# A Second Course in Commutative Algebra

Gaurav Goel
gauravgoel@college.harvard.edu

July 2022

This is a collection of (incomplete) lecture notes based on Math 221: Commutative Algebra taught by Mihnea Popa at Harvard in Fall 2021.

## Contents

# 1 Fundamentals

In these notes, a *ring* is a commutative unitary ring. We do not disallow $0 = 1$, although the zero ring has no proper ideals, so when we speak of any proper ideals (including prime or maximal ideals, which are always assumed to be proper), we implicitly assume that the ring is nonzero. We do require that a field be nonzero. For a prime ideal $\mathfrak{p} \subset R$, we let $\kappa(\mathfrak{p}) := \operatorname{Frac} R/\mathfrak{p}$.

## 1.1 Prime Avoidance and Minimal Primes

**Lemma 1.1.1.** Let $k$ be an infinite field, $V/k$ a vector space, $n \geq 2$ an integer, and $U, V_1, \ldots, V_n \subseteq V$ subspaces. If $U \subseteq \bigcup_i V_i$, then there is an $i$ such that $U \subseteq V_i$.

*Proof.* First, reduce to the case $U = V$ by replacing $V_i$ by $V_i \cap U$; therefore, we are reduced to showing that if $V_i$ are proper then $\bigcup_i V_i \subsetneq V$. Assume contrarily that $V = \bigcup_i V_i$. By removing redundancies assume that the decomposition is minimal, i.e. $V_i \not\subseteq \bigcup_{j\neq i} V_j$ for any $i$. For each $i$, pick a $v_i \in V_i \smallsetminus \bigcup_{j\neq i} V_j$, and look at the set $\{\alpha v_1 + (1-\alpha)v_2 : \alpha \in k\}$. All elements in here are distinct since $v_1$ and $v_2$ are linearly independent; therefore, this is an infinite set, and so there is some $i$ such that two different elements of this set lie in $V_i$. That would imply then that $v_1, v_2 \in V_i$, a contradiction. ∎

**Counterexample 1.1.2.** Lemma 1.1.1 is false if $k$ is not infinite; take $k = \mathbf{F}_2$, $U = V = \mathbf{F}_2^2 = \langle \mathrm{e}_1, \mathrm{e}_2 \rangle$, $n = 3$, $V_1 = \langle \mathrm{e}_1 \rangle, V_2 = \langle \mathrm{e}_2 \rangle$ and $V_3 = \langle \mathrm{e}_1 + \mathrm{e}_2 \rangle$.

**Lemma 1.1.3** (Prime Avoidance)**.** Let $R$ be a ring, $n \geq 2$ be an integer, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq R$ be ideals.

(a) Suppose that $\mathfrak{p} \subset R$ is a prime such that $\bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$. Then there is an $i$ such that $\mathfrak{a}_i \subseteq \mathfrak{p}$.
(b) Suppose that $\mathfrak{a} \subseteq R$ is an ideal such that $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{a}_i$. If either $R$ contains an infinite field or at most two of the $\mathfrak{a}_i$ are not prime, then there is an $i$ such that $\mathfrak{a} \subseteq \mathfrak{a}_i$.

*Proof.* For (a), note else that we may pick for each $i$ an $a_i \in \mathfrak{a}_i \smallsetminus \mathfrak{p}$ and then $\prod_i a_i \in \bigcap_i \mathfrak{a}_i \smallsetminus \mathfrak{p}$ using the primality of $\mathfrak{p}$. For (b), the case of when $R$ contains an infinite field follows from Lemma 1.1.1; for the proof in the second case, induct on $n$. When $n = 2$, there is no restriction on the $\mathfrak{a}_i$; if the result is false, then pick $x_1 \in \mathfrak{a} \smallsetminus \mathfrak{a}_2 \subseteq \mathfrak{a}_1 \smallsetminus \mathfrak{a}_2$ and $x_2 \in \mathfrak{a} \smallsetminus \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \smallsetminus \mathfrak{a}_1$. Then $x_1 + x_2 \in \mathfrak{a} \smallsetminus \mathfrak{a}_1 \cup \mathfrak{a}_2$, a contradiction. Suppose finally $n \geq 3$ and that $\mathfrak{a}_3, \ldots, \mathfrak{a}_n$ are prime. Inductively assume that $\mathfrak{a}$ does not belong to unions of $(n-1)$'s of the $\mathfrak{a}_i$'s, i.e. that for each $i$ there is an $x_i \in \mathfrak{a} \smallsetminus (\mathfrak{a}_1 \cup \cdots \cup \hat{\mathfrak{a}}_i \cup \cdots \cup \mathfrak{a}_n) \subseteq \mathfrak{a}_i \smallsetminus (\mathfrak{a}_1 \cup \cdots \cup \hat{\mathfrak{a}}_i \cup \cdots \cup \mathfrak{a}_n)$. Then $x_1 \cdots x_{n-1} \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1} \smallsetminus \mathfrak{a}_n$ by primality of $\mathfrak{a}_n$ whereas $x_n \in \mathfrak{a}_n \smallsetminus (\mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_{n-1})$, so if $x := x_1 \cdots x_{n-1} + x_n$, then $x \in \mathfrak{a} \smallsetminus \bigcup_i \mathfrak{a}_i$, a contradiction. ∎

**Lemma 1.1.4** (Existence of Minimal Primes)**.** Let $R$ be a ring and $\mathfrak{a} \subset R$ an ideal and $\mathfrak{p} \subset R$ a prime such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then there is a minimal prime lying over $\mathfrak{a}$ contained in $\mathfrak{p}$.

(a) There is a minimal prime lying over $\mathfrak{a}$.
(b) If $\mathfrak{a} \subset \mathfrak{p}$ for some prime $\mathfrak{p}$, then there is a minimal prime lying over $\mathfrak{a}$ contained in $\mathfrak{p}$.

*Proof.* Both (a) and (b) follow by applying Zorn's Lemma to a suitable set: (a) to $\mathbf{V}(\mathfrak{a})$ (and nonempty since $\mathfrak{a} \subseteq \mathfrak{m}$ for some maximal $\mathfrak{m}$) and (b) to $\mathbf{V}(\mathfrak{a}) \cap \operatorname{Spec} R_{\mathfrak{p}}$. If $(\mathfrak{p}_\alpha)$ is a chain in either then $\mathfrak{p} := \bigcap_\alpha \mathfrak{p}_\alpha$ is also a prime containing $\mathfrak{a}$: if $xy \in \mathfrak{p}$ but $x, y \notin \mathfrak{p}$, then there are $\alpha, \beta : x \notin \mathfrak{p}_\alpha, y \notin \mathfrak{p}_\beta$; WLOG $\mathfrak{p}_\alpha \subseteq \mathfrak{p}_\beta$, but then $y \notin \mathfrak{p}_\alpha$ either and then $xy \in \mathfrak{p}_\alpha$ but $x, y \notin \mathfrak{p}_\alpha$, a contradiction. ∎

## 1.2 Localization

**Definition 1.2.1** (Localization)**.**

(a) Let $R$ be a ring. A subset $S \subseteq R$ is called a *multiplicative system* or simply *multiplicative* if finite products of elements of $S$ lie in $S$. (Equivalently, $S$ is multiplicative iff $1 \in S$ and $s, t \in S \Rightarrow st \in S$.)
(b) In the above setting, the *localization* of $R$ with respect to $S$ is a ring $S^{-1}R$ with a homomorphism (called the *localization homomorphism*) $\eta : R \to S^{-1}R$ such that $\eta(S) \subseteq (S^{-1}R)^*$ and that $S^{-1}R$ is initial with respect to this property.
(c) In the above setting, if $M$ is an $R$-module, then the *localization* of $M$ with respect to $S$ is an $S^{-1}R$-module $S^{-1}M$ with an $R$-module homomorphism $\eta : M \to S^{-1}M$ such that any $R$-module homomorphism from $M$ to an $S^{-1}R$-module factors through $\eta$.

If the localization exists, then it is unique up to unique isomorphism commuting with the $\eta$'s. We give two explicit constructions: one is to take simply $S^{-1}R := R[\{x_s\}]_{s\in S}/(sx_s - 1)$. Another construction of $S^{-1}R$ is given by taking classes $s^{-1}x$ with $s^{-1}x = t^{-1}y$ iff there is a $u \in S$ such that $u(sy - tx) = 0$, defining addition and multiplication in the usual way, and $\eta : x \mapsto 1^{-1}x$. Similarly, $S^{-1}M$ is can be constructed explicitly by taking classes $s^{-1}m$. The universal property amounts to saying that the additive functor $S^{-1} : R\text{-}\mathsf{Mod} \to S^{-1}R\text{-}\mathsf{Mod}$ is left-adjoint to the forgetful functor $\eta_* : S^{-1}R\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$. Of course, the localization of modules can be obtained only from localization of rings: there is a natural isomorphism $S^{-1}R \otimes_R M \to S^{-1}M$ of $R$-modules and $S^{-1}R$-modules for any $R, S, M$ as above.

**Lemma 1.2.2.** Let $S \subseteq R$ be a multiplicative subset in a ring $R$ and $M$ be an $R$-module. Then

(a) The localization map $\eta : M \to S^{-1}M$ has kernel $\ker\eta := \{m \in M : um = 0 \text{ for some } u \in S\}$.
(b) The ring $S^{-1}R$ is degenerate iff $0 \in S$.
(c) The map $\eta : R \to S^{-1}R$ is injective iff $S$ contains no zero divisors.

*Proof.* For (a), we have $1^{-1}0 = 1^{-1}m$ iff there is a $u \in S$ such that $um = 0$. For (b), $S^{-1}R$ is degenerate iff $1 \in \ker\eta$ iff $0 \in S$. For (c), $\ker\eta = 0$ iff $ux = 0$ for $u \in S, x \in S$ implies $x = 0$, which is equivalent to $S$ containing no zero divisors. ∎

**Example 1.2.3.**

(a) If $S \subseteq T \subseteq R$ are both multiplicative, then the universal property gives us homomorphisms $S^{-1}R \to T^{-1}R$ and $S^{-1}M \to T^{-1}M$ for any module $M$. The kernel of $S^{-1}R \to T^{-1}R$ is given by $\{s^{-1}r \in S^{-1}R : ur = 0 \text{ for some } u \in T\}$.
(b) Given any ring $R$ and element $x \in R$, the system $S = \{1, x, x^2, \dots\}$ is multiplicative. The localization $S^{-1}R \cong R[x]/(xy - 1)$ is denoted by $R[x^{-1}]$. By the Lemma 1.2.2(b), this is zero iff $x$ is nilpotent.
(c) Given a ring $R$, the set $R \setminus \mathcal{Z}(R) \subset R$ of nonzerodivisors of $R$ (i.e. $R \setminus \mathcal{Z}(R) = \{s \in R : x \in R, xs = 0 \Rightarrow x = 0\}$) is a multiplicative subset. The localization $(R \setminus \mathcal{Z}(R))^{-1}R =: \operatorname{Quot} R$ is called the *total quotient ring* of $R$. By Lemma 1.2.2, the map $\eta : R \to \operatorname{Quot} R$ is injective. This is the largest localization of $R$ for which the localization map is injective: indeed, if $S$ is another subset such that $\eta : R \to S^{-1}R$ is injective, then $S \subseteq R \setminus \mathcal{Z}(R)$ and so by (a), $S^{-1}R$ embeds into $\operatorname{Quot} R$. The total quotient ring of $R$ satisfies the following universal property: if $\varphi : R \to S$ is a ring homomorphism such that $\varphi(R \setminus \mathcal{Z}(R)) \subseteq S \setminus \mathcal{Z}(S)$ (i.e. a nonzerodivisor in $R$ remains a nonzerodivisor in $S$), then $\varphi$ extends to a homomorphism $\operatorname{Quot} R \to \operatorname{Quot} S$.
(d) Let $R$ be a ring and $\mathfrak{p} \subseteq R$ an ideal. Then $\mathfrak{p}$ is prime iff $S := R \setminus \mathfrak{p}$ is multiplicative, in which case the localization $(R \setminus \mathfrak{p})^{-1}R =: R_{\mathfrak{p}}$ is called the *localization* of $R$ at $\mathfrak{p}$. Similarly, in this case, given an $R$-module $M$, we define the localization $M_{\mathfrak{p}}$ at a prime $\mathfrak{p}$.
(e) When $R$ is a domain, the construction in (c) is a special case of (d): a ring $R$ is a domain iff the ideal $(0)$ is prime iff $\mathcal{Z}(R) = (0)$, in which case the localization $R_{(0)} = \operatorname{Quot} R = \operatorname{Frac} R$ is called the *field of fractions* or *fraction field* of $R$. Again, the map $\eta : R \to \operatorname{Frac} R$ is injective. The field of fractions of an integral domain is universal with respect to injective homomorphisms out of it to fields; in other words, the functor from the category of integral domains and injective homomorphisms to the category of fields and field homomorphisms given by taking an integral domain to its fraction field is left adjoint to the forgetful functor. By (a), if $R$ is an integral domain, then all localizations of $R$ can be embedded in $\operatorname{Frac} R$ and are integral domains themselves.
(f) It is easy to see that if $R$ and $S$ are rings, then $\operatorname{Quot}(R \times S) \cong \operatorname{Quot}(R) \times \operatorname{Quot}(S)$. For instance, a nontrivial example of a total quotient ring is given by $\operatorname{Quot}(\mathbf{Z} \times \mathbf{Z}) \cong \mathbf{Q} \times \mathbf{Q}$.

**Lemma 1.2.4.** Let $R$ be a ring and $M$ be an $R$-module. Then TFAE:

(a) $M = 0$,
(b) $M_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$, and
(c) $M_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$.

*Proof.* The implications (a) $\Rightarrow$ (b) $\Rightarrow$ (c) are clear. For (c) $\Rightarrow$ (a), for any $0 \neq m \in M$, the annihilator $\operatorname{Ann}_R(m) = (0 :_R m) \subset R$ is proper, so there is a maximal $\mathfrak{m} \subset R$ such that $\operatorname{Ann}_R(m) \subseteq \mathfrak{m}$, so $1^{-1}m \neq 0 \in M_{\mathfrak{m}}$ by Lemma 1.2.2(a). ∎

**Theorem 1.2.5** (Localization Is Exact)**.** If $\mathscr{C}$ is a complex of $R$-modules, then $S^{-1}H\mathscr{C} \xrightarrow{\sim} H(S^{-1}\mathscr{C})$.

*Proof.* The existence of a map $S^{-1}H\mathscr{C} \to H(S^{-1}\mathscr{C})$ is clear by functoriality; it's given by $s^{-1}[n] \mapsto [s^{-1}n]$. For injectivity, note that if $[s^{-1}n] = 0$, then there is a $t^{-1}m$ such that $s^{-1}n = \partial(t^{-1}m) = t^{-1}\partial m$. Then there is a $u \in S$

such that $u(s\partial m - tn) = 0$ so that $utn = \partial(usm)$ and hence $s^{-1}[n] = (uts)^{-1}ut[n] = (uts)^{-1}[utn] = (uts)^{-1}[\partial(usm)] = (uts)^{-1}0 = 0$. For surjectivity, note that a class $[s^{-1}n]$ is given an element $s^{-1}n$ with $\partial(s^{-1}n) = s^{-1}\partial n = 0$, so there is a $u \in S$ such that $0 = u\partial n = \partial(un)$. Then $(us)^{-1}[un] \mapsto [s^{-1}n]$. ∎

**Corollary 1.2.6.** Let $R$ be a ring, $M, N, P$ modules over it, and $\varphi : M \to N$ and $\psi : N \to P$ homomorphisms.

(i) TFAE:
  (a) $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ is exact.
  (b) $M_\mathfrak{p} \xrightarrow{\varphi_\mathfrak{p}} N_\mathfrak{p} \xrightarrow{\psi_\mathfrak{p}} P_\mathfrak{p}$ is exact for all $\mathfrak{p}$.
  (c) $M_\mathfrak{m} \xrightarrow{\varphi_\mathfrak{m}} N_\mathfrak{m} \xrightarrow{\psi_\mathfrak{m}} P_\mathfrak{m}$ is exact for all $\mathfrak{m}$.

(ii) TFAE:
  (a) $\varphi : M \to N$ is injective (resp. surjective).
  (b) $\varphi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective (resp. surjective) for all $\mathfrak{p}$.
  (c) $\varphi_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ is injective (resp. surjective) for all $\mathfrak{m}$.

*Proof.* Part (i) follows from Lemma 1.2.4 and Theorem 1.2.5. Part (ii) follows by applying (i) and choosing one of the $M$ and $P$ to be zero. ∎

Finally, we relate submodules of the localization to submodules of the original module.

**Observation 1.2.7** (Submodules of Localization)**.** Let $R$ be a ring, $S \subseteq R$ multiplicative, $M$ an $R$-module, and $\eta : M \to S^{-1}M$ the localization.

(a) If $N \subseteq M$ is a submodule, then so is $S^{-1}N \subseteq S^{-1}M$ (by Theorem 1.2.5); if $N$ is f.g. over $R$, then so is $S^{-1}N$ over $S^{-1}R$ (by the images under $\eta$ of the generators).
(b) Conversely, if $L \subseteq S^{-1}M$ is a submodule, then so is $\eta^{-1}L \subseteq M$. These constructions satisfy $N \subseteq \eta^{-1}(S^{-1}N)$ and $L = S^{-1}(\eta^{-1}L)$ (surjectivity follows from $s^{-1}\ell \in L \Rightarrow \ell \in L$). (In general, equality need not hold in the first; for instance, if $S = R$.)
(c) Every $S^{-1}R$-submodule of $S^{-1}M$ is of the form $S^{-1}N$ for some $R$-submodule $N \subseteq M$. In particular, if $M$ is Noetherian as an $R$-module, then so is $S^{-1}M$ as an $S^{-1}R$-module.
(d) In particular, if $R$ is a Noetherian (resp. Artinian) ring, then every localization $S^{-1}R$ is also Noetherian (resp. Artinian), because every $S^{-1}R$-module $M$ is of the form $S^{-1}M'$ for some $R$-module $M'$, namely $M' = M$ itself.

Reinterpreting the above in the language of ideals gives us:

**Corollary 1.2.8** (Ideals in Localization)**.** Let $R$ be a ring and $S \subseteq R$ multiplicative and $\eta : R \to S^{-1}R$ the localization.

(a) If $\mathfrak{a} \subseteq R$ is an ideal, then so is $S^{-1}\mathfrak{a} \subseteq S^{-1}R$; if $\mathfrak{a}$ is f.g. then so is $S^{-1}\mathfrak{a}$. Further, $S^{-1}\mathfrak{a}$ is proper iff $\mathfrak{a} \cap S = \emptyset$.
(b) Conversely, if $\mathfrak{b} \subseteq S^{-1}R$ is an ideal, then so is $\eta^{-1}\mathfrak{b} \subseteq R$. These constructions satisfy $\mathfrak{a} \subseteq \eta^{-1}(S^{-1}\mathfrak{a})$ and $\mathfrak{b} = S^{-1}(\eta^{-1}\mathfrak{b})$.
(c) If $\mathfrak{q} \subset R$ is prime with $\mathfrak{q} \cap S = \emptyset$, then in fact $\mathfrak{q} = \eta^{-1}(S^{-1}\mathfrak{q})$ and $S^{-1}\mathfrak{q}$ is prime in $S^{-1}R$.
(d) The maps $\mathfrak{q} \mapsto S^{-1}\mathfrak{q}$ and $\mathfrak{Q} \mapsto \eta^{-1}\mathfrak{Q}$ give inverse bijective correspondences between primes $\mathfrak{q} \subseteq R$ disjoint form $S$ and primes $\mathfrak{Q} \subseteq S^{-1}R$.
(e) In particular, if $S = R \setminus \mathfrak{p}$ is the complement of a prime, then there is a bijective correspondance between primes $\mathfrak{q} \subset R$ contained in $\mathfrak{p}$ and primes of $R_\mathfrak{p}$. In particular, $R_\mathfrak{p}$ has a unique maximal ideal, namely $\mathfrak{p}R_\mathfrak{p}$, so it is *local* (see Theorem 1.3.3).

We present one neat corollary which will be helpful later.

**Corollary 1.2.9** (Contractions)**.** Let $\varphi : R \to S$ be a ring homomorphism and $\mathfrak{p} \subset R$ be a prime. Then there is a prime $\mathfrak{q} \subset S$ such that $\mathfrak{p} = \varphi^{-1}\mathfrak{q}$ iff $\mathfrak{p} = \varphi^{-1}(\varphi(\mathfrak{p})S)$.

*Proof.* By replacing $R$ by $R/\ker\varphi$, we can assume that $R \subseteq S$; the statement then says that if $\mathfrak{p} \subset R$ is a prime, then there is a prime $\mathfrak{q} \subset S$ lying over $\mathfrak{p}$ (i.e. with $\mathfrak{q} \cap R = \mathfrak{p}$) iff $\mathfrak{p} = (\mathfrak{p}S) \cap R$. If such a $\mathfrak{q}$ exists, then we have $\mathfrak{p} = \mathfrak{q} \cap R \subseteq (\mathfrak{q} \cap R)S \cap R \subseteq \mathfrak{q} \cap R = \mathfrak{p}$. Conversely, suppose that $\mathfrak{p} = (\mathfrak{p}S) \cap R$. Then $\mathfrak{p}S \cap (R \setminus \mathfrak{p}) = \emptyset$, so that by Corollary 1.2.8(a), the ideal $\mathfrak{p}S_\mathfrak{p} \subset S_\mathfrak{p} := (R \setminus \mathfrak{p})^{-1}S$ is proper and so is contained in a maximal $\mathfrak{m} \subset S_\mathfrak{p}$. If $\mathfrak{q} := \eta^{-1}\mathfrak{m}$ where $\eta : S \to S_\mathfrak{p}$ is the localization map, then $\mathfrak{q}$ is prime, disjoint from $R \setminus \mathfrak{p}$ by Corollary 1.2.8(d), and contains $\mathfrak{p}S$. Therefore, $\mathfrak{p} = \mathfrak{p}S \cap R \subseteq \mathfrak{q} \cap R \subseteq \mathfrak{p}$. ∎

## 1.3 Nilradical, Jacobson Radical, Local Rings

**Definition 1.3.1.** Let $R$ be a ring. Define the *nilradical* and *Jacobson radical* of $R$ respectively by

$$\mathrm{Nil}(R) := \bigcap_{\mathfrak{p}} \mathfrak{p} \text{ and } \mathrm{Jac}(R) := \bigcap_{\mathfrak{m}} \mathfrak{m}.$$

A ring $R$ is said to be *reduced* if $\mathrm{Nil}(R) = 0$. The *reduction* of an arbitrary ring $R$ is defined to be $R^{\mathrm{red}} := R/\mathrm{Nil}(R)$; this is a reduced ring.

**Lemma 1.3.2.** Let $R$ be a ring.

(a) If $\mathfrak{a} \subseteq R$ is an ideal, then the radical $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p}$. In particular, $\sqrt{0} = \mathrm{Nil}(R)$.
(b) We have the characterization $\mathrm{Jac}(R) = \{x \in R : \text{ for all } y \in R, 1 + xy \in R^*\}$.

*Proof.* For (a), replacing $R$ by $R/\mathfrak{a}$, it suffices to show that $\sqrt{0} = \mathrm{Nil}(R)$. One direction is clear. For the other, suppose that $x \in R$ is not nilpotent; then $R[x^{-1}]$ is not the zero ring by Example 1.2.3(a), and so has a maximal ideal say $\mathfrak{m}$. Then the preimage $\mathfrak{p} := \eta^{-1}\mathfrak{m} \subset R$, where $\eta : R \to R[x^{-1}]$ is the localization map, is a prime not containing $x$, so $x \notin \bigcap_{\mathfrak{p}} \mathfrak{p}$. For (b), if $x \in \mathrm{Jac}(R)$ and there is a $y \in R$ such that $1 + xy \notin R^*$, then there would be a maximal $\mathfrak{m} \subset R$ such that $1 + xy \in \mathfrak{m}$ and so $x, 1 + xy \in \mathfrak{m} \Rightarrow 1 \in \mathfrak{m}$, a contradiction. Conversely, if this holds but there is a maximal $\mathfrak{m} \subset R$ such that $x \notin \mathfrak{m}$, then $\mathfrak{m} + (x) = (1)$ and so $m + xy = 1$ for some $m \in \mathfrak{m}, y \in R$. Then $m = 1 + x(-y) \in R^* \cap \mathfrak{m}$, a contradiction. ∎

Since every maximal ideal is prime, $\mathrm{Nil}(R) \subseteq \mathrm{Jac}(R)$, but equality need not hold; see Counterexample 1.3.5 below.

**Theorem 1.3.3** (Local Rings)**.** For a nonzero ring $R$, TFAE:

(a) The set of nonunits $R \setminus R^*$ is an ideal.
(b) The ring $R$ has a unique maximal ideal.
(c) For any maximal ideal $\mathfrak{m} \subset R$, any element of $1 + \mathfrak{m}$ is a unit.

*Proof.* For (a) $\Rightarrow$ (b), note that every proper ideal of $R$ must be contained in $R \setminus R^*$, so if this set is an ideal then it is the unique maximal ideal. For (b) $\Rightarrow$ (a), note that this unique maximal ideal must contain every element of $R \setminus R^*$ and must also be contained in $R \setminus R^*$. For (b) $\Rightarrow$ (c), if $R$ has a unique maximal ideal $\mathfrak{m}$, then $\mathfrak{m} = \mathrm{Jac}(R)$ and so the result follows from Lemma 1.3.2(b). For (c) $\Rightarrow$ (b), let $\mathfrak{m}$ be some maximal ideal in $R$ (this uses that $R$ is nonzero) and $x \in \mathfrak{m}$. By Lemma 1.3.2(b) again, $x \in \mathrm{Jac}(R)$; this shows that $\mathfrak{m} \subseteq \mathrm{Jac}(R) \subseteq \mathfrak{m}$, so that $\mathrm{Jac}(R) = \mathfrak{m}$ is the unique maximal ideal. ∎

**Definition 1.3.4.** A ring $R$ is said to be *local* if it is nonzero and satisfies the equivalent conditions of Theorem 1.3.3. Local rings are usually denoted by the triple $(R, \mathfrak{m}, k)$ where $\mathfrak{m} \subset R$ is the maximal ideal and $k := R/\mathfrak{m}$ is the *residue field*.

Corollary 1.2.8(e) says that if $R$ is any ring and $\mathfrak{p} \subset R$ a prime, then $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}}, \mathrm{Frac}(R/\mathfrak{p}))$ is a local ring.

**Counterexample 1.3.5.** Let $k$ be a field and $R := k[X]_{(X)}$. Being the localization of the integral domain $k[X]$ at the prime $(X)$, this is a local ring with $\mathrm{Jac}(R) = Xk[X]_{(X)}$ as above. On the other hand, it is an integral domain and so $\mathrm{Nil}(R) = 0$.

## 1.4 Factorization Domains and Unique Factorization Domains

**Definition 1.4.1.** A ring $R$ is called a *factorization domain* (FD) if it is a domain and if every nonzero nonunit of $R$ can be factored into irreducibles. A ring $R$ is a *unique factorization domain* (UFD) if the factorization in the first part is unique upto the order of factors and units.

A ring $R$ is a UFD iff it is a FD and every irreducible of $R$ is prime. If a domain $R$ satisfies the a.c.c. for principal ideals, then $R$ is a FD (so every Noetherian domain is a FD); the proof is clear: start with a nonzero nonunit that does not factor into irreducibles; in particular, it is itself not irreducible, and so can be factored into two elements, neither irreducible nor units, and at least one of them does not factor into irreducibles; continue in this fashion to produce a strictly ascending chain of principal ideals.

In any ring $R$, the l.c.m. of two elements $x$ and $y$ is a generator of $(x) \cap (y)$, and the g.c.d. is the generator of a principal ideal containing $(x, y)$ which is minimal w.r.t. this property. We first need a lemma:

**Lemma 1.4.2.** Let $R$ be a domain. If $x, y \in R$ have an l.c.m., then they have a g.c.d.

*Proof.* Suppose $(x) \cap (y) = (\ell)$, so there is a $d$ with $xy = \ell d$. From $\ell \in (x)$ we get $y \in (d)$ and so by symmetry $(x, y) \subseteq (d)$. If $z$ is such that $(x, y) \subseteq (z)$, then $x = zx_1$ and $y = zy_1$ so that $zx_1y_1 \in (x) \cap (y) = (\ell)$. Now $\ell d = xy = z(zx_1y_1)$ then gives $(d) \subseteq (z)$ so we are done. ∎

**Theorem 1.4.3.** Let $R$ be a FD. Then TFAE:

(a) $R$ is a UFD.
(b) Every irreducible in $R$ is prime.
(c) The intersection of an arbitrary collection of principal ideals is principal.
(d) The intersection of two principal ideals is principal.
(e) Any two elements have a l.c.m.
(f) Any two elements have a g.c.d.
(g) Any minimal nonzero prime (i.e. prime of height one) is principal.

*Proof.* The implications (a) ⇔ (b) were noted above/are standard. The implication (a) ⇒ (c) is clear; if $\bigcap_{i\in I}(x_i) \neq 0$, then factorizing each $x_i = u_i \prod_\alpha p_\alpha^{\nu_{\alpha,i}}$ with $u_i \in R^\times$ and $p_\alpha$ distinct primes gives $\bigcap_{i\in I}(x_i) = \left(\prod_\alpha p_\alpha^{\max_i \nu_{\alpha,i}}\right)$. The implications (c) ⇒ (d) ⇒ (e) ⇒ (f) are now clear; we show (f) ⇒ (b), for which if $p$ is irreducible and nonzero $x, y \in R$ such that $p \mid xy$ but $p \nmid x$, then by irreducibility $\gcd(x, p) = 1$, and now $p \mid \gcd(xy, py) = \gcd(x, p)y = y$. For (b) ⇒ (g), let $\mathfrak{p}$ be a minimal nonzero prime, let $0 \neq f \in \mathfrak{p}$; factor $f$ into irreducibles and use the primality of $\mathfrak{p}$ to conclude $\mathfrak{p}$ contains an irreducible, and then use (b) to conclude from minimality that $\mathfrak{p}$ is principal.

The implication (g) ⇒ (b) is harder. Let $p$ be an irreducible, and let $\mathfrak{p}$ be a minimal prime over $(p)$ (by Lemma 1.1.4). By Theorem 7.3.1, $\mathfrak{p}$ has height one, and so by (g) we have $\mathfrak{p} = (q)$ for some $q \in R$. Now $p = qr$ for some $r \in R$, so by irreducibility we must have $r$ a unit, so that $\mathfrak{p} = (p)$. ∎

**Corollary 1.4.4.** Every Noetherian g.c.d. domain (e.g. a PID) is a UFD.

**Corollary 1.4.5.**

(a) If $R$ is a UFD and $S \subseteq R$ a multiplicative system, then so is $S^{-1}R$.
(b) Conversely, if $R$ is a Noetherian domain, $S \subseteq R$ the multiplicative system generated by a set $\Gamma$ of prime elements and $S^{-1}R$ is a UFD, then so is $R$.

*Proof.* The statement in (a) is clear. For (b), we use Theorem 1.4.3(g). Let $\mathfrak{p} \subset R$ be prime of height one. If $\mathfrak{p} \cap S \neq \emptyset$, then $\mathfrak{p}$ contains a $p \in \Gamma$ and then $\mathfrak{p} = (p)$ by minimality. Else $S^{-1}\mathfrak{p}$ is a height one prime of $S^{-1}R$, so $S^{-1}\mathfrak{p} = xS^{-1}R$ for some $x \in \mathfrak{p}$. Look at the collection of ideals $\{(x)\}$ of $R$ that arise thus; since $R$ is Noetherian, this has a maximal element, say generated by $p$. We claim that $\mathfrak{p} = (p)$. By maximality, $p$ is not divisible by any $q \in S$. If $x \in \mathfrak{p}$, then $sx = py$ for some $s \in S$ and $y \in R$. If $s = p_1 \cdots p_r$ with $p_i \in \Gamma$, then $p \notin (p_i)$ implies $y \in (p_i)$ for some $i$; then induction on $r$ shows $y \in (s)$, so that $x \in (p)$. Thus $\mathfrak{p} \subseteq (p)$. ∎

Finally, we have the harder result:

**Corollary 1.4.6.** Let $R$ be a Noetherian ring, and $\mathfrak{m}$ a maximal ideal. If the completion $\hat{R}_\mathfrak{m}$ is a UFD, then so is $R$.

*Proof.* For this, note that by Corollary 1.12.7(b), we have $R \hookrightarrow \hat{R}_\mathfrak{m}$, so in particular $R$ is a domain; further, $\hat{R}_\mathfrak{m}$ is a local ring by Example 1.12.4. By Theorem 1.4.3(b), it suffices to show that every irreducible in $R$ is prime, so let $p \in R$ be an irreducible and nonzero $x, y \in R$ such that $p \mid xy$ but $p \nmid x$. The idea will be to show that $\gcd_{\hat{R}_\mathfrak{m}}(p, x) = 1$ so that $p \mid y$ in $\hat{R}_\mathfrak{m}$, and from this we'll show that $p \mid y$ in $R$. We'll do this in three steps.

Step 1. If $\mathfrak{a} \subseteq R$ is any ideal, then $\mathfrak{a}\hat{R}_\mathfrak{m} \cap R = \mathfrak{a}$. Indeed, $\mathfrak{a}\hat{R}_\mathfrak{m} \cap R \subseteq \bigcap_n(\mathfrak{a} + \mathfrak{m}^n) = \mathfrak{a}$, where in the second step we've used Corollary 1.12.7(b) applied to $R/\mathfrak{a}$.
Step 2. If $u, v \in R$ are such that $u \mid v$ in $\hat{R}_\mathfrak{m}$, then $u \mid v$ in $R$. This follows from $v \in (u)\hat{R}_\mathfrak{m} \cap R = (u)$.
Step 3. If $p \in R$ is irreducible and $x \in R$ such that $p \nmid x$, then $\gcd_{\hat{R}_\mathfrak{m}}(p, x) = 1$.

∎

*Remark* 1. In fact, it suffices to assume that $\mathfrak{m}$ is contained in the Jacobian radical (see Samuel).

## 1.5 Gauß's Lemma and Eisenstein Irreducibility

**Definition 1.5.1.** Let $R$ be a UFD. A polynomial $f \in R[X]$ is called *primitive* if $\alpha \in R$ with $\alpha \mid f$ implies $\alpha \in R^*$ (or equivalently, $\gcd(\{[X^i]f : i \geq 0\}) = 1$).

Note that every $f \in (\operatorname{Frac} R)[X]$ can be written as $f = \operatorname{cont}(f) f_0$ for some $\operatorname{cont}(f) \in \operatorname{Frac} R$ and $f_0 \in R[X]$ primitive; further, $\operatorname{cont}(f)$ and $f_0$ are uniquely determined up to units. This element $\operatorname{cont}(f)$ is called the *content* of $f$, and $f_0$ is called the *primitive part* of $f$. Note that $f \in R[X]$ iff $\operatorname{cont}(f) \in R$, in which case $f$ is primitive iff $(\operatorname{cont}(f)) = (1)$.

**Theorem 1.5.2.** Suppose that $R$ is a UFD and let $K := \operatorname{Frac} R$.

(a) If $f, g \in R[X]$ are primitive, then so is $fg \in R[X]$.
(b) In general, if $f, g \in R[X]$ then $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$ and $(fg)_0 = f_0 g_0$ (upto units).
(c) (Gauß's Lemma) An $f \in R[X]$ can be written as product of nonconstant polynomials in $R[X]$ iff in $K[X]$. Further, these factorizations can be chosen to be $K$-multiples of each other.
(d) If $f \in R[X]$ is primitive, then $f$ is irreducible in $R[X]$ iff it is irreducible in $K[X]$.
(e) If $f, g \in R[X]$ and $f \mid g$ in $K[X]$ with $f$ primitive, then $f \mid g$ in $R[X]$.

*Proof.* For (a), let $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{i=0}^{m} b_i X^i$. If $p \in R$ is any prime, then since $f$ is primitive, there is a maximal $i$, with $0 \leq i \leq n$, such that $p \nmid a_i$. Similarly there is a maximal $j$, with $0 \leq j \leq m$ such that $p \nmid b_j$. In that case, $p \nmid [X^{i+j}](fg)$. For (b), $fg = (\operatorname{cont}(f) f_0)(\operatorname{cont}(g) g_0) = (\operatorname{cont}(f)\operatorname{cont}(g))(f_0 g_0)$, so the result follows from (a). For (c), one direction is clear. For the other direction, assume that $f = gh$ for $g, h \in K[X]$. Then $f_0 = g_0 h_0 \in R[X]$, so that $f = \operatorname{cont}(f) f_0 = (\operatorname{cont}(f) g_0) h_0$, where $\operatorname{cont}(f) g_0$ and $h_0 \in R[X]$ are both nonconstant. For (d), if $f$ is reducible in $K[X]$, then it is irreducible in $R[X]$ by (c). Conversely, primitivity implies that if $f$ is reducible in $R[X]$ then it is a product of nonconstant polynomials in $R[X]$. For (e), write $g = fq$ for some $q \in K[X]$. Then $\operatorname{cont}(q) = \operatorname{cont}(g) \in R$, so that $q \in R[X]$. ∎

**Corollary 1.5.3.** For any ring $R$, the ring $R$ is a UFD iff the polynomial ring $R[\{X_\lambda\}]_{\lambda \in \Lambda}$ is, for any $\Lambda$.

If $R[\{X_\lambda\}]_\lambda$ is a UFD, then $R$ is a domain; further, constant polynomials in $R[\{X_\lambda\}]_\lambda$ factor uniquely into irreducibles in $R[X]$, which are necessarily of degree 0, so that $R$ is a UFD. Conversely, we claim that it suffices to show the result for $\Lambda = \{*\}$, indeed from which the finite $\Lambda$ case follows by induction, and the general case follows from elements of the ring being *finite* combinations. In other words, we have to show that if $R$ is a UFD, then so is $R[X]$.

*Proof 1.* Let $K := \operatorname{Frac} R$. Let $f \in R[X]$ and write $f = \operatorname{cont}(f) f_0$; since $\operatorname{cont}(f)$ can be factored uniquely up to irreducibles in $R$ (and hence $R[X]$), it suffices to show that nonconstant primitive polynomials in $R[X]$ can be factored uniquely into irreducibles, so assume that $f \in R[X]$ is nonconstant primitive. Since $K[X]$ is a UFD, $f$ can be factored uniquely into irreducibles in $K[X]$. By Gauß's Lemma (Theorem 1.5.2(c)), there is a factorization of $f$ in $R[X]$ whose factors are $K$-multiples of factors in $K[X]$. Since $\operatorname{cont}(f) = 1$, the content of each must be 1. Therefore, Theorem 1.5.2(d) shows that these factors are irreducible in $R[X]$; we have shown the existence of factorizations. The uniqueness of factorization follows from that in $K[X]$: if $f = \prod_{i=1}^{r} f_i = \prod_{j=1}^{s} f'_j$ into irreducibles in $R[X]$, then each of the $f_i, f'_j$'s have content 1, and so are irreducible in $K[X]$ by Theorem 1.5.2(d); in particular, they have positive degrees. It follows from unique factorization in $K[X]$ that $r = s$ and after renumbering $f_i$ and $f'_i$ are associates in $K[X]$; and then they are associates in $R[X]$ by Theorem 1.5.2(e). ∎

*Proof 2.* Let $S \subseteq R[X]$ be the multiplicative system generated by the primes of $R$, which are also primes of $R[X]$. The localization $S^{-1}R[X] = K[X]$ is a UFD by Corollary 1.4.4, so we are done by Corollary 1.4.5(b).

∎

**Counterexample 1.5.4.** There are UFD's $R$ such that $R[\![X]\!]$ is not one, e.g. $R = k[X, Y, Z]/(X^2 + Y^3 + Z^7)_{(x,y,z)}$ for a field $k$ (see [TBD]).

**Corollary 1.5.5.** (Spec $R[X]$ for PID $R$.) If $R$ is a PID with $K := \operatorname{Frac} R$ and $\mathfrak{p} \subset R[X]$ is a prime, then $\mathfrak{p}$ is of one of the four following types:

(a) $(0)$.
(b) $(f)$ for some $f \in R[X]$ irreducible.
(c) $(p)$ for some $p \in R$ nonzero prime.

(d) $(p, f)$ for some $p \in R$ nonzero prime and $f \in R[X]$ monic such that $\overline{f} \in (R/p)[X]$ is irreducible. These primes are maximal, since the quotient by each such prime is an algebraic extension of the field $R/p$.

*Proof.* We have two cases: either $\mathfrak{p} \cap R = (0)$ or $\mathfrak{p} \cap R = (p)$ for some nonzero prime $p \in R$.

(a) Suppose $\mathfrak{p} \cap R = (0)$, and look at $(\mathfrak{p}) \subseteq K[X] = (R \setminus \{0\})^{-1}R[X]$. By the assumption, $\mathfrak{p} \cap (R \setminus \{0\}) = \emptyset$, so we have that $(\mathfrak{p}) \subseteq K[X]$ is proper. Since $K[X]$ is a PID, we have either that $(\mathfrak{p}) = (0)$, in which case $\mathfrak{p} = (0)$, or that $(\mathfrak{p}) = (f)$ for some $f \neq 0 \in K[X]$ irreducible. Now write $f = \mathrm{cont}(f)f_0$ for $f_0 \in R[X]$ primitive, so that $(\mathfrak{p}) = (f_0) \subseteq K[X]$. We claim that $\mathfrak{p} = (f_0) \subseteq R[X]$, and that $f_0$ is irreducible. For one direction, observe that $f_0 \in (\mathfrak{p})$, so there is a $0 \neq r \in R$ such that $rf_0 \in \mathfrak{p}$, but $r \notin \mathfrak{p}$ implies $f_0 \in \mathfrak{p}$. For the other direction, if $g \in \mathfrak{p}$, then $g \in (\mathfrak{p}) = (f_0) \in K[X]$, so that $f_0$ divides $g$ in $K[X]$. By Theorem 1.5.2(d) above, this means that $f_0$ divides $g$ in $R[X]$, so that $g \in (f_0) \subseteq R[X]$. This proves $\mathfrak{p} \subseteq (f_0) \subseteq R[X]$. Now $f_0 \neq 0 \in R[X]$ is a nonzero prime in a UFD, and hence irreducible.

(b) Suppose now that $\mathfrak{p} \cap R = (p)$ for some $p \in R$ nonzero prime. Then $R/p$ is a field, and we can look at $\overline{\mathfrak{p}} \subseteq R[X]/(p) \cong (R/p)[X]$, which is a again a PID. Therefore, either $\overline{\mathfrak{p}} = (0)$, in which case $\mathfrak{p} = (p)$, else $\overline{\mathfrak{p}} = (\overline{f})$ for some $\overline{f} \in (R/p)[X]$ irreducible, and WLOG monic. Then lifting back to $R[X]$, we get that $\mathfrak{p} = (p, f)$ for some $f \in R[X]$ monic such that it remains irreducible mod $p$.

■

*Remark* 2. The above proof basically analyzes the fibers of the map $\iota^* : \operatorname{Spec} R[X] \to \operatorname{Spec} R$.

Next, we recall a famous irreducibility criterion.

**Theorem 1.5.6** (Eisenstein Irreducibility)**.** Let $R$ be a ring and let $f = a_0X^n + \cdots + a_n \in R[X]$ be a polynomial for some $n \geq 1$. If there is a prime $\mathfrak{p} \subset R$ such that the following hold:

(a) The coefficient $a_0 \notin \mathfrak{p}$.
(b) For each $j = 1, \ldots, n$, we have $a_j \in \mathfrak{p}$.
(c) We have $a_n \notin \mathfrak{p}^2$.

Then $f$ is irreducible.

*Proof.* Examine the reduction of $f = gh$ in $R/\mathfrak{p}$ and use the following lemma. ■

**Lemma 1.5.7.** Let $R$ be a domain. If for some $n \geq 1$ we have $X^n = gh$ for some $g, h \in R[X]$, then there are $r, s \geq 0$ such that $r + s = n$ and $g = X^r, h = X^s$.

*Proof.* Examine the first nonzero coefficient of $g$ and $h$ and use that $R$ is a domain. ■

Such a polynomial $f$ is said to be *Eisenstein* at the prime $\mathfrak{p}$. Here we give a few example applications.

**Corollary 1.5.8.** Prime-power cyclotomic polynomials are irreducible.

*Proof.* We have for prime $p$ and integer $r \geq 1$ that

$$(X^{p^{r-1}} - 1)\Phi_{p^r}(X) = X^{p^r} - 1 \Rightarrow \Phi_{p^r}(X + 1) \equiv X^{p^{r-1}(p-1)} \pmod{p\mathbf{Z}[X]}$$

using that $(X + Y)^p = X^p + Y^p$ in $\mathbf{F}_p[X, Y]$. Also, $\Phi_{p^r}(1) = p \notin (p^2)$, so we are done by Gauß and Eisenstein. ■

**Corollary 1.5.9.** Complete description of affine plane $\mathbf{A}^2_k = \operatorname{Spec} k[X, Y]$ over algebraically closed $k$: the primes are

(a) the generic point (0) of dimension 2,
(b) the generic points of irreducible curves $(f)$ for $f \in k[X, Y]$ of dimension 1, and
(c) the closed points $(X - a, Y - b)$ of dimension 0.

**Corollary 1.5.10.** An $\alpha \in \overline{\mathbf{Q}}$ is an algebraic integer iff the minimal polynomial $\mu_\alpha \in \mathbf{Q}[X]$ belongs to $\mathbf{Z}[X]$. For instance, if $K = \mathbf{Q}[\sqrt{d}]$ is a quadratic number field for squarefree $d$ other than 1, we have

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \pmod 4, \\ \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{if } d \equiv 1 \pmod 4. \end{cases}.$$

*Proof.* To show the nontrivial direction, let $\mathscr{C} \subset \mathbf{Z}[X]$ be the collection of monic polynomials vanishing at $\alpha$, which is nonempty by hypothesis and hence contains an element $f$ of least degree. It suffices to show that $f$ is irreducible in $\mathbf{Q}[X]$, for which it suffices by Gauß's Lemma to show irreducibility in $\mathbf{Z}[X]$; if $f = gh$ with $g, h \in \mathbf{Z}[X]$ of degrees less than $f$, then WLOG both $g$ and $h$ are monic and then $0 = f(\alpha) = g(\alpha)h(\alpha)$ gives a contradiction. The second part is a standard consequene of the first. ∎

## 1.6 Cayley-Hamilton and Nakayama's Lemma

**Observation 1.6.1** (Cayley-Hamilton Theorem)**.** Let $R$ be a ring, $M$ be a finitely generated $R$-module, $\mathfrak{a} \subseteq R$ an ideal, and $\varphi \in \mathrm{End}_R(M)$ such that $\varphi M \subseteq \mathfrak{a}M$. Suppose $M = \sum_{i=1}^n Rx_i$ and $\varphi(x_i) = \sum_{j=1}^n a_{ij}x_j$ for some $a_{ij} \in \mathfrak{a}$, and let $A := [a_{ij}]$. Then multiplying on the left by the adjoint of the matrix $\varphi I_n - A$ shows that $\det(\varphi I_n - A)x_i = 0$ for all $i$. Therefore, $\varphi$ is a root of $\det(tI_n - A) \in R[t]$ in $\mathrm{End}_R(M)$, and so $\varphi$ satisfies an equation of the form $\varphi^n + a_1\varphi^{n-1} + \cdots + a_n = 0 \in \mathrm{End}_R(M)$ for some some $a_i \in \mathfrak{a}^i$.

**Corollary 1.6.2.** Let $R \subseteq S$ be a ring extension and $M$ a finitely generated $R$-module. Suppose for some $\alpha \in S$ we have that $M$ is also a faithful $R[\alpha]$-module (i.e. with $\mathrm{Ann}_{R[\alpha]} M = 0$), and suppose that $\mathfrak{a} \subseteq R$ is an ideal with $\alpha M \subseteq \mathfrak{a}M$. Then $\alpha \in S$ is the root of a monic polynomial equation of the form $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$, where the $a_i \in \mathfrak{a}^i$ for each $i$.

*Proof.* By the observation, there are $a_i \in \mathfrak{a}^i$ such that $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n \in \mathrm{Ann}_{R[\alpha]} M$. ∎

**Corollary 1.6.3** (Nakayama's Lemma)**.** Let $R$ be a ring.

(a) Let $M$ be a f.g. $R$-module and $\mathfrak{a} \subseteq R$ an ideal with $M = \mathfrak{a}M$. Then for some $a \in \mathfrak{a}$, we have $(1 + a)M = 0$.
(b) Let $M$ be a f.g. $R$-module and $\mathfrak{a} \subseteq \mathrm{Jac}(R)$ an ideal with $M = \mathfrak{a}M$. Then $M = 0$.
(c) Let $M$ be an $R$-module, and $N \subseteq M$ a submodule such that $M/N$ is finitely generated. If for some $\mathfrak{a} \subseteq \mathrm{Jac}(R)$ we have $M = N + \mathfrak{a}M$, then $M = N$.

*Proof.* For (a), apply the above to $\varphi = 1$. For (b), apply (a) with Lemma 1.3.2(b). For (c), apply (b) to $M/N$. ∎

**Corollary 1.6.4.** Let $(R, \mathfrak{m}, k)$ be a local ring and $M$ a finitely generated $R$-module. Then:

(a) $M/\mathfrak{m}M$ is a finite-dimensional $k$ vector space.
(b) Given $x_1, \ldots, x_n \in M$, the set $\{x_1, \ldots, x_n\}$ generates $M$ over $R$ iff $\{\overline{x}_1, \ldots, \overline{x}_n\}$ spans $M/\mathfrak{m}M$ over $k$.
(c) In the situation of (b), the former is a minimal set of generators iff the latter is a $k$-basis of $M/\mathfrak{m}M$.
(d) Any two minimal sets of generators for $M$ over $R$ have the same cardinality, namely $\dim_k(M/\mathfrak{m}M)$.
(e) In particular, if $\mathfrak{m} \neq 0$ is f.g., then $\mathfrak{m}$ is principal iff $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

*Proof.* The statement in (a) is clear. For (b), iff $x_1, \ldots, x_n \in M$ generate $M$ over $R$, then the images certainly span $M/\mathfrak{m}M$ over $k$. Conversely, suppose $x_1, \ldots, x_n \in M$ are such that $\{\overline{x}_1, \ldots, \overline{x}_n\}$ is a $k$-basis for $M/\mathfrak{m}M$. Let $N := \sum_{i=1}^n Rx_i \subseteq M$; by Corollary 1.6.3(c), we conclude that $M = N$, so $M$ is generated by the $x_i$. To show (c), if $\{x_1, \ldots, x_n\}$ is not a minimal set of generators, then some proper subset of it generates $M$ and hence also the images of these span $M/\mathfrak{m}M$. Similarly, if there is a proper subset of $\{x_1, \ldots, x_n\}$ whose images form a basis of $M/\mathfrak{m}M$, then applying the previous implication would show that this proper subset would be a set of generators for $M$. Then (d) follows immediately and (e) follows from taking $M = \mathfrak{m}$. ∎

**Corollary 1.6.5** (Miscellaneous Consequences)**.** Let $R$ be a ring and $M, N$ be a finitely generated $R$-modules.

(a) Every surjective endomorphism of $M$ is an isomorphism.
(b) If $M \otimes_R N = 0$, if $R$ is local then $M = 0$ or $N = 0$. In any case, this implies $\mathrm{Ann}_R(M) + \mathrm{Ann}_R(N) = R$.

*Proof.* For (a), let $\varphi$ be the surjective endomorphism. Define an $R[X]$-module structure on $M$ by $X$ acting as $\varphi$. Since $\varphi$ is surjective, if $\mathfrak{a} = (X) \subseteq R[X]$, then $M = \mathfrak{a}M$. By Nakayama's Lemma (Corollary 1.6.3(a)), there is an $a \in \mathfrak{a}$ such that $(1 + a)M = 0$. To show that $\varphi$ is injective, take an $m \in M$ such that $\varphi(m) = 0$; then $0 = (1 + a)m = m + a(\varphi)(m) = m$, where $a(\varphi)(m) = 0$ by $a \in (X)$ and $\varphi(m) = 0$. For (b), first suppose that $R$ is local and $M \neq 0$ but $M \otimes_R N = 0$. Then $M/\mathfrak{m}M \neq 0$ is nonzero by Nakayama's Lemma and so admits a surjection $M/\mathfrak{m}M \twoheadrightarrow k$. By right-exactness of the tensor product, this means that $0 = M \otimes_R N$ surjects onto $k \otimes_R N \cong N/\mathfrak{m}N$, and so again by Nakayama $N = 0$. Next assume that $R$ is arbitrary and that $\mathrm{Ann}_R(M) + \mathrm{Ann}_R(N) \subsetneq R$, and pick a prime $\mathfrak{p}$ containing $\mathrm{Ann}_R(M) + \mathrm{Ann}_R(N)$. Then $0 = (M \otimes_R N) \otimes_R R_\mathfrak{p} \cong M_\mathfrak{p} \otimes_{R_\mathfrak{p}} N_\mathfrak{p}$ implies by the preceding that either $M_\mathfrak{p} = 0$ or $N_\mathfrak{p} = 0$. If say $M_\mathfrak{p} = 0$, then for each of the finitely many generators $x_i$ of $M$, there is an element $u_i \in R \setminus \mathfrak{p}$ with $u_i x_i = 0$. Then $u = \prod_i u_i \in \mathrm{Ann}_R(M) \setminus \mathfrak{p}$, a contradiction. ∎

**Counterexample 1.6.6.** Corollary 1.6.5(a) is not true if we replace "surjective" by "injective,", e.g. by $\mathbf{Z} \xrightarrow{2} \mathbf{Z}$.

## 1.7 Length and the Jordan-Hölder Theorem

**Definition 1.7.1.** Let $R$ be a ring and $M$ be an $R$-module.

(a) We say that $M$ is *simple* if it is has no nontrivial proper submodules.
(b) A finite chain of submodules $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ is called a *composition series* of length $n \geq 1$ if each successive quotient $M_i/M_{i+1}$ is simple. The successive quotients $M_i/M_{i+1}$ are called the *composition factors* of the series.
(c) The *length* $\ell_R(M) \in \mathbf{N} \cup \{\infty\}$ is the infimum of the lengths of all composition series of $M$.

Note that every nontrivial simple module is isomorphic to a field quotient of $R$. A module has length 0 iff it is trivial, 1 iff it is simple, and has finite length iff it admits a finite composition series (e.g. $\ell_{\mathbf{Z}}(\mathbf{Z}) = \infty$). Length generalizes the notion of dimension: if $R = k$ is a field, then $\ell_k(M) = \dim_k M$.

We'll make use of the following lemma:

**Lemma 1.7.2.** Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ be a composition series of an $R$-module $M$, and let $N \subseteq M$ be a submodule. We have:

(a) Intersection with $N$ gives a sequence of submodules of $N$ as

$$N = M_0 \cap N \supseteq M_1 \cap N \supseteq \cdots \supseteq M_n \cap N = 0.$$

This sequence becomes a composition series for $N$ after eliminating repetitions.
(b) Taking quotients by $N$ gives s a sequence of submodules of $M/N$ as

$$M/N = M_0/N \supseteq (M_1 + N)/N \supseteq \cdots \supseteq (M_n + N)/N = 0.$$

This sequence becomes a composition series for $M/N$ after eliminating repetitions.

*Proof.* The map $M_i \cap N \hookrightarrow M_i \twoheadrightarrow M_i/M_{i+1}$ has kernel $M_{i+1} \cap N$ giving us $(M_i \cap N)/(M_{i+1} \cap N) \hookrightarrow M_i/M_{i+1}$, so by simplicity each successive quotient is either trivial or simple. Similarly, the composite map $M_i \hookrightarrow M_i + N \twoheadrightarrow (M_i+N)/(M_{i+1}+N) \cong ((M_i+N)/N)/((M_{i+1}+N)/N)$ is surjective and its kernel contains $M_{i+1}$, giving us a surjective map $M_i/M_{i+1} \twoheadrightarrow ((M_i + N)/N)/((M_{i+1} + N)/N)$, so by simplicity each quotient is either trivial or simple. ∎

We have:

**Theorem 1.7.3** (Jordan-Hölder)**.** Let $R$ be a ring and $M$ an $R$-module.

(a) If $\ell_R(M) < \infty$, then the lengths and the sets of factors of any two composition series of $M$ are the same. These factors are then called the *simple factors* of $M$.
(b) If $0 \to M' \to M \to M'' \to 0$ is an SES, then $\ell_R(M) = \ell_R(M') + \ell_R(M'')$. If $\ell_R(M) < \infty$, then the set of simple factors of $M$ is the union of the sets of simple factors of $M'$ and $M''$.
(c) More generally, if $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ is an exact sequence of $R$-modules of finite length, then $\sum_k (-1)^k \ell_R(M_k) = 0$.
(d) If $\ell_R(M) < \infty$, then every proper chain of submodules of $M$ has length at most $\ell_R(M)$ and can be refined to a composition series.

*Proof.* For (a), we induct on $n := \ell_R(M)$. If $n = 0$, then $M = 0$ and the result is trivial; hence assume $n > 0$. let $M = M_0 \supsetneq \cdots \supsetneq M_n = 0$ be a composition series of length $n$, and let $M = M'_0 \supsetneq \cdots \supsetneq M'_m = 0$ be another, for some $m \geq 0$. We have to show that $m = n$ and that the composition factors in both are the same. If $m = 0$, then $M = 0$ and $n = 0$, a contradiction; therefore, $m \geq 1$. If $M_1 = M'_1$, then we are done since $\ell_R(M_1) \leq n - 1$; therefore, assume that $M_1 \neq M'_1$. Since both $M/M_1$ and $M/M'_1$ are simple, we must have $M_1 + M'_1 = M$, and let $N := M_1 \cap M'_1$. By the previous lemma, the distinct submodules $M_i \cap N$ determine a composition series $N = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = 0$. By the second isomorphism theorem, we have

$$\frac{M_1}{N} = \frac{M_1}{M_1 \cap M'_1} \cong \frac{M_1 + M'_1}{M'_1} = \frac{M}{M'_1} \text{ and similarly } \frac{M'_1}{N} = \frac{M}{M_1}.$$

Therefore, we get two new composition series for $M$ that look like

$$M \supsetneq M_1 \supsetneq N \supseteq N_1 \supsetneq \cdots \supsetneq N_r = 0 \text{ and } M \supsetneq M_1' \supsetneq N \supseteq N_1 \supsetneq \cdots \supsetneq N_r = 0$$

that differ only at the first step; these trivially have the same length and same quotients. Now we claim that the first has the same length and the same quotients as our original series; indeed, starting at $M_1$ gives a composition series for $M_1$, and so by induction it has the same length $r = n-2$ and composition factors as given by starting the original series at $M_1$, and we are done.

For (b), we first show that the LHS is finite iff the RHS is. If $M'$ and $M'' = M/M'$ have a finite composition series, then juxtaposing them gives a finite composition series for $M$; conversely, if $M$ has a finite composition series, then so do $M'$ and $M''$ by the previous lemma. Finally, the rest of (b) follows from the juxtaposition mentioned above. The claim in (c) follows from (b) by an easy induction. For (d), the second claim is clear since every subquotient of $M$ has finite length; then the first follows from (a) and juxtaposition as before. ∎

**Example 1.7.4.** If $(R, \mathfrak{m}, k)$ is a Noetherian local ring and $n \geq 1$, then all the $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ for $1 \leq i \leq n$ are inductively finite-dimensional $k$-vector spaces, so that $\ell_R(R/\mathfrak{m}^n) = \sum_{i=1}^n \ell_k(\mathfrak{m}^{i-1}/\mathfrak{m}^i)$.

## 1.8 Noetherian and Artinian Rings and Modules

**Definition 1.8.1.**

i. An $R$-module $M$ is *Noetherian* if it satisfies any of the following equivalent properties:
   (a) The a.c.c. on submodules: every increasing sequence $0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ of submodules of $M$ eventually stabilizes.
   (b) Every nonempty collection of submodules of $M$ contains a maximal element.
   (c) Every submodule of $M$ is finitely generated.

   A ring $R$ is *Noetherian* if it is Noetherian as a module over itself.

ii. An $R$-module $M$ is *Artinian* if it satisfies any one of the following equivalent properties:
   (a) The d.c.c. on submodules.
   (b) Every nonempty collection of submodules contains a minimal element.

   A ring $R$ is *Artinian* if it is Artinian as a module over itself.

**Example 1.8.2.** Finite rings, finite products of fields, and $k[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^m$ for every $n, m \geq 1$ are both Noetherian and Artinian. The rings $\mathbf{Z}$, $\mathcal{O}_K$ and polynomial rings $k[X_1, \ldots, X_n]$ are Noetherian but not Artinian. If $R = k$ is a field, then a module $M$ is Artinian iff it is Noetherian iff it has finite dimension.

**Example 1.8.3.** For modules, the a.c.c. and d.c.c. are independent conditions: the $\mathbf{Z}$-module $\mathbf{Z}$ is Noetherian but not Artinian; for any prime $p$, the $\mathbf{Z}$-module $\mathbf{Z}[1/p^\infty]/\mathbf{Z}$ is Artinian but not Noetherian, since all its proper nonzero submodules are of the form $\mathbf{Z}[1/p^n]/\mathbf{Z}$ for some $n \geq 1$. This is not the case for rings; see Theorem 1.8.7 below.

**Theorem 1.8.4.** Let $R$ be a ring and $M$ an $R$-module.

(a) Let $M' \subseteq M$ be a submodule. If $N \subseteq N' \subseteq M$ are submodules such that both $N \cap M' = N' \cap M'$ and $(N + M')/M' = (N' + M')/M'$, then $N = N'$.
(b) If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of $R$-modules, then $M$ is Noetherian (resp. Artinian) iff $M'$ and $M''$ are. In particular, $M^{\oplus n}$ is Noetherian (resp. Artinian) for every $n \geq 1$ iff $M$ is.
(c) If $R$ is Noetherian (resp. Artinian), then each $R^{\oplus n}$ for $n \geq 1$ is. In particular, if $R$ is Noetherian (resp. Artinian) and $M$ a finitely generated $R$-module, then $M$ is Noetherian (resp. Artinian).
(d) If $M$ is a Noetherian (resp. f.g. Artinian) $R$-module, then $R/\operatorname{Ann}(M)$ is a Noetherian (resp. Artinian) ring. In particular, every ring admitting a faithful Noetherian module is Noetherian.

*Proof.* The statements in (a), (b) and (c) are clear. For (d), the submodules of $M$ as an $R$-module and $R/\operatorname{Ann} M$-module coincide, so WLOG $\operatorname{Ann} M = 0$. If $M$ is generated by $x_1, \ldots, x_n$, then the map $R \to M^n$ given by $[r] \mapsto (rx_1, \ldots, rx_n)$ is injective; now apply (b). ∎

**Theorem 1.8.5.** Here are some standard results on (identifying) Noetherian rings:

(a) (Generalized Hilbert Basis Theorem) If $R$ is Noetherian, then so are $R[X]$ and $R[\![X]\!]$.
(b) (Cohen's Theorem) The ring $R$ is Noetherian iff all the primes in $R$ are finitely generated.

(c) (Formanek's Theorem) Let $M$ be a f.g. faithful $R$-module. If the set of submodules of $M$ of the form $\mathfrak{a}M$ for ideals $\mathfrak{a} \subseteq R$ satisfies the a.c.c., then $R$ is Noetherian.
(d) (Eakin-Nagata Theorem) Let $R \subseteq S$ be a ring extension. If $S$ is Noetherian and a f.g. $R$-module, then $R$ is Noetherian.

*Proof.* See Matsumura §3; we note only that (d) follows from (c) by taking $M = S$. ∎

**Theorem 1.8.6.** Suppose $R$ is an Artinian ring.

(a) If $R$ is a domain, then $R$ is a field.
(b) Every prime of $R$ is maximal (i.e. $\dim R = 0$). In particular, $\mathrm{Jac}(R) = \mathrm{Nil}(R)$.
(c) The radical $\mathrm{Nil}(R)$ is nilpotent.
(d) If $\mathfrak{m} \subseteq R$ is maximal, then for every $k \geq 1$, the quotient $R/\mathfrak{m}^k$ is an Artinian local ring.
(e) The ring $R$ has only finitely many maximal ideals, i.e. it is semilocal.
(f) The reduction $R^{\mathrm{red}} := R/\mathrm{Nil}(R)$ is a finite product of fields. In particular, a reduced Artinian ring is a finite product of fields.
(g) The ring $R$ is a finite direct product of Artinian local rings.
(h) If $M$ is an Artinian $R$-module, then $M$ is finitely generated.
(i) In particular, $R$ is a Noetherian ring.

*Proof.*

(a) For any nonzero $a \in R$, apply the d.c.c. to $(a) \supseteq (a^2) \supseteq \cdots$.
(b) If $\mathfrak{p}$ is a prime, then $R/\mathfrak{p}$ is an Artinian domain.
(c) Let $\mathfrak{n} = \mathrm{Nil}(R)$. We have a decreasing chain of ideals $\mathfrak{n} \supseteq \mathfrak{n}^2 \supseteq \cdots$, so by the d.c.c. there exists $k \geq 1$ such that $\mathfrak{n}^k = \mathfrak{n}^{k+1} = \cdots$. If $\mathfrak{n}^k \neq 0$, then consider the family of ideals $\mathcal{A} = \{I \subseteq R : I\mathfrak{n}^k \neq 0\}$; this is nonempty since $\mathfrak{n} \in \mathcal{A}$, so it contains a minimal element, say $I_0$. Now $I_0\mathfrak{n}^k \neq 0$, so $\exists\, r \in I_0 : r\mathfrak{n}^k \neq 0$; then by minimality $I_0 = (r)$. But now $r\mathfrak{n} \subseteq (r)$ is such that $r\mathfrak{n} \cdot \mathfrak{n}^k = r\mathfrak{n}^k \neq 0$, so that by minimality $r\mathfrak{n} = (r)$. Therefore, $r = rs$ for some $s \in \mathfrak{n}$; then $r = rs^n$ for all $n \geq 1$. But $s \in \mathfrak{n} = \mathrm{Nil}(R)$ implies that there is some $n \geq 1$ such that $s^n = 0$; this means $r = 0$, contrary to hypothesis. Therefore, $\mathfrak{n}^k = 0$.
(d) If $\overline{I} \subseteq R/\mathfrak{m}^k$ is any ideal, then the lift $I$ satisfies $\mathfrak{m}^k \subseteq I \subseteq R$. If $\overline{I}$ is prime, then so is $I =: \mathfrak{p}$; then $\mathfrak{p} \supseteq \mathfrak{m}^k \Rightarrow \mathfrak{p} \supseteq \mathfrak{m}$, so by maximality $\mathfrak{p} = \mathfrak{m}$ and hence $I = \overline{\mathfrak{m}}$.
(e) Suppose $\mathcal{A}$ is the family of all finite intersections of maximal ideals in $R$; then this family has a minimal element $\bigcap_{i=1}^n \mathfrak{m}_i$. Then $\mathrm{mSpec}\, R = \{\mathfrak{m}_i\}_{i=1}^n$.
(f) Say $\mathrm{mSpec}\, R = \{\mathfrak{m}_i\}_{i=1}^n$; then $R^{\mathrm{red}} = R/\operatorname{Jac} R \cong \prod_{i=1}^n (R/\mathfrak{m}_i)$ by the Chinese Remainder Theorem.
(g) Say $\mathrm{mSpec}\, R = \{\mathfrak{m}_i\}_{i=1}^n$. Now $\mathrm{Jac}(R) = \mathrm{Nil}(R)$ is nilpotent, so there is a $k \geq 1$ such that $\mathrm{Jac}(R)^k = 0$. Then $0 \subseteq \prod_{i=1}^n \mathfrak{m}_i^k \subseteq (\bigcap_{i=1}^n \mathfrak{m}_i)^k = \mathrm{Jac}(R)^k = 0$, so by the CRT we have that $R = R/0 = R/\prod_{i=1}^n \mathfrak{m}_i^k \cong \prod_{i=1}^n (R/\mathfrak{m}_i^k)$; finish by (d).
(h) If $M$ is not finitely generated, then the family $\mathcal{A}$ of submodules of $M$ that are not finitely generated is nonempty, so we may choose a minimal element $M_0$; replacing $M$ by $M_0$ we can assume that every proper submodule of $M$ is finitely generated. We claim that $\mathfrak{p} = \mathrm{Ann}(M)$ is a prime of $R$: pick $a, b \in R$ such that $ab \in \mathfrak{p}$ but $a \notin \mathfrak{p}$. Then $(0 :_M a) \subsetneq M$, so it is finitely generated. From the SES $0 \to (0 :_M a) \to M \to aM \to 0$ we see that $aM$ is not finitely generated, so that $aM = M$. Then $0 = b(aM) = bM$ implies $b \in \mathfrak{p}$. But now $R/\mathfrak{p}$ is a field, and $M$ is an Artinian $R/\mathfrak{p}$ module that is not finitely generated–a contradiction.
(i) Since $R$ is an Artinian $R$-module, every ideal is also an Artinian $R$-module by Theorem 1.8.4(b); then it is finitely generated by (h).

∎

Said another way, we have:

**Theorem 1.8.7.** Let $R$ be any ring.

(a) For any $R$-module $M$, the length $\ell_R(M) < \infty$ iff $M$ is both Noetherian and Artinian.
(b) (Akizuki-Hopkins) The ring $R$ is Artinian iff $\ell_R(R) < \infty$. In particular, Artinian implies Noetherian.

*Proof.*

(a) If $\ell_R(M) < \infty$, then $\forall\, 0 \subseteq N_1 \subsetneq N_2 \subseteq M$ we have that $0 \leq \ell_R(N_1) < \ell_R(N_2) \leq \ell_R(M)$, so that $M$ satisfies both the a.c.c. and the d.c.c. Conversely, pick $M_1$ to be a minimal nonzero submodule, $M_2$ to be a minimal submodule properly containing $M_1$, and so on to get a series $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots$; this series must stabilize, and must stabilize to $M$, so that we get a finite composition series for $M$.

(b) The "if" is clear by (a). If $R$ is Artinian, then by (the proof of) Theorem 1.8.6, there are maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_N \subseteq R$, not necessarily distinct, such that $\prod_{i=1}^N \mathfrak{m}_i = 0$. Consider the chain $R \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_N = 0$, and consider the subquotients $Q_i := \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i$. Each $Q_i$ is an Artinian $R$-module, and hence an Artinian $R/\mathfrak{m}_i$-module, so that $\dim_{R/\mathfrak{m}_i}(Q_i) = \ell_{R/\mathfrak{m}_i}(Q_i) = \ell_R(Q_i) < \infty$. Then by additivity, we have that $\ell_R(R) = \sum_{i=1}^N \ell_R(Q_i) < \infty$.

■

## 1.9 Krull Dimension

**Definition 1.9.1.** Let $R$ be a ring.

(a) The *Krull dimension* of $R$ is the supremum of the lengths of chains of primes in $R$, i.e.

$$\dim R := \sup\{n : \text{ there are primes } \mathfrak{p}_i \subset R \text{ for } i = 0, \dots, n \text{ such that } \mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_n\}.$$

By convention, $\dim 0 := -1$.

(b) Let $M$ be an $R$-module. Define the *Krull dimension* of $M$ as $\dim M := \dim R/\operatorname{Ann} M$.

Let $\mathfrak{p} \subset R$ be a prime.

(c) The *height* of $\mathfrak{p}$ is the supremum of the lengths of chains contained at $\mathfrak{p}$, i.e. $\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}}$, and the *coheight* of $\mathfrak{p}$ is the supremum of the lenghts of chains containing $\mathfrak{p}$, i.e. $\operatorname{coht} \mathfrak{p} = \dim R/\mathfrak{p}$.

We have, $\dim R = \sup_{\mathfrak{p}}\{\operatorname{ht} \mathfrak{p}\} = \sup_{\mathfrak{p}}\{\operatorname{coht} \mathfrak{p}\}$. Next, $\dim R = 0$ iff all primes of $R$ are incomparable (e.g. if $R$ has only one prime). If $(R, \mathfrak{m}, k)$ is local, then $R = R_{\mathfrak{m}}$, so $\operatorname{ht} \mathfrak{m} = \dim R$. For any $\mathfrak{p}$, we have $\operatorname{ht} \mathfrak{p} + \operatorname{coht} \mathfrak{p} \leq \dim R$, and equality holds for most reasonable rings (e.g. coordinate rings of affine varieties, see Corollary 6.3.2(c)), but not always!

**Example 1.9.2.** A ring $R$ is a field iff it is a zero-dimensional domain. If $R$ is a PID that is not a field, then $\dim R = 1$. If $k$ is a field, then for any $n \geq 1$ we have $\dim k[X_1, \dots, X_n], \dim k[\![X_1, \dots, X_n]\!] \geq n$. If $k$ is a field, then $\dim k[X_1, X_2, \dots] = \infty$.

In fact, it is true that Artinian rings are exactly the zero-dimensional Noetherian rings, and that equalities hold in the above; these facts will be proven below in Corollary 7.1.2, Corollary 6.3.2 and Corollary 7.2.4(c) respectively.

**Counterexample 1.9.3.** Let $S := k[\![X, Y, Z]\!]$, ideal $\mathfrak{a} = (XY, XZ) \subset S$ and $R := S/I$. Then

(a) $\dim R = 2$.
(b) If $\mathfrak{p} = (y, z) \subseteq R$, then $\mathfrak{p}$ is prime with $\operatorname{ht} \mathfrak{p} = 0$ and $\operatorname{coht} \mathfrak{p} = 1$.

In particular, $\operatorname{ht} \mathfrak{p} + \operatorname{coht} \mathfrak{p} = 1 < 2 = \dim R$.

**Counterexample 1.9.4.** Here are some pathologies:

(a) A zero-dimensional non-Noetherian ring: take $R := k[X_1, X_2, \dots]/(X_1, X_2, \dots)^2 = k[\varepsilon_1, \varepsilon_2, \dots]$; this has a unique prime $(\varepsilon_1, \varepsilon_2, \dots)$ and is zero dimensional; on the other hand, $0 \subset (\varepsilon_1) \subset (\varepsilon_1, \varepsilon_2) \subset \cdots$ shows that it is non-Noetherian.
(b) A positive finite dimensional non-Noetherian ring: valuation rings of dimension $\geq 2$ are non-Noetherian by Theorem 5.1.6; the Krull dimension of a valuation ring is the height of its value group (the number of isolated subgroups). A standard example is the valuation ring of the $\mathbf{Z}^2$-valued valuation on $k(x, y)$ with $v(x^n y^m) = (n, m)$.
(c) An infinite dimensional Noetherian ring, due to Nagata. Let $R = k[X_1, X_2, \dots]$ and $m_1, m_2, \dots$ an increasing sequence such that for all $i \geq 1$ we have $m_{i+1} - m_i > m_i - m_{i-1}$. Let $\mathfrak{p}_i := (x_{m_i+1}, \dots, x_{m_{i+1}})$ and let $S := R \setminus \bigcup_i \mathfrak{p}_i$; then $S^{-1}R$ is the required example.

## 1.10 Graded Rings and Modules

**Definition 1.10.1.**

(a) If $I$ is any commutative monoid written additively, then an *$I$-graded* ring $S$ is a ring together with a family of additive subgroups $S_i$ for $i \in I$ such that $S = \bigoplus_{i \in I} S_i$ and such that for all $i, j \in I : S_i S_j \subseteq S_{i+j}$.

(b) If $S$ is a graded ring, then a *graded $S$-module* $M$ is an $S$-module with a family $M_i$ of submodules for $i \in I$ such that $M = \bigoplus_{i\in I} M_i$ and such that for all $i, j \in I : S_i M_j \subseteq M_{i+j}$.
(c) If $S$ is a graded ring and $M$ a graded $S$-module, then an element $m \in M$ is called *homogenous of degree $i$* if $m \in M_i$. In general, every element $m \in M$ can be uniquely decomposed into homogenous components: $m = \sum_{i\in I} m_i$ for $m_i$ homogenous.
(d) A submodule $N$ of a graded $S$-module $M$ is called *homogenous* if it satisfies the following equivalent conditions:
  (a) $N$ is generated by homogenous elements.
  (b) For $m \in M$ we have $m \in N$ iff each homogenous term $m_i \in N$.
  (c) $N = \bigoplus_{i\in I} N \cap M_i$.
  For a homogenous submodule $N \subseteq M$ we set $N_i := N \cap M_i$; then $M/N = \bigoplus_{i\in I} M_i/N_i$ is again a graded $S$-module.

**Example 1.10.2.**

(a) For an $n$-dimensional $k$-vector space $V$, we have that $\operatorname{Sym} V^* = \bigoplus_{d\geq 0} \operatorname{Sym}^d V^*$ is an $\mathbf{N}$-graded ring isomorphic to $k[X_1, \ldots, X_n]$ with its usual polynomial degree grading.
(b) If $R$ is any ring and $I \subseteq R$ an ideal, then:
  (i) The *Rees algebra* or *blowup* of $R$ along $I$ is the algebra $\operatorname{Rees}_R(I) = \operatorname{Bl}_I(R) := \bigoplus_{n\geq 0} I^n$.
  (ii) The *associated graded ring* to $R$ and $I$ is defined to be $\operatorname{gr}_I(R) := \bigoplus_{n\geq 0} I^n/I^{n+1}$. This is an $R/I$-algebra. If $I = (a_1, \ldots, a_r)$, then $\overline{a}_1, \ldots, \overline{a}_r \in I/I^2 = \operatorname{gr}_I(R)_1$ generate $\operatorname{gr}_I(R)$ over $\operatorname{gr}_I(R)_0 = R/I$; in fact, $\operatorname{gr}_I(R) = (R/I)[\overline{a}_1, \ldots, \overline{a}_r]$.
(c) In the above, if $M$ is an $R$-module, then he *associated graded module* to $R$ and $M$ is defined to be $\operatorname{gr}_I(M) := \bigoplus_{n\geq 0} I^n M/I^{n+1}M$. This is a graded $\operatorname{gr}_I(R)$-module.
(d) If $S$ is a graded ring and $M$ a graded $S$-module, then for any $j \in I$ we define the *twist of $M$ by $i$* to be the graded $S$-module $M[i]$ such that $M[i]_j := M_{i+j}$.

**Observation 1.10.3.** Suppose $S$ is an $I$-graded ring.

(a) $S_0$ is a subring of $S$.
(b) $S_i$ for every $i \in I$ is an $S_0$-module.
(c) If $I = \mathbf{N}$, then $S_+ := \bigoplus_{n>0} S_n$ is an ideal.
(d) If $M$ is a graded $S$-module, then each $M_i$ is an $S_0$-submodule of $M$.

We further have the following example, which follows from the lemma after:

**Example 1.10.4.** If $R$ is a Noetherian ring, then for any ideal $I \subseteq R$, we have that $\operatorname{Bl}_I(R)$ is a Noetherian ring.

**Lemma 1.10.5.** Let $S$ be an $\mathbf{N}$-graded ring. Then $S$ is Noetherian iff $S_0$ is Noetherian and $S$ is a f.g. $S_0$-algebra.

*Proof.* The "if" is obvious, so we prove the "only if": suppose $S$ is Noetherian; then so is $S_0 := S/S_+$. Now $S_+$ is a homogenous ideal and so finitely generated by homogenous elements $x_1, \ldots, x_r$, and then $S = S_0[x_1, \ldots, x_r]$; this is easiest to see by showing for each $n \geq 0$ that $S_n \subseteq S_0[x_1, \ldots, x_r]$ using $S_n = \sum_{i=1}^r x_i S_{n-d_i}$ where $d_i = \deg x_i$. ∎

## 1.11 Hilbert Function and Hilbert Polynomial

**Definition 1.11.1.** If $R, R'$ are any rings containing $\mathbf{Z}$ and $f : R \to R'$ any function, define the first *finite difference function* $\Delta^{[1]} f : R \to R'$ *of* $f$ to be the function

$$(\Delta^{[1]} f)(n) := f(n+1) - f(n).$$

Inductively define the $k^{\text{th}}$ finite difference function $\Delta^{[k]} f := \Delta^{[1]}(\Delta^{[k-1]} f) : R \to R'$ for $k \geq 2$.

*Remark* 3. It is inductively clear that:

(a) $(\Delta^{[k]} f)(n) = \sum_{r=0}^k (-1)^{r-1} \binom{k}{r} f(n+r)$.
(b) If $R \subseteq R'$ and $f$ comes from $R'[X]$ then for any $a \in R$, we have $f$ is given by $f(X) = \sum_{k=0}^\infty (\Delta^{[k]} f)(a) \binom{X-a}{k}$.
(c) If $R \subseteq R'$ and $f$ comes from $R'[X]$, then $f(\mathbf{Z}) \subseteq \mathbf{Z}$ iff for all $k : \Delta^{[k]} f(0) \in \mathbf{Z}$.

**Definition 1.11.2.** A function $f : \mathbf{N} \to \mathbf{Q}$ is *polynomial-like* if there is a polynomial $g \in \mathbf{Q}[X]$ such that $f(n) = g(n)$ for all but finitely many $n$. In such a case, $g$ is determined uniquely and we write $\deg f := \deg g$.

**Observation 1.11.3.** If $f : \mathbf{N} \to \mathbf{Q}$ is any function, then $f$ is polynomial-like of degree $d$ iff $\Delta^{[1]} f$ is polynomial-like of degree $d-1$. (By convention, $\deg 0 := -1$).

**Theorem 1.11.4** (Hilbert Polynomial)**.** Let $S = \bigoplus_{n\geq 0} S_n$ be an $\mathbf{N}$-graded ring such that $S_0$ is Artinian and such that $S$ is a finitely generated $S_0$-algebra that is generated over $S_0$ by $r$ elements $a_1, \dots, a_r \in S_1$. If $M$ is a finitely generated graded $S$-module, then we define the *Hilbert function*

$$h_M(n) := \ell_{S_0}(M_n) \text{ for } n \geq 0.$$

Then $h_M(n)$ is polynomial-like in $n$ of degree at most $r-1$.

**Definition 1.11.5.** The function $h_M : \mathbf{N} \to \mathbf{Q}$ is called the Hilbert function of $M$. The polynomial $p_M(\cdot)$ it eventually equals is called the Hilbert polynomial of $M$.

**Example 1.11.6.** Let $f \in k[X_1, \dots, X_m]$ be a homogenous polynomial of degree $d \geq 0$ where $k$ is a field, then the Hilbert function of $M = k[X_1, \dots, X_m]/(f)$ is given by

$$h_M(n) := \binom{n+m-1}{m-1} - \binom{n-d+m-1}{m-1}.$$

*Main Proof.* We proceed by induction on $r$. If $r = 0$, then $S = S_0$. Then $M$ is finitely generated over $S_0$, say $M = \bigoplus_{i=1}^{k} S_0 m_i$ with degrees $\deg m_i = d_i$ and WLOG $d_1 \leq \cdots \leq d_k$; then $M_n = 0$ for $n > d_k$. If $r > 0$, then consider the $S_0$-linear map $\mu_r : M_n \to M_{n+1}$ given by multiplication by $a_r$. Define $K_n$ and $L_{n+1}$ to be the kernel and cokernel respectively to get an exact sequence

$$0 \to K_n \to M_n \xrightarrow{a_r} M_{n+1} \to L_{n+1} \to 0.$$

Set $K = \bigoplus_{n\geq 0} K_n$ and $L = \bigoplus_{n\geq 0} L_n$. Then $K$ is a submodule of $M$ and $L = M/a_r M$ is a quotient of $M$, so that both of these are finitely generated Noetherian graded $S$-modules. In fact, $a_r K = a_r L = 0$, so that $K$ and $L$ can be viewed as $S/a_r S$ modules. From the above exact sequence we get that $\Delta^{[1]} h_M(n) = h_L(n+1) - h_K(n)$, so by induction and Observation 1.11.3 we are done. ∎

## 1.12 Completion and Artin-Rees

**Definition 1.12.1.** Let $R$ be a ring, $I \subseteq R$ an ideal and $M$ an $R$-module.

(a) A chain $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots$ of submodules of $M$ is called a *filtration* of $M$, denoted $(M_n)$.
(b) A filtration $(M_n)$ of $M$ is called an *$I$-filtration* if $IM_n \subseteq M_{n+1}$ for all $n$, and is called a *stable $I$-filtration* if $IM_n = M_{n+1}$ for all $n \gg 0$ (e.g. $M_n = I^n M$).

Every filtration $(M_n)$ of $M$ determines a topology on $M$ by taking $(M_n)_n$ to be a neighborhood basis of $0 \in M$. This topology depends in general on the filtration.

**Lemma 1.12.2.** If $(M_n)$ and $(M'_n)$ are stable $I$-filtrations of $M$, then they have bounded difference: there is an integer $N$ such that $M_{n+N} \subseteq M'_n$ and $M'_{n+N} \subseteq M_n$ for all $n \geq 0$. In particular, the topologies induced on $M$ by any two $I$-stable filtrations are the same.

*Proof.* It suffices to take $M'_n = I^n M$. Since $IM_n \subseteq M_{n+1}$ for all $n$, we have that $I^n M \subseteq M_n$; also $IM_n = M_{n+1}$ for all $n \geq N$ say, hence $M_{n+N} = I^n M_N \subseteq I^n M$. ∎

**Definition 1.12.3.** The topology determined on $M$ by any $I$-stable filtration is called the *$I$-adic topology.* We let $\hat{M}_I$ denote the completion of $M$ with respect to the $I$-adic topology, and let $M \to \hat{M}_I$ denote the completion map. This $\hat{M}_I$ can be constructed explicitly as $\varprojlim_n M/I^n M$, and so the completion map $M \to \hat{M}_I$ has kernel $K_M^I := \bigcap_{n\geq 0} I^n M$.

**Example 1.12.4.** Let $R$ be a ring. For any maximal ideal $\mathfrak{m} \subseteq R$, the completion $\hat{R}_\mathfrak{m}$ is a local ring. We show that the set of nonunits $\hat{R}_\mathfrak{m} \setminus \hat{R}_\mathfrak{m}^* = \ker(\hat{R}_\mathfrak{m} \twoheadrightarrow R/\mathfrak{m})$, from which we are done by Theorem 1.3.3(a). The inclusion $\supseteq$ is clear. For the other inclusion, first note that any $x \in \hat{R}_\mathfrak{m}$ is of the form $x = \sum_{i=0}^{\infty} x_i$ with $x_i \in \mathfrak{m}^i$; if $x_0 \notin \mathfrak{m}$, then there is a $y \in R$ such that $x_0 y \equiv 1 \pmod{\mathfrak{m}}$, and then $xy = 1 + (x_1 y + x_0 y - 1) + \sum_{i\geq 2} x_i y$, so it suffices to show the result for $x_0 = 1$, in which case we clearly have an explicit formula using the geometric series (cite MO).

If $R$ is a ring and $I \subseteq R$, then we form the graded ring $\mathrm{Bl}_I(R) = \bigoplus_{n\geq 0} I^n$. Similarly, if $M$ is an $R$-module and $(M_n)$ an $I$-filtration, then $\mathrm{Bl}_I(M) = \bigoplus_{n\geq 0} M_n$ is a graded $\mathrm{Bl}_I(R)$-module since $I^m M_n \subseteq M_{m+n}$.

**Theorem 1.12.5.** Let $R$ be a Noetherian ring, $I \subseteq R$ an ideal, $M$ a finitely generated $R$-module, and $(M_n)$ an $I$-filtration of $M$. Then the following are equivalent:

(a) $\mathrm{Bl}_I(M)$ is a finitely generated $\mathrm{Bl}_I(R)$-module.
(b) The $I$-filtration $(M_n)$ is stable.

*Proof.* Each $M_n$ is finitely generated over $R$, and hence so is each $L_n := \bigoplus_{r=0}^{n} M_r$: this is a subgroup of $\mathrm{Bl}_I(M)$ but not in general a $\mathrm{Bl}_I(R)$-submodule. However, it generates one, namely

$$\langle L_n \rangle = M_0 \oplus \cdots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \cdots \oplus I^r M_n \oplus \cdots,$$

which is therefore a finitely generated as an $\mathrm{Bl}_I(R)$-module. The $\langle L_n \rangle$ form an ascending chain of $\mathrm{Bl}_I(R)$-modules whose union is $\mathrm{Bl}_I(M)$. Since $\mathrm{Bl}_I(R)$ is Noetherian, $\mathrm{Bl}_I(M)$ is a finitely generated $\mathrm{Bl}_I(R)$-module iff the chain stops iff $\mathrm{Bl}_I(M) = \langle L_N \rangle$ for some $N \geq 0$ iff $M_{n+N} = I^n M_N$ for all $n \geq 0$. ∎

**Corollary 1.12.6** (Artin-Rees Lemma)**.** Suppose $R$ is a Noetherian ring, $I \subseteq R$ an ideal, $M$ a finitely generated $R$-module, and $N \subseteq M$ a submodule.

(a) If $(M_n)$ a stable $I$-filtration of $M$, then $N \cap M_n$ is a stable $I$-filtration of $N$.
(b) There is an integer $k \geq 0$ such that $I^{n+k} M \cap N = I^n (I^k M \cap N)$ for all $n \geq 0$.

*Proof.* For (a), we have $I(N \cap M_n) \subseteq IN \cap IM_n \subseteq N \cap M_{n+1}$, hence $N \cap M_n$ is an $I$-filtration. Hence it defines a graded $\mathrm{Bl}_I(R)$-submodule of $\mathrm{Bl}_I(M)$, which is finitely generated since $\mathrm{Bl}_I(R)$ is Noetherian and $\mathrm{Bl}_I(M)$ is finitely generated. Now apply the previous theorem. For (b), apply (a) to $M_n = I^n M$. ∎

**Corollary 1.12.7** (Krull)**.** Suppose $R$ is a Noetherian ring and $I$ an ideal.

(a) If $M$ a f.g. $R$-module, then there is an $a \in I$ such that $(1 + a)K_M^I = 0$. If $I \subseteq \mathrm{Jac}(R)$, then $K_M^I = 0$.
(b) In particular, if $I \subseteq \mathrm{Jac}(R)$, then $K_I^I = \bigcap_{n\geq 0} I^n = 0$. E.g., if $(R, \mathfrak{m})$ is a NLR, then $\bigcap_{n\geq 0} \mathfrak{m}^n = 0$.
(c) If $R$ is a domain and $I$ a proper ideal, then $\bigcap_{n\geq 0} I^n = 0$.

*Proof.* For (a), by the Artin-Rees Lemma, for $n \gg 0$ we have $K_M^I = I^n M \cap K_M^I \subseteq IK_M^I$, so we are done by Nakayama's Lemma. The statement (b) is clear. For (c), since $1 \notin I$, we must have $1 + a \neq 0$; then $1 + a$ is not a zero divisor, so that $K_I^I = 0$. ∎

[NB: An elementary proof of $K_I^I \subseteq IK_I^I$ was given by Perdry, as follows: say $I = (a_1, \ldots, a_n)$. If $b \in K_I^I$, then for each $k \geq 1$, there is a homogenous degree $k$ polynomial $p_k \in R[X_1, \ldots, X_n]$ such that $b = p_k(a_1, \ldots, a_n) =: p_k(a)$. In the Noetherian ring $R[X_1, \ldots, X_n]$ consider the chain $(p_1) \subseteq (p_1, p_2) \subseteq \cdots$; from this there is an $N \geq 1$ and $q_1, \ldots, q_N \in R[X_1, \ldots, X_n]$ with $q_i$ homogenous of degree $i$ such that $p_{N+1} = q_N p_1 + \cdots + q_1 p_N$. Then $b = p_{N+1}(b) = b(q_N(a) + \cdots + q_1(a))$ as needed.]

## 1.13 Trace, Norm, and Discriminant

**Definition 1.13.1.** Let $R \subseteq S$ be a finite extension of rings such that $S$ is a finitely generated free $R$-module. Given an element $\alpha \in S$, define its *trace* (resp. *norm*), denoted $\mathrm{N}_R^S(\alpha)$ (resp. $\mathrm{Tr}_R^S(\alpha)$) to be the trace (resp. determinant) of the $R$-module endomorphism of $S$ given by multiplication by $\alpha$.

**Example 1.13.2.** Finite field extensions $K/k$ (or more generally finite-dimensional algebras over fields, e.g. étale algebras) and rings of integers $\mathbf{Z} \subseteq \mathcal{O}_K$ are primary examples. For instance, for $\mathbf{R} \subseteq \mathbf{C}$ and $z \in \mathbf{C}$ we have $\mathrm{Tr}_{\mathbf{R}}^{\mathbf{C}}(z) = z + \overline{z} = 2\,\mathrm{Re}\, z$ and $\mathrm{N}_{\mathbf{R}}^{\mathbf{C}}(z) = z\overline{z} = |z|^2$.

**Observation 1.13.3.** Let $R \subseteq S$ be a ring extension such that $S$ is a finitely generated free $R$-module.

(a) For any $\alpha, \beta \in S$ and $\lambda, \mu \in R$ we have

$$\begin{aligned} \mathrm{Tr}_R^S(\lambda\alpha + \mu\beta) &= \lambda\,\mathrm{Tr}_R^S(\alpha) + \mu\,\mathrm{Tr}_R^S(\beta), \\ \mathrm{N}_R^S(\alpha\beta) &= \mathrm{N}_R^S(\alpha)\,\mathrm{N}_R^S(\beta), \\ \mathrm{Tr}_R^S(\lambda) &= (\mathrm{rank}_R\, S)\lambda, \text{ and} \\ \mathrm{N}_R^S(\lambda) &= \lambda^{\mathrm{rank}_R\, S}. \end{aligned}$$

(b) (Base Change) Suppose that $R$ is an $A$-algebra for some ring $A$. Then if $T$ is any other $A$-algebra, then the ring extension $R \otimes_A T \subseteq S \otimes_A T$ still satisfies the above condition, and we have for any $\alpha \in S$ that

$$\mathrm{Tr}^{S\otimes_A T}_{R\otimes_A T}(\alpha \otimes 1) = \mathrm{Tr}^S_R(\alpha) \otimes 1 \text{ and } \mathrm{N}^{S\otimes_A T}_{R\otimes_A T}(\alpha \otimes 1) = \mathrm{N}^S_R(\alpha) \otimes 1.$$

(c) (Transitivity) Let $S \subseteq T$ be a further ring extension so that $T$ is a finitely generated $S$-module. Then $T$ is also a finitely generated $R$-module, and we have further for any $\alpha \in T$ that

$$\mathrm{Tr}^T_R(\alpha) = \mathrm{Tr}^S_R \mathrm{Tr}^T_S(\alpha) \text{ and } \mathrm{N}^T_R(\alpha) = \mathrm{N}^S_R \mathrm{N}^T_S(\alpha).$$

This last is a consequence of the following lemma about block dtereminants:

**Lemma 1.13.4.** Let $R$ be any ring, $n \geq 1$, and $S \subseteq \mathrm{Mat}_n R$ a (commutative, unitary) subring of the $n \times n$ matrix ring over $R$. If $m \geq 1$ is any integer, then for any matrix $M \in \mathrm{Mat}_m S = \mathrm{Mat}_{nm} R$, we have $\det_R M = \det_R \det_S M$.

*Proof.* We induct on $m$, with $m = 1$ being clear. Hence assume $m \geq 2$, and write $M$ as

$$M = \begin{bmatrix} A & b \\ c & d \end{bmatrix}$$

where $A, b, c, d$ have dimensions $n(m-1) \times n(m-1)$, and $n(m-1) \times n$, and $n \times n(m-1)$ and $n \times n$ respectively. Since $S$ is commutative, we have that $c \cdot dI^S_{m-1} = dc$, and similarly $A \cdot dI^S_{m-1} = dA$. Therefore,

$$\begin{bmatrix} A & b \\ c & d \end{bmatrix} \begin{bmatrix} dI^S_{m-1} & 0 \\ -c & I^S_1 \end{bmatrix} = \begin{bmatrix} dA - bc & b \\ 0 & d \end{bmatrix},$$

so that taking $\det_S$ gives $\det_S M \cdot d^{m-1} = \det_S(dA - bc) \cdot d$ and hence taking $\det_R$ gives

$$(\det_R \det_S M)(\det_R d)^{m-1} = (\det_R \det_S(dA - bC))(\det_R d) = (\det_R(dA - bc))(\det_R d).$$

On the other hand, taking $\det_R$ directly gives

$$(\det_R M)(\det_R d)^{m-1} = (\det_R(dA - bc))(\det_R d).$$

Putting these together gives us

$$(\det_R \det_S M - \det_R M)(\det_R d)^{m-1} = 0.$$

If $\det_R d$ is not a zero divisor in $R$, we are done; we can now either reduce to this case by working in polynomial rings over $\mathbf{Z}$ OR replace our base ring $R$ by $R[x]$ and use $d_x := xI^R_n + d$ instead. Then $\det_R d_x$ is a monic polynomial of degree $n$ and the above holds as a polynomial identity with $M_x$ replacing $M$; in a polynomial ring, a monic polynomial is never a zero divisor, and so we conclude that other factor is 0, and now specialize to $x = 0$. ∎

**Theorem 1.13.5.** Let $L/K$ be a finite field extension and let $\overline{K}$ be an algebraic closure of $K$. Let $\Sigma := \mathrm{Hom}_K(L, \overline{K})$.

(a) For all $\alpha \in L$ we have

$$\mathrm{Tr}^L_K(\alpha) = [L : K]_i \sum_{\sigma\in\Sigma} \sigma\alpha \text{ and } \mathrm{N}^L_K(\alpha) = \left(\prod_{\sigma\in\Sigma} \sigma\alpha\right)^{[L:K]_i}.$$

(b) Given a $0 \neq \alpha \in L$, let $d := [K(\alpha) : K]$ and let its minimal polynomial be $\mu_\alpha(X) = X^d + a_1 X^{d-1} + \cdots + a_d = \prod_{i=1}^d (X - \alpha_i)$, where the last is the factorization in $\overline{K}[X]$. If $n := [L : K]$ and $e = [L : K(\alpha)]$, then

$$\mathrm{Tr}^L_K(\alpha) = \sum_{i=1}^d e\alpha_i = -ea_1 \text{ and } \mathrm{N}^L_K(\alpha) = \prod_{i=1}^d \alpha_i^e = (-1)^n a_d^e.$$

*Proof.* ∎

The trace map $\mathrm{Tr}^S_R : S \to R$ is an $R$-linear map; since $S$ is a ring, we get a bilinear pairing on $S$ given by $\langle x, y\rangle \mapsto \mathrm{Tr}^S_R(xy)$ called the *trace pairing*. This gives us an $R$-linear map $S \to S^*$ (where $S^*$ is its dual as an $R$-module, i.e. $\mathrm{Hom}_R(S, R)$) given by $x \mapsto \mathrm{Tr}^S_R(x\cdot)$.

**Definition 1.13.6.** Given an ordered free basis $s := (s_1, \ldots, s_n)$ of $S$ over $R$, define the *discriminant* $D(s)$ to be the determinant of the linear map $S \to S^*$ with respect to the bases $s$ and $s^*$, i.e. in other words,

$$D(s) := \det\Big[\mathrm{Tr}_R^S(s_i s_j)\Big]_{i,j=1}^n.$$

As usual for bilinear pairings, choosing a different basis $s'$ changes $D(s)$ by the square of a unit (namely, the determinant of the change of basis matrix), and so in general, we get a well-defined element $D_{S/R} \in R/(R^\times)^2$ depending only on $S$, which we call the relative discriminant of $S$ over $R$. (When $R = \mathbf{Z}$, we have $(\mathbf{Z}^\times)^2 = \{1\}$, and so this gives an honest element of $\mathbf{Z}$. In general, we get a well-defined ideal $D_{S/R} \subseteq R$ called the discriminant ideal. When $R = k$ is a field, we can care only about whether or not this ideal is zero.)

Now suppose that $R$ is a domain, $K = \mathrm{Frac}\, R$ and $L/K$ a finite extension with $\mathrm{char}\, K \nmid [L : K]$. In this case, the trace pairing $\mathrm{Tr}_K^L : L \to K$ is not identically zero (since $\mathrm{Tr}_K^L(1) = [L : K] \neq 0$) and hence nondegenerate, since $\mathrm{Tr}_K^L(x \cdot x^{-1}) \neq 0$ for every nonzero $x$). In particular, we get an isomorphism $L \to L^* = \mathrm{Hom}_K(L, K)$ given by $x \mapsto \mathrm{Tr}_K^L(x\cdot)$.

**Definition 1.13.7.** Given any $R$-submodule $M \subseteq L$, we define its *trace dual* to be

$$M^* := \{x \in L : \mathrm{Tr}_K^L(xy) \in R \text{ for all } y \in M\}.$$

This is another $R$-submodule of $L$. If $M$ is free with basis $s_1, \ldots, s_n$, then $M^*$ is free with basis $s_1^*, \ldots, s_n^*$, where $s_i^*$ are such that $s_i^* s_j = \delta_{ij}$.

**Example 1.13.8.** Let $K$ be a number field. We'll show that $\mathcal{O}_K := \mathrm{Cl}_K(\mathbf{Z})$ is a free $\mathbf{Z}$-module of rank $n := [K : \mathbf{Q}]$. Indeed, the above conditions are automatically satisfied. The key point is that if $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}_{\mathbf{Q}}^K(\alpha) \in \mathbf{Z}$; this follows immediately from Corollary 1.5.10 and Theorem 1.13.5. Let $v_1, \ldots, v_n \in K$ be a $\mathbf{Q}$-basis lying in $\mathcal{O}_K$ (this can always be achieved by rescaling) and let $M := \sum_{i=1}^n \mathbf{Z} v_i$. Then it suffices to observe that $M \subseteq \mathcal{O}_K \subseteq M^*$, and we are done by the structure theorem for finitely generated abelian groups. The discriminant $D_{\mathcal{O}_K/\mathbf{Z}} \in \mathbf{Z}$ is a fundamental invariant of $K$.

## 1.14 Derivations

Suppose $R$ is a ring, $S$ an $R$-algebra, and $M$ an $S$-module.

**Definition 1.14.1.** An *$R$-linear derivation (or simply an $R$-derivation) from $S$ to $M$* is an $R$-module homomorphism $D : S \to M$ that satisfies the *Liebniz Rule* that

$$\forall\, f, g \in S : D(fg) = gDf + fDg.$$

The set of all $R$-linear derivations from $S$ to $M$ is naturally an $S$-module denoted by $\mathrm{Der}_R(S, M)$.

*Remark* 4.

(a) Every ring $S$ is a $\mathbf{Z}$-algebra. A $\mathbf{Z}$-derivation is simply called a *derivation*, and in that case the module of derivations is written $\mathrm{Der}(S, M) := \mathrm{Der}_{\mathbf{Z}}(S, M)$.

(b) If $\phi : M \to M'$ is an $S$-module homomorphism and $D : S \to M$ an $R$-derivation, then it is immediate that the map $\phi \circ D : S \to M'$ is also an $R$-derivation. This gives an $S$-module homomorphism $\phi_* : \mathrm{Der}_R(S, M) \to \mathrm{Der}_R(S, M')$. It is immediate to check that this construction is functorial, so that taking $R$-derivations gives a covariant functor

$$\mathrm{Der}_R(S, -) : S\text{-}\mathsf{Mod} \to S\text{-}\mathsf{Mod}.$$

We shall see momentarily that this functor is representable.

(c) The case $M = S$ deserves special attention: we define $\mathrm{Der}_R(S) := \mathrm{Der}_R(S, S)$. If $D, D' \in \mathrm{Der}_R(S)$ then we can compose them to get another map $DD' : S \to S$ which is not in general a derivation. However, the bracket $[D, D'] = DD' - D'D$ is indeed a derivation, and this turns $\mathrm{Der}_R(S)$ into a Lie algebra over $R$.

**Lemma 1.14.2** (Basic Properties of Derivations)**.**

(a) If $e \in S$ is an idempotent, i.e. s.t. $e^2 = e$, then $D(e) = 0$ for any $R$-derivation $D \in \mathrm{Der}_R(S, M)$. In particular, $D(1) = 0$ for any $R$-derivation $D \in \mathrm{Der}_R(S, M)$.

(b) If $i : R \to S$ denotes the canonical map, then a derivation $D \in \mathrm{Der}(S, M)$ is $R$-linear iff $D \circ i = 0$. In this sense, $\mathrm{Der}_R(S, M) \subseteq \mathrm{Der}(S, M)$ is the submodule of derivations that vanish on $R$.

(c) For any $f, g \in S$, $R$-derivation $D \in \mathrm{Der}_R(S, M)$ and integer $n \geq 1$ we have that

$$D(f^n) = nf^{n-1}Df \text{ and } D^n(fg) = \sum_{i=0}^{n} \binom{n}{i} D^i f D^{n-i} g.$$

(d) If $n = 0 \in S$ for some $n \geq 1$, then for any element $f \in S$ and $D \in \mathrm{Der}_R(S, M)$ we have $D(f^n) = 0$. If $n = p$ is prime, then if $D \in \mathrm{Der}_R(S, M)$ then $D^p \in \mathrm{Der}_R(S, M)$ too.

*Proof.*

(a) This follows from $D(e) = D(e^2) = eDe + eDe = 2eDe \Rightarrow (2e-1)De = 0 \Rightarrow De = (2e-1)^2 De = 0$.
(b) If $D$ is $R$-linear, then $D(f(r)) = D(f(r) \cdot 1) = f(r)D(1) = 0$; the converse follows from the Liebniz Rule.
(c) Clear by induction on $n$.
(d) Clear from (3).

■

**Example 1.14.3.** If $S = R[X]$ is the polynomial ring, then a derivation $D \in \mathrm{Der}_R(S, M)$ is completely determined by $D(X) \in M$. For example, the derivation $\partial_X \in \mathrm{Der}_R(S, S)$ defined by taking $\partial_X X = 1$ is the usual formal derivative $\partial_X : R[X] \to R[X]$ with respect to $X$.

**Theorem 1.14.4** (Representability of $\mathrm{Der}_R(S, -)$/Module of Kähler Differentials)**.**
The covariant functor $\mathrm{Der}_R(S, -) : S\text{-}\mathsf{Mod} \to S\text{-}\mathsf{Mod}$ is representable. In other words, there is an $S$-module $\Omega_{S/R}$, called the *module of Kähler differentials* of $S$ over $R$, and a derivation $\mathrm{d} : S \to \Omega_{S/R}$, called the *universal derivation*, such that if $M$ is any $S$-module and $D \in \mathrm{Der}_R(S, M)$ any $R$-derivation, then there is a unique $S$-module homomorphism $\widetilde{D} : \Omega_{S/R} \to M$ such that $D = \widetilde{D} \circ \mathrm{d}$; in other words, such that the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{\mathrm{d}} & \Omega_{S/R} \\ & \searrow^{D} & \downarrow{\scriptstyle \exists!\, \widetilde{D}} \\ & & M \end{array}$$

From this it follows that we have a natural isomorphism of functors

$$\mathrm{Der}_R(S, -) \cong \mathrm{Hom}_S(\Omega_{S/R}, -) : S\text{-}\mathsf{Mod} \to S\text{-}\mathsf{Mod}.$$

*Proof.* The universal property determines $\Omega_{S/R}$ upto unique isomorphism preserving d; therefore, it suffices to show existence. We give two constructions:

(a) Consider the quotient of the free $S$-module generated by all symbols of the form $\{\mathrm{d}f : f \in S\}$ by the relations

$$\mathrm{d}(fg) = g\mathrm{d}f + f\mathrm{d}g \text{ and } \mathrm{d}(rf + sg) = r\mathrm{d}f + s\mathrm{d}g, \forall\, f, g \in S, r, s \in R.$$

The quotient $\Omega_{S/R}$ along with the map $d : S \to \Omega_{S/R} : f \mapsto \mathrm{d}f$ satisfies the universal property.
(b) Firstly, define $\mu : S \otimes_R S \to S$ by $\mu(f \otimes g) := fg$; then $\mu$ is an $R$-algebra homomorphism. Set $I := \ker \mu$ and $\Omega_{S/R} := I/I^2$, with the map $\mathrm{d} : S \to \Omega_{S/R}$ given by $f \mapsto 1 \otimes f - f \otimes 1 \pmod{I^2}$.

■

For $i \geq 0$, define $\Omega^i_{S/R} := \Lambda^i \Omega_{S/R}$; then the derivation $\mathrm{d} : S = \Omega^0_{S/R} \to \Omega^1_{S/R} = \Omega_{S/R}$ is the first step in a complex of $R$-modules

$$\Omega^\bullet_{S/R} : 0 \to \Omega^0_{S/R} \xrightarrow{\mathrm{d}=\mathrm{d}^0} \Omega^1_{S/R} \xrightarrow{\mathrm{d}^1} \cdots \to \Omega^i_{S/R} \xrightarrow{\mathrm{d}^i} \Omega^{i+1}_{S/R} \to \cdots,$$

where the map $\mathrm{d}^i : \Omega^i_{S/R} \to \Omega^{i+1}_{S/R}$ satisfies

$$\mathrm{d}^i(f\mathrm{d}\eta_1 \wedge \cdots \wedge \mathrm{d}\eta_i) = \mathrm{d}f \wedge \mathrm{d}\eta_1 \wedge \cdots \wedge \mathrm{d}\eta_i.$$

The complex $\Omega^\bullet_{S/R}$ is called the *de Rham complex* of $S$ relative to $R$, and its cohomology $H^\bullet_{\mathrm{dR}}(S; R)$ is called the *de Rham cohomology* of $S$ relative to $R$.

## 1.15 Abstract Dependence Relations

**Definition 1.15.1.** Let $S$ be a set. A *closure operator* on $S$ is a function $\mathrm{Cl} : 2^S \to 2^S$ that is

(a) *extensive*, i.e. $X \subseteq \mathrm{Cl}\, X$ for all $X \subseteq S$,
(b) *increasing*, i.e. $X \subseteq Y \Rightarrow \mathrm{Cl}\, X \subseteq \mathrm{Cl}\, Y$ for all $X \subseteq Y \subseteq S$, and
(c) *idempotent*, i.e. $\mathrm{Cl}\,\mathrm{Cl}\, X = \mathrm{Cl}\, X$ for all $X \subseteq S$.

A closure operation Cl is said to

(d) satisfy *MacLane-Steinitz exchange* if $x \in X \subseteq S$ and $y \in \mathrm{Cl}\, X \setminus \mathrm{Cl}(X \setminus \{x\})$ implies $x \in \mathrm{Cl}(X \setminus \{x\} \cup \{y\})$,
(e) be *finitary*, if for any $X \subseteq S$ we have $\mathrm{Cl}\, X = \bigcup_{X' \subseteq X \text{ finite}} \mathrm{Cl}\, X'$, and
(f) be *topological* if for any $X, Y \subseteq S$ we have $\mathrm{Cl}(X \cup Y) = \mathrm{Cl}(X) \cup \mathrm{Cl}(Y)$.

Closure operators are absolutely ubiquitous in mathematics, e.g. integral closure, algebraic closure, separable closure, abelian closure, unramified closure, differential closure, topological closure, acyclic closure (define on a set $S$ of edges of a graph a dependence relation where $e$ is dependent on $X$ if there is a path in $X$ that connects the same vertices as $e$), etc. Closure operators satisfying MacLane-Steinitz exchange are called *matroid closure operations*.

**Definition 1.15.2.** A *dependence relation* on a set $S$ is a finitary closure operation satisfying MacLane-Steinitz exchange, i.e. a map $\mathfrak{D} : 2^S \to 2^S$ satisfying (a)-(e). Given such a pair $(S, \mathfrak{D})$, we say that a subset $X \subseteq S$ is

(a) *a spanning set* if $\mathfrak{D}X = S$,
(b) *independent* if for all $x \in X$ we have $x \notin \mathfrak{D}(X \setminus \{x\})$, and
(c) *a basis* if it is both independent and a spanning set.

We say that $(S, \mathfrak{D})$ is of *finite dependency* if it admits a finite spanning set. Finally, we define the *fundamental set* of the dependence relation to be $\mathfrak{D}\emptyset$.

**Lemma 1.15.3.** Let $(S, \mathfrak{D})$ be a set with a dependence relation. Then

(a) we have transitivity, i.e. if $X, Y \subseteq S$ are subsets, then $X \subseteq \mathfrak{D}Y \Rightarrow \mathfrak{D}X \subseteq \mathfrak{D}Y$,
(b) if $X \subseteq S$ is independent and $y \in S \setminus \mathfrak{D}X$, then $X \cup \{y\}$ is independent, and
(c) if $X \subseteq S$ is any subset, then TFAE:
    (1) $X$ is a basis.
    (2) $X$ is a minimal spanning set,
    (3) $X$ is a maximal independent set, and
(d) if $(X_\alpha)$ is a totally ordered collection of independent subsets, then the union $\bigcup_\alpha X_\alpha$ is also independent.

*Proof.* The statement (a) follows from $X \subseteq \mathfrak{D}Y \Rightarrow \mathfrak{D}X \subseteq \mathfrak{D}^2Y = \mathfrak{D}Y$. For (b), to show that $X' := X \cup \{y\}$ we have to show that for all $x \in X'$ that $x \notin \mathfrak{D}(X' \setminus \{x\})$. This is clear if $x = y$ by hypothesis. If $x \in X$, then if $x \in \mathfrak{D}(X' \setminus \{x\})$, then $x \in \mathfrak{D}((X \setminus \{x\}) \cup \{y\}) \setminus \mathfrak{D}(X \setminus \{x\})$ implies by exchange that $y \in \mathfrak{D}X$, again contrary to hypothesis. For (c), to show (1) $\Rightarrow$ (2), let $X$ be a basis, so it is certainly spanning; if there were a proper spanning subset $X' \subsetneq X$, then picking an $x \in X \setminus X'$ would show $x \in S = \mathfrak{D}(X') \subseteq \mathfrak{D}(X \setminus \{x\})$, contradicting the independence of $X$. For (2) $\Rightarrow$ (1), suppose that $X$ is a minimal spanning set and that for some $x \in X$ we have $x \in \mathfrak{D}(X \setminus \{x\})$. Then $X \subseteq \mathfrak{D}(X \setminus \{x\})$ immplies by (a) that $S = \mathfrak{D}X \subseteq \mathfrak{D}(X \setminus \{x\})$, so that $X \setminus \{x\}$ is a proper subset that is also spanning, which is a contradiction. To show (1) $\Rightarrow$ (3), let $X$ be a basis, so it is certainly independent; if there were a proper independent superset $X' \supsetneq X$, then picking an $x \in X' \setminus X$ would show $x \in S = \mathfrak{D}(X) \subseteq \mathfrak{D}(X' \setminus \{x\})$, contradicting the independence of $X'$. For (3) $\Rightarrow$ (1), suppose that $X$ is a maximal independent set. If there is a $y \in S \setminus \mathfrak{D}X$, then by (b) we have $X \cup \{y\} \supsetneq X$ still independent, a contradiction; therefore, $\mathfrak{D}X = S$ as well. For (d), let $X := \bigcup_\alpha X_\alpha$. If there is an $x \in X$ such that $x \in \mathfrak{D}(X \setminus \{x\})$, then bythe finiteness property of dependence there is a finite subset $X' \subseteq X \setminus \{x\}$ such that $x \in \mathfrak{D}X'$. By the total ordering, there is an $\alpha$ so that $X' \cup \{x\} \subseteq X_\alpha$, and then $x \in \mathfrak{D}X' \subseteq \mathfrak{D}(X_\alpha \setminus \{x\})$ contradicts the independence of $X_\alpha$. Therefore, $X$ is independent. ∎

**Theorem 1.15.4** (Steinitz Exchange)**.** Let $(S, \mathfrak{D})$ be a set with a dependence relation. If $X, Y \subseteq S$ are subsets with $X$ independent and $Y$ spanning, then there is a $Y' \subseteq Y$ such that $X \cap Y' = \emptyset$ such that $X \cup Y'$ is a basis.

*Proof.* Let $\mathcal{A}$ be the collection of independent $Z \subseteq S$ such that $X \subseteq Z \subseteq X \cup Y$; then $\mathcal{A}$ is nonempty because $X \in \mathcal{A}$. By Lemma 1.15.3(d) and Zorn's Lemma, this has a maximal element $Z$. We claim that $Z$ is a basis; indeed, it is independent since $Z \in \mathcal{A}$. If there is a $y \in Y \setminus \mathfrak{D}Z$, then by Lemma 1.15.3(b) we have $Z \subsetneq Z \cup \{y\} \subseteq Y$ with $Z \cup \{y\}$ still independent, a contradiction to maximality. Therefore, $Y \subseteq \mathfrak{D}Z$ so by Lemma 1.15.3(a) we have $S = \mathfrak{D}Y \subseteq \mathfrak{D}Z$ and so $Z$ is spanning as well. ∎

**Corollary 1.15.5.** Let $(S, \mathfrak{D})$ be a set with a dependence relation.

(a) Every independent subset of $S$ can be completed to a basis.
(b) Every spanning subset of $S$ contains a basis.
(c) In particular, $S$ admits a basis.

Next suppose that $S$ has finite dependency.

(d) If $X, Y \subseteq S$ are subsets with $X$ independent and $Y$ a finite spanning set, then $|X'| \leq |Y|$ and there is a subset $Y'' \subseteq Y$ disjoint from $X'$ and of cardinality $|Y''| \leq |Y| - |X'|$ such that $X' \cup Y''$ is a basis.
(e) Any independent subset has cardinality smaller than any finite spanning set and is in particular finite.

Finally, irrespective of whether $S$ has finite dependency, we have:

(f) Any two bases of $S$ have the same cardinality.

**Definition 1.15.6.** Let $(S, \mathfrak{D})$ be a set with a dependence relation. The *dependency* of $(S, \mathfrak{D})$ is the cardinality of any basis and is denoted $\dep S$.

*Proof of Corollary 1.15.5.* For (a), apply Theorem 1.15.4 with $X$ the independent subset and $Y = S$. For (b), apply Theorem 1.15.4 with $X = \emptyset$ and $Y$ the spanning subset. For (c), apply (a) to $X = \emptyset$ (or equivalently (b) to $Y = S$). For (d), we induct on $|X'|$. When $|X'| = 0$, then certainly $|X'| \leq |Y|$ and by (b) there is a basis $Y'' \subseteq Y$. Now assume the inductive hypothesis and so $|X'| = n \geq 1$, say $X' = \{x_1, \ldots, x_n\}$. By applying the inductive hypothesis to $X' \setminus \{x_n\}$, we conclude that $n - 1 \leq |Y|$ and there is a subset $Y' \subseteq Y$ disjoint from $X' \setminus \{x_n\}$ of cardinality $|Y'| \leq |Y| - n + 1$ such that $(X' \setminus \{x_n\}) \cup Y'$ is a basis. If $x_n \in Y'$, then taking $Y'' := Y' \setminus \{x_n\}$ suffices; else assume that $x_n \notin Y'$. Then certainly $X' \cup Y'$ is spanning and $X' \subseteq X$ independent, so by Theorem 1.15.4, there is a $Y'' \subseteq Y'$ disjoint from $X'$ such that $X' \cup Y''$ is a basis. We can't have $Y'' = Y'$ because $X' \cup Y'$ is not independent since $x_n \in S = \mathfrak{D}((X' \setminus \{x_n\}) \cup Y') = \mathfrak{D}((X' \cup Y') \setminus \{x_n\})$ where $(X' \setminus \{x_n\}) \cup Y' = (X' \cup Y') \setminus \{x_n\}$ because $x_n \notin Y'$. Therefore, $Y'' \subsetneq Y'$ showing that $0 \leq |Y''| < |Y'| \leq |Y| - n + 1 \Rightarrow n \leq |Y|$ and that $|Y''| \leq |Y| - n$, so this $Y''$ works. For (e), let $X$ be an independent subset and $Y$ a finite spanning subset. By (d), we have $|X'| \leq |Y|$ for every finite $X' \subseteq X$ and so it follows that $X$ is finite with $|X| \leq |Y|$. For (f), this follows immediately from (e) if $S$ has finite dependency, so suppose now that $S$ does not have infinite dependency; then no basis of $S$ can be finite. Let $X$ and $Y$ be bases of $S$. For each $y \in Y$, we have $y \in S = \mathfrak{D}X = \bigcup_{X' \subseteq X} \mathfrak{D}X'$ so there is a finite subset $X_y \subseteq X$ such that $y \in \mathfrak{D}X_y$. Then $Y \subseteq \mathfrak{D}(\bigcup_{y \in Y} X_y)$. Then if $x \in X \setminus \bigcup_{y \in Y} X_y$, then $x \in S = \mathfrak{D}Y \subseteq \mathfrak{D}(\bigcup_y X_y) \subseteq \mathfrak{D}(X \setminus \{x\})$ contradicts the independence of $X$; therefore, $X = \bigcup_{y \in Y} X_y$. It follows that $|X| = \left|\bigcup_{y \in Y} X_y\right| \leq \left|\coprod_{y \in Y} X_y\right| \leq |Y \times \mathbf{N}| = |Y|$ where the last uses that $Y$ is infinite. By symmetry, of course, $|Y| \leq |X|$ as well, so we are done by Schröder-Bernstein. ∎

**Example 1.15.7.** Every vector space over a field has a basis, and any two bases have the same cardinality, with the dependency in this case being exactly the dimension. Any linearly independent subset can be completed to a basis with elements from a spanning subset. In this case, the fundamental set is nothing but 0.

**Definition 1.15.8.** Let $S$ be a set with a dependence relation $\mathfrak{D}$ and let $\varphi : T \to S$ be any set map. Define the pullback dependence relation $\varphi^*\mathfrak{D}$ via $(\varphi^*\mathfrak{D})(X) = \varphi^{-1}(\mathfrak{D}(\varphi(X))$ for any $X \subseteq T$.

**Example 1.15.9.** Let $V, W$ be vector spaces and $\varphi : V \to W$ be a linear map. If LD is the linear dependence relation on $W$, then the dependency $\dep \varphi^*\mathrm{LD}$ of the pullback $\varphi^*\mathrm{LD}$ is exactly the rank $\operatorname{rank}\varphi$. In this case, the fundamental set $(\varphi^*\mathrm{LD})(\emptyset) = \ker\varphi$.

# 2 Integrality

## 2.1 Fundamentals

**Definition 2.1.1.** Let $R \subseteq S$ be a ring extension. We say that $\alpha$ is

(a) *algebraic* over $R$ if there is an integer $n \geq 1$ and $a_0, \ldots, a_n \in R$ with $a_0 \neq 0$ such that

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \text{ and}$$

(b) *integral* over $R$ if it is algebraic and in the above we can choose $a_0 = 1$, and more generally
(c) *integral over an ideal* $\mathfrak{a} \subseteq R$ if it is algebraic and in the above we can choose $a_0 = 1$ and $a_1, \ldots, a_n \in \mathfrak{a}$.

Every element of $R$ is integral over $R$. If $R$ and $S$ are fields, then the two notions of algebraicity and integrality coincide. The classical examples of integral elements are the algebraic integers $\mathcal{O}_{\overline{\mathbf{Q}}} \subset \mathbf{C}$.

**Definition 2.1.2** (Integral Closure/Normalization)**.**

(a) If $R \subseteq S$ is an extension, then the subset of elements of $S$ that are integral over $R$ is called the *(relative) integral closure* or the *(relative) normalization* of $R$ in $S$. We denote it by $\mathrm{Cl}_S(R)$. The subring $R$ is said to be *integrally closed* or *relatively normal* in $S$ if $R = \mathrm{Cl}_S(R)$. On the other hand, we say that the extension $S \subseteq R$ is *integral* iff $\mathrm{Cl}_S(R) = S$.
(b) If $R$ is an integral domain, then the normalization $\mathrm{Cl}_{\mathrm{Frac}(R)}(R)$ is called the *(absolute) integral closure* or *(absolute) normalization* of $R$. The domain $R$ is said to be *integrally closed* or *normal* if $R = \mathrm{Cl}_{\mathrm{Frac}(R)}(R)$.

**Theorem 2.1.3** (Robust Characterizations of Integrality)**.** Let $R \subseteq S$ be a ring extension and $\alpha \in S$ an element. Then TFAE:

(a) The element $\alpha$ is integral over $R$.
(b) The subring $R[\alpha]$ is a finitely generated $R$-module.
(c) The subring $R[\alpha]$ is contained in a subring $R' \subseteq S$ which is a finitely generated $R$-module.
(d) There is a faithful $R[\alpha]$-module $M$ that is finitely generated as an $R$-module.

*Proof.* The implications (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d) are trivial. For (d) $\Rightarrow$ (a), apply Corollary 1.6.2 with $\mathfrak{a} = (1)$. ∎

**Corollary 2.1.4** (Properties of Integral Extensions)**.** Let $R \subseteq S \subseteq T$ be ring extensions.

(a) If $\alpha_1, \ldots, \alpha_n \in S$ are any elements over $R$, then the subalgebra $R[\alpha_1, \ldots, \alpha_n] \subseteq S$ is a finitely generated $R$-module iff all the $\alpha_i$ are integral over $R$.
(b) The normalization $\mathrm{Cl}_S(R)$ is a subring of $S$ containing $R$.
(c) (Transivity) If $T/S$ and $S/R$ are integral, then so is $T/R$.
(d) (Idempotence) The normalization $\mathrm{Cl}_S(\mathrm{Cl}_S\, R) = \mathrm{Cl}_S\, R$, i.e. $\mathrm{Cl}_S\, R$ is integrally closed in $S$.

*Proof.* For (a), note that the "only if" direction follows from Theorem 2.1.3(c). For the "if", proceed by induction on $n$; when $n = 1$, this follows from Theorem 2.1.3(b). When $n \geq 2$, define $R' := R[\alpha_1, \ldots, \alpha_{n-1}]$; by induction, this is a finitely generated $R$-module. Since $\alpha_n$ is integral over $R$, it is also integral over $R'$ and so by the $n = 1$, we have $R'[\alpha_n]$ is a finitely generated $R'$-module. By transitivity of module-finiteness, we conclude that $R[\alpha_1, \ldots, \alpha_n]$ is a finitely generated $R$-module. For (b), note that if $\alpha, \beta \in S$ are integral, then $R[\alpha, \beta]$ is a finitely generated $R$-module by (a), and so $R[\alpha - \beta], R[\alpha\beta] \subseteq R[\alpha, \beta]$ implies by Theorem 2.1.3(c) that $\alpha - \beta, \alpha\beta \in \mathrm{Cl}_S(R)$. For (c), suppose that $t \in T$ satisfies $t^n + s_1 t^{n-1} + \cdots + s_n = 0$ with $s_i \in S$. By (a), $S' := R[s_1, \ldots, s_n]$ is a finitely generated $R$-module. Since $t$ is integral over $S'$, we conclude that $S'[t]$ is a finitely generated $S'$-module. Again, by transitivity of module finiteness, we conclude that $S'[t]$ is a finitely generated $R$-module, so Theorem 2.1.3(c) shows that $t$ is integral over $R$. Finally, (d) follows immediately from (c) because by definition $\mathrm{Cl}_S(R)/R$ is integral. ∎

**Example 2.1.5.**

(a) The generalized rational root theorem says exactly that every UFD is normal.
(b) Let $K/\mathbf{Q}$ be an algebraic extension (e.g. a number field). Then the integral closure $\mathrm{Cl}_K(\mathbf{Z}) =: \mathcal{O}_K$ is called the *ring of algebraic integers* in $K$. It is easy to see that $K = (\mathbf{Z} \smallsetminus \{0\})^{-1}\mathcal{O}_K = \mathrm{Frac}\, \mathcal{O}_K$. By idempotence, $\mathcal{O}_K$ is normal but in general not a UFD (e.g. for $K := \mathbf{Q}[\sqrt{-23}]$).
(c) Here is an example of a domain that is not normal: the coordinate ring of a planar cuspidal curve. Let $k$ be a field and look at $R := k[X, Y]/(Y^2 - X^3)$. Since $Y^2 - X^3 \in k[X, Y]$ is irreducible and $k[X, Y]$ is a PID, $R$ is

an integral domain; let $K := \operatorname{Frac} R$. Let $x$ and $y$ denote the classes of $X$ and $Y$ respectively in $R$, so $y^2 = x^3$. Then $0 \neq x, y \in R$ and so we may look at the element $t := y/x \in K$. Then $t^2 - x = 0$, so $t \in \mathrm{Cl}_K(R)$, but $t \notin R$: else $Y = FX + G(Y^2 - X^3)$ for some $F, G \in k[X, Y]$, which is impossible. In fact, it is easy to see from an explicit isomorphism $K \cong k(t)$ that $\mathrm{Cl}_K(R) = R[t]$.

**Lemma 2.1.6.** Let $R \subseteq S$ be an integral extension.

(a) If $\mathfrak{b} \subseteq S$ is an ideal and $\mathfrak{a} := \mathfrak{b} \cap R$, then $S/\mathfrak{b}$ is integral over $R/\mathfrak{a}$.
(b) If $U \subseteq R$ is a multiplicative system, then $U^{-1}S$ is integral over $U^{-1}R$.
(c) If $S$ is a domain, then $R$ is a field iff $S$ is.
(d) If $\mathfrak{p} \subset R$ and $\mathfrak{q} \subset S$ are primes such that $\mathfrak{q} \cap R = \mathfrak{p}$, then $\mathfrak{p}$ is maximal iff $\mathfrak{q}$ is.

*Proof.* The statements (a) and (b) are clear. For (c), first assume that $R$ is a field and let $0 \neq s \in S$. There is an $n \geq 1$ and $a_i \in R$ such that $s^n + a_1 s^{n-1} + \cdots + a_n = 0$. Since $S$ is a domain, we can assume that $a_n \neq 0$, so since $R$ is a field $a_n^{-1} \in R$. Then $-a_n^{-1}(s^{n-1} + a_1 s^{n-2} + \cdots + a_{n-1}) \in S$ is a multiplicative inverse for $s$. Conversely, if $S$ is a field and $0 \neq r \in R$, then there is an $r^{-1} \in S$ and so there is an $n \geq 1$ and $a_i \in R$ such that $r^{-n} + a_1 r^{-n+1} + \cdots + a_n = 0$. Multiplying by $r^{n-1}$ gives us $r^{-1} = -(a_1 + a_2 r + \cdots + a_n r^{n-1}) \in R$. For (d), apply (a) and (c) to $R/\mathfrak{p} \subseteq S/\mathfrak{q}$. ∎

**Counterexample 2.1.7.** The part (c) of Lemma 2.1.6 needs $S$ to be a domain. A simple counterexample otherwise is $k \subseteq k[x]/(x^2)$.

We talk a little about integrality for domains.

**Lemma 2.1.8.** Let $R$ be an integral domain with $K := \operatorname{Frac} R$. Then:

(a) We have $R = \bigcap_{\mathfrak{p}} R_{\mathfrak{p}} = \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ (where the intersections are in $K$).
(b) If $S \subseteq R$ is any multiplicative subset, then $\mathrm{Cl}_K(S^{-1}R) = S^{-1}\,\mathrm{Cl}_K(R)$.
(c) If $R$ is normal, then every localization $S^{-1}R$ is too.
(d) TFAE:
  (i) $R$ is normal.
  (ii) $R_{\mathfrak{p}}$ is normal for all $\mathfrak{p}$.
  (iii) $R_{\mathfrak{m}}$ is normal for all $\mathfrak{m}$.

*Proof.* For (a), the inclusions $R \subseteq \bigcap_{\mathfrak{p}} R_{\mathfrak{p}} \subseteq \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ are clear; and if $x \in \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$, then for all $\mathfrak{m}$ we have $(R :_R x) \not\subseteq \mathfrak{m}$, and hence $(R :_R x) = (1)$, i.e. $x \in R$. For (b), note that by Lemma 2.1.6(b) we have $S^{-1}\,\mathrm{Cl}_K(R) \subseteq \mathrm{Cl}_K(S^{-1}R)$. Conversely, if $x \in \mathrm{Cl}_K(S^{-1}R)$, then there is an integer $n \geq 1$ and elements $a_i \in R, s_i \in S$ such that $x^n + s_1^{-1}a_1 x^{n-1} + \cdots + s_n^{-1}a_n = 0$. Define $s := s_1 \ldots s_n \in S$, and multiply throughout by $s^n$ to get that $sx \in \mathrm{Cl}_K(R)$, i.e. that $x \in S^{-1}\,\mathrm{Cl}_K(R)$. The implication (b) ⇒ (c) is trivial. For (d), the implication (i) ⇒ (ii) follows from (c), the implication (ii) ⇒ (iii) is trivial, and for (iii) ⇒ (i), if an element of $K$ is integral over $R$, then it is integral over $R_{\mathfrak{m}}$ for all $\mathfrak{m}$ and hence it belongs to $\bigcap_{\mathfrak{m}} R_{\mathfrak{m}} = R$. ∎

Finally, we touch the topic of integrality over an ideal.

**Lemma 2.1.9.** Let $R \subseteq S$ be a ring extension, and let $\mathfrak{a} \subseteq R$ be an ideal.

(a) The collection $\mathrm{Cl}_S(\mathfrak{a})$ of elements of $S$ integral over $\mathfrak{a}$ is exactly the radical $\sqrt{\mathfrak{a}\,\mathrm{Cl}_S(R)} \subseteq \mathrm{Cl}_S(R)$.
(b) If $S$ is a domain, then given an $\alpha \in \mathrm{Cl}_S(\mathfrak{a})$ if we write $\mu_\alpha(T) = T^n + a_1 T^{n-1} + \cdots + a_n \in (\operatorname{Frac} R)[T]$, then for each $i$ we have $a_i \in \sqrt{\mathrm{Cl}_S(\mathfrak{a})}$.
(c) In particular, in (b), if $R$ is normal, then the coefficients $a_i \in \sqrt{\mathfrak{a}}$.

*Proof.* For (a), if $x \in \mathrm{Cl}_S(\mathfrak{a})$ and $n \geq 1, a_i \in \mathfrak{a}$ are such that $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, then $x^n \in \mathfrak{a}\,\mathrm{Cl}_S(R)$ so $x \in \sqrt{\mathfrak{a}\,\mathrm{Cl}_S(R)}$. Conversely, if $x \in \sqrt{\mathfrak{a}\,\mathrm{Cl}_S(R)}$, then $x^n = \sum_j \alpha_j x_j$ for some $n \geq 1, \alpha_j \in \mathfrak{a}, x_j \in \mathrm{Cl}_S(R)$. Since each $x_j$ is integral over $R$, the ring $M := R[x_j]_j$ is a finitely generated $R$-module and $x^n M \subseteq \mathfrak{a}M$. By Observation 1.6.1, we have that $x^n + a_1 x^{n-1} + \cdots + a_n = 0 \in \mathrm{End}_R(M)$ for some $a_i \in \mathfrak{a}$, but since $1 \in M$, we have this identity in $S$. For (b), let $K := \operatorname{Frac} R$ and $L = \operatorname{Frac} S$ and look at the roots $\alpha_j$ of $\mu_\alpha$ in some $\overline{L}$. These also satisfy the same equation of integral dependence and so belong to $\mathrm{Cl}_S(\mathfrak{a})$; since the coefficients $a_i$ are polynomials in the $\alpha_i$, they belong to $\mathrm{Cl}_S(\mathfrak{a})$ as well. For (c), using (b) the $a_i \in \sqrt{\mathfrak{a}\,\mathrm{Cl}_S(R)} = \sqrt{\mathfrak{a}}$. ∎

## 2.2 Cohen-Seidenberg Theory

**Theorem 2.2.1** (Lying Over and Incomparability)**.** Let $R \subseteq S$ be an integral extension and $\mathfrak{p} \subset R$ a prime.

(a) (Lying Over) There is a prime $\mathfrak{q} \subset S$ such that $\mathfrak{q} \cap R = \mathfrak{p}$.
(b) (Incomparability) There are no inclusions between distinct primes $\mathfrak{q}$ of $S$ lying over $\mathfrak{p}$.

*Proof.* For (a), by Corollary 1.2.9, it suffices to show that $\mathfrak{p}S \cap R \subseteq \mathfrak{p}$. If $x \in \mathfrak{p}S \cap R$, then $x \in \sqrt{\mathfrak{p}S}$, so by Lemma 2.1.9(a), we have $x \in \mathrm{Cl}_S(\mathfrak{p})$ and so $x^n \in \mathfrak{p}$ for some $n \geq 1$, which shows that $x \in \mathfrak{p}$ by primality. For an alternative proof which also shows (b), localize both sides at $U := R \setminus \mathfrak{p}$ and use Lemma 2.1.6(b) to conclude that $S_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}S$ is integral over $R_{\mathfrak{p}}$. Then prime ideals of $S$ lying over $\mathfrak{p}$ are in canonical bijection with prime ideals of $S_{\mathfrak{p}}$ lying over $\mathfrak{p}R_{\mathfrak{p}}$, and so we reduce to the case that $R$ is local with $\mathfrak{p} = \mathfrak{m}$ the maximal ideal. For (a), note that if $\mathfrak{n} \subset S$ is any maximal ideal, then $\mathfrak{n} \cap R$ is maximal by Lemma 2.1.6(d) and so $\mathfrak{n} \cap R = \mathfrak{m}$ and $\mathfrak{n}$ lies over $S$. Conversely, if $\mathfrak{n} \subset S$ is a prime that satisfies $\mathfrak{n} \cap R = \mathfrak{m}$, then again by Lemma 2.1.6(d), $\mathfrak{n}$ is maximal; in particular, there are no inclusions between distinct such $\mathfrak{n}$. ∎

**Definition 2.2.2.** A ring extension $R \subseteq S$ satisfies

(a) *the going up property* if given any $n \geq 1$ and chain $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ of primes in $R$ and $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ in $S$ for some $0 \leq m < n$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq m$, the ascending chain of ideals can be completed: there are primes $\mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n$ in $S$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all $i$; and
(b) *the going down property* if given any $n \geq 1$ and chain $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ of primes in $R$ and $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ in $S$ for some $0 \leq m < n$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq m$, the descending chain of ideals can be completed: there are primes $\mathfrak{q}_{m+1} \supseteq \cdots \supseteq \mathfrak{q}_n$ in $S$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all $i$.

**Theorem 2.2.3** (Cohen-Seidenberg)**.**

(a) (Going Up) Any integral extension satisfies the going up property.
(b) (Going Down) If $R \subseteq S$ is integral with $S$ a domain and $R$ normal, then $R \subseteq S$ satisfies going down.

*Proof.* By Lying Over (Theorem 2.2.1(a)) and induction, we are immediately reduced to the case $n = 2, m = 1$.

(a) By Lemma 2.1.6(a), we have that $S/\mathfrak{q}_1$ is integral over $R/\mathfrak{p}_1$, so by Lying Over (Theorem 2.2.1(a)), there is a prime $\overline{\mathfrak{q}}_2$ of $S/\mathfrak{q}_1$ lying over $\mathfrak{p}_2/\mathfrak{p}_1$. Lifting to $S$, we get a prime $\mathfrak{q}_2$ of $S$ lying over $\mathfrak{p}_2$.
(b) It suffices to show using Corollary 1.2.8(d) and Corollary 1.2.9 that $\mathfrak{p}_2 S_{\mathfrak{q}_1} \subseteq \mathfrak{p}_2$. If $x \in \mathfrak{p}_2 S_{\mathfrak{q}_1}$, then $sx = y$ for some $s \in S \setminus \mathfrak{q}_1$ and $y \in \mathfrak{p}_2 S$. If the minimal polynomial of $y$ over $K := \mathrm{Frac}\, R$ is $\mu_y = T^n + a_1 T^{n-1} + \cdots + a_n \in K[T]$ then each $a_i \in \mathfrak{p}$ by Lemma 2.1.9(b). If $x \in \mathfrak{p}_2 S_{\mathfrak{q}_1} \cap R \setminus 0$, then $s = yx^{-1}$ with $x^{-1} \in K$, so the minimal polynomial of $s$ over $K$ is given by $\mu_s = T^n + b_1 T^{n-1} + \cdots + b_n \in K[T]$ with $b_i = x^{-i} a_i$. But $s$ is integral over $R$, so by Lemma 2.1.9(b) with $\mathfrak{a} = (1)$ we have $b_i \in R$ for each $i$. If $x \notin \mathfrak{p}_2$, then $x^i b_i = a_i \in \mathfrak{p}_2 \Rightarrow b_i \in \mathfrak{p}_2$ for all $i$ so that $s^n \in \mathfrak{p}_2 S \subseteq \mathfrak{p}_1 S \subseteq \mathfrak{q}_1$, which is a contradiction to $s \notin \mathfrak{q}_1$.

∎

**Corollary 2.2.4.** Let $R \subseteq S$ be an integral extension. Then

(a) $\dim R = \dim S$.

If $\mathfrak{p} \subset R$ and $\mathfrak{q} \subset S$ are primes with $\mathfrak{q} \cap R = \mathfrak{p}$, then

(b) $\mathrm{coht}\, \mathfrak{p} = \mathrm{coht}\, \mathfrak{q}$,
(c) $\mathrm{ht}\, \mathfrak{p} \geq \mathrm{ht}\, \mathfrak{q}$, and
(d) equality holds in (c) if the conditions in Theorem 2.2.3(b) (or more generally Theorem 2.2.7) hold.

*Proof.* For (a), note that Going Up and incomparability (Theorem 2.2.3(a) and Theorem 2.2.1(b)) give us a canonical bijection between (strict) chains of primes in $R$ and $S$. For (b), note that $S/\mathfrak{q}$ is integral over $R/\mathfrak{p}$ by Lemma 2.1.6(a), and so we are done by (a). If we have a chain of primes contained in $\mathfrak{q}$ of length $d$, then by intersecting with $R$ we get a chain of length $d$ in $R$ (where the inclusions are strict again by incomparability–Theorem 2.2.1(b)); this shows $\mathrm{ht}\, \mathfrak{p} \geq \mathrm{ht}\, \mathfrak{q}$. For (d), we can apply Going Down to go the other way. ∎

We will now give another proof of Going Down, for which we need a little preparation about extensions of normal domains that we do now.

**Definition 2.2.5.** Let $R$ be a normal domain with fraction field $K$. Let $L/K$ be a finite *Galois* extension of $K$ with Galois group $G := \mathrm{Gal}(L/K)$, and $S := \mathrm{Cl}_L(R)$. Then $S$ is also normal by idempotence and the fact that

$L = \operatorname{Frac} S$. Then $S$ is stable by the action of $G$. If $\mathfrak{p} \subset R$ is a prime, let $\mathcal{S}_\mathfrak{p}$ be the set of primes $\mathfrak{P} \subset S$ lying over $\mathfrak{p}$. Then $G$ acts on the set $\mathcal{S}_\mathfrak{p}$.

(a) For a $\mathfrak{P} \in \mathcal{S}_\mathfrak{p}$, we define its *decomposition group* $D_\mathfrak{P} \leq G$ to be the stabilizer under the $G$ action on $\mathcal{S}_\mathfrak{p}$.
(b) The kernel of the map $D_\mathfrak{P} \to \operatorname{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is called the *inertia subgroup* $I_\mathfrak{P}$ at $\mathfrak{P}$.
(c) The fixed field $L^{D_\mathfrak{P}}$ of $D_\mathfrak{P}$ is called the *decomposition field* of $\mathfrak{P}$, and the fixed field $L^{I_\mathfrak{P}}$ of $I_\mathfrak{P}$ is called the *inertia field* of $\mathfrak{P}$.
(d) We let $S^{D_\mathfrak{P}} := S \cap L^{D_\mathfrak{P}} = \operatorname{Cl}_{L^{D_\mathfrak{P}}}(R)$.

**Lemma 2.2.6.** In the setting of Definition 2.2.5, we have:

(a) The group $G$ acts transitively on the set $\mathcal{S}_\mathfrak{p}$, so $\mathcal{S}_\mathfrak{p}$ is finite. (The first result holds even if $L/K$ is only finite normal, and the second result holds even if $L/K$ is only finite separable.)
(b) The subgroups $D_\mathfrak{P}$ and $I_\mathfrak{P}$ are all conjugate under $G$.
(c) The field $L^{D_\mathfrak{P}}$ is the smallest intermediate extension $E$ such that $\mathfrak{P}$ is the only prime of $S$ lying over $\mathfrak{P} \cap E$.
(d) The canonical injection $R/\mathfrak{p} \hookrightarrow S^{D_\mathfrak{P}}/(\mathfrak{P} \cap S^{D_\mathfrak{P}})$ extends to an isomorphism $\kappa(\mathfrak{p}) \xrightarrow{\sim} \kappa(\mathfrak{P} \cap S^{D_\mathfrak{P}})$.
(e) The extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is is normal (so it is Galois if it is separable) and the homomorphism $D_\mathfrak{P}/I_\mathfrak{P} \to \operatorname{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is an isomorphism.

*Proof.* First note that we may replace $R$ and $S$ by $R_\mathfrak{p}$ and $S_\mathfrak{p} := (R \smallsetminus \mathfrak{p})^{-1}S$ by Corollary 1.2.8(e) and Lemma 2.1.8(b) to assume that $R$ is local with maximal ideal $\mathfrak{p}$; then the primes $\mathfrak{P}$ above it are also maximal by Lemma 2.1.6(d).

For (a), we only assume that $L/K$ is finite normal and $G = \operatorname{Aut}(L/K)$. Suppose we have $\mathfrak{P}, \mathfrak{Q} \in \mathcal{S}_\mathfrak{p}$ such that $\mathfrak{P} \neq \sigma\mathfrak{Q}$ for any $\sigma \in G$. Since by incomparability (Theorem 2.2.1(b)) $\mathfrak{P} \not\subseteq \sigma\mathfrak{Q}$ for any $\sigma \in G$, by Prime Avoidance (Lemma 1.1.3(b)) is an $x \in \mathfrak{P} \smallsetminus \bigcup_{\sigma\in G} \sigma\mathfrak{Q}$. Alternatively, since the elements of $\mathcal{S}_\mathfrak{p}$ are pairwise distinct maximal ideals, they are pairwise relatively prime; by the CRT, there is an $x \in S$ such that $x \equiv 0 \pmod{\mathfrak{P}}$ and $x \equiv 1 \pmod{\sigma\mathfrak{Q}}$ for all $\sigma$. Then by Lemma 2.1.9(c) (taking $\mathfrak{a} = 1$), the norm $\mathrm{N}_K^L(x) = \prod_{\sigma\in G} \sigma x \in R$ and in fact in $R \cap \mathfrak{P} = \mathfrak{p}$. But $\sigma x \notin \mathfrak{Q}$ for all $\mathfrak{Q}$, so by primality $\mathrm{N}_K^L(x) \notin \mathfrak{Q}$, contradicting that $\mathrm{N}_K^L(x) \in \mathfrak{p} = \mathfrak{Q} \cap R$. If $L/K$ is only finite separable, then by Lying Over, every prime $\mathfrak{P} \in \mathcal{S}_\mathfrak{p}$ lies below a prime of $\operatorname{Cl}_N(R)$ lying over $\mathfrak{p}$, and there are only finitely many of the latter by what we have shown. The claim in (b) follows immediately from (a), since $D_{\sigma\mathfrak{P}} = \sigma D_\mathfrak{P} \sigma^{-1}$ and $I_{\sigma\mathfrak{P}} = \sigma I_\mathfrak{P} \sigma^{-1}$.

For (c), Let $E$ be as above and $H = \operatorname{Gal}(L/E)$. By (a), all primes of $S$ lying over $\mathfrak{P} \cap E$ are conjugate under $H$ and so since there's only one such prime, it follows that $H \leq D_\mathfrak{P}$ and so by the Fundamental Theorem of Galois Theory (Theorem **??**) we have $E = L^H \supseteq L^{D_\mathfrak{P}}$. For (d), given a $\sigma \in G$, let $\mathfrak{Q}_\sigma := \sigma^{-1}\mathfrak{P} \cap S^{D_\mathfrak{P}}$ (and let $\mathfrak{Q} := \mathfrak{Q}_1$). If $\sigma \notin D_\mathfrak{P}$, then by (c) we have $\mathfrak{Q}_\sigma \neq \mathfrak{Q}$. Given any $x \in S^{D_\mathfrak{P}}$, by the CRT there is a $y \in S^{D_\mathfrak{P}}$ such that $y \equiv x \pmod{\mathfrak{Q}}$ and $y \equiv 1 \pmod{\mathfrak{Q}_\sigma}$ for all $\sigma \notin D_\mathfrak{P}$; so in particular $y \equiv x \pmod{\mathfrak{P}}$ and $y \equiv 1 \pmod{\sigma^{-1}\mathfrak{P}}$ for each $\sigma \notin D_\mathfrak{P}$ and hence $\sigma y \equiv 1 \pmod{\mathfrak{P}}$ for each $\sigma \notin D_\mathfrak{P}$. Now the norm $\mathrm{N}_K^{L^{D_\mathfrak{P}}}$ is a product of $y$ and other factors $\sigma y$ with $\sigma \notin D_\mathfrak{P}$, so it follows that $\mathrm{N}_K^{L^{D_\mathfrak{P}}}(y) \equiv x \pmod{\mathfrak{P}}$. Now the LHS lies in $R$ by Lemma 2.1.9, and so this last congruence holds in $S^{D_\mathfrak{P}}$, which says that the map $\kappa(\mathfrak{p}) \to \kappa(\mathfrak{Q})$ is surjective as needed.

For (e), note by integrality of $S$ that $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is algebraic. To show that $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is normal, we have to show the minimal polynomial of any element in $\kappa(\mathfrak{P})$ splits completely in $\kappa(\mathfrak{P})$. If $\overline{x} \in \kappa(\mathfrak{P})$ is any element and $x \in S$ any lift of $S$, then since $L/K$ is normal $\mu_x \in K[T]$ (where $K = \operatorname{Frac} R$) has coefficients in $R$ by Lemma 2.1.9(c) and hence splits into linear factors with all roots in $S$. Since $\mu_{\overline{x}} \mid \overline{\mu_x} \in \kappa(\mathfrak{P})$, we have that $\mu_{\overline{x}}$ has all its roots in $\kappa(\mathfrak{P})$ as well. For the second statement, we need to show surjectivity of $D_\mathfrak{P} \to \operatorname{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. By (d), we may replace $K$ by $L^{D_\mathfrak{P}}$ and $G$ by $D_\mathfrak{P}$ to assume that $\mathfrak{P}$ is the only prime of $S$ lying over $\mathfrak{p}$. Let $\overline{x}$ be a primitive element for the maximal separable extension $\kappa(\mathfrak{p})$ in $\kappa(\mathfrak{P})$ and $\overline{\sigma} \in \operatorname{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) = \operatorname{Aut}(\kappa(\mathfrak{p})[\overline{x}]/\kappa(\mathfrak{p}))$. Then $\overline{\sigma x}$ is a root of $\mu_{\overline{x}}$ and hence of $\overline{\mu_x}$, i.e. there is a zero $y$ of $\mu_x$ such that $y \equiv \overline{\sigma x} \pmod{\mathfrak{P}}$. Since $y$ is a zero of $\mu_x$, there is a $\sigma \in G$ such that $y = \sigma x$; then $\sigma x \equiv \overline{\sigma x} \pmod{\mathfrak{P}}$ means that $\sigma \in G$ maps to $\overline{\sigma} \in \operatorname{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. ∎

Given this, we give another proof of Going Down.

*Another Proof of Theorem 2.2.3(b).* Let $K = \operatorname{Frac} R$ and $L = \operatorname{Frac} S$. First suppose that $L/K$ is finite, and let $N$ be the normal closure of $L$; then $N/K$ is finite as well. Let $T = \operatorname{Cl}_N(R)$. By Going Up, there are primes $\mathfrak{P}_1 \supseteq \mathfrak{P}_2$ of $T$ over $\mathfrak{p}_1 \supseteq \mathfrak{p}_2$ in $R$. By Lying Over there is a prime $\mathfrak{P}_1' \subset T$ lying over $\mathfrak{q}_1$ and hence also over $\mathfrak{p}_1$. By Lemma 2.2.6(a), there is an automorphism $\sigma \in \operatorname{Gal}(N/K)$ such that $\sigma\mathfrak{P}_1 = \mathfrak{P}_1'$. Then $\mathfrak{q}_2 := \sigma\mathfrak{P}_2 \cap S$ works. In general, [to be done].

∎

As a final aside, we show a slightly stronger version of Going Down following the paper by Cohen and Seidenberg.

**Theorem 2.2.7** (Stronger Going Down)**.**

This is in some sense the strongest version possible, and Cohen-Seidenberg give counterexamples to show that none of the hypotheses can be dropped.

## 2.3 Extensions of Homomorphisms to Algebraically Closed Fields

**Lemma 2.3.1.** Let $R \subseteq S$ be a ring extension and $\Omega$ be an algebraically closed field. Let $\varphi : R \to \Omega$ be a homomorphism; we ask when it extends to a homomorphism $S \to \Omega$.

(a) If $R \subseteq S$ is integral, then $\varphi$ extends to homomorphism $\hat{\varphi} : S \to \Omega$.
(b) If $S$ is a domain and finitely generated $R$-algebra, then $\varphi$ extends to a homomorphism $\hat{\varphi} : S \to \Omega$. In fact, given any $0 \neq s \in S$ there is a $0 \neq r \in R$ such if $\varphi(r) \neq 0$, then $\hat{\varphi}$ can be chosen to satisfy $\hat{\varphi}(s) \neq 0$.
(c) If $S$ is a field, then given any $0 \neq \alpha \in S$, we have that $\varphi$ extends to either $R[\alpha] \to \Omega$ or $R[\alpha^{-1}] \to \Omega$. In particular, maximal extension ring $T$ of $\varphi$ in $S$ satisfies that for any $0 \neq \alpha \in S$ we have either $\alpha \in T$ or $\alpha^{-1} \in T$.

*Proof.* For (a), let $\mathfrak{p} := \ker\varphi$. Replacing $R$ by $R_{\mathfrak{p}}$ and $S$ by $S_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}S$ and using Lemma 2.1.6(b), we can reduce to the case when $(R, \mathfrak{m}, k)$ is local and $\ker\varphi = \mathfrak{m}$ is maximal. By Lying Over (Theorem 2.2.1(a)) and Lemma 2.1.6(d), there is a maximal $\mathfrak{n} \subseteq S$ such that $\mathfrak{n} \cap R = \mathfrak{m}$. Then $S/\mathfrak{n}$ is an algebraic extension of the field $k$ and $\Omega$ is an algebraically closed field containing $F := \varphi(k)$, so by Theorem 3.0.1(b) there is an extension $S/\mathfrak{n} \to \Omega$ extending $\varphi : k \to F$. Then $S \twoheadrightarrow S/\mathfrak{n} \to \Omega$ is an extension of $\varphi$.

For (b), by inducting on the minimal number of generators of $S$ as an $R$-algebra, we are reduced to the case $S = R[x]$. Suppose that $x$ is transcendental over $R$ and let $s = a_0x^n + \cdots + a_n$ for $a_i \in R$ with $a_0 \neq 0$. Define $r := a_0$. If $\varphi : R \to \Omega$ has $\varphi(a_0) \neq 0$, then there is an $\alpha \in \Omega$ such that $\varphi(a_0)\alpha^n + \cdots + \varphi(a_n) \neq 0$, since $\Omega$ is infinite. Then define $\hat{\varphi} : R[x] \to \Omega$ by sending $x \mapsto \alpha$. On the other hand, suppose that $x$ is algebraic; then so is $s$. Write down equations $a_0x^n + \cdots + a_n = 0$ and $b_0s^m + \cdots + b_m = 0$ satisfied by $x$ and $s$ with $n, m \geq 1$ and $a_i, b_j \in R$, and set $r := a_0b_m$. Then $S[r^{-1}] = R[r^{-1}][x]$ is integral over $R[r^{-1}]$. If $\varphi(r) \neq 0$, then it extends to $\varphi : R[r^{-1}] \to \Omega$ and hence by (a) to a $\hat{\varphi} : S[r^{-1}] \to \Omega$; the restriction of this to $S$ gives the required extension. This extension satisfies $\hat{\varphi}(s) \neq 0$ because if $\hat{\varphi}(s) = 0$, then $\varphi(b_m) = 0$ and so $\varphi(r) = 0$ as well.

For (c), as in (a) we may assume that $(R, \mathfrak{m}, k)$ is local and $\ker\varphi = \mathfrak{m}$ is maximal and we may let $F = \varphi(k)$ as before, so $\varphi : k \xrightarrow{\sim} F$. Let $\mathfrak{a} := \{f(X) \in R[X] : f(\alpha) = 0\} \subseteq R[X]$ and let $\mathfrak{b} := (\varphi(\mathfrak{a})) \subseteq F[X]$. Since $F[X]$ is a PID, we have $\mathfrak{b} = (\mu(X))$ for some $\mu(X) \in F[X]$. If $\mu(X)$ is either constantly 0 or nonconstant, then there is a $\beta \in \Omega$ such that $\mu(\beta) = 0$; then $\alpha \mapsto \beta$ gives an extension $R[\alpha] \to \Omega$. If $\mu(X)$ is a nonzero constant, then $\mathfrak{b} = (1)$. Since $\varphi : k \xrightarrow{\sim} F$, this implies that there is an $f(X) \in R[X]$ such that $\varphi(f)(X) = 1$, which is to say that there is an integer $n \geq 1$ and elements $a_0, \ldots, a_n \in R$ such that $a_0\alpha^n + \cdots + a_n = 0$ and $\varphi(a_0) = \varphi(a_1) = \cdots = \varphi(a_{n-1}) = \varphi(a_n) - 1 = 0$, and we can choose $n$ to be the smallest integer with this property, and by replacing $a_i$ by $a_ia_n^{-1}$, we may assume that $a_n = 1$ (this last is justified by the fact that $1 - a_n \in \ker\varphi = \mathfrak{m} = \operatorname{Jac} R \Rightarrow a_n \in R^\times$). The claim is that this latter case cannot hold for both $\alpha$ and $\alpha^{-1}$; indeed, suppose that $m \geq 1$ is the smallest integer for which there are $b_0, \ldots, b_{m-1} \in R$ and $b_0\alpha^{-m} + \cdots + b_{m-1}\alpha^{-1} + 1 = 0$ with $\varphi(b_0) = \cdots = \varphi(b_{m-1}) = 0$. We may assume WLOG that $n \geq m$. Multiplying throughout by $a_0\alpha^n$, we get the relation $a_0\alpha^n + a_0b_{m-1}\alpha^{n-1} + \cdots + a_0b_0\alpha^{n-m} = 0$. Here we have two cases. If $n = m$, then subtracting the two leaves us with $(a_1 - a_0b_{n-1})\alpha^{n-1} + \cdots + (1 - a_0b_0) = 0$. In this all coefficients of $\alpha^j$ for $j > 0$ reduce under $\varphi$ to 0, whereas the constant term reduces to 1; in particular, we must have $n \geq 2$, and this equation contradicts the minimality of $n$. The case $n > m$ is even easier because already $n \geq 2$ and the constant term is simply 1. ∎

# 3 Field Theory and Galois Theory

This set of notes is based on Szamuely, Lang, Cohn, Sam's notes, Matsumura, Fröhlich-Taylor, various online sources including Keith Conrad's notes, the Stacks project. We will assume the following, which is proved using Zorn's Lemma:

**Theorem 3.0.1.** Let $k$ be a field.

(a) There is an algebraic closure $\overline{k}$ of $k$, i.e. an algebraic extension that is itself algebraically closed. It is unique upto (non-unique) isomorphism. From now on, we will assume $k$ to be embedded in an algebraic closure $\overline{k}$ in a fixed manner.
(b) If $L/k$ is an algebraic extension and $\Omega$ any algebraically closed field containing $k$ (say $\Omega = \overline{k}$), then there is an embedding $L \to \Omega$ fixing $k$ elementwise.
(c) In the previous situation, take an algebraic closure $\overline{L}$ of $L$. Then the embedding $L \to \overline{k}$ can be extended to an isomorphism $\overline{L} \to \overline{k}$.

## 3.1 Separability I

**Definition 3.1.1.** A polynomial $f \in k[x]$ is separable if $f$ has no repeated roots in $\overline{k}$. An element of an algebraic extension $L/k$ is separable over $k$ if its minimal polynomial is separable; the extension $L/k$ is itself separable if all of its elements are separable over $k$.

**Lemma 3.1.2.**

(a) A nonconstant $f \in k[x]$ is separable iff $(f, f') = 1$.
(b) If $f$ is irreducible, then it is separable unless $f' = 0$.

*Proof.* For any $\alpha \in \overline{k}$, we can write $f = f(\alpha) + (x-\alpha)f'(\alpha) + (x-\alpha)^2 g$ for some $g \in \overline{k}[x]$. Therefore, $(x-\alpha)^2 \mid f$ in $\overline{k}[x]$ iff $f(\alpha) = f'(\alpha) = 0$. Therefore, $f$ has no repeated roots in $\overline{k}$ iff $f$ and $f'$ don't share a common root in $\overline{k}$ iff $(f, f') = 1$ (one way to show this quickly is to use that $k[x]$ is a PID). To show the second part, note that if $f' \neq 0$, then $\deg f' < \deg f$ and so $(f, f')$ is a factor of $f$ of strictly smaller degree and so if $f$ were irreducible, then $(f, f')$ would have to be a unit. ∎

**Counterexample 3.1.3.** $\mathbf{F}_p(t)[t^{1/p}] := \mathbf{F}_p(t)[x]/(x^p - t)$ of $\mathbf{F}_p(t)$ is not separable: $\mu_{t^{1/p}} = x^p - t \in \mathbf{F}_p(t)[x]$.

**Theorem 3.1.4** (Perfect Fields)**.** For a field $k$, TFAE:

(a) Either $\operatorname{char} k = 0$ or $\operatorname{char} k = p > 0$ and every element of $k$ is a $p^{\text{th}}$ power.
(b) Every algebraic extension of $k$ is separable.

In this case:

(c) Any algebraic extension of $k$ also satisfies (a) and (b).

*Proof.* For the implication (a) ⇒ (b), suppose that $k$ satisfies (a) and let $L/k$ be algebraic. Take any $\alpha \in L$ and consider its minimal polynomial $\mu_\alpha \in k[x]$. It is nonconstant and irreducible. If $\operatorname{char} k = 0$, then this automatically implies that $\mu'_\alpha \neq 0$, so we are done by Lemma 3.1.2(b). If $\operatorname{char} k = p > 0$ and $\mu'_\alpha = 0$, then we must have $\mu_\alpha(x) = a_0 x^{pn} + a_p x^{p(n-1)} + \cdots + a_{pn}$ for some coefficients $a_{pi} \in k$ for $i = 0, \ldots, n$. Since $k$ satisfies (a), each $a_{pi} = b_i^p$ for some $b_i \in k$ and then $\mu_\alpha(x) = (b_0 x^n + b_1 x^{n-1} + \cdots + b_n)^p$, contradicting the irreducibility of $\mu_\alpha$. Therefore, $\mu'_\alpha \neq 0$ and again we are done by Lemma 3.1.2(b). For the implication (b) ⇒ (a), suppose that every algebraic extension of $k$ is separable. If $\operatorname{char} k = 0$, we are done. If $k$ has characteristic $p > 0$, let $a \in k^\times$ be arbitrary. We have to show that it's a $p^{\text{th}}$ power. For that, look at $f = x^p - a$. If $b \in \overline{k}$ is a root of $f$, then the extension $k[b]$ of $k$ is algebraic and hence separable by hypothesis. The minimal polynomial $\mu_b \in k[x]$ of $b$ divides $f = (x-b)^p$ in $\overline{k}[x]$ and so must be of the form $(x-b)^j$ for some $1 \leq j \leq p$. But since $b$ is separable over $k$, we must have $j = 1$. In particular, $\mu_b(x) = x - b$ and this forces $b \in k$. For (c), let $M/k$ be an algebraic extension. If $L/M$ is an algebraic extension, then so is $L/k$ so is separable. If $\alpha \in L$ is any element, then $\mu_{\alpha,M} \in M[x]$ divides $\mu_{\alpha,k} \in k[x]$ in $M[x]$; since $\mu_{\alpha,k}$ has no repeated roots in $\overline{k}$, then neither can $\mu_{\alpha,M}$. In particular, $L/M$ is separable. ∎

**Definition 3.1.5.** A field satisfying the equivalent conditions of Theorem 3.1.4 is said to be *perfect*.

**Example 3.1.6.** All fields of characteristic zero, all algebraically closed fields and all finite fields are perfect. By Counterexample 3.1.3, $\mathbf{F}_p(t)$ is not perfect.

**Definition 3.1.7.** Given an algebraic extension $L/k$, we define its *separable degree* $[L : k]_s$ to be the number of distinct $k$-algebra homomorphisms $L \to \overline{k}$.

Note that separable degree is also multiplicative in towers: if $L/M/k$ is a tower of extensions, then $[L : k]_s = [L : M]_s[M : k]_s$; the restriction map $\mathrm{Hom}_k(L, \overline{k}) \to \mathrm{Hom}_k(M, \overline{k})$ is surjective with all fibers isomorphic to $\mathrm{Hom}_M(L, \overline{M})$ (where we're using the isomorphism $\overline{M} \to \overline{k}$ offered by Theorem 3.0.1(c)).

**Proposition 3.1.8.** Suppose that $L/k$ is a finite extension. Then $1 \leq [L : k]_s \leq [L : k]$. Further, the following are equivalent:

(a) We have $[L : k]_s = [L : k]$.
(b) The extension $L/k$ is separable.
(c) The extension $L/k$ is separably generated, i.e. there are finitely many separable $\alpha_1, \ldots, \alpha_m \in L$ such that $L = k[\alpha_1, \ldots, \alpha_m]$.

*Proof.* Since $L/k$ is finite, we can write $L = k[\alpha_1, \ldots, \alpha_m]$ for finitely many elements $\alpha_i \in k$. We induct on $m$. When $m = 0$, this is clear. When $m = 1$, we have $L = k[\alpha]$ and $n := [L : k] = \deg \mu_\alpha$. A $k$-homomorphism $L \to \overline{k}$ is then determined by the image of $\alpha$, which must be one of the roots of $\mu_\alpha$ contained in $\overline{k}$; there are at least one and at most $n$ of these (with equality iff $\alpha$ is separable). When $m > 1$, let $M := k[\alpha_1, \ldots, \alpha_{m-1}]$. Then $L = M[\alpha_m]$, so by the $m = 1$ case $1 \leq [L : M]_s \leq [L : M]$ and by induction $1 \leq [M : k]_s \leq [M : k]$. Therefore, $1 \leq [L : k]_s = [L : M]_s[M : k]_s \leq [L : M][M : k] = [L : k]$.

For (a) $\Rightarrow$ (b), suppose that $\alpha \in L$ is not separable over $k$. Then by the above discussion, $[k[\alpha] : k]_s < [k[\alpha] : k]$ and $[L : k[\alpha]]_s \leq [L : k[\alpha]]$ so $[L : k]_s = [L : k[\alpha]]_s[k[\alpha] : k]_s < [L : k[\alpha]][k[\alpha] : k] = [L : k]$. The implication (b) $\Rightarrow$ (c) is obvious, since $[L : k] < \infty$. For (c) $\Rightarrow$ (a), we again induct on $m \geq 0$ for which $L = k[\alpha_1, \ldots, \alpha_m]$ where $\alpha_i \in L$ are separable over $k$. If $m = 0$, the statement is clear. If $m = 1$ and $L = k[\alpha]$ then it is clear from the discussion above: since $\alpha$ is separable, $[L : k]_s = [L : k]$. If $m > 1$, then define $M$ as before. By induction, $[M : k]_s = [M : k]$. Since $L = M[\alpha_m]$ and $\alpha_m$ is separable over $k$, it follows that it is separable over $M$ and so by the $m = 1$ case, we get $[L : M]_s = [L : M]$. Now we are done by multiplicativity.

■

**Corollary 3.1.9.** If $L/k$ is a finite extension, then $\mathrm{Aut}(L/k)$ is finite and in fact $|\mathrm{Aut}(L/k)| \leq [L : k]_s \leq [L : k]$.

*Proof.* A $k$-embedding $L \to \overline{k}$ can be precomposed by a nontrivial element of $\mathrm{Aut}(L/k)$ to get a different one. Since the above shows that there's at least one emebdding, there are in fact at least $|\mathrm{Aut}(L/k)|$ of them. ■

**Corollary 3.1.10.** Given a tower $L/M/k$ of field extensions, $L/k$ is separable iff both $L/M$ and $M/k$ are.

*Proof.* To show the "only if" part, assume that $L/k$ is separable. If $\alpha \in M$ then $\alpha \in L$ as well, and then $\mu_\alpha \in k[x]$ is separable, so that $M/k$ is separable. If $\alpha \in L$, then $\mu_{\alpha,M} \in M[x]$ divides $\mu_{\alpha,k} \in k[x]$ in $M[x]$, so that since $\mu_{\alpha,k} \in k[x]$ has no repeated roots in $\overline{k}$ neither does $\mu_{\alpha,M}$ in $\overline{M} = \overline{k}$. Therefore, $L/M$ is separable. To show the "if" direction, assume first that $L/k$ is finite, so that both $L/M$ and $M/k$ are. Then using the proposition, we get $[L : k]_s = [L : M]_s[M : k]_s = [L : M][M : k] = [L : k]$, so that $L/k$ is separable. Now in general, let $\alpha \in L$. Assume that $a_0, \ldots, \alpha_n \in M$ are the coefficients of $\mu_{\alpha,M} \in M[x]$. Then the extension $k[\alpha, a_0, \ldots, a_n]/k$ is finite. Define $N := k[\alpha, a_0, \ldots, a_n] \cap M$. Since $N \subset M$, the first part shows that $N/k$ is separable. Also, $\mu_{\alpha,N} \in N[x]$ is the same as $\mu_{\alpha,M} \in M[x]$ and is therefore separable. It follows $k[\alpha, a_0, \ldots, a_n]/N$ is separable, so by the proof for the finite-dimensional case, $k[\alpha, a_0, \ldots, a_n]/k$ is separable. In particular, $\alpha \in L$ is separable over $k$. Since this holds for any $\alpha \in L$, this proves that $L/k$ is separable. ■

**Definition 3.1.11.** Given two algebraic extensions $L, M \subset \overline{k}$ of $k$ embedded inside $\overline{k}$ in a fixed way, their *compositum* $LM$ is the smallest subfield of $\overline{k}$ containing both $L$ and $M$.

**Corollary 3.1.12.** If $L, M \subset \overline{k}$ are finite separable extensions of $k$, then so is their compositum $LM$.

*Proof.* Since $M/k$ is separable, by implication (b) $\Rightarrow$ (c) there are finitely many separable $\alpha_1, \ldots, \alpha_m \in M$ such that $M = k[\alpha_1, \ldots, \alpha_m]$. Then $LM = L[\alpha_1, \ldots, \alpha_m]$ and the $\alpha_i \in LM$ are still separable over $M$, so by (c) $\Rightarrow$ (b), $LM/L$ is separable. By the previous corollary, $LM/k$ is separable. ■

In view of the above corollary, the compositum of all finite separable subextensions $\overline{k}$ of $k$ is a separable extension $k^s/k$ containing all finite separable subextensions $\overline{k}/k$.

**Definition 3.1.13.** The extension $k^s$ is called the *separable closure* of $k$ in $\overline{k}$.

It coincides with the algebraic closure iff $k$ is perfect. It is similar to the algebraic closure also in that it coincides for all fixed separable extensions of $k$:

**Corollary 3.1.14.** Given a finite subextension $L$ of $\overline{k}/k$, we have that $L^s = k^s \subset \overline{k}$ iff $L/k$ is separable.

*Proof.* If $L^s = k^s$, then $L \subset L^s = k^s$ implies that $L/k$ is separable. Conversely, if $L/k$ is separable and $x \in L^s$, then $x \in M$ for some finite separable $M/L$. Then by Corollary 3.1.10, the extension $M/k$ is finite separable as well, and hence $x \in k^s$. Conversely, if $x \in k^s$, then $x \in M$ for some $M/k$ finite separable. Then by Corollary 3.1.12, $LM/L$ is finite separable as well and so $x \in LM$ implies that $x \in L^s$. ∎

We will need one lemma on extensions of automorphisms of fields:

**Lemma 3.1.15.**

(a) If $L, L' \subset \overline{k}$ are two subextensions of $\overline{k}/k$, then every $k$-isomorphism $L \to L'$ extends to a $k$-automorphism of $\overline{k}$. In particular, every $k$-automorphism of a subextension $L$ of $\overline{k}$ extends to a $k$-automorphism of $\overline{k}$.

(b) Every $k$-automorphism of $\overline{k}$ preserves $k^s$. In particular, if $L, L' \subset k^s$ are two subextensions, then every $k$-isomorphism $L \to L'$ extends to a $k$-automorphism of $k^s$. In particular, every $k$-automorphism of a subextension $L$ of $k^s$ extends to a $k$-automorphism of $k^s$.

*Proof.* For (a), apply Theorem 3.0.1(c) to the map $L \to L' \subset \overline{k}$. For (b), note that such an automorphism sends $\beta \in k^s$ to another root $\beta'$ of $\mu_\beta$, so that $\mu_{\beta'} = \mu_\beta$ implies that $\beta' \in k^s$. Now we may apply (a) and restrict the automorphisms to $k^s$. ∎

Next, we will show:

**Theorem 3.1.16** (Primitive Element Theorem)**.** A finite separable extension can be generated by a single element.

*Proof.* Let $L/k$ be finite separable. If $k$ is finite, then so is $L$ and then $L^\times$ is cyclic, say $L^\times = \langle \alpha \rangle$. Then $L = k[\alpha]$. Now assume that $k$ is infinite. By Proposition 3.1.8(c), there are finitely many separable $\alpha_1, \ldots, \alpha_m \in L$ such that $L = k[\alpha_1, \ldots, \alpha_m]$. If $m = 1$, there is nothing to show. If $m = 2$, say $L = k[\alpha, \beta]$ for $\alpha, \beta \in L$ separable over $k$, let $n := [L : k]$ and let $\sigma_1, \ldots, \sigma_n$ be the $n$ distinct $k$-algebra homomorphisms $L \to \overline{k}$. Consider the polynomial

$$f = \prod_{i \neq j} (\sigma_i \alpha + x\sigma_i \beta - \sigma_j \alpha - x\sigma_j \beta) \in \overline{k}[x].$$

Since the $\sigma_i$ are distinct and $L$ is generated by $\alpha$ and $\beta$, the polynomial $f$ is nonzero. Therefore, since $k$ is infinite, there is a $c \in k$ such that $f(c) \neq 0$. Then if $\gamma := \alpha + c\beta$, then the elements $\sigma_i(\gamma) \in \overline{k}$ for $i = 1, \ldots, n$ are all distinct, so that the restrictions $\sigma_i|_{k[\gamma]}$ give at least $n$ distinct embeddings $k[\gamma] \to \overline{k}$. This shows that

$$[L : k] = n = [k[\gamma] : k]_s \leq [k[\gamma] : k] \leq [k[\gamma] : k][L : k[\gamma]] = [L : k],$$

so equality must hold everywhere and hence $L = k[\gamma]$. If $m > 2$, then if $M := k[\alpha_{m-1}, \alpha_m]$ then by the $m = 2$ case we have $M = k[\gamma]$ for some $\gamma$ and then $L = k[\alpha_1, \cdots, \alpha_{m-2}, \gamma]$, so we are done by induction. ∎

Next, we will show how an arbitrary extension is obtained by taking a separable extension followed by a purely inseparable extension. The converse is not true as shown by the following example.

**Counterexample 3.1.17** (Lipman)**.** Let $p$ be any prime and $K = \mathbf{F}_p(x, y)$. The polynomial $f(t) = t^{2p} + xt^p + y \in K[t]$ is irreducible, and the extension $L = K[t]/(f(t))$ of $K$ obtained by adjoint a root of $f$ annot be obtained as a separable extension of a purely inseparable extension of $K$.

Indeed, from Gauß's Lemma, it suffices to show that $f$ is irreducible in $\mathbf{F}_p[x, y, t]$, where it follows from Eisenstein's criterion applied to $\mathfrak{p} = (x, y) \subset \mathbf{F}_p[x, y]$.

## 3.2 Galois Extensions

**Definition 3.2.1.** Let $L/k$ be an algebraic extension. We say that $L/k$ is:

(a) *normal* if every irreducible polynomial in $k[x]$ that has *some* root in $L$ has all its roots in $k$, and
(b) *Galois* if $k = L^{\mathrm{Aut}(L/k)}$. In this case, we denote $\mathrm{Aut}(L/k)$ by $\mathrm{Gal}(L/k)$ and call it the *Galois* group of $L/k$.

**Example 3.2.2.** For any $k$, the extension $\overline{k}/k$ is always normal and in fact Galois by Lemma 3.1.15. The extension $\mathbf{Q}[\sqrt[3]{2}]/\mathbf{Q}$ is not normal, since $x^3 - 2 \in \mathbf{Q}[x]$ is irreducible and has a root, namely $\sqrt[3]{2}$, in $\mathbf{Q}[\sqrt[3]{2}]$, but not the others, since they are nonreal and $\mathbf{Q}[\sqrt[3]{2}] \subset \mathbf{R}$.

**Theorem 3.2.3.** An extension $L/k$ is Galois iff it is normal and separable.

*Proof.* The proof is broken into three steps:

Step 1. If $L/k$ is Galois, then it is normal and separable.

*Proof.* Fix an $\alpha \in L$. First observe that the set $\{\sigma\alpha : \sigma \in \mathrm{Gal}(L/k)\}$ is contained in $\{\beta \in L : \mu_\alpha(\beta) = 0\}$ and is hence finite. Let $\alpha = \alpha_1, \ldots, \alpha_n \in L$ be the distinct elements of this set and note that any $\sigma \in \mathrm{Gal}(L/k)$ simply permutes these. Look at $f = \prod_{i=1}^n (x - \alpha_i) \in L[x]$. Then by the division algorithm, we have that $f | \mu_\alpha$ in $L[x]$. In fact, for any $\sigma \in \mathrm{Gal}(L/k)$, we have that $f^\sigma = \prod_{i=1}^n (x - \alpha_i^\sigma) = f$, so all coefficients of $f$ lie in $L^{\mathrm{Aut}(L/k)} = k$; this shows that $f \in k[x]$. Then it follows that $f \mid \mu_\alpha \in k[x]$, but in $k[x]$ the latter is irreducible and the former is monic and of positive degree, so this is possible only if $f = \mu_\alpha$. In particular, $f$ has distinct roots so $\alpha$ is separable. To show normality, let $g \in k[x]$ be irreducible and have some root $\alpha$ in $L$. Then $g = \lambda\mu_\alpha$ for a unique $\lambda \in k^\times$. From above, $\mu_\alpha$ has all its roots in $L$, and hence so does $g$. ∎

Step 2. The extension $k^s/k$ is Galois.

*Proof.* Fix an $\alpha \in k^s \setminus k$; we have to show that there is a $\sigma \in \mathrm{Aut}(k^s/k)$ such that $\sigma\alpha \neq \alpha$. For that, let $\alpha' \in k^s$ be a root of $\mu_\alpha$ other than $\alpha$ (this exists because $\alpha$ is separable and not in $k$) and consider the isomorphism $k[\alpha] \to k[\alpha']$ obtained by sending $\alpha \mapsto \alpha'$. By Lemma 3.1.15, this extends to an automorphism $\widetilde{\sigma} \in \mathrm{Aut}(k^s/k)$ that moves $\alpha$. ∎

The group $G_k := \mathrm{Gal}(k^s/k)$ is called the *absolute Galois group* of $k$.

Step 3. If $L/k$ is separable, then we may fix an embedding $L \subset k^s$. For such a subfield $L$ of $k^s$, the following are equivalent:
(a) The extension $L/k$ is Galois.
(b) The extension $L/k$ is normal.
(c) Each automorphism $\sigma \in \mathrm{Gal}(k^s/k)$ preserves $L$, i.e. satisfies $L^\sigma = L$.

*Proof.* The proof of (a) ⇒ (b) was done in Step 1. The implication (b) ⇒ (c) follows from the fact that each $\sigma \in \mathrm{Gal}(k^s/k)$ must map an $\alpha \in L$ to a root of its minimal polynomial, showing $L^\sigma \subset L$. Now replacing $\sigma$ by $\sigma^{-1}$ this also shows $L^{\sigma^{-1}} \subset L \Rightarrow L \subset L^\sigma$, and these two combine to give $L^\sigma = L$. For (c) ⇒ (a), pick an $\alpha \in L \setminus k$. By Step 2, we may find a $\sigma \in \mathrm{Gal}(k^s/k)$ such that $\sigma\alpha \neq \alpha$; since $L^\sigma = L$, the restriction $\sigma|_L \in \mathrm{Aut}(L/k)$ moves $\alpha$. ∎

∎

**Corollary 3.2.4.** If $L/k$ is a Galois extension, then every $k$-automorphism of a Galois subextension $M/k$ of $L/k$ extends to an automorphism of $L/k$, i.e. the natural map $\mathrm{Gal}(L/k) \to \mathrm{Gal}(M/k)$ given by Step 3(c) above is surjective.

*Proof.* Embed $L \subset k^s$. By Lemma 3.1.15, every $k$-automorphism of $M$ extends to a $k$-automorphism of $k^s$, and such an automorphism restricts by Step 3(c) to a $k$-automorphism of $L$ extending $\sigma$. ∎

Now we build toward the fundamental theorem of finite Galois theory. For that we need few lemmata:

**Lemma 3.2.5.** Suppose that $L/k$ is a finite extension. If $L/k$ is Galois, then $[L : k] = |\mathrm{Aut}(L/k)|$.

The converse also holds, but that has to wait a little.

*Proof.* One direction is clear: irrespective of whether $L/k$ is Galois, Corollary 3.1.9 shows that $|\operatorname{Aut}(L/k)| \leq [L : k]$. To show the reverse inequality, fix an embedding $L \subset k^s \subset \overline{k}$ and let $n := [L : k]$. By Proposition 3.1.8 we have $[L : k]_s = n$, so there are $n$ distinct embeddings $L \to \overline{k}$. The image of any of these certainly lies in $k^s$. By Theorem 3.0.1(c), each of these embeddings $L \to \overline{k}$ extends to an automorphism of $\overline{k}/k$ and hence by the proof of Step 3 to an automorphism of $k^s/k$. Now since $L/k$ is normal, by Step 3(c) we conclude that these automorphisms restrict to $n$ distinct automorphisms of $L/k$ proving that $|\operatorname{Aut}(L/k)| \geq [L : k]$. ∎

**Example 3.2.6.** Both normality and separability are needed, as is clear from $\mathbf{Q}[\sqrt[3]{2}]/\mathbf{Q}$ and $\mathbf{F}_p(t)[t^{1/p}]/\mathbf{F}_p(t)$.

**Lemma 3.2.7.** If $L$ is any field and $H$ a finite group of automorphisms of $L$, then $[L : L^H] \leq |H|$.

*Proof.* Let $|H| = n$ and suppose we have $n + 1$ elements $\alpha_0, \cdots, \alpha_n \in L$ linearly independent over $L^H$. Consider the $n$ equations in the $n + 1$ unknowns $\sum_{j=0}^{n} \alpha_j^\sigma x_j = 0$ for $\sigma \in H$. This has a nontrivial solution $x_j = b_j$ in $L$; pick a solution with the fewest nonzero terms. By renumbering if possible, assume WLOG that $b_0 \neq 0$, so we may write $\alpha_0^\sigma = \sum_{j=1}^{n} \alpha_j^\sigma c_j$ for all $\sigma \in H$, where $c_j := -b_j b_0^{-1} \in L$. For $\sigma = 1$, this reads $\alpha_0 = \sum_{j=1}^{n} \alpha_j c_j$, so not all the $c_j$ can lie in $L^H$; by renumbering, say $c_1 \notin L^H$. By definition of $L^H$, there is a $\tau \in H$ such that $c_1^\tau \neq c_1$. Now replace $\sigma$ by $\sigma\tau^{-1}$ in the above equation, apply $\tau$ and note that $\sigma\tau^{-1}$ still runs over all elements of $H$ to conclude that $\alpha_0^\sigma = \sum_{j=1}^{n} \alpha_j^\sigma c_j^\tau$. Subtracting, we obtain that $\sum_{j=1}^{n} \alpha_j^\sigma (c_j^\tau - c_j) = 0$ for all $\sigma \in H$, and this is a shorter and nontrivial relation since $c_1^\tau \neq c_1$, a contradiction. ∎

**Corollary 3.2.8.** If $L$ is any field and $H$ a finite group of automorphisms of $L$, then $L/L^H$ is finite Galois with $\operatorname{Gal}(L^H/L) = H$. In particular, $[L : L^H] = |H|$.

*Proof.* By Lemma 3.2.7, $L/L^H$ is finite. For any subfield $M \subset L$, it is true that $M \subset L^{\operatorname{Aut}(L/M)}$; taking $M = L^H$ shows that $L^H \subset L^{\operatorname{Aut}(L/L^H)}$. On the other hand, it is also clear that $H \subset \operatorname{Aut}(L/L^H)$, so that $L^H \supset L^{\operatorname{Aut}(L/L^H)}$. This proves that $L^H = L^{\operatorname{Aut}(L/L^H)}$, which is exactly the statement that $L/L^H$ is Galois. Finally, we also have

$$|H| \leq |\operatorname{Aut}(L/L^H)| = [L : L^H] \leq |H|,$$

where the equality uses Lemma 3.2.5 and the second inequality uses Lemma 3.2.7. Therefore, we must have equality everywhere and, in particular, $H = \operatorname{Aut}(L/L^H)$ and $[L : L^H] = |\operatorname{Aut}(L/L^H)| = |H|$. ∎

**Lemma 3.2.9.** Let $L/k$ be a Galois extension. For any subextension $M$ of $L/k$, the extension $L/M$ is Galois.

*Proof.* By Corollary 3.1.10, both $L/M$ and $M/k$ are separable. By Theorem 3.2.3, it suffices to show that $L/M$ is normal. For that we use Corollary 3.1.14 to observe that $M^s = k^s$; and we have an embedding $L \subset M^s$. By Step 3(c), if $\sigma \in \operatorname{Gal}(M^s/M)$, then in particular $\sigma \in \operatorname{Gal}(k^s/k)$, so by the implication (a) ⇒ (c) in Step 3 we conclude that $\sigma(L) \subset L$. Now, by the implication (c) ⇒ (b), we conclude that $L/M$ is normal. ∎

In this case, $\operatorname{Gal}(L/M)$ can be thought of as a subgroup of $\operatorname{Gal}(L/k)$ in the obvious way.

**Theorem 3.2.10** (The Fundamental Theorem of Galois Theory for Finite Extensions)**.** Let $L/k$ be a finite Galois extension and let $G := \operatorname{Gal}(L/k)$.

(a) The maps
$$M \mapsto \operatorname{Gal}(L/M) \text{ and } H \mapsto L^H$$
give an inclusion-reversion bijection between subextensions $M$ of $L/k$ and subgroups $H$ of $G$.

(b) If $M, M'$ are two subextensions, $H, H' \leq G$ the corresponding subgroups and $\sigma \in G$, then we have that $M' = M^\sigma \Leftrightarrow H' = \sigma^{-1} H \sigma$.

(c) For a subextension $M$ of $L/k$, the extension $M/k$ is Galois iff $H$ is a normal subgroup of $G$, and then $G/H \xrightarrow{\sim} \operatorname{Gal}(M/k)$.

*Proof.* We fix an embedding $L \subset k^s$.

(a) That these maps are inclusion-reversing is clear. For any subextension $M$, by Lemma 3.2.9, we conclude that $L^{\operatorname{Aut}(L/M)} = M$. Finally, given an $H \leq G$, the extension $L/L^H$ is finite Galois with Galois group $H$ by Corollary 3.2.8. In particular, $\operatorname{Aut}(L/L^H) = H$. This proves that the maps are inverse bijections.

(b) By definition, $\tau \in H$ iff $\alpha^\tau = \alpha$ for all $\alpha \in M$. Suppose that $M' = M^\sigma$. Given $\tau \in H$ and $\alpha' \in M'$, write $\alpha' = \alpha^\sigma$ for some (unique) $\alpha \in M$ and then use $(\alpha')^{\sigma^{-1}\tau\sigma} = (\alpha^\tau)^\sigma = \alpha^\sigma = \alpha'$ to conclude that $\sigma^{-1}H\sigma \subset H'$. Since in this case we also have $M = (M')^{\sigma^{-1}}$, we conclude that $(\sigma^{-1})^{-1}H'\sigma^{-1} \subset H$ and so we must have $\sigma^{-1}H\sigma = H'$. For the converse, if $H' = \sigma^{-1}H\sigma$ and $\alpha \in M$, then the element $\alpha^\sigma$ has the property that for any $\tau' \in H'$ writing $\tau' = \sigma^{-1}\tau\sigma$ for some $\tau \in H$ we have $(\alpha^\sigma)^{\tau'} = \alpha^{\tau\sigma} = \alpha^\sigma$ so that $\alpha^\sigma \in L^{H'} = M'$. This shows $M^\sigma \subset M'$. On the other hand, $H = (\sigma^{-1})^{-1}H'\sigma^{-1}$ so we must have $(M')^{\sigma^{-1}} \subset M$.

(c) We claim that the extension $M/k$ is Galois iff for all $\sigma \in G$ we have $M^\sigma = M$. By (b), this would prove that $M/k$ is Galois iff $H \trianglelefteq G$. Suppose that $M/k$ is Galois and $\sigma \in G$. Then, by Corollary 3.1.15, we can find a $k$-automorphism $\widetilde{\sigma}$ of $k^s$ extending $\sigma$. By the implication (a) $\Rightarrow$ (c) in Step 3, we conclude that $M^\sigma = M^{\widetilde{\sigma}} = M$. Conversely, if $M^\sigma = M$ for every $\sigma \in G$ and $\widetilde{\sigma} \in \mathrm{Gal}(k^s/k)$ is arbitrary, then since $L/k$ is Galois, we may take $\sigma := \widetilde{\sigma}|_L \in G$ and then $M^{\widetilde{\sigma}} = M^\sigma = M$, so the implication (c) $\Rightarrow$ (a) proves the $M/k$ is Galois. For the final claim, the restriction homomorphism $G \to \mathrm{Gal}(M/k)$ is surjective by Corollary 3.2.4 and has kernel $H$.

■

Now we can prove the converse to Lemma 3.2.5.

**Corollary 3.2.11.** Suppose that $L/k$ is a finite extension. Then $L/k$ is Galois iff $[L : k] = |\mathrm{Aut}(L/k)|$.

*Proof.* One direction of this was proved in Lemma 3.2.5. Conversely, for $G = \mathrm{Aut}(L/k)$, the extension $L/L^G$ is (finite) Galois with Galois group $G$ by Corollary 3.2.8 so by the first part, $[L : L^G] = |G| = [L : k]$. Since $k \subseteq L^G$ forces $L^G = k$. ■

## 3.3 Splitting Fields

**Definition 3.3.1.** Given a polynomial $f \in k[x]$, the *splitting field* of $f$ is defined to be the finite subextension $L/k$ of $\overline{k}/k$ generated by all the roots of $f$ in $\overline{k}$.

If $f$ is separable, then its splitting field is contained in $k^s$. Classically, Galois extensions arose as splitting fields of separable polynomials.

**Lemma 3.3.2.** Suppose that $L/k$ is any extension. Then the following are equivalent:

(a) $L/k$ is finite Galois.
(b) $L/k$ is the splitting field of an irreducible separable $f \in k[x]$.
(c) $L/k$ is the splitting field of some separable $f \in k[x]$.

*Proof.* To show (a) $\Rightarrow$ (b), if $L/k$ is finite Galois, then by Theorem 3.1.16 we have $L = k[\alpha]$ for some separable $\alpha \in L$. Then the irreducible polynomial $\mu_\alpha \in k[x]$ has the root $\alpha$ in $L$ and so by normality all of its roots in $\overline{k}$ actually lie in $L$. In particular, $L = k[\alpha]$ is the extension of $k$ generated by all the roots of the irreducible separable $f := \mu_\alpha$. The implication (b) $\Rightarrow$ (c) is clear. Finally for (c) $\Rightarrow$ (a), note that the splitting field of a polynomial is finite, of a separable polynomial is separable by Proposition 3.1.8(c), and finally is normal because it clearly satisfies condition (c) in Step 3: indeed, any autmorphism $\sigma \in \mathrm{Gal}(k^s/k)$ sends a root of $f$ to another and hence preserves the splitting field. ■

If $f \in k[x]$ is separable of degree $n$, then its splitting field $L/k$ is Galois by the above and $\mathrm{Gal}(L/k)$ acts on $L$ by permuting the roots of $f$. In particular, this gives is an injection $\mathrm{Gal}(L/k) \to S_n$, showing that $[L : k] \leq n!$. This bound is sharp, as the following example shows.

**Theorem 3.3.3** (Fundamental Theorem of Symmetric Polynomials)**.** Let $R$ be any commutative unitary ring and $n \geq 1$, and consider the polynomial ring $R[x_1, \ldots, x_n]$ over $R$ in $n$ indeterminates. Then $S_n$ acts on $R[x_1, \ldots, x_n]$ by permuting the $x_i$; the ring of invariants $R[x_1, \ldots, x_n]^{S_n}$ is called the ring of *symmetric polynomials* in the $x_i$. If $\sigma_j \in R[x_1, \ldots, x_n]^{S_n}$ for $j = 1, \ldots, n$ are the elementary symmetric polynomials, then we have that

$$R[x_1, \ldots, x_n]^{S_n} = R[\sigma_1, \ldots, \sigma_n].$$

In other words, every symmetric polynomial over $n$ indeterminates over any ring is a polynomial in the elementary symmetric polynomials.

*Proof.* First assume that $R = k$ is a field. Let $L = k(x_1, \dots, x_n)$ be the fraction field of $k[x_1, \dots, x_n]$. Then the symmetric group $S_n$ also acts on $L$ via permuting the $x_i$; the fixed field $L^{S_n}$ is called the field of *symmetric rational functions*. By Corollary 3.2.8, $[L : L^{S_n}]$ is a finite Galois extension with Galois group $S_n$; in particular, $[L : L^{S_n}] = n!$. The field $L$ is the splitting field of the polynomial $f = \prod_{i=1}^{n}(x - x_i) = \sum_{j=0}^{n}(-1)^j \sigma_j x^j$, where $\sigma_0 := 1$. If $M := k(\sigma_1, \dots, \sigma_n) \subset L^{S_n}$, then $L$ is also the splitting field of $f$ over $M$, so by the above observation we have that

$$n! = [L : L^{S_n}] \leq [L : L^{S_n}][L^{S_n} : M] = [L : M] \leq n!,$$

so we must in fact have equality everywhere and hence $M = L^{S_n}$. In particular, every symmetric rational function is a rational function in the elementary symmetric polynomials.

To do the polynomial case, note that since $x_i$ are roots of $f$, they are integral over the subring $k[\sigma_1, \dots, \sigma_n] \subset L^{S_n}$. Therefore, the subring $k[x_1, \dots, x_n]^{S_n} := k[x_1, \dots, x_n] \cap L^{S_n}$ of symmetric polynomials is integral over $k[\sigma_1, \dots, \sigma_n]$. But as $L \supset k(\sigma_1, \dots, \sigma_n)$ is a finite extension, we must have $n = \operatorname{trdeg}_k L = \operatorname{trdeg}_k k(\sigma_1, \dots, \sigma_n)$, so that the $\sigma_i$ are algebraically independent over $k$. Thus $k[\sigma_1, \dots, \sigma_n]$ is isomorphic to a polynomial ring and in particular a UFD and hence integrally closed in its fraction field $L^{S_n}$ (by the generalized Gauß Rational Root Theorem); this shows that we must have $k[x_1, \dots, x_n]^{S_n} = k[\sigma_1, \dots, \sigma_n]$.

Next, we do $R = \mathbf{Z}$. Then it follows again from the integrality of $x_i$ over the $\sigma_j$ that $\mathbf{Z}[x_1, \dots, x_n]^{S_n}$ is an integral extension of $\mathbf{Z}[\sigma_1, \dots, \sigma_n]$. Now the $\sigma_j$ are also algebraically independent over $\mathbf{Z}$: if they weren't, then we would get an equation of algebraic dependence over arbitrary $k$ by the canonical map $\mathbf{Z} \to k$. Therefore, $\mathbf{Z}[\sigma_1, \dots, \sigma_n]$ is a polynomial ring, and hence a UFD, and hence integrally closed in its fraction field $\mathbf{Q}(x_1, \dots, x_n)$, so we must have that $\mathbf{Z}[x_1, \dots, x_n]^{S_n} = \mathbf{Z}[\sigma_1, \dots, \sigma_n]$.Finally, for the general case, it suffices to observe that $R[x_1, \dots, x_n]^{S_n} = R \otimes_{\mathbf{Z}} \mathbf{Z}[x_1, \dots, x_n]^{S_n} = R \otimes_{\mathbf{Z}} \mathbf{Z}[\sigma_1, \dots, \sigma_n] = R[\sigma_1, \dots, \sigma_n]$. ∎

This idea of using indeterminates also proves that every finite group arises as the Galois group of some extension:

**Proposition 3.3.4.** If $G$ is any finite group, then there is a finite Galois extension $L/M$ such that $\operatorname{Gal}(L/M) = G$. In fact, $M$ can be chosen to be of arbitrary characteristic.

*Proof.* Embed $G$ into $S_n$ for some $n \geq 1$, and take $k$ to be a field of the prescribed characteristic and consider the action of $G$ on $L = k(x_1, \dots, x_n)$ via permuting the $x_i$. Then taking $M := L^G$ suffices by Corollary 3.2.8. ∎

## 3.4 Infinite Galois Theory

**Lemma 3.4.1.** Let $K/k$ be a possibly infinite Galois extension. Then any finite subextension $L$ of $K/k$ is contained in a Galois subextension.

*Proof.* Indeed, fix an embedding $K \subset k^s$. By Corollary 3.1.10, $L/k$ is separable, so by Theorem 3.1.16 it is simple, i.e. $L = k[\alpha]$ for some separable $\alpha \in L$. Then the splitting field of $\alpha$ is a Galois extension of $k$ by Lemma 3.3.2. It is contained in $K$ since $K/k$ is normal and clearly contains $L$. ∎

This says that the structure of a Galois extension should be determined by its finite Galois subextensions, and this is indeed the case. For that we need to understand limits.

**Theorem 3.4.2** (Limits)**.**

(a) (Limits of Spaces) If $\{X_\mu\}_{\mu \in \Lambda}$ is a directed family of topological spaces, then $X := \varprojlim X_\mu \subset \prod_\mu X_\mu$ has the subspace topology.
   i. Assume that each $X_\mu$ is compact. If each $X_\mu$ is nonempty and Hausdorff, then so is $X$.
   ii. Assume that each $X_\mu$ is nonempty, finite, and discrete. (In this case, $X$ is called a *profinite space*.) Then $X$ is nonempty, compact, Hausdorff and totally disconnected.

(b) (Limits of Topological Groups) If $\{G_\mu\}$ is a directed family of topological groups, then $G := \varprojlim G_\mu \subset \prod_\mu G_\mu$ is a topological subgroup.
   i. The maps $G \to G_\mu$ are all continuous homomorphisms.
   ii. If the $G_\mu$ are finite and discrete (so $G$ is a *profinite group*), then $G$ is nonempty, compact, Hausdorff, and totally disconnected. Further, $\{\ker(G \to G_\mu)\}_\mu$ form a neighborhood base of open subsets at $1 \in G$. These are all normal, open and closed subgroups.

iii. If $G$ is a profinite group (or more generally any compact topological group), then the open subgroups of $G$ are precisely the closed subgroups of finite index.

*Proof.* First we prove (a).

i. If each $X_\mu$ is compact, by Tychonoff's theorem so is $\prod_\nu X_\nu$. For any pair $\lambda \preceq \mu$ in the directing set, let $X_{\lambda\mu} \subset \prod_\nu X_\nu$ consist of sequences $(x_\nu)$ such that $\phi_\lambda^\mu(x_\mu) = x_\lambda$. These are closed subsets: define $\psi_{\lambda\mu} : X_\mu \times X_\lambda \to X_\lambda \times X_\lambda$ by $(y, z) \mapsto (\phi_\lambda^\mu y, z)$; since $X_\lambda$ is Hausdorff, the diagonal $\Delta \subset X_\lambda \times X_\lambda$ is closed; since $\psi_{\lambda\mu}$ is continuous, $\psi_{\lambda\mu}^{-1}(\Delta) \subset X_\mu \times X_\lambda$ is closed; finally by definition of the product topology $X_{\lambda\mu} = \prod_{\nu\neq\lambda,\mu} X_\nu \times \psi_{\lambda\mu}^{-1}(\Delta)$ is closed. By directedness, the finite intersections of the $X_{\lambda\mu}$ are all nonempty; by compactness, the intersection $X = \bigcap_{\lambda\preceq\mu} X_{\lambda\mu}$ is nonempty.
ii. The first three claims are immediate from i. For the last one, it suffices to show that if $A \subset X$ is any subset containing $(x_\nu) \neq (y_\nu)$, then $A$ is disconnected. Indeed, in that case there is a $\mu$ such that $x_\mu \neq y_\mu$, and the subsets $A \cap \phi_\mu^{-1}\{x_\mu\} \ni (x_\nu)$ and $A \cap \phi_\mu^{-1}(X_\mu \smallsetminus \{x_\mu\}) \ni (y_\nu)$ provide a disconnection of $A$.

Now we show (b).

i. Clear, since they are the compositions $G \hookrightarrow \prod_\mu G_\mu \twoheadrightarrow G_\mu$.
ii. The first claim is clear from (a) ii. For the next, let $U \ni 1$ be an open set, and pick a basis open $\bigcap_{\lambda\in\Gamma} \phi_\lambda^{-1}(V_\lambda)$ containing 1 and contained in $U$ for some finite subset $\Gamma \subset \Lambda$ and opens $V_\lambda \subset G_\lambda$. Since 1 belongs to this basis open, $1 \in V_\lambda$ for each $\lambda \in \Gamma$. By directedness, there is a $\mu$ such that $\lambda \preceq \mu$ for each $\lambda \in \Gamma$, and then $1 \in \ker(G \to G_\mu) \subset \prod_{\lambda\in\Gamma} \phi_{\lambda^{-1}}(V_\lambda) \subset U$, and $\ker(G \to G_\mu) = \phi_\mu^{-1}\{1\}$ is open because $\{1\} \subset G_\mu$ is. These are all normal since they are kernels, and every open subgroup of a topological group is closed.
iii. Each open subgroup is closed and the disjoint union of its cosets provides an open cover of $G$, so there are at most finitely many of them. Conversely, if a subgroup is closed and of finite index, then it is open because it is the complement of the finite disjoint union of its nontrivial cosets, which are all closed.

■

Why are these relevant to us?

**Lemma 3.4.3.** Let $K/k$ be any Galois extension. Then the natural map $\mathrm{Gal}(K/k) \to \varprojlim \mathrm{Gal}(L/k)$ to the limit of finite Galois subextensions $L/k$ is a group isomorphism.

The induced topology on $\mathrm{Gal}(K/k)$ is called the *Krull topology* and makes $\mathrm{Gal}(K/k)$ a profinite group.

*Proof.* The map here is injective, since if $\sigma \in \mathrm{Gal}(K/k)$ does not fix $\alpha \in K$, then if $L$ is any finite Galois subextension of $K$ containing $\alpha$ obtained from Lemma 3.4.1, then $\sigma|_L$ is nontrivial. It is surjective, since given an element $(\sigma_L) \in \varprojlim \mathrm{Gal}(L/k)$, we may define $\sigma \in \mathrm{Gal}(K/k)$ simply by defining for $\alpha \in K$ the element $\sigma(\alpha) := \sigma_L(\alpha)$ for any finite Galois $L$ containing $\alpha$; the choices involved don't matter by compatibility, and we clearly have $\sigma \mapsto (\sigma_L)$. ■

**Example 3.4.4.** If $\mathbf{F}$ is a finite field, then $G_\mathbf{F} \cong \hat{\mathbf{Z}}$ generated topologically by the Frobenius map $a \mapsto a^{|\mathbf{F}|}$. The Galois group $\mathrm{Gal}(\mathbf{Q}[\mu_{p^\infty}]/\mathbf{Q}) \cong \mathbf{Z}_p^\times$ and similarly $\mathrm{Gal}(\mathbf{Q}[\mu]/\mathbf{Q}) \cong \hat{\mathbf{Z}}^\times$.

**Lemma 3.4.5.** If $K/k$ is a Galois extension, then for any Galois subextension $M$ of $K/k$, the projection $\mathrm{Gal}(K/k) \to \mathrm{Gal}(M/k)$ is surjective and continuous.

*Proof.* Surjectivity follows from Corollary 3.2.4 and continuity because it is continuous at the level of $\prod_{L/k} \mathrm{Gal}(L/k)$ where the product is over finite Galois subextensions contained in $K$ and those in $M$ respectively. ■

We are now able to prove the fundamental theorem of Galois theory.

**Theorem 3.4.6** (The Fundamental Theorem of Galois Theory)**.** Let $K/k$ be a Galois extension and $G := \mathrm{Gal}(K/k)$. The maps

$$M \mapsto \mathrm{Gal}(K/M) \text{ and } H \mapsto K^H$$

given an inclusion reversing bijection between subextensions $M$ of $L/k$ and *closed* subgroups $H$ of $G$. This further restricts to bijections between Galois (resp. finite, finite Galois) subextensions and closed normal (resp. open, open normal) subgroups. In the Galois case, the map $G/H \to \mathrm{Gal}(M/k)$ is an isomorphism of topological groups.

*Proof.* We first show that $\mathrm{Gal}(K/M)$ is open (resp. normal, closed) if $M/k$ is finite (resp. Galois, arbitrary). If $M/k$ is finite, then by Lemma 3.4.1, it is contained in a finite Galois subextension $L/k$ of $K/k$, so that $\mathrm{Gal}(K/M)$ contains the open subgroup $\mathrm{Gal}(K/L) = \ker(G \to \mathrm{Gal}(L/k))$. But $\mathrm{Gal}(K/M)$ can be written as a union of cosets of $\mathrm{Gal}(K/L)$ each of which is open, so $\mathrm{Gal}(K/M)$ is open as well. If $M/k$ is Galois, then $\mathrm{Gal}(K/M)$ is normal because it is the kernel of restriction $\mathrm{Gal}(K/k) \to \mathrm{Gal}(M/k)$. If $M/k$ is arbitrary, then $M = \bigcup_{L \subset M} L$ for finite Galois $L$; each $\mathrm{Gal}(K/L)$ is open and hence closed by what we have shown, and so $\mathrm{Gal}(K/M) = \bigcap_{L \subset M} \mathrm{Gal}(K/L)$ is closed as well.

These maps are clearly inclusion-reversing. Note that $M = K^{\mathrm{Gal}(K/M)}$ because $K/M$ is Galois by Lemma 3.2.9. On the other hand, suppose that $H \leq G$ is closed; we will show that $H \subset \mathrm{Gal}(K/K^H)$ is dense. Indeed, let $g \in \mathrm{Gal}(K/K^H)$. Then any neighborhood of $g$ contains an open set of the form $g\,\mathrm{Gal}(K/L)$ for some finite Galois $L/k$ by Theorem 3.4.2 (b) ii., and we need only show $g\,\mathrm{Gal}(K/L) \cap H \neq \emptyset$. Note that $g|_L$ fixes $L \cap K^H = L^{H|_L}$, so by finite Galois theory $g|_L \in \mathrm{Gal}(L/L^{H|_L}) = H|_L$. In particular, there is an $h \in H$ such that $g|_L = h|_L$, so that $g^{-1}h \in \mathrm{Gal}(K/L)$ and $H \ni h = g(g^{-1}h) \in g\,\mathrm{Gal}(K/L)$.

Next, we show that $K^H$ is finite (resp. Galois) if $H \leq G$ is open (resp. closed nomrmal). If $H \leq G$ is open, then $H$ contains $\mathrm{Gal}(K/L)$ for some finite Galois $L/k$ by Theorem 3.4.2 (b) ii., so then $K^H \subset K^{\mathrm{Gal}(K/L)} = L$ shows that $K^H$ is finite. If $H \leq G$ is closed and normal, then suppose that $L/k$ is any finite Galois subextension of $K$. By extension of automorphisms (Corollary 3.2.4), the group $H|_L \subset \mathrm{Gal}(L/k)$ is normal too, so by finite Galois theory $L \cap K^H = L^{H|_L}$ is normal. Since $K^H = \bigcup_{L \subset M} L \cap K^H$ (where $L$ ranges over finite Galois subextensions of $M$) is the union of normal extensions, it is also normal by say the criterion in Step 3 (c).

Finally, the map $\mathrm{Gal}(K/k) \to \mathrm{Gal}(M/k)$ is surjective and continuous with closed normal kernel $\mathrm{Gal}(K/M)$, and so the result follows from the continuity of the induced map $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/M) \to \mathrm{Gal}(M/k)$, which in turn follows from the definition of the quotient topology. (We use that a continuous bijection from a compact space to a Hausdorff space is a homeomorphism.)

■

*Exercise* 3.4.7. (Incompatiblity of the profinite and analytic topologies.) Every continuous homomorphism $G_{\mathbf{Q}} \to \mathrm{GL}_n \mathbf{C}$ for $n \geq 1$ factors through a finite group. This follows from considering a neighborhood $V$ of $1 \in \mathrm{GL}_n \mathbf{C}$ such that the only subgroup $H \leq \mathrm{GL}_n \mathbf{C}$ contained in $V$ is the trivial one.

## 3.5 Separability II: Étale Algebras

**Definition 3.5.1.** Given a field $k$, a $k$-algebra $A$ is called *separable* (over $k$) if $A \otimes_k L$ is a reduced ring for every field extension $L/k$.

**Proposition 3.5.2.**

(a) A subalgebra of a separable $k$-algebra is separable.
(b) A $k$-algebra is separable iff all of its finitely generated subalgebras are.
(c) A $k$-algebra is separable iff $A \otimes_k L$ is reduced for every finitely generated extension $L/k$.
(d) A $k$-algebra $A$ is separable iff for any extension $K/k$, the $K$-algebra $A \otimes_k K$ is separable.

*Proof.* The statement (a) follows from the facts that (i) tensoring over a field is exact, so if $B \subset A$ is a subalgebra, then so is $B \otimes_k L \subset A \otimes_k L$, and (ii) a subalgebra of a reduced algebra is reduced. One direction of (b) follows from (a), and the other direction and (c) follow from $A \otimes_k L = \bigcup_{B \subset A} B \otimes_k L = \bigcup_{M \subset L} A \otimes_k M$, where the first union is over finitely generated subalgebras $B \subset A$ and the second over finitely generated subextensions $M \subset L$. One direction of (d) follows from taking $K = k$ and noting $A \otimes_k k \cong A$; the other follows from observing that for any extension $L/K$ we have $(A \otimes_k K) \otimes_K L \cong A \otimes_k L$ as algebras. ■

First, we show that this notion coincides with the previous definition for field extensions. For that, we need to understand elements of $\overline{k} \setminus k^s$ a little better.

**Lemma 3.5.3.** If $\mathrm{char}\, k = p > 0$, then given any element $\alpha \in \overline{k}$, there is an integer $q \geq 1$ such that $\alpha^q \in k^s$. The unique smallest such $q$ is called the *inseparability height* of $\alpha$. The inseparability height $q$ is a power of $p$, i.e. $q = p^n$ for some $n \geq 0$, and finally $\mu_{\alpha,k^s} = x^q - \alpha^q \in k^s[x]$. In particular, $q = [k(\alpha) : k(\alpha^q)]$. Further, in this case we have that if the minimal polynomial $\mu_{\alpha^q,k} = x^n + a_1 x^{n-1} + \cdots + a_n \in k[x]$, then $\mu_{\alpha,k} = x^{qn} + a_1 x^{qn-1} + \cdots + a_n \in k[x]$.

*Proof.* When $\alpha \in k^s$, the whole statement is trivial, so assume $\alpha \in \overline{k} \setminus k^s$. Look at $f := \mu_{\alpha,k} \in k[x]$; by definition, this is not separable. By Proposition **??**(b), $f(x) = \widetilde{f}(x^q)$ for some $q = p^n$ where $n \geq 1$ and $\widetilde{f} \in k[x]$; pick the largest such possible $q$, which is a fair ask because of $\deg f < \infty$. Then the corresponding $\widetilde{f}$ is irreducible (because a nontrivial factorization of $\widetilde{f}$ would give rise to one for $f$) and separable (because the maximality of $q$ ensures that $\widetilde{f}' \neq 0$). Since $\alpha^q$ is a root of $\widetilde{f}$, the minimal polynomial $\mu_{\alpha^q,k} \mid \widetilde{f}$ in $k[x]$, so that $\alpha^q \in k^s$.

Now let $q$ denote the smallest *power of* $p$ such that $\alpha^q \in k^s$; the above proof shows that such a $q$ exists. We will show first that $\mu_{\alpha,k^s} = (x-\alpha)^q \in k^s[x]$, and then that $q$ is also the smallest integer $u \geq 1$ such that $\alpha^u \in k^s$. For the first one, note that $\mu_{\alpha,k^s} \mid x^q - \alpha^q = (x-\alpha)^q \in k^s[x]$, so that we must have $\mu_{\alpha,k^s} = (x-\alpha)^r$ for some integer $1 \leq r \leq q$. If we write $r = q't$ for some power $q'$ of $p$ and integer $t \geq 1$ such that $(p,t) = 1$, then we have that

$$\mu_{\alpha,k^s} = (x-\alpha)^{q't} = (x^{q'} - \alpha^{q'})^t = x^{q't} - t\alpha^{q'} x^{q'(t-1)} + \cdots \in k^s[x],$$

which implies that $\alpha^{q'} \in k^s$ since $-t \in k^\times$. But $q' \leq r \leq q$ and $q$ was chosen to be the smallest power of $p$ for which $\alpha^q \in k^s$, so we must have that $q' = r = q$ and $t = 1$, proving $\mu_{\alpha,k^s} = (x-\alpha)^q$. Finally, if $u \geq 1$ is any integer such that $\alpha^u \in k^s$, then we must have that $(x-\alpha)^q = \mu_{\alpha,k^s} \mid x^u - \alpha^u$, so that $u \geq q$; in particular, the smallest integer $u$ such that $\alpha^u \in k^s$ (i.e. the inseparability height of $\alpha$) is a power of $p$.

For the last statement, $\mu_{\alpha,k}$ clearly divides the latter and the result follows from degree considerations. ∎

**Theorem 3.5.4.** If $K/k$ is an algebraic field extension, then $K$ is separable as a $k$-algebra iff it is separable as a field extension.

*Proof.* Since both kinds of separability are detected by finite subextensions, we may assume WLOG that $K/k$ is finite (as an algebra and a field extension; these notions are equivalent since $K/k$ is algebraic). First suppose that $K/k$ is separable as an extension; then Theorem 3.1.16 says that $K = k[\alpha]$ for some separable $\mu_\alpha \in k[x]$. If $L/k$ is any extension, then since $\overline{k} \subset \overline{L}$, it follows that $\mu_\alpha \in L[x]$ is still separable, although no longer necessarily irreducible. Write $\mu_\alpha = \prod_{i=1}^n f_i$ for $f_i \in L[x]$ irreducible; since $\mu_\alpha$ is separable, the $(f_i)$ are pairwise coprime, and so the Chinese Remainder Theorem gives us that

$$K \otimes_k L \cong k[x]/(\mu_\alpha) \otimes_k L \cong L[x]/(\mu_\alpha) \cong \prod_{i=1}^n L[x]/(f_i).$$

Since each $(f_i)$ is irreducible, $L[x]/(f_i)$ is a field; therefore, $K \otimes_k L$ is a finite direct product of fields and hence separable. For the converse, fix an embedding $K \subset \overline{k}$. If $K/k$ is not a separable extension, there is an $\alpha \in K \setminus k^s$. By the previous lemma, $\mu_{\alpha,k^s} = (x-\alpha)^q$ for some $q = p^n > 1$ with $\alpha^q \in k^s$. Consider the element $\alpha \otimes 1 - 1 \otimes \alpha \in K \otimes_k K$; we claim that this is a nonzero nilpotent. To show that it is nonzero, since $1, \alpha \in K$ are linearly independent over $k$, we can pick a basis of $K/k$ containing these two; then we may consider the explicit basis of $K \otimes_k K$ produced by these, in which $\alpha \otimes 1$ and $1 \otimes \alpha$ are distinct elements, so that their difference is nonzero. On the other hand, the extension of scalars $K \otimes_k K \hookrightarrow (K \otimes_k K) \otimes_k k^s \cong (K \otimes_k k^s) \otimes_{k^s} (K \otimes_k k^s)$ is injective since $k$ is a field, and in the latter the element $(\alpha \otimes 1 - 1 \otimes \alpha)^q = \alpha^q \otimes 1 - 1 \otimes \alpha^q = \alpha^q \otimes 1 - \alpha^q \otimes 1 = 0$ because $\alpha^q \in k^s$; this proves that $(\alpha \otimes 1 - 1 \otimes \alpha)^q = 0 \in K \otimes_k K$ to begin with. ∎

If every finite separable extension $L/k$ is $k[x]/(f)$ for some irreducible separable $f$, then what do the algebras $k[x]/(f)$ for possibly reducible but separable $f$ look like? We are now ready to state and prove the main theorem of the section.

**Theorem 3.5.5** (Étale Algebras)**.** Let $A$ be a finite-dimensional algebra over a field $k$. Consider the following conditions.

(a) $A \cong k[x]/(f)$ for some separable $f \in k[x]$.
(b) $A$ is a finite direct product of separable field extensions of $k$.
(c) $A$ is separable as a $k$-algebra.
(d) $A \otimes_k \overline{k}$ is reduced.
(e) $A \otimes_k \overline{k}$ is isomorphic to a finite product of copies of $\overline{k}$.
(f) The discriminant of one (and hence any) basis of $A/k$ is nonzero.
(g) The trace pairing $\mathrm{Tr}_k^A$ is a perfect pairing.

Then the conditions (b) through (g) are equivalent and implied by (a). If $\dim_k A < |k|$ (in particular, if $k$ is infinite), then all the conditions are equivalent.

*Proof.* For (a) ⇒ (b), note that if $f = \prod_{i=1}^n f_i$ is the decomposition of $f$ into irreducibles, then the $f_i$ are all irreducible separable and pairwise coprime, so that each $k[x]/(f_i)$ is a finite separable field extension of $k$ and the Chinese Remainder Theorem gives us that $A \cong k[x]/(\prod_{i=1}^n f_i) \cong \prod_{i=1}^n k[x]/(f_i)$ as needed. For (b) ⇔ (c), note that taking the tensor product commutes with taking finite direct product[1], so that (b) ⇒ (c) follows from Theorem 3.5.4; indeed, if $A = \prod_{i=1}^n K_i$, then $A \otimes_k L = \prod_{i=1}^n (K_i \otimes_k L)$ and each $K_i \otimes_k L$ is reduced by the propsition and so, so is their product $A \otimes_k L$. For the implication (c) ⇒ (b), note first that taking $L = k$ in the definition shows that $A \otimes_k k \cong A$ is reduced, so since $A$ is a reduced Artinian ring, $A$ is a finite direct product of finite extensions of $k$, say $A \cong \prod_{i=1}^n K_i$. Suppose that one of these, say $K_j$, is not separable; then by Theorem 3.5.4, there is an extension $L/k$ such that $K_j \otimes_k L$ is not reduced, and has a nonzero nilpotent say $\beta_j$. Then the element $(0, 0, \ldots, 0, \beta_j, 0, \ldots, 0) \in \prod_{i=1}^n (K_i \otimes_k L) \cong A \otimes_k L$ is a nonzero nilpotent, contradicting that $A$ is a separable $k$-algebra. The implication (c) ⇒ (d) follows from taking $L = \overline{k}$ in the definition. The equivalence (d) ⇔ (e) follows immediately from the fact that $A \otimes_k \overline{k}$ is a reduced Artinian ring. For the implication (e) ⇒ (f), note that for any extension $L/k$ the discriminant of $A \otimes_k L$ as an $L$-algebra is nonzero iff that of $A$ as a $k$-algebra is; indeed, any basis of $A/k$ remains a basis of $A \otimes_k L/L$ and the same computation computes the discriminant of both. If $A \otimes_k \overline{k}$ is isomorphic to a finite product of copies of $\overline{k}$, then we can simply take a convenient basis given by the idempotents that represent projection onto these factors, and then the discriminant of this basis is clearly 1. The equivalence (f) ⇔ (g) is clear. Next, we show that (f) ⇒ (c), and this finishes the proof of the equivalence of conditions (b) through (g). Indeed, by the above argument, the discriminant of $A \otimes_k L/L$ is also nonzero for any extension $L/k$ of $k$, so it suffices to show that if $A/k$ is a finite dimensional algebra (of dimension say $n := \dim_k A$) with nonzero discriminant, then it is reduced. For that, assume that $A$ is not reduced, so that the radical $\sqrt{0}$ is positive dimensional, say of dimension $1 \leq r \leq n$. Extend a $k$-basis $\alpha_1, \ldots, \alpha_r$ of $\sqrt{0}$ to a $k$-basis $\alpha_1, \ldots, \alpha_r, \alpha_{r+1}, \ldots, \alpha_n$ of $A$. Then if either $i \leq r$ or $j \leq r$, then the $k$-linear map $\alpha_i \alpha_j : A \to A$ is nilpotent and hence has zero trace. Therefore, the matrix $[\mathrm{Tr}_k^A(\alpha_i \alpha_j)]$ has its first $r$ rows and columns identically zero; if $r \geq 1$, then it cannot have nonzero determinant.

Finally, it remains to show (b) ⇒ (a) when the said condition holds. For that, write $A = \prod_{i=1}^n K_i$ for finite separable $K_i/k$. By Theorem 3.1.16, we can inductively pick a monic irreducible $f_i \in k[x]$ so that $K_i \cong k[x]/(f_i)$, ensuring that each $f_j$ we pick is not equal to $f_i$ for $i < j$. This can be achieved by replacing $f_j(x)$ by $f_j(x + a)$ for $a \in k^\times$ if necessary; here we use that (i) there are at least $n$ differenct choices for $a$ by hypothesis and (ii) if $f(x) \in k[x]$ is irreducible, then $f(x + a)$ for $a \in k^\times$ are irreducible and pairwise coprime. Then the polynomials $f_i$ are irreducible separable and pairwise coprime, so that $A \cong k[x]/(f)$ for $f = \prod_{i=1}^n f_i$ again by the Chinese Remainder Theorem. ∎

When $A$ satisfies the equivalent conditions (b) through (f) of the above theorem, we say that $A$ is *étale* over $k$. In this case, the decomposition of $A$ into separable field extensions is essentially unique:

**Proposition 3.5.6.** Let $A = \prod_{i=1}^n K_i$ be a $k$-algebra that is a finite product of (not necessarily separable) extensions of $k$.

(a) Any surjective $k$-algebra homomorphism $A \to B$ is a projection onto a subproduct (followed by an isomorphism).
(b) Any $k$-algebra homomorphism $A \to L$ from $A$ to a *field extension* $L/k$ can be described uniquely as $\varphi \circ \pi_i$ for some $i$, where $\pi_i : A \to K_i$ is the projection and $\varphi : K \hookrightarrow L$ a $k$-embedding. In particular, as sets, we have that

$$\mathrm{Hom}_k(A, L) \cong \coprod_{i=1}^n \mathrm{Hom}_k(K_i, L).$$

If $A$ and $B$ are two $k$-algebras that are finite products of extensions of $k$, say $A = \prod_{i=1}^n K_i$ and $B = \prod_{j=1}^m L_j$, then $\mathrm{Hom}_k(A, B) \cong \coprod_{i,j} \mathrm{Hom}_k(K_i, L_j)$.

*Proof.* For (a), note that the projection of the kernel to $K_i$ gives an ideal of $K_i$, and so must be either 0 or $K_i$. In particular, the kernel is a subproduct, so the necessary isomorphism is given by the first isomorphism theorem. For (b), note that the image of $A$ in $L$ is a $k$-subalgebra of the field $L$ and hence an integral domain, so the projection given by (a) cannot have more than one factor in it. The last statement follows from

$$\mathrm{Hom}_k(A, B) \cong \prod_{j=1}^m \mathrm{Hom}_k(A, L_j) \cong \prod_{j=1}^m \coprod_{i=1}^n \mathrm{Hom}_k(K_i, L_j) \cong \coprod_{i,j} \mathrm{Hom}_k(K_i, L_j).$$

∎

[1] This uses that it commutes with the finite direct sum, and the corresponding isomorphism also turns out to be an algebra isomorphism.

**Corollary 3.5.7.** The decomposition of an étale algebra $A$ into a product of separable field extensions of $k$ is unique upto permutation and isomorphism of factors.

*Proof.* If $A \cong \prod_{i=1}^{n} K_i \cong \prod_{j=1}^{m} L_j$, then the number of factors is determined by the maximal number of inequivalent idempotents in $A$, showing $n = m$. Then the projections $\prod K_i \twoheadrightarrow L_j$ and $\prod L_j \twoheadrightarrow K_i$ show by Proposition 3.5.6(b) that each $K_i$ is isomorphic to some $L_j$ and conversely; this suffices. ∎

## 3.6 Grothendieck's Version of the Fundamental Theorem of Galois Theory

First, we talk about continuous group actions on discrete space.

**Lemma 3.6.1.** Let $G$ be a topological group acting (not necessarily continuously) on a discrete space $X$. Then the action of $G$ on $X$ is continuous iff each stabilizer $G_x$ for $x \in X$ is open in $G$.

*Proof.* Let $\mu : G \times X \to X$ denote the action. For $x \in X$, the intersection of the preimage $\mu^{-1}(x) = \{(g, y) : gy = x\}$ with each "slice" $G \times \{y\}$ is either a homeomorphic copy of $G_x \subset G$ (if $x$ and $y$ are in the same orbit) or empty (if not). Therefore, if $\mu$ is continuous, then $G_x = \mu^{-1}(x) \cap G \times \{x\} \subset G$ is open; conversely, if $G_x$ is open, then $\mu^{-1}(x) \subset G \times X$ is open for each $x \in X$. ∎

Again, we start with a field $k \subset k^s \subset \overline{k}$, and let $G_k := \mathrm{Gal}(k^s/k)$ be its absolute Galois group. Let $L/k$ be a finite separable extension; we don't consider $L$ as a subextension of $k^s$ in any particular way. We know that $|\mathrm{Hom}_k(L, k^s)| = [L : k]_s = [L : k] < \infty$, and so we may consider the finite set $\mathrm{Hom}_k(L, k^s)$ on which $G_k$ acts on the left by postcomposition. Given a $\varphi \in \mathrm{Hom}_k(L, k^s)$, the stabilizer $(G_k)_\varphi = \mathrm{Gal}(k^s/\varphi(L))$, which is an open normal subgroup of $G_k$ by the Fundamental Theorem of Galois Theory; therefore, the above lemma shows that this $G_k$ action is continuous. Further, this action is also transitive: indeed, if $\varphi, \psi \in \mathrm{Hom}_k(L, k^s)$, then by Lemma 3.1.15(b), the $k$-isomorphism $\psi \circ \varphi^{-1} : \varphi(L) \to \psi(L)$ of subextensions of $k^s$ extends to an element $\sigma \in G_k$, so that $\psi = \sigma \circ \varphi$. In particular, this shows that $\mathrm{Hom}_k(L, k^s)$ is a left coset space of some open subgroup in $G_k$; when $L/k$ is Galois, then it is in fact a quotient by an open normal subgroup, namely $\mathrm{Gal}(k^s/\varphi(L))$ for one (and hence any) $\varphi \in \mathrm{Hom}_k(L, k^s)$. If $L, L'$ are two such finite separable extensions and $\theta : L \to L'$ a $k$-homomorphism, then we get a pullback map $\theta^* : \mathrm{Hom}_k(L', k^s) \to \mathrm{Hom}_k(L, k^s)$, which is clearly a $G_k$-set morphism. Therefore, associating to an extension $L/k$ the set $\mathrm{Hom}_k(L, k^s)$ gives us a contravariant functor from the category of finite separable extensions of $k$ to the category of finite sets with transitive continuous left $G_k$-action; briefly, transitive finite left $G_k$-sets.

**Theorem 3.6.2.** The association $L \mapsto \mathrm{Hom}_k(L, k^s)$ gives an antiequivalence between the categories of finite separable extensions $L/k$ and transitive finite left $G_k$-sets. Further, under this antiequivalence, Galois extensions correspond to $G_k$-sets isomorphic to finite quotient groups of $G_k$.

*Proof.* We show that this functor is essentially surjective and fully faithful. For the first, let $S$ be a transitive finite left $G_k$-set and pick an $s \in S$. The stabilizer $(G_k)_s \subset G_k$ is an open subgroup, so by the Fundamental Theorem of Galois Theorem is of the form $\mathrm{Gal}(k^s/L)$ for some finite separable subextension $L/k$. Let $\iota : L \hookrightarrow k^s$ denote the inclusion, and define a $G_k$-homomorphism $\mathrm{Hom}_k(L, k^s) \to S$ by $g\iota \mapsto gs$ for $g \in G_k$. This is well-defined and injective by $\mathrm{Gal}(k^s/L) = (G_k)_s$ and surjective because is a map of transitive $G_k$-sets.

To show fully faithfulness, we have to show that for finite separable extensions $L, M/k$ the map $-^* : \mathrm{Hom}_k(L, M) \to \mathrm{Hom}_{G_k}(\mathrm{Hom}_k(M, k^s), \mathrm{Hom}_k(L, k^s))$ is bijective, for which we construct a map in the opposite direction. Let $\iota \in \mathrm{Hom}_k(M, k^s)$ be a fixed element. Then a $G_k$-homomorphism $\eta : \mathrm{Hom}_k(M, k^s) \to \mathrm{Hom}_k(L, k^s)$ determines and is determined by the element $\eta(\iota) \in \mathrm{Hom}_k(L, k^s)$ by transitivity. Since $\eta$ is a $G_k$-homomorphism, it follows that the stabilizers $(G_k)_\iota \subset (G_k)_{\eta(\iota)}$ and so by the Fundamental Theorem of Galois Theory, we conclude that

$$\mathrm{Gal}(k^s, \iota M) = (G_k)_\iota \subset (G_k)_{\eta(\iota)} = \mathrm{Gal}(k^s, \eta(\iota)N) \Rightarrow \iota M \supset \eta(\iota)N.$$

Therefore, the composite $L \xrightarrow{\eta} (\iota)N \subset \iota M \xrightarrow{\iota^{-1}} M$ is a $k$-algebra homomorphism, i.e. an element of $\mathrm{Hom}_k(L, M)$. The proof that these constructions give inverse bijections is left as a very easy exercise to the reader.

The last observation is clear from the above discussion. ∎

We can now ask what all finite left $G_k$-sets are (not necessarily transitive). Note that for an étale $k$-algebra $A$, the set $\mathrm{Hom}_k(A, k^s)$ is still acted on the left by $G_k$ and indeed the decomposition of Proposition 3.5.6(b)

is a $G_k$-set isomorphism. In particular, $\mathrm{Hom}_k(A, k^s)$ is a finite left $G_k$-set. The next theorem shows that these are, in fact, all.

**Theorem 3.6.3** (Fundamental Theorem of Galois Theory–Grothendieck's Version)**.** The association $A \mapsto \mathrm{Hom}_k(A, k^s)$ gives an antiequivalence of categories of étale algebras $A/k$ and finite left $G_k$-sets. Further, under this equivalence, separable field extensions correspond to transitive finite left $G_k$-sets, and Galois extensions correspond to finite quotient groups of $G_k$.

*Proof.* For essential surjectivity, let $S$ be a transitive finite $G_k$-set and write $S = \coprod_{i=1}^n S_i$ as a disjoint union of its orbits. By the previous theorem, for each $i = 1, \dots, n$, there is a finite separable extension $K_i/k$ and a $G_k$-set isomorphism $\mathrm{Hom}_k(K_i, k^s) \to S_i$. If we take $A := \prod_{i=1}^n K_i$, then it follows easily that

$$\mathrm{Hom}_k(A, k^s) \cong \coprod_{i=1}^n \mathrm{Hom}_k(L_i, k^s) \xrightarrow{\sim} \coprod_{i=1}^n S_i = S$$

is an isomorphism of $G_k$-sets. Similarly, for fully faithfulness, note that by Proposition 3.5.6(c) and the above theorem, we have that if $A = \prod_{i=1}^n K_i$ and $B = \prod_{j=1}^m L_j$ are two étale algebras, then

$$\mathrm{Hom}_k(A, B) \cong \coprod_{i,j} \mathrm{Hom}_k(K_i, L_j) \xrightarrow{\sim} \coprod_{i,j} \mathrm{Hom}_{G_k}(\mathrm{Hom}_k(L_j, k^s), \mathrm{Hom}_k(K_i, k^s)) \cong \mathrm{Hom}_{G_k}(\mathrm{Hom}_k(B, k^s), \mathrm{Hom}_k(A, k^s)),$$

where the last isomorphism follows from the fact that a $G_k$-morphism $\mathrm{Hom}_k(B, k^s) \to \mathrm{Hom}_k(A, k^s))$ must preserve decomposition into orbits.

The rest of the observations are clear from the above discussion. ∎

## 3.7 Transcendence Theory

**Definition 3.7.1.** Let $R \subseteq S$ be a ring extension and $X := \{s_\lambda\}_{\lambda \in \Lambda}$ a collection of elements of $X$.

(a) The *the ring generated over $R$ by $X$* is the smallest subring $R[X] \subseteq S$ containing both $R$ and $X$, i.e. the image of the evaluation homomorphism $\mathrm{eval}_X : R[T_\lambda]_{\lambda \in \Lambda} \to R$.
(b) We say that the subset $X$ is *algebraically independent* over $R$ if $\ker \mathrm{eval}_X = (0)$, in which case $R[T_\lambda]_{\lambda \in \Lambda}$ maps isomorphically to $R[X]$; otherwise we say that $X$ is algebraically dependent.
(c) If $s \in S$ is any element, then $s$ is said to be *transcendental* over $R$ if the set $X = \{s\}$ is algebraically independent; else it is algebraic.
(d) If $R$ and $S$ are fields, then the the *field generated over $R$ by $X$* is the smallest subfield $R(X) \subseteq S$ containing both $R$ and $X$, and it is simply $R(X) := \mathrm{Frac}\, R[X]$.

Now suppose that $k \subseteq L$ is a field extension. Define a function $\mathfrak{D} : 2^L \to 2^L$ by $\mathfrak{D}X = \mathrm{Cl}_L(k(X))$. We claim that this is a dependence relation, called *algebraic dependence* over $k$. Indeed, conditions (a) and (d) are trivial. To show (b), note that $\mathfrak{D}X$ is a field by Lemma 2.1.6(c) and so $\mathfrak{D}^2X = \mathrm{Cl}_L k(\mathfrak{D}X) = \mathrm{Cl}_L \mathfrak{D}X = \mathrm{Cl}_L(\mathrm{Cl}_L k(X)) = \mathrm{Cl}_L k(X) = \mathfrak{D}X$ where we have used Corollary 2.1.4(d). Finally, to show exchange, first note that $\mathfrak{D}X = \{y \in L : \exists n \geq 1, a_0, \dots, a_n \in k[X] : a_0 \neq 0 \text{ and } a_0 y^n + \cdots + a_n = 0\}$. Suppose that $x \in X \subseteq L$ and $y \in \mathfrak{D}X \setminus \mathfrak{D}(X \setminus \{x\})$; then for some $n \geq 1$ and $a_0, \dots, a_n \in k[X]$ with $a_0 \neq 0$ we have $a_0 y^n + \cdots + a_n = 0$. Rearrange the terms in this identity to write it out in powers of $x$, i.e. write it as $b_0 x^m + \cdots + b_m = 0$ for some $m \geq 0$ with $b_0 \neq 0$ and $b_i \in k[(X \setminus \{x\}) \cup \{y\}]$. If $m = 0$, then $b_0 = 0$ still has a nonzero power of $y$ and then shows that $y \in \mathfrak{D}(X \setminus \{x\})$, a contradiction; therefore $m \geq 1$ and we have shown that $x \in \mathfrak{D}((X \setminus \{x\}) \cup \{y\})$ as needed. It is immediate to see that that a subset $X \subseteq L$ is algebraically independent over $k$ as in the previous definition iff it is independent for the dependence relation $\mathfrak{D}$.

**Definition 3.7.2.** Let $k \subseteq L$ be a field extension and consider the dependence relation $\mathfrak{D}$ on $L$ of algebraic dependence over $k$. Then a basis for this dependence relation is called a *transcendence basis* for $L$ over $k$. The dependency of $L$ is called the *transcendence degree* of $L$ over $k$ and is written $\mathrm{trdeg}_k L$. More generally, if $R$ is a domain containing $k$, we define its transcendence degree over $k$ to be $\mathrm{trdeg}_k R := \mathrm{trdeg}_k \mathrm{Frac}\, R$.

Note that a field extension is algebraic iff it has transcendence degree 0. Clearly, $\mathrm{trdeg}_k k(X_1, \dots, X_n) = n$ almost by definition. Next, observe that if $k \subseteq K \subseteq L$ is a tower of extensions, then clearly $\mathrm{trdeg}_k L = \mathrm{trdeg}_k K + \mathrm{trdeg}_K L$.

**Example 3.7.3.** We show that $\operatorname{trdeg}_{\mathbf{Q}} \mathbf{C} = \mathfrak{c}$. For that, first note that if $k$ is a countable field, then so is $k[X]$ by separating by degree and then so is $k(X) = \operatorname{Frac} k[X]$ because it injects into $k[X] \times k[X]$. If $K/k$ is an algebraic extension of a countable field, then $K = \bigcup_{0 \neq f \in k[X]} \{\alpha \in K : f(\alpha) = 0\}$ being a countable union of finite sets is countable as well. Given this, if $X = \{x_n\}_{n \geq 1}$ is an atmost countable transcendence basis of $\mathbf{C}$ over $\mathbf{Q}$, then if we let $K_0 := \mathbf{Q}$ and $K_n := K_{n-1}(x_n)$ for $n \geq 1$, then $\mathbf{Q}(X) = \bigcup_{n \geq 0} K_n$ is a countable union of countable sets and so countable; and then the algebraicity of $\mathbf{C}$ over $\mathbf{Q}(X)$ would show that $\mathbf{C}$ is countable as well, which is absurd. The Lefschetz principle (as well as another proof of the Nullstellensatz for $k = \mathbf{C}$, see [TO CITE: HARRIS]) makes use of this observation.

## 3.8 Differential Bases

**Definition 3.8.1.** Let $k \subseteq L$ be a field extension. Then the module $\Omega_{L/k}$ of Kähler differentials is an $L$-vector space and so has a linear dependence relation LD. If $\mathrm{d} : L \to \Omega_{L/k}$ is the universal differential, then the pullback dependence relation $\mathrm{d}^*\mathrm{LD}$ on $L$ is called *differential dependence*.

Clearly, $\operatorname{dep} \mathrm{d}^*\mathrm{LD} = \dim_L \Omega_{L/k}$. In characteristic 0, we'll show that differential dependence is the exact same thing as algebraic dependence, from which it would follows that $\operatorname{trdeg}_k L = \dim_L \Omega_{L/k}$. This amounts to showing that if any differential extends uniquely across a separable algebraic extension. In positive characteristic $p$, differential bases are what are called *$p$-bases*.

# 4 Associated Primes and Primary Decomposition

## 4.1 Associated Primes

**Definition 4.1.1.** Let $R$ be a ring and $M$ be an $R$-module.

(a) The set $\mathrm{Ass}_R(M)$ of primes *associated* to $M$ is defined to be $\{\mathfrak{p} \subset R : \mathfrak{p} = \mathrm{Ann}(m) \text{ for some } m \in M\}$.
(b) The minimal primes in $\mathrm{Ass}_R(M)$ are called *isolated*, and the non-minimal ones are called *embedded*.
(c) The *support* $\mathrm{Supp}(M)$ of $M$ is defined to be $\{\mathfrak{p} \subset R : M_\mathfrak{p} \neq \emptyset\}$.

If $\mathfrak{a} \subseteq R$ is an ideal, then the primes associated to $M := R/\mathfrak{a}$ are called the *associated primes of* $\mathfrak{a}$.

If $\mathfrak{p} \in \mathrm{Ass}_R(M)$, then certainly $\mathfrak{p} \supseteq \mathrm{Ann}(M)$. If $\mathfrak{p} \subset R$ is prime, then $\mathfrak{p}$ is the only associated prime of $\mathfrak{p}$, i.e. $\mathrm{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$. If $\mathfrak{a} \subseteq R$ is any ideal, then $\mathrm{Supp}(R/\mathfrak{a}) = \mathbf{V}(\mathfrak{a})$.

**Theorem 4.1.2** (Associated Primes)**.** Let $R$ be a ring, $M, M', M''$ be $R$-modules, and $S \subseteq R$ be a multiplicative subset.

(a) If $\mathfrak{A} := \{\mathrm{Ann}(m) : 0 \neq m \in M\}$, then a maximal element of $\mathfrak{A}$ is prime.
(b) We have $\mathrm{Ass}_R(M) \subseteq \mathrm{Supp}(M) \subseteq \mathbf{V}(\mathrm{Ann}\, M)$.
(c) The union $\bigcup \mathrm{Ass}_R(M) \subseteq \mathcal{Z}(M)$.
(d) We have $\mathrm{Ass}_{S^{-1}R}(S^{-1}M) \supseteq \{\mathfrak{p}S^{-1}R : \mathfrak{p} \in \mathrm{Ass}_R(M), \mathfrak{p} \cap S = \emptyset\}$.
(e) If $0 \to M' \to M \to M'' \to 0$ is an SES, then $\mathrm{Ass}_R(M) \subseteq \mathrm{Ass}_R(M') \cup \mathrm{Ass}_R(M'')$.

Next suppose that $R$ is Noetherian and $M$ is finitely generated.

(f) If $0 \neq M$, then $\mathrm{Ass}_R(M) \neq \emptyset$.
(g) Equality holds in the second part of (b) (i.e. $\mathrm{Supp}(M) = \mathbf{V}(\mathrm{Ann}\, M)$[2] and in (c) and (d).
(h) If $0 \neq M$ and $M$ is finitely generated, then there is a filtration by submodules $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ such that each successive quotient $M_i/M_{i+1} \cong R/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i \subset R$. In particular, $\mathrm{Ass}_R(M)$ is finite.
(i) The sets of minimal elements of $\mathrm{Ass}_R(M)$, $\mathrm{Supp}(M)$ and $\mathbf{V}(\mathrm{Ann}\, M)$ coincide.
(j) If $\mathfrak{a} \subseteq R$ is any ideal, then either $\mathfrak{a}$ contains a nonzerodivisor of $M$ or $\mathfrak{a} \subseteq \mathrm{Ann}(m)$ for some $m \in M$.

*Proof.* For (a), suppose that $\mathfrak{a} = \mathrm{Ann}(m) \in \mathfrak{A}$ is a maximal and $xy \in \mathfrak{a}$ but $y \notin \mathfrak{a}$. Then $xym = 0$ but $ym \neq 0$ implies that $x \in \mathrm{Ann}(ym) \in \mathfrak{A}$ and $\mathrm{Ann}(m) \subseteq \mathrm{Ann}(ym)$ so by maximality $\mathfrak{a} = \mathrm{Ann}(m) = \mathrm{Ann}(ym) \ni x$. For (b), if $\mathfrak{p} \in \mathrm{Ass}_R(M)$, then for some $0 \neq m \in M$ we have $\mathfrak{p} = \mathrm{Ann}(m)$ and so $R/\mathfrak{p} \cong Rm \hookrightarrow M$. We claim that $0 \neq 1^{-1}m \in M_\mathfrak{p}$; indeed, if not, then $tm = 0$ for some $t \notin \mathfrak{p}$, which is not possible. (Equivalently, since $R/\mathfrak{p} \hookrightarrow M$ and $R_\mathfrak{p}$ is flat over $R$, tensoring gives us an injection $\kappa(\mathfrak{p}) = R/\mathfrak{p} \otimes_R R_\mathfrak{p} \hookrightarrow M_\mathfrak{p}$, and the former is a field.) Similarly, if $M_\mathfrak{p} \neq \emptyset$, then we must have $\mathfrak{p} \supseteq \mathrm{Ann}(M)$, so that $\mathrm{Supp}(M) \subseteq \mathbf{V}(\mathrm{Ann}\, M)$. The statement in (c) is clear. For (d), if $\mathfrak{p} = \mathrm{Ann}(m)$ and $\mathfrak{p} \cap S = \emptyset$, then we claim that $\mathfrak{p}S^{-1}R = \mathrm{Ann}(1^{-1}m)$. Indeed, $\mathfrak{p}S^{-1}R \subseteq \mathrm{Ann}(1^{-1}m)$ is clear; conversely, if $(s^{-1}x)(1^{-1}m) = 0$ for some $x \in R, s \in S$, then $txm = 0$ for some $t \in S$ and so $tx \in \mathrm{Ann}(m) = \mathfrak{p}$; since $t \notin \mathfrak{p}$, we conclude that $x \in \mathfrak{p}$, and so $\mathrm{Ann}(1^{-1}m) \subseteq \mathfrak{p}S^{-1}R$. For (e), suppose $\mathfrak{p} \in \mathrm{Ass}_R(M) \setminus \mathrm{Ass}_R(M')$; then there is an $m \in M \setminus M'$ such that $\mathfrak{p} = \mathrm{Ann}(m)$. We claim that $\mathfrak{p} = \mathrm{Ann}(\overline{m}) \in \mathrm{Ass}_R(M'')$. Indeed, $\mathfrak{p} \subseteq \mathrm{Ann}(\overline{m})$ clearly; conversely, if $x \in \mathrm{Ann}(\overline{m}) \setminus \mathfrak{p}$, then is such that $\mathrm{Ann}(xm) = \mathfrak{p}$, a contradiction.

For (f), if $0 \neq M$, then the $\mathfrak{A}$ of (a) is nonempty; by the Noetherian hypothesis it has a maximal element, and that is an associated prime of $M$ by (a). For (g), for the first one, suppose $\mathfrak{p}$ is a prime containing $\mathrm{Ann}(M)$ and $M_\mathfrak{p} = 0$; then for each of the finitely many generators $m_i$ of $M$ there is an $s_i \notin \mathfrak{p}$ such that $s_i m_i = 0$ and then $\prod_i s_i \in \mathrm{Ann}(M) \setminus \mathfrak{p}$, a contradiction. To show equality in (c), if $r \in \mathcal{Z}(M)$, then $r \in \mathrm{Ann}(m)$ for some $0 \neq m \in M$. Consider the set $\mathfrak{A}' := \{\mathrm{Ann}(m') : 0 \neq m' \in M, \mathrm{Ann}(m') \supseteq \mathrm{Ann}(m)\}$. This is nonempty since $\mathrm{Ann}(m) \in \mathfrak{A}'$. Therefore, by the Noetherian hypothesis it has a maximal element $\mathrm{Ann}(m') \in \mathfrak{A}'$. Then this $\mathrm{Ann}(m')$ is also maximal in the $\mathfrak{A}$ of (a), and so $\mathrm{Ann}(m') \in \mathrm{Ass}_R(M)$. It follows that $r \in \mathrm{Ann}(m) \subseteq \mathrm{Ann}(m') \subseteq \bigcup \mathrm{Ass}_R(M)$. For equality in (d), let $\mathfrak{P} \in \mathrm{Ass}_{S^{-1}R}(S^{-1}M)$ so $\mathfrak{P} = \mathrm{Ann}(s^{-1}m)$ for some $s \in S, m \in M$. Then by Corollary 1.2.8(d), we have $\mathfrak{P} = \mathfrak{p}S^{-1}R$ for some prime $\mathfrak{p} \subset R$ disjoint from $S$. In this case, if $x \in \mathrm{Ann}(m)$, then $1^{-1}x \in \mathrm{Ann}(s^{-1}m) = \mathfrak{P}$ and so $x \in \eta^{-1}\mathfrak{P} = \mathfrak{p}$ (again using Corollary 1.2.8(d) for the last step); this shows $\mathrm{Ann}(m) \subseteq \mathfrak{p}$. If $x \in \mathfrak{p}$, then $1^{-1}x \in \mathfrak{p}S^{-1}R = \mathfrak{P} = \mathrm{Ann}(s^{-1}m) \Rightarrow txm = 0$ for some $t \in S$, i.e. $tx \in \mathrm{Ann}(m)$ for some $t \in S$. Since $R$ is Noetherian, if $\mathfrak{p} = \langle x_i \rangle$, then picking $t_i$ as above and letting $t = \prod_i t_i \in S$, we conclude that $\mathfrak{p} \subseteq \mathrm{Ann}(tm)$. But $\mathfrak{P} = \mathrm{Ann}((ts)^{-1}tm)$ then shows by the above that $\mathrm{Ann}(tm) \subseteq \mathfrak{p}$ as well, so $\mathfrak{p} = \mathrm{Ann}(tm)$. For (h), we'll relabel the filtration as $M = M_n \supsetneq M_{n-1} \supsetneq \cdots \supsetneq M_0 = 0$ for convenience. Since $0 \neq M$, by (e) we have $\mathrm{Ass}_R(M) \neq \emptyset$, so let $\mathfrak{p}_1 = \mathrm{Ann}(m_1) \in \mathrm{Ass}_R(M)$ and consider $R/\mathfrak{p} \cong Rm_1 =: M_1 \hookrightarrow M$. If $M_1 = M$, we are done. Else, $M/M_1 \neq 0$, so

[2] Actually, this doesn't need $R$ to be Noetherian, only $M$ to be finitely generated, as is clear from the proof.

pick a $\mathfrak{p}_2 = \mathrm{Ann}(\overline{m_2}) \in \mathrm{Ass}_R(M/M_1)$. Then let $M_2 = Rm_1 + Rm_2$; in that case, $M_2/M_1 \cong R\overline{m_2} \cong R/\mathfrak{p}_2$. If $M_2 = M$ we are done; else continue. This process must terminate because $M$ is a Noetherian $R$-module. Finiteness of $\mathrm{Ass}_R(M)$ follows by induction on $n$ and repeatedly using (e). For (i), for any $\mathfrak{p} \in \mathbf{V}(\mathrm{Ann}\, M)$ by equality in (d), we have $\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p})$ is in bijection with primes $\mathfrak{q} \subseteq \mathfrak{p}$ such that $\mathfrak{q} \in \mathrm{Ass}_R(M)$ (so certainly $\mathfrak{q} \in \mathbf{V}(\mathrm{Ann}\, M)$), so that if $\mathfrak{p}$ is minimal in $\mathbf{V}(\mathrm{Ann}\, M)$, then $\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p})$ is either empty or $\{\mathfrak{p}R_\mathfrak{p}\}$. Since $M_\mathfrak{p} \neq 0$ by equality in the second part of (b), we have $\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) \neq \emptyset$ by (f), and so $\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) = \{\mathfrak{p}R_\mathfrak{p}\}$, so by equality in (d), we have $\mathfrak{p} \in \mathrm{Ass}_R(M)$. This shows that a minimal element of $\mathrm{Supp}(M)$ belongs to $\mathrm{Ass}_R(M)$ and hence is a minimal element of $\mathrm{Ass}_R(M)$. Conversely, if $\mathfrak{p} \in \mathrm{Ass}_R(M)$ is a minimal element, then by Lemma 1.1.4(b) there is a minimal prime of $\mathbf{V}(\mathrm{Ann}\, M)$ contained in $\mathfrak{p}$; by the above reasoning it belongs to $\mathrm{Ass}_R(M)$, but then by minimality of $\mathfrak{p}$ in $\mathrm{Ass}_R(M)$ it has to be equal to $\mathfrak{p}$. Therefore, a minimal element in $\mathrm{Ass}_R(M)$ remains minimal in $\mathrm{Supp}(M)$. For (j), apply equality in (c), finiteness of $\mathrm{Ass}_R(M)$, and Prime Avoidance (Lemma 1.1.3(b)). ∎

**Counterexample 4.1.3.** Theorem 4.1.2(f) is not true when $R$ is not Noetherian. For instance [TO CITE: MSE], take $R = M = \mathscr{C}(\mathbf{R}, \mathbf{R})$ to be the ring of continuous functions $\mathbf{R} \to \mathbf{R}$. If $0 \neq f \in \mathscr{C}(\mathbf{R}, \mathbf{R})$, then there exist $x \neq y \in \mathbf{R}$ with $f(x), f(y) \neq 0$. If $g, h \in \mathscr{C}(\mathbf{R}, \mathbf{R})$ are functions such that $g(x) = h(y) = 1$ but $gh = 0$, then $g, h \notin \mathrm{Ann}(f)$ but $gh \in \mathrm{Ann}(f)$, so $\mathrm{Ann}(f)$ is not prime.

## 4.2 Primary Submodules

**Theorem 4.2.1** (Primary Submodules)**.** Let $R$ be a ring and $M$ be an $R$-module. For a submodule $N \subseteq M$, TFAE:

(a) For all $x \in R$ and $m \in M$ if $xm \in N$ then either $m \in N$ or there is an $n \geq 1$ such that $x^n M \subseteq N$.
(b) The set $\mathcal{Z}(M/N) \subseteq \sqrt{\mathrm{Ann}(M/N)}$.

In this case:

(c) If $N \subsetneq M$ is proper, then $\sqrt{\mathrm{Ann}(M/N)}$ is prime.
(d) There is at most one prime associated to $M/N$, namely $\sqrt{\mathrm{Ann}(M/N)}$.

When $R$ is Noetherian, $M$ is finitely generated, and $N \subsetneq M$ proper, (a) and (b) are also equivalent to:

(e) There is a unique prime associated to $M/N$.

*Proof.* The equivalence of (a) and (b) is immediate. For (c), since $N \subsetneq M$, we have that $\sqrt{\mathrm{Ann}(M/N)}$ is proper. If $x, y \in R$ are such that $xy \in \sqrt{\mathrm{Ann}(M/N)}$, then there is a $k \geq 1$ such that $(xy)^k \in \mathrm{Ann}(M/N)$. If $y \notin \sqrt{\mathrm{Ann}(M/N)}$, then there is an $m \in M$ such that $y^k m \notin N$. By (a), we conclude that there is an $n \geq 1$ such that $x^{nk} M \subseteq N$, i.e. that $x \in \sqrt{\mathrm{Ann}(M/N)}$. To show (b) ⇒ (d), let $\mathfrak{p} \in \mathrm{Ass}_R(M/N)$ (so necessarily $N \subsetneq M$). Then for all $x \in \mathfrak{p}$ we have $x \in \mathcal{Z}(M/N)$ by Theorem 4.1.2(c) and so by (b) we have $\sqrt{\mathrm{Ann}(M/N)} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p} \subseteq \sqrt{\mathrm{Ann}(M/N)}$, so that $\mathfrak{p} = \sqrt{\mathrm{Ann}(M/N)}$.

When these conditions hold, the implication (b) ⇒ (e) is clear: since $M/N \neq 0$, we have $\mathrm{Ass}_R(M/N) \neq \emptyset$ by Theorem 4.1.2(f) and so we have $\mathrm{Ass}_R(M/N) = \{\sqrt{\mathrm{Ann}(M/N)}\}$ by (d). Conversely, if $\mathrm{Ass}_R(M/N) = \{\mathfrak{p}\}$, then by Theorem 4.1.2(g), we have $\mathcal{Z}(M/N) = \mathfrak{p}$. Since $\sqrt{\mathrm{Ann}(M/N)} = \bigcap_{\mathfrak{q} \supseteq \mathrm{Ann}(M/N)} \mathfrak{q}$, to show that $\mathcal{Z}(M/N) \subseteq \sqrt{\mathrm{Ann}(M/N)}$, it suffices to show that each prime $\mathfrak{q}$ containing $\mathrm{Ann}(M/N)$ contains $\mathfrak{p}$, so let $\mathfrak{q}$ be a prime containing $\mathrm{Ann}(M/N)$. By Lemma 1.1.4(b), we have that $\mathfrak{q}$ contains a minimal prime over $\mathrm{Ann}(M/N)$, but by Theorem 4.1.2(j), such a minimal prime must be an element of $\mathrm{Ass}_R(M)$, i.e. must be $\mathfrak{p}$. ∎

**Definition 4.2.2.** Let $R$ be a ring and $M$ an $R$-module. A proper submodule $N \subsetneq M$ is said to be *primary* if it satisfies equivalent conditions (a) and (b) of Theorem 4.2.1. In this case, if $\mathfrak{p} := \sqrt{\mathrm{Ann}(M/N)}$, then we say that $N$ is *primary* to prime $\mathfrak{p}$ or simply $\mathfrak{p}$-primary.

**Example 4.2.3.** If $R = \mathbf{Z}$, the primary ideals are (0) and $(p^r)$ for primes $p$, integers $r \geq 1$. In any ring $R$, any prime $\mathfrak{p}$ is $\mathfrak{p}$-primary. For any $r \geq 1$ we certainly have $\sqrt{\mathfrak{p}^r} = \mathfrak{p}$, but $\mathfrak{p}^r$ is not necessarily primary–see the next counterexample. However, this can be corrected by looking at *symbolic powers* of primes instead; see Definition 4.2.6. On the other hand, this *is* true if $\mathfrak{p} = \mathfrak{m}$ is maximal by the following lemma. From the same lemma we also get an example of a primary ideal that is not a prime power: take $I = (X, Y^2) \subseteq k[X, Y]$.

**Counterexample 4.2.4.** (The quadric cone in $\mathbf{A}^3$.) Let $R := k[X, Y, Z]/(XY - Z^2)$ and $\mathfrak{p} = (x, z)$. Now $xy = z^2 \in \mathfrak{p}^2$ but $x \notin \mathfrak{p}^2$ and also $y \notin \sqrt{\mathfrak{p}^2} = \mathfrak{p}$, which tells us that $\mathfrak{p}^2$ is not primary.

**Lemma 4.2.5.** Let $R$ be a ring.

(a) Prime ideals are primary.

(b) An ideal $\mathfrak{a}$ is primary iff every zero divisor in $R/\mathfrak{a}$ is nilpotent.
(c) If $\mathfrak{a}$ is primary, then $\sqrt{\mathfrak{a}}$ is prime and is the unique minimal prime containing $\mathfrak{a}$.
(d) If $\mathfrak{a} \subset R$ is an ideal such that $\sqrt{\mathfrak{a}} = \mathfrak{m}$ is maximal, then $\mathfrak{a}$ is $\mathfrak{m}$-primary.
(e) If $\mathfrak{a} \subset R$ is an ideal and $\mathfrak{m} \subset R$ a maximal ideal such that $\mathfrak{m}^n \subseteq \mathfrak{a} \subseteq \mathfrak{m}$ for some $n \geq 1$, then $\mathfrak{a}$ is $\mathfrak{m}$-primary.

*Proof.* The statements in (a) through (c) are clear ((c) uses that $\sqrt{\mathfrak{a}}$ is the intersection of primes containing $\mathfrak{a}$). For (d), suppose $xy \in \mathfrak{a}$ and $x \notin \sqrt{\mathfrak{a}} = \mathfrak{m}$. Then $\mathfrak{m} + (x) = (1)$, so $m + ax = 1$ for some $a \in R$. Now $m \in \sqrt{\mathfrak{a}}$ so for some $n \geq 1$ we have $m^n \in \mathfrak{a}$. Then $1 = 1^n = (m + ax)^n = m^n + bx$ for some $b \in R$, so multiplying by $y$ gives $y = m^n y + bxy \in \mathfrak{a}$. The statement in (e) is clear from (d). ∎

**Definition 4.2.6.** Let $R$ be a ring and $\mathfrak{p} \subset R$ a prime. Let $\eta : R \to R_{\mathfrak{p}}$ be the localization map. For any integer $n \geq 1$, define the $n^{\text{th}}$ *symbolic power* of $\mathfrak{p}$ to be $\mathfrak{p}^{(n)} := \eta^{-1}(\mathfrak{p}^n R_{\mathfrak{p}})$.

An element $x \in \mathfrak{p}^{(n)}$ iff there is an $s \notin \mathfrak{p}$ and $z \in \mathfrak{p}^n$ such that $sx = z$. These satisfy $\mathfrak{p}^n \subseteq \mathfrak{p}^{(n)} \subseteq \mathfrak{p}$ for every $n \geq 1$, and so $\sqrt{\mathfrak{p}^{(n)}} = \mathfrak{p}$. Further, $\mathfrak{p}^{(1)} \supseteq \mathfrak{p}^{(2)} \supseteq \cdots$. Finally, these are all $\mathfrak{p}$-primary, as is easily verified.

From now on, we make the assumption that $R$ is a Noetherian ring and $M$ a finitely generated $R$-module. From this we get some useful things like:

**Lemma 4.2.7.** If $\mathfrak{p} \subset R$ is a prime and $N_1, \ldots, N_r \subset M$ modules which are $\mathfrak{p}$-primary, then so is $N_1 \cap \cdots \cap N_r$.

*Proof.* By Theorem 4.1.2(e), we have $\emptyset \subsetneq \operatorname{Ass}_R M/\bigcap_i N_i \subsetneq \operatorname{Ass}_R \bigoplus_i M/N_i \subseteq \bigcup_i \operatorname{Ass}_R M/N_i = \{\mathfrak{p}\}$, and so we are done by Theorem 4.2.1(e). ∎

**Definition 4.2.8.** If $M$ is an $R$-module, and $N \subseteq M$ is a submodule, then a *primary decomposition* of $N$ is an expression

$$N = N_1 \cap \cdots \cap N_r$$

where the $N_i$ are $\mathfrak{p}_i$-primary submodules of $M$ for primes $\mathfrak{p}_i \subset R$. We say that this decomposition is *reduced* if all the $\mathfrak{p}_i$ are distinct and moreover $N$ is not the intersection of any proper subcollection of the $N_i$. In this case, the $N_i$ are called the *primary components* of $N$.

Any primary decomposition gives rise to a reduced decomposition; indeed, first discard the redudant $N_i$, and then use the previous lemma to intersect all $N_i$ that are primary to the same prime. Iterate this finitely many times if needed; this process must end eventually since we only started with finitely many $N_i$ to begin with. We now show the existence of a primary decomposition.

**Definition 4.2.9.** Given any $R$-module $M$, a proper submodule $N \subsetneq M$ is called *irreducible* if it cannot be written as $N = N_1 \cap N_2$ for $N_1, N_2 \subseteq M$ submodules with $N \subsetneq N_i$ for $i = 1, 2$.

**Theorem 4.2.10.** Let $R$ be a Noetherian ring and $M$ a f.g. $R$-module. Then:

(a) Every irreducible submodule of $M$ is primary.
(b) Every proper submodule of $M$ has a minimal primary decomposition.

*Proof.*

(a) Suppose $N \subseteq M$ is not primary; then we have to show that $N$ is reducible. Firstly, replacing $M$ by $M/N$, we can assume that $N = 0$. To say that 0 is not primary implies by Theorem 4.2.1(e) that $\operatorname{Ass} M$ contains two distinct primes, say $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Then there are $x_1, x_2 \in M$ such that $R/\mathfrak{p}_i \cong Rx_i \hookrightarrow M$ for $i = 1, 2$. It further follows that if $y_i \in Rx_i$ is any nonzero element, then $\operatorname{Ann}(y_i) = \mathfrak{p}_i$ (check; this uses that $\mathfrak{p}_i$ is prime). It follows that $Rx_1 \cap Rx_2 = (0)$, so that $(0)$ is reducible.
(b) We have to show the existence of a decomposition into irreducibles, which is a standard Noetherian induction.

∎

From this, we have:

**Corollary 4.2.11** (Lasker-Noether)**.** Every proper ideal of a Noetherian ring admits a primary decomposition.

Next, we turn to uniqueness. Here the picture cannot be too nice, as the following counterexamples show.

**Counterexample 4.2.12.** Let $I = (X^2, XY) \subseteq k[X, Y]$. Then $(X^2) \subset I \subset (X)$ and so $\sqrt{I} = (X)$, but this is not maximal; indeed, $XY \in I$ but $X \notin I$ and $Y \notin \sqrt{I}$ shows us that $I$ is not primary. Indeed, two reduced primary decompositions of $I$ are seen to be $I = (X, Y)^2 \cap (X) = (X^2, Y) \cap (X)$, where the first ideal is $(X, Y)$-primary (embedded) and the second $(X)$-primary (isolated). Geometrically, this scheme is a line with an embedded point.

**Counterexample 4.2.13.** As above in the coordinate ring of the quadric cone, we have $\mathfrak{p}^2 = (x^2, xz, z^2) = (x)(x, y, z) = (x) \cap (x, y, z)^2$. The first component is $\mathfrak{p}$-primary, and the second, embedded, component is $(x, y, z)$-primary. [TBD: Explain why counterexamples.]

Nonetheless, we do have a sort of uniqueness statement.

**Theorem 4.2.14** (Uniqueness of Primary Decomposition-I)**.** Let $R$ be a Noetherian ring and $M$ a f.g. $R$-module. Let $N \subsetneq M$ be a submodule. If $N = N_1 \cap \cdots \cap N_r$ is a reduced primary decomposition with $\mathfrak{p}_i = \sqrt{\operatorname{Ann}(M/N_i)}$, then $\operatorname{Ass}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. In particular, the primes are uniquely determined by $N$.

*Proof.* As before, replacing $M$ by $M/N$ we may reduce to $N = 0$. First suppose that $\mathfrak{p} = \operatorname{Ass} M$ so there is a $0 \neq x \in M$ such that $\mathfrak{p} = \operatorname{Ann}(x)$. By reordering if needed, we may assume that $x \notin N_1, \ldots, N_j$ but $x \in N_{j+1} \cap \cdots \cap N_r$; by hypothesis, $j \geq 1$, since $x \neq 0$. By the Noetherian hypothesis, there is a $k \gg 1$ such that $\mathfrak{p}_i^k M \subseteq N_i$ for each $i$, and so $(\bigcap_{i=1}^{j} \mathfrak{p}_i^k)x = 0$, i.e. $\bigcap_{i=1}^{j} \mathfrak{p}_i^k \subseteq \operatorname{Ann} x = \mathfrak{p}$. By Prime Avoidance, there is an $1 \leq i \leq j$ such that $\mathfrak{p}_i \subseteq \mathfrak{p}$; in fact, equality must hold. Indeed, if $a \in \mathfrak{p}$, then $ax = 0$ and $x \notin N_i$ implies by the primary hypothesis that $a \in \mathfrak{p}_i$. This shows that $\operatorname{Ass} M \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. To show the other direction, we'll show $\mathfrak{p}_1 \in \operatorname{Ass} M$. Since the decomposition is reduced, there is a nonzero $x \in \bigcap_{i=2}^{r} N_i \smallsetminus N_1$. Pick a minimal $k \geq 1$ such that $\mathfrak{p}_1^k x \subseteq N_1$ and $y \in \mathfrak{p}_1^{k-1} x \smallsetminus N_1$. We claim that $\mathfrak{p}_1 = \operatorname{Ann}(y)$. Indeed, $\subseteq$ is clear from $\bigcap_{i=1}^{r} N_i = 0$. Conversely, if $a \in \operatorname{Ann}(y)$, then $ay \in N_1$ but $y \notin N_1$ implies $a \in \sqrt{\operatorname{Ann}(M/N_1)} = \mathfrak{p}_1$. ∎

For another version of uniqueness, see AM Theorem 4.10, Eisenbud Theorem 3.10(c), or Dummit-Foote Theorem 21 of §15.2. Essentially, the isolated components are unique, but the embedded components aren't necessarily. [TBD].

**Corollary 4.2.15.** Let $\mathfrak{a}$ be a proper ideal in a Noetherian ring $R$.

(a) A prime $\mathfrak{p}$ contains $\mathfrak{a}$ iff $\mathfrak{p}$ contains one of the primes associated to $\mathfrak{a}$, iff $\mathfrak{p}$ contains one of the isolated primes of $\mathfrak{a}$. In other words, the isolated primes of $\mathfrak{a}$ are the minimal primes containing $\mathfrak{a}$. In particular, there are only finitely many such primes.
(b) The radical $\sqrt{\mathfrak{a}}$ is the intersection of all associated primes of $\mathfrak{a}$, and hence also of all isolated primes of $\mathfrak{a}$. In particular, $\mathfrak{a}$ is radical iff the primary components of a reduced primary decomposition of $\mathfrak{a}$ are all prime ideals. In this case, there are no embedded primes and the reduced primary decomposition is unique.
(c) There are primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ (not necessarily distinct) containing $\mathfrak{a}$ such that $\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}$.

*Proof.*

(a) One direction is clear; for the other, if $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ is a reduced primary decomposition, then $\mathfrak{a} \subseteq \mathfrak{p}$ implies by prime avoidance that $\mathfrak{q}_i \subseteq \mathfrak{p}$ for some $i$, and hence that $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$.
(b) This is clear from $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_r} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$. For the second statement, one direction is clear; for the other, we get in the above notation that $\mathfrak{a} = \sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$, which we claim is a reduced primary decomposition. Indeed, we claim that there are no embedded primes, since the integer $r$ is uniquely determined as $|\operatorname{Ass}(R/\mathfrak{a})|$ by the previous theorem, from which $\mathfrak{a}$ does not admit a primary decomposition with fewer that $r$ primes. From this, reducedness follows from prime avoidance and the primes being isolated (i.e. minimal). Finally, reducedness shows that for each $i$ there is an $x_i \in \bigcap_{j \neq i} \mathfrak{p}_j \smallsetminus \mathfrak{p}_i$ from which if $y \in \mathfrak{p}_i$ then $x_i y \in \mathfrak{q}_i$ and hence $y \in \mathfrak{q}_i$ from $x_i \notin \mathfrak{p}_i$ and the primariness of $\mathfrak{q}_i$. This shows that $\mathfrak{q}_i = \mathfrak{p}_i$ for each $i$, showing the uniquness of the reduced primary decomposition.
(c) By the Noetherian hypothesis, there is a $k \geq 1$ such that $\sqrt{\mathfrak{a}}^k \subseteq \mathfrak{a}$; this along with (b) finishes the proof.

∎

# 5 Valuation Rings and Dedekind Domains

## 5.1 Valuation Rings and Discrete Valuation Rings

**Definition 5.1.1.**

(a) An abelian group $\Gamma$ with a total order $\geq$ is an *ordered abelian group* if $\xi \geq \eta \Rightarrow \xi + \omega \geq \eta + \omega$ for all $\omega \in \Gamma$. We define an ordered abelian monoid $\hat{\Gamma} := \Gamma \cup \{\infty\}$ by $\infty + \xi = \infty$ and $\xi \leq \infty$ for all $\xi \in \hat{\Gamma}$.
(b) If $R$ is a domain, then a *valuation* on $R$ with values in $\Gamma$ is a map $v : R \to \hat{\Gamma}$ satisfying:
  (i) for $x \in R$ we have $v(x) = \infty \Leftrightarrow x = 0$,
  (ii) for $x, y \in R$ we have $v(xy) = v(x) + v(y)$ (so $v : R \to \hat{\Gamma}$ is a monoid homomorphism), and
  (iii) for $x, y \in R$ we have $v(x + y) \geq \inf\{v(x), v(y)\}$.

It is easy to see that if $R$ is a domain and $v : R \to \hat{\Gamma}$ is a valuation, then $v$ be can uniquely extended to a valuation on $\operatorname{Frac} R$ by $v(x/y) = v(x) - v(y)$ for $y \neq 0$. In this way, we note that for any $\Gamma$, the $\Gamma$-valued valuations on integral domains and their fraction fields are in canonical bijection. In this case, we define the *value group* of $v$ to be the subgroup $v((\operatorname{Frac} R)^*) \leq \Gamma$.

**Theorem 5.1.2** (Valuation Rings)**.** Let $R \subseteq K$ be a ring extension with $K$ a field. Then TFAE:

(a) For all $0 \neq \alpha \in K$ either $\alpha \in R$ or $\alpha^{-1} \in R$.
(b) The ideals of $R$ are totally ordered by inclusion.
(c) There is an ordered abelian group $\Gamma$ and a valuation $v : K \to \hat{\Gamma}$ such that $R = \{x \in K : v(x) \geq 0\}$.
(d) The ring $R$ is a local ring maximal with respect to dominance in $K$.

In this case:

(e) If $v$ is as in (c), then an element $x \in R$ is a unit iff $v(x) = 0$ and $R$ is local with $\mathfrak{m} = \{x \in K : v(x) > 0\}$.
(f) We have $K = \operatorname{Frac} R$.
(g) Any subring of $K$ containing $R$ also satisfies the above properties. In particular, every nonzero localization of $R$ satisfies these properties. Further, every quotient $R/\mathfrak{p}$ with $\mathfrak{p} \subset R$ also satisfies these properties (with respect to its fraction field).
(h) The ring $R$ is normal.
(i) The ring $R$ is Noetherian iff it is a PID (and in fact, in this case, $R$ is either a field or a DVR: see below).

**Definition 5.1.3.** A $R$ satisfying the equivalent conditions of Theorem 5.1.2 is called a *valuation ring* (of the valuation $v$).

*Proof.* For (a) $\Rightarrow$ (b), note that if $\mathfrak{a}, \mathfrak{b} \subseteq R$ are ideals with $\mathfrak{a} \not\subseteq \mathfrak{b}$, then there is a $0 \neq a \in \mathfrak{a} \setminus \mathfrak{b}$. For any $0 \neq b \in \mathfrak{b}$ we can't have $a/b \in R$ (because then $a \in \mathfrak{b}$), so by (a) we must have $b/a \in R$; this shows that $b \in aR \subseteq \mathfrak{a}$, proving $\mathfrak{b} \subseteq \mathfrak{a}$. For (b) $\Rightarrow$ (a), if $0 \neq \alpha \in K$ is any element then $\alpha = a/b$ for $0 \neq a, b \in R$. Then either $(b) \subseteq (a) \Rightarrow \alpha \in R$ or $(a) \subseteq (b) \Rightarrow \alpha^{-1} \in R$. For (a) $\Rightarrow$ (c), let $\Gamma := K^*/R^*$; given $\xi, \eta \in \Gamma$ represented by $x, y \in K^*$, define $\xi \geq \eta$ to mean $xy^{-1} \in R$. By (a), $\Gamma$ is a totally ordered abelian group. Extending the canonical homomorphism $v : K^* \to \Gamma$ by $v(0) = \infty$ gives us the required valuation. For the implication (c) $\Rightarrow$ (a), if $0 \neq \alpha \in K$ is any element then either $v(\alpha) \geq 0 \Rightarrow \alpha \in R$ or $v(\alpha) \leq 0 \Rightarrow v(\alpha^{-1}) = -v(\alpha) \geq 0 \Rightarrow \alpha^{-1} \in R$. Next, we show (c) $\Rightarrow$ (e). Indeed, if $x$ is a unit then there is a $y \in R$ such that $1 = xy \Rightarrow 0 = v(x) + v(y) \geq 0 \Rightarrow v(x) = v(y) = 0$; conversely, if $x \in R$ has $v(x) = 0$, then $v(x^{-1}) = -v(x) = 0$ and so $x^{-1} \in R$ as well. The second statement follows from $R \setminus R^* = \{x \in K : v(x) > 0\}$; by conditions (ii) and (iii) this is an ideal, so we are done by Theorem 1.3.3. Now we show (a) $\Leftrightarrow$ (d). For (a) $\Rightarrow$ (d), locality follows from (e). If $S$ is a local ring dominating $R$ and $0 \neq \alpha \in S$ is any element, then $\alpha \notin R \Rightarrow \alpha^{-1} \in \mathfrak{m}_R \subseteq \mathfrak{m}_S$ by (a), locality, and dominance; this last contradicts $\alpha \in S$. This shows that $S = R$. For (d) $\Rightarrow$ (a), suppose that $\alpha \notin R$ and let $S := R[\alpha]$. If $\mathfrak{m}S \subset S$ is proper, then it is contained in a maximal $\mathfrak{m}'$; then $\mathfrak{m} = \mathfrak{m}' \cap R$ implies $R$ is dominated by $S_{\mathfrak{m}'}$ and hence equals $S_{\mathfrak{m}'}$, implying $\alpha \in R$, a contradiction; therefore, we must have $\mathfrak{m}S = S$. Therefore, $1 = \sum_{i=0}^{n} c_i \alpha^i$ with $c_i \in \mathfrak{m}$ and so using $1 - c_0 \in R^*$ we see that $\alpha^{-1}$ is integral over $R$. In particular, $R[\alpha^{-1}]$ is an integral extension of $R$ and so by Theorem 2.2.1(a) there is a prime $\mathfrak{m}''$ of $R[\alpha^{-1}]$ lying over $\mathfrak{m}$. From this and the maximality of $R$ it follows that $R = R[\alpha^{-1}]_{\mathfrak{m}''} \ni \alpha^{-1}$.

For (f), any element $0 \neq \alpha \in K$ is either $\alpha/1$ or $1/\alpha^{-1}$. For (g), the first and second statements are clear; the third is clear from the fact that the "partially defined map" $K \dashrightarrow \operatorname{Frac}(R/\mathfrak{p})$ taking $x/y$ for $y \notin \mathfrak{p}$ to $[\overline{x}/\overline{y}]$ is surjective. For (h), if $0 \neq \alpha \in K$ satisfies $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$ for $a_i \in R$, then if $\alpha^{-1} \in R$, multiplying by $\alpha^{-n+1}$ shows that $\alpha \in R$. For (i), note that if $I = (a_1, \ldots, a_n)$, then using (b) by relabelling we have $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \Rightarrow I = (a_n)$.

■

The above shows that given a valuation ring $R \subseteq K$ of a field $K$, the valuation of $K$ as in (c) and the value group is determined by $R$ upto isomorphism.

**Theorem 5.1.4.** If $R \subseteq K$ is any extension with $K$ a field, then $\mathrm{Cl}_K(R) = \bigcap_{S \supseteq R} S$, where the intersection is over all valuation rings $S$ of $K$ containing $R$.

*Proof.* The inclusion $\mathrm{Cl}_K(R) \subseteq \bigcap_{S \supseteq R} S$ is clear by Theorem 5.1.2(h). Conversely, suppose $\alpha \notin \mathrm{Cl}_K(R)$. Then $\alpha \notin R[\alpha^{-1}]$, so that $\alpha^{-1} \notin R[\alpha^{-1}]^*$, so there is a maximal ideal $\mathfrak{m} \subseteq R[\alpha^{-1}]$ such that $\alpha^{-1} \in \mathfrak{m}$. Consider the map $\varphi : R[\alpha^{-1}] \twoheadrightarrow R[\alpha^{-1}]/\mathfrak{m} \hookrightarrow \overline{R[\alpha^{-1}]/\mathfrak{m}} = \Omega$. By Lemma 2.3.1(d), the $\varphi$ admits a maximal extension $\tilde{\varphi} : S \to \Omega$ to a valuation ring $S$ of $K$ containing $R[\alpha^{-1}]$. Then $\alpha^{-1} \in S$ is such that $\tilde{\varphi}(\alpha^{-1}) = 0$, so $S$ is a valuation ring of $K$ containing $R$ and not containing $\alpha$. ■

Given any ordered abelian group $\Gamma$, one can construct a field $K$ and a valuation $v$ on $K$ with value group precisely $\Gamma$ (see Atiyah-Macdonald).

**Definition 5.1.5.** A valuation $v$ of a field $K$ is said to be *discrete* if $K$ has value group $\mathbf{Z}$. In this case, an element $t \in K$ is called a *uniformizer* of $v$ if $v(t) = 1$.

**Theorem 5.1.6** (Discrete Valuation Rings)**.** Let $R$ be a ring. Then TFAE:

(a) $R$ is the valuation ring of a discrete valuation.
(b) $R$ is a Noetherian domain that is maximal[3] and not a field.
(c) $R$ is a Noetherian valuation ring that is not a field.
(d) $R$ is a local PID that is not a field.
(e) $R$ is a UFD with a unique irreducible upto associates.
(f) $R$ is a Noetherian local domain that is not a field and
  (1) the maximal ideal $\mathfrak{m}$ is principal, or
  (2) the dimension $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, or
  (3) every nonzero ideal in $R$ is of the form $\mathfrak{m}^n$ for some (unique) integer $n \geq 0$, or
  (4) $R$ is normal with $\dim R = 1$, or
  (5) $\dim R = 1$ and the only $\mathfrak{m}$-primary ideals of $R$ are the powers of $\mathfrak{m}$.
(g) $R$ is a local domain that is not a field, and every nonzero fractional ideal of $R$ is invertible.

In this case:

(h) If $t \in R$ is any uniformizer, then $\mathrm{Frac}\, R = R[t^{-1}]$.
(i) An element $t \in R$ is a uniformizer iff $\mathfrak{m} = (t)$ iff $t \in \mathfrak{m} \setminus \mathfrak{m}^2$.
(j) The only prime ideals of $R$ are (0) and $\mathfrak{m}$.
(k) Is $S \subseteq \mathrm{Frac}\, R$ is another DVR containing $R$, then $R = S$.

*Proof.* First we show (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (e) $\Rightarrow$ (a). For (a) $\Rightarrow$ (b), let $v$ be the discrete valuation. If $0 \neq \mathfrak{a} \subseteq R$ is any ideal and $a \in \mathfrak{a}$ of minimal $v(a)$, then $\mathfrak{a} = (a)$ so $R$ is a PID and hence Noetherian. Next, if $S \supseteq R$ is any ring, then look at $v(S) := \{v(s) : s \in S\}$. Since $R$ contains a uniformizer, this looks like $[n, \infty)$ for some $n = \inf v(S) \in \mathbf{Z}_{\leq 0} \cup \{-\infty\}$. If $n = 0$, then $S \subseteq R$ and so $S = R$. If $n \leq -1$, then since $S$ is a ring we must have $n = -\infty$. Then if $0 \neq \alpha \in \mathrm{Frac}\, R$ is any element, then there is an $s \in S$ such that $\alpha s^{-1} \in R \Rightarrow \alpha \in S$, and so $S = \mathrm{Frac}\, R$. This proves maximality. From $0 \to R^* \to K^* \to v(K^*) \cong \mathbf{Z} \to 0$, we have that $R$ is not a field. For (b) $\Rightarrow$ (c), it suffices to show by Theorem 5.1.2(d) that $R$ is local, so suppose contrarily that $R$ has two distinct maximal ideals $\mathfrak{m}$ and $\mathfrak{m}'$. Let $\alpha \in \mathfrak{m} \setminus \mathfrak{m}'$. Then we claim that $R \subsetneq R[\alpha^{-1}] \subsetneq \mathrm{Frac}\, R$, contradicting (b). Indeed, the first strict containment follows from $\alpha \in \mathfrak{m}$, and the second frollows from the fact that if $x \in \mathfrak{m}' \setminus \{0\}$, then $x^{-1} \notin R[\alpha^{-1}]$ as is easy to check. The implication (c) $\Rightarrow$ (d) is clear by Theorem 5.1.2(e) and (i). For (d) $\Rightarrow$ (e), note that a PID is a UFD. If $\mathfrak{m} = (t)$ for some $t \in R$, then $0 \neq t$ is irreducible. If $a \in R \setminus R^*$, then $a \in \mathfrak{m} = (t)$, so $t \mid a$; in particular, $t$ is the unique irreducible up to associates. For (e) $\Rightarrow$ (a), fix a $t$ irreducible. Then every $0 \neq x \in R$ can be written as $x = ut^n$ for some unique unit $u \in R^*$ and integer $n \geq 0$. Then the map $v : R \setminus \{0\} \to \mathbf{Z}$ by $ut^n \mapsto n$ (or rather its extension to $(\mathrm{Frac}\, R)^*$) is discrete with valuation ring $R$.

Next, we show that (a)-(e) imply (h)-(k). Indeed, (h) is clear. To show (i), if $v(t) = 1$, then $t$ is first a nonunit, then an irreducible, and hence the unique generator of $\mathfrak{m}$; conversely, if $\mathfrak{m} = (t)$ and $t'$ is a uniformizer, then $(t) = (t')$ so $t' = ut$ for some $u \in R^*$ and hence $v(t) = 1$. The last equivalence is clear because $v(\mathfrak{m}^n \setminus \mathfrak{m}^{n+1}) = n$

[3]This means that there are no rings properly contained between it and its field of fractions.

for any $n \geq 0$. To show (j), we have in fact shown in (e) that every ideal of $R$ is a power of $\mathfrak{m}$. Finally, (k) is clear from (b).

Next we clarify the parentheses around the word "unique" in (f)(3): in the situation of (f), if every nonzero ideal if the form the $\mathfrak{m}^n$ for some $n \geq 0$, then this $n$ is unique. Indeed, if $\mathfrak{m}^n = \mathfrak{m}^{n+k}$ for some $n \geq 0, k \geq 1$, then $\mathfrak{m}^n = \mathfrak{m}^{n+1} = \cdots = \mathfrak{m}^{n+k}$, so by Nakayama's Lemma we conclude that $\mathfrak{m}^n = 0$, so either $R = 0 \Rightarrow \mathfrak{m} = 0$ (if $n = 0$) or $\mathfrak{m} = \sqrt{\mathfrak{m}^n} = 0$ (if $n \geq 1$), in any case a contradiction to hypothesis.

Next, we show that (a)-(e) are equivalent to (f) and (g). It is clear that (d) $\Rightarrow$ (f)(1). The equivalence of (f)(1) and (f)(2) was Corollary 1.6.4(e). Next, we show that (f)(1)-(2) $\Rightarrow$ (f)(3). If $0 \subsetneq \mathfrak{a} \subsetneq R$ is an ideal, then there is an $n \geq 1$ such that $\mathfrak{a} \subseteq \mathfrak{m}^n$ but $\mathfrak{a} \nsubseteq \mathfrak{m}^{n+1}$ holds[4]; if we pick an $a \in \mathfrak{a} \setminus \mathfrak{m}^{n+1}$, then $a = ut^n$ for some $u \notin \mathfrak{m} \Rightarrow u \in R^*$. Therefore, $\mathfrak{m}^n = (t^n) = (a) \subseteq \mathfrak{a} \subseteq \mathfrak{m}^n$. Next, we show (f)(3) $\Rightarrow$ (f)(1); indeed, pick a $t \in \mathfrak{m} \setminus \mathfrak{m}^2$; then there is a unique $n \geq 0$ such that $(t) = \mathfrak{m}^n$ and then $n$ must be 1. Next, (f)(1)-(3) clearly imply (d); this shows the equivalence of (a)-(f)(3).

Next, suppose (a)-(f)(3). Then $R$ is normal by Theorem 5.1.2(i). From (j), we conclude that $\dim R = 1$; this proves (f)(4). Next, we show (f)(4) $\Rightarrow$ (f)(1). For that, suppose we have an element $0 \neq a \in \mathfrak{m}$. Then $\sqrt{(a)} = \bigcap_{\mathfrak{p} \supset (a)} = \mathfrak{m}$ by (j). Since $R$ is Noetherian, for some $n \gg 0$ we have $\mathfrak{m}^n \subseteq (a) \subseteq \mathfrak{m}$. Either $n = 1$ works, and we are done; or there is some $n \geq 2$ with $\mathfrak{m}^n \subseteq (a)$ but $\mathfrak{m}^{n-1} \nsubseteq (a)$. Let $b \in \mathfrak{m}^{n-1} \setminus (a)$, and let $t := a/b \in \operatorname{Frac} R$. Then $t^{-1}\mathfrak{m} \subseteq R$. If $t^{-1}\mathfrak{m} \subseteq \mathfrak{m}$, then $\mathfrak{m}$ is a faithful $R[t^{-1}]$ module that is a finitely generated $R$-module, so by Theorem 2.1.3(d), $t^{-1} \in \operatorname{Cl}_{\operatorname{Frac} R}(R) = R$, a contradiction to $b \notin (a)$. Therefore, $t^{-1}\mathfrak{m} = R$ and $\mathfrak{m} = (t)$. The implication (f)(3)-(4) $\Rightarrow$ (f)(5) is clear. To show (f)(5) $\Rightarrow$ (f)(3), suppose that (f)(5) holds. Since $R$ is a local domain and $\dim R = 1$, (j) follows. If $0 \subset \mathfrak{a} \subset R$ is any ideal, then since $R$ is Noetherian, $\mathfrak{a}$ admits a minimal primary decomposition; all the resulting primary ideals are $\mathfrak{m}$-primary by (j), and so by (f)(5) we have that $\mathfrak{a} = \mathfrak{m}^n$ for some $n \geq 1$, showing (f)(3). This finishes the proof of the equivalence of (a)-(f).

The implication (d) $\Rightarrow$ (g) is clear, since in a PID every nonzero fractional ideal is invertible. To finish the proof, we show that (g) $\Rightarrow$ (f)(3). Since every nonzero integral ideal is invertible, it is finitely generated by Theorem 5.2.3, so that $R$ is Noetherian. Let $\Sigma$ be the set of nonzero ideals that are not powers of $\mathfrak{m}$; using the fact that $R$ is Noetherian, it is easy to see that if nonempty, $\Sigma$ satisfies the hypotheses of Zorn's Lemma. Let $\mathfrak{a} \in \Sigma$ be a maximal element. Then $\mathfrak{a} \neq \mathfrak{m}, R$ so that $\mathfrak{a} \subset \mathfrak{m}$. Therefore, $\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{m} = R$ is a proper integral ideal containing $\mathfrak{a}$. If $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a}$, then $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$, so $\mathfrak{a} = 0$ by Nakayama's Lemma, a contradiction; hence $\mathfrak{m}^{-1}\mathfrak{a} \supsetneq \mathfrak{a}$. Since $\mathfrak{a}$ is not a power of $\mathfrak{m}$, neither can $\mathfrak{m}^{-1}\mathfrak{a}$ be, and so $\mathfrak{m}^{-1}\mathfrak{a} \in \Sigma$, contradicting the maximality of $\mathfrak{a}$.

■

**Example 5.1.7.** It follows that if $R$ is a Noetherian normal domain and $\mathfrak{p}$ a minimal nonzero prime of $R$, then $R_{\mathfrak{p}}$ is a Noetherian normal (Lemma 2.1.8) local domain of $\dim R_{\mathfrak{p}} = \operatorname{ht} \mathfrak{p} = 1$ (and so not a field), and hence a DVR.

## 5.2 Invertibility of Fractional Ideals

**Definition 5.2.1.** Let $R$ be a domain with $K := \operatorname{Frac} R$.

(a) A *fractional ideal* $\mathfrak{f}$ of $R$ is an $R$-submodule of $K$ such that $x\mathfrak{f} \subseteq R$ for some $x \in K^*$.

A fractional ideal contained in $R$ (i.e. a plain old ideal) is called an *integral* ideal; clearly $R = K$ iff every fractional ideal is integral. Equivalently, a fractional ideal of $R$ is an $R$-submodule of $K$ the form $x\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq R$ and $x \in K^*$; in fact, we can arrange that $x = r^{-1}$ for some $r \in R$. Clearly, the sum and product of fractional ideals is a fractional ideal. The finitely generated $R$-submodules of $K$ are fractional ideals, and conversely iff $R$ is Noetherian.

(b) If $\mathfrak{f}, \mathfrak{g}$ are fractional ideals of $R$, we define the *colon ideal* $(\mathfrak{g} : \mathfrak{f})$ to be $(\mathfrak{g} : \mathfrak{f}) := \{x \in K : x\mathfrak{f} \subseteq \mathfrak{g}\}$. In particular, we define the inverse $\mathfrak{f}^{-1} := (R : \mathfrak{f})$. When $\mathfrak{f} \neq 0$, the colon $(\mathfrak{g} : \mathfrak{f})$ is a fractional ideal as well: if $y \in \mathfrak{f} \setminus \{0\}$ and $z \in K^*$ such that $y\mathfrak{g} \subseteq R$, then $xy(\mathfrak{g} : \mathfrak{f}) \subseteq R$.

We start with a lemma.

**Lemma 5.2.2.** If $\mathfrak{f}$ is a nonzero fractional ideal of a domain $R$ and $\lambda : \mathfrak{f} \to R$ is any $R$-linear map, then there is a unique $b \in K$ such that $\lambda(x) = bx$ for all $x \in \mathfrak{f}$.

[4]This uses that $\bigcap_{n \geq 1} \mathfrak{m}^n = 0$, which is Corollary **??**; this can also be deduced from (f)(1): if $\mathfrak{m} = (t)$ and $0 \neq a \in \bigcap_n \mathfrak{m}^n$, then for each $n \geq 0$ there is an $a_n$ such that $a = a_n t^n$. Then $a_n = a_{n+1}t$ for each $n \geq 0$, and so $(a_0) \subseteq (a_1) \subseteq \cdots$ stabilizes by the Noetherian condition to give us $t \in R^*$, a contradiction.

*Proof.* First note that if $x = q/r \in \mathfrak{f}$ with $q, r \in R$, then $q = rx \in \mathfrak{f}$ as well and so $\lambda(q) = r\lambda(x) \Rightarrow \lambda(q/r) = \lambda(q)/r$. Now fix any nonzero $q_0 \in \mathfrak{f} \cap R$. Then for any $x = q/r$ we have

$$q_0\lambda(x) = q_0\lambda\left(\frac{q}{r}\right) = \lambda\left(\frac{qq_0}{r}\right) = q\lambda\left(\frac{q_0}{r}\right) = \frac{q}{r}\lambda(q_0) = x\lambda(q_0)$$

so $b = \lambda(q_0)/q_0$ works. ∎

**Theorem 5.2.3** (Invertible Ideals)**.** Let $R$ be a domain and $\mathfrak{f}$ be a nonzero fractional ideal. Then TFAE:

(a) We have $\mathfrak{f}\mathfrak{f}^{-1} = R$.
(b) There is some fractional ideal $\mathfrak{g}$ such that $\mathfrak{f}\mathfrak{g} = R$.
(c) The ideal $\mathfrak{f}$ is a projective $R$-module.
(d) The ideal $\mathfrak{f}$ is finitely generated and for all $\mathfrak{p}$, the fractional ideal $\mathfrak{f}_\mathfrak{p} := \mathfrak{f}R_\mathfrak{p}$ of $R_\mathfrak{p}$ is principal.
(e) The ideal $\mathfrak{f}$ is finitely generated and for all $\mathfrak{m}$, the fractional ideal $\mathfrak{f}_\mathfrak{m} = \mathfrak{f}R_\mathfrak{m}$ of $R_\mathfrak{m}$ is principal.

*Proof.* The implication (a) ⇒ (b) is trivial. For (b) ⇒ (a), first $\mathfrak{g} = R$ clearly implies $\mathfrak{g} \subseteq \mathfrak{f}^{-1}$. If $1 = \sum_{i=1}^n a_i b_i$ with $a_i \in \mathfrak{f}, b_i \in \mathfrak{g}$, then for any $x \in \mathfrak{f}^{-1}$ we have $x = \sum_{i=1}^n (xa_i)b_i \in \mathfrak{g}$, and so $\mathfrak{f}^{-1} \subseteq \mathfrak{g}$ as well. Next, if $\mathfrak{f}$ satisfies (a)-(b), then $\mathfrak{f}$ is f.g.; indeed, if $a_i \in \mathfrak{f}$ and $b_i \in \mathfrak{f}^{-1}$ are as above, then $\mathfrak{f}$ is generated by the $a_i$. To show (a) ⇒ (c), define a surjection $\varphi : R^n \twoheadrightarrow \mathfrak{f}$ by $\mathrm{e}_i \mapsto a_i$ and $\psi : \mathfrak{f} \to R^n$ by $x \mapsto \sum_{i=1}^n (b_i x)\mathrm{e}_i$. Then $\varphi \circ \psi = 1_\mathfrak{f}$, so $\psi$ splits $\mathfrak{f}$ off as a direct summand of $R^n$. To show (c) ⇒ (a), note that if we have a surjection $\varphi : R^I \to \mathfrak{f}$ for some free module $R^I$ with a splitting $\psi : \mathfrak{f} \to R^I$, then $\psi(x) = \sum_{i\in I} \lambda_i(x)\mathrm{e}_i$ gives us $R$-module homomorphisms $\lambda_i : \mathfrak{f} \to R$ which determine elements $b_i \in K$ by the previous lemma. Since for a fixed $0 \neq x$, all but finitely many $\lambda_i(x) = 0$, all but finitely many $b_i = 0$; let $b_1, \ldots, b_n$ be the nonzero ones. Then $\sum_{i=1}^n a_i b_i x = x$ for every $x \in \mathfrak{f}$, where $a_i = \varphi(\mathrm{e}_i)$, so that $\sum_{i=1}^n a_i b_i = 1$; since $b_i\mathfrak{f} = \lambda_i(\mathfrak{f}) \subseteq R$, we have $b_i \in \mathfrak{f}^{-1}$ and hence that $\mathfrak{f}\mathfrak{f}^{-1} = R$.

For (a) ⇒ (d), only the second part remains to be shown: if $\sum_{i=1}^n a_i b_i = 1$ as before and $\mathfrak{p}$ is a prime, then for some $j$ we must have $a_j b_j \in R_\mathfrak{p}^*$. Then $a_j R_\mathfrak{p} \subseteq \mathfrak{f}_p$; for the converse, for $x \in \mathfrak{f}_p$ we have $x = \sum_{i=1}^n a_i b_i x = a_j \sum_{i=1}^n (a_j b_j)^{-1} a_i b_i b_j x \subseteq a_j R_\mathfrak{p}$ because $a_i b_i \in R$ and $b_j x \in \mathfrak{f}^{-1}\mathfrak{f}R_\mathfrak{p} = R_\mathfrak{p}$. The implication (d) ⇒ (e) is trivial. Finally, for (e) ⇒ (a), we clearly have $(\mathfrak{f}^{-1})_\mathfrak{m} \subseteq \mathfrak{f}_\mathfrak{m}^{-1}$ and if $\mathfrak{f}$ is finitely generated, there is equality: if $\mathfrak{f}$ is generated by $a_i$ and $y \in \mathfrak{f}_\mathfrak{m}^{-1}$, then $ya_i \in R_\mathfrak{m}$, so there is an $s_i \in R \setminus \mathfrak{m}$ such that $ya_i s_i \in R$; therefore, if $s = \prod_i s_i$, then $(sy)a_i \in R$ for all $i$, and hence $sy \in \mathfrak{f}^{-1} \Rightarrow y \in (\mathfrak{f}^{-1})_\mathfrak{m}$. Since $\mathfrak{f}_\mathfrak{m}$ is principal, we have $\mathfrak{f}_\mathfrak{m}\mathfrak{f}_\mathfrak{m}^{-1} = R_\mathfrak{m}$. If $\mathfrak{f}\mathfrak{f}^{-1} \neq R$, then there is a maximal $\mathfrak{m}$ such that $\mathfrak{f}\mathfrak{f}^{-1} \subseteq \mathfrak{m}$; then $R_\mathfrak{m} = \mathfrak{f}_\mathfrak{m}\mathfrak{f}_\mathfrak{m}^{-1} = \mathfrak{f}_\mathfrak{m}(\mathfrak{f}^{-1})_\mathfrak{m} = (\mathfrak{f}\mathfrak{f}^{-1})_\mathfrak{m} \subseteq \mathfrak{m}R_\mathfrak{m}$, a contradiction. ∎

**Definition 5.2.4.** Let $R$ be a domain.

(a) A nonzero fractional ideal $\mathfrak{f}$ of $R$ satisfying the equivalent conditions of Theorem 5.2.3 is said to be *invertible* with inverse $\mathfrak{f}^{-1}$.

Clearly, fractional ideal inverses are unique if they exist, and the set of invertible fractional ideals of $R$ forms an abelian group with identity $R$.

(b) The group of invertible fractional ideals of $R$ is called the *ideal group* of $R$ and denoted $\mathrm{Ideal}(R)$.

The group $\mathrm{Ideal}(R)$ contains the set of nonzero principal fractional ideals as a subgroup.

(c) We define the *ideal class group* or *Picard group* of $R$, denoted by $\mathrm{Pic}(R)$, to be the group of invertible fractional ideals modulo the subgroup of nonzero principal fractional ideals.

In other words, $\mathrm{Pic}(R)$ is defined by the exact sequence $0 \to R^* \to K^* \to \mathrm{Ideal}(R) \to \mathrm{Pic}(R) \to 0$.

(d) The cardinality $h(R) := |\mathrm{Pic}(R)|$ is called the *ideal class number* of $R$.

**Example 5.2.5.** Let $R$ be a UFD; we show that $h(R) = 1$. Indeed, let $\mathfrak{f}$ be an invertible fractional ideal; then as noted above, $\mathfrak{f}$ is finitely generated say $\mathfrak{f} = R(x_i/y_i)_{i=1}^n$ for $x_i, y_i \in R$ with $\gcd(x_i, y_i) = 1$. If $z := \mathrm{lcm}(y_i)/\gcd(x_i)$, then clearly $z \in \mathfrak{f}^{-1}$; conversely, any $\theta = x/y \in \mathfrak{f}^{-1}$ with $\gcd(x, y) = 1$ can be shown to satisfy $\mathrm{lcm}(y_i) \mid x$ and $y \mid \gcd(x_i)$, so $\mathfrak{f}^{-1} = (z)$.

**Corollary 5.2.6.** Let $R$ be a domain.

(a) If $R$ is Noetherian and $\mathfrak{p} \subset R$ an invertible prime, then $\mathfrak{p}$ is minimal ($\mathrm{ht}\,\mathfrak{p} = 1$) and $R_\mathfrak{p}$ is a DVR.
(b) If $R$ is not Noetherian, then $R$ has an ideal that is not projective as an $R$-module.

*Proof.* For (a), if $\mathfrak{p}$ is invertible, it is nonzero by definition; by the above, the maximal ideal $\mathfrak{p}R_\mathfrak{p}$ of $R_\mathfrak{p}$ is principal, we are done by Theorem 5.1.6(f)(1). For (b), simply pick an ideal that is not finitely generated. ∎

**Example 5.2.7.** In the domain $R = \mathbf{Z}[X_i]_{i\geq 1}$, the ideal $(X_i)_{i\geq 1}$ is not finitely generated and hence a non-projective $R$-module.

## 5.3 Dedekind Domains

**Theorem 5.3.1** (Dedekind Domains)**.** Let $R$ be a domain. Then TFAE:

(a) The ring $R$ is Noetherian, and
  (1) is normal of dimension at most 1, or
  (2) for every nonzero $\mathfrak{p}$, the ring $R_\mathfrak{p}$ is a DVR, or
  (3) every primary ideal of $R$ is a prime power and $R$ has dimension at most 1.
(b) Every nonzero fractional ideal of $R$ is invertible.
(c) Every nonzero ideal of $R$ can be written as a product of prime ideals.

In this case:

(d) The factorization in (c) is unique.
(e) The group $\mathrm{Ideal}(R)$ is the free abelian group on the set of prime ideals of $R$.
(f) If $\mathfrak{f}, \mathfrak{g}, \mathfrak{h}$ are fractional ideals and $\mathfrak{fg} = \mathfrak{fh}$, then either $\mathfrak{f} = 0$ or $\mathfrak{g} = \mathfrak{h}$.
(g) The ring $R$ is a PID iff it is a UFD iff it has $h(R) = 1$.
(h) If $0 \neq \mathfrak{a}, \mathfrak{b} \subset R$ are ideals with prime factorization $\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i}$ and $\mathfrak{b} = \prod_i \mathfrak{p}_i^{f_i}$, then
  (1) ("Containment is division.") we have $\mathfrak{a} \supseteq \mathfrak{b}$ iff $\mathfrak{a} \mid \mathfrak{b}$ iff $e_i \leq f_i$ for all $i$,
  (2) we have $\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b}) = \prod_i \mathfrak{p}_i^{\min\{e_i, f_i\}}$ (so in particular $\mathfrak{a} + \mathfrak{b} = 1$ iff $e_i f_i = 0$ for all $i$), and
  (3) we have $\mathfrak{a} \cap \mathfrak{b} = \mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod_i \mathfrak{p}_i^{\max\{e_i, f_i\}}$.
(i) (Weak Approximation) If $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct primes and $e_i \geq 0$, then $R/\prod_i \mathfrak{p}_i^{e_i} \xrightarrow{\sim} \prod_i (R/\mathfrak{p}_i^{e_i})$; equivalently, for any $r_1, \ldots, r_n \in R$, there is an $r \in R$ unique up to an element of $\prod_i \mathfrak{p}_i^{e_i}$ such that $r \equiv r_i \pmod{\mathfrak{p}_i^{e_i}}$ for all $i$.
(j) If $\mathfrak{a} \subseteq R$ is any ideal, then
  (1) there is an ideal $\mathfrak{b}$ of $R$ with $\mathfrak{a} + \mathfrak{b} = 1$ such that $\mathfrak{ab}$ is principal,
  (2) if $0 \neq \mathfrak{a}$, then every ideal in $R/\mathfrak{a}$ is principal,
  (3) (generation by two elements) if $0 \neq \alpha \in \mathfrak{a}$, then there is a $\beta \in R$ such that $\mathfrak{a} = (\alpha, \beta)$.
  (4) If $\mathfrak{b}$ is an ideal such that $0 \subset \mathfrak{a} \subseteq \mathfrak{b} \subset R$, then there is a $\gamma \in \mathrm{Frac}\, R$ such that $\gamma\mathfrak{a} \subseteq R$ but $\gamma\mathfrak{a} \not\subseteq \mathfrak{b}$.

**Definition 5.3.2.** A domain $R$ satisfying the equivalent conditions of Theorem 5.3 is called a *Dedekind domain*.

*Proof.* First, for (a)(1) $\Rightarrow$ (a)(2), note that either $R$ is a field (and so has no nonzero primes) or each $R_\mathfrak{p}$ is a Noetherian (Observation 1.2.7(d)) normal (Lemma 2.1.8(c)) local domain of dimension 1 (since $\dim R_\mathfrak{p} = \mathrm{ht}\, \mathfrak{p} = 1$) that is not a field (since $\mathfrak{p}R_\mathfrak{p} \neq 0R_\mathfrak{p}$) and hence a DVR (Theorem 5.1.6(f)(4)). Conversely, for (a)(2) $\Rightarrow$ (a)(1), note that $\dim R = \sup_\mathfrak{p} \mathrm{ht}\, \mathfrak{p} = \sup_\mathfrak{p} \dim R_\mathfrak{p} \leq 1$. Then $R$ is normal by Lemma 2.1.8(d). For (a)(2) $\Rightarrow$ (b), we are done by Theorem 5.2.3(c). For (b) $\Rightarrow$ (a)(2), note first that if every nonzero ideal of $R$ is invertible, then $R$ is Noetherian by Theorem 5.2.3 and so the result follows from Corollary ∎

**Corollary 5.3.3.** A localization of a Dedekind domain is Dedekind.

*Proof.* The properties Noetherian, normal and of dimension at most 1 all descend via localization. ∎

## 5.4 Extensions of Dedekind Domains

**Theorem 5.4.1.** Let $R$ be a domain with fraction field $K$. Let $L/K$ be a finite extension. If either

(a) $R$ is Noetherian and normal and $L/K$ is separable, or
(b) $R$ is a finitely generated algebra over a field,

then the integral closure $S := \mathrm{Cl}_L(R)$ of $R$ in $L$ is a finitely generated $R$-module.

*Proof 1 of (a).* For (a), by algebraicity of $L/K$ it is easy to see that every $K$-basis of $L$ can be rescaled by elements of $R$ to lie in $S$; let $v_1, \ldots, v_n \in S$ be one such basis. Since $L/K$ is separable, the trace pairing $(x, y) \mapsto \mathrm{Tr}_K^L(xy)$ is nondegenerate (by Theorems 3.5.4 and 3.5.5). Using this pairing we find the dual basis $v_1^*, \ldots, v_n^* \in L$ with $\mathrm{Tr}_K^L(v_i^* v_j) = \delta_{ij}$. Write an $x \in S$ as $x = \sum_i x_i v_i^*$, then $xv_i \in S$ implies that $\mathrm{Tr}_K^L(xv_i) \in R$ by Lemma 2.1.9(c) by taking $\mathfrak{a} = (1)$. But now $\mathrm{Tr}_K^L(xv_i) = x_i$, so this shows that $S \subseteq \sum_j R v_j^*$; we finish by the Noetherian hypothesis. ∎

*Proof 2 of (a).* Replacing $L$ by its Galois clsoure, we may assume that $L/K$ is finite Galois with Galois group $G := \mathrm{Gal}(L/K)$. As before, let $v_1, \dots, v_n \in S$ be one such basis; and let $D$ be the discriminant of this basis, where $0 \neq D$ by separability. Again by Lemma 2.1.9(c) we have $D \in R$. If $x \in S$ is $x = \sum_j x_j v_j$ for some $x_j \in K$, then we'll show that $Dx_j \in R$ for each $j$. Indeed, by applying $\sigma_i \in G$ we get $\sigma_i x = \sum_j x_j \sigma_i v_j$. By Cramer's rule, we can write $x_j = y_j / \det|\sigma_i v_j|$ for some $y_j \in S$; clearly also $\det|\sigma_i v_j| \in S$. Then $Dx_j = y_j \det|\sigma_i v_j| \in \mathrm{Cl}_K(R) = R$. [In fact, this shows that we have $Dx_j^2 \in R$.] ∎

*Proof of (b).* By Noether normalization (Theorem 6.1.1), $R$ is integral over some polynomial $k[z_1, \dots, z_r]$, so by transitivity of integrality and algebraicity of $K$ over $k(z_1, \dots, z_r)$ we may assume WLOG that $R = k[z_1, \dots, z_r]$ is polynomial and so $K = k(z_1, \dots, z_r)$. Since $R$ is Noetherian, we can replace $L$ by its normal closure to assume that $L/K$ is normal. Let $F := L^{\mathrm{Aut}(L/K)}$, so that $L/F$ is Galois and $F/K$ is purely inseparable. If we show that $T := \mathrm{Cl}_F(R)$ is a finitely generated $R$-module, then it is Noetherian and is normal since $F = \mathrm{Frac}\, T$, so by (a) we would have that $S = \mathrm{Cl}_L(T)$ would be a finitely generated $T$-module, so we would be done by transitivity of module-finiteness. Therefore, we can suppose by replacing $L$ by $F$ that $L/K$ is purely inseparable. If $L = K$, this is trivial; else assume let $p := \mathrm{char}\, k > 0$. Then for some power $q$ of $p$, the field $L$ is generated by $q^{\text{th}}$ roots of finitely many rational functions. Extending $L$ further by adjoining $q^{\text{th}}$ roots of their coefficients, we may assume that $L = k'(z_1^{1/q}, \dots, z_r^{1/q})$ where $k'$ is obtained from $k$ by adjoining the $q^{\text{th}}$ roots of the coefficients. Then $S = \mathrm{Cl}_L(R) = k'[z_1^{1/q}, \dots, z_r^{1/q}]$ since this is ring is normal, has quotient field $L$, and is module-finite over $R$. ∎

**Theorem 5.4.2** (Ramification Formula)**.** Let $R$ be a Dedekind domain with fraction field $K$. Let $L/K$ be a finite extension and $S := \mathrm{Cl}_L(R)$ such that $S$ is a f.g. $R$-module (e.g. in the hypotheses of Theorem 5.4.1). Then:

(a) The ring $S$ is also a Dedekind domain.
(b) If $n := [L : K]$ and $\mathfrak{p} \subset R$ is a prime and $\mathfrak{p}S = \prod_i \mathfrak{P}_i^{e_i}$, and $f_i := [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})]$, then $\sum_{i=1}^n e_i f_i = n$.
(c) If $L/K$ is Galois and for each $i$ the extensions $\kappa(\mathfrak{P}_i)/\kappa(\mathfrak{p})$ are separable, then all the $e_i = |I_{\mathfrak{P}_i}|$ are all equal. Further, all the $f_i$ are equal too, so if there are $r$ distinct primes, then this formula reduces to $efr = n$.

*Proof.* For (a), ring $S$ is Noetherian since it is a f.g. $R$-module with $R$ Noetherian; it is normal because of idempotence and $L = \mathrm{Frac}\, S$; it is of dimension 1 by Corollary 2.2.4(a), so $S$ is Dedekind by Theorem 5.3(a)(1). For (b), By Weak Approximation (Theorem 5.3(i)) we have $S/\mathfrak{p}S \cong \prod_i S/\mathfrak{P}_i^{e_i}$. Since each $\mathfrak{P}_i S_{\mathfrak{P}_i}$ is principal, say $(q_i)$, by Theorem 5.3(a)(3), we get isomorphisms $q_i^j : S/\mathfrak{P}_i \xrightarrow{\sim} \mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ for each $j \geq 0$; this shows that $\sum_{i=1}^n e_i f_i = \dim_{\kappa(\mathfrak{p})}(S/\mathfrak{p}S)$. On the other hand, let $x_1, \dots, x_r \in S$ reduce to a $\kappa(\mathfrak{p})$-basis of $S/\mathfrak{p}S$. Then the $x_i$ also reduce to spanning set of $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ over $\kappa(\mathfrak{p})$, and so by Lemma 1.6.3(b) the elements $x_i$ generate $S_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$ and hence certainly span $L$ over $K$. If they are linearly dependent, say $\sum_j a_j x_j = 0$ with $a_j \in K$ not all zero, then multiplying by a suitable power of the generator of $\mathfrak{p}R_{\mathfrak{p}}$ we can assume that the $a_i$ are all in $R_{\mathfrak{p}}$ but not all in $\mathfrak{p}R_{\mathfrak{p}}$. Reducing mod $\mathfrak{p}R_{\mathfrak{p}}$, we get a nontrivial dependence relation over $\kappa(\mathfrak{p})$, which is not possible. This shows that $x_1, \dots, x_r$ form a basis of $L/K$ and hence $n := [L : K] = r := \dim_{\kappa(\mathfrak{p})}(S/\mathfrak{p}S)$. ∎

In fact, more generally we have:

**Theorem 5.4.3.** Let $R$ be a Noetherian one-dimensional domain with fraction field $K$. Let $L/K$ be a finite extension and let $S := \mathrm{Cl}_L(R)$. Then $S$ is a Dedekind domain.

In this case, we only have the inequality $[L : K] > \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$.

# 6 Noether Normalization

## 6.1 Noether Normalization Theorem

The main theorem of this section is:

**Theorem 6.1.1** (Noether Normalization)**.** Let $R$ be a finitely generated commutative $k$-algebra over a field $k$, say $R = k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/\mathfrak{a}$. Then there exists an $r \geq 0$ and elements $z_1, \dots, z_r \in R$ such that:

(a) The $z_i$'s are algebraically independent over $k$.
(b) $R$ is integral over $k[z_1, \dots, z_r]$.

Finally, if $k$ is an infinite field, then the $z_i$ can be chosen to be linear combinations of the $x_i$.

*Proof of Theorem 6.1.1.* Start with a set $\{z_j\}_{j=1}^r$ for some $r \geq 0$ with $R$ integral over $k[z_j]_{j=1}^r$ (e.g. we can start with $\{x_i\}_{i=1}^n$). Either the $z_i$ are algebraically independent, and we are done; or, $r \geq 1$ and there is a $0 \neq f \in k[Z_1, \dots, Z_r]$ such that $f(z_1, \dots, z_r) = 0$. By Strategy 6.1.2 (or Strategy 6.1.4 when $k$ is infinite) explained below, we can replace $z_j$ for $1 \leq j < r$ by $z'_j$ such that $k[z_1, \dots, z_r] = k[z'_1, \dots, z'_{r-1}, z_r]$ and such that the polynomial $f$ when written in these new variables is monic in $z_r$ (possibly after rescaling); and further, we can ensure that if $k$ is infinite then the $z'_j$ are linear combinations of the $z_j$. Having done this, we would conclude that $z_r$ is integral over $k[z'_1, \dots, z'_{r-1}]$, so by transitivity of integrality, $R$ would be integral over $k[z'_1, \dots, z'_{r-1}]$. We have now reduced $r$ by 1. Therefore, by repeating this process finitely many times we will arrive at an algebraically independent collection of the sort required. ∎

**Strategy 6.1.2.** Consider integers $w_1, \dots, w_{r-1} \geq 0$ to be specified later, and set $w_r = 1$. Set $z'_j := z_j - z_r^{w_j}$. In a typical monomial $d_I z^I$ after substitution, we get $d_I \left( \prod_{j=1}^{r-1} (z'_j + z_r^{w_j})^{i_j} \right) z_r^{i_r}$. This has term of highest degree in $z_r$ that looks like $z_r$ to the power $\sum_{j=1}^r i_j w_j$. If we can arrange all of these sums over varying $I$ to be distinct, then we could pick a unique highest order term of power of $z_r$ in the changed polynomial, so after scaling we would be done. This is always possible because of Lemma 6.1.3 below.

**Lemma 6.1.3.** Suppose $\mathcal{I} = \{(i_1, \dots, i_r) : r \geq 0, i_1, \dots, i_r \geq 0\}$ is a *finite* set of ordered $r$-tuples of nonnegative integers. Then there are nonnegative integers, called weights, denoted $w_1, \dots, w_{r-1}, w_r$, such that $w_r = 1$ and if $I \neq I' \in \mathcal{I}$ then $\sum_{j=1}^r i_j w_j \neq \sum_{j=1}^r i'_j w_j$.

*Proof.* We proceed by induction on $r$. If $r = 0, 1$, the result is clear. If $r \geq 2$, then by induction we can choose weights $w_2, \dots, w_r = 1$ such that $\sum_{j=2}^r i_j w_j = \sum_{j=2}^r i'_j w_j \Rightarrow I = I'$. Now choose $w_1 > \max_{I \in \mathcal{I}} \{\sum_{j=2}^r i_j w_j\}$. ∎

**Strategy 6.1.4.** Assume that $k$ is infinite. Set $z'_j := z_j - \alpha_j z_r$ for $1 \leq j < r$ for $\alpha_j$ to be determined later; note that if $z_j$ are linear combinations of $x_i$, then so are $z'_j$. Let $\sum_I c_I z^I$ be the sum of monomials of highest total degree $|I| =: N$ in $f$ (so $c_I \neq 0$ for at least one $I$), and look at $\sum_I c_I \left( \prod_{j=1}^{r-1} (z'_j + \alpha_j z_r)^{i_j} \right) z_r^{i_r}$. The coefficient of $z_r^N$ in this expansion is $c := \sum_I c_I \prod_{j=1}^{r-1} \alpha_j^{i_j}$. Since this is a nontrivial polynomial in $k[\alpha_j]_{j=1}^{r-1}$ and $k$ is infinite, we can choose $\alpha_1, \dots, \alpha_{r-1}$ such that $c \neq 0$. Clearly, none of the the homogenous terms of $f$ of total degree less than $N$ can contribute to the coefficient of $z_r^N$, scaling by $c$ we get a nontrivial relation of integral dependence of $z_r^N$ over $k[z'_1, \dots, z'_{r-1}]$.

∎

*Remark* 5. Geometrically, the Normalization Theorem says that every affine variety admits a finite surjective map to an affine space of its dimension. If the base field is infinite (as are usually the fields we work with in algebraic geometry), then in fact we can take this map to be a linear projection.

**Corollary 6.1.5.** If in addition $R$ is integral, then $r = \operatorname{trdeg}_k R$.

*Proof.* The integral closure $\operatorname{Cl}_{\operatorname{Frac} R}(k(z_1, \dots, z_n)) \subseteq \operatorname{Frac} R$ is a field by Lemma 2.1.6(c) and contains $R$, so it must be $\operatorname{Frac} R$. Therefore, $z_1, \dots, z_r \in \operatorname{Frac} R$ is a transcendence basis and $\operatorname{trdeg}_k \operatorname{Frac} R = r$. ∎

## 6.2 Zariski's Lemma, Hilbert's Nullstellensatz, Jacobson Rings

We begin with useful lemma.

**Lemma 6.2.1** (Artin-Tate Lemma)**.** Let $R \subseteq S \subseteq T$ be rings. Suppose that $R$ is Noetherian, $T$ is a finitely generated $R$-algebra, and that $T$ is integral over $S$ (equivalently, $T$ is a finite $S$-module). Then $S$ is a finitely generated $R$-algebra.

*Proof.* Let $x_1, \dots, x_m$ generate $T$ as an $R$-algebra, and $y_1, \dots, y_n$ generate $T$ as an $S$-module. Then there are expressions of the form $x_i = \sum_j s_{ij} y_j$ and $y_i y_j = \sum_k s_{ijk} y_k$ for $s_{ij}, s_{ijk} \in S$. Let $S' := R[s_{ij}, s_{ijk}]_{i,j,k}$. Since $R$ is Noetherian, so is $S'$, being a finitely-generated $R$-algebra. Any element of $T$ is a polynomial in the $x_i$ with coefficients in $R$; substituting the above, we see that each element of $T$ is module-finite over $S'$ generated by the $y_j$. Since $S'$ is Noetherian and $S$ is a submodule of the finitely generated $S'$-module $T$, we have that $S$ is module-finite over $S'$. Since $S'$ is a finitely-generated $R$ algebra, it follows that $S$ is a finitely generated $R$-algebra as well. ∎

We now come to one of the most fundamental results of the theory. This is so important that we give four proofs.

**Theorem 6.2.2** (Zariski's Lemma)**.** Let $k \subseteq K$ be a field extension. If $K$ is a finitely generated $k$-algebra, then it is a finite algebraic extension.

*Proof 1.* We induct on $n$, the minimal number of generators of $K$ as a $k$-algebra; the case $n = 0$ being trivial. So suppose that $K = k[x_1, \dots, x_n]$ for some $x_i \in K$ and $n \geq 1$. If $K$ is not algebraic over $k$, at least one of the $x_i$, WLOG $x_1$, is not algebraic over $k$. Then $k(T) \cong k(x_1) \subseteq K$, and $K$ is generated as a $k(x_1)$ algebra by $x_2, \dots, x_n$, so by induction $x_2, \dots, x_n$ are algebraic over $k(x_1)$. By clearing out denominators in equations of algebraic dependence, we can find an $f \in k[x_1]$ such that $fx_2, \dots, fx_r$ are integral over $k[x_1]$. Now let $g \in k[x_1]$ be an irreducible not dividing $f$; this is possible, since $k[x_1]$ is a PID with infinitely many irreducibles (say by the same argument as the infinitude of primes). Then $1/g \in k(x_1) \subseteq K = k[x_1, \dots, x_n]$ implies that there is an $N \gg 1$ such that $f^N/g \in k[x_1, fx_2, \dots, fx_n]$. Then $f^N/g \in k(x_1)$ is integral over $k[x_1]$. But $k[x_1]$ is a UFD and hence normal by the rational root theorem, so this shows that $f^N/g \in k[x_1]$, i.e. $f^N = gh$ for some $h \in k[x_1]$. This is a contradiction because $g$ is an irreducible that does not divide $f$. ∎

*Proof 2.* Let $K = k[x_1, \dots, x_n]$. If $K$ is not algebraic over $k$, then $n \geq 1$ we may reorder the $x_i$ to arrange that $x_1, \dots, x_r$ are algebraically independent over $k$ for some $r \geq 1$ and that each of $x_{r+1}, \dots, x_n$ are algebraic over $k(x_1, \dots, x_n)$. Applying Lemma 6.2.1 to $R = k, S = k(x_1, \dots, x_r), T = K$, it follows that the purely transcendental extension $k(x_1, \dots, x_r)$ is a finitely generated $k$-algebra, say $k(x_1, \dots, x_r) = k[y_1, \dots, y_s]$ for some $s \geq 1$. Then each $y_i = f_j/g_j$ for some polynomials $f_j, g_j$ in $x_1, \dots, x_r$. Since there are infinitely many irreducible polynomials in $k[x_1, \dots, x_n]$, we may pick an irreducible $g \in k[x_1, \dots, x_n]$ that does not divide $g_1 \cdots g_s$. Then the element $g^{-1} \in k[y_1, \dots, y_s]$ implies that $g^{-1}$ is polynomial in $y_1, \dots, y_s$, which is not possible; this contradiction shows that $K$ is algebraic over $k$. ∎

*Proof 3.* From Noether Normalization (Theorem 6.1.1), we can write $k \subseteq k[z_1, \dots, z_r] \subseteq K$ where the first extension is polynomial and the second extension is integral. But from Lemma 2.1.6(c), we get that since $K$ is a field, so must be $k[z_1, \dots, z_r]$. This is only possible if $r = 0$. ∎

*Proof 4.* Pick a $0 \neq \alpha \in k$ as in Lemma 2.3.1(b), and let $\Omega := \overline{k}$ and $\varphi : k \hookrightarrow \overline{k}$. Clearly $\varphi(\alpha) \neq 0$, so by Lemma 2.3.1(b) this extends to a homomorphism $K \to \overline{k}$. Since $K$ is a field, this last homomorphism is injective. Therefore, $K$ is algebraic over $k$. Since it is a finitely generated $k$-algebra, it is finite algebraic. ∎

We now present important classical corollaries of Zariski's Lemma.

**Theorem 6.2.3** (Hilbert's Nullstellensatz)**.** Let $k$ be an algebraically closed field and $n \geq 1$ an integer.

(a) If $\mathfrak{m} \subset k[X_1, \dots, X_n]$ is maximal, then there is a unique $(a_1, \dots, a_n) \in \mathbf{A}_k^n$ such that $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$.
(b) (Weak Nullstellensatz) If $\mathfrak{a} \subset k[X_1, \dots, X_n]$ is proper, then $\mathbf{V}(\mathfrak{a}) \neq \emptyset$.
(c) (Strong Nullstellensatz) If $\mathfrak{a} \subseteq k[X_1, \dots, X_n]$ is any ideal, then $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

*Proof.* Let $R := k[X_1, \dots, X_n]$. For (a), let $K := R/\mathfrak{m}$. By Zariski's Lemma (Theorem 6.2.2), $K/k$ is finite algebraic. Since $k$ is algebraically closed, this means that $K = k$ or more precisely that the map $k \hookrightarrow R \twoheadrightarrow K$ is an isomorphism. Therefore, each $X_i = a_i + m_i$ for some $a_i \in k, m_i \in \mathfrak{m}$, whence $(X_1 - a_1, \dots, X_n - a_n) \subseteq \mathfrak{m}$ and so equality must hold. For (b), if $\mathfrak{a}$ is proper, then it is contained in a maximal $\mathfrak{m}$, and then $\mathbf{V}(a) \supseteq \mathbf{V}(\mathfrak{m}) \neq \emptyset$ by (a). For (c), we use the Rabinowitsch trick: the inclusion $\sqrt{\mathfrak{a}} \subseteq \mathbf{I}(\mathbf{V}(\mathfrak{a}))$ is clear; for the other direction, assume $f \in$

$\mathbf{I}(\mathbf{V}(\mathfrak{a}))$. Now $f \in \sqrt{\mathfrak{a}}$ iff $\overline{f} \in \mathrm{Nil}(R/\mathfrak{a})$ iff $(R/\mathfrak{a})[\overline{f}^{-1}] = 0$ iff $(R/\mathfrak{a})[X_{n+1}]/(\overline{f}X_{n+1} - 1) \cong k[X_1, \dots, X_{n+1}]/(\mathfrak{a}, fX_{n+1} - 1) = 0$. But now $\mathbf{V}(\mathfrak{a}, fX_{n+1} - 1) = \emptyset$ by hypothesis, so we are done by (b). ∎

A fortiori, we realize that what the Nullstellensatz is saying that points of $\mathbf{A}^n_k$ correspond bijectively to maximal ideals of $k[X_1, \dots, X_n]$, and for any ideal $\mathfrak{a} \subseteq k[X_1, \dots, X_n]$ we have $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m}$. We call rings with this property *Jacobson rings*; this is developed systematically in the next theorem.

**Theorem 6.2.4** (Jacobson Rings)**.** For a ring $R$, TFAE:

(a) In every quotient ring of $R$, the nilradical equals the Jacobson radical.
(b) Every radical ideal in $R$ is the intersection of maximal ideals (containing it).
(c) Every prime ideal in $R$ is the intersection of maximal ideals (containing it).
(d) Every prime $\mathfrak{p} \subset R$ such that for some $0 \neq x \in R/\mathfrak{p}$ the localization $(R/\mathfrak{p})[x^{-1}]$ is a field is a maximal ideal.
(e) If $S$ is any quotient of $S$ that is an integral domain with the property that for some $0 \neq x \in S$ the localization $S[x^{-1}] = \mathrm{Frac}\, S$, then $x^{-1} \in S$ and $S$ is already a field.
(f) Every finitely generated algebra over $R$ that is a field is finitely generated as an $R$-module.

In this situation:

(g) If $S$ is a finitely generated $R$-algebra by $\varphi : R \to S$, then $S$ also satisfies the above conditions. Further, if $\mathfrak{m} \subset S$ is maximal, then so is $\varphi^{-1}\mathfrak{m} \subset R$.

**Definition 6.2.5.** A ring $R$ is said to be *Jacobson* if it satisifes the above equivalent conditions of Theorem 6.2.4.

It follows that fields and hence finitely generated algebras over fields are Jacobson. A simple example of a non-Jacobson ring is given in Counterexample 1.3.5 above.

*Proof of Theorem 6.2.4.* First we show (a) ⇒ (b) ⇒ (c) ⇒ (a). For (a) ⇒ (b), let $\mathfrak{a} \subseteq R$ be a radical ideal. Then in $R/\mathfrak{a}$ we have $0 = \mathrm{Nil}(R/\mathfrak{a}) = \mathrm{Jac}(R/\mathfrak{a}) = \bigcap_{\mathfrak{m} \subset R/\mathfrak{a}} \mathfrak{m}$, and so going back to $R$ we see that $\mathfrak{a} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m}$. The implication (b) ⇒ (c) is trivial, since every prime is radical. For (c) ⇒ (a), note that if $\mathfrak{a} \subseteq R$ is any ideal then $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m}$, where the first equality is Lemma 1.3.2(a) and the ssecond follows from (c). Passing to the quotient, we conclude again by Lemma 1.3.2(a) that $\mathrm{Nil}(R/\mathfrak{a}) = \sqrt{0_{(R/\mathfrak{a})}} = \bigcap_{\mathfrak{m} \subset R/\mathfrak{a}} \mathfrak{m} = \mathrm{Jac}(R/\mathfrak{a})$.

Next we show (c) ⇔ (d). Suppose (c) holds and $\mathfrak{p}$ and $x$ are given and lift the latter to $x \in R$. Since $x \notin \mathfrak{p}$, by (c) there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ not containing $x$. We claim that $\mathfrak{p} = \mathfrak{m}$. Indeed, if there were a $y \in \mathfrak{m} \smallsetminus \mathfrak{p}$, then looking at $1/y \in \mathrm{Frac}\, R/\mathfrak{p} = (R/\mathfrak{p})[x^{-1}]$ tells us that there is a $z \in R$ and $n \geq 1$ such that $x^n - yz \in \mathfrak{p} \subseteq \mathfrak{m}$, so $x^n \equiv yz \equiv 0 \pmod{\mathfrak{m}}$, contradicting $x \notin \mathfrak{m}$. For (d) ⇒ (c), suppose (d) holds and let $\mathfrak{p}$ be a prime. We have to show that given any $x \in \mathfrak{p}$, there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ such that $x \notin \mathfrak{m}$. Indeed, if $x \notin R/\mathfrak{p}$, then $(R/\mathfrak{p})[x^{-1}]$ is not the zero ring and so has a maximal ideal $\mathfrak{m}_0$; then $\mathfrak{m} := \varphi^{-1}\mathfrak{m}_0$ is a prime in $R$ containing $\mathfrak{p}$ and not containing $x$, where $\varphi : R \twoheadrightarrow R/\mathfrak{p} \xrightarrow{\eta} (R/\mathfrak{p})[x^{-1}]$. We claim that $\mathfrak{m}$ is maximal. Indeed, the composite $R \twoheadrightarrow R/\mathfrak{p} \xrightarrow{\eta} (R/\mathfrak{p})[x^{-1}] \twoheadrightarrow (R/\mathfrak{p})[x^{-1}]/\mathfrak{m}_0 := k$ has kernel exactly $\mathfrak{m}$ and so gives an injection $R/\mathfrak{m} \hookrightarrow k$; since $x \notin \mathfrak{m}$, this extends to a map $(R/\mathfrak{m})[x^{-1}] \hookrightarrow k$. But by construction of $k$ this map is also clearly surjective, and so an isomorphism. By (d), $\mathfrak{m}$ is maximal. Clearly, (e) ⇔ (d).

Finally, we show (e) ⇔ (f). For (e) ⇒ (f), suppose that $K$ is a field and a finitely generated $R$-algebra; let $\varphi : R \to K$ be the morphism that makes it into a $K$-algebra. Now the quotient $S := R/\ker\varphi$ is Jacobson by (a) and an integral quotient of $R$ that is a subring of $K$. Let $k := \mathrm{Frac}\, S$. Since $K$ is a finitely generated $R$-algebra, it is also a finitely generated $k$-algebra, so by Zariski's Lemma (Theorem 6.2.2), $K/k$ is finite algebraic. For the finitely many generators of $x_i$ of $K/k$, write down equations of algebraicity and take a large common denominator $0 \neq x \in S$ of the coefficients so that $S[x^{-1}] \hookrightarrow K$ is an integral extension. By Lemma 2.1.6(c), $S[x^{-1}]$ is a field, i.e. $S[x^{-1}] = \mathrm{Frac}\, S$. Therefore, by (e), $S$ is a field and $S[x^{-1}] = S$. Then $K$ is integral over $S$, and $S$ is clearly integral over $R$, so by transitivity $K$ is integral over $R$. It follows that $K$ is a finitely generated $R$-module by Corollary 2.1.4(a). Finally, assume (f) and suppose $S$ is given. Then $S[x^{-1}]$ is a finitely generated $R$-algebra that is a field, and so by (f) is integral over $R$. Writing an equation of integral dependence of $x^{-1}$ of degree $n \geq 1$ and multiplying throughout by $x^n$ shows then that $x^{-1} \in S^*$ and hence $S = S[x^{-1}] = \mathrm{Frac}\, S$ is a field.

To show (g), it suffices to show that $S$ satisfies (f). If $K$ is a finitely generated $S$-algebra that is a field, then by transitivity of algebra-finiteness, it it is also a finitely generated $R$-algebra. Since $R$ satisfies (f), $K$ is a finitely generated $R$-module, and hence certainly a finitely generated $S$-module. Finally, if $\mathfrak{m} \subset S$ is maximal, then $S/\mathfrak{m}$ is a finitely generated $R$-algebra that is a field, so by (f) again $S/\mathfrak{m}$ is integral over $R$. Then $R/\varphi^{-1}\mathfrak{m} \subseteq S/\mathfrak{m}$ is an integral extension of domains with $S/\mathfrak{m}$ a field, so by Lemma 2.1.6(d) we have that $\varphi^{-1}\mathfrak{m}$ is maximal. ∎

## 6.3 Dimension of Affine Varieties

**Theorem 6.3.1.** Let $k$ be field and $R$ an integral affine $k$-algebra. Then

$$\dim R = \operatorname{trdeg}_k R.$$

This is also the length of every maximal chain of primes in $R$ (such rings are called *universally catenary*).

*Proof.*

(a) To show that $\dim R \leq \operatorname{trdeg}_k R$, it suffices to show that if $\mathfrak{p} \subsetneq \mathfrak{q} \subseteq k[\mathbf{A}^n]$ are primes, then $\operatorname{trdeg}_k k[\mathbf{A}^n]/\mathfrak{q} < \operatorname{trdeg}_k k[\mathbf{A}^n]/\mathfrak{p}$; so suppose contrarily that both of these equal $r \geq 0$. Reorder the $X_i$ in $k[\mathbf{A}^n] = k[X_1, \ldots, X_n]$ if necessary to ensure that $x_1, \ldots, x_r$ is a transcendence basis for $k[\mathbf{A}^n]/\mathfrak{q}$. Then the $x_i$ are also algebraically independent in $k[\mathbf{A}^n]/\mathfrak{p}$ and so form a transcendence basis there as well. Let $S := k[X_1, \ldots, X_r] \setminus \{0\} \subseteq k[\mathbf{A}^n]$, which is a multiplicative subset disjoint from $\mathfrak{q}$. Then $S^{-1}k[\mathbf{A}^n] = k(X_1, \ldots, X_r)[X_{r+1}, \ldots, X_n]$. Then the quotient $S^{-1}k[\mathbf{A}^n]/\mathfrak{p}S^{-1}k[\mathbf{A}^n] \cong k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ is integral over the field $k(x_1, \ldots, x_r) = \operatorname{Frac} k[\mathbf{A}^n]/\mathfrak{p}$ and hence a field itself. This contradicts the fact that $\mathfrak{p}S^{-1}k[\mathbf{A}^n] \subsetneq \mathfrak{q}S^{-1}k[\mathbf{A}^n]$ is not maximal.

(b) To show that $\dim R \geq \operatorname{trdeg}_k R$ we induct on $r := \operatorname{trdeg}_k R$. If $r = 0$, then by Noether normalization $R$ is integral over $k$ and hence a field so that $\dim R = 0$. If $r > 0$, say WLOG that $R = k[\mathbf{A}^n]/\mathfrak{p} = k[x_1, \ldots, x_n]$ with $x_1$ transcendental over $k$. Let $S = k[x_1] \setminus \{0\}$ and notice that $S^{-1}k[\mathbf{A}^n]/\mathfrak{p}S^{-1}k[\mathbf{A}^n] \cong k(x_1)[x_2, \ldots, x_n]$ with $\operatorname{trdeg}_{k(x_1)} k(x_1)[x_2, \ldots, x_n] = r - 1$. By the inductive hypothesis, $\dim S^{-1}k[\mathbf{A}^n]/\mathfrak{p}S^{-1}k[\mathbf{A}^n] \geq r - 1$. Therefore, there is a chain $\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{r-1} \subsetneq k[\mathbf{A}^n]$ disjoint from $S$. In each quotient $k[\mathbf{A}^n]/\mathfrak{p}_i$, the element $x_1$ is not algebraic (since it's not algebraic in $k[\mathbf{A}^n]/\mathfrak{p}$) and so $\operatorname{trdeg}_k k[\mathbf{A}^n]/\mathfrak{p}_{r-1} > 0$. Again by Noether normalization, $k[\mathbf{A}^n]/\mathfrak{p}_{r-1}$ is not a field and inserting a maximal ideal we get a chain of length $r$ in $R$ (starting at $\mathfrak{p}$).

In fact, this last argument proves the last claim as well: it is clearly true if $r = 0$ and if $r > 0$ with $x_1$ transcendental as before, then if $\mathfrak{p} = \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell \subsetneq k[\mathbf{A}^n]$ is any chain with $\ell < r$, then $x_1$ is not algebraic in $k[\mathbf{A}^n]/\mathfrak{p}_\ell$ and so this chain is not maximal.

■

**Corollary 6.3.2.**

(a) The dimension $\dim \mathbf{A}^n_k = n$.
(b) If $R$ is any finitely generated algebra over any field (not necessarily integral), then $\dim R < \infty$.
(c) If $R$ is an integral affine $k$-algebra for a field $k$, then for any prime $\mathfrak{p}$ of $R$ we have $\operatorname{ht} \mathfrak{p} + \operatorname{coht} \mathfrak{p} = \dim R$.

*Proof.* The statement (a) is clear from $\operatorname{trdeg}_k k(\mathbf{A}^n_k) = n$. For (b), note that for any ring $R$ and ideal $\mathfrak{a} \subseteq R$ we have $\dim R/\mathfrak{a} \leq \dim R$; now apply this to $k[\mathbf{A}^n_k]$. The statement in (c) follows from the last statement of Theorem 6.3.1: simply patch together chains of the correct length. ■

# 7 Dimension Theory

## 7.1 Hilbert-Samuel Polynomial

**Theorem 7.1.1.** Let $M$ be a finitely generated module over a Noetherian ring $R$. Then TFAE:

(a) $M$ is Artinian.
(b) $\ell_R(M) < \infty$.
(c) $\operatorname{Ass}(M) \subseteq \operatorname{mSpec} R$.
(d) $\operatorname{Supp}(M) \subseteq \operatorname{mSpec} R$.
(e) $\dim M = 0$.

In this case,

(f) $\operatorname{Ass}(M) = \operatorname{Supp}(M)$.

*Proof.* If $M = 0$, this is clear; hence assume $M \neq 0$. The implication (a) $\Leftrightarrow$ (b) was proven in Theorem 1.8.7(a). By Theorem 4.1.2(h), there is a filtration $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ such that each quotient $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for primes $\mathfrak{p}_i$ such that $\operatorname{Ass}(M) \subseteq \{\mathfrak{p}_i\}_{i=1}^n$. Then by additivity, $\ell_R(M) < \infty$ iff each $\ell_R(R/\mathfrak{p}_i) = \ell_{R/\mathfrak{p}_i}(R/\mathfrak{p}_i) < \infty$ iff each $R/\mathfrak{p}_i$ is an Artinian domain (by Theorem 1.8.7(b)), which happens by Theorem 1.8.6(a) iff $\mathfrak{p}_i$ are maximal; proving (b) $\Leftrightarrow$ (c). For (c) $\Rightarrow$ (d), if $\mathfrak{p} \in \operatorname{Supp}(M)$, then there is a minimal element $\mathfrak{q}$ of $\operatorname{Supp}(M)$ contained in $\mathfrak{p}$. By Theorem 4.1.2(i), this $\mathfrak{q}$ belongs to $\operatorname{Ass} M$ and is hence a maximal ideal, so that $\mathfrak{q} = \mathfrak{p}$. The implication (d) $\Rightarrow$ (c) is trivial by Theorem 4.1.2(b). In all, we have shown the equivalence of (a) through (d) and that this implies (f). Now (e) is clearly equivalent to $\mathbf{V}(\operatorname{Ann} M) \subseteq \operatorname{mSpec} R$, and so Theorem 4.1.2(g) and our (d) imply (e); conversely, (e) implies (c) by Theorem 4.1.2(b). ∎

**Corollary 7.1.2.** For ring $R$, TFAE:

(a) $R$ is Artinian.
(b) $\ell_R(R) < \infty$.
(c) $R$ is Noetherian of dimension 0.
(d) $R$ is Noetherian and $\operatorname{Ass}(R) \subseteq \operatorname{mSpec} R$.

*Proof.* The implication (a) $\Leftrightarrow$ (b) was Theorem 1.8.7(b), as was (a) $\Rightarrow$ (c) when combined with Theorem 1.8.6(b), (h). The implications (c) $\Rightarrow$ (d) $\Rightarrow$ (b) are consequences of the previous theorem.

∎

In particular, a finitely generated module over an Artinian ring has finite length, and is consequently both Noetherian and Artinian.

**Theorem 7.1.3** (Ideals of Definition)**.** Let $(R, \mathfrak{m})$ be an NLR. For an ideal $\mathfrak{a} \subseteq R$, TFAE:

(a) The $\mathfrak{a}$-adic topology on $R$ is the same as the $\mathfrak{m}$-adic topology.
(b) There is an $n \geq 1$ such that $\mathfrak{m}^n \subseteq \mathfrak{a} \subseteq \mathfrak{m}$.
(c) The radical $\sqrt{\mathfrak{a}} = \mathfrak{m}$.
(d) The ideal $\mathfrak{a}$ is $\mathfrak{m}$-primary.
(e) The only prime associated to $\mathfrak{a}$ is $\mathfrak{m}$.
(f) The only prime containing $\mathfrak{a}$ is $\mathfrak{m}$, i.e. $\mathfrak{m}$ is a minimal prime over $\mathfrak{a}$.
(g) The Krull dimension $\dim R/\mathfrak{a} = 0$.
(h) The ring $R/\mathfrak{a}$ is Artinian.
(i) The length $\ell_R(R/\mathfrak{a}) < \infty$.

In this case:

(j) For any integer $n \geq 1$, the ideal $\mathfrak{a}^n$ also satisfies (a)-(f).
(k) Any proper ideal containing $\mathfrak{a}$ also satisfies (a)-(f).
(l) if $M$ is a f.g. $R$-module, then $M/\mathfrak{a}M$ is a f.g. $R/\mathfrak{a}$-module, and hence both Noetherian and Artinian and satisfies $\ell_R(M/\mathfrak{a}M) = \ell_{R/\mathfrak{a}}(M/\mathfrak{a}M) < \infty$.

**Definition 7.1.4.** Any ideal $\mathfrak{a} \subseteq R$ satisfying these equivalence conditions is called an *ideal of definition*.

*Proof.* The equivalence (a) ⇔ (b) is clear from the definition of the $\mathfrak{a}$-adic topology. The equivalence (b) ⇔ (c) is clear because $R$ is Noetherian. The equivalence (c) ⇔ (d) is Lemma 4.2.5(d). The equivalence (d) ⇔ (e) follows from the existence of a reduced primary decomposition. The equivalence (e) ⇔ (f) follows from Corollary 4.2.15(a). Now (f) happens iff $\operatorname{Spec} R/\mathfrak{a} = \operatorname{mSpec} R/\mathfrak{a}$, i.e. $\dim R/\mathfrak{a} = 0$, showing (f) ⇔ (g). The equivalence (g) ⇔ (h) follows from Corollary 7.1.2. Similarly, (h) ⇔ (i) is also clear from Corollary 7.1.2 since $\ell_R(R/\mathfrak{a}) = \ell_{R/\mathfrak{a}}(R/\mathfrak{a})$. The claim in (j) and (k) follow from (b), and (l) follows from Theorem 7.1.1. ∎

**Definition 7.1.5.** Let $(R, \mathfrak{m})$ be an NLR, $\mathfrak{a} \subset R$ an IOD, and $M$ a f.g. $R$-module. Define the *Hilbert-Samuel function* of $M$ w.r.t $\mathfrak{a}$ to be the function $\mathbf{N} \to \mathbf{N}$ given by

$$S^{\mathfrak{a}}_M(n) := \ell_R(M/\mathfrak{a}^n M).$$

In the above scenario, the component $\operatorname{gr}_{\mathfrak{a}}(R)_0 = R/\mathfrak{a}$ is Artinian, and the graded ring $\operatorname{gr}_{\mathfrak{a}}(R)$ is generated over $\operatorname{gr}_{\mathfrak{a}}(R)_0$ by the elements $\overline{a}_1, \dots, \overline{a}_r \in \operatorname{gr}_{\mathfrak{a}}(R)_1$ whenever $\mathfrak{a} = (a_1, \dots, a_r)$. Further, $\operatorname{gr}_{\mathfrak{a}}(M)$ is a finitely generated $\operatorname{gr}_{\mathfrak{a}}(R)$-module.

**Theorem 7.1.6** (Hilbert-Samuel Polynomial)**.** Let $(R, \mathfrak{m})$ be an NLR, $\mathfrak{a} \subset R$ an IOD, and $M$ a f.g. $R$-module.

(a) If $\mathfrak{a} = (a_1, \dots, a_r)$ for some $r \geq 1$, then $S^{\mathfrak{a}}_M$ is polynomial-like in $n$ of degree at most $r$, with the degree being independent of the choice $\mathfrak{a}$ of IOD. Define $d(M) := \deg S^{\mathfrak{a}}_M$.
(b) If $0 \to M' \to M \to M'' \to 0$ is an SES of f.g. $R$-modules, then $d(M) = \max\{d(M'), d(M'')\}$ and $S^{\mathfrak{a}}_{M'}(n) + S^{\mathfrak{a}}_{M''}(n) = S^{\mathfrak{a}}_M(n) + R(n)$ for some $R(n)$ polynomial-like of degree less than $d(M)$.

*Proof.*

(a) From the SES $0 \to \mathfrak{a}^n M/\mathfrak{a}^{n+1}M \to M/\mathfrak{a}^{n+1}M \to M/\mathfrak{a}^n M \to 0$ we get that

$$\Delta^{[1]} S^{\mathfrak{a}}_M(n) = \ell_R(\mathfrak{a}^n M/\mathfrak{a}^{n+1}M) = \ell_{\operatorname{gr}_{\mathfrak{a}}(R)_0}(\operatorname{gr}_{\mathfrak{a}}(M)_n) = h_{\operatorname{gr}_{\mathfrak{a}}(M)}(n)$$

which is polynomial-like in $n$ of degree at most $r-1$ by Theorem 1.11.4. Finally, if $N \geq 1$ is chosen so $\mathfrak{m}^N \subseteq \mathfrak{a} \subseteq \mathfrak{m}$, then for every $n \geq 0$ we have $\mathfrak{m}^{Nn} \subseteq \mathfrak{a}^n \subseteq \mathfrak{m}^n$ so that $S^{\mathfrak{m}}_M(Nn) \geq S^{\mathfrak{a}}_M(n) \geq S^{\mathfrak{m}}_M(n)$.

(b) WLOG $M'' = M/M'$ and so $M''/\mathfrak{a}^n M'' = M/(M' + \mathfrak{a}^n M)$ so that

$$S^{\mathfrak{a}}_M(n) = \ell_R(M/\mathfrak{a}^n M) = \ell_R(M/(M' + \mathfrak{a}^n M)) + \ell_R((M' + \mathfrak{a}^n M)/\mathfrak{a}^n M) = S^{\mathfrak{a}}_{M''}(n) + \ell_R(M'/(M' \cap \mathfrak{a}^n M)).$$

Let $\varphi(n) := \ell_R(M'/(M' \cap \mathfrak{a}^n M))$. It follows that $\varphi$ is polynomial-like; since all terms take only positive values, it follows that $d(M) = \max\{d(M''), \deg \varphi\}$. By the Artin-Rees Lemma (Lemma 1.12.6(b)), there is a $k \geq 0$ such that for all $n \geq k$ we have

$$\mathfrak{a}^n M' \subseteq M' \cap \mathfrak{a}^n M = \mathfrak{a}^{n-k}(M' \cap \mathfrak{a}^k M) \subseteq \mathfrak{a}^{n-k} M'$$

so that $S^{\mathfrak{a}}_{M'}(n) \geq \varphi(n) \geq S^{\mathfrak{a}}_{M'}(n-k)$ for all $n \geq k$; therefore, $d(M') = \deg \varphi$ and $S^{\mathfrak{a}}_{M'}$ and $\varphi$ share the same leading coefficient. It follows that the remainder $R := S^{\mathfrak{a}}_{M'} - \varphi$ has degree less than $d(M') \leq d(M)$.

∎

## 7.2 Main Theorem of Dimension Theory and Regular Rings

Let $(R, \mathfrak{m})$ be a NLR and $M$ a f.g. $R$-module. We have three notions of dimension of $M$:

(a) The Krull dimension $\dim M = \dim R/\operatorname{Ann} M$.
(b) The degree of the Hilbert-Samuel function $d(M) := \deg S^{\mathfrak{a}}_M$ for any IOD $\mathfrak{a}$.
(c) The *Chevalley dimension* $\delta(M)$, defined to be the minimum number $r$ of elements $a_1, \dots, a_r \in \mathfrak{m}$ such that $\dim M/(a_1, \dots, a_r)M = 0$.[5]

Here we have:

**Lemma 7.2.1.** For an NLR $(R, \mathfrak{m})$ and f.g. $R$-module $M$, we have

$$M = 0 \Leftrightarrow \dim M = -1 \Leftrightarrow d(M) = -1 \Leftrightarrow \delta(M) = -1 \text{ and } \ell_R(M) < \infty \Leftrightarrow \dim M = 0 \Leftrightarrow d(M) = 0 \Leftrightarrow \delta(M) = 0.$$

[5] We define $\delta(0) = -1$ and $\delta(M) = 0$ if $\dim M = 0$. This number is finite because $\dim M/\mathfrak{m}M = \dim R/\mathfrak{m} = 0$ by Theorem 7.1.3, so that $\delta(M)$ is less than the number of generators of $M$.

*Proof.* The only nontrivial implication in the first is $d(M) = -1 \Rightarrow M = 0$; the first implies that $S^{\mathfrak{m}}_M(n) = 0$ for $n \gg 1$, so $M = \mathfrak{m}^n M$ for $n \gg 1$, which implies by Nakayama that $M = 0$. The implication $\ell_R(M) < \infty \Leftrightarrow \dim M = 0$ was Theorem 7.1.1; the implication $\ell_R(M) < \infty \Leftrightarrow \delta(M) = 0$ are clear. We have $d(M) = 0$ iff $\Delta^{[1]} S^{\mathfrak{m}}_M(n) = h_{\mathrm{gr}_{\mathfrak{m}}(M)}(n)$ is zero for $n \gg 1$ iff $\mathfrak{m}^n M = \mathfrak{m}^{n+1} M$ iff $\mathfrak{m}^n M = 0$ (by Nakayama) iff $\mathfrak{m}^n \subseteq \operatorname{Ann} M$ iff $\operatorname{Ann} M$ is an IOD and so iff $\dim M = \dim R/\operatorname{Ann} M = 0$ (by Theorem 7.1.3). ∎

The main theorem of this section is:

**Theorem 7.2.2.** Let $(R, \mathfrak{m})$ be a NLR and $M$ a f.g. $R$-module. Then

$$\dim M = d(M) = \delta(M).$$

**Lemma 7.2.3.** If $R$ is an NLR and $\mathfrak{p} \subset R$ a prime, then $\dim R/\mathfrak{p} \leq d(R/\mathfrak{p})$.

*Proof.* We prove by induction on $n$ that if $\mathfrak{p}_n \subsetneq \cdots \subsetneq \mathfrak{p}_0$ is a chain of primes in an NLR $R$, then $n \leq d(R/\mathfrak{p}_n)$, the case $n = 0$ being clear. For $n \geq 1$, pick $x \in \mathfrak{p}_{n-1} \smallsetminus \mathfrak{p}_n$; then $\mathfrak{p}_n + xR \subseteq \mathfrak{p}_{n-1} \subsetneq R$ and so $R/(\mathfrak{p}_n + xR)$ is a nonzero f.g. $R$-module, so $\operatorname{Ass} R/(\mathfrak{p}_n + xR) \neq \emptyset$ by Theorem 4.1.2. Pick a $\mathfrak{q}$ in there, so $\mathfrak{p}_n \subsetneq \mathfrak{p}_n + xR \subseteq \mathfrak{q} \subseteq \mathfrak{p}_{n-1}$. Now from $\mathfrak{q} \subsetneq \mathfrak{q}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_0$ we have by induction $n - 1 \leq d(R/\mathfrak{q})$ and $R/(\mathfrak{p}_n + xR) \twoheadrightarrow R/\mathfrak{q}$, so by Theorem 7.1.6(b) that $d(R/\mathfrak{q}) \leq d(R/(\mathfrak{p}_n + xR))$. Next consider the SES $0 \to R/\mathfrak{p}_n \xrightarrow{\cdot \bar{x}} R/\mathfrak{p}_n \to R/(\mathfrak{p}_n + xR) \to 0$ (the first map being injective because $x \notin \mathfrak{p}_n$), from which it follows from Theorem 7.1.6(b) that $d(R/(\mathfrak{p}_n + xR)) \leq d(R/\mathfrak{p}_n) - 1$. Putting these together, we get $n - 1 \leq d(R/\mathfrak{q}) \leq d(R/(\mathfrak{p}_n + xR)) \leq d(R/\mathfrak{p}_n) - 1$ as needed.

∎

*Main Proof.* By the previous lemma, we need only do $M \neq 0$. We'll show $\dim M \leq d(M) \leq \delta(M) \leq \dim M$.

(a) For $\dim M \leq d(M)$: from Theorem 4.1.2, we get

$$\dim M = \dim R/\operatorname{Ann} M = \sup_{\mathfrak{p} \in \mathbf{V}(\operatorname{Ann} M)} \{\operatorname{coht} \mathfrak{p}\} = \sup_{\mathfrak{p} \in \operatorname{Ass}(M)} \{\operatorname{coht} \mathfrak{p}\},$$

since in the last the minimal elements of both sets coincide. Since $M \neq 0$ is f.g., $\operatorname{Ass}(M)$ is a nonempty finite set, so that $\exists \mathfrak{p} \in \operatorname{Ass}(M) : \dim M = \operatorname{coht} \mathfrak{p} = \dim R/\mathfrak{p}$. Since $\mathfrak{p} \in \operatorname{Ass}(M)$, we have $R/\mathfrak{p} \hookrightarrow M$; but then by Theorem 7.1.6(b), we have $d(R/\mathfrak{p}) \leq d(M)$. Therefore, it suffices to show the inequality for $M = R/\mathfrak{p}$, which is the content of Lemma 7.2.3.

(b) For $d(M) \leq \delta(M)$, we prove this by induction on $\delta(M)$. If $\delta(M) = 0$ then $\ell_R(M) < \infty$ so that $S^{\mathfrak{m}}_M$ is bounded and hence $d(M) = 0$. Next suppose $\delta(M) = r > 0$ and choose $a_1, \ldots, a_r \in \mathfrak{m}$ such that $\ell_R(M/(a_1, \ldots, a_r)M) < \infty$. For $0 \leq i \leq r$, set $M_i := M/(a_1, \ldots, a_i)M$; then clearly $\delta(M_i) = r - i$. Now

$$S^{\mathfrak{m}}_{M_1}(n) = \ell_R(M_1/\mathfrak{m}^n M_1) = \ell_R(M/(a_1 M + \mathfrak{m}^n M)) = \ell_R(M/\mathfrak{m}^n M) - \ell_R(a_1 M/(a_1 M \cap \mathfrak{m}^n M)).$$

Now observe that for $n \geq 1$, the map $M \xrightarrow{\cdot a_1} a_1 M \twoheadrightarrow a_1 M/(a_1 M \cap \mathfrak{m}^n M)$ has kernel $(\mathfrak{m}^n M : a_1) \supseteq \mathfrak{m}^{n-1} M$, so that $M/\mathfrak{m}^{n-1} M \twoheadrightarrow a_1 M/(a_1 M \cap \mathfrak{m}^n M)$, showing that $\ell_R(a_1 M \cap \mathfrak{m}^n M) \leq \ell_R(M/\mathfrak{m}^{n-1} M)$. Thus,

$$S^{\mathfrak{m}}_{M_1}(n) \geq S^{\mathfrak{m}}_M(n) - S^{\mathfrak{m}}_M(n-1) = \Delta^{[1]} S^{\mathfrak{m}}_M(n-1),$$

proving that $d(M_1) \geq d(M) - 1$. Inductively, this shows $d(M_r) \geq d(M) - r$. Now $\delta(M_r) = 0$, so that $d(M_r) = 0$, and hence $0 \geq d(M) - r$, proving $d(M) \leq r = \delta(M)$.

(c) For $\delta(M) \leq \dim M$, observe that $\dim M = 0 \Leftrightarrow \ell_R(M) < \infty \Leftrightarrow \delta(M) = 0$; hence assume $\dim M > 0$. Then $M \neq 0$ is f.g., so that $\operatorname{Ass}(M)$ is nonempty and finite. Since $\dim M = \sup_{\mathfrak{p} \in \operatorname{Ass}(M)} \{\operatorname{coht} \mathfrak{p}\}$, the set $P := \{\mathfrak{p} \in \operatorname{Ass}(M) : \operatorname{coht} \mathfrak{p} = \dim M\} = \{\mathfrak{p} \in \operatorname{Supp}(M) : \operatorname{coht} \mathfrak{p} = \dim M\}$ is nonempty and finite, say $P = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. Since $\operatorname{coht} \mathfrak{m} = 0$, we have $\mathfrak{m} \notin P$, so that by prime avoidance $\mathfrak{m} \not\subseteq \bigcup_{i=1}^t \mathfrak{p}_i$, so pick $x \in \mathfrak{m}$ such that $x \notin \mathfrak{p}_i$ for all $i$. Define $N := M/xM$. Now since $x \notin \mathfrak{p}_i$, the element $x/1 \in R_{\mathfrak{p}_i}$ is invertible, so that $N_{\mathfrak{p}_i} = 0$; this shows that $\operatorname{Supp}(N) \subseteq \operatorname{Supp}(M) \smallsetminus P$, so that

$$\dim N = \sup_{\mathfrak{p} \in \operatorname{Supp}(N)} \{\operatorname{coht} \mathfrak{p}\} \leq \sup_{\mathfrak{p} \in \operatorname{Supp}(M) \smallsetminus P} \{\operatorname{coht} \mathfrak{p}\} \leq \dim M - 1.$$

This means by induction that $\delta(N) \leq \dim N$, so that it suffices to show that $\delta(M) \leq \delta(N) + 1$; but that is clear: if $\ell_R(N/(a_1, \ldots, a_r)N) < \infty$ for some $a_1, \ldots, a_r \in \mathfrak{m}$, then $M/(x, a_1, \ldots, a_r)M \cong N/(a_1, \ldots, a_r)N$ so that $\delta(M) \leq r + 1$.

∎

Let's look at a few corollaries now.

**Corollary 7.2.4.**

(a) Let $(R, \mathfrak{m}, k)$ be a NLR. Any $R$-module has finite Krull dimension. The Krull dimension $\dim R$ is the minimal number of generators of any IOD. In particular, $\dim R \leq \dim_k \mathfrak{m}/\mathfrak{m}^2 < \infty$.[6]
(b) If $R$ is Noetherian, then every prime of $R$ has finite height. In particular, primes of $R$ satisfy the d.c.c.
(c) If $k$ is any field, then $\dim k[\![X_1, \ldots, X_n]\!] = n$.

*Proof.*

(a) For any ring $R$ and ideal $\mathfrak{a}$, clearly $\dim R/\mathfrak{a} \leq \dim R$; therefore, it suffices to show the result for $R$ itself, which is clear since $d(R)$ and $\delta(R)$ are clearly finite; this latter, $\delta(R)$, is the minimum number of generators of any IOD because $\dim R/\mathfrak{a} = 0$ iff $\mathfrak{a}$ is an IOD by Theorem 7.1.3. For the inequality $\dim R \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$, we note that this latter is finite since $\mathfrak{m}$ is f.g., and if $\overline{a}_1, \ldots, \overline{a}_r$ is $k$-basis of $\mathfrak{m}/\mathfrak{m}^2$, then by Corollary 1.6.4(c), the set $a_1, \ldots, a_r$ is a minimal set of generators of the IOD $\mathfrak{m}$.
(b) We have $\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}} < \infty$ by (a).
(c) That $\dim k[\![X_1, \ldots, X_n]\!] \geq n$ is clear; on the other hand, $\mathfrak{m} = (X_1, \ldots, X_n)$ is generated by $n$ elements, so $\dim k[\![X_1, \ldots, X_n]\!] \leq n$ by (a).

■

**Definition 7.2.5.**

(a) A ring $R$ is called a *regular local ring* if it is a Noetherian local ring $(R, \mathfrak{m})$ satisfying $\dim R = \dim_k \mathfrak{m}/\mathfrak{m}^2$ (equivalently, satisfying that $\mathfrak{m}$ is generated by $\dim R$ elements).
(b) A ring $R$ is called a *regular ring* if it is Noetherian and such that $R_{\mathfrak{p}}$ is a regular local ring for each $\mathfrak{p} \subset R$.

These are the nicest kinds of rings. For instance, if $X$ is any scheme and $x \in X$, we say that $X$ is *regular* at $x$ if $\mathcal{O}_{X,x}$ is a regular local ring; regularity is equivalent to smoothness for say algebraic varieties. Other examples of regular local rings are $k[\![X_1, \ldots, X_n]\!]$. An example of a regular ring is $k[X_1, \ldots, X_n]$, although this isn't necessarily obvious. Here are a few examples of what I mean by *nice*:

**Example 7.2.6.** A regular local ring of dimension 0 is a field. A regular local ring of dimension 1 is a DVR; indeed, by Theorem 5.1.6(f)(1), all that remains to be shown is that $R$ is a domain. Assume that $\mathfrak{m} = (t)$; it suffices to show that $t$ is not nilpotent, and that every nonzero element $a \in R$ can be written as $a = ut^n$ for some $u \in R^\times$ and $n \geq 0$. The first is clear because otherwise the only prime of $R$ is $\mathfrak{m}$, contradicting $\dim R = 1$. For the second, we have by Corollary **??** that $\bigcap_{n \geq 0} \mathfrak{m}^n = 0$. Therefore, given any nonzero $a \in R$, there is a unique $n \geq 0$ such that $a \in \mathfrak{m}^n \smallsetminus \mathfrak{m}^{n+1}$. Write $a = ut^n$; since $a \notin \mathfrak{m}^{n+1}$, we must have $u \notin \mathfrak{m}$, and so a unit since $R$ is local.

The really surprising result in this direction is:

**Theorem 7.2.7** (Auslander-Buchsbaum)**.** Every regular local ring is a UFD.

We'll build towards a proof of this below. Another homological proof can be given (Nagata showed that this is true if it's true for all rings of dimension 3; Auslander-Buchsbaum used their homological results to show this for rings of dimension 3).

## 7.3 Krull's Hauptidealsatz

Next, we have a classical theorem.

**Theorem 7.3.1** (Generalized Krull's Hauptidealsatz)**.** Let $R$ be a Noetherian ring and $\mathfrak{p} \subset R$ a prime. For any integer $n \geq 0$, TFAE:

(a) The height $\operatorname{ht} \mathfrak{p} \leq n$.
(b) The prime $\mathfrak{p}$ is minimal over an ideal generated by (at most) $n$ elements.

Geometrically, this is saying that if $k$ is an algebraically closed field and $X \subseteq \mathbf{P}_k^m$ is any variety, then for any $n \geq 0$ we have $\operatorname{codim} X \leq n$ iff $X$ is an irreducible component of a variety cut out by at most $n$ equations, i.e.

[6] The quantity $\dim_k \mathfrak{m}/\mathfrak{m}^2$ is called the *embedding dimension* of the NLR $(R, \mathfrak{m}, k)$.

$n$ equations cannot cut down more than $n$ dimensions. The "at most" is irrelevant because we can always take as many zeroes in the list of generators as we need.

*Proof 1.* We have $\operatorname{ht}\mathfrak{p} \le n \Leftrightarrow \dim R_{\mathfrak{p}} \le n \Leftrightarrow \exists$ IOD $\mathfrak{b} \subseteq R_{\mathfrak{p}}$ generated by $n$ elements. If $\mathfrak{b} = (s^{-1}a_1, \dots, s^{-1}a_n)$ for some $a_i \in \mathfrak{p}$ and $s \notin \mathfrak{p}$, then consider $\mathfrak{a} := (a_1, \dots, a_n) \subseteq \mathfrak{p}$. Since $\mathfrak{b} \subseteq \mathfrak{a}R_{\mathfrak{p}} \subseteq \mathfrak{p}R_{\mathfrak{p}}$, it follows from Theorem 7.1.3(f) and (k) that $\mathfrak{p}R_{\mathfrak{p}}$ is a minimal prime over $\mathfrak{a}R_{\mathfrak{p}}$, which says that $\mathfrak{p}$ is a minimal prime over $\mathfrak{a}$. Conversely, if $\mathfrak{a}$ is such an ideal, then $\mathfrak{a}R_{\mathfrak{p}}$ is an IOD (by Theorem 7.1.3(f)) generated by $n$ elements. ∎

[Cite: Hochster; see Wikipedia.]

*Proof 2.* For (a) ⇒ (b), we induct on $n$, with $n = 0$ being clear; hence assume $n \ge 1$. Of course, it suffices to show the case when $\operatorname{ht}\mathfrak{p} = n$ exactly. By Corollary 4.2.15(a) applied to $R_{\mathfrak{p}}$, there are only finitely many primes of $R$ minimal over (0) and contained in $\mathfrak{p}$. By Prime Avoidance (Lemma 1.1.3(b)), $\mathfrak{p}$ is not contained in the union of these, since otherwise it has height 0; in all, we can pick an element $x \in \mathfrak{p}$ that is not contained in any minimal prime contained in $\mathfrak{p}$. Then the height of $\mathfrak{p}/(x)$ as an ideal in $R/(x)$ is at most $n-1$; any chain of primes contained in $\mathfrak{p}$ of maximal length must have begun with a minimal prime of $R$, and these are not available in $R/(x)$. By induction, $\mathfrak{p}/(x)$ is a minimal prime over an ideal generated by at most $n-1$ elements of $R/(x)$; taking preimages and appending $x$ shows that $\mathfrak{p}$ is a minimal prime over an ideal generated by $n$ elements.

For (b) ⇒ (a), we again induct on $n$, with $n = 0$ clear; hence assume $n \ge 1$. First, by localizing $R$ at $\mathfrak{p}$ we may assume $(R, \mathfrak{p})$ is a local ring. First suppose $n = 1$ (this is the classical Hauptidealsatz) and suppose $\mathfrak{p}$ is minimal over $(a)$; then $R/(a)$ has only one prime, namely $\mathfrak{p}/(a)$, and so $\dim R/(a) = 0$, from which $R/(a)$ is Artinian (Corollary 7.1.2). If $\mathfrak{q} \subsetneq \mathfrak{p}$ is any prime, then the chain $(\mathfrak{q}^{(n)} + (a))/(a)$ in $R/(a)$ eventually stabilizes, saying there is an $n \ge 1$ such that $\mathfrak{q}^{(n)} + (a) = \mathfrak{q}^{(n+1)} + (a)$. It follows that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + a\mathfrak{q}^{(n)}$. Indeed, if $x \in \mathfrak{q}^{(n)}$, then by the above there is a $y \in \mathfrak{q}^{(n+1)}$ and $z \in R$ such that $x = y + az$. Since $a \notin \mathfrak{q}$ by minimality, it follows that $az \in \mathfrak{q}^{(n)}$ implies $z \in \mathfrak{q}^{(n)}$ because $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary. By Nakayama's Lemma (Lemma 1.6.3(c)), it follows that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$ and so $\mathfrak{q}^n R_{\mathfrak{q}} = \mathfrak{q}_{\mathfrak{q}}^{(n)} = \mathfrak{q}_{\mathfrak{q}}^{(n+1)} = \mathfrak{q}^{n+1}R_{\mathfrak{q}}$ (by Corollary 1.2.8(b)), and so again by Nakayama's Lemma 1.6.3(b) it follows that $\mathfrak{q}^n R_{\mathfrak{q}} = 0$. It follows from Example 1.7.4 and Corollary 7.1.2 that $R_{\mathfrak{q}}$ is Artinian, so that $\operatorname{ht}\mathfrak{q} = \dim R_{\mathfrak{q}} = 0$.

Now suppose $n \ge 2$ and suppose $\mathfrak{p}$ is minimal over $(a_1, \dots, a_n)$, so that $\mathfrak{p} = \sqrt{(a_1, \dots, a_n)}$ by Lemma 1.3.2(a). Let $\mathcal{A}$ be the collection of primes strictly contained in $\mathfrak{p}$; since $\mathfrak{p}$ is f.g., it is easy to see that every chain in $\mathcal{A}$ has an upper bound. If $\mathcal{A}$ is empty, then $\mathfrak{p}$ is minimal and $\operatorname{ht}\mathfrak{p} = 0$. Else, Zorn's Lemma applied to $\mathcal{A}$ gives us a prime $\mathfrak{q} \subsetneq \mathfrak{p}$ such that there is no prime strictly between them. By minimality, this $\mathfrak{q}$ cannot contain all the $a_i$; WLOG assume $a_1 \notin \mathfrak{q}$. Since every prime containing $\mathfrak{q} + (a_1)$ is between $\mathfrak{q}$ and $\mathfrak{p}$, it follows from Lemma 1.3.2(a) that $\sqrt{\mathfrak{q} + (a_1)} = \mathfrak{p}$, so that for each $i$ with $2 \le i \le n$ we have $a_i^{n_i} = x_i + y_i a_1$ for some $n_i \ge 1$, $x_i \in \mathfrak{q}$ and $y_i \in R$. In the ring $R/(x_2, \dots, x_n)$, every minimal prime over $\overline{a}_1$ contains all the $\overline{a}_i$'s and is hence $\overline{\mathfrak{p}}$; therefore, $\overline{\mathfrak{p}}$ is a minimal prime over $\overline{a}_1$, so by $n = 1$, the prime $\overline{\mathfrak{q}}$ is a minimal prime over $\overline{0}$, i.e. $\mathfrak{q}$ is a minimal prime over $(x_2, \dots, x_n)$. By induction, $\operatorname{ht}\mathfrak{q} \le n-1$, so that $\operatorname{ht}\mathfrak{p} \le n$ as needed. ∎

**Corollary 7.3.2.** Let $R$ be a Noetherian ring.

(a) If $x \in R$ is nonzero, not a unit, and not a zero divisor, then every minimal prime over $(x)$ has height 1.
(b) In the situation of (a), if further $R$ is local, then $\dim R/xR = \dim R - 1$.
(c) More generally, if $R$ is local, $M$ is a nonzero f.g. $R$-module, and $x$ is nonzero and neither a unit nor a zero divisor *for* $M$, then $\dim M/xM = \dim M - 1$.

*Proof.*

(a) By the theorem, it suffices to show that such a $\mathfrak{p}$ cannot have height 0, so suppose that is the case. Now $0 \ne x/1 \in R_{\mathfrak{p}}$ implies $\mathfrak{p} \in \operatorname{Supp} R$, but if $\mathfrak{p}$ is minimal then by Theorem 4.1.2 we have $\mathfrak{p} \in \operatorname{Ass} R$ and so $x \in \mathfrak{p} \subseteq \bigcup \operatorname{Ass} R = \mathfrak{Z}(R)$, a contradiction.
(b) By Lemma 1.1.4 and (a), $\dim R \ge 1$ and $\dim R/xR \le \dim R - 1$; to show the converse, if $\delta(R/xR) = r$, then there are $a_1, \dots, a_r \in \mathfrak{m}$ such that $(\overline{a}_1, \dots, \overline{a}_r) \subseteq R/xR$ is an $\mathfrak{m}/xR$-primary ideal, from which $(x, a_1, \dots, a_r) \subseteq R$ is $\mathfrak{m}$-primary (using say Theorem 7.1.3(h)), showing $\delta(R) \le \delta(R/xR) + 1$.
(c) Note that in this case, $\dim M \ge 1$; indeed, if $\dim M = 0$, then by Theorems 4.1.2 and 7.1.1 we have $\emptyset \subsetneq \operatorname{Ass} M \subseteq \operatorname{mSpec} R = \{\mathfrak{m}\}$, so $x \in \mathfrak{m} = \bigcup \operatorname{Ass} M = \mathfrak{Z}(M)$. Next, $\operatorname{Ann} M/xM \supseteq \operatorname{Ann} M + xR$ so $R/(\operatorname{Ann} M + xR) \twoheadrightarrow R/\operatorname{Ann}(M/xM)$ and hence $\dim M/xM \le \dim R/(\operatorname{Ann} M + xR)$. Now $R/(\operatorname{Ann} M + xR) \cong (R/\operatorname{Ann} M)/(\overline{x})$, and $\overline{x}$ is neither a unit (since $\overline{x} \in \overline{\mathfrak{m}}$) nor a zero divisor (if there is a $y \notin \operatorname{Ann} M$ such that $xy \in \operatorname{Ann} M$, then there is an $m \in M$ such that $ym \ne 0$ but $x(ym) = 0$, a contradiction to $x \notin \mathfrak{Z}(M)$). Therefore, by (b) we have $\dim R/(\operatorname{Ann} M + xR) = \dim M - 1$, so we have shown $\dim M/xM \le \dim M -$

1. For the other direction, proceed as in (b): if $\delta(M/xM) = r$, then there are $a_1, \dots, a_r \in \mathfrak{m}$ such that $\ell_R(M/(x, a_1, \dots, a_r)M) = \ell_R((M/xM)/(a_1, \dots, a_r)(M/xM)) < \infty$, so $\delta(M) \leq \delta(M/xM) + 1$.

■

## 7.4 Systems of Parameters

**Definition 7.4.1.** Let $(R, \mathfrak{m})$ be an NLR and $M$ a f.g. $R$-module of $\dim M = n$. Then a *system of parameters* (SOP) for $M$ is a collection of $n$ elements $a_1, \dots, a_n \in \mathfrak{m}$ such that $\dim M/(a_1, \dots, a_n)M = 0$.

For instance, a SOP for $M = R$ is a set of generators of an IOD of size $\dim R$; e.g. $\{X_1, \dots, X_n\}$ is a SOP for both $\dim k[X_1, \dots, X_n]_{(X_1,\dots,X_n)}$ and $k[\![X_1, \dots, X_n]\!]$.

**Theorem 7.4.2.** Let $(R, \mathfrak{m})$ be an NLR and $M$ a f.g. $R$-module of $\dim M = n$. Given any $t \geq 0$ and $a_1, \dots, a_t \in \mathfrak{m}$ we have $\dim M/(a_1, \dots, a_t)M \geq n - t$ with equality iff the set $\{a_1, \dots, a_t\}$ can be completed to a SOP.

*Proof.* Prove the inequality by induction on $t$, with $t = 0$ clear. If $t = 1$ and $\dim M/a_1M = r$, then there are $b_1, \dots, b_r \in \mathfrak{m}$ such that $0 = \dim(M/a_1M)/(b_1, \dots, b_r)(M/a_1M) = \dim M/(a_1, b_1, \dots, b_r)M$, so $n \leq r + 1$. If $t \geq 2$, then by the induction hypothesis and case $t = 1$ we have

$$\dim \frac{M}{(a_1, \dots, a_t)M} = \dim \frac{M/a_1M}{(a_2, \dots, a_t)(M/a_1M)} \geq \dim M/a_1M - (t-1) \geq (n-1) - (t-1) = n - t.$$

If the set can be completed to an SOP $\{a_1, \dots, a_n\}$, then if we let $I_t := (a_1, \dots, a_t)$ and $J_t := (a_{t+1}, \dots, a_n)$, we get

$$0 = \dim \frac{M}{(I_t + J_t)M} = \dim \frac{M/I_tM}{J_t(M/I_tM)} \geq \dim M/I_tM - (n-t) \geq (n-t) - (n-t) = 0,$$

so equality holds everywhere. Conversely, if $\dim M/I_tM = n - t$, then there are $a_{t+1}, \dots, a_n \in \mathfrak{m}$ such that if $J_t$ is as before, then $\dim M/(I_t + J_t)M = \dim(M/I_tM)/J_t(M/I_tM) = 0$, so $\{a_1, \dots, a_n\}$ is a SOP for $M$. ■

**Corollary 7.4.3.** Let $R$ be a NLR and $M$ a nonzero f.g. $R$-module. If $x$ is nonzero and neither a unit nor a zero divisor for $M$, then $x$ belongs to a SOP for $M$.

## 7.5 Regular Sequences, Depth, and Cohen-Macaulay Rings

**Definition 7.5.1.** Let $R$ be a ring and $M$ an $R$-module.

(a) A sequence of nonzero elements $a_1, \dots, a_n \in R$ is said to be *$M$-regular* if $(a_1, \dots, a_n)M \neq M$ and $a_i \notin \mathfrak{Z}(M/(a_1, \dots, a_{i-1})M)$ for $1 \leq i \leq n$.
(b) A *regular sequence* in $R$ is an $R$-regular sequence.
(c) If $\mathfrak{a} \subset R$ is any ideal, we define the *depth of $M$ in $\mathfrak{a}$*, written $\operatorname{depth}_{\mathfrak{a}} M$, to be the supremum over all $n$ such that $\mathfrak{a}$ contains an $M$-regular sequence of length $n$.

# 8 Homological Algebra

# 9 Applications

## 9.1 Auslander-Buchsbaum Theorem

**Theorem 9.1.1.** Every regular local ring is a UFD.

## 9.2 Application to Polynomial and Power Series Rings

**Theorem 9.2.1.** For a Noetherian ring $R$ and $n \geq 1$, we have $\dim R[X_1, \ldots, X_n] = \dim R[\![X_1, \ldots, X_n]\!] = \dim R + n$.

**Theorem 9.2.2.** Let $R$ be a regular UFD. Then so is the power series ring $R[\![X_1, \ldots, X_n]\!]$ for any $n \geq 1$.