Commutative Algebra

Dhruv Goel

Contents

Preface

Based on Math 221 Fall 2020 by Popa. I make no originality claims. Much from Szamuely, Lang, Cohn, Sam's notes, Matsumura, Frölich-Taylor, Conrad's notes, Poonen's notes, Stacks project. [TODO]

Conventions

- A *ring* is always taken to mean a commutative unitary ring, unless explicitly specified otherwise (as will be in sections ...).
- We do not disallow the zero ring, although when we speak of proper ideals (including prime or maximal ideals, which are always assumed to be proper), we implicitly assume that the ring is nonzero. The zero ring is not considered to be a field.
- For a ring R, we denote the subset of units of R by $R^\times \subset R$, so that a nonzero ring R is a field iff $R^\times = R \setminus \{0\}$.
- For subsets A, B of a set X, we take $A \subset B$ to mean $x \in A \Rightarrow x \in B$; therefore, the case $A = B$ is not excluded. If we want to specifically exclude this case, we write $A \subsetneq B$.
- The symbol $\mathbf{N}$ always refers to the set of all nonnegative integers, so that, in particular, $0 \in \mathbf{N}$.
- A *monoid* is always a commutative monoid written additively.

Chapter 1

Fundamentals

1.1 Localization

Definition 1.1.1 (Localization)**.** Let R be a ring.

(a) A subset $S \subset R$ is called *multiplicative* if finite products of elements of S are in S.
(b) If $S \subset R$ is a multiplicative system, the *localization of R with respect to S* is a ring $S^{-1}R$ and a homomorphism $\eta : R \to S^{-1}R$ such that $\eta(S) \subset (S^{-1}R)^\times$ and that $(S^{-1}R, \eta)$ is initial with respect to this property. The homomorphism η is called the *localization homomorphism*.
(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[1] $\eta : M \to S^{-1}M$ such that any R-module homomorphism from M to (the underlying R-module of) an $S^{-1}R$-module factors through η.

Remark 1.1.2.

(a) By the universal property, localization is unique up to unique isomorphism commuting with the η's–if it exists. We give three explicit constructions: one is to take simply $S^{-1}R := R[\{x_s\}]_{s\in S}/(sx_s - 1)$, and another 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 letting $\eta : x \mapsto 1^{-1}x$. The third construction first inverts a single element s (or equivalently the subset $S = \{1, s, s^2, \dots\}$ of powers of s) by consider the colimit $R[s^{-1}]$ of $R \xrightarrow{s} R \xrightarrow{s} R \cdots$ in the category of R-modules and equipping it with a suitable R-algebra structure; the general case is handled by noting that $S^{-1}R = \varinjlim_{s\in S} R[s^{-1}]$ as R-algebras.[2] Similarly, $S^{-1}M$ can be constructed in several ways; the most explicit is to take classes $s^{-1}m$ as in the second construction.
(b) 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 restriction of scalars functor $\eta_* : S^{-1}R\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$.This tells us that 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.
(c) Algebraically, localization of a ring R (resp. an R-module M) at a subset S is the "freest" way to make S invertible as elements of a ring to which R maps (resp. as endomorphisms of an R-module to which M maps). Geometrically, we can think of the localization of a ring R at a subset S as the operation of "throwing out (the vanishing locus of) S"; try to interpret Examples 1.1.4, 1.1.6 and Corollary 1.1.12 this way.

Lemma 1.1.3. Let $S \subset R$ be a multiplicative subset in a ring R and M be an R-module. Then the localization map $\eta : M \to S^{-1}M$ has kernel

$$\mathrm{Ann}_S(M) := \{m \in M : um = 0 \text{ for some } u \in S\}.$$

In particular,

(a) The localization $S^{-1}R$ is zero iff $0 \in S$.
(b) The localization homomorphism $\eta : R \to S^{-1}R$ is injective iff S contains no zero divisors.

Proof. We have $1^{-1}0 = 1^{-1}m$ iff there is a $u \in S$ such that $um = 0$; (a) and (b) follow immediately. ∎

[1] Here $S^{-1}M$ is considered an R-module by restriction of scalars via the map $\eta : R \to S^{-1}R$.
[2] Of course, in doing this, one should be familiar with arbitrary colimits of algebras.

Example 1.1.4 (Inverting an Element)**.** Given any ring R and $x \in R$, the subset $S = \{1, x, x^2, \dots\}$ of powers of x in R is multiplicative. The localization $S^{-1}R \cong R[y]/(xy-1)$ is denoted by $R[x^{-1}]$. By the Lemma 1.1.3(a), this is zero iff x is nilpotent.

Example 1.1.5 (Total Quotient Ring)**.** Given a ring R, the set $S = R \setminus \mathcal{Z}(R) \subset R$ of nonzerodivisors of R is multiplicative. The localization $S^{-1}R =: \operatorname{Quot} R$ is called the *total quotient ring* of R. By Lemma 1.1.3, 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 $S \subset R \setminus \mathcal{Z}(R)$ and so by Exercise 1.1, the natural morphism $S^{-1}R \to \operatorname{Quot} R$ is injective. The total quotient ring of R satisfies the following universal property: if $\varphi : R \to S$ is a ring homomorphism such that $\varphi(R \setminus \mathcal{Z}(R)) \subset S \setminus \mathcal{Z}(S)$ (i.e. φ takes nonzerodivisors in R to nonzerodivisors in S), then φ extends to a homomorphism $\operatorname{Quot} R \to \operatorname{Quot} S$.

Example 1.1.6 (Localization at a Prime)**.** Let R be a ring and $\mathfrak{p} \subset R$ an ideal. Then $\mathfrak{p}$ is prime iff its complement $S := R \setminus \mathfrak{p}$ is multiplicative, in which case the ring $S^{-1}R = (R \setminus \mathfrak{p})^{-1}R$ is called the *localization of R at $\mathfrak{p}$* and denoted $R_{\mathfrak{p}}$. Similarly, given an R-module M, the localization $S^{-1}M =: M_{\mathfrak{p}}$ is called the *localization of M at $\mathfrak{p}$*.

Example 1.1.7 (Field of Fractions)**.** When R is a domain, Example 1.1.5 is a special case of Example 1.1.6: 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 the *field of fractions* or *fraction field* of R. Again, the map $\eta : R \to \operatorname{Frac} R$ is injective. The fraction field of an integral domain is universal with respect to injective homomorphisms out of the domain to fields; in other words, the fraction field functor from the category of integral domains and injective homomorphisms to the category of fields and field homomorphisms is left adjoint to the forgetful functor. By Exercise 1.1, if R is an integral domain, then all localizations of R can be embedded in $\operatorname{Frac} R$ and are integral domains themselves.

For an example of a total quotient ring of a ring that is not a domain, see Exercise 1.2. One reason for the usefulness of this notion comes from the fact that many module-theoretic properties can be checked locally. One instance of this phenomenon is

Lemma 1.1.8. Let R be a ring and M be an R-module. Then for any element $x \in M$, the following are equivalent:

(a) $x = 0$,
(b) $[x] = 0 \in S^{-1}M$ for every multiplicative $S \subset R$,
(c) $[x] = 0 \in M_{\mathfrak{p}}$ for every prime $\mathfrak{p}$, and
(d) $[x] = 0 \in M_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$.

In particular, the following are equivalent:

(a) $M = 0$,
(b) $S^{-1}M = 0$ for every multiplicative $S \subset R$.
(c) $M_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$, and
(d) $M_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$.

Proof. Clearly, (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d). For (d) $\Rightarrow$ (a), for $0 \neq x \in M$, the annihilator $\operatorname{Ann}_R(x) \subset R$ is a proper ideal, so there is an $\mathfrak{m} \subset R$ such that $\operatorname{Ann}_R(x) \subset \mathfrak{m}$; then $0 \neq [x] \in M_{\mathfrak{m}}$ by Lemma 1.1.3. ∎

Theorem 1.1.9 (Localization Is Exact)**.** If $\mathscr{C}$ is a complex of R-modules and $S \subset R$ is a multi-

plicative subset, then the natural map $S^{-1}H\mathscr{C} \to H(S^{-1}\mathscr{C})$ given by functoriality is an isomorphism.

Proof. This map takes $s^{-1}[n] \mapsto [s^{-1}n]$. For injectivity, 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 $u(s \cdot \partial m - tn) = 0$ so that $utn = \partial(usm)$ and

$$s^{-1}[n] = (uts)^{-1}ut[n] = (uts)^{-1}[utn] = (uts)^{-1}[\partial(usm)] = (uts)^{-1}0 = 0.$$

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 1.1.10. Let R be a ring and $\varphi : M \to N$ and $\psi : N \to P$ homomorphisms of R-modules.

(i) The following are equivalent:
  (a) $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ is exact.
  (b) $S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}N \xrightarrow{S^{-1}\psi} S^{-1}P$ is exact for every multiplicative $S \subset R$.
  (c) $M_{\mathfrak{p}} \xrightarrow{\varphi_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{\psi_{\mathfrak{p}}} P_{\mathfrak{p}}$ is exact for all $\mathfrak{p}$.
  (d) $M_{\mathfrak{m}} \xrightarrow{\varphi_{\mathfrak{m}}} N_{\mathfrak{m}} \xrightarrow{\psi_{\mathfrak{m}}} P_{\mathfrak{m}}$ is exact for all $\mathfrak{m}$.

(ii) The following are equivalent:
  (a) $\varphi : M \to N$ is injective (resp. surjective).
  (b) $S^{-1}\varphi : S^{-1}M \to S^{-1}N$ is injective (resp. surjective) for every multiplicative $S \subset R$.
  (c) $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective (resp. surjective) for all $\mathfrak{p}$.
  (d) $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp. surjective) for all $\mathfrak{m}$.

Proof. Part (i) follows from Lemma 1.1.8 and Theorem 1.1.9. Part (ii) follows by applying (i) and choosing one of the M and P to be zero. ∎

The above corollary (specifically (ii)(b)) says that if R is a ring and $N \subset M$ an R-submodule, then for any multiplicative system $S \subset R$, the natural map $S^{-1}N \to S^{-1}M$ is injective, allowing us to think of $S^{-1}N$ as an $S^{-1}R$-submodule of $S^{-1}M$. We will implicitly use this identification in all that follows. This perspective allows us to relate submodules of the localization to submodules of the original module as in

Observation 1.1.11 (Submodules of Localization)**.** Let R be a ring, $S \subset R$ multiplicative, M an R-module, and $\eta : M \to S^{-1}M$ the localization map.

(a) If M is finitely generated over R, then so is $S^{-1}M$ over $S^{-1}R$, by the images under η of the generators.
(b) If $N \subset M$ is a submodule, then $N \subset \eta^{-1}(S^{-1}N)$.[3] For any $S^{-1}R$-submodule $L \subset S^{-1}M$ we have $L = S^{-1}(\eta^{-1}L)$.[4]
(c) Every $S^{-1}R$-submodule of $S^{-1}M$ is of the form $S^{-1}N$ for some R-submodule $N \subset M$. In particular, if M is Noetherian (resp. Artinian) 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.

[3] In general, equality need not hold; for instance, if $S = R$.
[4] The inclusion $L \subset S^{-1}\eta^{-1}L$ follows from noting that $s^{-1}\ell \in L \Rightarrow \ell \in \eta^{-1}L$.

Reinterpreting the above in the language of ideals gives us:

Corollary 1.1.12 (Ideals in Localization)**.** Let R be a ring and $S \subset R$ multiplicative and $\eta : R \to S^{-1}R$ the localization.

(a) If $\mathfrak{a} \subset R$ is an ideal, then so is $S^{-1}\mathfrak{a} \subset S^{-1}R$; if $\mathfrak{a}$ is finitely generated then so is $S^{-1}\mathfrak{a}$. Further, $S^{-1}\mathfrak{a}$ is proper iff $\mathfrak{a} \cap S = \emptyset$.
(b) If $\mathfrak{a} \subset R$ is an ideal, then $\mathfrak{a} \subset \eta^{-1}(S^{-1}\mathfrak{a})$. If $\mathfrak{b} \subset S^{-1}R$ is an ideal, then $\mathfrak{b} = S^{-1}(\eta^{-1}\mathfrak{b})$.
(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 so $S^{-1}\mathfrak{q}$ 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 bijections between primes $\mathfrak{q} \subset R$ disjoint from S and primes $\mathfrak{Q} \subset S^{-1}R$.
(e) In particular, if $S = R \smallsetminus \mathfrak{p}$ 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 a local ring (see Proposition/Definition 1.2.7).

Therefore, $\operatorname{Spec} S^{-1}R \subset \operatorname{Spec} R$ can be thought of as the set of primes disjoint from S. In particular, $\operatorname{Spec} R_\mathfrak{p}$ is the set of primes contained in $\mathfrak{p}$: we have "localized" to look only at primes contained in $\mathfrak{p}$. Finally, we present two neat results which will be helpful later.

Corollary 1.1.13 (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 $R \subset S$; 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 $\mathfrak{p} = \mathfrak{q} \cap R \subset (\mathfrak{q} \cap R)S \cap R \subset \mathfrak{q} \cap R = \mathfrak{p}$. Conversely, if $\mathfrak{p} = (\mathfrak{p}S) \cap R$, then $\mathfrak{p}S \cap (R \smallsetminus \mathfrak{p}) = \emptyset$, so that by Corollary 1.1.12(a), the ideal $\mathfrak{p}S_\mathfrak{p} \subset S_\mathfrak{p} := (R \smallsetminus \mathfrak{p})^{-1}S$ 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 $R \smallsetminus \mathfrak{p}$ by Corollary 1.1.12(d), and contains $\mathfrak{p}S$. Therefore, $\mathfrak{p} = \mathfrak{p}S \cap R \subset \mathfrak{q} \cap R \subset \mathfrak{p}$. ∎

Corollary 1.1.14. Let R be a domain with fraction field K, so that all localizations to follow can be considered as subsets of K. If $\mathfrak{a} \subset R$ is any ideal, then $\mathfrak{a} = \bigcap_\mathfrak{p} \mathfrak{a}R_\mathfrak{p} = \bigcap_\mathfrak{m} \mathfrak{a}R_\mathfrak{m}$. In particular, if $\mathfrak{a}, \mathfrak{b} \subset R$ are ideals such that $\mathfrak{a}R_\mathfrak{m} = \mathfrak{b}R_\mathfrak{m}$ for all maximal ideals $\mathfrak{m} \subset R$, then $\mathfrak{a} = \mathfrak{b}$.

Proof. The inclusions $\mathfrak{a} \subset \bigcap_\mathfrak{p} \mathfrak{a}R_\mathfrak{p} \subset \bigcap_\mathfrak{m} \mathfrak{a}R_\mathfrak{m}$ are clear. Suppose $x \in \bigcap_\mathfrak{m} \mathfrak{a}R_\mathfrak{m}$, and consider the ideal $(\mathfrak{a} :_R x) := \{y \in R : xy \in \mathfrak{a}\}$. If $(\mathfrak{a} :_R x)$ is a proper ideal, then there is a maximal ideal $\mathfrak{m} \subset R$ such that $(\mathfrak{a} :_R x) \subset \mathfrak{m}$, which contradicts $x \in \mathfrak{a}R_\mathfrak{m}$; this shows that $1 \in (\mathfrak{a} :_R x)$, i.e. $x \in \mathfrak{a}$. ∎

1.2 Some Affine Algebraic Geometry

1.2.1 Scheinnullstellensatz, Radicals, and Local Rings

For a ring R, we let $\operatorname{Spec} R$ denote the set of its prime ideals and call it the *spectrum* of R. For any subset $\mathfrak{a} \subset R$, we define $\mathbf{V}(\mathfrak{a}) := \{\mathfrak{p} : \mathfrak{p} \supset \mathfrak{a}\} \subset \operatorname{Spec} R$, and for any subset $X \subset \operatorname{Spec} R$, we let $\mathbf{I}(X) := \bigcap_{\mathfrak{p} \in X} \mathfrak{p}$. Clearly $\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\langle \mathfrak{a} \rangle)$, where $\langle \mathfrak{a} \rangle \subset R$ is the ideal generated by $\mathfrak{a}$; therefore, we can restrict ourselves to looking at ideals $\mathfrak{a}$. Then $\mathbf{V}$ and $\mathbf{I}$ give inclusion-reversing maps between the set of ideals in R and subsets of $\operatorname{Spec} R$; these are not inverse bijections, but rather inverse Galois correspondences, and hence inverse bijections on appropriate subsets–namely the set of subsets $X \subset \operatorname{Spec} R$ of the form $X = \mathbf{V}(\mathfrak{a})$ for some $\mathfrak{a}$, and the set of ideals $\mathfrak{a} \subset R$ of the form $\mathfrak{a} = \mathbf{I}(X)$ for some $X \subset \operatorname{Spec} R$.

Observation 1.2.1. Given a ring R, we have:

(a) $\mathbf{V}(0) = \operatorname{Spec} R$ and $\mathbf{V}(1) = \emptyset$,
(b) If $(\mathfrak{a}_i)$ is a family of ideals of R, then $\mathbf{V}\left(\bigcup_i \mathfrak{a}_i\right) = \mathbf{V}\left(\sum_i \mathfrak{a}_i\right) = \bigcap_i \mathbf{V}(\mathfrak{a}_i)$.
(c) If $\mathfrak{a}, \mathfrak{b} \subset R$ are ideals, then $\mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbf{V}(\mathfrak{a}\mathfrak{b}) = \mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b})$.

It follows from Observation 1.2.1 that the subsets of $\operatorname{Spec} R$ of the form $\mathbf{V}(\mathfrak{a})$ for $\mathfrak{a} \subset R$ satisfy the axioms for closed sets of a topology on $\operatorname{Spec} R$; this topology is called the *Zariski topology*. It is easy to see that if $X \subset \operatorname{Spec} R$ is any subset, then $\mathbf{V}(\mathbf{I}(X)) = \overline{X}$, where the closure is with respect to the Zariski topology. Conversely, if $\mathfrak{a} \subset R$ is any ideal, then $\mathbf{I}(\mathbf{V}(\mathfrak{a}))$ is given by

Theorem 1.2.2 (Scheinnullstellensatz)**.** Let R be a ring and $\mathfrak{a} \subset R$ an ideal. Then $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Proof. Replace R by $R/\mathfrak{a}$ to assume $\mathfrak{a} = 0$. To show the nontrivial inclusion, suppose that $x \in R$ is *not* nilpotent. Then $R[x^{-1}]$ is not the zero ring by Example 1.1.4, and therefore has a maximal ideal $\mathfrak{m}$. If $\eta : R \to R[x^{-1}]$ is the localization map, then the preimage $\eta^{-1}\mathfrak{m} \subset R$ is a prime not containing x. ∎

Remark 1.2.3. Geometrically, Theorem 1.2.2 says that the any regular function that vanishes at every point on the scheme $\operatorname{Spec} R$ is nilpotent, so the only regular function that vanishes that every point on a reduced affine scheme is zero. In light of the above discussion, we conclude from Theorem 1.2.2 that the maps $\mathbf{V}$ and $\mathbf{I}$ give inverse bijections between the set of closed subsets of $\operatorname{Spec} R$ and radical ideals of R. In algebraic geometry, this statement says that every closed subscheme of the affine scheme $\operatorname{Spec} R$ admits a unique reduced structure; this is true of all schemes and not just affine schemes.

Definition 1.2.4. Given a ring R, we define its *nilradical* to be

$$\operatorname{Nil}(R) := \sqrt{0} = \bigcap_{\mathfrak{p} \subset R} \mathfrak{p}.$$

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

Remark 1.2.5. Reduction is functorial, and the reduction of a reduced ring is itself; put another way, $R \to R^{\mathrm{red}}$ is initial with respect to homomorphisms out of R to reduced rings, i.e. if

$\varphi : R \to S$ is a homomorphism with S reduced, then φ factors as $R \to R^{\text{red}} \xrightarrow{\bar{\varphi}} S$ for some $\bar{\varphi} : R^{\text{red}} \to S$. In fact, the full subcategory of Ring consisting of reduced rings is reflective in the sense that the reduction functor is left adjoint to the inclusion; in particular, reduction commutes with arbitrary colimits.

Given that the intersection of all primes of a ring is interesting, it makes sense to look also at the intersection of all maximal ideals of a ring.

Proposition/Definition 1.2.6 (Jacobson Radical)**.** Let R be a ring and $x \in R$ be an element. Then the folowing are equivalent:

(a) The element x lies in every maximal ideal of R.
(b) For any $y \in R$ and unit $u \in R^\times$, we have $u + xy \in R^\times$.
(c) For any $y \in R$, we have $1 + xy \in R^\times$.

The ideal consisting of all such $x \in R$ is called the *Jacobson radical* of R, and is denoted by

$$\operatorname{Jac}(R) := \bigcap_{\mathfrak{m} \subset R} \mathfrak{m}.$$

Proof.

(a) $\Rightarrow$ (b) If x were to lie in every maximal ideal of R, but there were $y \in R$ and $u \in R^\times$ such that $u + xy \notin R^\times$, then there would be a maximal $\mathfrak{m} \subset R$ such that $u + xy \in \mathfrak{m}$. Then $x, u + xy \in \mathfrak{m} \Rightarrow u \in \mathfrak{m}$, a contradiction.
(b) $\Rightarrow$ (c) Clear.
(c) $\Rightarrow$ (a) If x were such but there were a maximal ideal $\mathfrak{m} \subset R$ such that $x \notin \mathfrak{m}$, then $\mathfrak{m} + (x) = (1)$ implies $m - xy = 1$ for some $m \in \mathfrak{m}, y \in R$, giving $m = 1 + xy \in R^\times \cap \mathfrak{m}$, a contradiction.

■

Proposition/Definition 1.2.7 (Local Rings)**.** For a nonzero ring R, the folowing are equivalent:

(a) The set of nonunits $R \setminus R^\times$ 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.

A ring R is said to be *local* if it is nonzero and satisfies these equivalent conditions. Finally, if R is a local ring, then for any proper ideal $\mathfrak{a} \subset R$, so is the quotient $R/\mathfrak{a}$.

Proof.

(a) $\Rightarrow$ (b) Every proper ideal of R is be contained in $R \setminus R^\times$, so if this subset is an ideal then it is the unique maximal ideal.
(b) $\Rightarrow$ (a) The unique maximal ideal contains every element of $R \setminus R^\times$ and must also be contained in $R \setminus R^\times$.
(b) $\Rightarrow$ (c) This follows from Proposition/Definition 1.2.6.
(c) $\Rightarrow$ (b) Let $\mathfrak{m}$ be some maximal ideal in R[5] and $x \in \mathfrak{m}$. By Proposition/Definition 1.2.6 again, $x \in \operatorname{Jac}(R)$; this shows that $\mathfrak{m} \subset \operatorname{Jac}(R) \subset \mathfrak{m}$, so that $\operatorname{Jac}(R) = \mathfrak{m}$ is the unique maximal ideal.

The last statement is clear. ■

[5] This uses that R is nonzero.

Local rings are usually denoted by the writing down 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 1.1.12(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, where the identification of the residue field is clear via a suitable universal property.

Remark 1.2.8. Since every maximal ideal is prime, it follows for any ring R that $\mathrm{Nil}(R) \subset \mathrm{Jac}(R)$, but equality need not hold in general, as any local domain other than a field (e.g. $\mathbf{Z}_{(p)}$ or $k[x]_{(x)}$) shows.

One other notion we will have occasion to use is that of semilocal rings:

Definition 1.2.9. A nonzero ring R is called *semilocal* if it has only finitely many maximal ideals.

In particular, any local ring is semilocal. An example of a non-local semilocal ring is a finite product of fields, e.g. $\mathbf{Q} \times \mathbf{Q}$. We shall meet more examples of semilocal rings in §1.3.

1.2.2 Minimal Primes and Prime Avoidance

Next up are a couple of other very useful geometrical results.

Lemma 1.2.10. Let R be a ring, and $\mathfrak{a} \subset R$ be a proper ideal. There is a minimal prime over $\mathfrak{a}$. In fact, if we fix a prime $\mathfrak{p}$ containing $\mathfrak{a}$, then there is a minimal prime over $\mathfrak{a}$ which is contained in $\mathfrak{p}$.

A prime of R minimal over $\mathfrak{a} = (0)$ is simply called a *minimal prime*. The above result shows, in particular, that any nonzero ring admits a minimal prime.

Proof. It suffices to show the latter result, since every proper ideal is contained in some maximal (and hence prime) ideal. Apply Zorn's Lemma to $\mathbf{V}(\mathfrak{a}) \cap \mathrm{Spec}\, R_\mathfrak{p}$ ordered by reverse inclusion: if $(\mathfrak{q}_\alpha)$ is a chain then $\mathfrak{q} := \bigcap_\alpha \mathfrak{q}_\alpha$ is also a prime containing $\mathfrak{a}$, as follows. If $xy \in \mathfrak{q}$ but $x, y \notin \mathfrak{q}$, then there are α, β such that $x \notin \mathfrak{q}_\alpha, y \notin \mathfrak{q}_\beta$; without loss of generality, if $\mathfrak{q}_\alpha \subset \mathfrak{q}_\beta$, then $y \notin \mathfrak{q}_\alpha$ and so $xy \in \mathfrak{q}_\alpha$ but $x, y \notin \mathfrak{q}_\alpha$, a contradiction to the primality of $\mathfrak{q}_\alpha$. ∎

Remark 1.2.11. Geometrically, this lemma says that if $X = \mathbf{V}(\mathfrak{a}) \subset \mathrm{Spec}\, R$ is any closed subscheme of an affine scheme, then X contains a maximal irreducible component. The second part says that if we fix any point in X, then there is a maximal irreducible component of X containing this given point. We will see in Corollary 3.2.10(a) below that in the Noetherian setting there are only finitely many irreducible components.

Lemma 1.2.12 (Prime Avoidance)**.** Let R be a ring, n a positive integer, and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ ideals.

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

Stated equivalently, (b) reads that if $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ are ideals such that either R contains an infinite field or at most two of the $\mathfrak{a}_i$ are not prime, then if $\mathfrak{a} \subset R$ is any ideal such

that $\mathfrak{a} \not\subset \mathfrak{a}_i$ for all $i = 1, \ldots, n$, then $\mathfrak{a} \not\subset \bigcup_{i=1}^{n} \mathfrak{a}_i$, i.e. there is an $x \in \mathfrak{a}$ such that $x \notin \mathfrak{a}_i$ for all $i = 1, \ldots, n$.

Proof.

(a) Else, pick for each i an $a_i \in \mathfrak{a}_i \smallsetminus \mathfrak{p}$; then $\prod_i a_i \in \bigcap_i \mathfrak{a}_i \smallsetminus \mathfrak{p}$ using the primality of $\mathfrak{p}$.

(b) We leave the case of when R contains an infinite field to the reader (see Exercise 1.7). 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 $x_1 \in \mathfrak{a} \smallsetminus \mathfrak{a}_2 \subset \mathfrak{a}_1 \smallsetminus \mathfrak{a}_2$ and $x_2 \in \mathfrak{a} \smallsetminus \mathfrak{a}_1 \subset \mathfrak{a}_2 \smallsetminus \mathfrak{a}_1$. Then $x_1 + x_2 \in \mathfrak{a} \smallsetminus \mathfrak{a}_1 \cup \mathfrak{a}_2$, a contradiction. Suppose now that $n \geq 3$ and $\mathfrak{a}_3, \ldots, \mathfrak{a}_n$ are prime. Inductively, we may 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

$$x_i \in \mathfrak{a} \smallsetminus (\mathfrak{a}_1 \cup \cdots \cup \hat{\mathfrak{a}}_i \cup \cdots \cup \mathfrak{a}_n) \subset \mathfrak{a}_i \smallsetminus (\mathfrak{a}_1 \cup \cdots \cup \hat{\mathfrak{a}}_i \cup \cdots \cup \mathfrak{a}_n).$$

Then $x_1 \cdots x_{n-1} \subset \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1} \smallsetminus \mathfrak{a}_n$ 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.

■

Remark 1.2.13. Usually, only the statement in (b) is called the Prime Avoidance Lemma. Geometrically, (a) says that if a point (or irreducible closed subscheme) of an affine scheme is contained in a finite union of closed subschemes, then it must be contained in one of them. Similarly, the statement in (b), or its contrapositive, can be stated geometrically in many ways; here are two:

(i) If finitely many points (or irreducible closed subschemes) of an affine scheme are contained in an open subset, then there is a smaller principal open subset containing all of them.

(ii) If $X_1, \ldots, X_n$ are irreducible subvarieties of an affine variety X and $f_1, \ldots, f_m$ functions on X such that for any X_i there is an f_j such that f_j doesn't vanish identically on X_i, then there is some linear combination of the f_j's that doesn't vanish identically on any of the X_i's.

1.2.3 Krull Dimension

Let us end this section with one final important notion.

Definition 1.2.14. Let R be a ring.

(a) The *Krull dimension* of R, denoted $\dim R$, is the supremum of the lengths of chains of primes in R, i.e. it is the supremum of the set of integers $n \geq 0$ such that there are primes $\mathfrak{p}_i \subset R$ for $i = 0, \ldots, n$ such that

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n.$$

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

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

(c) Let $\mathfrak{p} \subset R$ be a prime. The *height of* $\mathfrak{p}$ is the supremum of lengths of chains of primes contained in $\mathfrak{p}$, i.e. $\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}}$, and the *coheight* of $\mathfrak{p}$ is the supremum of lengths of chains of primes containing $\mathfrak{p}$, i.e. $\operatorname{coht} \mathfrak{p} := \dim R/\mathfrak{p}$.

Example 1.2.15.

(a) For a ring R, we have $\dim R = 0$ iff all primes of R are incomparable (e.g. if R has only one prime). For a domain R, this happens iff R is a field.
(b) If $(R, \mathfrak{m}, k)$ is a local ring then $\operatorname{ht} \mathfrak{m} = \dim R$.
(c) If R is a PID that is not a field, then $\dim R = 1$.
(d) If k is a field, then $\dim k[X_1, \ldots, X_n] \geq n$ and $k[\![X_1, \ldots, X_n]\!] \geq n$. Also, $\dim k[X_1, X_2, \ldots] = \infty$. In fact, equality holds in the first two, but this will have to wait (see [TO DO]).
(e) If R is a ring and $\mathfrak{p} \subset R$ a prime, then $\operatorname{ht} \mathfrak{p} + \operatorname{coht} \mathfrak{p} \leq \dim R$ and equality holds for most reasonable rings (e.g. coordinate rings of affine varieties, see [TO DO])), but not always! See Example 10.5.2.

We will have much to say about dimension soon.

1.3 Noetherian and Artinian Rings and Modules

Proposition/Definition 1.3.1. Let R be a ring.

i. An R-module M is *Noetherian* if it satisfies the following equivalent properties:
   (a) The ascending chain condition (a.c.c.) on submodules of M: every increasing sequence $M_0 \subset M_1 \subset M_2 \subset \cdots$ 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.
   (d) Given any sequence a of elements $a_1, a_2, \ldots$ in M, there is an integer $m_0 = m_0(a) \geq 1$ such that for each $m > m_0$, there are $f_{mn} \in R$ for $n = 1, \ldots, m_0$ with $a_m = \sum_{n=1}^{m_0} f_{mn} a_n$.

   The ring R is *Noetherian* if it is Noetherian as a module over itself, or equivalently if every ideal in R is finitely generated.

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

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

Example 1.3.2.

(a) If $R = k$ is a field, then an R-module M is Noetherian iff it is Artinian iff it has finite dimension.
(b) The $\mathbf{Z}$-module $\mathbf{Z}$ is Noetherian but not Artinian. For any prime p, the $\mathbf{Z}$-module $\mathbf{Z}[1/p]/\mathbf{Z}$ is Artinian but not Noetherian (see Exercise 1.9).
(c) Finite rings, finite products of fields, and finite-dimensional algebras over fields (for instance, the rings $k[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^m$ for $n, m \geq 1$) are both Noetherian and Artinian.[6]
(d) The rings $\mathbf{Z}, \mathcal{O}_K$ and $k[X_1, \ldots, X_n]$ for fields k are Noetherian but not Artinian.
(e) Given any ring R, the polynomial ring $R[X_1, X_2, \ldots]$ over R in countably many variables is not Noetherian (nor Artinian[7].)

Observation 1.3.3. Let R be a ring and M an R-module.

(a) Let $M' \subset M$ be a submodule. If $N \subset N' \subset M$ are submodules such that $N \cap M' = N' \cap M'$ and $(N + M')/M' = (N' + M')/M'$, then $N = N'$.
(b) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules, then M is Noetherian (resp. Artinian) iff both M' and M'' are.
(c) If M is Noetherian (resp. Artinian), then so is $M^{\oplus n}$ for each $n \geq 1$.
(d) If R is Noetherian (resp. Artinian) and M a finitely generated R-module, then M is Noetherian (resp. Artinian).

Let's start with one criterion relating length to the conditions of being Noetherian or Artinian.

Lemma 1.3.4. A module has finite length iff it is both Noetherian and Artinian.

Proof. Let M be an R-module. If $\ell_R(M) < \infty$, then for all submodules $0 \subset N \subsetneq N' \subset M$ we

[6] The phrase "both Noetherian and Artinian" is redundant for rings, where the apparent symmetry between the definitions of the two conditions is misleading. See Theorem 1.3.10.

[7] See previous footnote.

have

$$0 \leq \ell_R(N) < \ell_R(N') \leq \ell_R(M),$$

so that M satisfies both the a.c.c. and the d.c.c. on submodules. If M is Noetherian, then Lemma 10.1.2 allows us to produce a series of submodules

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$$

with simple successive quotients. If M is also Artinian, this series must eventually terminate. ■

1.3.1 Noetherian Rings

Next up are some standard results on (identifying) Noetherian rings:

Theorem 1.3.5 (Generalized Hilbert Basis Theorem)**.** If R is Noetherian, then so are $R[X]$ and $R[\![X]\!]$.

Proof. Let $\mathfrak{a} \subset R[X]$ be an ideal. For each $m \geq 0$, let $\mathfrak{a}_m \subset R$ be the ideal consisting of leading coefficients of polynomials in $\mathfrak{a}$ of degree m. Since R is Noetherian, each $\mathfrak{a}_m$ is finitely generated and we may find an $m_0 \geq 1$ such that $\mathfrak{a}_{m_0} = \mathfrak{a}_{m_0+1} = \cdots$. For each $0 \leq m \leq m_0$, let a_{mn} be finitely many generators of $\mathfrak{a}_m$, and pick polynomials $f_{mn} \in \mathfrak{a}$ of degree m with these leading coefficients. We claim that (f_{mn}) generate $\mathfrak{a}$. To show this, we proceed by induction on the degree of $f \in \mathfrak{a}$ to show that $f \in (f_{mn})$, with the case of negative degree (i.e. zero) being trivial. Hence suppose that $\deg f = d \geq 0$, and let a be the leading coefficient of f. If $d \leq m_0$, then we can write $a = \sum_n c_n a_{dn}$ for some $c_n \in R$, and then $f - \sum_n c_n f_{dn} \in \mathfrak{a}$ has degree less than d. If $d \geq m_0 + 1$, then $a = \sum_n c_n a_{m_0 n}$ for some $c_n \in R$, and then $f - \sum_n c_n X^{d-m_0} f_{m_0 n} \in \mathfrak{a}$ has degree less than d.

The proof for $R[\![X]\!]$ is similar. Let $\mathfrak{a} \subset R[\![X]\!]$, and for each $m \geq 0$, let $\mathfrak{a}_m \subset R$ be the ideal of leading cofficients of power series in $\mathfrak{a} \cap (X^m)$. Then let m_0, a_{mn} and $f_{mn} \in \mathfrak{a}$ be as before; again, we claim that the (f_{mn}) generate $\mathfrak{a}$. Given an $f \in \mathfrak{a}$, take an R-linear combination f_0 of the f_{0n} so that $f - f_0 \in \mathfrak{a} \cap (X)$. Then take an R-linear combination f_1 of the f_{1n} so that $f - f_0 - f_1 \in \mathfrak{a} \cap (X^2)$. Continue to produce $f_2, \ldots, f_{m_0}$ so that $f - f_0 - f_1 - \cdots - f_{m_0} \in \mathfrak{a} \cap (X^{m_0+1} b)$. Now since $\mathfrak{a}_{m_0} = \mathfrak{a}_{m_0+1}$, take a linear combination f_{m_0+1} of the $X f_{m_0 n}$ so $f - f_0 - f_1 - \cdots - f_{m_0} - f_{m_0+1} \in \mathfrak{a} \cap (X^{m_0+2})$. Similarly, produce $f_{m_0+2}, f_{m_0+3}, \ldots$. For each $m \geq m_0$, write $f_m = \sum_n a_{mn} X^{m-m_0} f_{m_0 n}$ and for each n, let $g_n = \sum_{m=m_0}^{\infty} a_{mn} X^{m-m_0} \in R[\![X]\!]$. Then $f = f_0 + \cdots + f_{m_0-1} + \sum_n g_n f_{m_0 n}$. ■

Theorem 1.3.6 (Cohen)**.** Let R be a ring. Any ideal of R which is maximal (with respect to inclusion) in the collection of ideals of R which are not finitely generated is prime. In particular, if all prime ideals of R are finitely generated, then R is Noetherian.

Proof. Let $\mathfrak{a}$ be this maximal element. If $\mathfrak{a}$ is not prime, then there are $x, y \in R$ such that $x, y \notin \mathfrak{a}$ but $xy \in \mathfrak{a}$. By maximality, $\mathfrak{a} + (x)$ and $(\mathfrak{a} : x) \supset \mathfrak{a} + (y)$ are finitely generated, so pick generators $u_1, \ldots, u_n, x$ of $\mathfrak{a} + (x)$ with $u_j \in \mathfrak{a}$ and $v_1, \ldots, v_m$ of $(\mathfrak{a} : x)$. Then $\mathfrak{a} = (u_1, \ldots, u_n, v_1 x, \ldots, v_m x)$, which is a contradiction. ■

Theorem 1.3.7. Let R be a ring and M an R-module. If M is Noetherian (resp. finitely generated Artinian), then $R/\operatorname{Ann}(M)$ is a Noetherian (resp. Artinian) ring. In particular, if R admits a faithful Noetherian module, then it is Noetherian.

Proof. The submodules of M as an R-module and $R/\operatorname{Ann} M$-module coincide, so we may reduce to the case $\operatorname{Ann} M = 0$, i.e. when M is faithful. If M is generated by $x_1, \ldots, x_n$, then the map $R \to M^{\oplus n}$ given by $[r] \mapsto (rx_1, \ldots, rx_n)$ is injective; now apply Observation 1.3.3(b). ■

Theorem 1.3.8 (Eakin-Nagata-Formanek)**.** Let R be a ring.

(a) Let M be a finitely generated faithful R-module. If the set of submodules of M of the form $\mathfrak{a}M$ for ideals $\mathfrak{a} \subset R$ satisfies the ascending chain condition, then R is Noetherian.
(b) Let $R \subset S$ be a ring extension. If S is Noetherian and a finitely generated R-module, then R is Noetherian.

Proof. For (b), take $M = S$ in (a). To show (a), by Theorem 1.3.7, it suffices to show that M is a Noetherian R-module. Suppose not, so that the collection

$$\mathfrak{A} := \{\mathfrak{a}M : \mathfrak{a} \subset R \text{ ideal and } M/\mathfrak{a}M \text{ is not Noetherian}\}$$

is nonempty. By assumption, this collection has a maximal element, say $\mathfrak{a}M$. Replacing M by $M/\mathfrak{a}M$ and R by $R/\operatorname{Ann}(M/\mathfrak{a}M)$, we can assume that M is non-Noetherian but for any nonzero ideal $\mathfrak{a} \subset R$, the quotient $M/\mathfrak{a}M$ is Noetherian. Now let

$$\mathscr{B} := \{N \subset M : M/N \text{ is a faithful } R\text{-module}\}.$$

If M is generated by $x_1, \ldots, x_n$, then a submodule $N \subset M$ is in B iff for all $r \in R \smallsetminus \{0\}$ we have $\{rx_1, \ldots, rx_n\} \not\subset N$. Therefore, Zorn's Lemma applies to $\mathscr{B}$ and produces a maximal element $N_0 \in \mathscr{B}$. If M/N_0 is Noetherian, then by Theorem 1.3.7 the ring R is Noetherian and hence so is M, which is a contradiction. Therefore, replacing M by M/N_0 gives us an R-module M with the following three properties:

(i) M is not a Noetherian R-module.
(ii) For any nonzero ideal $\mathfrak{a} \subset R$, the quotient $M/\mathfrak{a}M$ is Noetherian.
(iii) For any nonzero submodule $N \subset M$, the quotient M/N is not a faithful R-module.

Let $N \subset M$ be any nonzero submodule. By (iii), there is a nonzero $r \in R$ such that $rM \subset N$. By (ii), the quotient M/rM is Noetherian, so that the submodule $N/rM \subset M/rM$ is finitely generated. Since M and hence rM is finitely generated as well, it follows that N is finitely generated. Since this is true for every $N \subset M$, it follows that M is Noetherian, contradicting (i).

■

1.3.2 Artinian Rings

We end this section with a closer examination of Artinian rings.

Theorem 1.3.9. Let R be an Artinian ring.

(a) If R is a domain or a reduced local ring, then R is a field.
(b) Every prime ideal of R is maximal (i.e. $\dim R = 0$).
(c) The radical $\operatorname{Nil}(R) = \operatorname{Jac}(R)$ is nilpotent.
(d) R is semilocal.
(e) R is a finite direct product of Artinian local rings.

Proof.

(a) Given a nonzero $a \in R$, applying the d.c.c. to $(a) \supset (a^2) \supset \cdots$ gives us an integer $k \geq 1$ such that $(a^k) = (a^{k+1})$. By Exercise 1.10 applied to the case where R is a domain or a local ring, there is a unit $u \in R^\times$ such that $a^{k+1} = ua^k$, i.e. $a^k(a-u) = 0$. If R is a domain, then this implies that $a = u$, so we are done. If R is a local ring and $a \notin R^\times$, then $u \in R^\times$ implies that $a - u \in R^\times$ (Proposition/Definition 1.2.6 and 1.2.7), and so $a^k = 0$. If R is also reduced, it follows that $a = 0$, which is a contradiction. Therefore, we must have $a \in R^\times$.

(b) If $\mathfrak{p} \subset R$ is a prime ideal, then $R/\mathfrak{p}$ is an Artinian domain, so we are done by (a).

(c) Let $\mathfrak{n} = \mathrm{Nil}(R) = \mathrm{Jac}(R)$. By the d.c.c. applied to $\mathfrak{n} \supset \mathfrak{n}^2 \supset \cdots$, there is a $k \geq 1$ such that $\mathfrak{n}^k = \mathfrak{n}^{k+1} = \cdots$. If $\mathfrak{n}^k \neq 0$, then the family of ideals $\mathscr{A} = \{\mathfrak{a} \subset R : \mathfrak{a}\mathfrak{n}^k \neq 0\}$ is nonempty since $\mathfrak{n} \in \mathscr{A}$. Since R is Artinian, $\mathscr{A}$ contains a minimal element, say $\mathfrak{a}$. Now $\mathfrak{a}\mathfrak{n}^k \neq 0$, so there is an $r \in \mathfrak{a}$ such that $r \cdot \mathfrak{n}^k \neq 0$; then by minimality $\mathfrak{a} = (r)$. But now $r \cdot \mathfrak{n} \subset (r)$ is such that $r \cdot \mathfrak{n} \cdot \mathfrak{n}^k = r \cdot \mathfrak{n}^k \neq 0$, so that by minimality $r \cdot \mathfrak{n} = (r)$. Therefore, $r = rs$ for some $s \in \mathfrak{n}$, so that $r = rs^n$ for all $n \geq 1$. But $s \in \mathfrak{n} = \mathrm{Nil}(R)$, so this means $r = 0$, contrary to hypothesis. Therefore, $\mathfrak{n}^k = 0$.

(d) Consider the collection of all finite intersections of maximal ideals of R, which is nonempty as soon as R is not the zero ring. Since R is Artinian, this has a minimal element, say $\bigcap_{i=1}^n \mathfrak{m}_i$. We claim that $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ are all the maximal ideals of R. Indeed, if $\mathfrak{m} \subset R$ is any other maximal ideal, then minimality gives us $\bigcap_{i=1}^n \mathfrak{m}_i = \mathfrak{m} \cap \bigcap_{i=1}^n \mathfrak{m}_i \subset \mathfrak{m}$, so by Lemma 1.2.12(a) there is an i such that $\mathfrak{m}_i \subset \mathfrak{m}$, whence $\mathfrak{m}_i = \mathfrak{m}$ by maximality.

(e) By (c) and (d), there is a $k \geq 1$ such that $\mathfrak{n}^k = 0$ where $\mathfrak{n} = \bigcap_{i=1}^n \mathfrak{m}_i = \prod_{i=1}^n \mathfrak{m}_i$. Since the $\{\mathfrak{m}_i^k\}_i$ are pairwise comaximal, the Chinese Remainder Theorem gives us that

$$R = R/\prod_{i=1}^n \mathfrak{m}_i^k \cong \prod_{i=1}^n R/\mathfrak{m}_i^k.$$

Each quotient $R/\mathfrak{m}_i^k$ is Artinian (because it is a quotient of R), and local (thanks to Exercise 1.8).

■

This result shows that Artinian local rings are nonreduced analogs of fields.

Theorem 1.3.10 (Akizuki-Hopkins)**.** An Artinian ring is Noetherian.

Proof 1 of Theorem 1.3.10. Let R be an Artinian ring. We will show that if M is an Artinian R-module, then M is finitely generated; this suffices, since every ideal of R is an Artinian R-module by Observation 1.3.3(b). If M is not finitely generated, then the family $\mathscr{A}$ 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 $M[a] := (0 :_M a) \subsetneq M$, so it is finitely generated. From the short exact sequence

$$0 \to M[a] \to M \xrightarrow{\cdot a} aM \to 0$$

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. ■

Proof 2 of Theorem 1.3.10. We will show that a ring R is Artinian iff $\ell_R(R) < \infty$. The "if" direction, as well as the result of the theorem, follow then from Lemma 1.3.4. By (the proof

of) Theorem 1.3.9(e), there are maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_N \subset R$, not necessarily distinct, with $\prod_{i=1}^{N} \mathfrak{m}_i = 0$. Consider the chain $R \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_N = 0$, 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 so an Artinian $k_i := R/\mathfrak{m}_i$-module, hence a Noetherian k_i-module (Examples 1.3.2(a)), and hence a Noetherian R-module. It follows then from Lemma 1.3.4 that each $\ell_R(Q_i) < \infty$. From the additivity of length (Corollary 10.1.6), we conclude that

$$\ell_R(R) = \sum_{i=1}^{N} \ell_R(Q_i) < \infty.$$

■

We shall prove later (§3.3) that a Noetherian ring of dimension zero is Artinian.

1.4 Unique Factorization I

In this section we study unique factorization of elements into irreducibles in domains.

Definition 1.4.1. A domain R is said to be *atomic* if every nonzero nonunit of R can be written as a product of irreducible elements.

If a domain R satisfies the ascending chain condition on principal ideals (e.g. if R is Noetherian), then R is atomic, although the converse does not hold (see [1]). We will need

Definition 1.4.2. Let R be a ring, and $x, y \in R$ elements.

(a) An element $\ell \in R$ is said to be a *least common multiple* (l.c.m.) of x and y if $x, y \mid \ell$ and if $\ell' \in R$ is any other element such that $x, y \mid \ell'$, then $\ell \mid \ell'$.
(b) An element $g \in R$ is said to be a *greatest common divisor* (g.c.d.) of x and y if $g \mid x, y$ and if $g' \in R$ is any other element such that $g' \mid x, y$, then $g' \mid g$.

By Exercise 1.10, l.c.m.s and g.c.d.s are unique in strongly associate rings when they exist.

Theorem/Definition 1.4.3 (Unique Factorization Domains)**.** The following conditions on an atomic domain are equivalent:

(a) The factorization of any nonzero element into irreducibles is unique up to reordering of factors and multiplication by units.
(b) Every irreducible element is prime.
(c) The intersection of an arbitrary collection of principal ideals is principal.
(d) The intersection of any two principal ideals is principal.
(e) Any two elements have a least common multiple.
(f) Any two elements have a greatest common divisor.
(g) Any minimal nonzero prime (i.e. prime of height one) is principal.

An atomic domain satisfying these conditions is said to be a *unique factorization domain* (UFD).

Proof.

(a) $\Leftrightarrow$ (b) Standard and left to the reader (see Exercise 1.13).
(a) $\Rightarrow$ (c) Factoring each $x_i = u_i \prod_\alpha p_\alpha^{v_{\alpha,i}}$ with $u_i \in R^\times$ and p_α distinct primes gives $\bigcap_i (x_i) = \left(\prod_\alpha p_\alpha^{\max_i v_{\alpha,i}} \right)$, where the intersection is zero iff $\max_i v_{\alpha,i}$ does not exist (i.e. is ∞) for some α.
(c) $\Rightarrow$ (d) Clear.
(d) $\Rightarrow$ (e) Clear from the definition of the least common multiple.
(e) $\Rightarrow$ (f) If R is any domain and $x, y \in R$ elements which have a least common multiple, then x and y have a greatest common divisor. Indeed, if $(x) \cap (y) = (z)$, then there is a $d \in R$ with $xy = zd$. From $\ell \in (x)$ we get $y \in (d)$, and similarly $x \in (d)$, so that $(x, y) \subset (d)$. If d' is some other element such that $(x, y) \subset (d')$, thne $x = d'x_0$ and $y = d'y_0$ whence $d'x_0y_0 \in (x) \cap (y) = (z)$ and hence $zd = xy = (d'x_0y_0)d' \in (zd')$, and so $(d) \subset (d')$.
(f) $\Rightarrow$ (b) Let p be an irreducible element, and suppose $x, y \in R$ are such that $p \mid xy$ but $p \nmid y$. By irreducibility of p, it is easy to see (check!) that $\gcd(x, p) = 1$ and now $p \mid \gcd(xy, py) = \gcd(x, p)y = y$.
(b) $\Rightarrow$ (g) Let $\mathfrak{p}$ be a minimal nonzero prime, and let $0 \neq f \in \mathfrak{p}$. Factor f into irreducibles and use

the primality of $\mathfrak{p}$ to conclude that $\mathfrak{p}$ contains an irreducible element. Conclude from (b) using the minimality of $\mathfrak{p}$ that $\mathfrak{p}$ is principal.

(g) $\Rightarrow$ (b) This is harder. Let p be an irreducible element, and let $\mathfrak{p}$ be a minimal prime over (p) (Lemma 1.2.10). By Theorem 3.4.1, $\mathfrak{p}$ has height one and hence is principal by hypothesis; say $\mathfrak{p} = (q)$ for some prime $q \in R$. Now $p = qr$ for some $r \in R$, so by irreducibility of p and primality of q we conclude that r is a unit, whence $\mathfrak{p} = (p)$.

■

Corollary 1.4.4. A PID is a UFD.

Proof. A PID is Noetherian and hence atomic; we are done by Theorem/Definition 1.4.3(c), say. ■

Corollary 1.4.5 (Nagata)**.** Let R be a domain and $S \subset R$ multiplicative. Consider the statements:

(a) The ring R is a UFD.
(b) The localization $S^{-1}R$ is a UFD.

Then (a) $\Rightarrow$ (b), and (b) $\Rightarrow$ (a) if R satisfies the ascending chain condition on principal ideals (e.g. if R is Noetherian) and S is generated by a set of prime elements.

Proof. The implication (a) $\Rightarrow$ (b) is clear; for (b) $\Rightarrow$ (a) under the given conditions, we use Theorem/Definition 1.4.3(g). Let Γ be a generating set for S and $\mathfrak{p} \subset R$ be a 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 $S^{-1}\mathfrak{p} \subset S^{-1}R$ is a prime of height one, so by hypothesis we have $S^{-1}\mathfrak{p} = xS^{-1}R$ for some $x \in \mathfrak{p}$. Look at the collection of ideals $\{(x)\}$ that arise in this way; by Zorn's lemma and the hypothesis on R, this has a maximal element (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 $s = q_1 \cdots q_N$ with $q_j \in \Gamma$, then $p \notin (q_j)$ implies $y \in (q_j)$ for each j. By induction on N, it follows that $y \in (s)$, and so $x \in (p)$. Thus $\mathfrak{p} \subset (p)$ as needed. ■

Let us now look at some important classes of examples of UFDs. The first of these comes from PIDs, which often arise as Euclidean domains.

Definition 1.4.6. A domain R is said to be *Euclidean* if there is some function $d : R \smallsetminus \{0\} \to \mathbf{Z}_{>0}$ such that for all $a, b \in R$ with $b \neq 0$, there are $q, r \in R$ such that

$$a = bq + r$$

and either $r = 0$ or $d(r) < d(b)$.

The function d, called the *Euclidean function*, is not part of the definition, only the existence of such a d is; in general, a Euclidean domain admits many different Euclidean functions. Briefly, a Euclidean domain is a domain in which you can perform Euclid's algorithm.

Example 1.4.7.

(a) For $R = K$ a field, the function $d \equiv 1$ is Euclidean.
(b) For $R = \mathbf{Z}$, the function $d(n) = |n|$ is Euclidean.
(c) For $R = \mathbf{Z}[\mathrm{i}]$ or $R = \mathbf{Z}[\omega]$, the norm function $d(\alpha) = \mathrm{N}(\alpha)$ is Euclidean.
(d) For $R = K[X]$, the polynomial ring over the field K, the function $d(f) = \deg f$ is Euclidean.

(e) For $R = K[\![X]\!]$, the $d(f) = \operatorname{ord}_X f$ taking a power series to the highest power of X dividing it is Euclidean.

Corollary 1.4.8. A Euclidean domain is a PID and hence a UFD.

Proof. This is standard, so we only indicate a sketch, and that too only of the UFD part. If R is Euclidean and d a Euclidean function, then the function $\tilde{d} : R \setminus \{0\} \to \mathbf{Z}_{>0}$ defined by $\tilde{d}(x) = \min_{y \neq 0} d(xy)$ is also Euclidean with the additional property that $\tilde{d}(x) \mid \tilde{d}(y)$ if $x \mid y$; replace d by $\tilde{d}$ to assume this property. Show that if $x, y \in R \setminus \{0\}$, then $d(x) \leq d(xy)$ with equality iff y is a unit, and use this (and the well-ordering principle) to show that R satisfies the ascending chain condition on principal ideals, and is hence atomic. Finally, perform Euclid's algorithm to find the greatest common divisor of any two elements and use Theorem/Definition 1.4.3(f). For details and a slightly different argument, see [2]. Proofs of this result can also be found in any algebra textbook. ■

Remark 1.4.9. Note that there are PIDs which are not Euclidean. Two standard examples are $R = \mathbf{Z}[(1+\sqrt{-19})/2]$ and $R = \mathbf{R}[X,Y]/(X^2+Y^2+1)$; see [2] for proofs of these claims.

We end by relating the unique factorization in a domain R to that in polynomial rings over it.

Corollary 1.4.10. Let R be a ring. The following are equivalent:

(a) R is a UFD.
(b) $R[X]$ is a UFD.
(c) $R[X_1, \ldots, X_n]$ is UFD for any $n \geq 1$.
(d) $R[X_\lambda]_{\lambda \in \Lambda}$ is a UFD for any Λ.
(e) $R[X_\lambda]_{\lambda \in \Lambda}$ is a UFD for some Λ.

Proof. In what follows, let $K := \operatorname{Frac} R$ be the fraction field of R.

(a) $\Rightarrow$ (b) We prove the result when $R[X]$ satisfies the ascending chain condition on principal ideals (e.g. when R is Noetherian, using Theorem 1.3.5); then we can argue as follows.[8] If $S \subset R[X]$ is the set of all non-units in R, then S is a multiplicative subset generated by primes in R, which are primes in $R[X]$ by Exercise 1.12. Since the localization $S^{-1}R[X] = K[X]$ is a PID and hence UFD (Example 1.4.7(d) and Corollary 1.4.8), we are done by Corollary 1.4.5.

(b) $\Rightarrow$ (c) Follows from the previous implication by induction.

(c) $\Rightarrow$ (d) Any element of $R[X_\lambda]_{\lambda \in \Lambda}$ belongs to $R[X_\lambda]_{\lambda \in \Lambda'}$ for some finite $\Lambda' \subset \Lambda$; in particular, any nonzero nonunit in the former admits a factorization into primes in this finite polynomial ring. Since these elements are still prime in $R[X_\lambda]_{\lambda \in \Lambda}$ (Exercise 1.12(b)), we are done by Exercise 1.13(b).

(d) $\Rightarrow$ (e) Clear.

[8] In general, this result is usually proven with the help of Gauss's Lemma. Here's an outline; see Exercise 1.13 for a different proof. Let $K = \operatorname{Frac} R$. An $f \in R[X]$ is said to be *primitive* if $\alpha \in R$ and $\alpha \mid f$ implies $\alpha \in R^\times$. Firstly, any $f \in K[X]$ can be written as λf_0 for some $\lambda \in K$ and primitive $f_0 \in R[X]$; if $0 \neq f$, then λ and f_0 are determined uniquely up to units of R and are called the *content* and *primitive part* of f respectively. Then content and primitive parts are both multiplicative functions (this is Gauss's Lemma), from which it follows that if $f, g \in R[X]$ are nonzero such that $f \mid g$ in $K[X]$ and f is primitive, then $f \mid g$ in $R[X]$. Finally, from this it follows that a primitive $f \in R[X]$ that is prime in $K[X]$ is prime in $R[X]$. Then we are done by Exercise 1.13(b); the unique factorization of an $f \in R[X]$ comes from factoring the content in R and the primitive part into primitives in $K[X]$.

(e) $\Rightarrow$ (a) Note that $R \subset R[X_\lambda]_{\lambda\in\Lambda}$, so if the latter is domain, so is the former. Any nonzero nonunit in R can be factored uniquely into primes in the latter, but this factorization cannot have any elements of positive degree (thanks to Exercise 1.12(a)). Since primes of $R[X_\lambda]_{\lambda\in\Lambda}$ that lie in R are primes of R (Exercise 1.12(b)), we are done by Exercise 1.13(b).

■

It is not true in general that if R is a UFD, then so is $R[\![X]\!]$; see Example 10.5.1. However, if R is a *regular* UFD, then so is $R[\![X]\!]$ (this is Theorem 9.1.2), so that, in particular, rings such as $\mathbf{Z}[\![X_1,\ldots,X_n]\!]$ and $k[\![X_1,\ldots,X_n]\!]$ (where k denotes a field) are UFDs. We will have much to say about unique factorization at the end of the course.

1.5 Cayley-Hamilton Theorem, Nakayama's Lemma, Krull Intersection Theorem

Observation 1.5.1 (Cayley-Hamilton Theorem)**.** Let R be a ring, M be a finitely generated R-module, $\mathfrak{a} \subset R$ an ideal, and $\varphi \in \mathrm{End}_R(M)$ such that $\varphi M \subset \mathfrak{a}M$. Suppose that $M = \sum_{i=1}^n Rx_i$ and write $\varphi(x_j) = \sum_{i=1}^n a_{ij}x_i$ for some $a_{ij} \in \mathfrak{a}$, and let $A := [a_{ij}]$. Then multiplying on the left by the adjoint of the matrix $\varphi I_n - A \in \mathrm{Mat}_n(K[\varphi])$ shows that $\det(\varphi I_n - A)x_i = 0$ for all i. Therefore, φ 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 1.5.2. Let $R \subset S$ be a ring extension and M a finitely generated R-module. Suppose for some $s \in S$ we have that M is also a faithful $R[s]$-module (i.e. with $\mathrm{Ann}_{R[s]} M = 0$), and suppose that $\mathfrak{a} \subset R$ is an ideal with $sM \subset \mathfrak{a}M$. Then $s \in S$ is the root of a monic polynomial equation of the form $s^n + a_1 s^{n-1} + \cdots + a_n = 0$, 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 $s^n + a_1 s^{n-1} + \cdots + a_n \in \mathrm{Ann}_{R[s]} M = 0$. ■

Corollary 1.5.3 (Nakayama's Lemma)**.** Let R be a ring.

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

Proof.

(a) Apply Corollary 1.5.2 to $\varphi = 1$.
(b) Apply (a) and use Proposition/Definition 1.2.6. Alternatively, if $M \neq 0$, then use Lemma 10.1.2 to produce a surjection $\varphi : M \to R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset R$. Since $\mathfrak{a} \subset \mathfrak{m}$, we must have $\mathfrak{a}M \subset \mathfrak{m}M \subset \ker\varphi \subsetneq M$, a contradiction to hypothesis.
(c) Apply (b) to M/N.

■

Corollary 1.5.4. Let $(R, \mathfrak{m}, k)$ be a local ring and M a finitely generated R-module. Then:

(a) 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. In particular, $M/\mathfrak{m}M$ is a finite-dimensional vector space over k.
(b) In the situation of (a), the former is a minimal set of generators of M over R iff the latter is a k-basis of $M/\mathfrak{m}M$. In particular, any two minimal sets of generators for M over R have the same size, namely $\dim_k(M/\mathfrak{m}M)$.
(c) If $\mathfrak{m} \neq 0$ is finitely generated, then $\mathfrak{m}$ is principal iff $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

Proof.

(a) If $x_1, \ldots, x_n \in M$ 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 $N := \sum_{i=1}^n Rx_i \subset M$; by Corollary 1.5.3(c), we conclude that $M = N$, so M is generated by the x_i.
(b) 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

$\{x_1,\dots,x_n\}$ 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.

(c) Take $M=\mathfrak{m}$ in (b).

■

Let us end this section with a few miscellaneous consequences.

Corollary 1.5.5 (Krull Intersection Theorem)**.** Let R be a ring, $\mathfrak{a}\subset R$ be an ideal, and $K_\mathfrak{a} := \bigcap_{N\geq 0}\mathfrak{a}^N$. If R is Noetherian, then $K_\mathfrak{a}=\mathfrak{a}K_\mathfrak{a}$. If, in addition, $1+a$ is not a zero divisor for any $a\in\mathfrak{a}$ (e.g. if $\mathfrak{a}\subset \mathrm{Jac}(R)$ or if R is a domain and $\mathfrak{a}\subset R$ a proper ideal), then $K_\mathfrak{a}=0$.

The ideal $K_\mathfrak{a}$ is the kernel of the completion map $R\to\hat{R}_\mathfrak{a}$ (see §**??**), so that if $K_\mathfrak{a}=0$ then R embeds into its $\mathfrak{a}$-adic completion. This result gives us conditions for when this happens; for instance, this always happens for a Noetherian local ring R with maximal ideal $\mathfrak{a}=\mathfrak{m}$.

Proof. The second statement follows immediately from the first and Corollary 1.5.3(a). For the first statement, let $\mathfrak{a}=(a_1,\dots,a_n)$ and let $b\in K_\mathfrak{a}$. For each $N\geq 1$, there is a polynomial $p_N\in R[X_1,\dots,X_n]$ such that p_N is homogeneous of degree N and $b=p_N(a_1,\dots,a_n)=:p_N(a)$. Since the ring $R[X_1,\dots,X_n]$ is Noetherian (Theorem 1.3.5), there is an integer $N\geq 1$ and polynomials $q_1,\dots,q_N\in R[X_1,\dots,X_n]$ such that each q_j is homogeneous of degree j and $p_{N+1}=q_Np_1+\cdots+q_1p_N$. Then

$$b=p_{N+1}(a)=(q_N(a)+\cdots+q_1(a))\,b\in\mathfrak{a}K_\mathfrak{a}.$$

■

This elementary proof is due to Perdry [3]. The hypothesis on I in the second half of the statement cannot be easily strengthened: if $R=\mathbf{Q}\times\mathbf{Q}$ and $I=\mathbf{Q}\times 0$, then R is Noetherian (Example 1.3.2(c)) but $I^2=I$ and so $K_I=I\neq 0$, and there is a non-Noetherian domain with a proper ideal $I\subset R$ such that $K_I\neq 0$ (Example 10.5.4). This result is also an immediate consequence of the Artin-Rees Lemma (Lemma **??**).

Corollary 1.5.6. Every surjective endomorphism of a finitely generated module is an isomorphism.

Proof. Specifying an endomorphism φ of an R-module M is the same as specifying a $R[X]$-module structure lifting the R-module structure on M (where X acts by φ). If φ is surjective, then $M=\mathfrak{a}M$ with $\mathfrak{a}=(X)\subset R[X]$. By Nakayama's Lemma (Corollary 1.5.3(a)), there is an $a\in\mathfrak{a}$ such that $(1+a)M=0$. Now if $m\in M$ is 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 $\varphi(m)=0$. ■

Counterexample 1.5.7. Corollary 1.5.6 is false if we replace "surjective" by "injective": take $\mathbf{Z}\xrightarrow{2}\mathbf{Z}$. See also Exercise 1.11.

Corollary 1.5.8. Let R be a ring and M,N be a finitely generated R-modules. If $M\otimes_R N=0$, then $\mathrm{Ann}_R(M)+\mathrm{Ann}_R(N)=R$. In particular, if R is local, then either $M=0$ or $N=0$.

Proof. First suppose that $(R,\mathfrak{m},k)$ is local and $M\neq 0$ but $M\otimes_R N=0$. Then $M/\mathfrak{m}M\neq 0$ by Nakayama and so there is 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 $N=0$. In general, if $\mathrm{Ann}_R(M)+\mathrm{Ann}_R(N)$ is contained in some prime $\mathfrak{p}$, 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 first part 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 some $u_i \in R \setminus \mathfrak{p}$ with $u_i x_i = 0$. Then $u = \prod_i u_i \in \mathrm{Ann}_R(M) \setminus \mathfrak{p}$, a contradiction. ■

Remark 1.5.9. Geometrically, Corollary 1.5.8 asserts that the support of the tensor product $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ of two coherent $\mathcal{O}_X$-modules $\mathcal{F}, \mathcal{G}$ on a locally Noetherian scheme X is exactly the intersection of the supports of $\mathcal{F}$ and $\mathcal{G}$.

1.6 Gradings, Filtrations and All That

Just as affine algebraic geometry deals with ideals in rings, *projective algebraic geometry* deals with homogeneous ideals in graded rings.

Definition 1.6.1. Let I be a monoid.

(a) An *I-graded ring* S is a ring together with a family of additive subgroups S_i indexed by $i \in I$ such that $S = \bigoplus_{i\in I} S_i$ and for all $i, j \in I$ we have $S_i S_j \subset S_{i+j}$.
(b) If S is an I-graded ring, then a *graded module* over S is an S-module M with a family of submodules M_i indexed by $i \in I$ such that $M = \bigoplus_{i\in I} M_i$ and for all $i, j \in I$ we have $S_i M_j \subset M_{i+j}$.
(c) If S is an I-graded ring and M a graded S-module, then the *twist* of M by $i \in I$ is the graded S-module $M(i)$ defined by $M(i)_j := M_{i+j}$.

Similarly, given a base ring k, it is easy to guess the definition of an I-graded k-algebra. Given an I-graded ring S, the submodule $S_0 \subset S$ is a ring, each S_i a module over S_0, and S is naturally a graded S_0-algebra. Similarly, if M is a graded S-module, then each M_i is an S_0-submodule of M. Given an I-graded ring S and a graded S-module M, for each $i \in I$, a nonzero element $m \in M_i$ is said to be *homogeneous of degree i*. Every element $m \in M$ can be uniquely decomposed into its homogeneous components.

Proposition/Definition 1.6.2. Let I be a monoid, S an I-graded ring, and M a graded S-module. The following conditions on an S-submodule N of M are equivalent:

(a) For an $m \in M$, we have $m \in N$ iff each homogeneous component m_i of m is in N.
(b) The submodule N is generated over S by homogeneous elements of M.
(c) The natural map $\bigoplus_{i\in I} N \cap M_i \to N$ is an isomorphism.

In this case, we say that N is a *homogeneous submodule* of M.

The proof of the equivalence of the above conditions is fairly clear; details are left to the reader. In the above setting, if $N \subset M$ is a homogeneous submodule, then N is itself a graded S-module with grading $N_i := N \cap M_i$. In this case, the quotient $M/n = \bigoplus_{i\in I} M_i/N_i$ is also a graded S-module.

Example 1.6.3.

(a) If V be a finite-dimensional vector space over a field k, then the *symmetric aglebra*

$$\mathrm{Sym}^* V^\vee := \bigoplus_{d\geq 0} \mathrm{Sym}^d V^\vee$$

is an $\mathbf{N}$-graded k-algebra. If V has dimension $n+1 \geq 1$, then choosing a basis for V gives an isomorphism between $\mathrm{Sym}^* V^\vee$ and the polynomial ring $k[X_0, X_1, \ldots, X_n]$ which is also clearly $\mathbf{N}$-graded. If k is a field of characteristic two, then the exterior algebra $\Lambda^* V^\vee$ is also an $\mathbf{N}$-graded k-algebra.
(b) Given homogeneous polynomials $F_1, \ldots, F_r \in k[X_0, \ldots, X_n]$, the quotient ring

$$S := k[X_0, \ldots, X_n]/(F_1, \ldots, F_r)$$

is an $\mathbf{N}$-graded k-algebra; this is the *homogeneous coordinate ring of the projective variety V defined by the vanishing of the F_i, i.e. $V = \mathbf{V}(F_1, \ldots, F_r) \subset \mathbf{P}^n_k$.*

Example 1.6.4. Let R be a ring and $\mathfrak{a} \subset R$ be an ideal.

(a) The *Rees algebra* or *blowup* of R along $\mathfrak{a}$ is the graded R-algebra $\mathrm{Bl}_{\mathfrak{a}}(R) := \bigoplus_{n\geq 0} \mathfrak{a}^n$.
(b) The *associated graded ring* to R and $\mathfrak{a}$ is defined to be $\mathrm{gr}_{\mathfrak{a}}(R) := \bigoplus_{n\geq 0} \mathfrak{a}^n/\mathfrak{a}^{n+1}$. If $\mathfrak{a} = (a_1, \ldots, a_r)$, then $\overline{a}_1, \ldots, \overline{a}_r \in \mathfrak{a}/\mathfrak{a}^2 = \mathrm{gr}_{\mathfrak{a}}(R)_1$ generate $\mathrm{gr}_{\mathfrak{a}}(R)$ over $\mathrm{gr}_{\mathfrak{a}}(R)_0 = R/\mathfrak{a}$.
(c) If M is an R-module, then the *associated graded module* to M and $\mathfrak{a}$ is defined by $\mathrm{gr}_{\mathfrak{a}}(M) := \bigoplus_{n\geq 0} \mathfrak{a}^n M/\mathfrak{a}^{n+1}M$. This is a graded $\mathrm{gr}_{\mathfrak{a}}(R)$-module.

Note that if R is a Noetherian ring, then for any ideal $\mathfrak{a} \subset R$, the blowup $\mathrm{Bl}_{\mathfrak{a}}(R)$ is a Noetherian ring; this follows from the next lemma.

Lemma 1.6.5. The following conditions on an $\mathbf{N}$-graded ring S are equivalent:

(a) S is a Noetherian ring.
(b) S_0 is a Noetherian ring and the ideal $S_+ := \bigoplus_{i\geq 1} S_i \subset S$ is a finitely generated.
(c) S_0 is a Noetherian ring and S is a finitely generated S_0-algebra.

Proof. ■

1.6.1 Hilbert Functions and Polynomials

Definition 1.6.6. Let R, S be rings and $f : R \to S$ a function. For each $k \geq 1$, we recursively define the k^{th} finite difference function of f denoted $\Delta^{[k]} f : R \to S$ by

$$\Delta^{[1]} f(r) := f(r+1) - f(r) \text{ and } \Delta^{[k]} f := \Delta^{[1]}(\Delta^{[k-1]} f) \text{ for } k \geq 2.$$

It is inductively clear that for any $k \geq 1$ we have $\Delta^{[k]}(f)(r) := \sum_{i=0}^{k} (-1)^{i-1} \binom{k}{i} f(r+i)$.
If R i

1.6.2 Completion and the Artin-Rees Lemma

1.7 Exercises

Exercise 1.1. Let R be a ring and $S, T \subset R$ be multiplicative subsets such that $S \subset T$. The universal property of localizations gives us homomorphisms $S^{-1}R \to T^{-1}R$ and $S^{-1}M \to T^{-1}M$ for any module M. Show that the kernel of $S^{-1}R \to T^{-1}R$ is

$$\{s^{-1}r \in S^{-1}R : tr = 0 \text{ for some } t \in T\}.$$

Exercise 1.2. Show that if R and S are rings, then $\mathrm{Quot}(R \times S) \cong \mathrm{Quot}(R) \times \mathrm{Quot}(S)$. Conclude that $\mathrm{Quot}(\mathbf{Z} \times \mathbf{Z}) \cong \mathbf{Q} \times \mathbf{Q}$. Does the same result also hold for arbitrary (possibly infinite) products of rings?

Exercise 1.3. Show that the following conditions on a ring R are equivalent.

(a) The underlying abelian group of R is torsion-free. In other words, if $\varepsilon \in R$ is such that for some $n \in \mathbf{Z}_{\geq 1}$, we have $n\varepsilon = 0$, then $\varepsilon = 0$.
(b) The natural map $R \to \mathbf{Q} \otimes_{\mathbf{Z}} R$ is injective.
(c) There is a $\mathbf{Q}$-algebra K and a ring monomorphism $R \to K$.

A ring satisfying these equivalent conditions is called *torsion-free*.

Exercise 1.4. Let R be a ring and $S \subset R$ a multiplicative subset. Show that if M is an R-module and $N \subset M$ an R-submodule, then for any $x \in M$, the following are equivalent.

(a) $x \in N$.
(b) $[x] \in S^{-1}N$ for every multiplicative $S \subset R$.
(c) $[x] \in N_{\mathfrak{p}}$ for all $\mathfrak{p}$.
(d) $[x] \in N_{\mathfrak{m}}$ for all $\mathfrak{m}$.

Exercise 1.5. Let $\mathfrak{a}, \mathfrak{b} \subset R$ be two ideals of the ring R. Consider the following conditions:

(a) Every prime containing $\mathfrak{a}$ also contains $\mathfrak{b}$, i.e. $\mathbf{V}(\mathfrak{a}) \subset \mathbf{V}(\mathfrak{b})$.
(b) We have $\mathfrak{b} \subset \sqrt{\mathfrak{a}}$.
(c) There is an $N \gg 1$ such that $\mathfrak{b}^N \subset \mathfrak{a}$.

Show that (a) and (b) are equivalent and implied by (c), and that (c) is equivalent to (a) and (b) if $\mathfrak{b}$ is finitely generated (e.g. if R is Noetherian).

Exercise 1.6. Let R be a ring. Show that:

(a) If $S \subset R$ a multiplicative subset, then $\mathrm{Nil}(S^{-1}R) = S^{-1}\mathrm{Nil}(R) = \mathrm{Nil}(R) \cdot S^{-1}R$.
(b) The following are equivalent:
  (i) R is reduced.
  (ii) $S^{-1}R$ is reduced for each multiplicative $S \subset R$.
  (iii) $R_{\mathfrak{p}}$ is reduced for each $\mathfrak{p}$.
  (iv) $R_{\mathfrak{m}}$ is reduced for each $\mathfrak{m}$.

Exercise 1.7.

(a) Suppose that k is an infinite field, V a k-vector space, n a positive integer, and $U, V_1, \ldots, V_n \subset V$ subspaces. Show that if $U \subset \bigcup_{i=1}^{n} V_i$, then there is an i with $1 \leq i \leq n$ such that $U \subset V_i$. In particular, a vector space over k cannot be a finite union of proper subspaces.
(b) Show by example that the statement in (a) is false if we do not require k to be infinite.

Exercise 1.8. Show that if R is a ring and $\mathfrak{m} \subset R$ a maximal ideal, then for each integer $n \geq 1$, the quotient ring $R/\mathfrak{m}^n$ is a local ring. What is the unique maximal ideal of $R/\mathfrak{m}^n$?

Exercise 1.9. For any natural number N, let $\mathbf{Z}\langle 1/N\rangle := \{q \in \mathbf{Q} : Nq \in \mathbf{Z}\} \subset \mathbf{Q}$ be the abelian subgroup of $\mathbf{Q}$ generated by $1/N$, so that for any natural number n, we have a chain of additive subgroups

$$\mathbf{Z} \subset \mathbf{Z}\langle 1/n\rangle \subset \mathbf{Z}\langle 1/n^2\rangle \subset \cdots \subset \mathbf{Z}[1/n] \subset \mathbf{Q}.$$

Show that if $n = p$ is prime, then these are all the subgroups of (the underlying additive subgroup of) the ring $\mathbf{Z}[1/n]$ which contain $\mathbf{Z}$. Conclude that the $\mathbf{Z}$-module $\mathbf{Z}[1/p]/\mathbf{Z}$ is Artinian but not Noetherian. What happens when n is not prime?

Exercise 1.10. A ring R is said to be *strongly associate* if the following holds: if $r,s \in R$ are such that $(r) = (s)$ (i.e. the principal ideals generated by r and s are the same), then there is a unit $u \in R^\times$ such that $r = us$. Show that domains, local rings, principal ideal rings, and Artinian rings are strongly associate. Find a ring that is not strongly associate.

Exercise 1.11.

(a) ([4, Exercise 6.1]) Let M be a Noetherian (resp. Artinian) module, and $\varphi : M \to M$ an endomorphism. Show that if φ is surjective (resp. injective), then φ is an isomorphism.
(b) (Ross) Prove or disprove and salvage if possible: if R is a ring, then $R \ncong R[X]$ as rings.

Exercise 1.12. Let R be a ring.

(a) Show that R is a domain iff the polynomial ring $R[X]$ is, and in this case (and only in this case) the degree function $\deg : R[X] \to \mathbf{Z}_{\geq 0} \cup \{-\infty\}$ is additive (i.e., satisfies $\deg(fg) = \deg(f) + \deg(g)$ for $f,g \in R[X]$).
(b) Show that given a $p \in R$, this p is a prime element in R iff it is a prime element in $R[X]$.

Generalize to an arbitrary number of variables.

Exercise 1.13. Show that the following conditions on a domain are equivalent:

(a) The domain is a UFD.
(b) Every nonzero nonunit is a finite product of *prime* elements.
(c) (Kaplansky) Every nonzero prime ideal contains a prime element.

Use Kaplansky's criterion (c) to give alternative proofs of Corollary 1.4.5 and Corollary 1.4.10.

Exercise 1.14.

(a) Prove or disprove and salvage if possible: If R is a UFD and $\mathfrak{a} \subset R$ an ideal, then $R/\mathfrak{a}$ is a UFD. Do the same for when $R = K[X_1,\ldots,X_n]$ for some field K and $\mathfrak{a} = (f)$ is principal.
(b) (Klein-Nagata) Fix an $n \geq 1$ and let $R := \mathbf{C}[X_1,\ldots,X_n]$ and $f := X_1^2 + \cdots + X_n^2$. Then $R/(f)$ is a UFD if $n \geq 5$. What happens when $1 \leq n \leq 4$?
(c) (Samuel) Let K be any field, $R = K[X,Y,Z]$ and $f = X^2 + Y^3 + Z^7$. Then $R/(f)$ is a UFD.

Chapter 2

Derivations

2.1 Derivations and Kähler Differentials

Definition 2.1.1. Suppose R is a ring, S an R-algebra, and M an S-module. 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 for all $f, g \in S$ we have

$$D(fg) = f \cdot Dg + g \cdot Df.$$

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

Remark 2.1.2.

(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 2.1.3 (Basic Properties of Derivations)**.**

(a) If $e \in S$ is an idempotent, 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, $\mathrm{Der}_R(S,M) \subset \mathrm{Der}(S,M)$ 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

$$D(f^n) = nf^{n-1}Df.$$

If, $M = S$, then we also have

$$D^n(fg) = \sum_{i=0}^{n} \binom{n}{i} D^i f \cdot D^{n-i} g.$$

(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 $D \in \mathrm{Der}_R(S)$ then $D^p \in \mathrm{Der}_R(S)$ too.

Proof.

(a) This follows from $D(e) = D(e^2) = 2e \cdot D(e) \Rightarrow (2e-1)D(e) = 0 \Rightarrow D(e) = (2e-1)^2 D(e) = 0$.

(b) If D is R-linear, then $D(r) = D(r \cdot 1) = r \cdot D(1) = 0$; the converse follows from the Liebniz Rule.

(c) Clear by induction on n.
(c) Clear from (d).

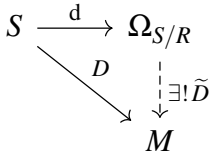
■

Example 2.1.4. If $S = R[X_\lambda]_{\lambda\in\Lambda}$ is the polynomial ring, then a derivation $D \in \mathrm{Der}_R(S,M)$ is completely determined by the family $D(X)_\lambda \in M$, since by the Leibniz rule we have for $F \in S$ that

$$DF = \sum_\lambda \frac{\partial F}{\partial X_\lambda} DX_\lambda,$$

where $\partial F/\partial X_\lambda$ is the usual formal derivative of F with respect to X_λ. In particular, we have $\mathrm{Der}_R(S) \cong \bigoplus_\lambda S\langle \mathrm{d}X_\lambda\rangle$ is the free S-module on the symbols $\mathrm{d}X_\lambda$ for $\lambda \in \Lambda$, and $\mathrm{Der}_R(S,M) \cong \mathrm{Der}_R(S)\otimes_S M$ for any S-module M.

Theorem 2.1.5 (Kähler Differentials)**.** The functor $\mathrm{Der}_R(S,-) : S\text{-Mod} \to S\text{-Mod}$ 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:



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

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

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

$$-\mathrm{d}(fg) + f\,\mathrm{d}g + g\,\mathrm{d}f \text{ and } -\mathrm{d}(rf+sg) + r\,\mathrm{d}f + s\,\mathrm{d}g,$$

for all $f,g \in S$ and $r,s \in R$. The quotient $\Omega_{S/R}$ along with the map $\mathrm{d} : S \to \Omega_{S/R} : f \mapsto [\mathrm{d}f]$ satisfies the universal property.

(b) Firstly, define $\mu : S\otimes_R S \to S$ by $\mu(f\otimes g) := fg$; then μ 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 $f \mapsto 1\otimes f - f\otimes 1 \pmod{I^2}$.[1] Now given an R-derivation $D : S \to M$, we get an R-module homomorphism $\delta : S\otimes_R S \to M$ given on pure tensors by $f\otimes g \mapsto f\cdot Dg$. This satisfies the property that for $x,y \in S\otimes_R S$ we have

$$\delta(xy) = \mu(x)\delta(y) + \mu(y)\delta(x),$$

[1] Note that $S\otimes_R S/I \cong S$ and the S-module structure on $\Omega_{S/R}$ comes from noting that it (being a quotient of I) is an $S\otimes_R S$-module annihilated by I, and hence an $S\otimes_R S/I \cong S$-module; equivalently, S-module structure on $\Omega_{S/R}$ given by multiplication on either the right or the left is the same.

and so vanishes on I^2. From this we get the map $\tilde{D} : \Omega_{S/R} \to M$, which is easily seen to be an S-module homomorphism with $\tilde{D} \circ d = D$. Finally, since for $f \otimes g \in S \otimes_R S$ we have

$$f \otimes g = (f \otimes 1)(1 \otimes g - g \otimes 1) + fg \otimes 1,$$

it follows that if $x = \sum_i f_i \otimes g_i \in I$ then $x \equiv \sum_i f_i \mathrm{d}g_i \pmod{I^2}$, so that $\Omega_{S/R}$ is generated as an S-module by the $\mathrm{d}s$, showing uniqueness of $\tilde{D}$.

■

Remark 2.1.6. 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.

To define it we simply set $\mathrm{d}'(b/s) = (1/s)\mathrm{d}b - (1/s^2)b\mathrm{d}s$. To see that this is well-defined, note that if $b/s = b'/s'$ in $S^{-1}B$, then there is a $t \in S$ such that $t(s'b - b's) = 0$. Differentiating $t^2(s'b - b's) = 0$ and using the Leibniz Rule then yields that $t^2(s'\mathrm{d}b + b\mathrm{d}s' - b'\mathrm{d}s - s\mathrm{d}b') = 0$. Therefore,

$$\begin{aligned}
&t^2\left(s^2(s'\mathrm{d}b' - b'\mathrm{d}s') - (s')^2(s\mathrm{d}b - b\mathrm{d}s)\right)\\
=&t^2\left(ss'(s\mathrm{d}b' - s'\mathrm{d}b) - (s^2b'\mathrm{d}s' - (s')^2b\mathrm{d}s)\right)\\
=&t^2\left(ss'(b\mathrm{d}s' - b'\mathrm{d}s) - (s^2b'\mathrm{d}s' - (s')^2b\mathrm{d}s)\right)\\
=&t^2(s'b - b's)(s'\mathrm{d}s' + s'\mathrm{d}s) = 0,
\end{aligned}$$

whence $\mathrm{d}'(b/s) = \mathrm{d}'(b'/s')$. The linearity of d' and the Leibniz Rule follow immediately from it being well-defined and the corresponding properties of d. Finally, d' evidently vanishes on A because d does, and hence defines an A-derivation, finishing the proof.

2.2 Fundamental Exact Sequences

2.3 Smoothness

Chapter 3

Primary Decomposition

In this chapter, we discuss the fundamentals of associated primes and primary decomposition in the Noetherian setting. We prove the Lasker-Noether Theorem, and end with a few applications to Artinian rings and to Krull's Hauptidealsatz.

3.1 Associated Primes

Definition 3.1.1. Let R be a ring and M an R-module.

(a) A prime $\mathfrak{p} \subset R$ of R is said to be *associated to* M if the following equivalent conditions hold:
  (i) There is a nonzero $m \in M$ such that $\mathfrak{p} = \operatorname{Ann}(m)$.
  (ii) There is an injection of R-modules $R/\mathfrak{p} \hookrightarrow M$.

The set of all primes associated to M is denoted by $\operatorname{Ass}_R(M)$.

(b) The minimal elements of $\operatorname{Ass}_R(M)$ are called *isolated*, and the others are called *embedded* primes.
(c) A $\mathfrak{p} \subset R$ is said to be *associated to an ideal* $\mathfrak{a} \subset R$ if it is associated to the R-module $R/\mathfrak{a}$.

Note that the only prime associated to a prime ideal $\mathfrak{p} \subset R$ is $\mathfrak{p}$ itself, i.e. $\operatorname{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$. We let $\mathscr{Z}(M) := \bigcup_{0 \neq m \in R} \operatorname{Ann}(m)$ be the set of zero-divisors of M in R; then clearly $\bigcup \operatorname{Ass}_R(M) \subset \mathscr{Z}(M)$. Here are some generalities on associated primes.

Lemma 3.1.2. Let R be a ring and M an R-module.

(a) If $\mathscr{A}$ is the collection of ideals of R of the form $\operatorname{Ann}(m)$ for nonzero $m \in M$, then any maximal element of $\mathscr{A}$ is prime.
(b) There is an inclusion $\operatorname{Ass}_R(M) \subset \operatorname{Supp}(M) \subset \mathbf{V}(\operatorname{Ann} M)$, and equality holds in the latter if M is finitely generated.[1]
(c) If $S \subset R$ is a multiplicative subset, then $\operatorname{Ass}_{S^{-1}R}(S^{-1}M) \supset \operatorname{Ass}_R(M) \cap \operatorname{Spec} S^{-1}R$.
(d) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence, then

$$\operatorname{Ass}_R(M') \subset \operatorname{Ass}_R(M) \subset \operatorname{Ass}_R(M') \cup \operatorname{Ass}_R(M'').$$

Proof.

(a) Suppose $\mathfrak{a} = \operatorname{Ann}(m) \in \mathscr{A}$ is maximal and $x, y \in R$ are such that $xy \in \mathfrak{a}$ but $y \notin \mathfrak{a}$. Then $ym \neq 0$ and $\operatorname{Ann}(m) \subset \operatorname{Ann}(ym)$, so by maximality $\operatorname{Ann}(ym) = \operatorname{Ann}(m) = \mathfrak{a}$, whence $xym = 0$ implies $x \in \mathfrak{a}$.
(b) If $\mathfrak{p} = \operatorname{Ann}(m)$ for some nonzero $m \in M$, then $[m] \in M_{\mathfrak{p}}$ is nonzero. Equivalently, since $R/\mathfrak{p} \hookrightarrow M$ and $R_{\mathfrak{p}}$ is flat over R, we have $\kappa(\mathfrak{p}) = R_{\mathfrak{p}} \otimes_R R/\mathfrak{p} \hookrightarrow R_{\mathfrak{p}} \otimes_R M = M_{\mathfrak{p}}$, and $\kappa(\mathfrak{p})$ is a field. For the second part, the inclusion $\operatorname{Supp}(M) \subset \mathbf{V}(\operatorname{Ann} M)$ is clear; for the other, suppose that M is finitely generated and $\mathfrak{p} \in \mathbf{V}(\operatorname{Ann} M)$ but $M_{\mathfrak{p}} = 0$. Then for each of the finitely many generators m_i of M, there is an $s_i \in R \smallsetminus \mathfrak{p}$ such that $s_i m_i = 0$, and then $\prod_i s_i \in \operatorname{Ann}(M) \smallsetminus \mathfrak{p}$ is a contradiction.
(c) We show that if $\mathfrak{p} = \operatorname{Ann}(m)$ for some $0 \neq m \in M$ and $\mathfrak{p} \cap S = \emptyset$, then $S^{-1}\mathfrak{p} = \operatorname{Ann}([m])$ for $0 \neq [m] \in S^{-1}M$. The inclusion $S^{-1}\mathfrak{p} \subset \operatorname{Ann}([m])$ is clear. For the converse, suppose that $(s^{-1}x)[m] = 0$ for some $s \in S$ and $x \in R$; then $txm = 0$ for some $t \in S$. Since $t \notin \mathfrak{p}$ but $tx \in \mathfrak{p}$, we must have $x \in \mathfrak{p}$.
(d) The first inclusion is clear. For the second, if $\mathfrak{p} \in \operatorname{Ass}_R(M) \smallsetminus \operatorname{Ass}_R(M')$, then there is an $m \in M \smallsetminus M'$ such that $\mathfrak{p} = \operatorname{Ann}(m)$, and then we claim that $\mathfrak{p} = \operatorname{Ann}([m])$ for $0 \neq [m] \in M''$. The inclusion $\mathfrak{p} \subset \operatorname{Ann}([m])$ is clear; conversely, if $x \in \operatorname{Ann}([m]) \smallsetminus \mathfrak{p}$, then $xm \in M'$ and $\mathfrak{p} = \operatorname{Ann}(xm) \in \operatorname{Ass}_R(M')$, a contradiction to hypothesis.

[1] Recall that $\operatorname{Supp}(M)$ is the set of primes $\mathfrak{p} \subset R$ such that $M_{\mathfrak{p}} \neq 0$. Equivalently, $\operatorname{Supp}(M) \subset \operatorname{Spec} R$ is the support of the quasicoherent sheaf $\tilde{M}$ on the affine scheme $\operatorname{Spec} R$.

■

In (c), we are of course identifying $\operatorname{Spec} S^{-1}R$ with a subset of $\operatorname{Spec} R$ via Corollary 1.1.12(d).

Remark 3.1.3. In Lemma 3.1.2(b), the hypothesis of finite generation is necessary for equality to hold in the second inclusion. A simple counterexample otherwise is given by taking $R = \mathbf{Z}$ and $M = \bigoplus_p \mathbf{Z}/p$, where the sum is over all primes $p \in \mathbf{Z}$. Then $\operatorname{Ann} M = 0$ and $(0) \in \mathbf{V}(\operatorname{Ann} M) \smallsetminus \operatorname{Supp}(M)$ because $E_{(0)} = E \otimes_{\mathbf{Z}} \mathbf{Q} = 0$.

The notion of associated primes behaves best in the Noetherian setting.

Theorem 3.1.4. Let R be a Noetherian ring and M a nonzero finitely generated R-module.

(a) The set $\operatorname{Ass}_R(M)$ is nonempty and finite.
(b) The map $M \to \prod_{\mathfrak{p} \in \operatorname{Ass}_R(M)} M_{\mathfrak{p}}$ is injective.
(c) We have $\bigcup \operatorname{Ass}_R(M) = \mathscr{Z}(M)$. In particular, if $\mathfrak{a} \subset R$ is any ideal, then either $\mathfrak{a}$ contains a nonzerodivisor of M, or $\mathfrak{a} \subset \operatorname{Ann}(m)$ for some $0 \neq m \in M$.
(d) Equality holds in Lemma 3.1.2(c).
(e) The sets of minimal elements of $\operatorname{Ass}_R(M)$ and $\operatorname{Supp}(M) = \mathbf{V}(\operatorname{Ann} M)$ coincide.

Part (e) says that the isolated primes associated to M are exactly the minimal elements in (e.g. irreducible components in) the support of M. If R is not Noetherian, then it is possible that $\operatorname{Ass}_R(M)$ is empty for nonzero M; see Example 10.5.6.

Proof.

(a) That $\operatorname{Ass}_R(M)$ is nonempty is immediate from Lemma 3.1.2(a) and the Noetherian hypothesis. For the finiteness, we show that there is an integer $n \geq 1$ and sequence of submodules $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ with each successive quotient of the form $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i \subset R$; then by Lemma 3.1.2(d), it would follow that $\operatorname{Ass}_R(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. To show this, note that since $\operatorname{Ass}_R(M)$ is nonempty, there is a prime $\mathfrak{p}_1$ and an injection $R/\mathfrak{p}_1 \hookrightarrow M$. Take M_1 to be the image of this map. If $M_1 = M$ we are done; else apply this procedure to M/M_1 and continue recursively. Since M is Noetherian, this procedure must eventually terminate.
(b) If the kernel is nonzero, then by (a) it has an associated prime, which is then associated to M as well (by Lemma 3.1.2(d)). This gives us an element $0 \neq m \in M$ with $\mathfrak{p} = \operatorname{Ann}(m)$ but $[m] = 0 \in M_{\mathfrak{p}}$, which can't happen.
(c) As noted above, the inclusion $\bigcup \operatorname{Ass}_R(M) \subset \mathscr{Z}(M)$ holds unconditionally. Conversely, if $r \in \mathscr{Z}(M)$ then $r \in \operatorname{Ann}(m)$ for some $0 \neq m \in M$. Then the submodule $Rm \subset M$ is nonzero, so in the Noetherian case it has an associated prime $\mathfrak{p}$ by (a), i.e. there is an $s \in R$ such that $\mathfrak{p} = \operatorname{Ann}(sm)$. Then $\mathfrak{p}$ is also associated to M (Lemma 3.1.2(d)) and

$$r \in \operatorname{Ann}(m) \subset \operatorname{Ann}(sm) = \mathfrak{p} \subset \bigcup \operatorname{Ass}_R(M).$$

The second statement follows from the first along with (a) and prime avoidance (Lemma 1.2.12(b)).
(d) Let $\mathfrak{p} \in \operatorname{Ass}_{S^{-1}R}(S^{-1}M) \subset \operatorname{Spec} S^{-1}R \subset \operatorname{Spec} R$, so there are $s \in S, m \in M$ with $S^{-1}\mathfrak{p} = \operatorname{Ann}(s^{-1}m)$. Clearly, $\operatorname{Ann}(m) \subset \mathfrak{p}$ and for each $x \in \mathfrak{p}$, there is a $t \in S$ such that $tx \in \operatorname{Ann}(m)$. By the Noetherian hypothesis, if $x_1, \ldots, x_n$ are generators for $\mathfrak{p}$ and $t_1, \ldots, t_n$ as mentioned, then it is easy to see that $\mathfrak{p} = \operatorname{Ann}(tm)$ for $t = \prod_{i=1}^n t_i$.

(e) For any prime $\mathfrak{p} \subset R$, by (d), the set $\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) = \mathrm{Ass}_R(M) \cap \mathrm{Spec}\, R_\mathfrak{p}$ consists of primes $\mathfrak{q} \in \mathrm{Ass}_R(M) \subset \mathrm{Supp}(M)$ contained in $\mathfrak{p}$. Therefore, if $\mathfrak{p} \in \mathrm{Supp}(M)$ is a minimal element, then either $\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) = \emptyset$ or $\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) = \{\mathfrak{p}\}$, and the former cannot hold thanks to (a).

■

3.2 Primary Decomposition, Lasker-Noether Theorem

Proposition/Definition 3.2.1 (Primary Submodules)**.** Let R be a ring, M an R-module and $N \subsetneq M$ a proper submodule. Consider the following conditions.

(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 $x^n M \subset N$.
(b) We have $\mathscr{Z}(M/N) \subset \sqrt{\text{Ann}(M/N)}$.
(c) The ideal $\sqrt{\text{Ann}(M/N)}$ is prime and either $\text{Ass}_R(M/N) = \emptyset$ or $\text{Ass}_R(M/N) = \{\sqrt{\text{Ann}(M/N)}\}$.
(d) There is a unique prime associated to M/N.

Then (a) $\Leftrightarrow$ (b) $\Rightarrow$ (c). Further, if R is Noetherian and M finitely generated, then all conditions are equivalent. A submodule $N \subset M$ is said to be *primary* if it is proper and satisfies the equivalent conditions (a) and (b). If $\mathfrak{p} := \sqrt{\text{Ann}(M/N)}$, then we say that N is *primary to prime* $\mathfrak{p}$ or simply $\mathfrak{p}$-primary.

Proof.

(a) $\Leftrightarrow$ (b) Clear.
(b) $\Rightarrow$ (c) Let $x, y \in R$ and $n \geq 1$ be such that $(xy)^n \in \text{Ann}(M/N)$. If $y \notin \sqrt{\text{Ann}(M/N)}$, then there is an $m \in M$ such that $y^n m \notin N$. By (a) we conclude that $x^n \in \sqrt{\text{Ann}(M/N)}$, whence $x \in \sqrt{\text{Ann}(M/N)}$. Now suppose $\mathfrak{p} \in \text{Ass}_R(M/N)$; then by Lemma 3.1.2(b) we have

$$\sqrt{\text{Ann}(M/N)} \subset \mathfrak{p} \subset \bigcup \text{Ass}_R(M/N) \subset \mathscr{Z}(M/N) \subset \sqrt{\text{Ann}(M/N)}.$$

Now suppose that R is Noetherian and M finitely generated.

(c) $\Rightarrow$ (d) Clear from Theorem 3.1.4(a).
(d) $\Rightarrow$ (b) Suppose $\text{Ass}_R(M/N) = \{\mathfrak{p}\}$. By Theorem 3.1.4(c) we have $\mathscr{Z}(M/N) = \mathfrak{p}$. By Theorem 1.2.2, it suffices to show that if $\mathfrak{q}$ is a prime containing $\text{Ann}(M/N)$, then $\mathfrak{q} \supset \mathfrak{p}$. By Lemma 1.2.10, $\mathfrak{q}$ contains a minimal prime over $\text{Ann}(M/N)$, but by Theorem 3.1.4(e), this minimal prime is $\mathfrak{p}$.

■

Note that the above proof shows that if $N \subset M$ is a primary submodule and $\text{Ass}_R(M/N)$ is nonempty (e.g. if R is Noetherian and M finitely generated), then $\mathscr{Z}(M/N) = \sqrt{\text{Ann}(M/N)}$. In the special case of $M = R$, primary *ideals* are the primary objects of study.

Lemma 3.2.2 (Primary Ideals)**.** Let R be a ring.

(a) A proper ideal $\mathfrak{a} \subset R$ is primary iff every zero divisor in $R/\mathfrak{a}$ is nilpotent, so primes are primary.
(b) If $\mathfrak{a} \subset R$ is primary then $\sqrt{\mathfrak{a}}$ is the unique minimal prime containing $\mathfrak{a}$ and $\mathfrak{a}$ is $\sqrt{\mathfrak{a}}$-primary.
(c) If $\mathfrak{a} \subset R$ is an ideal such that $\sqrt{\mathfrak{a}} = \mathfrak{m} \subset R$ is maximal, then $\mathfrak{a}$ is $\mathfrak{m}$-primary.

Proof. The statement in (a) is clear and (b) follows from Theorem 1.2.2. For (c), suppose $xy \in \mathfrak{a}$ but $y \notin \sqrt{\mathfrak{a}} = \mathfrak{m}$. Then $\mathfrak{m} + (y) = (1)$ so $m + ry = 1$ for some $m \in \mathfrak{m}$ and $r \in R$. Since $m \in \sqrt{\mathfrak{a}}$, there is an $n \geq 1$ such that $m^n \in \mathfrak{a}$. Then $1 = 1^n = (m+ry)^n = m^n + sy$ for some $s \in R$, so $x = xm^n + sxy \in \mathfrak{a}$. ■

Example 3.2.3.

(a) If R is a PID, then the primary ideals of R are (0) and (p^r) for p prime and $r \geq 1$ (Exercise 3.1).
(b) In general, if R is a ring, $\mathfrak{p} \subset R$ a prime, and $r \geq 1$, then $\mathfrak{p}^r$ need not be $\mathfrak{p}$-primary (Exercise 3.2), although condition always holds when $\mathfrak{p}$ is maximal (Lemma 3.2.2(c)). For instance, if $R = k[X,Y]$, then the ideal $\mathfrak{a} = (X, Y^2)$ is a primary ideal that is not a prime power.
(c) The best replacement in (b) are the *symbolic powers*. Namely, if R is a ring and $\mathfrak{p} \subset R$ a prime ideal, then for each integer $n \geq 1$, we define the n^{th} *symbolic power* of $\mathfrak{p}$ to be $\mathfrak{p}^{(n)} := \eta^{-1}(\mathfrak{p}^n R_{\mathfrak{p}}) = \{x \in R : sx \in \mathfrak{p}^n \text{ for some } s \notin \mathfrak{p}\}$, where $\eta : R \to R_{\mathfrak{p}}$ is the localization map. Then $\mathfrak{p}^n \subset \mathfrak{p}^{(n)} \subset \mathfrak{p}$ for each n, we have $\mathfrak{p} = \mathfrak{p}^{(1)} \supset \mathfrak{p}^{(2)} \supset \cdots$, and each $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

The goal now is a *primary decomposition* of an arbitrary submodule $N \subset M$.

Definition 3.2.4. Let R be a ring and M an R-module. Let $N \subsetneq M$ be a submodule.

(a) A *primary decomposition* of N is an expression of the form

$$N = N_1 \cap N_2 \cap \cdots \cap N_r$$

where $r \geq 1$ is an integer and $N_1, \ldots, N_r$ are primary submodules of M.
(b) For $i = 1, \ldots, r$, let $\mathfrak{p}_i := \sqrt{\operatorname{Ann}(M/N_i)}$, so that each N_i is $\mathfrak{p}_i$-primary. The above primary decomposition is said to be *reduced* if the $\mathfrak{p}_i$ are pairwise distinct and N is not the intersection of any proper collection of $\{N_1, \ldots, N_r\}$; in this case, we call the N_i the *primary components* of N.

The existence and uniqueness of a primary decomposition is best achieved in the Noetherian setting. This is convenient, as the following lemma shows.

Lemma 3.2.5. Let R be a Noetherian ring and M a finitely generated R-module.

(a) Suppose that $\mathfrak{p} \subset R$ is a prime, $r \geq 1$ an integer, and $N_1, \ldots, N_r \subset M$ submodules which are $\mathfrak{p}$-primary. Then the intersection $N_1 \cap \cdots \cap N_r$ is also $\mathfrak{p}$-primary.
(b) If $N \subsetneq M$ is a submodule that admits a primary decomposition, then it admits a reduced primary decomposition. In fact, any primary decomposition of N gives rise to a reduced primary decomposition.

Proof.

(a) By Lemma 3.1.2(d) and Theorem 3.1.4(a), we have

$$\emptyset \subsetneq \operatorname{Ass}_R\left(M/\bigcap_i N_i\right) \subset \operatorname{Ass}_R\left(\bigoplus_i M/N_i\right) \subset \bigcup_i \operatorname{Ass}_R(M/N_i) = \{\mathfrak{p}\}.$$

(b) Consider the primary decomposition of N which involves the least number r of factors; by (a), this must be reduced. More constructively, given a primary decomposition, we may discard redundant N_i and use (a) to intersect all the remaining N_i that are primary to the same prime; iterating this procedure finitely many times yields a reduced primary decomposition.

■

We are ready for the main existence theorem.

Theorem 3.2.6 (Primary Decomposition: Existence)**.** Let R be a Noetherian ring and M a finitely generated R-module. Every propery submodule of M admits a reduced primary decomposition.

Proof. We say that a submodule $N \subset M$ is *irreducible* if it is proper and it cannot be written as $N = N_1 \cap N_2$ for some submodules $N_1, N_2 \subset M$ with $N \subsetneq N_1$ and $N \subsetneq N_2$. From Noetherian induction, it is clear that every proper submodule of N can be written as an intersection of irreducible submodules; therefore, we will finish by showing that every irreducible $N \subset M$ is primary. For this suppose that $N \subset M$ is a proper submodule that is not primary; we have to show that N is not irreducible. Replacing M by M/N, we may assume $N = 0$. To say that 0 is not primary implies by Proposition/Definition 3.2.1(d) that there are two distinct primes $\mathfrak{p}_1, \mathfrak{p}_2$ associated to M, so that there are elements $x_1, x_2 \in M$ with $R/\mathfrak{p}_i \cong Rx_i \hookrightarrow M$ for $i = 1, 2$. It remains to check (do!) that if $y_i \in Rx_i$ is any nonzero element, then $\mathrm{Ann}(y_i) = \mathfrak{p}_i$; then it follows that $Rx_1 \cap Rx_2 = (0)$, so that (0) is reducible. ■

Applying this to $M = R$ immediately yields

Corollary 3.2.7 (Lasker-Noether)**.** Every proper ideal of a Noetherian ring admits a reduced primary decomposition.

Finally, we turn to uniqueness; here the picture cannot be too nice, as evidenced by the following example.

Example 3.2.8.

(a) (Line with Embedded Point) Let k be a field, $R = k[X, Y]$ and $\mathfrak{a} = (X^2, XY)$. Then $\sqrt{\mathfrak{a}} = (X)$, and so $XY \in \mathfrak{a}$ but $X \notin \mathfrak{a}$ and $Y \notin \sqrt{\mathfrak{a}}$ shows that $\mathfrak{a}$ is not primary. Indeed, two reduced primary decompositions of $\mathfrak{a}$ are seen to be

$$\mathfrak{a} = (X, Y)^2 \cap (X) = (X^2, Y) \cap (X),$$

where in each case the first ideal is (X, Y)-primary (embedded) and the second is (X)-primary (isolated).

(b) (Quadric Cone) Let k be a field, $R = k[x, y, z] := k[X, Y, Z]/(XY - Z^2)$ and $\mathfrak{p} = (x, z)$. Then even though $\sqrt{\mathfrak{p}^2} = \mathfrak{p}$, the ideal $\mathfrak{p}^2$ is not primary (Exercise 3.2(a)), and indeed we have

$$\mathfrak{p}^2 = (x) \cap (x, y, z)^2,$$

where the first ideal is $\mathfrak{p}$-primary, and the second ideal is (x, y, z)-primary. In particular, in the primary decomposition of the ideal $\mathfrak{p}^2$, we have the "embedded point" (x, y, z) showing up.

Nonetheless, we do have a couple of uniqueness statements.

Theorem 3.2.9 (Primary Decomposition: Uniqueness I)**.** Let R be a Noetherian ring, M a finitely generated R-module and $N \subset M$ a proper submodule. If $r \geq 1$ and submodules $N_1, \ldots, N_r \subset M$ are such that $N = N_1 \cap \cdots \cap N_r$ is a reduced primary decomposition with $\mathfrak{p}_i := \sqrt{\mathrm{Ann}(M/N_i)}$ for $i = 1, \ldots, r$, then

$$\mathrm{Ass}(M/N) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}.$$

In particular, the prime ideals occuring in a reduced primary decomposition of N are uniquely determined by N.

Proof. Replacing M by M/N, we may assume $N = 0$. First suppose that $\mathfrak{p} \in \mathrm{Ass}(M)$, so there is a $0 \neq m \in M$ with $\mathfrak{p} = \mathrm{Ann}(m)$. By relabelling if needed, pick a j with $1 \leq j \leq r$ such that $m \in (N_{j+1} \cap \cdots \cap N_r) \smallsetminus (N_1 \cup \cdots \cup N_j)$. By the Noetherian hypothesis, there is an integer $k \gg 1$ such that $\mathfrak{p}_i^k \cdot M \subset N_i$ for all $i = 1, \ldots, r$, so that $\bigcap_{i=1}^{j} \mathfrak{p}_i^k \subset \mathrm{Ann}(m) = \mathfrak{p}$. By Lemma 1.2.12(a), there is an i with $1 \leq i \leq j$ such that $\mathfrak{p}_i \subset \mathfrak{p}$. We claim that equality must hold; indeed, if $x \in \mathfrak{p}$, then $xm = 0$ but $m \notin N_i$ implies that $x \in \mathfrak{p}_i$ by the primary hypothesis.

For the other direction, we'll show $\mathfrak{p}_1 \in \mathrm{Ass}(M)$. Since the decomposition of N is reduced, there is an $m \in \bigcap_{i=2}^{r} N_i \smallsetminus N_1$. Let $k \geq 1$ be the smallest integer such that $\mathfrak{p}_1^k \cdot (m) \subset N_1$, and pick a $n \in \mathfrak{p}_1^{k-1}(m) \smallsetminus N_1$. The claim is $\mathfrak{p}_1 = \mathrm{Ann}(n)$. Indeed, $\mathfrak{p}_1 \subset \mathrm{Ann}(n)$ follows from $\bigcap_{i=1}^{r} N_i = 0$, and if $x \in \mathrm{Ann}(n)$, then $xn = 0$ but $n \notin N_1$ implies by the primary hypothesis that $x \in \mathfrak{p}_1$. ∎

Corollary 3.2.10. Let R be a Noetherian ring and $\mathfrak{a} \subset R$ be a proper ideal.

(a) The following conditions on a prime $\mathfrak{p} \subset R$ are equivalent:
  (i) The prime $\mathfrak{p}$ contains $\mathfrak{a}$.
  (ii) The prime $\mathfrak{p}$ contains a prime associated to $\mathfrak{a}$.
  (iii) The prime $\mathfrak{p}$ contains an isolated prime of $\mathfrak{a}$.

  In other words, the minimal primes containing $\mathfrak{a}$ are exactly the isolated primes of $\mathfrak{a}$, and in particular there are only finitely many of these.

(b) The radical $\sqrt{\mathfrak{a}}$ is the intersection of all the associated primes of $\mathfrak{a}$, and hence all the isolated primes of $\mathfrak{a}$. In particular, $\mathfrak{a}$ is radical iff the primary components of any reduced primary decomposition of $\mathfrak{a}$ are all prime ideals. In this case, there are no embedded primes and the primary decomposition is unique.

(c) There is an integer $n \geq 1$ and not necessarily distinct primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset R$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{a}$.

Proof.

(a) The implications (iii) $\Leftrightarrow$ (ii) $\Rightarrow$ (i) are clear (using Theorem 3.1.4(a), (e) and 3.1.2(b)). For (i) $\Rightarrow$ (ii), by Corollary 3.2.7, $\mathfrak{a}$ has a reduced primary decomposition, say of the form $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ for some $r \geq 1$ with each $\mathfrak{q}_i$ a $\mathfrak{p}_i$-primary ideal for some prime $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, with each $\mathfrak{p}_i \in \mathrm{Ass}(R/\mathfrak{a})$ by Theorem 3.2.9. Then $\mathfrak{a} \subset \mathfrak{p}$ implies by Lemma 1.2.12(a) that there is an i with $1 \leq i \leq r$ such that $\mathfrak{q}_i \subset \mathfrak{p}$, whence $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$.

(b) In the notation of (a), we have $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_r} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$, so we are done by Theorem 3.2.9. If the primary components of some reduced primary decomposition of $\mathfrak{a}$ are primes, then $\mathfrak{a}$ is certainly radical; conversely, if $\mathfrak{a}$ is radical, then it is the intersection of its associated primes: say $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$. We claim that this expression is the only reduced primary decomposition of $\mathfrak{a}$ (upto rearrangement). Indeed, the integer r in this decomposition is uniquely determined as $\#\,\mathrm{Ass}(R/\mathfrak{a})$ from Theorem 3.2.9, whence $\mathfrak{a}$ does not admit a primary decomposition with fewer than r primes; from this reducedness of this decomposition follows, as well as the fact that there are no embedded primes associated to $\mathfrak{a}$. Finally, if $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ is any other reduced primary decomposition, then again by Theorem 3.2.9 we have $s = r$, and after rearranging if needed we can assume $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$ for each $i = 1, \ldots, r$. By reducedness, for each i, there is an $x \in \bigcap_{j \neq i} \mathfrak{p}_j \smallsetminus \mathfrak{p}_i$; then if $y \in \mathfrak{p}_i$, then $xy \in \mathfrak{a} \subset \mathfrak{q}_i$ and $x \notin \mathfrak{p}_i$ with $\mathfrak{q}_i$ being $\mathfrak{p}_i$-primary implies that $y \in \mathfrak{q}_i$, showing that in fact $\mathfrak{q}_i = \mathfrak{p}_i$.

(c) Since R is Noetherian, there is an integer $m \geq 1$ such that $(\sqrt{\mathfrak{a}})^m \subset \mathfrak{a}$, so we are done by (b).

■

We should note also that Corollary 3.2.10(c) can be deduced very directly by Noetherian induction (Exercise 3.6). Finally, we turn to the final version of uniqueness. For this, we will need some more preparation on how primary components interact with localization.

Theorem 3.2.11 (Primary Decomposition: Uniqueness II)**.**

3.3 Artinian Rings Revisited

Let us discuss some applications of primary decomposition here. The first one is to finish our discussion on Artinian rings. For this, we'll need one more piece of terminology: if R is a ring, we will denote by $\mathrm{mSpec}\, R$ its maximal spectrum, i.e. the set of its maximal ideals. The first result then is

Theorem 3.3.1. Let R be a Noetherian ring and M be a finitely generated R-module. The following conditions are equivalent:

(a) M is Artinian.
(b) The length $\ell_R(M)$ of M is finite.
(c) $\mathrm{Ass}_R(M) \subset \mathrm{mSpec}\, R$, i.e. every prime associated to M is maximal.
(d) $\mathrm{Supp}(M) \subset \mathrm{mSpec}\, R$, i.e. M is supported on maximal ideals.

In this case, $\mathrm{Ass}_R(M) = \mathrm{Supp}(M)$.

Proof. Since M is Noetherian, (a) $\Leftrightarrow$ (b) is the content of Lemma 1.3.4, (d) $\Rightarrow$ (c) follows from Lemma 3.1.2(b) and (c) $\Rightarrow$ (d) follows from Theorem 3.1.4(e). For the rest, we choose, using the proof of Theorem 3.1.4(a), an integer $n \geq 1$ and a sequence of submodules $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ with each successive quotient of the form $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i$. We claim that

$$\mathrm{Ass}_R(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \mathrm{Supp}(M).$$

The first of these inclusions was shown in the proof of Theorem 3.1.4(a); for the second one, note that for each $i = 1, \ldots, n$, we have

$$0 \neq \mathrm{Frac}(R/\mathfrak{p}_i) \cong (R/\mathfrak{p}_i)_{\mathfrak{p}_i} \cong (M_i/M_{i-1})_{\mathfrak{p}_i} \cong (M_i)_{\mathfrak{p}_i}/(M_{i-1})_{\mathfrak{p}_i},$$

whence $(M_i)_{\mathfrak{p}_i} \subset M_{\mathfrak{p}_i}$ is nonzero. Finally, by the additivity of length (Corollary 10.1.6) $\ell_R(M)$ is finite iff for each $i = 1, \ldots, n$, the length $\ell_R(R/\mathfrak{p}_i) = \ell_{R/\mathfrak{p}_i}(R/\mathfrak{p}_i)$ is finite, which happens iff $\mathfrak{p}_i$ is maximal (by Lemma 1.3.4 and Theorem 1.3.9(a)); this proves both (b) $\Rightarrow$ (c) and (d) $\Rightarrow$ (b). Then Theorem 3.1.4(e) implies in this case that $\mathrm{Ass}_R(M) = \mathrm{Supp}(M)$. ∎

In particular, if R is an Artinian ring and M a finitely generated R-module, then $\ell_R(M) < \infty$, so that M is also Noetherian (using Lemma 1.3.4). This gives another proof of Theorem 1.3.10. Finally, from this result we immediately obtain the required characterization of Artinian rings.

Corollary 3.3.2. For a ring R, the following are equivalent:

(a) R is Artinian.
(b) $\ell_R(R) = 0$.
(c) R is Noetherian of dimension zero, i.e. $\mathrm{Spec}\, R = \mathrm{mSpec}\, R$.
(d) R is Noetherian and $\mathrm{Ass}_R(R) \subset \mathrm{mSpec}\, R$.

Proof.

(a) $\Rightarrow$ (b) This is Theorem 1.3.9(b).
(b) $\Rightarrow$ (c) By Lemma 1.3.4, R is Noetherian and Artinian. From Theorem 3.3.1(d) we conclude that $\mathrm{Spec}\, R = \mathrm{Supp}\, R \subset \mathrm{mSpec}\, R$, so $\dim R = 0$.
(c) $\Rightarrow$ (d) This follows from the implication (d) $\Rightarrow$ (c) in Theorem 3.3.1.

(d) $\Rightarrow$ (a) This follows from the implication (c) $\Rightarrow$ (a) in Theorem 3.3.1.

■

3.4 Krull's Hauptidealsatz

We are now ready to use this machinery about Artinian rings to prove one very important and classical result from commutative algebra.

Theorem 3.4.1 (Generalized Krull's Hauptidealsatz)**.** For an integer $n \geq 0$, a prime ideal in a Noetherian ring has height at most n iff it is minimal over an ideal generated by at most n elements.

Geometrically, this statement says that a subvariety of codimension n in affine or projective space is (a component of) a subvariety cut out by at most n equations; conversely, any irreducible component of a variety cut out by at most n equations has codimension at most n. For instance, an affine or projective hypersurface can be cut out by one global equation, and any irreducible component of a subvariety cut out by one equation is a hypersurface (i.e. has codimension 1).

Proof. We induct on n. For $n = 0$, that $\operatorname{ht}\mathfrak{p} = 0$ iff $\mathfrak{p}$ is minimal follows from $\operatorname{ht}\mathfrak{p} = \dim R_{\mathfrak{p}}$. Hence suppose $n \geq 1$, and that we have shown the result for $n-1$.

First suppose that R is a Noetherian ring with a prime $\mathfrak{p} \subset R$ of height n. Using Observation 1.1.11(d), Corollary 1.1.12(e), and Corollary 3.2.10(a) on $R_{\mathfrak{p}}$, there are only finitely many minimal primes of R contained in $\mathfrak{p}$. By Prime Avoidance (Lemma 1.2.12(b)) and the fact that $\mathfrak{p}$ is *not* minimal, $\mathfrak{p}$ is not contained in the union of these; so pick an element $x \in \mathfrak{p}$ not contained in any minimal prime contained in $\mathfrak{p}$. It follows that in the quotient $R/(x)$, we have $\operatorname{ht}\mathfrak{p}/(x) \leq n-1$. By induction, $\mathfrak{p}/(x)$ is minimal over an ideal generated by at most $n-1$ elements; by taking preimages and appending x shows that $\mathfrak{p}$ is minimal over a prime generated by at most n elements.

Conversely, suppose R is a Noetherian ring with prime $\mathfrak{p}$ that is minimal over an ideal generated by n elements. By localizing at $\mathfrak{p}$, we may assume that $(R,\mathfrak{p})$ is local. First suppose $n = 1$, so $\mathfrak{p}$ is minimal over (x) for some $x \in R$; we have to show that if $\mathfrak{q} \subsetneq \mathfrak{p}$ is any prime, then $\operatorname{ht}\mathfrak{q} = 0$. Now the ring $R/(x)$ has only one prime, namely $\mathfrak{p}/(x)$, so that $\dim R/(x) = 0$. From Corollary 3.3.2, it follows that $R/(x)$ is Artinian. Therefore, if $\mathfrak{q} \subsetneq \mathfrak{p}$ is any prime, then the sequence $(\mathfrak{q}^{(n)} + (x))/(x)$ of symbolic powers of $\mathfrak{q}$ (Example 3.2.3(c)) taken in $R/(x)$ eventually stabilizes. In particular, there is an integer $n \geq 1$ such that $\mathfrak{q}^{(n)} + (x) = \mathfrak{q}^{(n+1)} + (x)$. ∎

3.5 Exercises

Exercise 3.1. Show that in a PID, nonzero primary ideals are exactly the powers of prime ideals.

Exercise 3.2. Let k be a field, $R = k[x,y,z] := k[X,Y,Z]/(XY - Z^2)$, and $\mathfrak{p} = (x,z)$.

(a) Show that R is a domain and $\mathfrak{p} \subset R$ a prime ideal such that $\mathfrak{p}^2$ is not a primary ideal.
(b) For each integer $n \geq 1$, describe the n^{th} symbolic power $\mathfrak{p}^{(n)}$.

Exercise 3.3. Consider the following conditions on a ring R.

(a) R has a unique minimal prime ideal.
(b) The nilradical $\mathrm{Nil}(R)$ is prime.
(c) Every zero-divisor of R is nilpotent.
(d) R is nonzero, and the ideal $(0) \subsetneq R$ is primary.
(e) There is a unique prime associated to the zero ideal $(0) \subset R$.

Show that (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) $\Leftrightarrow$ (d) $\Rightarrow$ (e), and if R is Noetherian, then all conditions are equivalent. A ring satisfying equivalent conditions (a)-(d) is said to be *primary* or *irreducible*.[2] Check that a ring R is an integral domain iff it is reduced and irreducible.

Exercise 3.4. Let R be a primary ring such that $\mathrm{Ass}_R(R)$ is nonempty (e.g. if R is Noetherian). Show that $\mathscr{Z}(R) = \mathrm{Nil}(R)$, i.e. the zero-divisors of R are precisely the nilpotent elements. Show that the hypothesis on $\mathrm{Ass}_R(R)$ is necessary.

Exercise 3.5. Let R be a primary ring and $S \subset R$ a multiplicative subset. Show that the localization $S^{-1}R$, if not zero, is primary. Does the converse hold in general?

Exercise 3.6. Let R be a Noetherian ring and $\mathfrak{a} \subset R$ a proper ideal. Show directly (i.e. using Noetherian induction and without using primary decomposition) that there is an integer $n \geq 1$ and not necessarily distinct primes $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset R$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{a}$.

[2] This latter terminology is due to the fact that, geometrically, this corresponds to the affine scheme $\mathrm{Spec}\, R$ being irreducible. We will use both interchangeably.

Chapter 4

Integrality and Cohen-Seidenberg Theory

4.1 Fundamentals of Integrality

Definition 4.1.1. Let $R \subset S$ be a ring extension. We say that an element $s \in S$ 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

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

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

If R is a field, then the notions of algebraicity and integrality over R coincide.

Definition 4.1.2 (Integral Closure/Normalization)**.**

(a) If $R \subset S$ is a ring 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 $\mathrm{Cl}_S(R)$.
(b) On the one hand, 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 $S \subset R$ is *integral* iff $\mathrm{Cl}_S(R) = S$.
(c) If R is an integral domain, then the normalization $\mathrm{Cl}_{\mathrm{Frac}(R)}(R)$ of R in its fraction field is called the *absolute integral closure* or *absolute normalization* of R.
(d) A domain R is said to be *integrally closed* or *normal* if $R = \mathrm{Cl}_{\mathrm{Frac}(R)}(R)$.

Theorem 4.1.3 (Robust Characterizations of Integrality)**.** Let $R \subset S$ be a ring extension and $s \in S$ an element. Then the following are equivalent:

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

Proof. It is clear that (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d). For (d) $\Rightarrow$ (a), apply Corollary 1.5.2 with $\mathfrak{a} = (1)$. ■

Corollary 4.1.4 (Properties of Integral Extensions)**.** Let $R \subset S \subset T$ be ring extensions.

(a) If $s_1, \ldots, s_n \in S$ are any elements over R, then the subalgebra $R[s_1, \ldots, s_n] \subset S$ is a finitely generated R-module iff all the s_i are integral over R.
(b) The normalization $\mathrm{Cl}_S(R)$ is a subring of S containing R.
(c) (Transitivity) If T/S and S/R are integral, then so is T/R.
(d) (Idempotence) We have $\mathrm{Cl}_S(\mathrm{Cl}_S R) = \mathrm{Cl}_S R$, i.e. $\mathrm{Cl}_S R$ is integrally closed in S.

Proof.

(a) The "only if" direction follows from Theorem 4.1.3(c). For the "if", proceed by induction on n; when $n = 1$, this follows from Theorem 4.1.3(b). When $n \geq 2$, define $R' := R[s_1, \ldots, s_{n-1}]$; by induction, this is a finitely generated R-module. Since s_n is integral over R, it is also integral over R' and so by the $n = 1$, we have $R'[s_n]$ is a finitely generated R'-module. By transitivity of module-finiteness, we conclude that $R[s_1, \ldots, s_n]$ is a finitely generated R-module.

(b) If $s,t \in S$ are integral, then $R[s,t]$ is a finitely generated R-module by (a), and so the inclusions $R[s-t], R[st] \subset R[s,t]$ imply by Theorem 4.1.3(c) that $s-t, st \in \mathrm{Cl}_S(R)$.
(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 4.1.3(c) shows that t is integral over R.
(d) This immediately from (c) because $\mathrm{Cl}_S(R)/R$ is integral by definition.

■

Example 4.1.5. The Rational Root Theorem asserts that a UFD is normal.

Example 4.1.6 (Algebraic Integers)**.** Let $K/\mathbf{Q}$ be any field extension (e.g. a number field). Then the integral closure $\mathrm{Cl}_K(\mathbf{Z}) =: \mathcal{O}_K$ of $\mathbf{Z}$ in K is called the *ring of algebraic integers* in K. It is easy to see that if $K/\mathbf{Q}$ is algebraic, then $K = (\mathbf{Z} \smallsetminus \{0\})^{-1}\mathcal{O}_K = \mathrm{Frac}\,\mathcal{O}_K$. By idempotence, $\mathcal{O}_K$ is normal but in general is not a UFD (e.g. for $K := \mathbf{Q}[\sqrt{-23}]$). When K is any algebraically closed field, this construction returns the ring $\mathcal{O}_{\overline{\mathbf{Q}}}$ of all algebraic integers.

Example 4.1.7 (Plane Cuspidal Cubic)**.** The coordinate ring of a planar cuspidal curve is a domain that is not normal. 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 $K := \mathrm{Frac}\,R$. 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 that $K = k(t) \cong k(\mathbf{P}^1)$ and $\mathrm{Cl}_K(R) = k[t]$.

Lemma 4.1.8. Let $R \subset S$ be an integral ring extension.

(a) If $\mathfrak{b} \subset S$ is an ideal and $\mathfrak{a} := \mathfrak{b} \cap R$, then $S/\mathfrak{b}$ is integral over $R/\mathfrak{a}$.
(b) If $U \subset R$ 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 in (a) and (b) are clear, and (d) follows from (a) and (c) applied to $R/\mathfrak{p} \subset S/\mathfrak{q}$. 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 $r^{-1} = -(a_1 + a_2 r + \cdots + a_n r^{n-1}) \in R$. ■

Note that part (c) of Lemma 4.1.8 needs S to be a domain; consider $k \subset k[x]/(x^2)$.

Lemma 4.1.9. Let R be an integral domain with $K := \mathrm{Frac}\,R$. Then:

(a) If $S \subset R$ is any multiplicative subset, then $\mathrm{Cl}_K(S^{-1}R) = S^{-1}\mathrm{Cl}_K(R)$.
(b) The following are equivalent:
  (i) R is normal.
  (ii) $S^{-1}R$ is normal for every multiplicative $S \subset R$.
  (iii) $R_\mathfrak{p}$ is normal for all $\mathfrak{p}$.
  (iv) $R_\mathfrak{m}$ is normal for all $\mathfrak{m}$.

Proof.

(a) By Lemma 4.1.8(b) we have $S^{-1}\mathrm{Cl}_K(R) \subset \mathrm{Cl}_K(S^{-1}R)$. 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 $x^n + s_1^{-1}a_1x^{n-1} + \cdots + s_n^{-1}a_n = 0$. 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 $x \in S^{-1}\mathrm{Cl}_K(R)$.

(b) The implication (i) $\Rightarrow$ (ii) follows from (b). The implications (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) are clear. For (iv) $\Rightarrow$ (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 $\bigcap_\mathfrak{m} R_\mathfrak{m} = R$, where in the last step we have used Corollary 1.1.14.

■

Finally, we briefly discuss integrality over an ideal.

Lemma 4.1.10. Let $R \subset S$ be a ring extension, and let $\mathfrak{a} \subset R$ be an ideal.

(a) The collection $\mathrm{Cl}_S(\mathfrak{a})$ of elements of S integral over $\mathfrak{a}$ is $\sqrt{\mathfrak{a}\mathrm{Cl}_S(R)}$.

(b) Suppose that S is a domain, and let $K := \mathrm{Frac}\, R$. Given an $s \in \mathrm{Cl}_S(\mathfrak{a})$, if the minimal polynomial of s over K is $\mu_s(X) = X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$, then for each i we have $a_i \in \mathrm{Cl}_K(\mathfrak{a})$. In particular, if R is normal, then the coefficients $a_i \in \sqrt{\mathfrak{a}}$.

Proof.

(a) If x is integral over $\mathfrak{a}$ and $n \geq 1, a_i \in \mathfrak{a}$ are such that $x^n + a_1x^{n-1} + \cdots + a_n = 0$, 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 $n \geq 1$ and elements $\alpha_j \in \mathfrak{a}, x_j \in \mathrm{Cl}_S(R)$. Since each x_j is integral over R, the ring $M := R[x_j]_j$ is a finitely generated R-module and $x^nM \subset \mathfrak{a}M$. By Observation 1.5.1, we have that $x^n + a_1x^{n-1} + \cdots + a_n = 0 \in \mathrm{End}_R(M)$ for some $a_i \in \mathfrak{a}$, but since $1 \in M$, we have this identity in S.

(b) Let $L := \mathrm{Frac}\, S$ and look at the roots s_j of μ_s in some extension of 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 s_i, they belong to $\mathrm{Cl}_S(\mathfrak{a})$ as well. Therefore, they belong to $\mathrm{Cl}_S(\mathfrak{a}) \cap K = \mathrm{Cl}_K(\mathfrak{a})$. If R is normal, then by (a) we have $\mathrm{Cl}_K(\mathfrak{a}) = \sqrt{\mathfrak{a}\mathrm{Cl}_K(R)}$, so that if R is normal, i.e. $R = \mathrm{Cl}_K(R)$, then this is just $\sqrt{\mathfrak{a}}$.

■

Corollary 4.1.11. Let R be a normal domain, $K = \mathrm{Frac}\, R$ be its fraction field, L/K an algebraic extension and $S = \mathrm{Cl}_L(R)$. An $\alpha \in L$ is in S iff the minimal polynomial $\mu_\alpha(X) \in K[X]$ of α over K is in $R[X]$.

This corollary reduces the check of integrality to that of identifying the minimal polynomial; some applications of this can be found in Exercises 4.1 and 4.2.

Proof. The "if" implication is clear; for the "only if", take $\mathfrak{a} = R$ in Lemma 4.1.10(b). ■

4.2 Cohen-Seidenberg Theory

In this section, we develop the basic Cohen-Seidenberg theory of primes in integral extensions, which allow us to relate the Krull dimensions of two rings in an integral extension.

Theorem 4.2.1. Let $R \subset S$ be an integral extension and $\mathfrak{p} \subset R$ be 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 1.1.13, it suffices to show that $\mathfrak{p}S \cap R \subset \mathfrak{p}$. If $x \in \mathfrak{p}S \cap R$, then $x \in \sqrt{\mathfrak{p}S}$, so by Lemma 4.1.10(a), we have $x \in \mathrm{Cl}_S(\mathfrak{p})$ and so $x^n \in \mathfrak{p}$ for some $n \geq 1$, from which we get $x \in \sqrt{\mathfrak{p}} = \mathfrak{p}$. For an alternative proof which also shows (b), localize both sides at $U := R \setminus \mathfrak{p}$ and use Lemma 4.1.8(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 4.1.8(d) and so $\mathfrak{n} \cap R = \mathfrak{m}$ and $\mathfrak{n}$ lies over $\mathfrak{m}$. Conversely, if $\mathfrak{n} \subset S$ is a prime that satisfies $\mathfrak{n} \cap R = \mathfrak{m}$, then again by Lemma 4.1.8(d), $\mathfrak{n}$ is maximal; in particular, there are no inclusions between distinct $\mathfrak{n}$. ■

Remark 4.2.2. Geometrically, Theorem 4.2.1 is saying that if $\varphi : R \to S$ is an injective integral morphism, then $\operatorname{Spec}\varphi$ is surjective and that a point of a given fiber of this map is not a specialization of another one in the same fiber.

Example 4.2.3. Let $K/\mathbf{Q}$ be a number field, and $\mathcal{O}_K = \mathrm{Cl}_K(\mathbf{Z})$ its ring of integers. Given any prime $\mathfrak{p} \subset \mathcal{O}_K$, there is a prime $\mathfrak{P} \subset \mathcal{O}_{\overline{\mathbf{Q}}}$ in the ring of all algebraic integers such that $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, and no two such primes $\mathfrak{P}, \mathfrak{P}'$ are comparable. Can you locate the hidden use of Zorn's Lemma in this proof?

Definition 4.2.4. A ring extension $R \subset S$ satisfies

(a) *the going up property* if given any $n \geq 1$ and chain $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ of primes in R and $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ in S for some $1 \leq m < n$ 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 $\mathfrak{q}_{m+1} \subset \cdots \subset \mathfrak{q}_n$ 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 $\mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$ of primes in R and $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ in S for some $1 \leq m < n$ 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 $\mathfrak{q}_{m+1} \supset \cdots \supset \mathfrak{q}_n$ in S such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all i.

Theorem 4.2.5 (Cohen-Seidenberg)**.**

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

Proof. By Lying Over (Theorem 4.2.1(a)) and induction, we are reduced to the case $n = 2, m = 1$.

(a) By Lemma 4.1.8(a), $S/\mathfrak{q}_1$ is integral over $R/\mathfrak{p}_1$, so by Lying Over (Theorem 4.2.1(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 1.1.12(d) and Corollary 1.1.13 that $\mathfrak{p}_2 S_{\mathfrak{q}_1} \cap R \subset \mathfrak{p}_2$. 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 $K := \operatorname{Frac} R$ is $\mu_y(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X]$ then each $a_i \in \operatorname{Cl}_K(\mathfrak{p}_2) = \mathfrak{p}_2$ by Lemma 4.1.10(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 $\mu_s(X) = X^n + b_1 X^{n-1} + \cdots + b_n \in K[X]$ with $b_i = x^{-i} a_i$. But s is integral over R, so by Corollary 4.1.11 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 $s^n \in \mathfrak{p}_2 S \subset \mathfrak{p}_1 S \subset \mathfrak{q}_1$, which is a contradiction to $s \notin \mathfrak{q}_1$.

■

For a different proof of Going Down using a little Galois Theory, see [5, Theorem 13.9]. Cohen and Seidenberg's very readable original paper [6] treats the slightly more general case where R is assumed to be a normal domain and no zero-divisors of S lie in R. Then also give counterexamples to show that the hypotheses cannot be easily weakened. A reader interested in this aspect of the theory is highly encouraged to read this paper. Finally, we note that Going Down also holds under the assumption that the extension $R \subset S$ is *flat*; see [5, Lemma 10.11]. This (along with Chevalley's Theorem) is the key ingredient in the proof that flat morphisms locally of finite presentation are open.

The Cohen-Seidenberg Theorems enable use to relate the dimensions of rings related by an integral extension. This comparison result is

Corollary 4.2.6. Let $R \subset S$ 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) $\operatorname{coht} \mathfrak{p} = \operatorname{coht} \mathfrak{q}$,
(c) $\operatorname{ht} \mathfrak{p} \geq \operatorname{ht} \mathfrak{q}$, and
(d) equality holds in (c) whenever the result of the Going Down Theorem 4.2.5(b) holds.

Proof.

(a) Going Up and Incomparability (Theorem 4.2.5(a) and Theorem 4.2.1(b)) give us a canoncial bijection between (strict) chains of primes in R and S.
(b) The ring $S/\mathfrak{q}$ is integral over $R/\mathfrak{p}$ by Lemma 4.1.8(a), and so we are done by (a).
(c) If we have a chain of primes contained in $\mathfrak{q}$ of length n, then by intersecting with R we get a chain of length n in $\mathfrak{p}$ (where the inclusions are strict again by incomparability–Theorem 4.2.1(b)).
(d) Apply Going Down to go the other way.

■

4.3 Extensions of Homomorphisms to Algebraically Closed Fields

In this section, we discuss some general results on when homomorphisms to an algebraically closed field extend across ring extensions. These results will be very helpful when we return to dimension questions later.

Theorem 4.3.1. Let $R \subset S$ be a ring extension and Ω be an algebraically closed field. Let $\varphi : R \to \Omega$ be a homomorphism; we ask when it extends to a homomorphism $\hat{\varphi} : S \to \Omega$.

(a) If $R \subset S$ is integral, then φ extends to homomorphism $\hat{\varphi} : S \to \Omega$.
(b) (Lang's Lemma) If S is a domain and finitely generated R-algebra, φ extends to a $\hat{\varphi} : S \to \Omega$. In fact, given any $0 \neq s \in S$ there is a $0 \neq r \in R$ depending on s 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 φ extends to either $R[\alpha] \to \Omega$ or $R[\alpha^{-1}] \to \Omega$.

Proof.

(a) Let $\mathfrak{p} := \ker \varphi$. Replacing R by $R_{\mathfrak{p}}$ and S by $S_{\mathfrak{p}} := (R \smallsetminus \mathfrak{p})^{-1}S$ and using Lemma 4.1.8(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 4.2.1(a)) and Lemma 4.1.8(d), there is a maximal $\mathfrak{n} \subset S$ such that $\mathfrak{n} \cap R = \mathfrak{m}$. Then $S/\mathfrak{n}$ is an algebraic extension of the field k and Ω is an algebraically closed field containing $F := \varphi(k)$, so by the well-known case of algebraic extensions of fields, there is an extension $S/\mathfrak{n} \to \Omega$ extending $\varphi : k \to F$. Then $\hat{\varphi} : S \twoheadrightarrow S/\mathfrak{n} \to \Omega$ is the required extension of φ.

(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 some $n \in \mathbf{Z}_{\geq 0}$ and $a_0, \ldots, a_n \in R$ 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 Ω is infinite. Then define $\hat{\varphi} : R[x] \to \Omega$ by sending $x \mapsto \alpha$. Now 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 $a_i, b_j \in R$ with $a_0, b_m \neq 0$, and set $r := a_0b_m$. (That $r \neq 0$ uses that S is domain.) Then $S[r^{-1}] = R[r^{-1}][x]$ is integral over $R[r^{-1}]$. If $\varphi(r) \neq 0$, then φ extends to a map $R[r^{-1}] \to \Omega$ 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.

(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 $\mathfrak{a} := \{f(X) \in R[X] : f(\alpha) = 0\} \subset R[X]$ and let $\mathfrak{b} := (\varphi(\mathfrak{a})) \subset F[X]$. 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 step 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 α and α^{-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 without loss of generality that $n \geq m$. Multiplying throughout by $a_0\alpha^n$, we get the relation $a_0\alpha^n + a_0 b_{m-1}\alpha^{n-1} + \cdots + a_0 b_0 \alpha^{n-m} = 0$. Here we have two cases. If $n = m$, then subtracting the two and multiplying by $(1 - a_0 b_0)^{-1}$ gives us $(a_1 - a_0 b_{m-1})(1 - a_0 b_0)^{-1}\alpha^{n-1} + \cdots + 1 = 0$. If $n \geq 2$, we have contradicted the minimality of n; if $n = 1$, then we have concluded the absurdity $1 = 0$.

■

4.4 Exercises

Exercise 4.1. Let $d \in \mathbf{Z}$ be a squarefree integer. Show that

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

Exercise 4.2. Let k be a field and $f(X) \in k[X]$ be a nonconstant separable polynomial. Let $R := k[X]$ and $K := \operatorname{Frac} k[X] = k(X)$.

(a) Show that $Y^2 - f(X) \in K[Y]$ is irreducible.

Let $L = K[\sqrt{f}] := K[Y]/(Y^2 - f(X))$; this is an algebraic field extension of K. Let $S := \mathrm{Cl}_L(R)$.

(b) Show that if $\operatorname{char} k \neq 2$, then $S = R[\sqrt{f}]$.

(c) Show by example that the result of (b) is false in general if $\operatorname{char} k = 2$. Can this result be salvaged?

Chapter 5

Field Theory

5.1 Linear Disjointness

In this section, we study the basic condition of abstract linear disjointness. To set this notion up, consider first the case of a large embedding field. Let Ω/k be a field extension, and let $k \subset K/L \subset \Omega$ be two subextensions. In this setting, we let $K[L] = L[K]$ denote the smallest subring of Ω containing K and L, and let KL denote the compositum of K and L in Ω, i.e. the smallest sub*field* of Ω containing both K and L, so that $KL = \operatorname{Frac} K[L]$ with $KL = K[L]$ if either K or L is algebraic over k (see Exercise 5.1).

Proposition/Definition 5.1.1. Let Ω/k be a field extension, and let $k \subset K, L \subset \Omega$ be two subextensions. The following conditions are equivalent:

(a) If a collection $\{x_\lambda\}$ of elements of K is linearly independent over k, then the same collection considered in Ω is linearly independent over L.
(b) The same as (a) with K and L interchanged.
(c) If $\{x_\lambda\}$ (resp. $\{y_\mu\}$) is a collection of elements of K (resp. L) linearly independent over k and $c_{\lambda\mu} \in k$ are elements, all but finitely many zero, such that $\sum c_{\lambda\mu} x_\lambda y_\mu = 0 \in \Omega$, then each $c_{\lambda\mu} = 0$.
(d) The natural map $K \otimes_k L \to \Omega$ is injective.
(e) The natural map $K \otimes_k L \to K[L]$ is an isomorphism.

When one of K and L is finite over k, say L, then these conditions are also equivalent to

(f) We have $[KL : K] = [L : k]$.

When these equivalent conditions are satisfied, we say that K and L are *linearly disjoint over k in Ω*. Further,

(g) If $\Lambda \subset \Omega$ is any field containing the compositum KL, then K and L are linearly disjoint over k in Ω iff they are so in Λ; in particular, this holds for $\Lambda = KL$.
(h) In this setting, K and L are linearly disjoint over k in Ω iff for all finitely generated subextensions $K' \subset K$ and $L' \subset L$, the fields K' and L' are linearly disjoint over k in Ω.
(i) If K and L are linearly disjoint over k in Ω, then $K \cap L = k$.

Proof. Note that the natural map $K \otimes_k L \to K[L]$ is surjective, so an isomorphism iff it is injective. The equivalence of (a)-(e) is clear from the properties of tensor product over a field k. When L is finite over k, then $K[L] = KL$ is the compositum of K and L in Ω (Exercise 5.1), so that (e) and (f) are equivalent for dimension reasons. The claims (g) and (h) are clear; for (i), if $\theta \in K \cap L \smallsetminus k$, then $1 \otimes \theta - \theta \otimes 1 \in K \otimes_k L$ is a nonzero element of the kernel of the map to Ω. ∎

When K and L are both finite over k, the condition (f) is clearly equivalent also to $[KL : k] = [K : k][L : k]$. The converse of (i) is not true; see Theorem 5.1.3 and Remark 5.1.4. Let us now immediately study the dependence of this notion on Ω, or equivalently the notion of "abstract" linear disjointness of two field extensions; the original source for the following very clear treatment is [7].

Proposition/Definition 5.1.2. Let k be a field, and $K, L \supset k$ two field extensions, not necessarily embedded in any larger field.

(a) The field extensions K and L are said to be *somewhere linearly disjoint over k* if there is a field extension $\Omega \supset k$ and k-embeddings $i : K \hookrightarrow \Omega$ and $j : L \hookrightarrow \Omega$ such that $i(K)$ and

$j(L)$ are linearly disjoint over k in Ω; this is equivalent to $K \otimes_k L$ being a domain.

(b) The field extensions K and L are said to be *everywhere linearly disjoint over k* if for every field extension $\Omega \supset k$ and k-embeddings $i : K \hookrightarrow \Omega$ and $j : L \hookrightarrow \Omega$, the fields $i(K)$ and $j(L)$ are linearly disjoint over k in Ω; this is equivalent to $K \otimes_k L$ being a field.

(c) If either K or L is algebraic over k, then conditions (a) and (b) are equivalent, i.e. if K, L are somewhere linearly disjoint over k, then they are everwhere linearly disjoint over k. In this case, we say that K and L are *(abstractly) linearly disjoint over k*.

See also Exercise 5.8.

Proof.

(a) If there is such a field extension Ω, then $K \otimes_k L \cong i(K) \otimes_k j(L) \xrightarrow{\sim} i(K)[j(L)] \subset \Omega$ is a domain; conversely, if $K \otimes_k L$ is a domain, taking $\Omega = \operatorname{Frac} K \otimes_k L$ suffices.

(b) If $K \otimes_k L$ is a field, then for any field Ω, the natural map $K \otimes_k L \to \Omega$ must be injective; conversely, if $K \otimes_k L$ is *not* a field, then it has a nontrivial maximal ideal $\mathfrak{m} \subset K \otimes_k L$, and taking $\Omega := K \otimes_k L/\mathfrak{m}$ gives us a field extension in which K and L are *not* linearly disjoint over k.

(c) In light of Exercise 5.4, the implication (b) $\Rightarrow$ (a) always holds, and if K or L is algebraic (i.e. integral) over k, the implication (a) $\Rightarrow$ (b) follows from the stability of integrality under basechange and Lemma 4.1.8(c). Alternatively, suppose there is a field extension $\Omega \supset k$ containing K and L such that K and L are linearly disjoint over k in Ω. Then by Proposition/Definition 5.1.1(e), the natural map $K \otimes_k L \to K[L]$ is an isomorphism. By Exercise 5.1, if either K or L is algebraic over k, then $K[L] = KL$ is the compositum of K and L in Ω, and hence in this case $K \otimes_k L$ is a field, whence K and L are everywhere linearly disjoint over k.

■

Here is a good illustration of these definitions.

Theorem 5.1.3. Let k be a field and $K, L \supset k$ be two algebraic extensions such that at least one of K and L is normal over k and at least one of K and L is separable over k. Then K and L are (abstractly) linearly disjoint over k iff for some further field extension Ω containing K and L we have $K \cap L = k$.

By Proposition/Definitions 5.1.2 if this condition holds, then $K \cap L = k$ in *any* Ω.

Proof. One direction was shown in Propositions/Definitions 5.1.1(i) and 5.1.2(c) above; for the other, suppose that we are given such an Ω, and further that K is separable over k; then in light of Proposition 5.1.2(c), we only need to show that $K \cap L = k$ implies that K and L are linearly disjoint over k in Ω.

First suppose that K is also normal, so that K/k is Galois; this result is then called the "Theorem on Natural Irrationalities." By Proposition/Definition 5.1.1(h), we may assume that $K, L/k$ are finite, and by replacing K by its normal closure we may assume further that K is finite Galois. By the Primitive Element Theorem, K is the splitting field of a single separable polynomial over k, in which case KL is the splitting field of the same polynomial over L and hence KL/L is Galois as well. Since $K \cap L = k$, there is a restriction map $\operatorname{Gal}(KL/L) \to \operatorname{Gal}(K/k)$, which is easily seen to be an isomorphism, giving us $[KL : L] = [K : k]$. Then we are done by Proposition/Definition 5.1.1(f).

Now suppose only that K is separable, but L is normal over k. As in the previous step, we may assume that K and L are both finite over k. Let S (resp. I) denote the separable (resp. purely inseparable) closure of k in L, so that S/k is Galois and so, by the case already shown, we have $[KS : K] = [S : k]$. Now KS/k is separable and I/k purely inseparable, so that by Exercise 5.9, KS and I are linearly disjoint over k in Ω; in particular, $[KL : KS] = [KSI : KS] = [I : k]$. Then the result follows again from Proposition/Definition 5.1.1(f) along with the computation

$$[KL : K] = [KL : KS][KS : K] = [I : k][S : k] = [I : k][L : I] = [L : k],$$

where we are using in the second-to-last step that $I = L^{\mathrm{Aut}(L/k)}$, whence L/I is Galois with Galois group $\mathrm{Aut}(L/k) \cong \mathrm{Gal}(S/k)$, and so in particular $[L : I] = [S : k]$. ■

Remark 5.1.4. There is no easy way to strengthen the preceding theorem, in the following sense.

(a) Taking $k = \mathbf{Q}$, $K = \mathbf{Q}[\sqrt[3]{2}]$, and $L = \mathbf{Q}[\omega\sqrt[3]{2}]$ inside say $\Omega = \mathbf{C}$ (where $\omega^2 + \omega + 1 = 0$) gives us an example where both K and L are separable over k and $K \cap L = k$ in Ω, but K and L are not linearly disjoint over k, since $KL = \mathbf{Q}[\sqrt[3]{2}, \omega]$ has degree 6 over k. Note that neither K nor L is normal over k.

(b) Given a prime $p > 0$, taking $k = \mathbf{F}_p(s,t)$, $K = k[X]/(X^{p^2} + sX^p + t)$, and $L = k^{1/p^\infty}$ inside an algebraic closure Ω of k gives us an example where L/k is normal and $K \cap L = k$ in Ω, but K and L are not linearly disjoint over k. Note that neither K nor L is separable over k. See §5.3 and [8] for details, and also Exercise 5.6 for a similar example.[1]

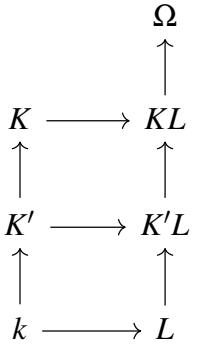
Finally, one result that is used quite often is

Theorem 5.1.5 (Transitivity of Linear Disjointness)**.** Let $k \subset \Omega$ be a field extension, and let $k \subset K' \subset K \subset \Omega$ and $k \subset L \subset \Omega$ be subextensions. Then K and L are linearly disjoint over k in Ω iff K' and L are linearly disjoint over k in Ω and K and $K'L$ are linearly disjoint over K' in Ω.

Proof. Consider the sequence of maps

$$K \otimes_k L \xrightarrow{\sim} K \otimes_{K'} (K' \otimes_k L) \twoheadrightarrow K \otimes_{K'} K'[L] \twoheadrightarrow K[L].$$

If K and L are linearly disjoint over k in Ω, then clearly so are K' and L; further, the composite map $K \otimes_k L \to K[L]$ above is an isomorphism, forcing the map $K \otimes_{K'} K'[L] \to K[L]$ to be an isomorphism as well, which implies that K and $K'[L]$ are linearly disjoint over K', and then so are K and $K'L$ since $K'L = \mathrm{Frac}\, K'[L]$ (Exercise 5.3).



[1] I would be interested in seeing an example where both K and L are normal but Theorem 5.1.3 fails. I also suspect that this result needs a suitable p-dimension to be at least 2 (so, e.g., that there is no counterexample with $k = \mathbf{F}_p(s)$).

Conversely, if K' and L are linearly disjoint over k in Ω, then the natural map $K' \otimes_k L \to K'[L]$ is injective, and hence, since tensoring over a field is exact, so is $K \otimes_{K'} (K' \otimes_k L) \to K \otimes_{K'} K'[L]$. If further K and $K'L$ are linearly disjoint over K' in Ω, then so are K and $K'[L]$ (again see Exercise 5.3), and hence the map $K \otimes_{K'} K'[L] \to K[K'[L]] = K[L]$ is injective as well. These two facts combined then imply that the map $K \otimes_k L \to K[L]$ is also injective, so that K and L are linearly disjoint over k. ■

5.2 Some Dependence Relations Involving Fields

We use the abstract study of dependence relations (§10.2) to some more sophisticated concrete examples: that of algebraic dependence, p-dependence and differential dependence.

5.2.1 Algebraic Dependence

Theorem/Definition 5.2.1. Let $k \subset K$ be a field extension. The map $\mathscr{D} : 2^K \to 2^K$ defined by sending X to the integral closure of $k(X)$ in K, i.e.

$$\mathscr{D}X = \mathrm{Cl}_K(k(X))$$

is a dependence relation on K, called *algebraic dependence* over k.

A basis for this dependence relation is called a *transcendence basis* for K/k, and the dependency of K with respect to this relation is called the *transcendence degree of K over k*, written $\mathrm{trdeg}_k K$. More generally, if R is a domain containing k, we define its *transcendence degree over k*, written $\mathrm{trdeg}_k R$ to be $\mathrm{trdeg}_k R := \mathrm{trdeg}_k \operatorname{Frac} R$.

Proof. Conditions (a), (b), and (d) in Definition 10.2.1 are clear, and (c) follows from transitivity of integral closure: for any X, the set $\mathscr{D}X$ is a field by Lemma 4.1.8(c) and so

$$\mathscr{D}^2X = \mathrm{Cl}_K k(\mathscr{D}X) = \mathrm{Cl}_K \mathscr{D}X = \mathrm{Cl}_K(\mathrm{Cl}_K k(X)) = \mathrm{Cl}_K k(X) = \mathscr{D}X,$$

where in the second to last step have used Corollary 4.1.4(d). It remains to show (e). Suppose that $x \in X \subset K$ and $y \in \mathscr{D}X \smallsetminus \mathscr{D}(X \smallsetminus \{x\})$; then for some $n \geq 1$ and $a_0, \ldots, a_n \in k(X)$ with $a_0 \neq 0$ we have $a_0 y^n + \cdots + a_n = 0$. Clearing denominators, we may assume that each $a_i \in k[X]$. 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 each $b_i \in k[(X \smallsetminus \{x\}) \cup \{y\}]$. If $m = 0$, then $b_0 = 0$ still has a nonzero power of y and then shows that $y \in \mathscr{D}(X \smallsetminus \{x\})$, a contradiction; therefore $m \geq 1$ and we have shown that $x \in \mathscr{D}((X \smallsetminus \{x\}) \cup \{y\})$ as needed. ∎

The fundamental set of this relation is the field $\mathrm{Cl}_K(k)$, i.e. the algebraic closure of k in K. An element $x \in K$ is said to be *transcendental* over k iff $\{x\}$ is algebraically independent over k, which is equivalent to saying that $x \notin \mathrm{Cl}_K(k)$. It is a straightforward consequence of the definition that a family of elements $\{x_\lambda\}$ in K is algebraically independent over k iff the natural map $k[X_\lambda] \to K$ taking $X_\lambda \mapsto x_\lambda$ is injective, and hence extends to an isomorphims $k(X_\lambda) \to k(x_\lambda)$. This family is, in addition, a transcendence basis for K/k iff K is in addition algebraic over $k(x_\lambda)$. In particular, K/k is algebraic iff $\mathrm{trdeg}_k K = 0$ and $\mathrm{trdeg}_k k(X_1, \ldots, X_n) = n$ for any $n \geq 0$. Finally, it is easy to see that if $k \subset K \subset L$ is a tower of extensions, then $\mathrm{trdeg}_k L = \mathrm{trdeg}_k K + \mathrm{trdeg}_K L$ (Exercise 5.7), and that any finitely generated field extension has finite transcendence degree–indeed, if $K = k(a_1, \ldots, a_n)$, then there is a subset of $\{a_1, \ldots, a_n\}$ that is a transcendence basis for K over k.

Remark 5.2.2. It is not necessarily true that if K/k has finite transcendence degree then it is finitely generated; indeed, consider $k = \mathbf{Q}$ and $K = \overline{\mathbf{Q}}$.

Example 5.2.3. Let $\Omega/\mathbf{Q}$ be a field extension with $|\Omega| = \mathfrak{c}$ (e.g., $\Omega = \mathbf{R}, \mathbf{C}, \mathbf{Q}_p, \overline{\mathbf{Q}_p}, \mathbf{C}_p$, etc.). We show that $\mathrm{trdeg}_{\mathbf{Q}} \Omega = \mathfrak{c}$. 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 Ω 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 Ω over $\mathbf{Q}(X)$ would show that Ω is countable as well, which is false. The Lefschetz principle (as well as another proof of the Nullstellensatz for $k = \Omega$ when algebraically closed, see [9, Lecture 5]) makes use of this observation.

Example 5.2.4. Let k be a field, $n \geq 1$ an integer, and $f \in k[X_1, \ldots, X_n]$ be an irreducible polynomial. Then $R := k[X_1, \ldots, X_n]/(f)$ is an integral domain; we claim that $\operatorname{trdeg}_k R = n - 1$. Indeed, let $K := \operatorname{Frac} R$. Write $f = a_0 X_n^m + a_1 X^{m-1} + \cdots + a_m$ for some $m \geq 0$ and each $a_i \in k[X_1, \ldots, X_{n-1}]$ with $a_0 \neq 0$. By relabelling the X_i if necessary, we may assume that $m \geq 1$. If $x_1, \ldots, x_n$ denote the classes of $X_1, \ldots, X_n$ in R (and so K) respectively, then we claim that $\{x_1, \ldots, x_{n-1}\}$ form a transcendence basis for K over k. Indeed, the equation $\overline{f} = 0$ in K shows that x_n is algebraically dependent on $\{x_1, \ldots, x_{n-1}\}$, so these elements form an algebraic spanning set. To show that they are algebraically independent, suppose that there is a polynomial $g \in k[X_1, \ldots, X_{n-1}]$ such that $g(x_1, \ldots, x_{n-1}) = 0$. Then $g \in k[X_1, \ldots, X_{n-1}] \cap (f) = (0) \subset k[X_1, \ldots, X_n]$ as needed.[2]

One further idea that we will use is that of

Definition 5.2.5. Let L/k be a field extension.

(a) A *separating transcendence basis for* L/k is a transcendence basis X for L/k such that the algebraic extension $L/k(X)$ is separably algebraic.
(b) The extension L/k is said to be *separably generated* if it admits a separating transcendence basis.

Note that in characteristic zero, any transcendence basis is a separating transcendence basis and every field extension is separably generated.

5.2.2 p-dependence

Next up is a phenomenon special to characteristic $p > 0$, due to Teichmüller from 1936.

Theorem/Definition 5.2.6. Let $k \subset L$ be a field extension in characteristic $p > 0$. The map $\mathscr{D} : 2^K \to 2^K$ defined by sending X to the smallest subfield of K containing k, K^p and X, i.e.

$$\mathscr{D}X = k(K^p, X)$$

is a dependence relation on K, called *p-dependence* over k.

A basis for this dependence relation is called a *p-basis* for K/k, and the dependency of K with respect to this relation is called the *p-dimension* of K over k, written $p\text{-}\dim_k K$.

Proof. Conditions (a)-(d) are clear; again, we have to show (e). Suppose $x \in X \subset K$ and $y \in \mathscr{D}X \smallsetminus \mathscr{D}(X \smallsetminus \{x\})$. Let $L := \mathscr{D}(X \smallsetminus \{x\})$ for convenience, so that $\mathscr{D}X = L(x)$ and $y \in L(x) \smallsetminus L$.

[2]Note that the converse of this observation is also true: if $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ is a prime ideal such that $R := k[X_1, \ldots, X_n]/\mathfrak{p}$ has $\operatorname{trdeg}_k R = n - 1$, then $\mathfrak{p}$ is principal. This is dimension theory combined with Krull's Hauptidealsatz; see [TODO].

Note that since $x^p \in L$ but $x \notin L$, it follows that $[L(x) : L] = p$.[3] Now $L \subsetneq L(y) \subset L(x)$ and the primality of p forces $L(x) = L(y)$, whence $x \in L(y)$, as needed. ■

The fundamental set of this relation is the field $k(K^p)$. A family of elements $B = \{x_\lambda\}$ in K is p-indepedent over k iff for any finite subset $B' \subset B$ of cardinality $n \geq 0$, we have $[k(K^p, B') : k(K^p)] = p^n$, or equivalently iff the set Γ_B of p-monomials

$$\Gamma_B := \left\{ x^e = \prod_\lambda x_\lambda^{e_\lambda} \right\}$$

in B (where $e = (e_\lambda)$ runs over the set of tuples indexed by B such that $0 \leq e_\lambda \leq p-1$ for each λ and $e_\lambda = 0$ for all but finitely many λ) is linearly independent over $k(K^p)$. This family B is further a p-basis if in addition we have $k(K^p, B) = K$, or equivalently iff Γ_B is a $k(K^p)$-basis of K.

Example 5.2.7. Let p be a prime, $n \geq 0$ an integer and $K := \mathbf{F}_p(X_1, \ldots, X_n)$ and let $k = K^p$. Then $\{X_1, \ldots, X_n\}$ is a p-basis for K/k, so $p\text{-dim}_k K = n$. Conversely, if K/k is any extension field generated by m-elements (i.e. $K = k(a_1, \ldots, a_m)$), then there is a subset of $\{a_1, \ldots, a_n\}$ that is a p-basis for K/k, and in particular $p\text{-dim}_k K \leq m$. In particular, $\mathbf{F}_p(X,Y)/\mathbf{F}_p(X^p, Y^p)$ is not a simple extension, illustrating the necessity of the separability hypothesis in the Primitive Element Theorem.

5.2.3 Differential Dependence

Finally, here is a more sophisticated notion of dependence that we shall use in these notes.

Definition 5.2.8. Let $k \subset K$ be a field extension. Then the module $\Omega_{K/k}$ of Kähler differentials is an K-vector space and so has a linear dependence relation LD_K. If $\mathrm{d} : K \to \Omega_{K/k}$ is the universal differential, then the pullback dependence relation (Exercise 10.5) $\mathrm{d}^*\mathrm{LD}_K$ on K is called the relation of *k-differential dependence* on K.

It follows from the definition that a collection $\{x_\lambda\}$ of elements k-differentially spans K (resp. is k-differentially independent, is a k-differential basis) iff the collection $\{\mathrm{d}x_\lambda\}$ of its differentials K-linearly spans $\Omega_{K/k}$ (resp. is K-linearly independent, is a K-linear basis). Consequently, $\dep \mathrm{d}^*\mathrm{LD}_K = \dim_K \Omega_{K/k}$.

[3] This uses Exercise 5.10.

5.3 Separability

In this section, we talk about separability of algebras and non-algebraic field extensions. In this section, all algebras are commutative.

Definition 5.3.1. Given a field k, a k-algebra A is called *separable* (over k) if $A_L := A \otimes_k L$ is a reduced ring for every field extension L/k.

Remark 5.3.2. If a k-algebra A is separable, then every k-subalgebra of A is also separable. Since reducedness can be detected at the element level and tensoring over k is exact, we see that A is separable over k iff all of its finitely generated subalgebras are, iff $A \otimes_k L$ is reduced for every finitely generated extension L/k, and iff for any extension K/k, the algebra A_K is separable over K. In the language of algebraic geometry, separability corresponds to geometric reducedness.

For future use, we record one elementary but important fact here as a lemma.

Lemma 5.3.3. Let k be a field, $n \geq 1$ an integer, and $A_1, \ldots, A_n$ be k-algebras. The direct product k-algebra $A_1 \times \cdots \times A_n$ is separable iff each A_i for $i = 1, \ldots, n$ is.

Proof. If the product is separable, then so is each A_i because each A_i is (isomorphic to) a k-subalgebra of the product. For the other direction, check that the tensor product over a field k commutes with taking finite direct product of k-algebras, i.e. for every field extension L/k, the natural map $(A_1 \times \cdots \times A_n)_L \to (A_1)_L \times \cdots \times (A_n)_L$ is an isomorphism of L-algebras. ■

Now let us understand the field extensions which satisfy this definition a little better.

Theorem/Definition 5.3.4 (Separable Field Extensions)**.** For a field extension K/k, the following are equivalent.

(a) The field K is separable as a k-algebra, i.e. for every extension L/k, the ring $K \otimes_k L$ is reduced.
(b) For every finite purely inseparable extension L/k, the ring $K \otimes_k L$ is reduced.
(c) There is a perfect extension L/k such that $K \otimes_k L$ is reduced.
(d) Let $\bar{k}$ be an algebraic closure of k. Then $K \otimes_k \bar{k}$ is reduced.
(e) For every algebraically closed extension Ω of k and for all $n \geq 1$ and k-linearly independent elements $a_1, \ldots, a_n$ of Ω, there are $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}_k(\Omega)$ such that $\det\big(\sigma_i(a_j)\big)_{i,j} \neq 0$.
(f) If $\mathrm{char}\, k = p > 0$, then K and k^{1/p^∞} are linearly disjoint over k.
(g) If $\mathrm{char}\, k = p > 0$, then K and $k^{1/p}$ are linearly disjoint over k.
(h) Every finitely generated subextension of K is separably generated.
(i) For any subfield $k' \subset k$ the map $K \otimes_k \Omega_{k/k'} \to \Omega_{K/k'}$ is injective.
(j) The map $K \otimes_k \Omega_k \to \Omega_K$ is injective.
(k) Any derivation of k to an arbitrary K-vector space M extends to a derivation of K to M.

An extension satisfying these equivalent conditions is said to be a *separable* field extension. Further,

(h) Suppose that $K = k(a_1, \ldots, a_n)$ is finitely generated and separable. Then there is a subset of $\{a_1, \ldots, a_n\}$ that is a separating transcendence basis for K/k.
(i) If K/k is separably generated, then it is separable.
(j) If K/k is algebraic, then the above definition agrees with the usual definition of algebraic

separability, i.e. K/k is separable iff the minimal polynomial over k of any element of K is a separable polynomial.

(k) If K/k is finite, then K/k is separable iff it is étale over k iff the trace pairing on K is perfect (or equivalently nondegenerate).

Remark 5.3.5. From the above theorem, it is clear that in characteristic zero every field extension is separable. It is not true that with the finitely generated hypothesis that a separable extension is separably generated (i.e. that (j) holds); see Example 10.5.7.

Proof.

(a) $\Rightarrow$ (b) Suppose $\operatorname{char} k = p > 0$. It suffices to show that if $L \subset k^{1/p^\infty}$ is any finitely generated subextension, then K and L are linearly disjoint over k. For that, note that L/k is a finite purely inseparable extension and pick an $N \gg 1$ such that $L^{p^N} \subset k$. Since $A := K \otimes_k L$ is a finite-dimensional K-algebra, it is an Artinian ring; since $A^{p^N} \subset K$, it follows that every non-unit of A is nilpotent and hence A is local (Proposition/Definition 1.2.7); since, addition, it is reduced by hypothesis, it follows from Theorem 1.3.9(a) that A is a field, and hence K and L are linearly disjoint over k.

(b) $\Rightarrow$ (c) Clear, since $k^{1/p} \subset k^{1/p^\infty}$.

(c) $\Rightarrow$ (d) If $\operatorname{char} k = 0$, we are done. If $\operatorname{char} k = p > 0$, replace K by this finitely generated extension to assume that K is finitely generated; then we will show (h) using the definition (c) for separability. After relabelling, assume that $a_1, \dots, a_r \in K$ are a transcendence basis for K/k, $a_{r+1}, \dots, a_s \in K$ are separably algebraic over $k(a_1, \dots, a_r)$. We induct on $n - s$. If $n - s = 0$, we are done. Now suppose that $s \leq n-1$ and $y := a_{s+1}$ is not separably algebraic over $k(a_1, \dots, a_r)$. Let $f(Y^p) \in k(a_1, \dots, a_r)[Y]$ be the minimal polynomial of a_{s+1} over $k(a_1, \dots, a_r)$, and minimally clear denominators to get a polynomial $F(X, Y^p) \in k[X,Y] := k[X_1, \dots, X_m, Y]$ such that $F(a_1, \dots, a_r, a_{s+1}^p) = 0$. Now if $\partial F/\partial X_i = 0$ for $1 \leq i \leq r$, then there is a polynomial $G(X,Y) \in k^{1/p}[X,Y]$ such that $F = G^p$; then

$$k[a_1, \dots, a_r, a_{s+1}] \otimes_k k^{1/p} \cong k[X,Y]/(F) \otimes_k k^{1/p} \cong k^{1/p}[X,Y]/(G^p)$$

is a nonreduced subring of $K \otimes_k k^{1/p}$, so $K \otimes_k k^{1/p}$ cannot be a domain, contradicting the linear disjointness hypothesis. Therefore, $\partial F/\partial X_i \neq 0$ for some $1 \leq i \leq r$; after further relabelling, we may assume $\partial F/\partial X_1 \neq 0$. Then a_1 is separable algebraic over $k(a_2, \dots, a_r, a_{s+1})$, and so are $a_{r+1}, \dots, a_s$. For transcendence degree reasons, $a_2, \dots, a_r, a_{s+1}$ must be a transcendence basis for K/k. Setting $a_1' := a_{s+1}$, $A_{s+1} = a_1$ and $a_j' = a_j$ for all $j \neq 1, s+1$. we have reduced $n - s$ by 1, finishing the proof.

(d) $\Rightarrow$ (a) It suffices to assume that K is finitely generated; then it suffices to show (i) using definition (a), i.e. that if K is a separably generated field extension, then K is separable as a k-algebra. Let Γ be a separating transcendence basis for K over k. Now $k(\Gamma) \otimes_k L$ is a ring of fractions of the domain $k[\Gamma] \otimes_k L \cong L[\Gamma]$ and is hence a domain with field of fractions $L(\Gamma)$. Thus

$$K \otimes_k L \cong K \otimes_{k(\Gamma)} (k(\Gamma) \otimes_k L) \hookrightarrow K \otimes_{k(\Gamma)} L(\Gamma),$$

and we are reduced to the case where K/k is separably algebraic. Again we may assume that K is finitely generated, so that K is then finite separable. By the Primitive Element Theorem, $K \cong k[X]/(f)$ for some separable $f \in k[X]$, and then $K \otimes_k L \cong L[X]/(f)$. Now $f \in L[X]$ is still separable, although no longer necessarily irreducible; say $f = \prod_{i=1}^n f_i$

for distinct irreducibles f_i which are pairwise coprime. Then the Chinese Remainder Theorem gives us

$$L[x]/(f) \cong \prod_{i=1}^{n} L[X]/(f_i),$$

which is a finite product of fields and hence reduced.

(c) $\Rightarrow$ (e)

(e) $\Rightarrow$ (f) Take k' to be the prime subfield of k.

(f) $\Leftrightarrow$ (g) Both are equivalent to the surjectivity of $\mathrm{Hom}_K(\Omega_K, M) \to \mathrm{Hom}_K(K \otimes_k \Omega_k, M)$ for each M.

(f) $\Rightarrow$ (c)

(h) This was shown in the proof of the implication (c) $\Rightarrow$ (d).

(i) This was shown in the proof of the implication (d) $\Rightarrow$ (a).

(j) Clear from (d) or (h); one direction of this was also shown in the proof of (d) $\Rightarrow$ (a).

(k) Immediate from Theorem/Definitions 5.3.4 and 5.4.1 below.

■

Corollary 5.3.6. Let $k \subset K \subset L$ be a tower of field extensions.

(a) If L/k is separable, then so is K/k. If, in addition, K/k is algebraic, then L/K is separable as well.

(b) If K/k and L/K are separable, then so is L/k.

Proof.

(a) The separability of K/k is an immediate consequence of Theorem/Definition 5.3.4(c). Suppose now that K/k is algebraic as well.

■

One simple consequence of the above definition is the characterization of fields with only separable extensions.

Theorem/Definition 5.3.7 (Perfect Fields)**.** Let k be a field. Then the following are equivalent:

(a) Either $\mathrm{char}\, k = 0$ or $\mathrm{char}\, k = p > 0$ and $k = k^{1/p}$, i.e. every element of k is a p^{th} power.

(b) Every field extension of k is separable.

(c) Every algebraic extension of k is separable.

(d) Every finite extension of k is separable.

Fields satisfying these equivalent conditions are called *perfect fields*.

Proof. The implication (a) $\Rightarrow$ (b) follows from Theorem 5.3.4(c), and (b) $\Rightarrow$ (c) $\Rightarrow$ (d) are clear. For (d) $\Rightarrow$ (a), suppose $\mathrm{char}\, k = p > 0$. If $x \in k^{1/p} \smallsetminus k$, then the finite extension $k(x)$ of k is not separable. ■

Example 5.3.8. Note that all fields of characteristic zero, all algebraically closed fields, all finite fields, and all algebraic extensions of perfect fields are perfect (the last by Corollary 5.3.6(a)). A simple example of a field that is not perfect is $\mathbf{F}_p(t)$.

Theorem 5.3.9. Let k be a field and X be a geometrically integral k-scheme. Then the field extension $k(X)/k$ is a separable extension and k is algebraically closed in $k(X)$. If X is locally of finite type over k, then $k(X)$ is also finitely generated.

Proof. Replace X by an affine open to assume $X = \operatorname{Spec} A$ for a domain A. It follows from geometric integrality of X that if k'/k is any algebraic extension field, then $A_{k'} = A \otimes_k k'$ is still a domain, and hence so is the localization $k(X) \otimes_k k'$, showing that $k(X)$ and k' are (abstractly) linearly disjoint over k. Applying this to $k' = k^{1/p}$ shows that $k(X)$ is separable over k (Theorem 5.3.4(c)); applying this to $k' = \mathrm{Cl}_{k(X)}(k)$ shows that k is algebraically closed in $k(X)$. If X is locally of finite type over k, then A can be taken to be a finitely generated k-algebra, and then $k(X) = \operatorname{Frac} A$ is a finitely generated extension of k. ■

Remark 5.3.10. Let k be a field and X an integral k-scheme. Consider the following conditions:

(a) X is geometrically integral over k.
(b) The function field $k(X)$ and an algebraic closure $\bar{k}$ are linearly disjoint over k.
(c) The field k is algebraically closed in the function field $k(X)$.

Then (a) $\Leftrightarrow$ (b) $\Rightarrow$ (c). If k is perfect, then all conditions are equivalent.

Indeed, (a) $\Rightarrow$ (b) was proven in Theorem 5.3.9, (b) $\Rightarrow$ (a) is standard algebraic geometry [TOCITE Liu], (b) $\Rightarrow$ (c) is clear from the definitions, and the implication (c) $\Rightarrow$ (b) when k is perfect is Exercise 5.5. Finally, Exercise 5.6 shows that these conditions are not always equivalent if k is not perfect.

Theorem 5.3.11. Let K/k be a finitely generated field extension. Then

$$\operatorname{trdeg}_k K \leq \dim_K \Omega_{K/k} < \infty$$

with equality in the former iff K/k is separable. In this last case, a collection $x_1, \ldots, x_n \in K$ of elements is a separating transcendence basis of K/k iff $\mathrm{d}x_1, \ldots, \mathrm{d}x_n$ form a K-linear basis of $\Omega_{K/k}$.

5.4 Étale Algebras and Grothendieck's Reformulation of Galois Theory

In this section, we study Grothendieck's reformulation of infinite Galois theory over a field k as the computation of the étale fundamental group $\pi_1^{\text{ét}} \operatorname{Spec} k$. For this, the fundamental objects of interest are étale algebras. Again, all algebras in this section are assumed to be commutative.

Theorem/Definition 5.4.1 (Étale Algebras)**.** Let k be a field and $\overline{k}$ a fixed algebraic closure of k with a given embedding $k \hookrightarrow \overline{k}$. For a finite-dimensional algebra A over k, consider the following conditions.

(a) There is an isomorphism of k-algebras $A \cong k[X]/(f)$ for some separable $f \in k[X]$.
(b) A is a finite direct product of finite separable field extensions of k.
(c) A is separable as a k-algebra.
(d) $A_{\overline{k}}$ is a reduced ring.
(e) $A_{\overline{k}}$ is a finite direct product of copies of $\overline{k}$.
(f) The discriminant of one (and hence any) basis of A/k is nonzero.
(g) The trace pairing on A is perfect (or equivalently nondegenerate).

The conditions (b)-(g) are equivalent and implied by (a). If $\dim_k A \leq \#k$ (in particular, if k is infinite), then all conditions are equivalent. A k-algebra A is said to be *étale* over k if it is finite-dimensional, commutative, and satisfies the equivalent conditions (b)-(g).

Proof.

(a) $\Rightarrow$ (b) The irreducible factors of f are all distinct and separable, and hence pairwise coprime; we are done by the Chinese Remainder Theorem.
(b) $\Rightarrow$ (c) Apply Theorem 5.3.4 and Lemma 5.3.3.
(c) $\Rightarrow$ (b) A is Artinian since it is finite-dimensional over k. If A is local, then by Theorem 1.3.9(a), A is a field, and then we are done by Theorem 5.3.4. In general, by Theorem 1.3.9(e), A is a finite direct product of Artinian local rings, and it is easy to see from the proof of that result that if A is a k-algebra, then so is each factor. By Lemma 5.3.3, each factor is separable, and so we are done by the local case.
(c) $\Rightarrow$ (d) Clear from the definition.
(d) $\Rightarrow$ (e) Again, since $A_{\overline{k}}$ is a reduced Artinian ring, we are done by the same argument as in (c) $\Rightarrow$ (b).
(e) $\Rightarrow$ (f) The discriminant is stable under base change, and the discriminant of a finite direct product of copies of $\overline{k}$ is clearly nonzero (take a basis of idempotents).
(f) $\Leftrightarrow$ (g) Clear from the definition of the discriminant and the trace pairing.
(f) $\Rightarrow$ (c) Again, since the discriminant is stable under base change, it suffices to show that if A is a finite-dimensional algebra over a field with nonzero discriminant, then A is reduced. Suppose $n := \dim_k A$ and let $r := \dim_k \sqrt{0A}$; suppose instead that $1 \leq r \leq n$. Pick an (ordered) k-basis $\alpha_1, \ldots, \alpha_n$ of A such that $\alpha_1, \ldots, \alpha_r$ form a basis for $\sqrt{0A}$. 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 $[\operatorname{Tr}_k^A(\alpha_i \alpha_j)]_{ij}$ has its first r rows and columns identically zero, so if $r \geq 1$, it cannot have nonzero determinant.
(b) $\Rightarrow$ (a), when $\dim_k A \leq \#k$. Find an integer $n \geq 1$ and finite separable field extensions $K_1, \ldots, K_n$ of k such that $A \cong \prod_{i=1}^n K_i$. For each $i = 1, \ldots, n$, use the Primitive Element Theorem to pick monic irreducible $f_i \in k[X]$ so that $K_i \cong k[X]/(f_i)$, ensuring that each new f_i is not

equal to f_j for $j < i$. 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 there are at least $(n-1)$ different choices for a by hypothesis and that if $f \in k[X]$ is irreducible, then the $\{f(X+a)\}_{a\in k^\times}$ are irreducible and pairwise coprime. Then the polynomials f_i are irreducible, separable, and pairwise coprime, and we may take $f = \prod_{i=1}^n f_i$.

■

The hypothesis that $\dim_k A \leq \#k$ in the implication (b) $\Rightarrow$ (a) is necessary; see Exercise 5.11.

Finally, we want to mention that the ddecomposition of an étale algebra as a product of field extensions is essentially unique; this is a consequence of the following general observation.

Lemma 5.4.2. Let k be a field, $n \geq 1$ an integer and $K_1, \ldots, K_n$ field extensions of k. Let $A := \prod_{i=1}^n K_i$ be their product.

(a) Given a k-algebra B and a surjective k-algebra morphism $\varphi : A \to B$, the map φ can be decomposed as a projection onto a subproduct followed by an isomorphism.
(b) Further, if B is a field extension of k, then the projection map is a projection onto a single factor. In particular, we have

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

(c) If $m \geq 1$ is another integer and $L_1, \ldots, L_m$ field extensions of k with $B = \prod_{j=1}^m L_j$, then

$$\mathrm{Hom}_k(A,B) \cong \coprod_{i,j} \mathrm{Hom}_k(K_i,L_j).$$

(d) In particular, $A \cong B$ iff $n = m$ and there is a permutation $\sigma : [n] \to [n]$ such that $K_i \cong L_{\sigma(i)}$ as k-algebras for $i = 1, \ldots, n$.

Proof.

(a) The projection of the kernel to each K_i is an ideal of K_i.
(b) The image of A in B is a k-subalgebra of a field, and hence an integral domain.
(c) Follows from $\mathrm{Hom}_k(A,B) \cong \prod_{j=1}^m \mathrm{Hom}_k(A,L_j)$ combinted with (b).
(d) Clear from (c): note that n is determined as the number of inequivalent idempotents of A, and projections $\prod_i K_i \twoheadrightarrow L_j$ and $\prod_j L_j \twoheadrightarrow K_i$ show that each K_i is isomorphic to some L_j.

■

Now suppose k is a field, and we fix an embedding $k \hookrightarrow \overline{k}$ as above. Let k^s denote the separable closure of k in $\overline{k}$, so $k \subset k^s \subset \overline{k}$. If L/k is any finite separable extension, then $\#\mathrm{Hom}_{k\text{-}\mathsf{Alg}}(L,k^s) = [L:k]_s = [L:k] < \infty$, and so $X_L := \mathrm{Hom}_{k\text{-}\mathsf{Alg}}(L,k^s)$ is a finite set.[4] The absolute Galois group $G_k = \mathrm{Gal}(k^s/k)$ acts on X_L by postcomposition, and for each $\varphi \in X_L$, the stabilizer $(G_k)_\varphi = \mathrm{Gal}(k^s/\varphi(L))$ is an open subgroup of G_k by the Fundamental Theorem of Infinite Galois Theory, and so X_L is a discrete G_k-set (see Exercise 5.13). Finally, this

[4] In the terminology of algebraic geometry, this is the set $X_L = \mathrm{Spec}(L)(k^s)$ of k^s-valued points of the geometrically reduced separated finite-type k-scheme (i.e. k-variety) $\mathrm{Spec}(L)$ in the category of k-schemes.

action is transitive by the extension property of homomorphisms from algebraic extensions to algebraically closed fields. In conclusion, X_L is a left coset space for some open subgroup in G_k. When L/k is Galois, X_L is isomorphic to a quotient of G_k by an open normal subgroup, namely $\mathrm{Gal}(k^s/\varphi(L))$ for one (and hence any) $\varphi \in X_L$. If K and L are two finite separable extensions and $\theta : K \to L$ a k-homomorphism, then we get a pullback map $\theta^* : X_L \to X_K$, which is clearly a G_k-set morphism.

Theorem 5.4.3. In the above set-up, the association $L \mapsto X_L$ gives an antiequivalence between the categories of finite separable extensions L/k and transitive finite (left) G_k-sets. Further, Galois extensions correspond to finite quotients of G_k.

Proof. For essential surjectivity, let X be a transitive finite left G_k-set, and pick an $x \in X$. By Exercise 5.13, the stabilizer of x in G_k is an open subgroup, and so by the Fundamental Theorem of Infinite Galois Theory is of the form $\mathrm{Gal}(k^s/L)$ for some finite separable subextension L/k of k^s. Let $\iota : L \hookrightarrow k^s$ be the inclusion; then the map $X_L \to X$ given by $g\iota \mapsto gx$ is an isomorphism of G_k-sets.

It remains to show that if $K, L/k$ are finite separable extensions, then the map

$$-^* : \mathrm{Hom}_k(K,L) \to \mathrm{Hom}_{G_k}(X_L, X_K)$$

is a bijection. For this, we construct an inverse. Fix an $\iota \in X_L$; then a G_k-homomorphism $\eta : X_L \to X_K$ determines and is determined by the element $\eta(i) \in X_K$ by transitivity. If η is a G_k-homomorphism, then $\mathrm{Gal}(k^s/\iota(L)) = (G_k)_\iota \subset (G_k)_{\eta(\iota)} = \mathrm{Gal}(k^s/\eta(\iota)(K))$, so by the Fundamental Theorem we get $\iota(L) \supset \eta(\iota)(K)$. The composite $\theta_\eta : K \xrightarrow{\eta(\iota)} \iota(L) \xrightarrow{\iota^{-1}} L$ is a k-algebra homomorphism with $\theta_\eta^* = \eta$. Checking that this construction gives inverse bijections is left to the reader. ∎

We can now ask what all the finite left G_k-sets are, not necessarily transitive ones. Note that if A is an étale k-algebra, then $X_A := \mathrm{Hom}_{k\text{-}\mathsf{Alg}}(A, k^s)$ is also a left G_k-set. If we pick n and K_i as in Lemma 5.4.2 as given by Theorem/Definition 5.4.1(b), the decomposition in Lemma 5.4.2(b) of the form

$$X_A \cong \coprod_{i=1}^n X_{K_i}$$

is an isomorphism of G_k-sets. In particular, X_A is a finite left G_k set. The main theorem we are after here says exactly that these are, in fact, all.

Theorem 5.4.4 (Fundamental Theorem of Galois Theory, Grothendieck's Version)**.** The association $A \mapsto X_A$ gives an antiequivalence between the categories of étale algebras A/k and finite left G_k-sets. Further,

(a) separable field extensions correspond to transitive finite left G_k-sets, and
(b) Galois extensions correspond to finite quotients of G_k.

Proof. Again, for essential surjectivity, let X be a finite left G_k-set, and decompose it into its G_k-orbits: pick an integer $n \geq 1$ and G_k-invariant subsets $X_1, \ldots, X_n \subset X$ such that $X = \coprod_{i=1}^n X_i$ and the action of G_k on each X_i is transitive. For each $i = 1, \ldots, n$, by Theorem 5.4.3, there is a finite separable extension K_i/k and a G_k-set isomorphism $X_{K_i} \to X_i$. Taking $A = \prod_{i=1}^n K_i$, it follows that the composition

$$X_A \cong \coprod_{i=1}^n X_{K_i} \xrightarrow{\sim} \coprod_{i=1}^n X_i = X$$

is a G_k-set isomorphism. Similarly, to show full faithfulness, suppose we have étale k-algebras A, B, and we pick n, m, K_i and L_j as in Lemma 5.4.2 so $A \cong \prod_{i=1}^{n} K_i$ and $B \cong \prod_{j=1}^{m} L_j$. Then we get G_k-set isomorphisms

$$\mathrm{Hom}_{k\text{-}\mathsf{Alg}}(A,B) \cong \coprod_{i,j} \mathrm{Hom}_k(K_i, L_j) \xrightarrow{\sim} \coprod_{i,j} \mathrm{Hom}_{G_k}(X_{L_j}, X_{K_i}) \cong \mathrm{Hom}_{G_k}(X_B, X_A),$$

where we are using Lemma 5.4.2(c), Theorem 5.4.3, and that a G_k-set morphism $X_B \to X_A$ must preserve the decomposition into G_k-orbits. Everything else is clear from Theorem 5.4.3. ■

As remarked earlier, this theorem amounts to the computation $\pi_1^{\text{ét}} \mathrm{Spec}(k) \cong G_k$.

5.5 Exercises

Exercise 5.1. Suppose we have field extensions $k \subset K, L \subset \Omega$ as in Proposition/Definition 5.1.1. Show that if either K or L is algebraic over k, then $K[L] = KL$, i.e. that the smallest subring of Ω containing K and L is a field. Come up with an example of fields k, K, L, and Ω as above for which $K[L] \subsetneq KL$.

Exercise 5.2.

(a) Let K, L be finite extensions of a field k such that $[K : k]$ and $[L : k]$ are relatively prime. Show that K and k are linearly disjoint over k.
(b) Show that $f(X) := X^5 + 4X^3 + 6X + 14 \in \mathbf{Q}[\sqrt{5}, \cos(2\pi/7)][X]$ is irreducible.

Exercise 5.3. Suppose $k \subset \Omega$ is a field extension, and that $k \subset K, L \subset \Omega$ intermediate *domains*. We say that K and L are linearly disjoint over k in Ω iff the natural map $K \otimes_k L \to \Omega$ is injective. Show that K and L are linearly disjoint over k in Ω iff their fraction fields $\operatorname{Frac} K$ and $\operatorname{Frac} L$ are
.

Exercise 5.4. Show that if k is a field and $K, L \supset k$ two extension fields, then there is a field extension of k containing k-isomorphic copies of K and L.

Exercise 5.5. Partially generalize Theorem 5.1.3 as follows. Let k be a field and K/k be any extension such that k is algebraically closed in K. If L/k is a Galois extension (e.g. if k is perfect and L is an algebraic closure of k), then K and L are linearly disjoint over k.

Exercise 5.6. Let $\mathbf{F}$ be any imperfect field, so that $p := \operatorname{char} \mathbf{F} > 0$, and pick an $s \in \mathbf{F} \smallsetminus \mathbf{F}^p$. Let $k := \mathbf{F}(t)$.

(a) Show that $X^p + sY^p + t \in k[X, Y]$ is irreducible.

Let $K := \operatorname{Frac} k[X, Y]/(X^p + sY^p + t)$. Let $k \to L$ be an algebraic closure of k, let $K \to \Omega$ be an algebraic closure of K, and extend the natural map $k \to K \to \Omega$ to an inclusion $L \to \Omega$. In what follows, identify k, K, and L with their images in Ω.

(b) Show that $K \cap L = k$ (i.e. k is algebraically closed in K), but that K and L are not linearly disjoint over k in Ω. In particular, K and $L \cong \overline{k}$ are not abstractly linearly disjoint over k.

Exercise 5.7. Let $k \subset K \subset L$ be a tower of field extensions. Show that $\operatorname{trdeg}_k L = \operatorname{trdeg}_k K + \operatorname{trdeg}_K L$.

Exercise 5.8. Let k be a field, and $K, L \supset k$ be two extension fields of k. Show that if K and L are everywhere linearly disjoint over k, then one of K or L is algebraic over k.

Exercise 5.9. Let k be a field and $K, L \supset k$ be two algebraic extensions of k. Show directly (i.e. without quoting Theorem 5.1.3) that if K is separable and L is purely inseparable, then K and L are linearly disjoint over k.

Exercise 5.10. Let k be a field and $f(X) \in k[X]$ be a polynomial such that for every field extension K of k, if f has a root in K then f splits over K. Show that all irreducible factors of f have the same degree. In particular, if in addition f has prime degree and does not have a root in k, then f is irreducible over k.

Exercise 5.11. Show that the étale $\mathbf{F}_2$-algebra $A = \mathbf{F}_2^3$ is not isomorphic to $\mathbf{F}_2[X]/(f)$ for any $f \in \mathbf{F}_2[X]$.

Exercise 5.12. Let G be a profinite group and $n \geq 1$ an integer. Show that any continuous homomorphism $\rho : G \to \mathrm{GL}_n \mathbf{C}$ factors through a finite quotient of G.

Exercise 5.13. Let G be a topological group acting on a set X. Show that the following are equivalent:

(a) The action of G on X is continuous for the discrete topology on X.
(b) For each $x \in X$, the stabilizer $G_x \subset G$ of x in G is an open subgroup of G.
(c) Every element $x \in X$ is stabilized by some open subgroup $U_x \subset G$, i.e. $X = \bigcup_{U \leq G} X^U$, where the union is over open subgroups $U \leq G$.

In this situation, we call X a *discrete G-set*.

Chapter 6

Dimension Theory

6.1 Noether Normalization and Zariski's Lemma

The main theorem of this section is:

Theorem 6.1.1 (Noether Normalization)**.** Let R be a finitely generated commutative k-algebra with k a field. Then there exists an integer $r \geq 0$ and elements $z_1, \ldots, z_r \in R$ such that:

(a) The z_i's are algebraically independent over k, i.e. the map $k[Z_1, \ldots, Z_r] \to R$ given by $Z_j \mapsto z_j$ for $j = 1, \ldots, r$, is injective.
(b) R is integral over the image $k[z_1, \ldots, z_r]$.

Finally, if k is infinite, and we express R as $R \cong k[x_1, \ldots, x_n] = k[X_1, \ldots, X_n]/\mathfrak{a}$ for some integer $n \geq 0$ and ideal $\mathfrak{a} \subset k[X_1, \ldots, X_n]$, then the z_i can be chosen to be linear combinations of the x_i.

Proof. 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 any generating set, say $\{x_i\}_{i=1}^n$ if we are in the second situation). Either the z_i are algebraically independent, and we are done; or, $r \geq 1$ and there is a $0 \neq f \in k[Z_1, \ldots, Z_r]$ such that $f(z_1, \ldots, z_r) = 0$. As explained below, we can replace Z_j for $1 \leq j < r$ by Z'_j such that $k[Z_1, \ldots, Z_r] = k[Z'_1, \ldots, Z'_{r-1}, Z_r]$ 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 $k[z'_1, \ldots, z'_{r-1}]$, where each z'_j is the image of Z'_j, and then by Corollary 4.1.4(c), R would be integral over $k[z'_1, \ldots, z'_{r-1}]$. 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.

For the transformation steps, first assume that k is infinite. Set $Z'_j := Z_j - \alpha_j Z_r$ for $1 \leq j < r$ for $\alpha_1, \ldots, \alpha_{r-1} \in k$ to be determined later. 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 nonzero polynomial in $k[\alpha_j]_{j=1}^{r-1}$ and k is infinite, we can choose $\alpha_1, \ldots, \alpha_{r-1}$ 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, so scaling by c^{-1}, we are done.

In the general case, consider integers ("weights") $w_1, \ldots, w_{r-1} \geq 0$ to be specified later, and set $w_r = 1$. Set $Z'_j := Z_j - Z_r^{w_j}$ for $1 \leq j < r$. In a typical monomial $c_I Z^I$ in f after substitution, we get a term of the form $c_I \left(\prod_{j=1}^{r-1} (Z'_j + Z_r^{w_j})^{i_j} \right) Z_r^{i_r}$. 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 pick the w_j in such a way that all of these sums over varying I are 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 6.1.2 below. ∎

Lemma 6.1.2. Suppose that $r \geq 1$ is an integer, and $\mathcal{S} = \{(i_1, \ldots, i_r) : i_1, \ldots, i_r \geq 0\}$ a *finite* set of ordered r-tuples of nonnegative integers. Then there are nonnegative integers $w_1, \ldots, w_{r-1}, w_r$, such that $w_r = 1$ and if $I \neq I' \in \mathcal{S}$ then $\sum_{j=1}^r i_j w_j \neq \sum_{j=1}^r i'_j w_j$.

Proof. Proceed by induction on r, with $r = 1$ clear. If $r \geq 2$, then by induction choose $w_2, \ldots, w_{r-1}, w_r \geq 0$ with $w_r = 1$ such that $\sum_{j=2}^r i_j w_j = \sum_{j=2}^r i'_j w_j \Rightarrow I = I'$. Now choose $w_1 > \max_{I \in \mathcal{S}} \{\sum_{j=2}^r i_j w_j\}$. ∎

Remark 6.1.3. 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 6.1.4. If in addition R is an integral domain, then $r = \mathrm{trdeg}_k R$.

Proof. The integral closure $\mathrm{Cl}_{\mathrm{Frac}\,R}(k(z_1,\ldots,z_n)) \subset \mathrm{Frac}\,R$ is a field by Lemma 4.1.8(c) and contains R, so it must be $\mathrm{Frac}\,R$. Therefore, $z_1,\ldots,z_r \in \mathrm{Frac}\,R$ is a transcendence basis and $\mathrm{trdeg}_k \mathrm{Frac}\,R = r$. ■

Remark 6.1.5. We will show below [TOCITE] that for $r \in \mathbf{Z}_{\geq 0}$ that $\dim k[Z_1,\ldots,Z_r] = r$. It will then follow from Corollary 4.2.6(a) that $\dim R = r$ as well. In all, this will show that if R is a finitely generated commuative k-algebra for some field k that is an integral domain, then $\dim R = \mathrm{trdeg}_k R$.

Now we derive plenty of delicious consequences. We begin with useful lemma.

Lemma 6.1.6 (Artin-Tate Lemma)**.** Let $R \subset S \subset T$ 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 $m,n \geq 1$ be integers such that we can pick generators $x_1,\ldots,x_m$ of T as an R-algebra, and $y_1,\ldots,y_n$ of 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 (Theorem 1.3.5). Any element of T is a polynomial in the x_i with coefficients in R; substituting the above, we see that T is generated as an S'-module by the y_j; in particular, it is module-finite over S'. Since S' is Noetherian and S is a submodule of the finitely generated S'-module T, the ring 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. ■

Remark 6.1.7. Here is one historically significant application of the Artin-Tate Lemma: the construction of quotient varieties. Let k be a field, $n \geq 1$ an integer and G a finite group acting on a finitely generated k-algebra T, and we are interested in studying the G-invariants T^G. Lemma 6.1.6 applied to $R = k$ and $S = T^G$ says that the ring S of invariants is finitely generated.[1] A closer examination of the proof, however, reveals that it is not constructive; a variant of this proof in this special case, essentially due to Noether and Hilbert, was the impetus behind the development of a lot of commutative algebra (including the definition of Noetherian ring and the Hilbert Basis Theorem), and initially got Hilbert under fire (Gordan denounced this proof as "theology, not mathematics!") [TOCITE]. It was a long time before this proof technique, and nonconstructive techniques in commutative algebra, became mainstream.

We now come to one of the most fundamental results of the algebraic theory of dimension, of which we give five proofs.

Theorem 6.1.8 (Zariski's Lemma)**.** Let $k \subset K$ be a field extension. If K is a finitely generated k-algebra, then it is a finite algebraic extension.

[1] In modern algebraic geometry, this is saying that the quotient of the finitely generated affine k-scheme $\mathrm{Spec}(T)$ by the action of G is still of the same type, i.e., a geometric quotient of $\mathrm{Spec}(T)$ by G exists in this category. It is also clear that if T is reduced, then so is T^G: the quotient of an affine k-variety by a finite group G is also one.

Proof 1. Induct on $n \in \mathbf{Z}_{\geq 0}$, the minimal number of generators of K as a k-algebra, the case $n = 0$ being trivial. Suppose $n \geq 1$ and $K = k[x_1, \ldots, x_n]$ for some $x_1, \ldots, x_n \in K$. If K is not algebraic over k, at least one of the x_i, say x_1, is not algebraic over k. Then $k(T) \cong k(x_1) \subset K$, and K is generated as a $k(x_1)$ algebra by $x_2, \ldots, x_n$, so by induction $x_2, \ldots, x_n$ 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 $fx_2, \ldots, fx_r$ 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.[2] Then $1/g \in k(x_1) \subset K = k[x_1, \ldots, x_n]$ implies that there is an $N \gg 1$ such that $f^N/g \in k[x_1, fx_2, \ldots, fx_n]$. Then $f^N/g \in k(x_1)$ is integral over $k[x_1]$. But $k[x_1]$ is a UFD and hence normal (Example 4.1.5), so $f^N/g \in k[x_1]$, i.e. $f^N = gh$ for some $h \in k[x_1]$, a contradiction. ■

Proof 2. Let $K = k[x_1, \ldots, x_n]$. If K is not algebraic over k, then $n \geq 1$ we may reorder the x_i to arrange that $x_1, \ldots, x_r$ are algebraically independent over k for some $r \geq 1$ and that each of $x_{r+1}, \ldots, x_n$ are algebraic over $k(x_1, \ldots, x_r)$. Applying Lemma 6.1.6 to $R = k, S = k(x_1, \ldots, x_r), T = K$, it follows that the purely transcendental extension $k(x_1, \ldots, x_r)$ is a finitely generated k-algebra, say $k(x_1, \ldots, x_r) = k[y_1, \ldots, y_s]$ for some $s \geq 1$. Then each $y_i = f_j/g_j$ for some polynomials f_j, g_j in $x_1, \ldots, x_r$. Since there are infinitely many irreducible polynomials in $k[x_1, \ldots, x_n]$, we may pick an irreducible $g \in k[x_1, \ldots, x_n]$ that does not divide $g_1 \cdots g_s$. Then the element $g^{-1} \in k[y_1, \ldots, y_s]$ implies that g^{-1} is polynomial in $y_1, \ldots, y_s$, 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 $k \subset k[z_1, \ldots, z_r] \subset K$ where the first extension is polynomial and the second extension is integral. But from Lemma 4.1.8(c), we get that since K is a field, so must be $k[z_1, \ldots, z_r]$. This is only possible if $r = 0$. ■

Proof 4. Taking $R = k$, $S = K$, and $\varphi : k \hookrightarrow \Omega$ an algebraic closure of k, in Lang's Lemma (Theorem 4.3.1(b)) gives an extension $\hat{\varphi} : K \to \Omega$. Since K is a field, this last homomorphism is injective, and so K is algebraic over k. Since it is a finitely generated k-algebra, it is finite algebraic. ■

Finally, we record a more "geometric" proof of this result as well, which uses a little more algebraic geometry.

Proof 5. If K is not algebraic over k, then there is an inclusion $k[X] \hookrightarrow K$ of the polynomial ring $k[X]$ into K. This gives rise to a dominant morphism $\pi : \operatorname{Spec} K \to \mathbf{A}^1_k$ of finite-type k-schemes. By Chevalley's Theorem, the image of π is constructible, but the image of π is the generic point of $\mathbf{A}^1_k$, which is *not* constructible. ■

[2] For instance, by the same argument as the infinitude of primes.

6.2 Some Classical Algebraic Geometry

6.2.1 The Classical Nullstellensatz

In classical algebraic geometry, we look at the vanishing loci of polynomials in affine space.

Definition 6.2.1. For an integer $n \geq 1$ and ring k, the *k-points of affine n-space* is the set

$$\mathbf{A}^n(k) = \{(a_1, \ldots, a_n) : a_i \in k\}$$

of ordered n-tuples of elements of k.

In what follows, we fix an $n \in \mathbf{Z}_{\geq 1}$. In modern algebraic geometry, this is the set of k-points of the universal affine n-space $\mathbf{A}^n_{\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[X_1, \ldots, X_n]$. In classical algebraic geometry, in the absence of the notion of Spec, this was the geometric space on which algebraic geometry was done. Here's a version that we will set up.

Fix a field k and an algebraic closure $\overline{k}$ of k. Associate to each subset $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ its vanishing locus $\mathbf{V}(\mathfrak{a}) \subset \mathbf{A}^n(\overline{k})$, and to each subset $X \subset \mathbf{A}^n(\overline{k})$ the ideal $\mathbf{I}(X) \subset k[X_1, \ldots, X_n]$ of polynomials over k vanishing on it. Then with this notation we have

Theorem 6.2.2 (Hilbert's Nullstellensatz)**.**

(a) If $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ is a proper ideal, then $\mathbf{V}(\mathfrak{a}) \neq \emptyset$.
(b) If $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ is any ideal, then $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Proof.

(a) Since $\mathfrak{a}$ is proper, there is a maximal ideal $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ containing $\mathfrak{a}$. Then $\mathbf{V}(\mathfrak{m}) \subset \mathbf{V}(\mathfrak{a})$. Therefore, it suffices to do the case when $\mathfrak{a}$ is maximal. In this case, the quotient $K := k[X_1, \ldots, X_n]/\mathfrak{a}$ is a field extension which is a finitely generated k-algebra, and hence by Zariski's Lemma 6.1.8, it is a finite algebraic extension. In particular, there is a k-embedding $\varphi : K \to \overline{k}$, and then the point $(\varphi(\overline{X}_1), \ldots, \varphi(\overline{X}_n)) \in \mathbf{V}(\mathfrak{a}) \subset \mathbf{A}^n(\overline{k})$.
(b) The inclusion $\sqrt{\mathfrak{a}} \subset \mathbf{I}(\mathbf{V}(\mathfrak{a}))$ is clear. For the other direction, we use the *Rabinowitsch trick*: if $f \in \mathbf{I}(\mathbf{V}(\mathfrak{a}))$, then in $k[X_1, \ldots, X_{n+1}]$, the ideal $\mathfrak{b} := (\mathfrak{a}, f \cdot X_{n+1} - 1)$ has the property that $\mathbf{V}(\mathfrak{b}) = \emptyset$. By (a), $\mathfrak{b} = (1)$. Therefore,

$$0 = k[X_1, \ldots, X_n]/\mathfrak{b} \cong (k[X_1, \ldots, X_n]/\mathfrak{a})\,[X_{n+1}]/(\overline{f} \cdot X_{n+1} - 1) \cong (k[X_1, \ldots, X_n]/\mathfrak{a})\,[\overline{f}^{-1}],$$

which by Example 1.1.4 gives us that $\overline{f} \in \operatorname{Nil}(k[X_1, \ldots, X_n]/(\mathfrak{a}))$ as needed.

■

Corollary 6.2.3. Suppose that $k = \overline{k}$, i.e., that k is algebraically closed. Then there is a bijection between $\mathbf{A}^n(k)$ and the maximal ideals of $k[X_1, \ldots, X_n]$, given by sending a point $(a_1, \ldots, a_n)$ to the ideal $(X_1 - a_1, \ldots, X_n - a_n)$.

Proof. This map is clearly well-defined and injective. For an arbitrary maximal ideal $\mathfrak{m} \subset k[X_1, \ldots, X_n]$, as in Theorem 6.2.2(a), the quotient $K = k[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite algebraic extension of k. Since k is algebraically closed, this means that the natural map $k \to k[X_1, \ldots, X_n]/\mathfrak{m}$ is an isomorphism. For $i = 1, \ldots, n$, if the element $a_i \in k$ maps to the class of X_i in K, then $\mathfrak{m} \supset (X_1 - a_1, \ldots, X_n - a_n)$; but the latter is already a maximal ideal. ■

In fact, the above set-up can be used to give an antitone Galois connection between the k-subvarieties of $\mathbf{A}^n(\bar{k})$ and radical ideals in $k[X_1,\dots,X_n]$; but that belongs properly to a course on classical algebraic geometry. This observation is also the starting point of modern algebraic geometry, which systematically studies not only maximal ideals of polynomial rings over a field but rather all prime ideals of arbitrary rings as its "points".

6.2.2 Jacobson Rings

The Nullstellensatz implies that (when k is algebraically closed) for any ideal $\mathfrak{a} \subset k[X_1,\dots,X_n]$ we have $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{m}\supset\mathfrak{a}} \mathfrak{m}$ (check!). We call rings with this property *Jacobson rings*; this is developed systematically in

Theorem/Definition 6.2.4 (Jacobson Rings)**.** The following conditions on a ring R are equivalent:

(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.
(c) Every prime ideal in R is the intersection of maximal ideals.
(d) If S is a domain quotient of R and there is a $0 \neq x \in S$ such that $S[x^{-1}]$ is a field, then S is a field.
(e) Every finitely generated algebra over R that is a field is finitely generated as an R-module.

A ring satisfying the above equivalent conditions is said to be a *Jacobson ring*. In this situation:

(f) If S is a finitely generated R-algebra by $\varphi : R \to S$, then S is also Jacobson. Further, if $\mathfrak{m} \subset S$ is maximal, then so is $\varphi^{-1}\mathfrak{m} \subset R$ and hence $S/\mathfrak{m}$ is a finite algebraic extension of $R/\varphi^{-1}\mathfrak{m}$.

Remark 6.2.5. Geometrically, a morphism of Jacobson schemes which is locally of finite type (e.g., that of varieties over a field) maps closed points to closed points; this fact enabled classical algebraic geometers to stick to closed points in their interpretation of the *geometry* of algebraic geometry.

Proof.

(a) $\Rightarrow$ (b) Let $\mathfrak{a} \subset R$ be a radical ideal. Then in $R/\mathfrak{a}$ we have $0 = \mathrm{Nil}(R/\mathfrak{a}) = \mathrm{Jac}(R/\mathfrak{a}) = \bigcap_{\mathfrak{m}\subset R/\mathfrak{a}} \mathfrak{m}$, so in R we have $\mathfrak{a} = \bigcap_{\mathfrak{m}\supset\mathfrak{a}} \mathfrak{m}$.

(b) $\Rightarrow$ (c) Clear.

(c) $\Rightarrow$ (a) If $\mathfrak{a} \subset R$ is any ideal, then $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\supset\mathfrak{a}} \mathfrak{p} = \bigcap_{\mathfrak{m}\supset\mathfrak{a}} \mathfrak{m}$, where the first statement is Theorem 1.2.2, and the second uses the hypothesis (c). Therefore, $\mathrm{Nil}(R/\mathfrak{a}) = \sqrt{0(R/\mathfrak{a})} = \bigcap_{\mathfrak{m}\subset R/\mathfrak{a}} \mathfrak{m} = \mathrm{Jac}(R/\mathfrak{a})$.

(c) $\Rightarrow$ (d) Let $\mathfrak{p} := \ker(R \to S)$, and lift x to an $\tilde{x} \in R \smallsetminus \mathfrak{p}$. By hypothesis, there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ but not $\tilde{x}$; this corresponds to a maximal ideal of S not containing x and hence by Corollary 1.1.12(d) a proper prime ideal of $S[x^{-1}]$, which must be (0); therefore, $\mathfrak{p} = \mathfrak{m}$.

(d) $\Rightarrow$ (c) We have to show that given a prime $\mathfrak{p}$ and $x \notin \mathfrak{p}$, there is a maximal $\mathfrak{m}$ containing $\mathfrak{p}$ such that $x \notin \mathfrak{m}$. In this case, $(R/\mathfrak{p})[x^{-1}]$ is not the zero ring and therefore 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) applied to $S = R/\mathfrak{m}$, we conclude that $\mathfrak{m}$ is maximal.

(d) $\Rightarrow$ (e) Suppose that K is a field and a finitely generated R-algebra via $\varphi : R \to K$. Replacing R by $R/\ker\varphi$, we may assume that R is a domain; let $k := \operatorname{Frac} R$. Since K is a finitely generated R-algebra, it is also a finitely generated k-algebra, so by Zariski's Lemma (Theorem 6.1.8), 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 $0 \neq x \in R$ of the coefficients so that $R[x^{-1}] \hookrightarrow K$ is an integral extension. By Lemma 4.1.8(c), $R[x^{-1}]$ is a field, so that by hypothesis $R = k$. Since K/k is finite, we are done.

(e) $\Rightarrow$ (d) Let S and x be as given. Since $S[x^{-1}]$ is a finitely generated R-algebra that is a field, by (e) it 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 $S = S[x^{-1}]$ is a field.

(f) The ring S clearly satisfies (e). Finally, if $\mathfrak{m} \subset S$ is maximal, then $S/\mathfrak{m}$ is a finitely generated R-algebra that is a field, so by (e) again $S/\mathfrak{m}$ is integral over R. Then $R/\varphi^{-1}\mathfrak{m} \subset S/\mathfrak{m}$ is an integral extension of domains with $S/\mathfrak{m}$ a field, so by Lemma 4.1.8(d), $\varphi^{-1}\mathfrak{m}$ is maximal.

■

Example 6.2.6.

(a) Fields and hence finitely generated algebras over fields are Jacobson; this is the classical Nullstellensatz.

(b) A Dedekind domain is Jacobson iff it has infinitely many prime ideals (Exercise 6.1). In particular, if K is a number field, then $\mathcal{O}_K$ is a Jacobson ring.

(c) A local domain that is not a field is not Jacobson; see also Exercise 6.2.

6.2.3 Dimension of Affine Varieties

Let us now return to a little bit of dimension theory. The first promised result is

Theorem 6.2.7. Let k be a field and $n \in \mathbf{Z}_{\geq 0}$. Then $\dim k[X_1, \ldots, X_n] = n$.

6.3 Hilbert-Samuel Polynomials

6.4 The Main Theorem of Dimension Theory and Regular Rings

6.5 Krull's Hauptidealsatz Revisited

6.6 Systems of Parameters, Regular Sequences, Depth, and Cohen-Macaulay Rings

6.7 Exercises

Exercise 6.1. Show that a Dedekind domain is a Jacobson ring iff it has infinitely many prime ideals.

Exercise 6.2. Show that a local ring is a Jacobson ring iff it has Krull dimension zero.

Chapter 7

Valuation Rings and Dedekind Domains

7.1 Valuation Rings and Discrete Valuation Rings

An abelian group Γ with a translation-invariant total order $\leq$ is said to be an *ordered abelian group*; to such a group we associate an ordered abelian monoid $\Gamma^+ := \Gamma \sqcup \{\infty\}$ by defining $\infty + \xi = \infty$ and $\xi \leq \infty$ for all $\xi \in \Gamma$.

Definition 7.1.1. Let R be a domain, and Γ be an ordered abelian group.

(a) A Γ-*valued valuation on* R is a monoid homomorphism $v : (R, \cdot) \to \Gamma^+$ satisfying that for $x \in R$ we have $v(x) = \infty$ iff $x = 0$, and for all $x, y \in R$ we have

$$v(x+y) \geq \min\{v(x), v(y)\}.$$

In the above situation, v can be uniquely extended to a Γ-valued valuation on the fraction field $K := \operatorname{Frac} R$ by $v(x/y) = v(x) - v(y)$ whenever $x, y \in R$ with $y \neq 0$. Therefore, it suffices to talk about valuations on fields.

(b) Suppose K is a field and $v : K \to \Gamma^+$ is a valuation. Then we define the *value group* of v to be the subgroup $v(K^\times) \subset \Gamma$, the *valuation ring* of v to be

$$\mathcal{O}_v := \{x \in K : v(x) \geq 0\},$$

and the *maximal ideal* to be

$$\mathfrak{m}_v := \{x \in R : v(x) > 0\}.$$

(c) A valuation $v : K \to \Gamma$ is said to be a *discrete valuation* if the value group of v is isomorphic to $\mathbf{Z}$ as an ordered abelian group; in this case, identifying the value group with $\mathbf{Z}$, we say that an element $\pi \in K$ is a *uniformizing parameter*, or *uniformizer*, if $v(\pi) = 1$ (i.e. if $v(\pi) > 0$ is a generator of the value group).

Remark 7.1.2. If Γ is any ordered abelian group, then there is a field K and a Γ-valued valuation on K with value group Γ; in fact, K can be chosen to be of any characteristic, and indeed $K = \operatorname{Frac} k[\Gamma]$ suffices for any base field k. See [4, Exercise 5.33]. For a suitable choice of Γ, this can be used to construct a nonempty scheme with no closed points. See [10, Exercise 3.3.27].

Remark 7.1.3. It is easy to check (do!) that in (b) above, given $x \in K^\times$ we have $v(x^{-1}) = -v(x)$, we have $x \in \mathcal{O}_v^\times$ iff $v(x) = 0$, and that $\mathfrak{m}_v = \mathcal{O}_v \smallsetminus \mathcal{O}_v^\times$ is an ideal, so by Proposition/Definition 1.2.7, the nomenclature above is justified: $\mathcal{O}_v$ is a local domain with the unique maximal ideal $\mathfrak{m}_v$. In this case, note that $K = \operatorname{Frac} \mathcal{O}_v$; in fact, for any $x \in K^\times$ we have either $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$. And indeed, this property characterizes all rings that arise in this way; this is the content of Theorem/Definition 7.1.5 below.

Example 7.1.4 (TODO: Examples)**.**

Theorem/Definition 7.1.5 (Valuation Rings)**.** Let $R \subset K$ be a ring extension with K a field. Then the following are equivalent:

(a) For all $x \in K^\times$, either $x \in R$ or $x^{-1} \in R$.
(b) The ideals of R are totally ordered by inclusion and $K = \operatorname{Frac} R$.
(c) There is an ordered abelian group Γ and a Γ-valued valuation v on K such that $R = \mathcal{O}_v$.
(d) The ring R is a local ring maximal with respect to dominance in K.[1]

[1] This last property says that if $S \subset K$ is a local ring such that $R \subset S$ and $\mathfrak{m}_R \subset \mathfrak{m}_S$, then $R = S$.

A domain R satisfying these equivalent properties (for some field K, which must *a posteriori* be the fraction field of R) is said to be a *valuation ring*.

Proof.

(a) $\Rightarrow$ (b) Let $\mathfrak{a}, \mathfrak{b} \subset R$ be ideals, and suppose there is a $x \in \mathfrak{a} \smallsetminus \mathfrak{b}$. Then for any nonzero $y \in \mathfrak{b}$, the fraction x/y cannot be in R, and hence $y/x \in R$, whence $y \in \mathfrak{a}$. This shows $\mathfrak{b} \subset \mathfrak{a}$.

(b) $\Rightarrow$ (a) Given $z \in K^\times$; since $K = \operatorname{Frac} R$, there are nonzero $x, y \in R$ with $z = x/y$; use the total ordering to compare the ideals (x) and (y).

(a) $\Rightarrow$ (c) Let $\Gamma := K^\times / R^\times$, and given $\xi, \eta \in \Gamma$ represented by $x, y \in K^\times$ respectively, say $\xi \leq \eta$ iff $yx^{-1} \in R$. Then, by (a), Γ is an ordered abelian group, and the natural projection $v : K^\times \to \Gamma$ extended by $v(0) = \infty$ is the required valuation.

(c) $\Rightarrow$ (a) This was observed above (Remark 7.1.3).

(a) $\Rightarrow$ (d) Locality follows from the implication (a) $\Rightarrow$ (b) combined with Remark 7.1.3. If $S \subset K$ is a local ring such that $R \subset S$ and $\mathfrak{m}_R \subset \mathfrak{m}_S$ and $x \in S \smallsetminus R$, then $x^{-1} \in \mathfrak{m}_R \subset \mathfrak{m}_S$, contradicting $x \in S$.

(d) $\Rightarrow$ (a) Let $\mathfrak{m} \subset R$ be the maximal ideal and for $x \in K \smallsetminus R$, set $S := R[x]$. If the ideal $\mathfrak{m}S \subset S$ is proper, then it is contained in a maximal ideal $\mathfrak{n} \subset S$, and then $\mathfrak{n} \cap R = \mathfrak{m}$ implies that S is properly dominated by $S_{\mathfrak{n}}$. Since we are assuming this cannot happen, we must have $\mathfrak{m}S = S$, and hence there is an integer $n \geq 1$ and elements $c_0, c_1, \ldots, c_n \in \mathfrak{m}$ such that $1 = \sum_{i=0}^{n} c_i x^i$. By Proposition/Definition 1.2.7, we have $1 - c_0 \in R^\times$,and so this equation implies that $x^{-1} \in \mathrm{Cl}_K(R)$, and hence by Theorem 4.2.1(a) there is a prime $\mathfrak{p}$ of $R[x^{-1}]$ lying over $\mathfrak{m}$. Then it follows from maximality that $x \in R[x^{-1}]_{\mathfrak{p}} = R$.

■

Corollary 7.1.6. Let R be a valuation ring and $K := \operatorname{Frac} R$ its fraction field.

(a) Any subring of K containing R is also a valuation ring; in particular, every nonzero localization of R is a valuation ring.

(b) Every quotient of R by a prime ideal (i.e. every integral domain quotient of R) is a valuation ring.

(c) The domain R is normal, i.e. $\mathrm{Cl}_K(R) = R$.

Proof. The statement (a) is clear from Theorem/Definition 7.1.5, and (b) follows from the same combined with the fact that if $\mathfrak{p} \subset R$ is a prime, then $R_{\mathfrak{p}} \to \operatorname{Frac}(R/\mathfrak{p})$ is surjective (check!). For (c), if $x \in K^\times$ is such that for some integer $n \geq 1$ and elements $a_1, \ldots, a_n \in R$ we have $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ and $x^{-1} \in R$, then multiplying throughout by x^{-n+1} yields also that $x \in R$. ■

Corollary 7.1.7. Let $R \subset K$ be any extension with K a field. Then the normalization of R in K is the intersection of all valuation rings of K containing R.

Proof. One inclusion follows from Corollary 7.1.6(c). Conversely, if $x \notin \mathrm{Cl}_K(R)$, then $x^{-1} \notin R[x^{-1}]^\times$, and hence there is a maximal ideal $\mathfrak{m}$ of $R[x^{-1}]$ containing x. Let Ω be an algebraic closure of $R[x^{-1}]/\mathfrak{m}$ with a fixed embedding thereof, and consider the natural map $\varphi : R[x^{-1}] \to \Omega$. By Zorn's Lemma, this admits a maximal extension $\hat{\varphi} : S \to \Omega$ to a subring S of K, which by Theorem 4.3.1(c) is a valuation ring of K containing $R[x^{-1}]$. Since $x^{-1} \in S$ with $\hat{\varphi}(x^{-1}) = 0$, we conclude that S is a valuation ring of K containing R but not containing x. ■

Finally, we are able to characterize discrete valuation rings (i.e. valuation rings of discrete valuations), abbreviated DVRs, as rings with rather special properties.

Theorem 7.1.8 (DVRs)**.** The following conditions on a (nonzero) ring R are equivalent:

(a) R is the valuation ring of a discrete valuation.
(b) R is a Noetherian domain that is not a field, but is maximal with respect to inclusion of subrings in its fraction 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 element up to associates, i.e. multiplication by units.
(f) R is a Noetherian local domain that is not a field and if $\mathfrak{m}$ (resp. k) is its maximal ideal (resp. residue field), then
  (1) $\mathfrak{m}$ is principal (or equivalently[2] $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$),
  (2) every nonzero ideal in R is of the form $\mathfrak{m}^n$ for some (necessarily unique[3]) integer $n \geq 0$,
  (3) $\dim R = 1$ and R is normal, or
  (4) $\dim R = 1$ and the only $\mathfrak{m}$-primary ideals of R are powers of $\mathfrak{m}$.
(g) R is a local domain that is not a field and every fractional ideal of R is invertible.

In this case,

(h) An element $\pi \in R$ is a uniformizer iff $\mathfrak{m} = (\pi)$ iff $\pi \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$, and in this case $\operatorname{Frac} R = R[\pi^{-1}]$. In particular, the discrete valuation as in (a), when normalized to be $\mathbf{Z}$-valued, is determined uniquely.
(i) The only prime ideals of R are (0) and $\mathfrak{m}$.

Proof.

Step 1. First, we show the equivalence of (a)-(e).

(a) $\Rightarrow$ (b) Let v be a discrete valuation on $K := \operatorname{Frac} R$ with valuation ring $R = \mathcal{O}_v$; without loss of generality, we may assume that v is $\mathbf{Z}$-valued. If $\mathfrak{a} \subset R$ is a nonzero ideal, and an element $x \in \mathfrak{a}$ is chosen with minimal $v(x)$, then $\mathfrak{a} = (x)$, showing that R is a PID. If R were a field, then $\mathfrak{m}_v = 0$ and hence $v(x) = 0$ for all $x \in R$, contradicting that the value group of v is nonzero. Finally, if S is a ring with $R \subset S \subset K$, then since R has a uniformizer, the set $v(S)$ is of the form $[n, \infty)$ for some (unique) $n = \inf v(S) \in \mathbf{Z}_{\leq 0} \cup \{-\infty\}$. If $n = 0$, then $S \subset R$. If $n \leq -1$, then, since S is a ring, we must have $n = -\infty$. In this case, given any $x \in K^\times$, there is an $s \in S$ such that $xs^{-1} \in R$, which implies $x \in S$; therefore, $S = K$.

(b) $\Rightarrow$ (c) In light of Theorem/Definition 7.1.5(d), it only remains to show that R is local. Suppose contrarily that there are maximal ideals $\mathfrak{m}, \mathfrak{n} \subset R$ and an element $x \in \mathfrak{m} \smallsetminus \mathfrak{n}$. Then we claim that $R \subsetneq R[x^{-1}] \subsetneq K = \operatorname{Frac} R$, a contradiction. The first containment follows from $x \in \mathfrak{m}$, and the second follows from the fact that $\mathfrak{n}$ is nonzero and if $0 \neq y \in \mathfrak{n}$, then $y^{-1} \notin R[x^{-1}]$ (check!).

[2] This is Corollary 1.5.4(c).

[3] If $(R, \mathfrak{m}, k)$ is a nonzero Noetherian local domain that is not a field and every nonzero ideal in R is of the form $\mathfrak{m}^n$ for some integer $n \geq 0$, then this integer is unique. Indeed, if there are integer $n \geq 0$ and $k \geq 1$ such that $\mathfrak{m}^n = \mathfrak{m}^{n+k}$, then $\mathfrak{m}^n = \mathfrak{m}^{n+1} = \cdots = \mathfrak{m}^{n+k}$ and so by Nakayama's Lemma (Corollary 1.5.3) we conclude that $\mathfrak{m}^n = 0$. If $n = 0$, this contradicts our assumption that R is nonzero; if $n \geq 1$, then $\mathfrak{m} = \sqrt{\mathfrak{m}^n} = \sqrt{0} = 0$, contradicting our assumption that R is not a field.

(c) $\Rightarrow$ (d) Using Theorem/Definition 7.1.5, we have to show that a Noetherian valuation ring is a PID; for this if $\mathfrak{a} \subset R$ is any ideal and we pick an integer $n \geq 0$ and generators $x_1, \ldots, x_n \in \mathfrak{a}$ of $\mathfrak{a}$, then by the total ordering of ideals, there is a k with $1 \leq k \leq n$ such that (x_k) contains all $(x_1), \ldots, (x_n)$,and then $\mathfrak{a} = (x_k)$.

(d) $\Rightarrow$ (e) A PID is a UFD (Corollary 1.4.4). If we take a generator π of the maximal ideal $\mathfrak{m} \subset R$, then $0 \neq \pi$ is irreducible. If $x \in R \smallsetminus R^\times$, then by locality $x \in \mathfrak{m} = (\pi)$ and hence $\pi \mid x$; this shows that π is the unique irreducible element up to associates.

(e) $\Rightarrow$ (a) Let π be an irreducible element. Then for each nonzero $x \in R$, there is a unique integer $n = n(x) \geq 0$ and unit $u \in R^\times$ such that $x = u\pi^n$. The map $x \mapsto n(x)$ extends to a discrete valuation on $\operatorname{Frac} R$ with valuation ring R.

Step 2. Next, we show that (a)-(e) imply (h) and (i).

(h) If π is a uniformizer for some discrete valuation v, then it is irreducible, and hence a generator of the maximal ideal by (e). If $\mathfrak{m} = (\pi)$ and $\pi \in \mathfrak{m}^2 = (\pi^2)$, then since R is a domain, we would conclude that π is a unit, which is a contradiction. Finally, if $\pi \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$ and v is a discrete valuation on $K = \operatorname{Frac} R$ with valuation ring R, then we may pick a uniformizer ϖ for v. By what we have already shown, ϖ is the unique irreducible in R up to associates and is a generator of $\mathfrak{m}$. In the UFD R, we can factor π uniquely as $\pi = u\varpi^n$ for a unit $u \in R^\times$ and integer $n \geq 0$; then $\pi \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$ implies that $n = 1$, and hence π is also a uniformizer for v. Then we conclude that, in fact, for any $x \in K^\times$ where $K = \operatorname{Frac} R$, we can uniquely write $x = u\pi^n$ for a unit $u \in R^\times$ and $n \in \mathbf{Z}$, so certainly $K = R[\pi^{-1}]$. That the (normalized) discrete valuation is uniquely determined is clear, since we have characterized uniformizers with respect to any discrete valuation as generators of $\mathfrak{m}$ or elements of $\mathfrak{m} \smallsetminus \mathfrak{m}^2$.

(i) We have shown in (a)-(e) and (h) that every nonzero ideal in R is of the form $\mathfrak{m}^n$ for some $n \geq 1$, any the only prime ideal of this form is $\mathfrak{m}$.

Step 3. Now we finish the proof.

(f1) $\Rightarrow$ (f2) By Corollary 1.5.5, we have $\bigcap_{n \geq 0} \mathfrak{m}^n = 0$.[4] In particular, if $\mathfrak{a} \subset R$ is a nonzero proper ideal, then there is a unique integer $n \geq 1$ such that $\mathfrak{a} \subset \mathfrak{m}^n$ but $\mathfrak{a} \not\subset \mathfrak{m}^{n+1}$. Fix an $x \in \mathfrak{a} \smallsetminus \mathfrak{m}^{n+1}$. Write $\mathfrak{m} = (\pi)$ and use $\mathfrak{a} \subset \mathfrak{m}^n$ to write $x = u\pi^n$ for some $u \in R$. Since $x \notin \mathfrak{m}^{n+1}$, we must have $u \notin \mathfrak{m}$, so u is a unit. Then $\mathfrak{m}^n = (\pi^n) = (x) \subset \mathfrak{a}$.

(f2) $\Rightarrow$ (f1) By uniqueness, there is a $\pi \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$; then there is a unique integer $n \geq 0$ such that $(\pi) = \mathfrak{m}^n$, and we must have $n = 1$.

Clearly, (d) implies (f1), and (f1) and (f2) together imply (d). Next, (a)-(e) imply (f3) by combining Corollary 7.1.6(c) with the already proven implication (a) $\Rightarrow$ (i) in Step 2. Hence the implication (f1)-(f2) $\Rightarrow$ (f4) is also clear, as is the implication (d) $\Rightarrow$ (g). The next few implications then finish the proof.

(f3) $\Rightarrow$ (f1) First note that (f3) $\Rightarrow$ (i).

(f4) $\Rightarrow$ (f2)

(g) $\Rightarrow$ (f2)

■

[4] In the present case, this can also be deduced very simply: if $\mathfrak{m} = (\pi)$ and $0 \neq x \in K_{\mathfrak{m}}$, then for each integer $n \geq 0$ there is an $x_n \in R$ such that $x = x_n \pi^n$. Then $x_n = x_{n+1}\pi$ for each $n \geq 0$; the ascending chain $(x_0) \subset (x_1) \subset \cdots$ stabilizes by the Noetherian condition to give us the contradiction $\pi \in R^\times$.

7.2 Invertibility of Fractional Ideals

7.3 Dedekind Domains

7.4 Extensions of Dedekind Domains

Theorem 7.4.1. 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 the 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 $v_1, \dots, v_n \in S$ be one such basis. Since L/K is separable, the trace pairing $(x,y) \mapsto \mathrm{Tr}^L_K(xy)$ is nondegenerate (by Theorems 5.3.4[TODO] and 5.4.1(g)). Using this pairing we find the dual basis $v_1^*, \dots, v_n^* \in L$ with $\mathrm{Tr}^L_K(v_i^* v_j) = \delta_{ij}$. Write an $x \in S$ as $x = \sum_i x_i v_i^*$, then for each i, the inclusion $xv_i \in S$ implies that $x_i = \mathrm{Tr}^L_K(xv_i) \in R$ by Lemma 4.1.10(b) by taking $\mathfrak{a} = (1)$, combined with Theorem 10.3.5(b). Therefore, $S \subset \sum_j R v_j^*$; we finish by the Noetherian hypothesis. ∎

Proof 2 of (a). Replacing L by its Galois closure (and using that R is Noetherian), we may assume that L/K is finite Galois with Galois group $G := \mathrm{Gal}(L/K)$. As in the first proof, let $v_1, \dots, v_n \in S$ be an a basis of L/K; and let D be the discriminant with respect to this basis (Definition 10.3.6), where $0 \neq D$ by separability as before. Again by Lemma 4.1.10 and Theorem 10.3.5(b), 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 $x_j = y_j/\delta$ for some $y_j \in S$, where $\delta := \det\big(\sigma_i v_j\big)_{i,j}$ and $D = \delta^2$ (by Theorem 10.3.5(a) and Definition 10.3.6); clearly also $\delta \in S$. Then $Dx_j = y_j \delta \in \mathrm{Cl}_K(R) = R$. 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 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 over K (say the splitting field in some algebraic closure of L of the minimal polynomials over K of some generating set of L as a field extension of K) to assume that L/K is normal. Let $I := L^{\mathrm{Aut}(L/K)}$, so that L/I is Galois and I/K is purely inseparable (see [11, Theorem 4.23] if needed). If we show that $T := \mathrm{Cl}_I(R)$ is a finitely generated R-module, then it is Noetherian and is normal since $I = \mathrm{Frac}\, T$, 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 I that L/K is purely inseparable. If $L = K$ (e.g. if $\mathrm{char}\, K = 0$), this is trivial; else assume that $p := \mathrm{char}\, k > 0$. Then for some power q of p, the field L is generated by q^{th} roots of finitely many rational functions. Extending L further by adjoining q^{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^{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 integral over R and is normal in its quotient field L; visibly, S and is module-finite over R. ∎

Theorem 7.4.2 (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 7.4.1). 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 $L = \operatorname{Frac} S$; it is of dimension 1 by Corollary 4.2.6(a), so S is Dedekind by Theorem **??**(a)(1). For (b), By Weak Approximation (Theorem **??**(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 **??**(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 $x_1, \ldots, x_r \in S$ 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 1.5.3(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 $x_1, \ldots, x_r$ 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 7.4.3. 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 $[L : K] > \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$.

Chapter 8

A Little Homological Algebra

8.1 Projective, Injective, and Flat Modules

For this chapter only, we do not require that rings be commutative, and work carefully with left- and right- modules over possibly noncommutative rings, although (a) the whole setup can more-or-less be carried out in any suitable abelian category, and (b) the reader will not lose much by focusing on the commutative case on the first pass. For a (possibly noncommutative) ring R, we let R-Mod denote the category of left R-modules (i.e. $(R,\mathbf{Z})$-bimodules), and let Mod-R denote the category of right R-modules (i.e. $(\mathbf{Z},R)$-bimodules). Let $\mathsf{Ab} = \mathbf{Z}$-Mod be the category of abelian groups. The first key observation here is

Lemma 8.1.1 (The Definitive Tensor-Hom Adjunction)**.** Let A,B,C be rings. Let X be an (A,B)-bimodule, Y be a (B,C)-bimodule, and Z be an (A,C)-bimodule. There are isomorphisms of abelian groups

$$\mathrm{Hom}_{(A,B)}(X,\mathrm{Hom}_{(\mathbf{Z},C)}(Y,Z)) \cong \mathrm{Hom}_{(A,C)}(X\otimes_B Y,Z) \cong \mathrm{Hom}_{(B,C)}(Y,\mathrm{Hom}_{(A,\mathbf{Z})}(X,Z)).$$

These isomorphisms are natural in A,B,C,X,Y, and Z.

Proof. Let $\varphi : X \to \mathrm{Hom}_{(\mathbf{Z},C)}(Y,Z)$ be an (A,B)-bimodule homomorphism. Consider the map $X\times Y \to Z$ given by $(x,y)\mapsto \varphi(x)(y)$. This is B-balanced, and so descends to a map $\tilde{\varphi}: X\otimes_B Y \to Z$ which is easily seen to be an (A,C)-bimodule homomorphism. The resulting map $\mathrm{Hom}_{(A,B)}(X,\mathrm{Hom}_{(\mathbf{Z},C)}(Y,Z)) \to \mathrm{Hom}_{(A,C)}(X\otimes_B Y,Z)$ given by $\varphi\mapsto\tilde{\varphi}$ is the required isomorphism. The second part is similar, and the naturality statement is clear from the proof; the details are left to the reader. ■

A ring homomorphism $f : R \to S$ makes S an (R,R)-bimodule and gives rise to three functors:

(a) the extension-of-scalars functor $f^* : R\text{-Mod} \to S\text{-Mod}$ given by $M \mapsto S\otimes_R M$,
(b) the restriction-of-scalars functor $f_* : S\text{-Mod} \to R\text{-Mod}$,
(c) the dualizing-of-scalars functor $f^! : R\text{-Mod} \to S\text{-Mod}$ given by $M \mapsto \mathrm{Hom}_R(S,M)$, with S-module structure given by $(s\cdot\varphi)(t) := \varphi(ts)$ for $s,t\in S$ and $\varphi' in f^! M$.

Corollary 8.1.2. If $f : R \to S$ is a ring homomorphism, then $f^* \dashv f_* \dashv f^!$. In particular, f^* is right-exact, f_* is exact, and $f^!$ is left-exact.

Proof. If M is a left R-module and N a left S-module, then there are natural abelian group isomorphisms

$$\mathrm{Hom}_S(f^*M,N) = \mathrm{Hom}_S(S\otimes_R M,N) \cong \mathrm{Hom}_R(M,\mathrm{Hom}_S(S,N)) \cong \mathrm{Hom}_R(M,f_*N),$$

where in the second step we have applied the second of the two isomorphisms in Lemma 8.1.1 applied to $A = X = S, B = R, C = \mathbf{Z}, Y = M$ and $Z = N$, and in the third step we have used that $\mathrm{Hom}_S(S,N) \cong N$ as S-modules, whence $\mathrm{Hom}_S(S,N) \cong f_*N$ as R-modules. Similarly, there are natural abelian group isomorphisms

$$\mathrm{Hom}_R(f_*N,M) \cong \mathrm{Hom}_R(S\otimes_S N,M) \cong \mathrm{Hom}_S(N,\mathrm{Hom}_R(S,M)) = \mathrm{Hom}_S(N,f^!M),$$

where in the first step we have used $N \cong S\otimes_S N$ as S-modules, and in the second step the second isomorphism from Lemma 8.1.1 applied to $A = R, B = X = S, C = \mathbf{Z}, Y = N$ and $Z = M$. ■

Corollary 8.1.3. Let R be a ring, and T be a left R-module.

(a) The functor $\mathrm{Hom}_R(T,-) : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is right adjoint, and hence left exact.
(b) The functor $\mathrm{Hom}_R(-,T) : R\text{-}\mathsf{Mod}^{\mathrm{op}} \to \mathsf{Ab}$ is right adjoint, and hence left-exact.
(c) The functor $- \otimes_R T : \mathsf{Mod}\text{-}R \to \mathsf{Ab}$ is left adjoint, and hence right-exact.

Similarly, if T is a right R-module, then:

(d) The functor $T \otimes_R - : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is left-adjoint, and hence right-exact.

Proof.

(a) Let M be a (left) $\mathbf{Z}$-module and N a left R-module; then Lemma 8.1.1 applied to $A = R, B = C = \mathbf{Z}, X = T, Y = M, Z = N$ gives us the required natural isomorphism

$$\mathrm{Hom}_R(T \otimes_{\mathbf{Z}} M, N) \cong \mathrm{Hom}_{\mathbf{Z}}(M, \mathrm{Hom}_R(T,N)).$$

(b) Let M, N be as in (a); then Lemma 8.1.1 applied to $A = R, B = C = \mathbf{Z}, X = N, Y = M, Z = T$ gives us the required natural isomorphisms

$$\mathrm{Hom}_{\mathbf{Z}}(M, \mathrm{Hom}_R(N,T)) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbf{Z}}(M,T)) \cong \mathrm{Hom}_{R\text{-}\mathsf{Mod}^{\mathrm{op}}}(\mathrm{Hom}_{\mathbf{Z}}(M,T), N).$$

(c) Let M be a right R-module and N a left $\mathbf{Z}$-module; then Lemma 8.1.1 applied to $A = C = \mathbf{Z}, B = R, X = M, Y = T, Z = N$ gives us the required natural isomorphisms

$$\mathrm{Hom}_{\mathbf{Z}}(M \otimes_R T, N) \cong \mathrm{Hom}_{(\mathbf{Z},R)}(M, \mathrm{Hom}_{\mathbf{Z}}(T,N)).$$

(d) Similar and left to the reader.

■

This leads us directly to

Proposition/Definition 8.1.4 (Projective Modules)**.** Let R be a ring, and P be a left R-module. The following conditions are equivalent:

(a) The functor $\mathrm{Hom}_R(P,-) : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is exact.
(b) If $M \to N \to 0$ is exact in R-Mod, then so is $\mathrm{Hom}_R(P,M) \to \mathrm{Hom}_R(P,N) \to 0$ in Ab.
(c) If $M \to N \to 0$ is exact in R-Mod and $P \xrightarrow{f} N$ a morphism, then there exists a lift $\tilde{f} : P \to M$ of f, i.e. there is a dashed arrow making the following diagram commutative:

$$\begin{array}{ccccc} & & & & P \\ & & \overset{\tilde{f}}{\swarrow} & & \downarrow f \\ M & \longrightarrow & N & \longrightarrow & 0. \end{array}$$

(d) Every short exact sequence $0 \to L \to M \to P \to 0$ in R-Mod splits. (See Exercise 8.1.)
(e) P is the direct summand of a free module.

The module P is said to be *projective* if it satisfies these equivalent conditions.

Proof. In light of Corollary 8.1.3(a) and the fact that every module is the quotient of a free module, the implications (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (e) are clear. Therefore, it suffices to show that (e) $\Rightarrow$ (c), which follows from observations that a free module is projective, and given a family P_i of modules, the direct sum $\bigoplus_i P_i$ is projective iff each P_i is. ■

The following consequences of the definition are clear.

Corollary 8.1.5.

(a) If R is a (commutative) PID, then every projective module over R is free.[1]
(b) A finitely generated module is projective iff it is a direct summand of a finitely generated free module.
(c) Every module is a quotient of a projective module, i.e. for any ring R, the category R-Mod has enough projectives. In particular, every module admits a projective (in fact a free) resolution.
(d) Suppose that R is commutative, and that $\{P_j\}_j$ is a finite family of projective modules. Then the tensor product $\bigotimes_j P_j$ is also projective.

The dual definition is

Proposition/Definition 8.1.6 (Injective Modules)**.** Let R be a ring and Q a left R-module. The following conditions are equivalent:

(a) The functor $\mathrm{Hom}_R(-,Q) : R\text{-Mod} \to \mathsf{Ab}$ is exact.
(b) If $0 \to L \to M$ is exact in R-Mod, then so is $\mathrm{Hom}_R(M,Q) \to \mathrm{Hom}_R(L,Q) \to 0$ in Ab.
(c) If $0 \to L \to M$ is exact in R-Mod and $L \xrightarrow{f} Q$ a morphism, then there exists an extension $\tilde{f} : M \to Q$ of f, i.e. there is a dashed arrow making the following diagram commutative:

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \longrightarrow & M \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \tilde{f}} & \\ & & Q. & & \end{array}$$

(d) Every short exact sequence $0 \to Q \to M \to N \to 0$ in R-Mod splits.
(e) (Baer) The condition in (c) for the special case where $M = R$, so $L = \mathfrak{a} \subset R$ is a (left) ideal.

Proof. Thanks to Corollary 8.1.3(b), the implications (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) $\Rightarrow$ (d), (e) are clear.

(d) $\Rightarrow$ (c) Given a solid diagram as in (c), complete it to a pushout diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \longrightarrow & M \\ & & \downarrow{\scriptstyle f} & & \downarrow \\ 0 & \longrightarrow & Q & \longrightarrow & P. \end{array}$$

Since the map $L \to M$ is injective, so is the map $Q \to P$ (Exercise 8.2). Since by assumption the sequence $0 \to Q \to P \to P/Q \to 0$ splits, we have a splitting map $p : P \to Q$; then the composition $M \to P \xrightarrow{p} Q$ gives the extension $\tilde{f}$. Alternatively, use Proposition 8.1.9(b) to find an injective M such that $Q \hookrightarrow M$; then since $0 \to Q \to M \to M/Q \to 0$

[1] Recall, if needed, that any submodule M of a free module F over a PID is free of rank at most that of F. This is well-known in the finitely generated case, but we do not need the hypothesis of finite generation. Indeed, let R be a PID and F be a free module with free basis $\{e_i\}_{i\in I}$. Let $p_i : F \to R$ denote the projection onto the i^{th} coordinate. Well-order I, and for each i, let $F_i \subset F$ be the free module generated by the e_j with $j \leq i$, so that for each i we have $F_i = \bigcap_{j>i} \ker p_j$ and $\ker p_i = \bigcup_{j<i} F_j$. Now suppose that $M \subset F$ is a submodule, and for each i, let $M_i := M \cap F_i$. Then $p_i(M_i) \subset R$ has the form Ra_i for some $a_i \in R$; pick, for each i, an element $m_i \in M_i$ such that $p_i(m_i) = a_i$, ensuring that $m_i = 0$ if $a_i = 0$. It is then easy to see via transfinite induction on I that the nonzero m_i constitute a free basis for M.

splits, we see that $M \cong Q \oplus M/Q \cong Q \times M/Q$, so we are done by the observation that given a family Q_i of modules, the direct product $\prod_i Q_i$ is injective iff each Q_i is.

(e) $\Rightarrow$ (c) Given a solid diagram as in (c), consider the partially ordered set

$$\mathcal{C} = \{(L', f') : L \subset L' \subset M, f' : L' \to Q \text{ such that } f'|_L = f\}.$$

By Zorn's Lemma, this has a maximal element, say (L_0, f_0). Suppose for the sake of contradiction that $L_0 \subsetneq M$, and pick an $m \in M \setminus L_0$. Let $\mathfrak{a} := (L_0 :_R m) = \{r \in R : rm \in L_0\}$, and define a map $\varphi : \mathfrak{a} \to Q$ by $\varphi(r) = f_0(rm)$. By assumption, there is a lift $\tilde{\varphi} : R \to Q$ of φ to R. Define the map $f_1 : L_0 + Rm \to Q$ by $f_1(\ell + rm) = f_0(\ell) + \tilde{\varphi}(r)$; this is well-defined because if $\ell + rm = \ell' + r'm$, then $\ell - \ell' = (r - r')m \in L_0$, whence $r - r' \in \mathfrak{a}$ and so

$$\tilde{\varphi}(r - r') = \varphi(r - r') = f_0((r - r')m) = f_0(\ell - \ell').$$

From this, we see that $(L_0, f_0) < (L_0 + Rm, f_1)$ in $\mathcal{C}$, contradicting the maximality of (L_0, f_0).

■

Let us now give some examples. For this, we need the following comparison lemma.

Lemma 8.1.7. Let $f : R \to S$ be a ring homomorphism.

(a) If P is a projective R-module, then $f^*P = S \otimes_R M$ is a projective S-module.
(b) If Q is an injective R-module, then $f^!Q = \mathrm{Hom}_R(S, Q)$ is an injective S-module.

Proof.

(a) The functor $\mathrm{Hom}_S(f^*P, -) \cong \mathrm{Hom}_R(P, f_* -)$ is a composition of two exact functors, where $\mathrm{Hom}_R(P, -)$ is exact because P is projective and the fact that f_* is exact was observed in Corollary 8.1.2.
(b) Identical to (a), using $\mathrm{Hom}_S(-, f^!Q) \cong \mathrm{Hom}_R(f_* -, Q)$ instead.

■

In all, it suffices to exhibit injective modules over *one* ring, say $R = \mathbf{Z}$. We do a little better.

Definition 8.1.8. Given a ring R and an R-module Q, we say that Q is *divisible* if for every nonzerodivisor[2] $r \in R$, we have $rQ = Q$, i.e. given any $q \in Q$, there is a $q' \in Q$ such that $q = rq'$.

Proposition 8.1.9 (Enough Injectives in R-Mod)**.** Let R be a ring.

(a) Every injective R-module is divisible, and the converse holds if the R is a (commutative) PID.
(b) Every module is a submodule of an injective module, i.e. the category R-Mod has enough injectives. In particular, every module admits an injective resolution.

Proof.

[2]By this, we mean that if $ar = 0$ for $a \in R$, then $a = 0$. An r not satisfying this condition is called a right zerodivisor. Of course, over commutative rings, it is clear what a nonzerodivisor is.

(a) Let Q be an injective R-module, $q \in Q$ and $r \in R$ a nonzerodivisor. Define the R-module homomorphism $f : (r) \to Q$ by $f(ar) = aq$ for $a \in R$; this is well-defined because if $ar = a'r$, then $(a-a')r = 0$ and hence $a = a'$ because r is a nonzerodivisor. Since Q is injective, there is an extension $\tilde{f} : R \to Q$ of f. Setting $q' := \tilde{f}(1)$, we conclude that

$$q = f(r) = \tilde{f}(r) = r\tilde{f}(1) = rq'$$

as needed. Now suppose that R is a (commutative) PID, and Q a divisible R-module; to show that Q is injective, we use Baer's criterion (Proposition/Definition 8.1.6(e)). Assume that there is a morphism $f : \mathfrak{a} \to Q$. Since R is a PID, $\mathfrak{a} = (r)$ for some $r \in R$. If $r = 0$, then $\tilde{f} = 0$ works; else r is a nonzerodivisor, so by divisibility there is a $q' \in Q$ such that $f(r) = rq'$. Then the map $\tilde{f} : R \to Q$ by $\tilde{f}(s) = sq'$ is an extension of f.

(b) First we show the result for $R = \mathbf{Z}$, so R-Mod $=$ Ab. Let G be any abelian group. Pick a short exact sequence $0 \to K \to F \to G \to 0$ with F free so that $F/K \cong G$. The composite $F \hookrightarrow \mathbf{Q} \otimes_{\mathbf{Z}} F \twoheadrightarrow (\mathbf{Q} \otimes_{\mathbf{Z}} F)/K$ has kernel K, and hence gives us an embedding $G \cong F/K \hookrightarrow (\mathbf{Q} \otimes_{\mathbf{Z}} F)/K$, where the last group is divisible and hence injective thanks to (a).
Now suppose that R is any ring, and let $f : \mathbf{Z} \to R$ be the natural homomorphism. Suppose that M is any R-module. By the previous case, we can find an injective $\mathbf{Z}$-module Q such that $f_*M \hookrightarrow Q$. Since the left adjoint f_* is faithful, it follows that the unit map $M \to f^! f_* M$ of the adjunction $f_* \dashv f^!$ is a monomorphism (check!); then we have the composition of monomorphisms

$$M \hookrightarrow f^! f_* M \hookrightarrow f^! Q,$$

where the second step uses that $f^!$ is left exact (Corollary 8.1.2). Since $f^!Q$ is an injective R-module thanks to Lemma 8.1.7(b), we are done.

■

The final notion that we will need is that of a *flat* R-module.

Definition 8.1.10.

[Faithfully exact functors by Ishikawa]

8.2 Derived Functors: Tor and Ext

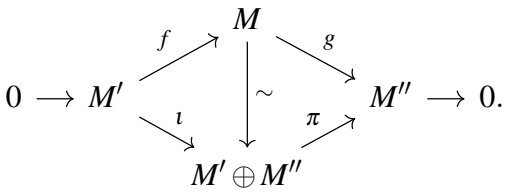
Example 8.2.1 (Lie Algebra (Co)homology)**.**

Example 8.2.2 (Hochschild (Co)homology)**.**

8.3 Exercises

Exercise 8.1. Let $\mathscr{A}$ be any abelian category; think $\mathscr{A} = R\text{-Mod}$ for some ring R if needed. Let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be a short exact sequence in $\mathscr{A}$. Show that the following conditions are equivalent:

(a) The monomorphism f splits, i.e. there is a morphism $p : M \to M'$ such that $pf = 1_{M'}$.
(b) The epimorphism g splits, i.e. there is a morphism $i : M'' \to M$ such that $gi = 1_{M''}$.
(c) There is an isomorphism of short exact sequences



(d) There is a morphism of short exact sequences as in (c), i.e. the condition in (c), except we do not necessarily require the map $M \to M' \oplus M''$ to be an isomorphism a priori.

When these equivalent conditions are satisfied, the sequence $0 \to M' \to M \to M'' \to 0$ is called *split*.

Exercise 8.2. Given a ring R and a diagram

$$\begin{array}{ccc} L & \xrightarrow{g} & M \\ {\scriptstyle f}\downarrow & & \\ Q & & \end{array}$$

in R-Mod, explicitly identify the colimit P of this diagram (called the *pushout*) as a quotient of $M \oplus Q$. Let $f' : M \to P$ and $g' : Q \to P$ denote the maps that complete the pushout square, i.e.

$$\begin{array}{ccc} L & \xrightarrow{g} & M \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ Q & \xrightarrow{g'} & P. \end{array}$$

Show that if f (resp. g) is a monomorphism, then so is f' (resp. g'), and the same holds with the word "monomorphism" replaced by "epimorphism".

Exercise 8.3. Show that the following conditions on a commutative ring R are equivalent:

(a) R is a reduced Artinian ring.
(b) R is a finite direct product of fields.
(c) Every R-module is projective.
(d) Every R-module is injective.
(e) Every short exact sequence of modules over R splits.
(f) Every R-module is semisimple.
(g) The global dimension $\operatorname{gd} R$ of R is zero.
(h) R is semisimple as a module over itself.

Chapter 9

Applications

9.1 Unique Factorization II

Theorem 9.1.1 (Auslander-Buchsbaum)**.** A regular local ring is a UFD.

Theorem 9.1.2. If R is a regular UFD, then so are $R[X]$ and $R[\![X]\!]$.

Corollary 9.1.3. If K is a field, then for any $n \geq 1$ the ring $K[\![X_1, \ldots, X_n]\!]$ is a UFD.

Proof. Clear from Theorem 9.1.2 by induction, since K is trivially a regular UFD. ■

Theorem 9.1.4. Let R be a Noetherian ring. Then $\dim R[X] = \dim R[\![X]\!] = \dim R + 1$.

Corollary 9.1.5. 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.

Chapter 10

Appendices

10.1 Length and the Jordan-Hölder Theorem

In this section, the base ring R is not necessarily commutative, and the word "R-module" refers to a left R-module. Much of what follows can be generalized to arbitrary abelian categories without much more effort.

Definition 10.1.1. Let R be a ring and M be an R-module.

(a) We say that M is *simple* if it is nonzero and 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} for $i = 0, \ldots, n-1$ 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.

When R is commutative, every simple module is isomorphic to a field quotient of R. In general, a module has length 0 iff it is trivial, length 1 iff it is simple, and finite length iff it admits a finite composition series, so, for instance, $\ell_{\mathbf{Z}}(\mathbf{Z}) = \infty$. The notion of length generalizes that of dimension[1]: if $R = k$ is a field, then $\ell_k(M) = \dim_k M$.

Lemma 10.1.2. Let R be a ring and M be a nonzero R-module. If M is finitely generated, then M has a maximal proper submodule, and hence a simple quotient.

Proof. The collection $\mathscr{A}$ of all proper submodules of M is nonempty since $0 \in \mathscr{A}$. To invoke Zorn's Lemma, it remains to show that if (N_α) is a chain in $\mathscr{A}$, then $\bigcup_\alpha N_\alpha$ is proper. This follows from the fact that M is finitely generated: if $\bigcup_\alpha N_\alpha = M$, then finitely many generators of M lie in some N_α thanks to the total ordering. ■

Counterexample 10.1.3. Lemma 10.1.2 is false if we do not assume M to be finitely generated: take $R = \mathbf{Z}$ and $M = \mathbf{Q}$. The only simple $\mathbf{Z}$-modules are finite fields of prime order, but every $\mathbf{Z}$-module homomorphism from $\mathbf{Q}$ to a finite field is zero (Exercise 10.1). This gives us another proof of the well-known fact that $\mathbf{Q}$ is not a finitely generated abelian group.

Lemma 10.1.4. Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ be a composition series of an R-module M, and let $N \subset M$ be a submodule. Then:

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

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

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

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

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

In particular, for any submodule $N \subset M$ we have $\max\{\ell_R(N), \ell_R(M/N)\} \leq \ell_R(M)$.

Proof.

[1] At least in a naive way that conflates all infinite cardinalities.

(a) For each i, the map $M_i \cap N \hookrightarrow M_i \twoheadrightarrow M_i/M_{i+1}$ has kernel $M_{i+1} \cap N$ giving us an injection

$$(M_i \cap N)/(M_{i+1} \cap N) \hookrightarrow M_i/M_{i+1}.$$

(b) Similarly, for each i, the composite map

$$M_i \hookrightarrow M_i + N \twoheadrightarrow \frac{M_i+N}{M_{i+1}+N} \cong \frac{(M_i+N)/N}{(M_{i+1}+N)/N}$$

is surjective and its kernel contains M_{i+1}, giving us a surjection from M_i/M_{i+1} to this last module.

■

The key result is

Theorem/Definition 10.1.5 (Jordan-Hölder)**.** Let R be a ring and M an R-module. If $\ell_R(M) < \infty$, then the lengths and the multisets of factors of any two composition series of M are the same, so that $\ell_R(M)$ is the length of *any* composition series of M. The multiset of composition factors that appear in any composition series of M is called the multiset of *simple factors* of M.

Proof. We induct on $n := \ell_R(M)$. If $n = 0$, then $M = 0$ and the result is trivial; hence assume $n \geq 1$. 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 by induction, 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 that $N := M_1 \cap M'_1 \subsetneq M_1, M'_1$. By Lemma 10.1.4, N has finite length; pick any finite composition series $N = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = 0$ for it. Then

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

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

$$M \supsetneq M_1 \supsetneq N \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = 0 \text{ and } M \supsetneq M'_1 \supsetneq N \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = 0$$

that differ only at the first step; these trivially have the same length and same composition factors. The same observation above (about when the first submodule in two composition series is the same) tells us that the first of these has the same length and the same factors as our original series; in particular, $r = n-2$. This in turn tells us, by looking at the second composition series, that $\ell_R(M'_1) \leq n-1$, and so by induction the composition series $M'_1 \supsetneq M'_2 \supsetneq \cdots \supsetneq M'_m$ for it must have length $n-1$, giving us $m = n$. That the multisets of composition factors agree follows immediately (check!). ■

Corollary 10.1.6. Let R be a ring.

(a) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules, then

$$\ell_R(M) = \ell_R(M') + \ell_R(M'').$$

If $\ell_R(M) < \infty$, then the multiset of simple factors of M is the union of those of M' and M''.

(b) If M is an R-module of finite length $\ell_R(M)$, then every proper chain of submodules of M has length at most $\ell_R(M)$ and can be refined to a composition series.

Proof.

(a) First observe 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 Lemma 10.1.4. The rest of the result follows from juxtaposition of two composition series.

(b) The second claim is clear since every subquotient of M has finite length by Lemma 10.1.4; then the first claim follows from Theorem 10.1.5.

■

The notion of simple modules can be generalized a little to that of *semisimple* modules.

Proposition/Definition 10.1.7. The following conditions on an R-module M are equivalent:

(a) M is the direct sum of some family of simple modules.
(b) M is the sum of some family of simple modules.
(c) Every short exact sequence $0 \to M' \to M \to M'' \to 0$ splits.

A module satisfying these equivalent properties is said to be *semisimple* or *completely reducible*.

Proof. The implication (a) $\Rightarrow$ (b) is clear.

(b) $\Rightarrow$ (a) Let $M = \sum_{i \in I} M_i$ with each M_i simple. We claim that there is a subset $I' \subset I$ such that $M = \bigoplus_{i \in I'} M_i$. Indeed, suppose without loss of generality that each $M_i \neq 0$ and consider the collection $\mathcal{C}$ of subsets J of I such that the sum $\sum_{j \in J} M_j$ is a direct sum. This is nonempty since $\emptyset \in \mathcal{C}$, and it is easy to see that Zorn's Lemma applies to $\mathcal{C}$, whence we get some maximal subset $I' \in \mathcal{C}$. Let $N := \bigoplus_{i \in I'} M_i = \sum_{i \in I'} M_i \subset M$. For each $j \in I$, if $M_j \cap N = 0$, then $I' \cup \{j\}$ is a strictly larger element of $\mathcal{C}$; therefore, $M_j \cap N \neq 0$, whence by simplicity of M_j we conclude that $M_j \subset N$. It follows then that $M = \sum_{j \in I} M_j \subset N$, whence $M = N$.

(b) $\Rightarrow$ (c) Let $M' \hookrightarrow M$ be a submodule of M, and consider the collection

$$\mathcal{N} = \{N \subset M : N \text{ is the sum of simple modules and } N \cap M' = 0\}$$

of submodules of M. Using Zorn's Lemma, pick a maximal element N of $\mathcal{N}$; we claim that $M' \oplus N \xrightarrow{\sim} M$, giving a splitting of $M' \hookrightarrow M$. Indeed, $M' \cap N = 0$ by construction, and if $M' + N \subsetneq M$, then there is a simple module S in the family given that is not contained in $M' + N$. From the simplicity of S we conclude that $S \cap (M' + N) = 0$, whence $S + N \supsetneq N$ is a bigger element of $\mathcal{N}$, contradicting our choice of N.

(c) $\Rightarrow$ (b) First note that the condition (c) passes to subquotients. Now, let $M' \subset M$ be the sum of all simple submodules of M. If $M' \subsetneq M$, choose a splitting of $M' \hookrightarrow M$ to produce a complementary submodule $M'' \subset M$, and pick a nonzero $m \in M''$. Find by Lemma 10.1.2 a maximal proper submodule $P \subset Rm$. Since (c) applies to Rm, pick a complementary submodule $S \subset Rm$ to P in Rm; then $S \cong Rm/P$ implies that S is simple and hence nonzero. But then $S \subset M'$ by definition of M', contradicting the fact that $M' \cap M'' = 0$.

■

Semisimple modules are the basic objects of study in *representation theory*.

10.2 Dependence Relations

In this section we develop the fundamentals of abstract dependence relations that serve as the foundation for a lot of key concepts in commutative algebra and combinatorics.

Definition 10.2.1. Let S be a set. A *closure operator* on S is a map $\mathrm{Cl} : 2^S \to 2^S$ that is

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

A closure operation Cl is said to

(d) be *finitary*, if for any $X \subset S$ we have $\mathrm{Cl}X = \bigcup_{\substack{X' \subset X \\ |X'| < \infty}} \mathrm{Cl}X'$.
(e) satisfy *MacLane-Steinitz exchange* if $x \in X \subset S$ and $y \in \mathrm{Cl}X \smallsetminus \mathrm{Cl}(X \smallsetminus \{x\})$ together imply that $x \in \mathrm{Cl}(X \smallsetminus \{x\} \cup \{y\})$,

Closure operators are ubiquitous in mathematics, with some examples being integral closure, algebraic closure, separable closure, abelian closure, unramified closure, differential closure, topological closure, graph closure, etc. Closure operators satisfying MacLane-Steinitz exchange are called *matroid closure operations*; readers familiar with matroids will recognize that the above conditions are reformulations of the matroid axioms.[2]

Definition 10.2.2. A *dependence relation* on a set S is a finitary closure operation satisfying MacLane-Steinitz exchange, i.e. a map $\mathscr{D} : 2^S \to 2^S$ satisfying (a)-(e). Given such a pair $(S, \mathscr{D})$, we say that a subset $X \subset S$ is

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

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

Here we think of $\mathscr{D}X$ as the set of elements of S which are *dependent* on those in X. We will show below that any two bases of S have the same cardinality; this cardinality is then called the *dependence* of S. The classic example of this phenomenon is

Example 10.2.3 (Linear Dependence)**.** Let V be a vector space over a field k. Then the map $\langle \cdot \rangle : 2^V \to 2^V$ taking a subset $X \subset V$ to its linear span $\langle X \rangle$ is a dependence relation on V, namely the relation of *linear dependence*, often written LD. In this case, the fundamental set is $\{0\}$ and the dependence of (V, LD) is exactly $\dim_k V$.

Lemma 10.2.4. Let $(S, \mathscr{D})$ be a set with a dependence relation. Then

[2]Usually, matroids are defined on finite sets because duality theory is an essential feature of finite matroids that the above set of axioms do not provide in the infinite case. A recent workaround has been found by Bruhn et al. ([12]), which replaces axiom (d) by the axiom that for any independent set X and any set Y, the collection $\mathscr{A}$ of independent $Z \subset S$ such that $X \subset Z \subset X \cup Y$ has a maximal element. As the reader can verify, with this replacement, the theory below proceeds with minimal changes–the only results below which essentially use axiom (d) are Lemma 10.2.4(d) and Proposition/Definition 10.2.7(b) in the infinite case; notably, Theorem 10.2.5 goes through, with the first line in the proof even easier. However, since the only matroids we will come across in this course satisfy the above axioms (and we will hardly have any direct use for duality of infinite matroids), we will restrict ourselves to looking at these only.

(a) if $X, Y \subset S$ are subsets, then $X \subset \mathscr{D}Y \Rightarrow \mathscr{D}X \subset \mathscr{D}Y$,
(b) if $X \subset S$ is independent and $y \in S \setminus \mathscr{D}X$, then $X \cup \{y\}$ is independent,
(c) if $X \subset S$ is any subset, then the following are equivalent:
    (1) X is a basis,
    (2) X is a minimal spanning set,
    (3) X is a maximal independent set, and
(d) if (X_α) is a totally ordered collection of independent subsets, then $\bigcup_\alpha X_\alpha$ is also independent.

Proof.

(a) We have $X \subset \mathscr{D}Y \Rightarrow \mathscr{D}X \subset \mathscr{D}^2Y = \mathscr{D}Y$.
(b) Let $X' := X \cup \{y\}$. We have to show that for all $x \in X'$ that $x \notin \mathscr{D}(X' \setminus \{x\})$. This is clear if $x = y$ by hypothesis. If $x \in X \cap \mathscr{D}(X' \setminus \{x\})$, then $x \in \mathscr{D}((X \setminus \{x\}) \cup \{y\}) \setminus \mathscr{D}(X \setminus \{x\})$ implies by exchange that $y \in \mathscr{D}X$, again contrary to hypothesis.
(c) For (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 give $x \in S = \mathscr{D}(X') \subset \mathscr{D}(X \setminus \{x\})$, 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 $x \in \mathscr{D}(X \setminus \{x\})$. Then $X \subset \mathscr{D}(X \setminus \{x\})$ implies by (a) that $S = \mathscr{D}X \subset \mathscr{D}(X \setminus \{x\})$, 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 $x \in S = \mathscr{D}(X) \subset \mathscr{D}(X' \setminus \{x\})$, contradicting the independence of X'. For (3) $\Rightarrow$ (1), suppose that X is a maximal independent set. If there is a $y \in S \setminus \mathscr{D}X$, then by (b), $X \cup \{y\} \supsetneq X$ is still independent, which is a contradiction.
(d) Let $X := \bigcup_\alpha X_\alpha$. If there is an $x \in X$ such that $x \in \mathscr{D}(X \setminus \{x\})$, then, since $\mathscr{D}$ is finitary, there is a finite subset $X' \subset X \setminus \{x\}$ such that $x \in \mathscr{D}X'$. By the total ordering, there is an α with $X' \cup \{x\} \subset X_\alpha$, and then $x \in \mathscr{D}X' \subset \mathscr{D}(X_\alpha \setminus \{x\})$ contradicts the independence of X_α.

■

Theorem 10.2.5 (MacLane-Steinitz Exchange)**.** Let $(S, \mathscr{D})$ be a set with a dependence relation. If $X, Y \subset S$ are subsets with X independent and Y spanning, then X can be completed to a basis by borrowing elements from Y: there is a subset $Y' \subset Y$ such that $X \cap Y' = \emptyset$ and $X \cup Y'$ is a basis.

Proof. Let $\mathscr{A}$ be the collection of independent $Z \subset S$ such that $X \subset Z \subset X \cup Y$; then $\mathscr{A}$ is nonempty because $X \in \mathscr{A}$. By Lemma 10.2.4(d) and Zorn's Lemma, this has a maximal element Z. We claim that Z is a basis; indeed, it is independent since $Z \in \mathscr{A}$. If there is a $y \in Y \setminus \mathscr{D}Z$, then by Lemma 10.2.4(b) we have $Z \subsetneq Z \cup \{y\} \subset Y$ with $Z \cup \{y\}$ still independent, a contradiction to maximality. Therefore, $Y \subset \mathscr{D}Z$ so by Lemma 10.2.4(a) we have $S = \mathscr{D}Y \subset \mathscr{D}Z$; therefore, Z is spanning as well. ■

Corollary 10.2.6. Let $(S, \mathscr{D})$ 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.

Proof.

(a) Apply Theorem 10.2.5 with X the independent subset and $Y = S$.
(b) Apply Theorem 10.2.5 with $X = \emptyset$ and Y the spanning subset.
(c) Apply (a) to $X = \emptyset$ or (b) to $Y = S$.

■

Proposition/Definition 10.2.7. Let $(S, \mathscr{D})$ be a set with a dependence relation.

(a) If $X, Y \subset S$ are subsets with X independent and Y a finite spanning set , then $|X| \leq |Y|$. In particular, any independent subset in a set with finite dependency is finite.
(b) Any two bases of S have the same cardinality.

The *dependency* of $(S, \mathscr{D})$ is the cardinality of any basis and is denoted $\dep S$.

Proof.

(a) We will show: if $X, Y \subset S$ are subsets with X independent and Y a finite spanning set, then $|X| \leq |Y|$ and there is a $Y' \subset Y$ of size $|Y'| \leq |Y| - |X|$ such that $X \cap Y' = \emptyset$ and $X \cup Y'$ is a basis. First suppose that $|X|$ itself is finite, and show the statement by induction on $|X|$. When $|X| = 0$, then certainly $|X| \leq |Y|$ and by Corollary 10.2.6(b) there is a basis $Y' \subset Y$. If $|X| = n \geq 1$, say $X = \{x_1, \ldots, x_n\}$, then by applying the inductive hypothesis to $X' := X \smallsetminus \{x_n\}$, we conclude that $n - 1 \leq |Y|$ and there is a subset $Y_0' \subset Y$ disjoint from X' of size $|Y_0'| \leq |Y| - n + 1$ such that $X' \cup Y_0'$ is a basis. If $x_n \in Y_0'$, then taking $Y' := Y_0' \smallsetminus \{x_n\}$ suffices; else assume that $x_n \notin Y_0'$. In this case, the set $X \cup Y_0'$ is spanning but not independent, since $x_n \in S = \mathscr{D}(X' \cup Y_0') = \mathscr{D}((X \cup Y_0') \smallsetminus \{x_n\})$ where $X' \cup Y_0' = (X \cup Y_0') \smallsetminus \{x_n\}$ because $x_n \notin Y_0'$. Since X is independent and $X \cup Y_0'$ spanning, by Theorem 10.2.5, there is a $Y' \subset Y_0'$ disjoint from X such that $X \cup Y'$ is a basis, and necessarily we must have $Y' \subsetneq Y_0'$. This shows $0 \leq |Y'| < |Y_0'| \leq |Y| - n + 1 \Rightarrow n \leq |Y|$ and that $|Y'| \leq |Y| - n$. The first part of the argument then shows that the assumption that $|X|$ is finite always holds: if $|X|$ were infinite, then we may apply the above argument to any subset $X' \subset X$ of size greater than $|Y|$ to obtain a contradiction.
(b) This follows immediately from (a) 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 $y \in S = \mathscr{D}X = \bigcup_{\substack{X' \subset X \\ |X'| < \infty}} \mathscr{D}X'$, so there is a finite $X_y \subset X$ such that $y \in \mathscr{D}X_y$. Then $Y \subset \mathscr{D}(\bigcup_{y \in Y} X_y)$. If $x \in X \smallsetminus \bigcup_{y \in Y} X_y$, then $x \in S = \mathscr{D}Y \subset \mathscr{D}(\bigcup_y X_y) \subset \mathscr{D}(X \smallsetminus \{x\})$ 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 the Cantor-Schröder-Bernstein Theorem.

■

10.3 Trace, Norm, and Discriminant

Definition 10.3.1. Let $R \subset S$ 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 $\mathrm{Tr}_R^S(\alpha)$ (resp. $\mathrm{N}_R^S(\alpha)$) to be the trace (resp. determinant) of the R-module endomorphism of S given by multiplication by α.

Example 10.3.2. Finite field extensions K/k, or more generally finite-dimensional algebras over fields, e.g. étale algebras, and rings of integers $\mathbf{Z} \subset \mathcal{O}_K$ are primary examples (see Example 10.3.8). For instance, for $\mathbf{R} \subset \mathbf{C}$ and $z \in \mathbf{C}$ we have $\mathrm{Tr}_{\mathbf{R}}^{\mathbf{C}}(z) = z + \bar{z} = 2\,\mathrm{Re}\, z$ and $\mathrm{N}_{\mathbf{R}}^{\mathbf{C}}(z) = z\bar{z} = |z|^2$.

Observation 10.3.3. Let $R \subset S$ be a ring extension such that S is a finitely generated free R-module of rank $n \geq 1$.

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

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

(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 $R \otimes_A T \subset S \otimes_A T$ still satisfies the above condition, and we have for any $\alpha \in S$ that

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

(c) (Transitivity) Let $S \subset T$ 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

$$\mathrm{Tr}_R^T(\alpha) = \mathrm{Tr}_R^S\,\mathrm{Tr}_S^T(\alpha) \text{ and } \mathrm{N}_R^T(\alpha) = \mathrm{N}_R^S\,\mathrm{N}_S^T(\alpha).$$

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

Lemma 10.3.4. Let R be any ring, $n \geq 1$, and $S \subset \mathrm{Mat}_n R$ a (commutative, unitary) subring of the $n \times n$ matrix ring over R. For any $m \geq 1$ and matrix $M \in \mathrm{Mat}_m S \subset \mathrm{Mat}_{mn} R$, we have $\det_R^{mn} M = \det_R^n \det_S^m M$.

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 $c \cdot dI_{m-1}^S = dc$, and similarly $A \cdot dI_{m-1}^S = dA$. Therefore,

$$\begin{bmatrix} A & b \\ c & d \end{bmatrix} \begin{bmatrix} dI_{m-1}^S & 0 \\ -c & I_1^S \end{bmatrix} = \begin{bmatrix} dA - bc & b \\ 0 & d \end{bmatrix},$$

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 $\det_R = \det_R^{mn}$ 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 the "universal case" of polynomial rings over $\mathbf{Z}$, or replace our base ring R by $R[x]$ and use $d_x := xI_n^R + d$ 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 10.3.5. 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

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

(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

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

Proof. This belongs to elementary field theory; see [11, Propositions 8.6, 8.12]. ■

The trace map $\mathrm{Tr}_R^S : S \to R$ is an R-linear map; since S is a ring, we get a bilinear pairing on S given by $\langle x, y \rangle \mapsto \mathrm{Tr}_R^S(xy)$ 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 $x \mapsto \mathrm{Tr}_R^S(x\cdot)$.

Definition 10.3.6. 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,

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

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 $D_{S/R} \subset R$ called the discriminant ideal.

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 10.3.7. Given any R-submodule $M \subset L$, 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 10.3.8. 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 4.1.11 and Theorem 10.3.5. 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 $M \subset \mathcal{O}_K \subset M^*$, and we are done by the structure theorem for finitely generated abelian groups. The discriminant $D_K := D_{\mathcal{O}_K/\mathbf{Z}} \in \mathbf{Z}$ is a fundamental invariant of K.

10.4 Derived Functors in Abelian Categories

In this section, we review the generalities of (the naive approach to) derived functors on abelian categories. We use cohomological terminology, and the translation into homological language (i.e. left-derived functors, etc.) is left to the reader. In the following, a functor is always covariant.

Definition 10.4.1. Let $\mathcal{A}, \mathcal{B}$ be abelian categories and $F : \mathcal{A} \to \mathcal{B}$ be an additive functor. A (cohomological) *δ-functor extending F* is a triple $(F^\bullet, \iota, \delta)$, where

(a) $F^\bullet = (F^q)_{q \in \mathbf{Z}_{\geq 0}}$ is a sequence of additive functors $F^q : \mathcal{A} \to \mathcal{B}$ indexed by $q \in \mathbf{Z}_{\geq 0}$, and
(b) ι is a natural isomorphism $\iota : F \Rightarrow F^0$,
(c) δ is a natural assignment $\underline{A} \to \delta^\bullet_{\underline{A}} = (\delta^q_{\underline{A}})_{q \in \mathbf{Z}_{\geq 0}}$ to each short exact sequence

$$\underline{A} : 0 \to A' \to A \to A'' \to 0$$

in $\mathcal{A}$, a sequence of morphisms $\delta^q_{\underline{A}} : F^q(A'') \to F^{q+1}(A')$ in $\mathcal{B}$ indexed by $q \in \mathbf{Z}_{\geq 0}$ such that the sequence

$$\cdots \to F^q(A') \to F^q(A) \to F^q(A'') \xrightarrow{\delta^q_{\underline{A}}} F^{q+1}(A') \to \cdots \qquad (*)$$

(with $F^{-1} := 0$) is a cochain complex.[3]

If for each short exact sequence $\underline{A}$, the sequence $(*)$ is exact, we say further that this δ-functor is *exact*.

A δ-functor is often denoted simply by $F^\bullet : \mathcal{A} \to \mathcal{B}$, with ι and δ implicit (in writing δ, the sub- and superscripts are often dropped too). The morphisms $\delta^\bullet$ are called the *connecting homomorphisms*. Further, ι is often used to identify F and F^0; we will sometimes use this convention to make life simpler.[4]

Now, let $F, G : \mathcal{A} \to \mathcal{B}$ be additive functors between abelian categories, $F^\bullet, G^\bullet : \mathcal{A} \to \mathcal{B}$ be δ-functors extending F and G respectively, and $\eta : F \Rightarrow G$ be a natural transformation. A *δ-transformation from $F^\bullet$ to $G^\bullet$ extending η* is a sequence $\eta^\bullet = (\eta^q)_{q \in \mathbf{Z}_{\geq 0}}$ of natural transformations $\eta^q : F^q \Rightarrow G^q$ such that $\iota_{G^\bullet} \circ \eta = \eta^0 \circ \iota_{F^\bullet}$ as natural transformations $F \Rightarrow G^0$, and $\eta^\bullet$ commutes with connecting morphisms, i.e. for each short exact sequence $\underline{A}$ in $\mathcal{A}$ and $q \in \mathbf{Z}_{\geq 0}$, the following diagram commutes:

$$\begin{array}{ccc} F^q(A'') & \xrightarrow{\delta^q} & F^{q+1}(A') \\ \downarrow{\scriptstyle \eta^q_{A''}} & & \downarrow{\scriptstyle \eta^{q+1}_{A'}} \\ G^q(A'') & \xrightarrow{\delta^q} & G^{q+1}(A'). \end{array}$$

It is clear what the notion of a composition of δ-transformations should mean. The δ-transformation $\eta^\bullet$ is said to be a *δ-isomorphism* if there is a natural transformation $\theta : G \Rightarrow F$ and a δ-transformation $\theta^\bullet$ extending it such that $\theta^\bullet \circ \eta^\bullet = 1_{F^\bullet}$ and $\eta^\bullet \circ \theta^\bullet = 1_{G^\bullet}$.

[3] Naturality means that given a morphism $\underline{f} = (f', f, f'') : \underline{A} \to \underline{B}$ of short exact sequences in $\mathcal{A}$ and for each $q \geq 0$, we have $F^{q+1}(f') \circ \delta^q_{\underline{A}} = \delta^q_{\underline{B}} \circ F^q(f'')$ as maps $F^q(A'') \to F^{q+1}(B')$ in $\mathcal{B}$.

[4] Sometimes it *is* important to keep this distinction and the natural isomorphism ι in mind; in this case, we'll point it out. [TODO]

Finally, suppose $F : \mathcal{A} \to \mathcal{B}$ is an additive functor and $F^\bullet : \mathcal{A} \to \mathcal{B}$ a δ-functor extending F. The δ-functor $F^\bullet$ is said to be *universal* if it is exact, and if $G : \mathcal{A} \to \mathcal{B}$ is any other additive functor, $G^\bullet : \mathcal{A} \to \mathcal{B}$ a δ-functor extending G and $\eta : F \Rightarrow G$ a natural transformation, there is a unique δ-transformation $\eta^\bullet : F^\bullet \to G^\bullet$ extending η.

It follows that there is at most one universal δ-functor extending a given functor $F : \mathcal{A} \to \mathcal{B}$, up to unique δ-isomorphism extending the identity transformation $1_F : F \Rightarrow F$; in fact, any δ-transformation extending 1_F between universal δ-functors extending a given functor F must be a δ-isomorphism. A/"the" universal δ-functor extending $F : \mathcal{A} \to \mathcal{B}$ is called a/"the" *right derived functor* of F, and denoted $\mathsf{R}^\bullet F : \mathcal{A} \to \mathcal{B}$. Note that if F admits a right derived functor, then F is left-exact.

Remark 10.4.2. If $\mathsf{R}^\bullet F$ exists, then F is exact iff $\mathsf{R}^q F = 0$ for each $q \geq 1$ iff $\mathsf{R}^1 F = 0$.

Here's a simple criterion to check the universality of a δ-functor:

Definition 10.4.3. Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor between abelian categories.

- Given an $A \in \mathrm{Ob}(\mathcal{A})$, an *$F$-effacement* of A is a mono $i : A \to I$ such that $F(i) = 0$.
- The functor F is said to be *effaceable* if every $A \in \mathrm{Ob}(\mathcal{A})$ admits an F-effacement.

If F is effaceable, then F-effacements can be constructed functorially:

Lemma 10.4.4. Let $F : \mathcal{A} \to \mathcal{B}$ be an effaceable functor, and let $f : A \to A'$ be a morphism in $\mathcal{A}$. If $i : A \to I$ is any F-effacement, then there is an F-effacement $i' : A' \to I'$ and a morphism $\tilde{f} : I \to I'$ such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i'} \\ I & \xrightarrow{\tilde{f}} & I'; \end{array}$$

Proof. Let $j : I \oplus A' \hookrightarrow J$ be an F-effacement, and let $I' := \mathrm{coker}(A \xrightarrow{j \circ (i,f)} J)$. Let $i' : A' \to I'$ be the negative of the composite $A' \xrightarrow{\iota_{A'}} I \oplus A' \xrightarrow{j} J \twoheadrightarrow I'$, and $\tilde{f} : I \to I'$ be the composite $I \xrightarrow{\iota_I} I \oplus A' \xrightarrow{j} J \twoheadrightarrow I'$. ∎

Theorem 10.4.5. If $F^\bullet : \mathcal{A} \to \mathcal{B}$ is an exact δ-functor such that F^q is effaceable for each $q \geq 1$, then $F^\bullet$ is universal, and hence the right derived functor $\mathsf{R}^\bullet F^0$.

Proof. Given a δ-functor $G^\bullet$ and a natural transformation $\eta^0 : F^0 \Rightarrow G^0$, we recursively construct natural transformations $\eta^q : F^q \Rightarrow G^q$ that commute with the connecting homomorphisms. The base $q = 0$ is given; suppose $q \geq 1$. By effaceability, there is a monomorphism $i : A \to I$ with $F^q(i) = 0$. Consider the short exact sequence $0 \to A \xrightarrow{i} I \to I/A \to 0$ and the corresponding long sequences to get

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & F^{q-1}I & \longrightarrow & F^{q-1}(I/A) & \xrightarrow{\delta_F^{q-1}} & F^q A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \eta^{q-1}I} & & \downarrow{\scriptstyle \eta^{q-1}(I/A)} & & \vdots{\scriptstyle \exists!} & & \\ \cdots & \longrightarrow & G^{q-1}I & \longrightarrow & G^{q-1}(I/A) & \xrightarrow{\delta_G^{q-1}} & G^q A & \longrightarrow & \cdots \end{array}$$

The exactness of the top row proves the unique such a δ-transformation if one exists. We use the above to define the map $\eta^q A : F^q A \to G^q A$.

(a) This map is independent of the choice of effacement. Suppose that $i : A \to I$ and $i' : A \to I'$ are both F^q-effacements. Then so is $(i, i') : A \to I \oplus I'$ because $(i, i') = \iota_I \circ i + \iota_{I'} \circ i'$ and F^q is additive. Consider the morphism of SES's given by

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{(i,i')} & I \oplus I' & \longrightarrow & (I \oplus I')/A & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \pi_I} & & \downarrow{\scriptstyle \exists} & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & I & \longrightarrow & I/A & \longrightarrow & 0 \end{array}$$

Using this, the naturality of LES's for $F^\bullet$ and $G^\bullet$ and the naturality of η^{q-1}, it follows that the map $F^q A \to G^q A$ obtained in this way is the same for the effacement $i : A \to I$ and $(i, i') : A \to I \oplus I'$.

(b) The map η^q is a natural transformation. Suppose $f : A \to A'$ is a morphism. Then pick any effacements $i : A \to I$ and $i' : A' \to I'$ and morphism $\tilde{f} : I \to I'$ as in Lemma 10.4.4, and consider the morphism of SES's given by

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & I & \longrightarrow & I/A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \tilde{f}} & & \downarrow{\scriptstyle \exists} & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & I' & \longrightarrow & I'/A' & \longrightarrow & 0. \end{array}$$

Using this, the naturality of LES's for $F^\bullet$ and $G^\bullet$ and the naturality of η^{q-1}, we conclude that η^q is a natural transformation.

(c) Finally, η^q commutes with δ^{q-1}, i.e. given an SES $0 \to A' \to A \to A'' \to 0$ in $\mathcal{A}$, the diagram

$$\begin{array}{ccc} F^{q-1}A'' & \xrightarrow{\delta_F^{q-1}} & F^q A' \\ \downarrow{\scriptstyle \eta^{q-1}A''} & & \downarrow{\scriptstyle \eta^q A'} \\ G^{q-1}A'' & \xrightarrow{\delta_G^{q-1}} & G^q A' \end{array}$$

commutes. Indeed, note that if $i : A \to I$ is any F-effacement, then the map $A' \to A \xrightarrow{i} I$ is also an F-effacement. Then we get a morphism of SES's given by

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \exists} & & \\ 0 & \longrightarrow & A' & \longrightarrow & I & \longrightarrow & I/A' & \longrightarrow & 0 \end{array}$$

Using this, the naturality of LES's for $F^\bullet$ and $G^\bullet$ and the naturality of η^{q-1}, we get the result.

■

One general situation in which right derived functors of left-exact functors exists is when category $\mathcal{A}$ has enough injectives (so that every object has an injective resolution). This is a standard consequence of:

Lemma 10.4.6 (Fundamental Lemma of Homological Algebra)**.** In an abelian category $\mathcal{A}$, if $T \to J^\bullet$ is any resolution and $A \to I^\bullet$ an injective resolution, then any morphism $f : T \to A$ lifts to a morphism $f^\bullet : J^\bullet \to I^\bullet$ of complexes that extends f, and this extension is unique up to homotopy equivalence.

Proof. ■

Corollary 10.4.7. Let $F : \mathcal{A} \to \mathcal{B}$ be a left-exact additive functor of abelian categories. Suppose that $\mathcal{A}$ has enough injectives. Then the right derived functor $\mathsf{R}^\bullet F$ of F exists.

Proof. For each object A, pick an injective resolution $A[0] \to I^\bullet$ of A, apply F to this resolution to get the complex $F(I^\bullet)$, and define $F^q(A)$ to be the q^{th}-cohomology object of the complex $F(I^\bullet)$, namely

$$F^q(A) := \mathrm{H}^q(F(I^\bullet)) := \ker(FI^q \to FI^{q+1})/\operatorname{im}(FI^{q-1} \to FI^q).$$

Lemma 10.4.6 guarantees that the isomorphism type of $F^q(A)$ is independent of the choice of resolution, and that the construction F^q is functorial. Left-exactness of F implies that for each A, the map $F(A) \to F(I^0)$ induces an isomorphism $\iota_A : F(A) \to F^0(A)$, and naturality of ι_A in A follows again from Lemma 10.4.6. Finally, δ can be constructed by taking simultaneous resolutions and taking the long exact cohomology sequence corresponding to a short exact sequence of resolutions, with naturality following again from Lemma 10.4.6 and the naturality of long exact sequences. Finally, each F^q for $q \geq 1$ according to this definition is effaceable because an injective object is its own resolution, and we have assumed that $\mathcal{A}$ has enough injectives; therefore, universality follows from Theorem 10.4.5. ■

Example 10.4.8. Let $\mathcal{A}$ be an abelian category with enough injectives. Given a fixed object $M \in \mathrm{Ob}(\mathcal{A})$, the functor $\mathrm{Hom}_{\mathcal{A}}(M,-) : \mathcal{A} \to \mathsf{Ab}$ is left exact. The (components of the) right derived functor of this functor are called the Ext functors $\mathrm{Ext}^q_{\mathcal{A}}(M,-) : \mathcal{A} \to \mathsf{Ab}$ for $q \geq 0$, i.e. $\mathrm{Ext}^\bullet_{\mathcal{A}}(M,-) = \mathsf{R}^\bullet \mathrm{Hom}_{\mathcal{A}}(M,-)$. The reason for this name is that $\mathrm{Ext}^1_{\mathcal{A}}(M,N)$ classifies the extensions of M by N: given an extension $0 \to N \to E \to M \to 0$, the class in $\mathrm{Ext}^1_{\mathcal{A}}(M,N)$ is given by taking the image of $1_M \in \mathrm{Hom}_{\mathcal{A}}(M,M)$ under δ^0; on the other hand, given an element of $\mathrm{Ext}^1_{\mathcal{A}}(M,N)$, pick an SES $0 \to N \to I \to I/N \to 0$ with I injective to lift it to an element of $\varphi \in \mathrm{Hom}_{\mathcal{A}}(M, I/N)$, and then form the extension E as the pullback of $I \to I/N$ and $\varphi : M \to I/N$.

Unfortunately, this method is not very useful in practice because injective resolutions, even when they exist, are hard to write down by hand. To compute these derived functors in practice, one usually uses *acyclic resolutions*:

Definition 10.4.9. Let $F : \mathcal{A} \to \mathcal{B}$ be a left exact functor and suppose $\mathcal{A}$ has enough injectives, so that the right derived functor $\mathsf{R}^\bullet F$ exists.

(a) An object A of $\mathcal{A}$ is said to be *F-acyclic* if $\mathsf{R}^q F(A) = 0$ for all $q \geq 1$.
(b) A resolution $A[0] \to J^\bullet$ of A is an *F-acyclic resolution* if all the J^q for $q \geq 0$ are F-acyclic.

Lemma 10.4.10. In the set-up of the previous definition, if $A[0] \to J^\bullet$ is an F-acyclic resolution of an object A, then the right derived functors of F can be computed by taking the cohomology of $F(J^\bullet)$, i.e. for each $q \geq 0$, there is an isomorphism

$$\mathrm{H}^q(F(J^\bullet)) \xrightarrow{\sim} \mathsf{R}^q F(A).$$

Proof. Induct on q; the case $q = 0$ follows from the left exactness of F and the exact sequence $0 \to A \to J^0 \to J^1$. Next, to show $q = 1$, use $0 \to A \to J^0 \to J^0/A \to 0$ and $\mathsf{R}^1 F J^0 = 0$ to get

$$\operatorname{coker}\left(\mathsf{R}^0 F J^0 \to \mathsf{R}^0 F(J^0/A)\right) \xrightarrow{\sim} \mathsf{R}^1 FA,$$

and $0 \to J^0/A \to J^1 \to J^2$ to get

$$\mathsf{R}^0 F(J^0/A) \xrightarrow{\sim} \ker\left(\mathsf{R}^0 F J^1 \to \mathsf{R}^0 F J^2\right);$$

putting these together, we get $\mathrm{H}^1(F(J^\bullet)) \xrightarrow{\sim} \mathsf{R}^1 FA$. Finally, for $q \geq 2$, use inductively that there is an acyclic resolution $(J^0/A)[0] \to J^{\bullet+1}$ and the exact sequence $0 \to A \to J^0 \to J^0/A \to 0$ to get

$$\mathrm{H}^q(F(J^\bullet)) = \mathrm{H}^{q-1}(F(J^{\bullet+1})) \xrightarrow{\sim} \mathsf{R}^{q-1} F(J^0/A) \xrightarrow{\sim} \mathsf{R}^q FA.$$

■

Therefore, to compute derived functors of a functor F, it remains to identify appropriate F-acyclic objects. This can often be done using:

Lemma 10.4.11 (Acyclic Cohomology)**.** Let $F : \mathcal{A} \to \mathcal{B}$ be a left exact functor between abelian categories and suppose $\mathcal{A}$ has enough injectives. Let $\mathcal{T} \subset \mathrm{Ob}(\mathcal{A})$ be a class of objects in $\mathcal{A}$ such that:

(a) every injective object of $\mathcal{A}$ is in $\mathcal{T}$, and
(b) if $0 \to A' \to A \to A'' \to 0$ is exact and $A', A \in \mathcal{T}$, then $A'' \in \mathcal{T}$, and the resulting sequence $0 \to FA' \to FA \to FA'' \to 0$ is exact.

Then all elements of $\mathcal{T}$ are F-acyclic, so $\mathcal{T}$-resolutions can be used to compute the derived functor $\mathsf{R}^\bullet F$.

Proof. We show by induction on $q \geq 1$ that $\mathsf{R}^q F T = 0$ for all $T \in \mathcal{T}$. For $q = 1$, given a T, take a monomorphism $T \hookrightarrow I$ for injective I and consider the SES $0 \to T \to I \to I/T \to 0$. By the LES and (b), we get that $0 \to \mathsf{R}^1 FT \to \mathsf{R}^1 FI$ is exact, but $\mathsf{R}^1 FI = 0$ since I is injective and hence F-acyclic. For $q \geq 2$, the sequence $\mathsf{R}^{q-1} F(I/T) \to \mathsf{R}^q FT \to \mathsf{R}^q FI$ is exact, but the first term is zero by (a), (b), and induction; the last term is zero since I is F-acyclic as before. ■

10.5 Pathologies, or Counterexamples in Commutative Algebra

Example 10.5.1. A UFD R such that $R[\![X]\!]$ is not a UFD. Consider $S := k[x,y,z] := k[X,Y,Z](X^2 + Y^3 + Z^7)$, and the localization $R = S_{(x,y,z)}$. By Exercise 1.14(c), S and hence R is a UFD.

Example 10.5.2. A ring R and a prime $\mathfrak{p} \subset R$ such that $\operatorname{ht}\mathfrak{p} + \operatorname{coht}\mathfrak{p} < \dim R$. Consider the ring $R := k[\![X,Y,Z]\!]/(XY,XZ)$. Then $\dim R = 2$. If $\mathfrak{p} = (y,z) \subset R$, then $\mathfrak{p}$ is prime with $\operatorname{ht}\mathfrak{p} = 0$ but $\operatorname{coht}\mathfrak{p} = 1$.

Example 10.5.3. A zero-dimensional non-Noetherian ring. Take

$$R = k[\varepsilon_1, \varepsilon_2, \dots] := k[X_1, X_2, \dots]/(X_1^2, X_2^2, \dots).$$

This has a unique prime, namely $(\varepsilon_1, \varepsilon_2, \dots)$ and is hence zero dimensional; the increasing chain $0 \subset (\varepsilon_1) \subset (\varepsilon_1, \varepsilon_2) \subset \cdots$ show that R is non-Noetherian.

Example 10.5.4. A positive finite-dimensional non-Noetherian ring, and a domain in which the Krull intersection theorem fails. Valuation rings of dimension at least two are not Noetherian ([TO CITE]). The Krull dimension of a valuation ring is the height (i.e. number of isolated subgroups) of its value group. A standard example is the valuation ring of the $\mathbf{Z}^2$-valued valuation on $k(x,y)$ with $v(x^n y^m) = (n,m)$. This is also an example of a domain in which the Krull intersection theorem fails.

Example 10.5.5. (Nagata) An infinite-dimensional Noetherian ring. Let $R := k[X_1, X_2, \dots]$ and $m_1, m_2, \dots$ an increasing sequence of positive integers such that $m_{i+1} - m_i > m_i - m_{i-1}$ for all $i \geq 1$. 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.

Example 10.5.6. A nonzero module with no associated primes. Let $R = C(\mathbf{R}, \mathbf{R})$ be the ring of continuous functions $f : \mathbf{R} \to \mathbf{R}$. If $f \in R$ is a nonzero element, then there are $x \neq y \in \mathbf{R}$ such that $f(x)f(y) \neq 0$. Let $g, h \in R$ be functions such that $g(x) = h(y) = 1$ and $gh = 0$, then $g, h \notin \operatorname{Ann}(f)$ but $gh \in \operatorname{Ann}(f)$; consequently, $\operatorname{Ann}(f)$ is not prime. In particular, $\operatorname{Ass}_R(R) = \emptyset$.

Example 10.5.7. A separable field extension K/k that is not separably generated. Let $p > 0$ be a prime, $k = \mathbf{F}_p$ be a field let $K = k(X, X^{1/p}, X^{1/p^2}, \dots)$. On the one hand, k is perfect, and hence every extension K/k is separable. On the other hand, $k(X) \hookrightarrow K$ with K algebraic over $k(X)$ implies that $\operatorname{trdeg}_k K = 1$. If $f \in K$ is a separating transcendence basis, then K is separably algebraic over $k(f)$; but there is an $N \geq 1$ such that $f \in k(X^{1/p^N})$ and then $K/k(X^{1/p^N})$ is a nontrivial purely inseparable superextension, which is a contradiction.

10.6 Exercises

Exercise 10.1. Show that for any finite field $\mathbf{F}_q$, the only group homomorphism $(\mathbf{Q},+) \to (\mathbf{F}_q,+)$ is the trivial one.

Exercise 10.2. Let R be a ring. If $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ is an exact sequence of R-modules, each of finite length, then the lengths of these modules are related by $\sum_{i=1}^{n}(-1)^i \ell_R(M_i) = 0$.

Exercise 10.3. Using the structure theorem for finitely generated abelian groups, determine which of these have finite lengths (as $\mathbf{Z}$-modules). For the ones that do, determine their lengths and multisets of simple factors.

Exercise 10.4. Let $(R,\mathfrak{m},k)$ be a Noetherian local ring.

(a) Show that for each $i \geq 1$, the quotient $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ is a finite-dimensional vector space over k.
(b) Show that for any $n \geq 0$,

$$\ell_R(R/\mathfrak{m}^n) = \sum_{i=1}^{n} \dim_k(\mathfrak{m}^{i-1}/\mathfrak{m}^i).$$

Exercise 10.5.

(a) Let S be a set with a dependence relation $\mathscr{D}$ and let $\varphi : T \to S$ be any set map. Show that the map $\varphi^*\mathscr{D} : 2^T \to 2^T$ defined by $(\varphi^*\mathscr{D})(X) = \varphi^{-1}(\mathscr{D}(\varphi(X))$ for any $X \subset T$ is a dependence relation on T. This is called the *pullback of the relation* $\mathscr{D}$ under the map φ. What are the spanning sets of $\varphi^*\mathscr{D}$? What are the independent sets? What is its fundamental set? What can you say about the special situation in which the map φ is injective?
(b) 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 what is the dependency of the pullback relation $\varphi^*\mathrm{LD}$? What is its fundamental set?

Exercise 10.6. Let $\mathscr{D}$ and $\mathscr{E}$ be two dependence relations on the same set S. Consider the following conditions on S.

(a) For every subset $X \subset S$, we have $\mathscr{E}X \subset \mathscr{D}X$.
(b) For every subset $i_T : T \hookrightarrow S$, each $i_T^*\mathscr{E}$-spanning subset of T is $i_T^*\mathscr{D}$-spanning.
(c) Each $\mathscr{D}$-independent subset is $\mathscr{E}$-independent (and hence $\dep\mathscr{D} \leq \dep\mathscr{E}$).

Show that (a) $\Leftrightarrow$ (b) $\Rightarrow$ (c). Are all the conditions equivalent?

Exercise 10.7. Let $\mathscr{D}$ and $\mathscr{E}$ be two dependence relations on the same set S. Prove or disprove and salvage if possible: if the $\mathscr{D}$-independent subsets and $\mathscr{E}$-independent subsets coincide, then $\mathscr{D} = \mathscr{E}$.

Exercise 10.8. Let $G = (V,E)$ be a graph. Consider the map $\mathrm{Cl} : 2^E \to 2^E$ defined by saying that for any $X \subset E$, the set $\mathrm{Cl}X$ is the set edges whose endpoints are connected to each other by a path in X. Check that this defines a dependence relation on E; this is often called the graph closure operator. Explore the properties of this operator. What are spanning (resp. independent) subsets? What is a basis? When does it have finite dependency? What is the dependency of this relation? What is its fundamental set?

Exercise 10.9. Let V be a real vector space. A subset $K \subset V$ is said to be *convex* if for all $x, y \in K$ and $t \in [0,1]$ we have $tx + (1-t)y \in K$. Is the map $\mathrm{Conv} : 2^V \to 2^V$ sending a subset $X \subset V$ to its convex hull $\mathrm{Conv}(X)$, i.e. the intersection of all convex subsets of V containing X, a closure operator? Is it finitary? Does it satisfy MacLane-Steinitz exchange? How far can you generalize the notion of spanning sets, independent sets, bases, etc. for this operation?

Chapter 11

Possible Hints to Selected Exercises

Exercise 1.7(a). First replace the V_i by $U \cap V_i$ to reduce to the case $U = V$. Draw a picture.

Exercise 1.10. For the counterexample, consider the ring $R = C[0,1]$ of continuous functions $f : [0,1] \to \mathbf{R}$. For more on this, see [13].

Exercise 1.13. For (c) $\Rightarrow$ (b), show that the localization of R at the multiplicative subset generated by all primes in R is a field. For the alternative proof of implication (b) $\Rightarrow$ (a) in Corollary 1.4.5, suppose $\mathfrak{p} \subset R$ is a nonzero prime ideal but $\mathfrak{p} \cap S = \emptyset$. Use (c) and the ACCP hypothesis on R to produce a prime element $\pi \in S^{-1}\mathfrak{p}$ which lies in R and is not divisible by any element in S; then use Corollary 1.1.12(c). For the alternative proof of the key implication (a) $\Rightarrow$ (b) in Corollary 1.4.10, let $\mathfrak{p} \subset R[X]$ be a nonzero prime. If $\mathfrak{p} \cap R \neq (0)$, use Exercise 1.12(b). If $\mathfrak{p} \cap R = (0)$, then $\mathfrak{p}K[X]$ is prime by Corollary 1.1.12, and so contains an irreducible polynomial $f(X)$ in $K[X]$; then consider the primitive part of $f(X)$ and use Gauss's Lemma as in the proof of Corollary 1.4.10 given. See [11, Theorem A.4.5].

Exercise 1.14. We give hints for (b); (c) is similar. Work with the ring

$$S = \mathbf{C}[z,w,x_3,\ldots,x_n] := \mathbf{C}[Z,W,X_3,\ldots,X_n]/(ZW + X_3^2 + \cdots + X_n^2)$$

instead. Show that S is a domain, $z \in S$ is a prime element, and the elements $z, x_3, \ldots, x_n \in S$ are algebraically independent over $\mathbf{C}$ (this can be done by hand here, or using Example 5.2.4), whence $S[z^{-1}] \cong \mathbf{C}[Z,X_3,\ldots,X_n,Z^{-1}]$ is a UFD. Now finish using Corollary 1.4.5. In fact, the result in (b) is true over any field k of characteristic not two; this can be done first by adjoining a $\sqrt{-1}$ if needed and reducing to the above case, and then using "descent" from the field $k[\sqrt{-1}]$ to k. See [14, Theorem 6.2]. This ring (coordinate ring of the affine cone over smooth quadric four-fold) is the standard example of a ring that is factorial (i.e. a UFD) but not regular.

Exercise 3.6. Consider an ideal with the property that it does not contain a product of primes, and which is maximal with respect to inclusion.

Exercise 4.2(c). Consider $f(X) = X^5 + X^4 + X^2 + 1$, when $\sqrt{X} \in S$. If $f_0 \in k[X]$ is the polynomial of least degree such that $K(\sqrt{f_0}) = K(\sqrt{f})$, then $S = R[\sqrt{f_0}]$. When k is perfect, we can always choose $f_0 = X$. In general, f_0 can be found in terms of f; see [15, Example 4.23] (but beware the errors).

Exercise 5.4. Either consider a maximal ideal of $K \otimes_k L$, or fix a set Γ of sufficiently large cardinality and consider $\overline{k(\Gamma)}$.

Exercise 5.5. If L/k is finite, use the Theorem on Natural Irrationalities ([11, Theorem 5.5]).

Exercise 5.6(b). Here's one outline. Show that the natural map $\mathbf{F}[X,Y] \to K$ is injective and so yields an isomorphism $\mathbf{F}(X,Y) \to K$ of field extensions of $\mathbf{F}$; this reduces the problem to showing that $\mathbf{F}(X^p + sY^p) \subset \mathbf{F}(X,Y)$ is algebraically closed. Next, show that there is an $\mathbf{F}$-algebra homomorphism $\varphi : \mathbf{F}[X,Y] \to \mathbf{F}[s^{1/p}][T]$ with $\ker\varphi = (X^p + sY^p)$. Finally, suppose there is an $f \in \mathbf{F}(X,Y) \smallsetminus \mathbf{F}(X^p + sY^p)$ algebraic over the latter, and write $f = g/h$ for some nonzero coprime $g,h \in \mathbf{F}[X,Y]$ chosen so as to minimize the "size" $|f| = \deg_X g + \deg_X h$. Applying φ to a suitable equation adapted from the one demonstrating the algebraicity of f, produce another algebraic element of smaller size.

Exercise 5.9. When K is finite, a power of the minimal polynomial over L of a generator of K/k lies in $k[X]$.

Exercise 5.12. Consider an open subset $V \subset \mathrm{GL}_n \mathbf{C}$ containing the identity such that V does not contain any nontrivial subgroup of $\mathrm{GL}_n \mathbf{C}$.

Exercise 8.3. For (h) $\Rightarrow$ (d), use Baer's criterion. For (h) $\Rightarrow$ (a), use that a semisimple module has finite length iff it is finitely generated, and that if R is a direct simple of simple ideals, then the kernel of each projection map onto a factor is a maximal ideal.

Exercise 10.6. The conditions in (a) and (b) are said to define a *strong map* of matroids $\mathscr{E} \Rightarrow \mathscr{D}$, and (c) a *weak map* of matroids $\mathscr{E} \to \mathscr{D}$.

Exercise 10.8. First try to answer these questions when G is finite.

Bibliography

[1] A. Zaks, "Atomic Rings without a.c.c. on Principal Ideals," *Journal of Algebra*, vol. 74, pp. 223–231, 1982.

[2] K. Conrad, "Remarks about Euclidean Domains." Available online here.

[3] H. Perdry, "An Elementary Proof of Krull's Intersection Theorem," *The American Mathematical Monthly*, vol. 111, no. 4, pp. 356–357, 2004.

[4] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.

[5] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, vol. 150 of *Graduate Texts in Mathematics*. Springer, 1995.

[6] I. S. Cohen and A. Seidenberg, "Prime Ideals and Integral Dependence," *Bulletin of the American Mathematical Society*, vol. 52, pp. 252–261, 1946.

[7] A. Critch, "What does "linearly disjoint" mean for abstract field extensions?." MathOverflow. `https://mathoverflow.net/q/8324`(version: 2009-12-09).

[8] grghxy (https://math.stackexchange.com/users/239509/grghxy), "Does an inseparable extension have a purely inseparable element?." Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/1276333 (version: 2015-05-10).

[9] J. Harris, *Algebraic Geometry: A First Course*, vol. 133 of *Graduate Texts in Mathematics*. Springer, 1992.

[10] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, vol. 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, 2002.

[11] P. Morandi, *Fields and Galois Theory*, vol. 167 of *Graduate Texts in Mathematics*. Springer, 1996.

[12] H. Bruhn, R. Diestel, M. Kriesell, R. Pendavingh, and P. Wollan, "Axioms for Infinite Matroids," *Advances in Mathematics*, vol. 239, pp. 18–46, 2013.

[13] D. D. Anderson, M. Axtell, S. J. Forman, and J. Stickles, "When are associates unit multiples?," *Rocky Mountain J. Math.*, vol. 34, no. 3, Fall 2004. Available online here.

[14] G. Scheja and U. Storch, *Lehrbuch der Algebra: Unter Einschluß der linearen Algebra, Teil 2*. Mathematische Leitfäden, Vieweg+Teubner Verlag Wiesbaden, 1988.

[15] D. Lorenzini, *An Invitation to Arithmetic Geometry*, vol. 9 of *Graduate Studies in Mathematics*. American Mathematical Society, 1996.