\in A}$.

Proof: ($\subseteq$:) Let $a \in \cup V(I_j)$. Then there exists j such that $a \in V(I_j)$. Let $f(x) = x - c_j$. Since $f(a) = a - c_j = 0, a = c_j$.

($\supseteq$:) Clearly, $c_j \in V(I_j) \subseteq \cup V(I_j)$.

However, $\cap I_j = (0)$ as if not, then there would exist nonzero $f \in k[x]$ such that $f \in I_j$ for all $j \geq 1$ which would imply $f(x) = g_j(x)(x - c_j)$ which would imply $f(c_j) = 0$ for all c_j and since the number of roots is less than the degree, $f = 0$ a contradiction. So $V(\cap I_j) = V((0)) = \mathbb{A}^1_k$. However, once can choose $\{c_i\} \subsetneq \mathbb{A}^1_k$. For example, take $k = \mathbb{C}$ and $c_\alpha \in \mathbb{Q}$. So $\cup_{j=1}^{\infty} V(I_j) \subsetneq \cap V(I_j)$.

Definition. Hartshorne, p. 5, presented by Ela. Let X be a topological space.

X is *Noetherian* if it satisfies the descending chain condition (DCC) on closed subsets, i.e. for any sequence $Y_1 \supseteq Y_2 \supseteq Y_3 \supseteq \cdots$ of closed subsets of X, $\exists$ an integer r such that $Y_r = Y_{r+1} = \cdots$.

A subset Y of X is*irreducible* if $Y \neq Y_1 \cup Y_2$, for every pair Y_1, Y_2 of proper subsets so that each is closed in Y.

Theorem. Hartshorne 1.6, Ela. Every algebraic set in $\mathbb{A}^n$ can be expressed uniquely as a union of varieties, no one containing another.

Lemma. Hartshorne 1.5, Ela. If X is Noetherian topological space, then

(1) Every nonempty closed subset Y of X is a finite union $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_r$ of irreducible closed subsets Y_i.

(2) If $Y_i \not\supseteq Y_j$, for $i \neq j$, then the Y_i are uniquely determined. They are called the *irreducible components* of Y.

Section 1.2. Hilbert's Nullstellensatz.

There are some notions we need to review before learning the material of this sections.

Definition. For rings $R \subseteq S \subseteq T$, we say S is **finitely generated** as a ring over R, if $S = R[s_1, ..., s_t]$. Note that although $R[x]$ is finitely generated as a ring over R, it is not as a module.

Example. The gaussian integers $\mathbb{Z}[i]$ is finitely generated over $\mathbb{Z}$ as both a ring and an ideal. However $\mathbb{Z}[\frac{1}{2}]$ and $\mathbb{Z}[e]$ are only finitely generated as rings and not modules.

Proposition.[5.1 in AM] $R[S]$ is finitely generated as a module if and only if s is **integral** (i.e. there exists a monic polynomial $f(s) \in R[x]$ such that $f(s) = 0$) over R.

Notes.

(1) If R is a field, then s is algebraic if and only if s is integral.

(2) If z is integral, then $k[z]$ is a field

Proof. We see $k[x] \to k[z]$ has ker $= (f)$ where f is the minimal polynomial for z (Since PID, (f) is maximal). Then $k[x]/(f) \cong k[z]$ is a field.

Lemma.[From AM Ch 5]

(1) If $w_1, ..., w_\ell$ are integral over R, then every element of $R[w_1, ..., w_\ell]$ is integral over R.

(2) If $R \subseteq S \subseteq T$ where S is integral over R and T is integral over S, then T is integral over R.

Lemma (1.9). Ueno, p. 7. Let R be an integral domain that is finitely generated over a field K (K need not be algebraically closed). If R is a field, then R is algebraic over K.

Proof. Let $R = k[z_1, ...z_m]$ and induct on m. If $m = 1$, then $R = k[z_1]$. If z_1 is not algebraic, then it is transcendental, which implies $k[x] \cong k[z_1]$ but $k[x]$ is not a field, contradiction. Thus z_1 is algebraic, which implies integral, which implies $k[z_1]$ is integral over k. Suppose $m > 1$. Let $R = k[z_1][z_2, ..., z_m] = k(z_1)[z_2, ..., z_m]$ since R is a field. Now $k(z_1)$ is a field and $z_2, ..., z_m$ are algebraic over $k(z_1)$ by induction. Then for all $2 \leq j \leq m$ there exists $f_j \in k(z_1)[x]$ such that $f_j(z_j) = 0$. Write

$$f_j(x) = A_j(z_1)x^{n_j} + B_j^{(1)}(z_1)x^{n_j-1} + \dots B_j^{(n_j)}(z_1), \text{ where } A_j(z_1), B_j^{(\ell)}(z_1) \in k(z_1). \tag{9.1}$$

We can multiply by elements of $k[z_1]$ such that $A_j(z_1), B_j^{(\ell)}(z_1) \in k[z_1]$. Define $S = k[z_1, \frac{1}{\prod_{j=2}^m A_j(z_1)}] \subseteq R$. Call $A(z_1) = \prod_{j=2}^m A_j(z_1)$ and note that $\frac{1}{A_j(z_1)} \in S$ for all j. Also

$$R \supseteq S[z_2, ..., z_m] \supseteq k[z_1, ..., z_m] = R.$$

Thus $R = S[z_2, ..., z_m]$. Revise equation (1) by dividing by $A_j(z_1)$ to get

$$g_j(x) = \frac{f_j(x)}{A_j(z_1)} = x^{n_j} + (\textit{lower terms}) \in S[x]$$

with z_j as a root. Therefore z_j is integral over S. By the Lemma, R is integral over S.
Claim: S is a field.

Proof. Let $a \in S \setminus \{0\}$. Then $a^{-1} \in R$ a field which implies a^{-1} is integral over S. Say $(a^{-1})^\ell + b_{\ell-1}(a^{-1})^{\ell-1} + \ldots + b_1 a^{-1} + b_0 = 0$ for $b_i \in S$. Multiply by a^ℓ to get $1 + b_{\ell-1}a + \ldots + b_1 a^{\ell-1} + b_0 a^\ell = 0$. Thus

$$1 = -a(b_{\ell-1} + b_{\ell-2}a + \dots b_0 a^{\ell-1})$$

which says $a^{-1} \in S$.
Claim: z_1 is algebraic over k.

Proof. Suppose not. Then Z_1 is transcendental over k which implies $k[z_1] \cong k[x]$, which has infinitely many irreducible polynomials. So there exists $F(z_1)$, irreducible as an element of $k[z_1]$ and relatively prime to $A(z_1)$. Consider $0 \neq \frac{F(z_1)}{A(z_1)} \in S = k[z_1, \frac{1}{A(z_1)}]$. Then its inverse exists in S which implies there exists $G(z_1) \in k[z_1]$ such that $\frac{G(z_1)}{A(z_1)} \cdot \frac{F(z_1)}{A(z_1)} = 1$. This contradicts the face that $k[z_1]$ is a UFD (as we get $G(z_1)F(z_1) = A(z_1)^2$). Thus z_1 is algebraic.

Thus z_1 is integral over k which implies $k[z_1]$ is a field. So $k[z_1] = S$. Since we now have R is integral over S and S is integral over k, we see R is integral over k.

□

By Prop 1.5 in AM, this says that R is finitely generated as a module.

Theorem (1.7: Weak Hilbert Nullstellensatz). Ueno, p. 6. Let I be an ideal of $k[x_1, \dots, x_n]$, where k is an algebraically closed field. If $1 \notin I$, then $V(I) \neq \emptyset$.

Proof. If $I \neq k[x_1, ..., x_n]$, then there exists a maximal ideal $M \in k[x_1, ..., x_n]$ such that $\supseteq I$. Then $V(M) \subseteq V(I)$. Thus it suffices to show $V(M) \neq \emptyset$. Let $K = k[x_1, ..., x_n]/M$ and note this is a field.

Claim: k embeds in K via the map $\phi(a) = a + M$.

Proof. : Clearly ϕ is a ring homomorphism and it is 1-1 as $\ker \phi = \{0\}$ (as $\phi(a) = 0 + M$ implies $a \in M$, but $a \neq 0$ implies a is a unit).

Now K is a field finitely generated as a ring over k. By Lemma 1.9, every element is algebraic over k. Since $\overline{k} = k$, we know $x_i + M = a_i + M$ for some $a_i \in k$. This implies $x_a - a_i \in M$ and thus $J = (x_1 - a_1, ..., x_n - a_n) \subseteq M$. Of course J is a maximal ideal as when we mod out by it we get the field k. So $J = M$. Then $(a_1, ..., a_n) \in V(M)$ which implies $V(M) \neq \emptyset$. □

Corollary (1.8). Ueno, p. 7. Let $\mathbf{m}$ be a maximal ideal of $k[x_1, \ldots, x_n]$, where k is an algebraically closed field. Then $\mathbf{m} = (x_1 - a_1, \ldots, x_n - a_n)$, for some $a_i \in k$.

Problem 2 A maximal ideal of a polynomial ring $\mathbb{R}[x]$ of one variable over the field $\mathbb{R}$ can be expressed as either $(x - a)$ for $a \in \mathbb{R}$ or $(x^2 + ax + b)$ for $a, b \in \mathbb{R}$ and $a^2 - 4b < 0$.

Proof. Let M be a maximal ideal in $\mathbb{R}[x]$. Since this is a PID, $M = (f)$. Suppose $f(x) = g(x)h(x)$. Then $M = (f) \subseteq (g) \subseteq \mathbb{R}[x]$. Since M is maximal, either $(f) = (g)$ (in which case $(h) = \mathbb{R}[x]$) or $(g) = \mathbb{R}[x]$ (in which case $(h) = (f)$). Thus f is irreducible. Since $[\mathbb{C} : \mathbb{R}] = 2$ and $\mathbb{C}$ is algebraically closed, we see $\deg f \leq 2$. If $\deg f = 1$, then $(f) = (x - a)$. If $\deg f = 2$, then $(f) = (x^2 + ax + b)$. By the quadratic formula, this is only irreducible when $a^2 - 4b \leq 0$. □

Definition. For a subset V in a the $n-$dimensional affine space $\mathbb{A}_k^n$ over an algebraically closed field k, define the ideal $I(V) = \{f \in k[x_1, ..., x_n] | f(a_1, ..., a_n) = 0 \text{ for all } (a_1, ..., a_n) \in V\}$.

Notes.

(1) For an ideal J, $J \subset I(V(J))$.

(2) If $V(J') \subset V(J)$ then $I(V(J)) \subset I(V(J'))$.

Proof. If $f \in I(V(J))$, then $f(a_1, ..., a_n) = 0$ for all $(a_1, ..., a_n) \in V(J)$ which implies for all $(a_1, ..., a_n) \in V(J')$. Thus $I(V(J)) \subset I(V(J'))$.

Theorem (1.10). Ueno , p. 9. *Hilbert's Nullstellensatz.* Let J be an ideal of $k[x_1, \ldots, x_n]$, where k is an algebraically closed field. Then $I(V(J)) = \sqrt{J}$.

Proof. Recall from Proposition 1.4 (3), we proved $V(\sqrt{J}) = V(J)$. Thus $\sqrt{J} \subseteq I(V(\sqrt{J})) = I(V(J))$. To prove the other containment, let $f \in I(V(J))$. Let x_0 be a new variable and define $A_0 = k[x_0, ..., x_n]$. Define $\widetilde{J} = (J, 1 - x_0 f(x_1, ..., x_n)) \leq A_0$. Note $JA_0 \leq \widetilde{J}$ which implies $V(\widetilde{J}) \subseteq V(J)$. If $V(\widetilde{J}) \neq \emptyset$, then there exists $(a_0, ..., a_n) \in V(\widetilde{J}) \setminus \{0\} \subseteq k^{n+1}$. Then $1 - a_0 f(a_1, ..., a_n) = 0$ and $f(a_1, ..., a_n) = 0$ as $V(\widetilde{J}) \subseteq V(J)$. Thus $1 = 0$ a contradiction. So $V(\widetilde{J}) = \emptyset$ which implies $\widetilde{J} = A_0$. So $1 \in \widetilde{J}$ which implies $1 = h(x_0, ..., x_n)(1 - x_0 f(x_1, ..., x_n)) + \sum_{j=1}^{\ell} g_j(x_0, ..., x_n) f_i(x_1, ..., x_n)$ where J is generated by $f_i \in k[x_1, ..., x_n]$. Set $x_0 = \frac{1}{f}$. Then $1 = \sum_{j=1}^{\ell} g_j(\frac{1}{f}, x_1, ..., x_n) f_i(x_1, ..., x_n)$. So $g_j = \frac{\alpha_j}{f^{t_j}}$ for $\alpha_j \in k[x_1, ..., x_n]$. Then $1 = \sum \frac{\alpha_j}{f^{t_j}} f_i$ which implies $f^N = \sum \alpha_j f_i f^{N - t_j} \in J$ (since J is an ideal and contains f_i)where $N = \max\{t_j\}$. Since $f^N \in J$, we see $f \in \sqrt{J}$. □

Note: As a result of this theorem, to study algebraic sets $V(J)$, we focus on **reduced ideals,** that is, ideals J such that $J = \sqrt{J}$.

Exercise 1.11, Ueno, p. 10: If $V, W \subseteq \mathbb{A}^n$, then

(i) $V \supseteq W \implies I(V) \subseteq I(W)$

(ii) $V(J_1) \supsetneq V(J_2) \implies \sqrt{J_1} \subsetneq \sqrt{J_2}$.

Exercise 1.12 Let $V(I) \neq \emptyset, \mathbb{A}_k^n$ be an algebraic set. Prove $V(I)^C = \mathbb{A}_k^n \setminus V(I)$ is not an algebraic set.

Proof. Suppose for contradiction that there exists some ideal J in $k[x_1, ..., x_n]$ such that $V(I)^C = V(J)$. Then $V(I \cap J) = V(I) \cup V(J) = \mathbb{A}_k^n$. By Hilbert's Nullstellensatz, $\sqrt{I \cap J} = I(V(J \cap I)) = I(\mathbb{A}_k^n) = (0)$. Then $J \cap I \subseteq \sqrt{J \cap I} = (o)$. If $I, J \neq (0)$, then there exists nonzero $f \in I$ and $g \in J$ which implies $fg \neq 0$ but $fg \in I \cap J = (0)$. So either I or $J = (0)$. If $I = (0)$, then $V(I) = \mathbb{A}_k^n$ and if $J = (0)$, $V(I) = \mathbb{A}_k^n \setminus V(J) = (0)$. Either way, we obtain a contradiction. Thus there does not exist J, which implies $V(I)^C$ is not an algebraic set. □

Exercise 1.13, Ueno, p. 11: Let $\mathcal{O} = \{V(I)^c \mid I \text{ is an ideal of } k[x_1, \ldots, x_n]\}$. Then

(i) $\emptyset, \mathbb{A}_k^n \in \mathcal{O}$.

(ii) $O_1, O_2 \in \mathcal{O} \implies O_1 \cap O_2 \in \mathcal{O}$.

(iii) $O_\lambda \in \mathcal{O}, \forall \lambda \in \Lambda \implies \cup_{\lambda \in \Lambda} O_\lambda \in \mathcal{O}$.

If C is a closed set in $\mathbb{A}_k^1$, then $C = \emptyset$ or $C = \mathbb{A}_k^1$ or $C =$ a finite set of points.

Section 1.3. Affine Algebraic Varieties.

Definition. Let V be an algebraic set in $\mathbb{A}_k^n$ (where k is an algebraically closed field). Say V is **reducible** if there exist algebraic sets V_1, V_2 such that $V = V_1 \cap V_2$ with $V \neq V_i$. Otherwise, V is called **irreducible**. An irreducible algebraic set is said to be an **affine algebraic variety**.

Note. This differs from A&M's definition of an algebraic variety. They say a variety is any algebraic set- irreducible or not.

Proposition (1.14). Ueno, p. 12. An algebraic set V is irreducible $\iff$ $I(V)$ is a prime ideal.

Proof. ($\Leftarrow$:) Contrapositive. Let $V(J)$ be reducible. Then there exists ideals J_1, J_2 such that $V(J) \neq V(J_i)$ and $V(J) = V(J_1) \cap V(J_2)$. Then $V(J_i) \subsetneq V(J)$ implies $I(V(J)) \subsetneq I(V(J_i))$ by the note above. Thus there exists $f_i \in I(V(J_i)) \setminus I(V(J))$. Since $V(J) = V(J_1) \cup V(J_2)$, $f_1 \cdot f_2 \in I(V(J))$. Of course, this says $I(V(J))$ is not a prime idea.

($\Rightarrow$:) Let $V(J)$ be irreducible and suppose $I(V(J))$ was not prime. The there exists $f_1, f_2 \notin I(V(J))$ such that $f_1 \cdot f_2 \in I(V(J))$. Let J_i be the ideal generated by $I(V)$ and f_i. Since $f_i \notin I(V)$, $J_i \supsetneq I(V(J))$ which implies $V(J_i) \subsetneq V(I(V(J)) \subset V(J)$. But $f_1 \cdot f_2 \in I(V)$ implies either f_1 or f_2 is zero at all $(a_1, ..., a_n) \in V$. Thus $V(J) = V(J_1) \cup V(J_2)$, a contradiction. Thus $I(V(J))$ is prime. □

Note. Since $I(\mathbb{A}_k^n) = (0)$ is a prime ideal, Prop 1.14 tells us that $\mathbb{A}_k^n$ is irreducible and is thus, by definition, an affine algebraic variety. As a result, we will refer to $\mathbb{A}^1$ as an **affine line** and $\mathbb{A}^2$ as an **affine plane**.

Lemma. Let $U \subseteq \mathbb{A}_k^n$ be an algebraic set and $J \subseteq k[\underline{x}]$. Then $J \subseteq I(U) \iff V(J) \supseteq U$.

Proposition. *1.2 p3, Hartshorne Let $Y \subseteq \mathbb{A}_k^n$. Then the closure of Y, $\overline{Y}$, is an algebraic set, namely $V(I(Y))$.*

Proof. Let $\mathcal{G} = \{X \subseteq \mathbb{A}_k^n | X \text{ is closed}, X \supseteq Y\}$. Then $\overline{Y} = \bigcap_{x \in \mathcal{G}} X$. We will show by double containment.

$\subseteq$**:** Clearly, $Y \subseteq V(I(Y))$. Thus $V(I(Y)) \in \mathcal{G}$.

$\supseteq$**:** Let $X \in \mathcal{G}$. Thus $X = V(J)$ for some ideal J. Then $V(J) = X \supseteq Y$ implies $J \subseteq I(V(J)) \subseteq I(Y)$. This says $V(J) \supseteq V(I(Y))$. Since $\overline{Y} = \bigcap_{X \in \mathcal{G}}$, $Y \supseteq V(I(Y))$.

□

Definition. For an algebraic set $V \subseteq \mathbb{A}_k^n$, the set $k[v] := k[x_1, ..., x_n]/I(V)$ is called the **coordinate ring** of V.

Example 1.15 Let $J = (f) \subset K[\underline{x}]$. Then Prop 1.14 tells us J is a prime ideal if and only if f is an irreducible polynomial. Say $V(J)$ is called an **affine hyperspace**.

Corollary (1.16). Ueno, p. 13. An algebraic set V is irreducible $\iff$ its coordinate ring $k[V]$ is a domain.

Definition. If a set-theoretic map from an algebraic set $V \subseteq \mathbb{A}_k^m$ to an algebraic set $W \subseteq \mathbb{A}_k^n$ can be expressed in terms of polynomials, the map is said to be a **morphism** from V to W. Namely, for coordinate rings, $k[V] = k[x_1, ..., x_m]/I(v)$ and $k[W] = k[y_1, ..., y_n]/I(W)$, a map $\phi : V \to W$ is a morphism if ϕ can be expressed as

$$y_j = f_j(x_1, ..., x_m) \in k[x_1, ..., x_m],$$

that is, $\phi((a_1,...,a_m)) = (f_1(a_1,...,a_m),...,f_n(a_1,...,a_m))$.

Note. If there are relations among $a_1,...,a_m$, then ϕ is not uniquely determined by the polynomials f_i. We'll see a more precise definition later.

Definition. For a commutative ring R, we denote the totality of maximal ideals of R by Spm R and call it the **maximal spectrum** of R.

Proposition (1.20). Ueno, p. 18. Let $U \subseteq \mathbb{A}_k^n$ be an algebraic set. Then there is a one-to-one correspondence:
{ points of V} $\to$ Max-spec $(k[V])$.

Proposition (1.21). Ueno, p. 19. Let $\varphi : V \to W$ be a morphism between algebraic sets $V \subseteq \mathbb{A}_k^m$ and $W \subseteq \mathbb{A}_k^n$, where k is an algebraically closed field. Then there is induced a k-homomorphism $\varphi^\#$ between the coordinate rings $\varphi^\# : k[W] \to k[V]$ such that, for each maximal ideal $\mathbf{m}_{\underline{a}} = (x_1 - a_1, \ldots, x_m - a_m)$ of $k[V]$, where $\underline{a} = (a_1, \ldots, a_m) \in V$, we have that the inverse image $(\varphi^\#)^{-1}(\mathbf{m}_{\underline{a}}) = \mathbf{m}_{\underline{b}} = (y_1 - b_1, \ldots, y_n - b_n)$ in $k[W]$, where $\underline{b} = \varphi(\underline{a}) = \varphi(a_1, \ldots, a_m)) \in \varphi(V)$.

Conversely, if $\varphi : V \to W$ is a set-theoretic map and $\varphi^\# : k[W] \to k[V]$ is a k-homomorphism such that, for each $\underline{a} = (a_1, \ldots, a_m) \in V$, where $\underline{a} = (a_1, \ldots, a_m) \in V$, $(\varphi^\#)^{-1}(\mathbf{m}_{\underline{a}}) = \mathbf{m}_{\underline{b}} = (y_1 - b_1, \ldots, y_n - b_n)$, and $\underline{b} = \varphi(\underline{a}) = \varphi(a_1, \ldots, a_m)) \in \varphi(V)$, then $\varphi : V \to W$ is a morphism between the algebraic sets.

Definition. A pair $(V, k[V])$ is said to be an **affine (algebraic) variety**. When V is irreducible, then $(V, k[V])$ is called an **irreducible affine variety**. Furthermore, when $(\psi, \psi^\#) : (V, k[V]) \to (W, k[W])$ is an isomorphism, we regard $(V, k[V])$ and $(W, k[W])$ as the same.

Lemma (1.23). Ueno, p. 22. Let $\Psi : S \to R$ be a k- homomorphism of k-algebras. Then the inverse image $\Psi^{-1}(\mathbf{m})$ of a maximal ideal $\mathbf{m}$ of R is a maximal ideal of S.

Definition. For a finitely generated algebra over an algebraically closed field k, (Spm R, R) is said to be an affine algebraic variety. For (Spm R, R), an element of R is called a regular function on the affine algebraic variety.

10. Curves and Bezout's Theorem, corresponding to Ueno sections, pp. 26 - 37—Deanna Turk

Assume that k is an algebraically closed field.

Definition. $C \subseteq \mathbb{A}^2(k)$ is a *(plane) affine algebraic curve* (aka *curve*) if there exists a nonconstant $f \in k[x, y]$ with $C = V(f)$. We write $C : f = 0$, and f is called an equation for C. (We often refer to "the curve f".)

We would like to be able to talk about the number of intersection points of two curves. Recall that C is *reducible* if there exist curves C_1, C_2 such that $C = C_1 \cup C_2$, where $C \neq C_1$ and $C \neq C_2$.

Theorem. *If $C : f = 0$ is a curve, then C is irreducible $\Leftrightarrow$ f is irreducible. (Assuming f is separable)*

Definition. Given $f \in k[x, y]$, we can write $f = f_1 f_2 \ldots f_r$ uniquely (up to constant multiples) where each f_i is irreducible (not necessarily distinct). Let $C_i : f_i = 0$ for each $i = 1, ..., r$. Then the C_i are called the *(irreducible) components* of C.

Suppose f and g correspond to C and D, which are two curves that share a common component. Then finding the number of points on $C \cap D$ is the same as finding the number of points in $C \cap D$ that are *not* in the common component, and counting the points in the common component. Since we don't really want to worry about how many points are on a particular component, we will restrict ourselves to looking at curves with no common components. Furthermore, from the definition of component, if f and g have no common component then f and g have no common factor, so $gcd(f, g) = 1$.

Definition. If f and g are two curves with $gcd(f,g) = 1$ and $p = (a,b)$ is a point of intersection, then $\mathfrak{m}_p = (x-a, y-b)$ is a maximal ideal containing (f,g). Define the *intersection multiplicity* of f and g *at* p to be

$$I_p(f,g) = \dim_k \frac{k[x,y]_{\mathfrak{m}_p}}{(f,g)_{\mathfrak{m}_p}}.$$

The *intersection multiplicity* of f and g is $\sum_{i=1}^{t} I_{p_i}(f,g)$, where $P_1, ..., P_t$ are the points of intersection of f and g.

Examples (1) For $f(x,y) = x^2 + (y+1)^2 - 1$ and $g(x,y) = y$, $I_{(0,0)}(f,g) = 2$. (Here f is the unit circle translated to just below the x-axis). Intuitively (and from the geometric picture, since $y = 0$ is a tangent line), we know the intersection multiplicity of f and g at $(0,0)$ should be two. To see this, notice that
$(x^2 + (y+1)^2 - 1, y) = (x^2 + y^2 + 2^y + 1 - 1, y) = (x^2 + y(y+2), y) = (x^2, y)$ as ideals. Using the formula above:

$$I_{(0,0)}(f,g) = \dim_{\mathbb{C}} \left(\frac{\mathbb{C}[x,y]_{(x,y)}}{(x^2+(y+1)^2-1, y)_{(x,y)}} \right) = \dim_{\mathbb{C}} \left(\frac{\mathbb{C}[x,y]_{(x,y)}}{(x^2,y)_{(x,y)}} \right) = \dim_{\mathbb{C}} \left(\frac{\mathbb{C}[x,y]}{(x^2,y)} \right)_{(x,y)}.$$

There is only one maximal ideal in $\mathbb{C}[x,y]$ containing (x^2, y), namely the ideal (x,y), which means that

$$\frac{\mathbb{C}[x,y]}{(x^2,y)}$$

is a local ring, and hence localizing it doesn't change the ring structure. In particular, the dimension of this ring over k is still the intersection multiplicity of f and g at the origin. Since $\{1, x\}$ is a basis for this ring as a vector space over $\mathbb{C}$, f and g intersect twice at $(0,0)$, i.e. $I_{(0,0)}(f,g) = 2$.
(2) For $f(x,y) = x$ and $g(x,y) = x - y$, $I_{(0,0)}(f,g) = 1$. Again, intuition tells us that these curves intersect once at $(0,0)$. To see this via the formula:

$$I_{(0,0)}(f,g) = \dim_{\mathbb{C}} \left(\frac{\mathbb{C}[x,y]_{(x,y)}}{(x, x-y)_{(x,y)}} \right) = \dim_{\mathbb{C}} \left(\frac{\mathbb{C}[x,y]}{(x,y)} \right)_{(x,y)}.$$

Since $\frac{\mathbb{C}[x,y]}{(x,y)} \cong \mathbb{C}$ is local, localizing does not change the ring, and hence the intersection multiplicity at $(0,0)$ is $\dim_{\mathbb{C}} \mathbb{C} = 1$.

If f and g are lines, we would like them to intersect once. But what do we do when $f(x,y) = x$ and $g(x,y) = x - 1$? Answer: Go to projective space!

Definition. Define an equivalence class $\sim$ on $\mathbb{A}^{n+1}(k)$ by $a \sim b$ if and only if there exists $\lambda \in k^\times$ such that $a = \lambda b$. Then $\mathbb{P}^n(k) = \mathbb{A}^{n+1}(k) \setminus \{0\} / \sim$ is the n-dimensional *projective space* over k. Points in $\mathbb{P}^n(k)$ are often written as $[a_0 : a_1 : \ldots : a_n]$ (think of ratios).

Notice that there is a very natural embedding of $\mathbb{A}^n(k)$ in $\mathbb{P}^n(k)$ via $(a_1, .., a_n) \mapsto [1 : a_1 : \ldots : a_n]$. A point in $\mathbb{P}^n(k)$ with a zero in the first coordinate is called a *point at infinity*, and we can think of $\mathbb{P}^n(k)$ as a union of affine space and a bunch of stuff at infinity.
However, there's nothing special about the first coordinate; we could just as easily have chosen the points at infinity to be points in $\mathbb{P}^n(k)$ with zeros in the i^{th} coordinate, and modified the injection $\mathbb{A}^n(k) \to \mathbb{P}^n(k)$ accordingly.

Definition. The *degree* of a monomial $cx_0^{r_0} \ldots x_n^{r_n} \in k[x_0, ..., x_n]$ is $\sum_{i=0}^{n} r_n$ for $c \neq 0$. The *degree* of $F \in k[x_0, ..., x_n]$ is the largest degree of its monomial nonzero terms.

Definition. If $F \in k[x_0, ..., x_n]$, then F is *homogeneous* if each monomial in F has the same degree.

Example. $f(x,y) = x^2 + xy$ and $g(x,y) = x^3 - x^2 y$ are homogeneous, but $h(x,y) = x^2 + x^2 y$ is not.

Observation. Let F be homogeneous and let $a = (a_0, ..., a_n) \in \mathbb{A}^{n+1}(k)$. Then

$$\begin{aligned} F(a) = 0 &\iff \lambda^{\deg F} F(a) = 0 \text{ for } \lambda \in k^\times \\ &\iff F(\lambda a) = 0 \text{ for } \lambda \in k^\times \\ &\iff F(b) = 0 \text{ for all } b \sim a \text{ in } \mathbb{P}^n(k). \end{aligned}$$

This means that we can talk about points in $\mathbb{P}^n(k)$ as satisfying F, instead of just talking about points in affine space.

Definition. $C \subseteq \mathbb{P}^2(k)$ is a *projective algebraic curve* if there exists a nonconstant $F \in k[x_0, x_1, x_2]$ with $C = \{p \in \mathbb{P}^2(k) | F(p) = 0\} \equiv V_+(F)$.

Define irreducibility and components in the same way as the affine case.

Definition. For $f \in k[x, y]$, the *homogenization* of f is $\hat{f} = x_0^{\deg f} f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$. For $F \in k[x_0, x_1, x_2]$, the *dehomogenization* of F (with respect to x_0) is $f(x, y) = F(1, x, y)$.
Notice that if $x_0 \not| F$, then $\deg f = \deg F$ and $F = \hat{f}$.

Going back and forth between affine space and projective space can often give us a lot of information. We finish by looking at an example in which we see the usefulness of being able to choose different lines at infinity, and then mentioning an interesting theorem.

Example. Let $f(x, y) = x$ and $g(x, y) = x - 1$. Then $\hat{f} = x_1$ and $\hat{f} = x_1 - x_0$ are both homogeneous. We noticed before, in not quite so many words, that if we dehomogenize $\hat{f}$ and $\hat{g}$ with respect to x_0, we have no intersections. However, notice that $[0 : 0 : 1]$ is a point of intersection, so if we dehomogenize with respect to x_2, we get the curves $x = 0$ and $x - y = 0$ (since $f(x_0, x_1) = F(x, y, 1)$), which do intersect once. Intuitively, the parallel lines f and g meet once at a point of infinity.

Bezout's Theorem. *Two plane curves f and g with no common components have exactly* $\deg f \deg g$ *intersections.*

11. Abstract Nonsense—Scott

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

Objects: $\mathrm{Ob}(\mathcal{C})$ *Arrows*: $\mathrm{Arr}(\mathcal{C})$ *Domains*: $\mathrm{dom}_{\mathcal{C}}$ and *Codomains*: $\mathrm{cod}_{\mathcal{C}}$.

One writes $A \xrightarrow{f} B \in \mathrm{Ob}(\mathcal{C})$ for $f \in \mathrm{Arr}(\mathcal{C})$ with $\mathrm{dom}_{\mathcal{C}} f = A$ and $\mathrm{cod}_{\mathcal{C}} f = B \in \mathrm{Ob}(\mathcal{C})$. There are identity arrows and composite arrows:

$$\begin{array}{ccc} A \\ {\scriptstyle 1_A}\downarrow \\ A \in \mathcal{C} \end{array} \quad \text{and} \quad \begin{array}{ccc} A & \xrightarrow{gf} & C \\ {\scriptstyle f}\downarrow & \nearrow_{g} & \\ B \in \mathcal{C} & & \end{array} \quad \text{for} \quad \begin{array}{ccc} A & & C \\ {\scriptstyle f}\downarrow & \nearrow_{g} & \\ B \in \mathcal{C} & & \end{array}$$

These satisfy the left- and right-identity and associative laws:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle f}\downarrow & \swarrow^{1_B} & \downarrow{\scriptstyle g} \\ B & \xrightarrow{g} & C, \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{h(gf)=(hg)f} & D \\ {\scriptstyle f}\downarrow & {\scriptstyle gf}\searrow \quad \nearrow{\scriptstyle hg} & \uparrow{\scriptstyle h} \\ B & \xrightarrow{g} & C \in \mathcal{C} \end{array} \quad \text{for} \quad \begin{array}{ccc} A & & D \\ {\scriptstyle f}\downarrow & & \uparrow{\scriptstyle h} \\ B & \xrightarrow{g} & C \in \mathcal{C} \end{array}$$

Now set $\mathrm{Hom}_{\mathcal{C}}(A, B) = \{f \mid A \xrightarrow{f} B \in \mathcal{C}\} \subseteq \mathrm{Arr}(\mathcal{C})$.

A *functor* $F\mathcal{D} \to \mathcal{C}$ between categories is a system of maps, written $F : \mathrm{Ob}\ (\mathcal{D}) \to \mathrm{Ob}(\mathcal{C})$ such that

$\mathrm{Hom}_{\mathcal{D}}(A, B) \to \mathrm{Hom}_{\mathcal{C}}(FA, FB)$, $\forall A, B \in \mathcal{C}$, so that $F(1_A) = 1_{F(A)}$ and $F(gf) = (Fg)(Ff)$, for $A \xrightarrow{f} B \xrightarrow{g} C \in \mathcal{C}$.

Examples. (Ring), (R-mod), (Top), (Set) are categories. $(-)_P$: (R-mod)$\to$ (R_P-mod), $(\otimes_R N)$: (R-mod)$\to$ R-mod),

Spec: (Ring)$\to$(Top) are functors.

Left Adjoint Criterion: Let$\mathcal{A} \xrightarrow{U} \Sigma$ be a functor and suppose for every $X \in \Xi$ that $FX \in \mathcal{A}$ and $X \xrightarrow{\nu_X} U(FX) \in \Sigma$ are given so that for every $A \in \mathcal{A}$ and $X \xrightarrow{f} UA \in \Sigma$, there is a unique $FX \xrightarrow{\overline{f}} A \in \mathcal{A}$ so that $f = (U(\overline{f}))\nu_X$.

$$\begin{array}{ccc} X & \xrightarrow{\nu_X} & UFX \\ & \overset{f}{\searrow} & \downarrow{\scriptstyle U(\overline{f})} \\ & & UA \in \Sigma, \end{array} \qquad\qquad \begin{array}{c} FX \\ \downarrow{\scriptstyle \overline{f}} \\ A \in \mathcal{A}. \end{array}$$

Then F extends uniquely to a functor $\Sigma \xrightarrow{F} \mathcal{A}$ so that:

(L) F preserves coproducts and directed limits, and

(R) U preserves products and projective limits.

Proposition: Suppose that the category $\mathcal{C}$ is (R-mod) or (R-alg) and that f is an surjective homomorphism in $\mathcal{C}$, that is, $f : A \xrightarrow{\text{onto}} B$, for $A, B \in \mathcal{C}$. If $A \xrightarrow{g} C \in \mathcal{C}$ has $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(g)$, then there is a unique $\xrightarrow{\overline{g}} C \in \mathcal{C}$ such that $\overline{g}f = g$ and moreover both $\mathrm{Ker}(\overline{g}) = f(\mathrm{Ker}(g)$ and $\mathrm{Im}(\overline{g}) = \mathrm{Im}\, g$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \overset{g}{\searrow} & \downarrow{\scriptstyle \overline{g}} \\ & & C \in \mathcal{C}. \end{array}$$

Using these ideas gives an explanation of some of the items in Ueno, for example the $\varphi*$ map.