These notes summarize the material covered in the Spring 2013 graduate algebra course taught by S. Paul Smith. Written by Josh Swanson; any errors are likely mine.

Note: "A3" below refers to the April 3rd lecture, and similarly with May and June.

Theorem 1 (Hilbert's Basis Theorem, A1) *If R is a commutative noetherian ring, so is the polynomial ring $R[x]$.* □

Definition 1 A **graded ring** is a ring R with a direct sum decomposition (as an abelian group)

$$R = R_0 \oplus R_1 \oplus \cdots,$$

where $R_i R_j \subset R_{i+j}$ for all i, j. The elements of $\cup R_i$ are called **homogeneous**.

Remark 1 (A1) If R is a graded ring, so is its center, $Z(R)$. □

Remark 2 (A1, A3) I is a **graded ideal** if it satisfies these equivalent conditions:

1. I is generated by homogeneous elements.
2. $I = \bigoplus_{n=0}^{\infty}(I \cap R_n)$.

Remark 3 (A1) If R is graded ideal, then R/I is a graded ring in such a way that $\pi: R \to R/I$ preserves degree. □

Definition 2 (A3) Let R be a graded ring. A **graded left R-module** is a left R-module M endowed with an abelian group decomposition

$$M = \oplus_{n=-\infty}^{\infty} M_n,$$

where $R_i \cdot M_n \subset M_{i+n}$. □

Definition 3 (A3) If M and N are graded left R-modules and $f: M \to N$ is an R-module homomorphism, we say f **preserves degree** if $f(M_i) \subseteq N_i$. □

Theorem 2 (Hilbert, A3) *If G is a finite group of degree-preserving automorphisms of $\mathbb{C}[x_1, \ldots, x_n]$, then the set of G-invariant polynomials, $\mathbb{C}[x_1, \ldots, x_n]^G$, is finitely generated as a k-algebra.*

Remark 4 (A3) $\mathbb{C}[x_1, \ldots, x_n]^G$ is a graded subalgebra of $\mathbb{C}[x_1, \ldots, x_n]$ because it is equal to $\bigoplus_{k=0}^{\infty} \mathbb{C}[x_1, \ldots, x_n]_k^G$, where subscript k denotes the degree k elements. □

Remark 5 (A3) Because G is finite and $\operatorname{char} \mathbb{C} = 0$, the G-invariants have a complement as a G-module:

$$\mathbb{C}[x_1, \ldots, x_n]_k = \mathbb{C}[x_1, \ldots, x_n]_k^G \oplus E,$$

where E is a G-module. Similarly,

$$\mathbb{C}[x_1, \ldots, x_n] = \mathbb{C}[x_1, \ldots, x_n]^G \oplus D,$$

where D is a G-module. □

Proposition 1 (A3) *Let S be a commutative graded ring and R a graded subring such that $S = R \oplus K$ as R-modules for some graded R-submodule K of S. If S is a finitely generated k-algebra, then so is R.* □

Proposition 2 (A5) *Let S be a graded quotient of the polynomial ring $k[x_1, \dots, x_n]$ with $S_0 = k$. Let R be a graded subalgebra of S (i.e. $R = \bigoplus_{i=0}^{\infty}(R \cap S_i)$). If there exists a graded R-submodule K of S such that $S = R \oplus K$ as R-modules, then R is a finitely generated k-algebra.* □

Corollary 1 (A5) *If $G \subseteq GL(n,k)$, let G act on automorphisms of $k[x_1, \dots, x_n]$ by extending its action on $kx_1 + kx_2 + \cdots + kx_n$. If $k[x_1, \dots, x_n]^G$ has a graded complement in $k[x_1, \dots, x_n]$ that is a $k[x_1, \dots, x_n]^G$-module then $k[x_1, \dots, x_n]^G$ is finitely generated as a k-algebra.* □

Proposition 3 (A5) *Let $R \subseteq S$ be commutative rings and suppose $S = R \oplus K$ as R-modules for some R-submodule K of S. If S is noetherian, then so is R.* □

Proposition 4 (A5) *Let R be an integral domain, $F = \mathrm{frac}(R)$, and $\mathcal{S} \subseteq R$ such that $1 \in \mathcal{S}$ and $0 \notin \mathcal{S}$. Define*

$$R[\mathcal{S}^{-1}] \coloneqq \{q \in F \mid q = xs_1^{-1} \cdots s_n^{-1} \text{ for some } x \in R, s_i \in \mathcal{S}\}.$$

Then $R[\mathcal{S}^{-1}]$ is a noetherian ring if R is noetherian. □

Definition 4 (A5) Let $R \subseteq T$ be commutative domains. We say $x \in T$ is **integral over** R if it satisfies a monic polynomial over R with coefficients in R. □

Remark 6 (A5)

1. Every element of R is integral over R.
2. $\sqrt{p}$ is integral over $\mathbb{Z}$ because it satisfies the monic polynomial $x^2 - p = 0$.
3. e, π are not integral over $\mathbb{Q}$.

Proposition 5 (A8) *Let $R \subseteq T$ be commutative domains and $x \in T$. The following are equivalent:*

1. *x **is integral over** R.*
2. *$R[x]$ is a finitely generated R-module.*
3. *There exists a ring T' such that $R[x] \subseteq T' \subseteq T$ and T' is a finitely generated R-module.*

Definition 5 (A8) Let $R \subseteq T$ be commutative rings. If T is a finitely generated R-module, call T a **finite R-algebra**.

Remark 7 (A8) If $R \subseteq S \subseteq T$, S is a finite R-algebra, and T is a finite S-algebra, then T is a finite R-algebra. □

Corollary 2 (A8) *Let $R \subseteq T$ be rings and $a_1, \dots, a_n \in T$ where each a_j is integral over R. Then the ring $R[a_1, \dots, a_n]$ is a finite R-algebra and every element in $R[a_1, \dots, a_n]$ is integral over R.* □

Definition 6 (A8) Let $R \subseteq T$ be commutative domains. Say T **is integral over** R if every element of T is integral over R.

Corollary 3 (A8) *Let $R \subseteq T$ be commutative domains such that T is a finitely generated R-algebra. Then T is integral over R if and only if T is a finite R algebra.* □

Theorem 3 (Noether Normalization, A8, A10) *Let k be a field and $R = k[a_1, \dots, a_n]$ a finitely generated commutative k-algebra. Then there exists $m \le n$ and algebraically independent elements $y_1, \dots, y_m \in R$ such that R is integral over the polynomial ring $k[y_1, \dots, y_n] \subseteq R$.* □

Lemma 1 (A10) *Let T be a commutative domain and $R \subseteq T$ such that T is integral over R. Then T is a field if and only if R is a field.* □

Corollary 4 (A10) *If k is a field and $k[a_1, \dots, a_n]$ is a finitely generated k-algebra that is a field, then $\dim_k k[a_1, \dots, a_n]$ is finite.* □

Theorem 4 (Hilbert's "Weak" Nullstellensatz, A10, A12) *Let k be an algebraically closed field. The maximal ideals of $k[x_1, \dots, x_n]$ are given precisely by*

$$(p_1, \dots, p_n) \leftrightarrow (x_1 - p_1, \dots, x_n - p_n),$$

for $p_i \in k$ arbitrary. □

Definition 7 (A12) We write $\mathbb{A}^n_k$ or just $\mathbb{A}^n$ for k^n and call it **affine n-space**.

- The **Zariski topology** is defined by declaring the *closed* sets to be the zero loci of finite sets of polynomials. These are called **affine algebraic varieties**.
- If J is an ideal in $k[x_1, ...x_n]$, then

  $$V(J) := \{p \in \mathbb{A}^n \mid f(p) = 0, \text{ for every } f \in J\},$$

  and this is closed. Because J is finitely generated, if $J = (f_1, \dots, f_r)$ then $V(J) = V(f_1, \dots, f_r)$.
- If $X \subseteq \mathbb{A}^n$, we define

  $$I(X) := \{f \in S \mid f(p) = 0 \text{ for every } p \in X\}.$$

Proposition 6 (A12) *Let I, J, and $\{I_\lambda\}$ be ideals in $k[x_1, \dots, x_n]$.*

1. *$I \subseteq J \Rightarrow V(I) \supseteq V(J)$;*
2. *$V(0) = \mathbb{A}^n$;*
3. *$V(S) = \varnothing$;*
4. *$\bigcap_\lambda V(I_\lambda) = V(\Sigma_\lambda I_\lambda)$;*
5. *$V(I) \cup V(J) = V(IJ) = V(I \cap J)$.*

Proposition 7 (A12) *Let $X, Y \subseteq \mathbb{A}^n$.*

1. *$X \subseteq Y \Rightarrow I(X) \supseteq I(Y)$;*
2. *$X \subseteq V(I(X))$, with equality if and only if X is a closed variety.*
3. *If J is an ideal of $k[x_1, \dots, x_n]$, then $J \subseteq I(V(J))$.*

Example 1 (A12) There are two ways for $J \subsetneq I(V(J))$.

1. If J is not "reduced": $\mathbb{A}^1$, $J = (x^2) \subset k[x]$. Then $(x) = I(\{0\}) = I(V(J)) \neq (x^2)$.
2. If k is not algebraically closed: $\mathbb{R}[x]$, $V(x^2 + 1) = \varnothing$, $I(V(x^2 + 1)) = I(\varnothing) = \mathbb{R}[x]$

Lemma 2 (A15) *Let $X \subseteq \mathbb{A}^n$. Then*

1. *$V(I(X)) = \overline{X}$*

2. *If X is closed, then $V(I(X)) = X$.*

Definition 8 (A15) If J is an ideal of a commutative ring R, its *radical* is

$$\sqrt{J} := \{a \in R \mid a^n \in J \text{ for } n >> 0\}.$$

Notice $J \subseteq \sqrt{J}$, J is an ideal, and $V(J) = V(\sqrt{J})$. □

Theorem 5 (Hilbert's Nullstellensatz, "Strong" Form, A15) *Let k be an algebraically closed field. Let $A = k[x_1, ...x_n]$ be the polynomial ring and J an ideal in A. Then*

1. *If $J \neq A$, then $V(J) \neq \varnothing$.*
2. *$I(V(J)) = \sqrt{J}$.*
3. *There is a bijection*

$$\begin{array}{ccc} \{\textit{radical ideals}\} & \leftrightarrow & \{\textit{closed subsets of } \mathbb{A}^n\} \\ J = \sqrt{J} & \mapsto & V(J) \\ I(X) & \leftarrow\!\shortmid & X = \overline{X} \end{array}.$$

Definition 9 (A15, A17) If $X \subseteq \mathbb{A}^n$, define the **coordinate ring** or the **ring of regular polynomial functions on** X to be

$$\mathcal{O}(X) := \frac{k[x_1, \ldots, x_n]}{I(X)}.$$

Each element of $\mathcal{O}(X)$ is a well-defined function $f: X \to k$. If $k = \overline{k}$, there is a bijection

$$\begin{array}{ccc} \{\text{closed subsets of } X\} & \leftrightarrow & \{\text{radical ideals in } \mathcal{O}(X)\} \\ Y & \mapsto & I(Y) \lhd \mathcal{O}(X) \end{array}.$$

Moreover, the points of X are in bijection with the maximal ideals in $\mathcal{O}(X)$. □

Lemma 3 (A17) *If X and Z are disjoint closed subsets of $\mathbb{A}^n$ over $k = \overline{k}$, then there exists a function $g \in k[x_1, \ldots, x_n]$ such that $g(x) = 0$ for all $x \in X$ and $g(z) = 1$ for all $z \in Z$.* □

Definition 10 (A17) An ideal p in a commutative ring R is **prime** if it satisfies the following equivalent conditions:

1. R/p is a domain.
2. $xy \in p \Rightarrow$ either $x \in p$ or $y \in p$.
3. If I and J are ideals such that $IJ \subseteq p$, then either $I \subseteq p$ or $J \subseteq p$.

Remark 8 (A17) Let R be a domain and $x \in R$ be a non-zero non-unit. Then xR is prime $\Leftrightarrow$ x is prime. Where a non-zero, non-unit element x is prime if whenever $x|yz$, then $x|y$ or $x|z$. □

Theorem 6 (A17) *Every ideal in a noetherian ring contains a finite product of primes.* □

Theorem 7 (A19) *Let J be an ideal in a commutative noetherian ring R. Then there exists a finite number of minimal primes over J, $p_1, \ldots, p_n$ and moreover $\sqrt{J} = p_1 \cap \cdots \cap p_n$.* □

Lemma 4 (A19) *If $p_1 \supseteq p_2 \supseteq \cdots$ is a descending chain of prime ideals in a commutative ring, then $\bigcap_{i=1}^{\infty} p_i$ is prime.* □

Lemma 5 (A19) *If I is an ideal in a commutative ring, then there exist minimal primes over I.* □

Remark 9 (A19) If p is prime, then $p = \sqrt{p}$. $\square$

Definition 11 (A19) A topological space X is **noetherian** if every descending chain of *closed* subspaces is eventually constant.

Remark 10 (A19) Every affine algebraic variety is noetherian. $\square$

Definition 12 (A19) A topological space X is **irreducible** if it is not the union of two proper closed subspaces.

Example 2 (A19) In a commutative noetherian ring, $\sqrt{J} = p_1 \cap \ldots \cap p_n$, so $V(\sqrt{J}) = V(p_1) \cup \cdots \cup V(p_n)$. $\square$

Remark 11 (A19) If R is a UFD, $\sqrt{xR} = p_1 R \cap \cdots \cap p_n R$ where $p_1, \cdots, p_n$ are the prime divisors of x. $\square$

Example 3 (A19) In $\mathbb{A}^2$, the union of the two axes is not irreducible in the Zariski topology because $V(xy) = V(x) \cup V(y)$. $\square$

Proposition 8 (A19) *Let X be a closed subvariety of $\mathbb{A}^n$. The following are equivalent*

1. *X is irreducible*
2. *$I(X)$ is prime*
3. *$\mathcal{O}(X)$ is a domain*

Definition 13 (A22) A function $f: X \to Y$ is a **morphism** (or **polynomial map** or **regular map**) if there are elements $f_1, \ldots, f_m \subseteq \mathcal{O}(X)$ such that $f(p) = (f_1(p), \ldots, f_n(p))$ for all $p \in X$. $\square$

Theorem 8 (A22) *Let $X \subseteq \mathbb{A}^n$, $Y \subseteq \mathbb{A}^m$ be closed subvarieties.*

1. *A morphism $f: X \to Y$ induces a k-algebra homomorphism*
$$f^\sharp : \mathcal{O}(Y) \to \mathcal{O}(X) \quad \textit{by} \quad f^\sharp(g) \coloneqq g \circ f.$$
2. *Every k-algebra homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$ is of the form $f^\sharp$ for some morphism $f: X \to Y$.*
3. *If $X \xrightarrow{f} Y \xrightarrow{h} Z$ are morphisms, then $(h \circ f)^\sharp = f^\sharp \circ h^\sharp$.*
4. *The category of affine algebraic varieties over k is anti-equivalent to the category of finitely generated reduced commutative k-algebras. (Any ring R is **reduced** if $\sqrt{0} = 0$.)*

Corollary 5 (A22) *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties. Then $X \cong Y \Leftrightarrow \mathcal{O}(X) \cong \mathcal{O}(Y)$.* $\square$

Example 4 (A24) Let $C \subseteq \mathbb{A}^2$ be the curve $y = f(x)$, for some polynomial f. Then $C \cong \mathbb{A}^1$. That is, $\mathcal{O}(C)$ is isomorphic to the polynomial ring in one variable. $\square$

Example 5 (A24) The closed sets on $\mathbb{A}^1$ are the finite sets and $\mathbb{A}^1$. So every bijective function $f: \mathbb{A}^1 \to \mathbb{A}^1$ is a homeomorphism in the Zariski topology, but not all are morphisms. Only those of the form $x \mapsto \alpha x + \beta$, $\beta \in k$ are morphisms. $\square$

Lemma 6 (A24) *If k is a field of characteristic $p > 0$ and R is a commutative k-algebra, the function $r \mapsto r^p$ is a k-algebra homomorphism. In particular, if $\operatorname{char}(k) = p > 0$ and X is a closed subvariety of $\mathbb{A}^n$ the function $F: X \to X$ defined by $F(a_1, \ldots, a_n) = (a_1^p, \ldots, a_n^p)$ is a morphism because $F^\sharp: \mathcal{O}(X) \to \mathcal{O}(X)$ is $r \mapsto r^p$. F is the **Frobenius morphism**.* $\square$

Example 6 Let $C = V(y^2 - x^3)$. Define $f: \mathbb{A}^1 \to C$ by $f(\alpha) = (\alpha^2, \alpha^3)$. Although f is a morphism, its inverse $(\alpha, \beta) \mapsto \beta\alpha^{-1}$ if $\alpha \neq 0$ and $(\alpha, \beta) \mapsto 0$ if $\alpha = 0$ is not a morphism.

This is captured by $f^\sharp$: $f^\sharp: \mathcal{O}(C) = k[x,y]/(y^2 - x^3) \to k[t]$ by $f^\sharp(x) = t^2$, $f^\sharp(y) = t^3$, so $f^\sharp$ is not surjective. □

Proposition 9 (A24) *Let $f: X \to Y$ be a morphism between Zariski-closed subspaces of $\mathbb{A}^n$ and $\mathbb{A}^m$ and $f_\sharp: \mathcal{O}(Y) \to \mathcal{O}(X)$ the corresponding k-algebra homomorphism.*

1. *If $Z \subseteq Y$ is closed, then $f^{-1}(Z) = V(f_\sharp(I(Z)))$.*
2. *f is continuous.*
3. *If $W \subseteq X$ is closed, then*
   (a) $I(f(W)) = I(\overline{f(W)}) = f_\sharp^{-1}(I(W))$
   (b) $\overline{f(W)} = V(f_\sharp^{-1} I(W))$
4. $\ker(f_\sharp) = I(f(X))$ *and* $\overline{f(X)} = V(\ker(f_\sharp))$.
5. *ϕ is injective $\Leftrightarrow$ $f(x)$ is dense in Y.*
6. *The fibers $f^{-1}(y)$ for $y \in Y$ are closed.*
7. *$\mathfrak{m}_{f(X)} = \phi^{-1}(\mathfrak{m}_X)$ is the maximal ideal in $\mathcal{O}(Y)$ vanishing at $f(X)$.*

Example 7 (A24) A morphism that sends a closed set to a non-closed set: Let $C = V(xy - 1) \subset \mathbb{A}^2$ and take $f: F \to \mathbb{A}^1$. Then $f^\sharp: \mathcal{O}(\mathbb{A}^1) = k[t] \to k[x,y]/(xy-1) = \mathcal{O}(C)$ by $t \mapsto x$. The image of f is $\mathbb{A}^1 - \{0\}$, so $f(C)$ is not closed. □

Proposition 10 (A26) *Let $f: X \to Y$ be a morphism of affine varieties and $f^\sharp: \mathcal{O}(Y) \to \mathcal{O}(X)$. Suppose $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(Y)$-module.*

1. *The fibers of f are finite.*
2. *If $f^\sharp$ is injective, then f is surjective.*
3. *If $Z \subseteq X$ is closed, then $f(Z)$ is closed in Y.*

Lemma 7 (A26) *Let R be a commutative ring.*

1. *R artinian $\Rightarrow$ every prime ideal in R is maximal.*
2. *R noetherian and every prime ideal in R maximal $\Rightarrow$ R is artinian.*
3. *If R is a finite dimensional k-algebra then R has only a finite number of prime ideals and they are all maximal.*

Proposition 11 (A26) *If $A \subseteq B$ are commutative rings and B is a finitely generated A-module and $\mathfrak{p}$ a prime ideal in A, the there exists a prime ideal $\mathfrak{q}$ in B such that $\mathfrak{q} \cap A = \mathfrak{p}$.* □

Definition 14 (A29) Let S be a multiplicatively closed subset of a commutative ring R containing 1 but not containing 0. Say $(m,s) \sim (m',s')$ if there is some $t \in S$ such that $t(ms' - m's) = 0$. Define $M[S^{-1}]$ to be the R-module whose elements are equivalence classes "m/s" $= [(m,s)]$ with addition and the r-action defined as usual for fractions.

In fact, $M[S^{-1}]$ can be given an $R[S^{-1}]$-module structure. $M[S^{-1}]$ is a *localization of M*. One may localize rings by viewing them as modules over themselves. □

Proposition 12 (A29) *If $0 \to L \to M \to N \to 0$ is an exact sequence of R-modules, then $0 \to L[S^{-1}] \to M[S^{-1}] \to N[S^{-1}] \to 0$ is an exact sequence of $R[S^{-1}]$-modules. That is, localization is an exact functor.* $\square$

Definition 15 (A29) If R is commutative and $\mathfrak{p}$ is prime, then

$$R_{\mathfrak{p}} := R[R - \mathfrak{p}]$$

is the **local ring at** $\mathfrak{p}$. $\square$

Definition 16 (A29) A commutative ring R is **local** if it has a unique maximal ideal. $\square$

Lemma 8 (A29) *If I is an ideal in $R[S^{-1}]$ then I is generated by $I \cap R$, i.e. $I = (I \cap R)R[S^{-1}]$.* $\square$

Lemma 9 (A29) *$\mathfrak{p}R_{\mathfrak{p}}$ is the unique maximal ideal in $R_{\mathfrak{p}}$.* $\square$

Lemma 10 (A29) *Let R be a commutative ring and M a non-zero finitely generated R-module. Then there exists a submodule $N \subseteq M$ such that M/N is a simple module.* $\square$

Lemma 11 (Nakayama, A29) *Let R be a local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module. If $\mathfrak{m}M = M$, then $M = 0$.* $\square$

Definition 17 (A29) Let R be a commutative ring. Its **spectrum** is

$$\operatorname{spec}(R) := \{\text{all prime ideals}\}.$$

Proposition 13 (A29) *The **Zariski topology on** $\operatorname{spec}(R)$ is defined by declaring that the closed subsets to be those of the form*

$$V(I) := \{p \in \operatorname{spec}(R) \mid I \subseteq \mathfrak{p}\},$$

as I ranges over all ideals in R. Indeed, we allow arbitrary subsets B of R in place of I; note that $V(B) = V((B))$. $\square$

Proposition 14 (M1) *Let $\phi: R \to S$ be a ring homomorphism and define $f: \operatorname{spec}(S) \to \operatorname{spec}(R)$ by $f(\mathfrak{p}) = \phi^{-1}(\mathfrak{p}) = \{x \in R \mid \phi(x) \in \mathfrak{p}\}$. Then f is continuous with respect to the Zariski topology.* $\square$

Lemma 12 (M1) *The closed points in $\operatorname{spec}(R)$ are exactly the maximal ideals. Denote these by $\max(R)$.* $\square$

Proposition 15 (M1) *Let $k = \overline{k}$ and $X \subseteq \mathbb{A}^n$ be a subvariety. The map $\Phi: X \to \operatorname{spec}(\mathcal{O}(X))$ where $\Phi(X) = \mathfrak{m}_X = \{f \in \mathcal{O}(X) \mid f(x) = 0\}$ is a homeomorphism onto its image, i.e. $X \cong \max \mathcal{O}(X)$.* $\square$

Lemma 13 (M1) *Let $R \subseteq S$ be an integral extension. If $V \subseteq R$ is multiplicatively closed, $0 \notin V$, and $1 \in V$, then $R[V^{-1}] \subseteq S[V^{-1}]$ is an integral extension.* $\square$

Theorem 9 (Lying Over and Going Up, M3) *Given $R \subseteq S$ an integral extension of domains, $\mathfrak{p} \in \operatorname{spec}(R)$, $\mathfrak{q}' \in \operatorname{spec}(S)$ such that $\mathfrak{q}' \subseteq \mathfrak{p}$, there exists $\mathfrak{q} \in \operatorname{spec}(S)$ such that $\mathfrak{q}' \subseteq \mathfrak{q}$ and $\mathfrak{q} \cap R = \mathfrak{p}$.*

$$\begin{tikzcd}
R \arrow[r, hook] \arrow[d, dash] & S \arrow[d, dash] \\
\mathfrak{p} = \mathfrak{q} \cap R \arrow[r, hook] & \exists\, \mathfrak{q} \\
& \mathfrak{q}' \arrow[u, hook] \arrow[ul, hook]
\end{tikzcd}$$

Corollary 6 (M3) *Let $f: X \to Y$ be a morphism between irreducible affine varieties such that $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(Y)$-module via $f^\sharp: \mathcal{O}(Y) \to \mathcal{O}(X)$. Suppose also that $f^\sharp$ is injective. Then*

1. *If X is closed, then $f(X)$ is closed.*
2. *Given closed subsets $Z \subseteq Y$ and $W' \subseteq X$ such that $f(W') \supseteq Z$, there exists a closed irreducible set $W \subseteq W'$ such that $f(W) = Z$. In particular, f is surjective.*

Theorem 10 (Noether Normalization, M3) *Let $X \subseteq \mathbb{A}^n$ be a closed irreducible subvariety. Noether normalization $\Rightarrow$ there exists a polynomial ring $k[y_1, \dots, y_n] \subseteq \mathcal{O}(X)$ such that $\mathcal{O}(X)$ is integral over $k[y_1, \dots, y_m]$. This inclusion corresponds to a morphism $X \xrightarrow{f} \mathbb{A}^m$ such that*

1. *The fibers of f are finite.*
2. *f is surjective.*
3. *If X is closed, then $f(X)$ is closed.*

Definition 18 (M3) Let X be an affine variety. We call a morphism $\sigma: X \to X$ an **automorphism of** X if the corresponding homomorphism $\sigma^\sharp: \mathcal{O}(X) \to \mathcal{O}(X)$ is a k-algebra automorphism. □

Theorem 11 (Hilbert-Noether, M6) *Suppose R is a finitely generated commutative k-algebra and a domain. Suppose G is a finite group of k-algebra automorphisms of R. Take*

$$R^G = \{f: f^g = f \text{ for every } g \in G\}.$$

Then

1. *R^G is a finitely generated k-algebra.*
2. *R is a finitely generated R^G-module.*

Definition 19 (M6) Let $G \subseteq \mathrm{Aut}(X)$ be a finite group of automorphisms. Write X/G for the set of orbits. Define it as an algebraic variety to have coordinate ring

$$\mathcal{O}(X)^G = \{f \in \mathcal{O}(X) \mid \sigma^\sharp(f) = f, \forall \sigma \in G\}.$$

Also define $\pi: X \to X/G$ to be the morphism corresponding to the inclusion $\mathcal{O}(X)^G \hookrightarrow \mathcal{O}(X)$.

1. $\pi: X \to X/G$ is surjective.
2. The fibers of π are exactly the G orbits, i.e. π sets up a bijection between points of X/G and the G-orbits.
3. The degree of π is $|G|$.
4. If $\rho: X \to Y$ is a morphism that is constant on G-orbits, then there is a unique morphism $\delta : X/G \to Y$ such that $\rho = \delta \circ \pi$.

$$\begin{tikzcd} X \arrow[r, "\rho"] \arrow[d, "\pi"] & Y \\ X/G \arrow[ur, dashed, "\delta"] & \end{tikzcd}$$

Definition 20 (M6) Let $f\colon X \to Y$ be a morphism such that $f^\sharp\colon \mathcal{O}(Y) \to \mathcal{O}(X)$ is such that $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}O(Y)$-module. We define $k(X) := \operatorname{frac} \mathcal{O}(X)$. Suppose also $f^\sharp$ is injective, making the following diagram commute:

$$\begin{tikzcd} \mathcal{O}(Y) \arrow[r] \arrow[d, hook] & \mathcal{O}(X) \arrow[d, hook] \\ k(Y) \arrow[r, dashed, "\exists!"] & k(X) \end{tikzcd}$$

Since $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(Y)$-module, $k(X)$ is a finite dimensional $k(Y)$-vector space. Define $\deg(f) := [k(X) : k(Y)]$. ◻

Theorem 12 (M6) *There exists a proper closed subvariety $Z \subseteq X$ such that $[f^{-1}(y)] = \deg(f)$ for all $y \in Y - Z$.* ◻

Definition 21 (M8) *$Ext^n_R(M, N)$***:** Let R be a ring. Suppose $0 \to N \to N' \to N'' \to 0$ and $0 \to M \to M' \to M'' \to 0$ are exact sequences of R-modules. Then there are exact sequences

$$\begin{aligned} 0 &\to \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(M, N') \to \operatorname{Hom}_R(M, N'') \\ &\to \operatorname{Ext}^1_R(M, N) \to \operatorname{Ext}^1_R(M, N'0 \to \operatorname{Ext}^1_R(M, N'') \\ &\to \operatorname{Ext}^2_R(M, N) \to \cdots, \\ 0 &\to \operatorname{Hom}_R(M'', N) \to \operatorname{Hom}_R(M', N) \to \operatorname{Hom}_R(M, N) \\ &\to \operatorname{Ext}^1_R(M'', N) \to \operatorname{Ext}^1_R(M', N) \to \operatorname{Ext}^1_R(M, N) \\ &\to \operatorname{Ext}^2_R(M'', N) \to \cdots. \end{aligned}$$

Indeed, $\operatorname{Ext}^0_R(M, N) = \operatorname{Hom}_R(M, N)$. If R is commutative, then $\operatorname{Ext}^n_R(M, N)$ is an R-module. ◻

Definition 22 (M8) A **projective resolution** of an R-module M is an exact sequence

$$\cdots \to P_n \to \cdots \xrightarrow{\alpha_2} P_! \xrightarrow{\alpha_1} P_0 \xrightarrow{\epsilon} M \to 0,$$

where each P_i is a projective left R-module.

Example 8 (M8) Let $R = k[x]/(x^2)$, $M = R/(x)$.

$$\cdots \to R \xrightarrow{x} R \xrightarrow{x} R \to M \to 0.$$

Definition 23 (M8) Apply the functor $\operatorname{Hom}_R(-, N)$ to the projective resolution above to get a cochain complex

$$0 \to \operatorname{Hom}_R(M, N) \xrightarrow{\epsilon'} \operatorname{Hom}_R(P_0, N) \xrightarrow{\alpha_1'} \operatorname{Hom}_R(P, N) \xrightarrow{\alpha_2'} \cdots,$$

where $\alpha_n' = (-) \circ \alpha_n$. Take homology:

$$\operatorname{Ext}^n_R(M, N) := \frac{\ker \alpha_{n+1}'}{\operatorname{im} \alpha_n'}.$$

(We can analogously use an injective resolution.)

Theorem 13 (M8) $\operatorname{Ext}^n_R(M, N)$ *is independent of the choice of resolution.* ◻

Definition 24 (M8) A **chain complex** (C, d) is a sequence of abelian groups and homomorphisms

$$\cdots \to C_{n+1} \overset{d_{n+1}}{\to} C_n \overset{d_n}{\to} C_{n-1} \overset{\cdots}{\to}$$

such that $d^2 = 0$.

- The n**-cycles** are $Z_n(C) \coloneqq \ker d_n$,
- the n**-boundaries** are $B_n(C) \coloneqq \operatorname{im} d_{n+1}$,
- and the n**th homology groups** are $H_n(C) \coloneqq \frac{Z_n(C)}{B_n(C)}$.

Definition 25 (M8) A **chain map** $f_\cdot\colon (D_\cdot, d'_\cdot) \to (C_\cdot, d_\cdot)$ is a collection of maps and homomorphisms $f_n\colon D_n \to C_n$ such that the following commutes:

$$\begin{tikzcd}
D_n \arrow[r, "d'_n"] \arrow[d, "C_n"] & D_{n-1} \arrow[d, "f_{n-1}"] \\
C_n \arrow[r, "d_n"] & C_{n-1}.
\end{tikzcd}$$

(This gives an abelian category of chain complexes.) □

Lemma 14 (M8) *If $f\colon D_\cdot \to C_\cdot$ is a chain map, it induces maps $H_n(f_n)\colon H_n(D) \to H_n(C)$ for all n.* □

Definition 26 (M8) Let $f, g\colon D \to C$ be chain maps. We say f is **null-homotopic** if for all n there exists $s_n\colon D_n \to C_{n+1}$ such that $f_n = d_{n+1}s_n + s_{n-1}d_n$.

$$\begin{tikzcd}
\cdots \arrow[r] & D_n \arrow[r, "d'_n"] \arrow[dl, "s_n"'] \arrow[d, "f_n"] & D_{n-1} \arrow[r] \arrow[dl, "s_{n-1}"'] \arrow[d, "f_{n-1}"] & \cdots \arrow[d] \\
C_{n+1} \arrow[r, "d_{n+1}"] & C_n \arrow[r, "d_n"] & C_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

We say f **is homotopic to** g if $f - g$ is null-homotopic.

Lemma 15 (M8) *Homotopic maps induce the same map on homology, i.e. $f \sim g \Rightarrow H_n(f_n) = H_n(g_n)$.* □

Proposition 16 (M10) *Let $\beta\colon M' \to M$ be a module homomorphism. Let $\cdots \to P'_0 \to M'$ and $\cdots \to P_0 \to M$ be projective resolutions. Then there exists $\widehat{\beta}_\cdot\colon P'_\cdot \to P_\cdot$ that "lifts" β, and $\widehat{\beta}$ is unique up to homotopy. That is,*

$$\begin{tikzcd}
\cdots \arrow[r] & P'_1 \arrow[r, "d'_1"] \arrow[d, "\exists\, \widehat{\beta}_1"] & P'_0 \arrow[r, "\epsilon'"] \arrow[d, "\exists\, \widehat{\beta}_2"] & M' \arrow[r] \arrow[d, "\beta"] & 0 \\
\cdots \arrow[r] & P_1 \arrow[r, "d_1"] & P_0 \arrow[r, "\epsilon"] & M \arrow[r] & 0
\end{tikzcd}$$

Theorem 14 (M13) *Let $0 \to C''_\cdot \overset{i}{\to} C'_\cdot \overset{p}{\to} C_\cdot \to 0$ be an exact sequence of complexes. For each n, there exists a natural homomorphism*

$$\delta_n\colon H_n(C) \to H_{n-1}(C'')$$

defined by $\delta_n(z + B_n(C)) = i_{n-1}^{-1} d'_n P_n^{-1}(z) + B_{n-1}(C'')$. □

Definition 27 (M13) Isomorphism of functors Let $F, G\colon \mathcal{C} \to \mathcal{D}$ be functors. A **natural transformation** $\tau\colon F \to G$ is a collection of morphisms τ_X for $X \in \operatorname{Ob}(\mathcal{C})$, $\tau_x\colon FX \to GX$, such that if $f\colon X \to Y$ is a morphism, then the diagram below commutes:

$$\begin{array}{ccc} FX & \xrightarrow{\tau_X} & GX \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ FY & \xrightarrow{\tau_Y} & GY \end{array}$$

If τ_X is an isomorphism for all $X \in \mathcal{C}$, we say that τ is a **natural isomorphism** and that F **and** G **are isomorphic functors**, $F \cong G$. We say $\mathcal{C}$ and $\mathcal{D}$ are **equivalent** if there are functors $F: \mathcal{C} \to \mathcal{D}$ and $G: \mathcal{D} \to \mathcal{C}$ such that $F \circ G \cong \mathrm{id}_{\mathcal{D}}$ and $G \circ F \cong \mathrm{id}_{\mathcal{C}}$. □

Theorem 15 (M15) *Let $E^n: \mathrm{Mod}(R) \to \mathrm{Ab}$ be a sequence of contravariant functor for $n \geq 0$ such that*

1. *for every short exact sequence $0 \to M \to M' \to M'' \to 0$ in $\mathrm{Mod}(R)$, there is a long exact sequence with natural connected homomorphisms*

$$\cdots \to E^n(M'') \to E^n(M') \to E^n(M) \xrightarrow{\delta_n} E^{n+1}(M'') \to \cdots;$$

2. *there exists a right R-module N such that $E^0(-) \cong \mathrm{Hom}_R(-, N)$;*

3. *$E^n(P) = 0$ for all $n \geq 1$ and all projectives P.*

If $F^n: \mathrm{Mod}(R) \to \mathrm{Ab}$ is another sequence of contravariant functors satisfying these conditions and $F^0(-) \cong \mathrm{Hom}_R(-, N)$ for the same N, then $F^n \cong E^n$ for all n. □

Lemma 16 (M15) *Let P be an R-module. The following are equivalent.*

1. *P is projective.*

2. $\mathrm{Ext}^1_R(P, -) = 0$.

3. $\mathrm{Ext}^n_R(P, -) = 0$ *for all $n \geq 1$.*

Definition 28 (M15) The **projective dimension** of a module M is the smallest n such that $\mathrm{Ext}^{n+i}_R(M, -) = 0$ for all $i \geq 0$.

Example 9 (M15) The projective dimension of M is 0 if and only if M is projective. □

Definition 29 (M15) The **global homological dimension** of R is the smallest n such that $\mathrm{Ext}^{n+i}_R(-, -) = 0$ for all $i \geq 1$.

Remark 12 (M15)

- The global dimension of R is 0 if and only if R is semisimple.
- If R is a PID, then the global dimension of R is 1.
- If M is a finitely generated R-module, M is torsion if and only if the projective dimension of M is 1.
- The global dimension of $k[x_1, \ldots, x_n]$ is n.
- The projective dimension of $k[x_1, \ldots, x_n]/\mathfrak{m}$ is n for all maximal ideals $\mathfrak{m}$.
- The projective dimension of $k[x_1, \ldots, x_n]/\mathfrak{p}$ is the transcendence degree of its field of fractions, which is $n - \dim V(\mathfrak{p})$, when $\mathfrak{p}$ is prime.
- If X is an irreducible affine variety, then the global dimension of $\mathcal{O}(X)$ is finite if and only if X is "smooth".

Definition 30 (M17) **Tensor products of vector spaces**: given bases v_i of V and w_j of W, $v_i \otimes w_j$ is a bases for $V \otimes_k W$, where V, W are k-vector spaces. There is a linear map $V \otimes W^* \xrightarrow{\Phi} \mathrm{Hom}_k(W, V)$ given by $\Phi(v \otimes \lambda)(w) = \lambda(w)v$. This is injective, and moreover if $\dim V, \dim W < \infty$, then Φ is a linear isomorphism. Moreover, $V \otimes V^* \xrightarrow{\cong} \mathrm{Hom}_k(V, V)$.

If v_i is a basis for V and λ_i is the dual basis for V^*, then $\Phi(\sum v_i \otimes \lambda_i) = \mathrm{id}_V$. If $\dim V, \dim W < \infty$, then $V \otimes W \xrightarrow{\Phi} \mathrm{Hom}_k(W^*, V)$ is an isomorphism. □

Definition 31 (M17) The **double dual functor** $(-)**$ from finite dimensional vector spaces to itself is isomorphic to the identity functor. (There is also a single dual functor.) □

Definition 32 (M17) If $T: U \to U'$ is a linear transformation, then $\mathrm{rank}(T)$ is the smallest n such that T factors as $U \to k^n \to U'$.

Example 10 (M17) The rank one 2×2 matrices are those of the form

$$k^2 \xrightarrow{(cd)} k \xrightarrow{(a;b)} k^2$$

. □

Proposition 17 (M17) *Let V and W be finite dimensional vector spaces and $f \in V \otimes W$. Then* $\mathrm{rank}(f)$ *is the smallest n such that $f = v_1 \otimes w_1 + \cdots + v_n \otimes w_n$ for some $v_i \in V$ and $w_i \in W$.* □

Definition 33 (M17) Let R be any ring. Let M be a right R-module and N a left R-module. Define the **tensor product** $M \otimes_R N$ as follows. First let F be the free abelian group with basis $(m, n) \in M \times N$. Let K be the subgroup generated by elements

$$\begin{aligned}(m, n + n') - (m, n) - (m, n')\\ (m + m', n) - (m, n0 - (m', n)\\ (mr, n) - (m, rn)\end{aligned}$$

for all $m, m' \in M$, $n \in N$, $r \in R$. Define $M \otimes_R N$ as an abelian group to be F/K. Write $m \otimes n$ for the coset $(m, n) + K$. The relations ensure $\otimes$ is "bilinear", and $mr \otimes n = m \otimes rn$.

Example 11 (M17)

- $\frac{\mathbb{Z}}{3\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{2\mathbb{Z}} = 0$
- More generally, if I and J are ideals in a commutative ring such that $I + J = R$, then
$$\frac{R}{I} \otimes_R \frac{R}{J} = 0.$$
- Even more generally,
$$\frac{R}{I} \otimes_R N \cong \frac{N}{IN}.$$

Proposition 18 (M17) *Let $\alpha: M \times N \to M \otimes_R N$ be the homomorphism of abelian groups $\alpha(m, n) = m \otimes n$. If $f: M \times N \to G$ is a homomorphism to an abelian group G such that*

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

for all $m, m' \in M$, $n, n' \in N$, $r \in R$, then there exists a unique group homomorphism $\phi: M \otimes_R N \to G$ such that $f = \phi \circ \alpha$:

$$\begin{tikzcd} M \times N \arrow[r, "\alpha"] \arrow[dr, "\alpha"'] & M \otimes_R N \arrow[d, dashed, "\phi"] \\ & G \end{tikzcd}$$

Lemma 17 (M20) *Let R, S be rings.*

1. *For modules $(M_R, {}_RN_S, X_S)$, there is an isomorphism of abelian groups*

$$\Phi: \mathrm{Hom}_S(M \otimes_R N, X) \xrightarrow{\cong} \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, X))$$
$$\Phi(f)(m)(n) := f(m \otimes n).$$

2. *For modules $({}_SM_R, {}_RN, {}_SY)$, there is an isomorphism of abelian groups*

$$\Phi: \mathrm{Hom}_S(M \otimes_R N, Y) \xrightarrow{\cong} \mathrm{Hom}_R(N, \mathrm{Hom}_S(M, Y))$$

given by

$$\Phi(f)(n)(m) := f(m \otimes n).$$

Remark 13 (M20) If M_R, ${}_RN_S$, then

- $M \otimes_R N$ is a right S-module via $(m \otimes n)s = m \otimes (ns)$.
- $\mathrm{Hom}_S(N, X)$ is a right R-module via $\alpha \cdot r)(n) = \alpha(rn)$.

Definition 34 (M20) Let $\mathcal{C}, \mathcal{D}$ be categories and let $F: \mathcal{C} \to \mathcal{D}$ and $G: \mathcal{D} \to \mathcal{C}$ be functors. We say F **is left adjoint to** G and G **is right adjoint to** F if there are bifunctorial isomorphisms

$$\tau_{\mathcal{C},\mathcal{D}}: \mathrm{Hom}_{\mathcal{D}}(FC, D) \xrightarrow{\cong} \mathrm{Hom}_{\mathcal{C}}(C, GD)$$

for all $C \in \mathcal{C}$ and $D \in \mathcal{D}$. That is, if $\alpha: C \to C'$ in $\mathcal{C}$, then the following commutes:

$$\begin{tikzcd} \mathrm{Hom}_{\mathcal{D}}(FC, D) \arrow[r, "\tau_{C,D}"] & \mathrm{Hom}_{\mathcal{C}}(C, GD) \\ \mathrm{Hom}_{\mathcal{D}}(FC', D) \arrow[r, "\tau_{C',D}"] \arrow[u, "(-)\circ F_\alpha"] & \mathrm{Hom}_{\mathcal{C}}(C', GD), \arrow[u, "(-)\circ\alpha"'] \end{tikzcd}$$

and similarly if $\beta: D \to D'$. □

Theorem 16 (M20) *Let R and S be rings, ${}_RN_S$ a bimodule. Then $- \otimes_R N: \mathrm{Mod}^r(R) \to \mathrm{Mod}^r(S)$ is left adjoint to* $\mathrm{Hom}_S(N, -): \mathrm{Mod}^r(S) \to \mathrm{Mod}^r(R)$ *(where r indicates right-modules). The isomorphisms*

$$\tau_{M,X}: \mathrm{Hom}_S(FM, X) \xrightarrow{\cong} \mathrm{Hom}_R(M, GX)$$

are the Φ's in the previous lemma. □

Proposition 19 (M20) *If $F: \mathcal{C} \to \mathcal{D}$ and $G: \mathcal{D} \to \mathcal{C}$ are an adjoint pair of functors with F left adjoint to G in abelian categories, then F is right exact and G is left exact.*

Example 12 (M22) If ${}_RN_S$, then $- \otimes_R N: \mathrm{Mod}^r R \to \mathrm{Mod}^r S$ is left adjoint to $\mathrm{Hom}_S(N, -): \mathrm{Mod}^r S \to \mathrm{Mod}^r R$. Thus $- \otimes_R N$ is right exact, and $\mathrm{Hom}_S(N, -)$ is left exact. □

Lemma 18 (M22) *The following are equivalent.*

1. $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ *is an exact sequence of left R-modules*

2. $0 \to \mathrm{Hom}_R(X, A) \xrightarrow{\alpha^*} \mathrm{Hom}_R(X, B) \xrightarrow{\beta^*} \mathrm{Hom}_R(X, C)$ *is exact for all X.*

The following are also equivalent.

1. $A \to B \to C \to 0$ *is exact.*

2. $0 \to \mathrm{Hom}_R(C, Y) \to \mathrm{Hom}_R(B, Y) \to \mathrm{Hom}_R(A, Y)$ *is exact for all Y.*

Lemma 19 (M22) *If M is a left R-module, themap $M \xrightarrow{f} R \otimes_R M$ given by $f(m) = 1 \otimes m$ is an isomorphism of left R-modules.* □

Lemma 20 (Change of Rings, M22) *Suppose $f: R \to S$ is a ring homomorphism. We have functors*

$$f^* = S \otimes_R -: \mathrm{Mod}^\ell R \to \mathrm{Mod}^\ell S$$
$$f_* = \mathrm{Hom}_S(S, -): \mathrm{Mod}^\ell S \to \mathrm{Mod}^\ell R$$
$$f' = \mathrm{Hom}_R(S, -): \mathrm{Mod}^\ell R \to \mathrm{Mod}^\ell S,$$

where f^* is left adjoint to f_*, f_* is left adjoint to f', so f^* is right exact, f_* is exact, and f' is left exact. □

Lemma 21 (M24) *The map $\frac{R}{I} \otimes_R M \xrightarrow{f} \frac{M}{IM}$ given by $f([r + I] \otimes m) = [rm + IM]$ is an isomorphism. Similarly $\frac{R}{I} \otimes_R \frac{R}{J} = \frac{R}{I+J}$.* □

Definition 35 (M24) A left R-module M is **flat** if $0 \to X \otimes_R M \to Y \otimes_R M \to Z \otimes_R M \to 0$ is exact for all short exact sequences of right R-modules $0 \to X \to Y \to Z \to 0$, that is, if $- \otimes_R M$ is an exact functor.

Example 13 (M24) R is flat as a module over itself, since $X \cong X \otimes_R R$. □

Proposition 20 (M24) *$\otimes$ distributes over (arbitrary) $\oplus$.*

1. *A module $N_1 \oplus N_2$ is a flat R-module if and only if N_1, N_2 are flat R-modules.*

2. *In particular, projective R-modules are flat.*

3. *If R is noetherian, every finitely generated flat R-module is projective.*

4. *More generally, finitely presented flat modules over arbitrary rings are projective.*

Example 14 (M24) $\mathbb{Q}$ is a flat $\mathbb{Z}$-module but is not projective. □

Lemma 22 (M24) *There is a natural isomorphism*

$$M \otimes_R R[S^{-1}] \to M[S^{-1}]$$

given by

$$m \otimes xs^{-1} \mapsto mxs^{-1}.$$

Lemma 23 (M29) *The map $g: M \to M[S^{-1}]$ given by $g(m) = m \otimes 1$ is an R-module homomorhism, and* $\ker g = \{m \in M \mid ms = 0$ *for some* $s \in S\}$. □

Definition 36 (M29) If R is any ring, M is a right R-module, and N is a left R-module, we define the **Tor** groups $\mathrm{Tor}_i^R(M, N)$ for $i \geq 0$ as follows. Take a projective resolution of M (by projective right R-modules), and define the Tor groups $\mathrm{Tor}_i^R(M, N)$ as the homology groups associated to the complex obtained from the projective resolution by applying the $- \otimes_R N$ functor. □

Theorem 17 (M29) *1.* $\mathrm{Tor}_0^R(M,N) = M \otimes_R N$*;*

2. $\mathrm{Tor}_i^R(M,N)$ *does not depend on the choice of projective resolution;*

3. If $0 \to X \to Y \to Z \to 0$ *is an exact sequence of left* R*-modules, then there is a long exact sequence*

$$\begin{aligned}\cdots \to \mathrm{Tor}_n^R(M,X) \to \mathrm{Tor}_n^R(M,Y) \to \mathrm{Tor}_n^R(M,Z) \to \\ \mathrm{Tor}_{n-1}^R(M,X) \to \cdots \to \mathrm{Tor}_1(M,Z) \\ M \otimes_R X \to M \otimes_R Y \to M \otimes_R Z \to 0.\end{aligned}$$

4. If $Q. \to N \to 0$ *is a projective resolution of* N*, then* $\mathrm{Tor}_i^R(M,N)$ *is isomorphic to the homology group of the complex* $M \otimes_R Q$*.*

5. If $0 \to A \to B \to C \to 0$ *is an exact sequence of right* R*-modules, there is a long exact sequence*

$$\cdots \to \mathrm{Tor}_1(C,N) \to A \otimes_R N \to B \otimes_R N \to C \otimes_R N \to 0;$$

6. $\mathrm{Tor}_n^R(M,-) = 0$ *for all* $n \geq 1$ *if and only if* M *is a flat right* R*-module;*

7. $\mathrm{Tor}_n^R(-,N) = 0$ *for all* $n \geq 0$ *if and only if* N *is a flat left* R*-module.*

Remark 14 (M29) If R is commutative, M, N are projective, then $M \otimes_R N$ is projective. □

Example 15 (M29) If $R = k[x_1, \ldots, x_n]$, $k = R/(x_1, \ldots, x_n)$, then $\mathrm{Tor}_i^R(k,k) \cong k^{\binom{n}{i}}$ □

Definition 37 (M31) A **Dedekind domain** is a ring with the following properties:

- Commutative noetherian domain that is not a field;
- Integrally closed in its field of fractions;
- Every non-zero prime ideal is maximal.

Example 16 (M31) 1. Rings of integers in number fields: a **number field** is a finite field extension of $\mathbb{Q}$. The **ring of integers** in K, sometimes written $\mathcal{O}_K$, is the integral closure of $\mathbb{Z}$ in K, i.e. the set of elements of K which satisfy a monic polynomial with coefficients in $\mathbb{Z}$.

2. If C is a "smooth" irreducible affine curve, then $\mathcal{O}(C)$ is a Dedekind domain. For instance, $y^2 = x^3$ gives $k[t^2, t^3]$. This is not a smooth curve, and the ideal (t^2, t^3) is not "generated by one and a half elements"; see below for a definition.

3. If R is a domain and $\mathfrak{p}$ is a minimal nonzero prime ideal, then $R_\mathfrak{p}$ is a Dedekind domain if and only if $\frac{\mathfrak{p}R_\mathfrak{p}}{(\mathfrak{p}R_\mathfrak{p})^2}$ is a 1-dimensional vector space over the field $\frac{R_\mathfrak{p}}{\mathfrak{p}R_\mathfrak{p}}$.

   If X is a smooth affine algebraic variety of dimension n and $Y \subset X$ is an irreducible subvariety of dimension $n-1$ and $\mathfrak{p}$ is the ideal $I(Y)$, then $\mathcal{O}(X)_\mathfrak{p}$ is a Dedekind domain.

Definition 38 (M31) Let R be a commutative noetherian domain and K its field of fractions. A non-zero R-submodule of K is a **fractional ideal** if $xM \subset R$ for some $0 \neq x \in R$.

Remark 15 (M31)

- Fractional ideals are noetherian R-modules.
- If M is a nonzero finitely generated R-submodule of K, then M is a fractional ideal.
- Every nonzero ideal in R is a fractional ideal.

- A product of fractional ideals is a fractional ideal.
- If M and N are fractional ideals, then $M \cap N \neq 0$.
- The set of fractional ideals forms an abelian monoid (a group except without inverses).

Definition 39 (M31) If M is a fractional ideal, we define

$$M^{-1} := \{x \in K \mid xM \subseteq R\}.$$

Note that M^{-1} is also a fractional ideal, and $MM^{-1} \subseteq R$.

Example 17 (M31) $\mathrm{Hom}_R(M, R) \cong M^{-1}$ as R-modules. □

Proposition 21 (J3) *Let $\mathfrak{m}$ be a maximal ideal in a Dedekind domain, then $\mathfrak{m}\mathfrak{m}^{-1} = R$.* □

Theorem 18 (J3) *Every nonzero ideal in a Dedekind domain is a product of maximal ($\Leftrightarrow$ prime) ideals in a unique way.*

Corollary 7 (J3) *The set of fractional ideals for a Dedekind domain is a group under multiplication with identity R.* □

Definition 40 (J3) The **principal ideals** (a slight abuse of notation) in the group of fractional ideals are those generated by a single element as an R-module. In a Dedekind domain, they form a subgroup, and the quotient of of the group of fractional ideals by this subgroup is the **ideal class group** or the **Picard group** of R. The **class number** of K is the order of the ideal class group. □

Proposition 22 (J3) *If $\mathfrak{m}$ is a maximal ideal in a Dedekind domain R, then $R\mathfrak{m}$ is a valuation ring. The valuation of $x \in K - \{0\}$ is the largest n such that $x \in \mathfrak{m}^n$.* □

Proposition 23 (J5) *Let R be a Dedekind domain, $\mathfrak{m}$ a maximal ideal, and $k = R/\mathfrak{m}$. Then*

1. $\dim_k \mathfrak{m}^n/\mathfrak{m}^{n+1} = 1$ *for all $n \geq 0$ $(\mathfrak{m}^0 = R)$;*
2. *If $t \in \mathfrak{m} - \mathfrak{m}^2$, then $\mathfrak{m}^d = \mathfrak{m}^n + Rt^d$ for all integers $1 \leq d \leq n$.*
3. *The only ideals containing $\mathfrak{m}^d$ are $\mathfrak{m}^n$ for $n \leq d$.*

Lemma 24 (J5) *If $R_1, \dots, R_n$ are rings in which every ideal is principal, so is $R = R_1 \oplus \cdots \oplus R_n$.* □

Proposition 24 (J5) *Every ideal in a Dedekind domain can be generated by "one and a half elements". This means that given an ideal I and an arbitrary element $0 \neq x \in I$, there is some element $y \in I$ such that $I = (x, y)$.*

Lemma 25 (J5) *If I is a non-zero ideal in a Dedekind domain R, then R/I has finite length.* □

Proposition 25 (J5) *Let $\mathfrak{m}$ be a maximal ideal in a Dedekind domain R.*

1. *$R\mathfrak{m}$ is a PID.*
2. *If $t \in \mathfrak{m}R_{\mathfrak{m}} - \mathfrak{m}^2R_{\mathfrak{m}}$, then (t^n) for $n \geq 0$ are all the nonzero ideals of $R\mathfrak{m}$.*
3. *$R\mathfrak{m}$ is a valuation ring.*