18.705F11 Lecture Notes — Exercises

1. Rings and Ideals

Exercise **(1.5)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and $P := R[X_1, \ldots, X_n]$ the polynomial ring. Construct an isomorphism ψ from $P/\mathfrak{a}P$ onto $(R/\mathfrak{a})[X_1, \ldots, X_n]$.

Answer: Let $\kappa\colon R \to R/\mathfrak{a}$ be the quotient map. Form the homomorphism $\varphi\colon P \to (R/\mathfrak{a})[X_1, \ldots, X_n]$ such that $\varphi|R = \kappa$ and $\varphi(X_i) = X_i$. Then

$$\varphi\Big(\sum a_{(i_1,\ldots,i_n)} X_1^{i_1} \cdots X_n^{i_n}\Big) = \sum \kappa(a_{(i_1,\ldots,i_n)}) X_1^{i_1} \cdots X_n^{i_n}.$$

Since κ is surjective, so is φ. Since $\mathrm{Ker}(\kappa) = \mathfrak{a}$, it follows that

$$\mathrm{Ker}(\varphi) = \sum \mathfrak{a} X_1^{i_1} \cdots X_n^{i_n} = \mathfrak{a}P.$$

Therefore, φ induces the desired isomorphism ψ by (1.4.1). □

Exercise **(1.8)**. — Let R be ring, $P := R[X_1, \ldots, X_n]$ the polynomial ring. Let $m \le n$ and $a_1, \ldots, a_m \in R$. Set $\mathfrak{p} := \langle X_1 - a_1, \ldots, X_m - a_m \rangle$. Prove that $P/\mathfrak{p} = R[X_{m+1}, \ldots, X_n]$.

Answer: First, assume $m = n$. Set $P' := R[X_1, \ldots, X_{n-1}]$ and

$$\mathfrak{p}' := \langle X_1 - a_1, \ldots, X_{n-1} - a_{n-1} \rangle \subset P'.$$

By induction on n, we may assume $P'/\mathfrak{p}' = R$. However, $P = P'[X_n]$. Hence $P/\mathfrak{p}'P = (P'/\mathfrak{p}')[X_n]$ by (1.5). Thus $P/\mathfrak{p}'P = R[X_n]$.

We have $P/\mathfrak{p} = (P/\mathfrak{p}'P)\big/\mathfrak{p}(P/\mathfrak{p}'P)$ by (1.7). But $\mathfrak{p} = \mathfrak{p}'P + \langle X_n - a_n \rangle P$. Hence $\mathfrak{p}(P/\mathfrak{p}'P) = \langle X_n - a_n \rangle (P/\mathfrak{p}'P)$. So $P/\mathfrak{p} = R[X_n]/\langle X_n - a_n \rangle$. So $P/\mathfrak{p} = R$ by (1.6).

In general, $P = (R[X_1, \ldots, X_m])[X_{m+1}, \ldots, X_n]$. Thus $P/\mathfrak{p} = R[X_{m+1}, \ldots, X_n]$ by (1.5). □

Exercise **(1.12)** (*Chinese Remainder Theorem*). — Let R be a ring.

(1) Let $\mathfrak{a}$ and $\mathfrak{b}$ be *comaximal* ideals; that is, $\mathfrak{a} + \mathfrak{b} = R$. Prove

$$\text{(a)}\ \ \mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b} \quad \text{and} \quad \text{(b)}\ \ R/\mathfrak{ab} = (R/\mathfrak{a}) \times (R/\mathfrak{b}).$$

(2) Let $\mathfrak{a}$ be comaximal to both $\mathfrak{b}$ and $\mathfrak{b}'$. Prove $\mathfrak{a}$ is also comaximal to $\mathfrak{bb}'$.

(3) Let $\mathfrak{a}$, $\mathfrak{b}$ be comaximal, and $m, n \ge 1$. Prove $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are comaximal.

(4) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be pairwise comaximal. Prove

(a) $\mathfrak{a}_1$ and $\mathfrak{a}_2 \cdots \mathfrak{a}_n$ are comaximal;
(b) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$;
(c) $R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \xrightarrow{\sim} \prod (R/\mathfrak{a}_i)$.

Answer: To prove (1)(a), note that always $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Conversely, $\mathfrak{a} + \mathfrak{b} = R$ implies $x + y = 1$ with $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. So given $z \in \mathfrak{a} \cap \mathfrak{b}$, we have $z = xz + yz \in \mathfrak{ab}$.

To prove (1)(b), form the map $R \to R/\mathfrak{a} \times R/\mathfrak{b}$ that carries an element to its pair of residues. The kernel is $\mathfrak{a} \cap \mathfrak{b}$, which is $\mathfrak{ab}$ by (1). So we have an injection

$$\varphi\colon R/\mathfrak{ab} \hookrightarrow R/\mathfrak{a} \times R/\mathfrak{b}.$$

To show that φ is surjective, take any element $(\bar{x}, \bar{y})$ in $R/\mathfrak{a} \times R/\mathfrak{b}$. Say $\bar{x}$ and $\bar{y}$ are the residues of x and y. Since $\mathfrak{a} + \mathfrak{b} = R$, we can find $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = y - x$. Then $\varphi(x + a) = (\bar{x}, \bar{y})$, as desired. Thus (1) holds.

To prove (2), note that

$$R = (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}+\mathfrak{b}') = (\mathfrak{a}^2+\mathfrak{b}\mathfrak{a}+\mathfrak{a}\mathfrak{b}')+\mathfrak{b}\mathfrak{b}' \subseteq \mathfrak{a}+\mathfrak{b}\mathfrak{b}' \subseteq R.$$

To prove (3), note that (2) implies $\mathfrak{a}$ and $\mathfrak{b}^n$ are comaximal for any $n \ge 1$ by induction on n. Hence, $\mathfrak{b}^n$ and $\mathfrak{a}^m$ are comaximal for any $m \ge 1$.

To prove (4)(a), assume $\mathfrak{a}_1$ and $\mathfrak{a}_2 \cdots \mathfrak{a}_{n-1}$ are comaximal by induction on n. By hypothesis, $\mathfrak{a}_1$ and $\mathfrak{a}_n$ are comaximal. Thus (2) yields (a).

To prove (4)(b) and (4)(c), again proceed by induction on n. Thus (1) yields

$$\mathfrak{a}_1 \cap (\mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n) = \mathfrak{a}_1 \cap (\mathfrak{a}_2 \cdots \mathfrak{a}_n) = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n;$$
$$R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \xrightarrow{\sim} R/\mathfrak{a}_1 \times R/(\mathfrak{a}_2 \cdots \mathfrak{a}_n) \xrightarrow{\sim} \prod (R/\mathfrak{a}_i). \qquad \square$$

Exercise **(1.13)**. — First, given a prime number p and a $k \ge 1$, find the idempotents in $\mathbb{Z}/\langle p^k\rangle$. Second, find the idempotents in $\mathbb{Z}/\langle 12\rangle$. Third, find the number of idempotents in $\mathbb{Z}/\langle n\rangle$ where $n = \prod_{i=1}^N p_i^{n_i}$ with p_i distinct prime numbers.

Answer: First, let $m \in \mathbb{Z}$ be idempotent modulo p^k. Then $m(m-1)$ is divisible by p^k. So either m or $m-1$ is divisible by p^k, as m and $m-1$ have no common prime divisor. Hence 0 and 1 are the only idempotents in $\mathbb{Z}/\langle p^k\rangle$.

Second, since $-3+4=1$, the Chinese Remainder Theorem (1.12) yields

$$\mathbb{Z}/\langle 12\rangle = \mathbb{Z}/\langle 3\rangle \times \mathbb{Z}/\langle 4\rangle.$$

Hence m is idempotent modulo 12 if and only if m is idempotent modulo 3 and modulo 4. By the previous case, we have the following possibilities:

$$\begin{aligned} m &\equiv 0 \pmod 3 \quad\text{and}\quad m \equiv 0 \pmod 4;\\ m &\equiv 1 \pmod 3 \quad\text{and}\quad m \equiv 1 \pmod 4;\\ m &\equiv 1 \pmod 3 \quad\text{and}\quad m \equiv 0 \pmod 4;\\ m &\equiv 0 \pmod 3 \quad\text{and}\quad m \equiv 1 \pmod 4.\end{aligned}$$

Therefore, $m \equiv 0,\ 1,\ 4,\ 9 \pmod{12}$.

Third, for each i, the two numbers $p_1^{n_1} \cdots p_{i-1}^{n_{i-1}}$ and $p_i^{n_i}$ have no common prime divisor. Hence some linear combination is equal to 1 by the Euclidean Algorithm. So the principal ideals they generate are comaximal. Hence by induction on N, the Chinese Remainder Theorem yields

$$\mathbb{Z}/\langle n\rangle = \prod_{i=1}^N \mathbb{Z}/\langle p_i^{n_i}\rangle.$$

So m is idempotent modulo n if and only if m is idempotent modulo p^{n_i} for all i; hence, if and only if m is 0 or 1 modulo p^{n_i} for all i by the first case. Thus there are 2^N idempotents in $\mathbb{Z}/\langle n\rangle$. $\square$

Exercise **(1.14)**. — Let $R := R' \times R''$ be a *product* of rings, $\mathfrak{a} \subset R$ an ideal. Show $\mathfrak{a} = \mathfrak{a}' \times \mathfrak{a}''$ with $\mathfrak{a}' \subset R'$ and $\mathfrak{a}'' \subset R''$ ideals. Show $R/\mathfrak{a} = (R'/\mathfrak{a}') \times (R''/\mathfrak{a}'')$.

Answer: Set $\mathfrak{a}' := \{x' \mid (x', 0) \in \mathfrak{a}\}$ and $\mathfrak{a}'' := \{x'' \mid (0, x'') \in \mathfrak{a}\}$. Clearly $\mathfrak{a}' \subset R'$ and $\mathfrak{a}'' \subset R''$ are ideals. Clearly,

$$\mathfrak{a} \supset \mathfrak{a}' \times 0 + 0 \times \mathfrak{a}'' = \mathfrak{a}' \times \mathfrak{a}''.$$

The opposite inclusion holds, because if $\mathfrak{a} \ni (x', x'')$, then

$$\mathfrak{a} \ni (x', x'') \cdot (1, 0) = (x', 0) \quad\text{and}\quad \mathfrak{a} \ni (x', x'') \cdot (0, 1) = (0, x'').$$

Finally, the equation $R/\mathfrak{a} = (R/\mathfrak{a}') \times (R/\mathfrak{a}'')$ is now clear from the construction of the residue class ring. $\square$

2. Prime Ideals

Exercise **(2.2)**. — Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals, and $\mathfrak{p}$ a prime ideal. Prove that these conditions are equivalent: (1) $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$; and (2) $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{p}$; and (3) $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$.

Answer: Trivially, (1) implies (2). If (2) holds, then (3) follows as $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. Finally, assume $\mathfrak{a} \not\subset \mathfrak{p}$ and $\mathfrak{b} \not\subset \mathfrak{p}$. Then there are $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ with $x, y \notin \mathfrak{p}$. Hence, since $\mathfrak{p}$ is prime, $xy \notin \mathfrak{p}$. However, $xy \in \mathfrak{a}\mathfrak{b}$. Thus (3) implies (1). $\square$

Exercise **(2.4)**. — Given a prime number p and an integer $n \geq 2$, prove that the residue ring $\mathbb{Z}/\langle p^n \rangle$ does not contain a domain.

Answer: Any subring of $\mathbb{Z}/\langle p^n \rangle$ must contain 1, and 1 generates $\mathbb{Z}/\langle p^n \rangle$ as an abelian group. So $\mathbb{Z}/\langle p^n \rangle$ contains no proper subrings. However, $\mathbb{Z}/\langle p^n \rangle$ is not a domain, because in it, $p \cdot p^{n-1} = 0$ but neither p nor p^{n-1} is 0. $\square$

Exercise **(2.5)**. — Let $R := R' \times R''$ be a *product* of two rings. Show that R is a domain if and only if either R' or R'' is a domain and the other is 0.

Answer: Suppose R is a domain. Since $(1,0)\cdot(0,1) = (0,0)$, either $(1,0) = (0,0)$ or $(0,1) = (0,0)$. Correspondingly, either $R' = 0$ and $R = R''$, or $R'' = 0$ and $R = R''$. The assertion is now obvious. $\square$

Exercise **(2.10)**. — Let R be a domain, and $R[X_1, \ldots, X_n]$ the polynomial ring in n variables. Let $m \leq n$, and set $\mathfrak{p} := \langle X_1, \ldots, X_m \rangle$. Prove $\mathfrak{p}$ is a prime ideal.

Answer: Simply combine (2.9), (2.3), and (1.8) $\square$

Exercise **(2.11)**. — Let $R := R' \times R''$ be a *product* of rings. Show every prime ideal of R has the form $\mathfrak{p}' \times R''$ with $\mathfrak{p}' \subset R'$ prime or $R' \times \mathfrak{p}''$ with $\mathfrak{p}'' \subset R''$ prime.

Answer: Simply combine (1.14), (2.9), and (2.5). $\square$

Exercise **(2.15)**. — Let k be a field, R a nonzero ring, and $\varphi\colon k \to R$ a homomorphism. Prove φ is injective.

Answer: By (1.1), $1 \neq 0$ in R. So $\mathrm{Ker}(\varphi) \neq k$. So $\mathrm{Ker}(\varphi) = 0$ by (2.14). Thus φ is injective. $\square$

Exercise **(2.18)**. — Prove the following statements or give a counterexample.

(1) The complement of a multiplicative set is a prime ideal.
(2) Given two prime ideals, their intersection is prime.
(3) Given two prime ideals, their sum is prime.
(4) Given a ring homomorphism $\varphi\colon R \to R'$, the operation φ^{-1} carries maximal ideals of R' to maximal ideals of R.
(5) In (1.7), κ^{-1} takes maximal ideals of $R/\mathfrak{a}$ to maximal ideals of R.

Answer: (1) False. In the ring $\mathbb{Z}$, consider the set S of powers of 2. The complement T of S contains 3 and 5, but not 8; so T is not an ideal.

(2) False. In the ring $\mathbb{Z}$, consider the prime ideals $\langle 2\rangle$ and $\langle 3\rangle$; their intersection $\langle 2\rangle \cap \langle 3\rangle$ is equal to $\langle 6\rangle$, which is not prime.

(3) False. Since $2 \cdot 3 - 5 = 1$, we have $\langle 3\rangle + \langle 5\rangle = \mathbb{Z}$.

(4) False. Let $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. Then $\varphi^{-1}\langle 0\rangle = \langle 0\rangle$.

(5) True. The assertion is immediate from (1.7). □

Exercise **(2.21)**. — Prove that, in a PID, elements x and y are *relatively prime* (share no prime factor) if and only if the ideals $\langle x\rangle$ and $\langle y\rangle$ are comaximal.

Answer: Say $\langle x\rangle + \langle y\rangle = \langle d\rangle$. Then $d = \gcd(x, y)$, as is easy to check. The assertion is now obvious. □

Exercise **(2.24)**. — Preserve the setup of (2.23). Let $f := a_0X^n + \cdots + a_n$ be a polynomial of positive degree n. Assume that R has infinitely many prime elements p, or simply that there is a p such that $p \nmid a_0$. Show that $\langle f\rangle$ is not maximal.

Answer: Set $\mathfrak{a} := \langle p, f\rangle$. Then $\mathfrak{a} \supsetneqq \langle f\rangle$, because p is not a multiple of f. Set $k := R/\langle p\rangle$. Since p is irreducible, k is a domain by (2.6) and (2.8). Let $f' \in k[X]$ denote the image of f. By hypothesis, $\deg(f') = n \geq 1$. Hence f' is not a unit by (2.3) since k is a domain. Therefore, $\langle f'\rangle$ is proper. But $P/\mathfrak{a} \xrightarrow{\sim} k[X]/\langle f'\rangle$ by (1.5) and (1.7). So $\mathfrak{a}$ is proper. Thus $\langle f\rangle$ is not maximal. □

3. Radicals

Exercise **(3.6)**. — Let A be a ring, $\mathfrak{m}$ a maximal ideal such that $1+m$ is a unit for every $m \in \mathfrak{m}$. Prove A is local. Is this assertion still true if $\mathfrak{m}$ is not maximal?

Answer: Take $y \in A$. Let's prove that, if $y \notin \mathfrak{m}$, then y is a unit. Since $\mathfrak{m}$ is maximal, $\langle y\rangle + \mathfrak{m} = A$. Hence there exist $x \in R$ and $m \in \mathfrak{m}$ such that $xy + m = 1$, or in other words, $xy = 1 - m$. So xy is a unit by hypothesis; whence, y is a unit. Thus A is local by (3.4).

The assertion is not true if $\mathfrak{m}$ is not maximal. Indeed, take any ring that is not local, for example $\mathbb{Z}$, and take $\mathfrak{m} := \langle 0\rangle$. □

Exercise **(3.10)**. — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{p}$ an ideal of R. Prove

(1) there is an ideal $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ if and only if $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$;

(2) if $\mathfrak{p}$ is prime with $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$, then there's a prime $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Answer: In (1), given $\mathfrak{q}$, note $\varphi(\mathfrak{p}) \subset \mathfrak{q}$, as always $\varphi(\varphi^{-1}(\mathfrak{q})) \subset \mathfrak{q}$. So $\mathfrak{p}R' \subset \mathfrak{q}$. Hence $\varphi^{-1}(\mathfrak{p}R') \subset \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. But, always $\mathfrak{p} \subset \varphi^{-1}(\mathfrak{p}R')$. Thus $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$. The converse is trivial: take $\mathfrak{q} := \mathfrak{p}R'$.

In (2), set $S := \varphi(R - \mathfrak{p})$. Then $S \cap \mathfrak{p}R' = \emptyset$, as $\varphi(x) \in \mathfrak{p}R'$ implies $x \in \varphi^{-1}(\mathfrak{p}R')$ and $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$. So there's a prime $\mathfrak{q}$ of R' containing $\mathfrak{p}R'$ and disjoint from S by (3.9). So $\varphi^{-1}(\mathfrak{q}) \supset \varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$ and $\varphi^{-1}(\mathfrak{q}) \cap (R - \mathfrak{p}) = \emptyset$. Thus $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. □

Exercise **(3.11)**. — Use Zorn's lemma to prove that any prime ideal $\mathfrak{p}$ contains a minimal prime ideal.

Answer: Let $\mathcal{S}$ be the set of all prime ideals contained in $\mathfrak{p}$. Then $\mathfrak{p} \in \mathcal{S}$, so $\mathcal{S} \neq \emptyset$. Order $\mathcal{S}$ by reverse inclusion. To apply Zorn's Lemma, we must show that, for any decreasing chain $\{\mathfrak{p}_\lambda\}$ of prime ideals, the intersection $\mathfrak{p}_0 := \bigcap \mathfrak{p}_\lambda$ is a prime ideal. So take $x, y \notin \mathfrak{p}_0$. Then there exists λ such that $x, y \notin \mathfrak{p}_\lambda$. Since $\mathfrak{p}_\lambda$ is prime, $xy \notin \mathfrak{p}_\lambda$. Hence $xy \notin \mathfrak{p}_0$. Thus $\mathfrak{p}_0$ is prime. □

Exercise **(3.14)**. — Find the nilpotents in $\mathbb{Z}/\langle n\rangle$. In particular, take $n = 12$.

Answer: An integer m is nilpotent modulo n if and only if some power m^k is divisible by n. The latter holds if and only if every prime factor of n occurs in m. In particular, in $\mathbb{Z}/\langle 12\rangle$, the nilpotents are 0 and 6. □

Exercise **(3.15)**. — Let $\varphi\colon R \to R'$ be a ring map, $\mathfrak{b} \subset R'$ a subset. Prove

$$\varphi^{-1}\sqrt{\mathfrak{b}} = \sqrt{\varphi^{-1}\mathfrak{b}}.$$

Answer: Below, (1) is clearly equivalent to (2); and (2), to (3); and so forth:

(1) $x \in \varphi^{-1}\sqrt{\mathfrak{b}}$;	(4) $\varphi(x^n) \in \mathfrak{b}$ for some n;
(2) $\varphi x \in \sqrt{\mathfrak{b}}$;	(5) $x^n \in \varphi^{-1}\mathfrak{b}$ for some n;
(3) $(\varphi x)^n \in \mathfrak{b}$ for some n;	(6) $x \in \sqrt{\varphi^{-1}\mathfrak{b}}$. □

Exercise **(3.16)**. — Let R be a ring, $\mathfrak{a} \subset \sqrt{\langle 0\rangle}$ an ideal, and $P := R[Y]$ the polynomial ring in one variable. Let $u \in R$ be a unit, and $x \in R$ a nilpotent.

(1) Prove (a) that $u + x$ is a unit in R and (b) that $u + xY$ is a unit in P.
(2) Suppose $w \in R$ maps to a unit of $R/\mathfrak{a}$. Prove that w is a unit in R.

Answer: In (1), say $x^n = 0$. Set $y := -xu^{-1}$. Then (a) holds as

$$(u + x) \cdot u^{-1}(1 + y + y^2 + \cdots + y^{n-1}) = 1.$$

Now, u is also a unit in P, and $(xY)^n = 0$; hence, (a) implies (b).

In (2), say $wy \in R$ maps to $1 \in R/\mathfrak{a}$. Set $z := wy - 1$. Then $z \in \mathfrak{a}$, so z is nilpotent. Hence, $1+z$ is a unit by (1)(a). So wy is a unit. Then $w \cdot y(wy)^{-1} = 1$. □

Exercise **(3.19)**. — Let R be a ring, and $\mathfrak{a}$ an ideal. Assume $\sqrt{\mathfrak{a}}$ is finitely generated. Show there is an $n \geq 1$ such that $\big(\sqrt{\mathfrak{a}}\big)^n \subset \mathfrak{a}$.

Answer: Let $x_1, \ldots, x_m$ be generators of $\sqrt{\mathfrak{a}}$. For each i, there is n_i such that $x_i^{n_i} \in \mathfrak{a}$. Set $n := 1 + \sum(n_i - 1)$. Given $a \in \sqrt{\mathfrak{a}}$, write $a = \sum_{i=1}^m y_i x_i$ with $y_i \in R$. Then a^n is a linear combination of terms of the form $x_1^{j_1} \cdots x_m^{j_m}$ with $\sum_{i=1}^m j_i = n$. Hence $j_i \geq n$ for some i, because if $j_i \leq n_i - 1$ for all i, then $\sum j_i \leq \sum(n_i - 1)$. Thus $a^n \in \mathfrak{a}$, as desired. □

Exercise **(3.20)**. — Let R be a ring, $\mathfrak{q}$ an ideal, $\mathfrak{p}$ a finitely generated prime. Prove that $\mathfrak{p} = \sqrt{\mathfrak{q}}$ if and only if there is $n \geq 1$ such that $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$.

Answer: If $\mathfrak{p} = \sqrt{\mathfrak{q}}$, then $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$ by (3.19). Conversely, if $\mathfrak{q} \supset \mathfrak{p}^n$, then clearly $\sqrt{\mathfrak{q}} \supset \mathfrak{p}$. Further, since $\mathfrak{p}$ is prime, if $\mathfrak{p} \supset \mathfrak{q}$, then $\mathfrak{p} \supset \sqrt{\mathfrak{q}}$. □

Exercise **(3.22)**. — Let R be a ring. Assume R is reduced and has finitely many minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Prove that $\varphi\colon R \to \prod(R/\mathfrak{p}_i)$ is injective, and for each i, there is some $(x_1, \ldots, x_n) \in \mathrm{Im}(\varphi)$ with $x_i \neq 0$ but $x_j = 0$ for $j \neq i$.

Answer: Clearly $\mathrm{Ker}(\varphi) = \bigcap \mathfrak{p}_i$. Now, R is reduced and the $\mathfrak{p}_i$ are its minimal primes; hence, (3.17) and (3.11) yield

$$\langle 0\rangle = \sqrt{\langle 0\rangle} = \bigcap \mathfrak{p}_i.$$

Thus $\mathrm{Ker}(\varphi) = \langle 0\rangle$, and so φ is injective.

Finally, fix i. Since $\mathfrak{p}_i$ is minimal, $\mathfrak{p}_i \not\supset \mathfrak{p}_j$ for $j \neq i$; say $a_j \in \mathfrak{p}_j - \mathfrak{p}_i$. Set $a := \prod_{j\neq i} a_j$. Then $a \in \mathfrak{p}_j - \mathfrak{p}_i$ for all $j \neq i$. Thus $\mathrm{Im}(\varphi)$ meets $R/\mathfrak{p}_i$. □

4. Modules

Exercise **(4.3)**. — Let R be a ring, M a module. Consider the set map

$$\theta\colon \mathrm{Hom}(R, M) \to M \quad \text{defined by} \quad \theta(\rho) := \rho(1).$$

Show that θ is an isomorphism, and describe its inverse.

Answer: First off, θ is R-linear, because

$$\theta(x\rho + x'\rho') = (x\rho + x'\rho')(1) = x\rho(1) + x'\rho'(1) = x\theta(\rho) + x'\theta(\rho').$$

Set $H := \mathrm{Hom}(R, M)$. Define $\eta\colon M \to H$ by $\eta(m)(x) := xm$. It is easy to check that $\eta\theta = 1_H$ and $\theta\eta = 1_M$. Thus θ and η are inverse isomorphisms by (4.2). □

Exercise **(4.12)**. — Let R be a domain, and $x \in R$ nonzero. Let M be the submodule of $\mathrm{Frac}(R)$ generated by $1,\ x^{-1},\ x^{-2}, \ldots$. Suppose that M is finitely generated. Prove that $x^{-1} \in R$, and conclude that $M = R$.

Answer: Suppose M is generated by $m_1, \ldots, m_k$. Say $m_i = \sum_{j=0}^{n_i} a_{ij}x^{-j}$ for some n_i and $a_{ij} \in R$. Set $n := \max\{n_i\}$. Then $1,\ x^{-1}, \ldots, x^{-n}$ generate M. So

$$x^{-(n+1)} = a_n x^{-n} + \cdots + a_1 x^{-1} + a_0$$

for some $a_i \in R$. Thus

$$x^{-1} = a_n + \cdots + a_1 x^{n-1} + a_0 x^n \in R.$$

Finally, as $x^{-1} \in R$ and R is a ring, also $1,\ x^{-1},\ x^{-2}, \ldots \in R$; so $M \subset R$. Conversely, $M \supset R$ as $1 \in M$. Thus $M = R$. □

Exercise **(4.14)**. — Let Λ be an infinite set, R_λ a ring for $\lambda \in \Lambda$. Endow $\prod R_\lambda$ and $\bigoplus R_\lambda$ with componentwise addition and multiplication. Show that $\prod R_\lambda$ has a multiplicative identity (so is a ring), but that $\bigoplus R_\lambda$ does not (so is not a ring).

Answer: Consider the vector (1) whose every component is 1. Obviously, (1) is a multiplicative identity of $\prod R_\lambda$. On the other hand, no restricted vector (e_λ) can be a multiplicative identity in $\bigoplus R_\lambda$; indeed, because Λ is infinite, e_μ must be zero for some μ. So $(e_\lambda) \cdot (x_\lambda) \neq (x_\lambda)$ if $x_\mu \neq 0$. □

Exercise **(4.15)**. — Let R be a ring, L, M, and N modules. Consider a diagram

$$L \underset{\rho}{\overset{\alpha}{\rightleftarrows}} M \underset{\sigma}{\overset{\beta}{\rightleftarrows}} N$$

where α, β, ρ, and σ are homomorphisms. Prove that

$$M = L \oplus N \quad \text{and} \quad \alpha = \iota_L,\ \beta = \pi_N,\ \sigma = \iota_N,\ \rho = \pi_L$$

if and only if the following relations hold:

$$\beta\alpha = 0,\ \beta\sigma = 1,\ \rho\sigma = 0,\ \rho\alpha = 1,\ \text{and } \alpha\rho + \sigma\beta = 1.$$

Answer: If $M = L \oplus N$ and $\alpha = \iota_L$, $\beta = \pi_N$, $\sigma = \iota_N$, $\rho = \pi_L$, then the definitions immediately yield $\alpha\rho + \sigma\beta = 1$ and $\beta\alpha = 0$, $\beta\sigma = 1$, $\rho\sigma = 0$, $\rho\alpha = 1$.

Conversely, assume $\alpha\rho + \sigma\beta = 1$ and $\beta\alpha = 0$, $\beta\sigma = 1$, $\rho\sigma = 0$, $\rho\alpha = 1$. Consider the maps $\varphi\colon M \to L \oplus N$ and $\theta\colon L \oplus N \to M$ given by $\varphi m := (\rho m,\, \beta m)$ and $\theta(l, n) := \alpha l + \sigma n$. They are inverse isomorphisms, because

$$\varphi\theta(l, n) = (\rho\alpha l + \rho\sigma n,\ \beta\alpha l + \beta\sigma n) = (l, n) \quad \text{and} \quad \theta\varphi m = \alpha\rho m + \sigma\beta m = m.$$

Lastly, $\beta = \pi_N\varphi$ and $\rho = \pi_L\varphi$ by definition of φ, and $\alpha = \theta\iota_L$ and $\sigma = \theta\iota_N$ by definition of θ. □

Exercise **(4.16)**. — Let R be a ring, N a module, Λ a set, M_λ a module for $\lambda \in \Lambda$. Show that the injections $\iota_\kappa\colon M_\kappa \to \bigoplus M_\lambda$ induce an injection

$$\bigoplus \operatorname{Hom}(N,\, M_\lambda) \hookrightarrow \operatorname{Hom}(N,\, \bigoplus M_\lambda),$$

and that it is an isomorphism if N is finitely generated.

Answer: For $\lambda \in \Lambda$, let $\alpha_\lambda\colon N \to M_\lambda$ be maps, almost all 0. Then

$$\big(\sum \iota_\lambda\alpha_\lambda\big)(n) = \big(\alpha_\lambda(n)\big) \in \bigoplus M_\lambda.$$

So if $\sum \iota_\lambda\alpha_\lambda = 0$, then $\alpha_\lambda = 0$ for all λ. Thus the ι_κ induce an injection.

Assume N is finitely generated, say by $n_1, \dots, n_k$. Let $\alpha\colon N \to \bigoplus M_\lambda$ be a map. Then each $\alpha(n_i)$ lies in a finite direct subsum of $\bigoplus M_\lambda$. So $\alpha(N)$ lies in one too. Set $\alpha_\kappa := \pi_\kappa\alpha$ for all $\kappa \in \Lambda$. Then almost all α_κ vanish. So (α_κ) lies in $\bigoplus \operatorname{Hom}(N,\, M_\lambda)$, and $\sum \iota_\kappa\alpha_\kappa = \alpha$. Thus the ι_κ induce a surjection, so an isomorphism. □

Exercise **(4.17)**. — Let R be a ring, $\mathfrak{a}$ an ideal, Λ a set, M_λ a module for $\lambda \in \Lambda$. Show $\mathfrak{a}\big(\bigoplus M_\lambda\big) = \bigoplus \mathfrak{a}M_\lambda$. Show $\mathfrak{a}\big(\prod M_\lambda\big) = \prod \mathfrak{a}M_\lambda$ if $\mathfrak{a}$ is finitely generated.

Answer: First, $\mathfrak{a}\big(\bigoplus M_\lambda\big) \subset \bigoplus \mathfrak{a}M_\lambda$ because $a \cdot (m_\lambda) = (am_\lambda)$. Conversely, $\mathfrak{a}\big(\bigoplus M_\lambda\big) \supset \bigoplus \mathfrak{a}M_\lambda$ because $(a_\lambda m_\lambda) = \sum a_\lambda\iota_\lambda m_\lambda$ since the sum is finite.

Second, $\mathfrak{a}\big(\prod M_\lambda\big) \subset \prod \mathfrak{a}M_\lambda$ as $a(m_\lambda) = (am_\lambda)$. Conversely, say $\mathfrak{a}$ is generated by $f_1, \dots, f_n$. Then $\mathfrak{a}\big(\prod M_\lambda\big) \supset \prod \mathfrak{a}M_\lambda$. Indeed, take $(m'_\lambda) \in \prod \mathfrak{a}M_\lambda$. Then for each λ, there is n_λ such that $m'_\lambda = \sum_{j=1}^{n_\lambda} a_{\lambda j}m_{\lambda j}$ with $a_{\lambda j} \in \mathfrak{a}$ and $m_{\lambda j} \in M_\lambda$. Write $a_{\lambda j} = \sum_{i=1}^{n} x_{\lambda ji}f_i$ with $x_{\lambda ji} \in R$. Then

$$(m'_\lambda) = \bigg(\sum_{j=1}^{n_\lambda}\sum_{i=1}^{n} f_i x_{\lambda ji} m_{\lambda j}\bigg) = \sum_{i=1}^{n} f_i \bigg(\sum_{j=1}^{n_\lambda} x_{\lambda ji} m_{\lambda j}\bigg) \in \mathfrak{a}\Big(\prod M_\lambda\Big). \qquad \square$$

5. Exact Sequences

Exercise **(5.5)**. — Let M' and M'' be modules, $N \subset M'$ a submodule. Set $M := M' \oplus M''$. Using (5.3)(1) and (5.4) and (5.2), prove $M/N = M'/N \oplus M''$.

Answer: By (5.3)(1) and (5.4), the two sequences $0 \to M'' \to M'' \to 0$ and $0 \to N \to M' \to M'/N \to 0$ are exact. So by (5.2), the sequence

$$0 \to N \to M' \oplus M'' \to (M'/N) \oplus M'' \to 0$$

is exact. Thus (5.4) yields the assertion. □

Exercise **(5.6)**. — Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Prove that, if M' and M'' are finitely generated, then so is M.

Answer: Let $m''_1, \dots, m''_n \in M$ map to elements generating M''. Let $m \in M$, and write its image in M'' as a linear combination of the images of the m''_i. Let $m'' \in M$ be the same combination of the m''_i. Set $m' := m - m''$. Then m' maps to 0 in M''; so m' is the image of an element of M'.

Let $m'_1, \dots, m'_l \in M$ be the images of elements generating M'. Then m' is a linear combination of the m'_j. So m is a linear combination of the m''_i and m'_j. Thus the m'_i and m''_j together generate M. □

Exercise **(5.10)**. — Let M', M'' be modules, and set $M := M' \oplus M''$. Let N be a submodule of M containing M', and set $N'' := N \cap M''$. Prove $N = M' \oplus N''$.

Answer: Form the sequence $0 \to M' \to N \to \pi_{M''}N \to 0$. It splits by (5.9) as $(\pi_{M'}|N) \circ \iota_{M'} = 1_{M'}$. Finally, if $(m', m'') \in N$, then $(0, m'') \in N$ as $M' \subset N$; hence, $\pi_{M''}N = N''$. □

Exercise **(5.11)**. — Criticize the following misstatement of (5.9): given a short exact sequence $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$, there is an isomorphism $M \simeq M' \oplus M''$ if and only if there is a section $\sigma\colon M'' \to M$ of β.

Answer: We have $\alpha\colon M' \to M$, and $\iota_{M'}\colon M' \to M' \oplus M''$, but (5.9) requires that they be compatible with the isomorphism $M \simeq M' \oplus M''$, and similarly for $\beta\colon M \to M''$ and $\pi_{M''}\colon M' \oplus M'' \to M''$.

Let's construct a counterexample (due to B. Noohi). For each integer $n \ge 2$, let M_n be the direct sum of countably many copies of $\mathbb{Z}/\langle n\rangle$. Set $M := \bigoplus M_n$.

First, let us check these two statements:

(1) For any finite abelian group G, we have $G \oplus M \simeq M$.
(2) For any finite subgroup $G \subset M$, we have $M/G \simeq M$.

Statement (1) holds since G is isomorphic to a direct sum of copies of $\mathbb{Z}/\langle n\rangle$ for various n by the structure theorem for finite abelian groups [**Artin**, (6.4), p. 472].

To prove (2), write $M = B \bigoplus M'$, where B contains G and involves only finitely many components of M. Then $M' \simeq M$. Therefore, (5.10) and (1) yield

$$M/G \simeq (B/G) \oplus M' \simeq M.$$

To construct the counterexample, let p be a prime number. Take one of the $\mathbb{Z}/\langle p^2\rangle$ components of M, and let $M' \subset \mathbb{Z}/\langle p^2\rangle$ be the cyclic subgroup of order p. There is no retraction $\mathbb{Z}/\langle p^2\rangle \to M'$, so there is no retraction $M \to M'$ either, since the latter would induce the former. Finally, take $M'' := M/M'$. Then (1) and (2) yield $M \simeq M' \oplus M''$. □

Exercise **(5.13)**. — Referring to (4.8), give an alternative proof that β is an isomorphism by applying the Snake Lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & N/M & \longrightarrow & 0 \\ & & \big\downarrow & & \big\downarrow{\scriptstyle\kappa} & & \big\downarrow{\scriptstyle\beta} & & \\ 0 & \to & M/L & \to & N/L & \xrightarrow{\lambda} & (N/L)\big/(M/L) & \to & 0 \end{array}$$

Answer: The Snake Lemma yields an exact sequence,

$$L \xrightarrow{1} L \to \mathrm{Ker}(\beta) \to 0;$$

hence, $\mathrm{Ker}(\beta) = 0$. Moreover, β is surjective because κ and λ are. □

Exercise **(5.14)** (*Five Lemma*). — Consider this commutative diagram:

$$\begin{array}{ccccccccc} M_4 & \xrightarrow{\alpha_4} & M_3 & \xrightarrow{\alpha_3} & M_2 & \xrightarrow{\alpha_2} & M_1 & \xrightarrow{\alpha_1} & M_0 \\ {\scriptstyle\gamma_4}\downarrow & & {\scriptstyle\gamma_3}\downarrow & & {\scriptstyle\gamma_2}\downarrow & & {\scriptstyle\gamma_1}\downarrow & & {\scriptstyle\gamma_0}\downarrow \\ N_4 & \xrightarrow{\beta_4} & N_3 & \xrightarrow{\beta_3} & N_2 & \xrightarrow{\beta_2} & N_1 & \xrightarrow{\beta_1} & N_0 \end{array}$$

Assume it has exact rows. Via a chase, prove these two statements:

(1) If γ_3 and γ_1 are surjective and if γ_0 is injective, then γ_2 is surjective.
(2) If γ_3 and γ_1 are injective and if γ_4 is surjective, then γ_2 is injective.

Answer: Let's prove (1). Take $n_2 \in N_2$. Since γ_1 is surjective, there is $m_1 \in M_1$ such that $\gamma_1(m_1) = \beta_2(n_2)$. Then $\gamma_0\alpha_1(m_1) = \beta_1\gamma_1(m_1) = \beta_1\beta_2(n_2) = 0$ by commutativity and exactness. Since γ_0 is injective, $\alpha_1(m_1) = 0$. Hence exactness yields $m_2 \in M_2$ with $\alpha_2(m_2) = m_1$. So $\beta_2(\gamma_2(m_2) - n_2) = \gamma_1\alpha_2(m_2) - \beta_2(n_2) = 0$.

Hence exactness yields $n_3 \in N_3$ with $\beta_3(n_3) = \gamma_2(m_2) - n_2$. Since γ_3 is surjective, there is $m_3 \in M_3$ with $\gamma_3(m_3) = n_3$. Then $\gamma_2\alpha_3(m_3) = \beta_3\gamma_3(m_3) = \gamma_2(m_2) - n_2$. Hence $\gamma_2(m_2 - \alpha_3(m_3)) = n_2$. Thus γ_2 is surjective.

The proof of (2) is similar. □

Exercise **(5.15)** (*Nine Lemma*). — Consider this commutative diagram:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & L' & \to & L & \to & L'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M' & \to & M & \to & M'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & N' & \to & N & \to & N'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Assume all the columns are exact and the middle row is exact. Prove that the first row is exact if and only if the third is.

Answer: The first row is exact if the third is owing to the Snake Lemma (5.12) applied to the bottom two rows. The converse is proved similarly. □

Exercise **(5.16)**. — Consider this commutative diagram with exact rows:

$$\begin{array}{ccccc} M' & \xrightarrow{\beta} & M & \xrightarrow{\gamma} & M'' \\ {\scriptstyle\alpha'}\downarrow & & {\scriptstyle\alpha}\downarrow & & {\scriptstyle\alpha''}\downarrow \\ N' & \xrightarrow{\beta'} & N & \xrightarrow{\gamma'} & N'' \end{array}$$

Assume α' and γ are surjective. Given $n \in N$ and $m'' \in M''$ with $\alpha''(m'') = \gamma'(n)$, show that there is $m \in M$ such that $\alpha(m) = n$ and $\gamma(m) = m''$.

Answer: Since γ is surjective, there is $m_1 \in M$ with $\gamma(m_1) = m''$. Then $\gamma'\big(n-\alpha(m_1)\big) = 0$ as $\alpha''(m'') = \gamma'(n)$ and as the right-hand square is commutative. So by exactness of the bottom row, there is $n' \in N'$ with $\beta'(n') = n-\alpha(m_1)$. Since α' is surjective, there is $m' \in M'$ with $\alpha'(m') = n'$. Set $m := m_1 + \beta(m')$. Then $\gamma(m) = m''$ as $\gamma\beta = 0$. Further, $\alpha(m) = \alpha(m_1)+\beta'(n') = n$ as the left-hand square is commutative. Thus m works. □

Exercise **(5.21)**. — Show that a free module $R^{\oplus\Lambda}$ is projective.

Answer: Given $\beta\colon M \twoheadrightarrow N$ and $\alpha\colon R^{\oplus\Lambda} \to N$, use the UMP of (4.10) to define $\gamma\colon R^{\oplus\Lambda} \to M$ by sending the standard basis vector e_λ to any *lift* of $\alpha(e_\lambda)$, that is, any $m_\lambda \in M$ with $\beta(m_\lambda) = \alpha(e_\lambda)$. (Note that the Axiom of Choice is needed to make a simultaneous choice of all lifts if Λ is infinite.) Clearly $\alpha = \beta\gamma$. Thus $R^{\oplus\Lambda}$ is projective. □

6. Direct limits

Exercise **(6.3)**. — (1) Show that the condition (6.2)(1) is equivalent to the commutativity of the corresponding diagram:

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{C}}(B,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \\
\downarrow & & \downarrow \\
\mathrm{Hom}_{\mathcal{C}}(A,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(C)\big)
\end{array}$$

(2) Given $\gamma\colon C \to D$, show (6.2)(1) yields the commutativity of this diagram:

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{C}}(B,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \\
\downarrow & & \downarrow \\
\mathrm{Hom}_{\mathcal{C}}(A,D) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(D)\big)
\end{array}$$

Answer: The left-hand vertical map is given by composition with α, and the right-hand vertical map is given by composition with $F(\alpha)$. So the composition of the top map and the right-hand map sends β to $F(\beta)F(\alpha)$, whereas the composition of the left-hand map with the bottom map sends β to $F(\beta\alpha)$. These two images are always equal if and only if the diagram commutes. Thus (1) holds if and only if the diagram commutes.

As to (2), the argument is similar. □

Exercise **(6.5)**. — Let $\mathcal{C}$ and $\mathcal{C}'$ be categories, $F\colon \mathcal{C} \to \mathcal{C}'$ and $F'\colon \mathcal{C}' \to \mathcal{C}$ an adjoint pair. Let $\varphi_{A,A'}\colon \mathrm{Hom}_{\mathcal{C}'}(FA,\, A') \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(A,\, F'A')$ denote the natural bijection, and set $\eta_A := \varphi_{A,FA}(1_{FA})$. Do the following:

(1) Prove η_A is natural in A; that is, given $g\colon A \to B$, the induced square

$$\begin{array}{ccc}
A & \xrightarrow{\eta_A} & F'FA \\
{\scriptstyle g}\downarrow & & \downarrow{\scriptstyle F'Fg} \\
B & \xrightarrow{\eta_B} & F'FB
\end{array}$$

is commutative. We call the natural transformation $A \mapsto \eta_A$ the *unit* of $(F,\, F')$.

(2) Given $f'\colon FA \to A'$, prove $\varphi_{A,A'}(f') = F'f' \circ \eta_A$.

(3) Prove the natural map $\eta_A\colon A \to F'FA$ is *universal* from A to F'; that is,

given $f\colon A \to F'A'$, there is a unique map $f'\colon FA \to A'$ with $F'f' \circ \eta_A = f$.

(4) Conversely, instead of assuming (F, F') is an adjoint pair, assume given a natural transformation $\eta\colon 1_{\mathcal{C}} \to F'F$ satisfying (1) and (3). Prove the equation in (2) defines a natural bijection making (F, F') an adjoint pair, whose unit is η.

(5) Identify the units in the two examples in (6.4): the "free module" functor and the "polynomial ring" functor.

(Dually, we can define a *counit* $\varepsilon\colon FF' \to 1_{\mathcal{C}'}$, and prove similar statements.)

ANSWER: For (1), form this canonical diagram, with horizontal induced maps:

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathcal{C}'}(FA,\, FA) & \xrightarrow{(Fg)_*} & \mathrm{Hom}_{\mathcal{C}'}(FA,\, FB) & \xleftarrow{(Fg)^*} & \mathrm{Hom}_{\mathcal{C}'}(FB,\, FB) \\
\Big\downarrow{\scriptstyle \varphi_{A,\,FA}} & & \Big\downarrow{\scriptstyle \varphi_{A,\,FB}} & & \Big\downarrow{\scriptstyle \varphi_{B,\,FB}} \\
\mathrm{Hom}_{\mathcal{C}}(A,\, F'FA) & \xrightarrow{(F'Fg)_*} & \mathrm{Hom}_{\mathcal{C}}(A,\, F'FB) & \xleftarrow{g^*} & \mathrm{Hom}_{\mathcal{C}}(B,\, F'FB)
\end{array}$$

It commutes since φ is natural. Follow 1_{FA} out of the upper left corner to find $F'Fg \circ \eta_A = \varphi_{A,\,FB}(g)$ in $\mathrm{Hom}_{\mathcal{C}}(A,\, F'FB)$. Follow 1_{FB} out of the upper right corner to find $\varphi_{A,\,FB}(g) = \eta_B \circ g$ in $\mathrm{Hom}_{\mathcal{C}}(A,\, F'FB)$. Thus $(F'Fg) \circ \eta_A = \eta_B \circ g$.

For (2), form this canonical commutative diagram:

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{C}'}(FA,\, FA) & \xrightarrow{f'_*} & \mathrm{Hom}_{\mathcal{C}'}(FA, A') \\
\Big\downarrow{\scriptstyle \varphi_{A,\,FA}} & & \Big\downarrow{\scriptstyle \varphi_{A,A'}} \\
\mathrm{Hom}_{\mathcal{C}}(A,\, F'FA) & \xrightarrow{(F'f')_*} & \mathrm{Hom}_{\mathcal{C}}(A,\, F'A')
\end{array}$$

Follow 1_{FA} out of the upper left-hand corner to find $\varphi_{A,A'}(f') = F'f' \circ \eta_A$.

For (3), given an f', note that (2) yields $\varphi_{A,A'}(f') = f$; whence, $f' = \varphi^{-1}_{A,A'}(f)$. Thus f' is unique. Further, an f' exists: just set $f' := \varphi^{-1}_{A,A'}(f)$.

For (4), set $\psi_{A,A'}(f') := F'f' \circ \eta_A$. As η_A is universal, given $f\colon A \to F'A'$, there is a unique $f'\colon FA \to A'$ with $F'f' \circ \eta_A = f$. Thus $\psi_{A,A'}$ is a bijection:

$$\psi_{A,A'}\colon\ \mathrm{Hom}_{\mathcal{C}'}(FA, A') \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(A,\, F'A').$$

Also, $\psi_{A,A'}$ is natural in A, as η_A is natural in A and F' is a functor. And, $\psi_{A,A'}$ is natural in A', as F' is a functor. Clearly, $\psi_{A,\,FA}(1_{FA}) = \eta_A$. Thus (4) holds.

For (5), use the notation of (6.4). Clearly, if F is the "free module" functor, then $\eta_\Lambda\colon \Lambda \to R^{\oplus\Lambda}$ carries an element of Λ to the corresponding standard basis vector. Further, if F is the "polynomial ring" functor and if A is the set of variables $X_1, \ldots, X_n$, then $\eta_A(X_i)$ is just X_i viewed in $R[X_1, \ldots, X_n]$. □

EXERCISE **(6.9)**. — Let $\alpha\colon L \to M$ and $\beta\colon L \to N$ be two maps. Their *pushout* is defined as the universal example of an object P equipped with a pair of maps $\gamma\colon M \to P$ and $\delta\colon N \to P$ such that $\gamma\alpha = \delta\beta$. In terms of the definitions, express the pushout as a direct limit. Show directly that, in ((Sets)), the pushout is the disjoint union $M \sqcup N$ modulo the smallest equivalence relation $\sim$ with $m \sim n$ if there is $\ell \in L$ with $\alpha(\ell) = m$ and $\beta(\ell) = n$. Show directly that, in ((R-mod)), the pushout is the direct sum $M \oplus N$ modulo the image of L under the map $(\alpha, -\beta)$.

ANSWER: Let Λ be the category with three objects λ, μ, and ν and two non-identity maps $\lambda \to \mu$ and $\lambda \to \nu$. Define a functor $\lambda \mapsto M_\lambda$ by $M_\lambda := L$, $M_\mu := M$,

$M_\nu := N$, $\alpha^\lambda_\mu := \alpha$, and $\alpha^\lambda_\nu := \beta$. Set $Q := \varinjlim M_\lambda$. Then writing

$$\begin{array}{ccccc} N & \xleftarrow{\beta} & L & \xrightarrow{\alpha} & M \\ {\scriptstyle\eta_\nu}\downarrow & & {\scriptstyle\eta_\lambda}\downarrow & & {\scriptstyle\eta_\mu}\downarrow \\ Q & \xleftarrow{1_R} & Q & \xrightarrow{1_R} & Q \end{array} \qquad \text{as} \qquad \begin{array}{ccc} L & \xrightarrow{\alpha} & M \\ {\scriptstyle\beta}\downarrow & & {\scriptstyle\eta_\mu}\downarrow \\ N & \xrightarrow{\eta_\nu} & Q \end{array}$$

we see that Q is equal to the pushout of α and β; here $\gamma = \eta_\mu$ and $\delta = \eta_\nu$.

In ((Sets)), take γ and δ to be the inclusions followed by the quotient map. Clearly $\gamma\alpha = \delta\beta$. Further, given P and maps $\gamma'\colon M \to P$ and $\delta'\colon N \to P$, they define a unique map $M \sqcup N \to P$, and it factors through the quotient if and only if $\gamma'\alpha = \delta'\beta$. Thus $(M \sqcup N)/\sim$ is the pushout.

In ((R-mod)), take γ and δ to be the inclusions followed by the quotient map. Then for all $\ell \in L$, clearly $\iota_M\alpha(\ell) - \iota_N\beta(\ell) = (\alpha(\ell), -\beta(\ell))$. So $\iota_M\alpha(\ell) - \iota_N\beta(\ell)$ is in $\mathrm{Im}(L)$; hence, $\iota_M\alpha(\ell)$ and $\iota_N\beta(\ell)$ have the same image in the quotient. Thus $\gamma\alpha = \delta\beta$. Given $\gamma'\colon M \to P$ and $\delta'\colon N \to P$, let $\varphi\colon M \oplus N \to P$ be the induced map. Clearly φ factors through the quotient if and only if with $\gamma'\alpha = \delta'\beta$. Thus $(M \oplus N)/\,\mathrm{Im}(L)$ is the pushout. □

Exercise **(6.16)**. — Let $\mathcal{C}$ be a category, Σ and Λ small categories.

(1) Prove $\mathcal{C}^{\Sigma\times\Lambda} = (\mathcal{C}^\Lambda)^\Sigma$ with $(\sigma, \lambda) \mapsto M_{\sigma,\lambda}$ corresponding to $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$.

(2) Assume $\mathcal{C}$ has direct limits indexed by Σ and by Λ. Prove $\mathcal{C}$ has direct limits indexed by $\Sigma \times \Lambda$.

Answer: In $\Sigma \times \Lambda$, a map $(\sigma, \lambda) \to (\tau, \mu)$ factors in two ways:

$$(\sigma, \lambda) \to (\tau, \lambda) \to (\tau, \mu) \quad \text{and} \quad (\sigma, \lambda) \to (\sigma, \mu) \to (\tau, \mu).$$

So, given a functor $(\sigma, \lambda) \mapsto M_{\sigma,\lambda}$, there is a commutative diagram like (6.13.1). It shows that the map $\sigma \to \tau$ in Σ induces a natural transformation from $\lambda \mapsto M_{\sigma,\lambda}$ to $\lambda \mapsto M_{\tau,\lambda}$. Thus the rule $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$ is a functor from Σ to $\mathcal{C}^\Lambda$.

A map from $(\sigma, \lambda) \mapsto M_{\sigma,\lambda}$ to a second functor $(\sigma, \lambda) \mapsto N_{\sigma,\lambda}$ is a collection of maps $\theta_{\sigma,\lambda}\colon M_{\sigma,\lambda} \to N_{\sigma,\lambda}$ such that, for every map $(\sigma, \lambda) \to (\tau, \mu)$, the square

$$\begin{array}{ccc} M_{\sigma\lambda} & \longrightarrow & M_{\tau\mu} \\ {\scriptstyle\theta_{\sigma,\lambda}}\downarrow & & \downarrow{\scriptstyle\theta_{\tau,\mu}} \\ N_{\sigma\lambda} & \longrightarrow & N_{\tau\mu} \end{array}$$

is commutative. Factoring $(\sigma, \lambda) \to (\tau, \mu)$ in two ways as above, we get a commutative cube. It shows that the $\theta_{\sigma,\lambda}$ define a map in $(\mathcal{C}^\Lambda)^\Sigma$.

This passage from $\mathcal{C}^{\Sigma\times\Lambda}$ to $(\mathcal{C}^\Lambda)^\Sigma$ is reversible. Thus (1) holds.

Assume $\mathcal{C}$ has direct limits indexed by Σ and Λ. Then $\mathcal{C}^\Lambda$ has direct limits indexed by Σ by (6.13). So the functors $\varinjlim_{\lambda\in\Lambda}\colon \mathcal{C}^\Lambda \to \mathcal{C}$ and $\varinjlim_{\sigma\in\Sigma}\colon (\mathcal{C}^\Lambda)^\Sigma \to \mathcal{C}^\Lambda$ exist, and they are the left adjoints of the diagonal functors $\mathcal{C} \to \mathcal{C}^\Lambda$ and $\mathcal{C}^\Lambda \to (\mathcal{C}^\Lambda)^\Sigma$ by (6.6). Hence the composition $\varinjlim_{\lambda\in\Lambda} \varinjlim_{\sigma\in\Sigma}$ is the left adjoint of the composition of the two diagonal functors. But the latter is just the diagonal $\mathcal{C} \to \mathcal{C}^{\Sigma\times\Lambda}$ owing to (1). So this diagonal has a left adjoint, which is necessarily $\varinjlim_{(\sigma,\lambda)\in\Sigma\times\Lambda}$ owing to the uniqueness of adjoints. Thus (2) holds. □

Exercise **(6.17)**. — Let $\lambda \mapsto M_\lambda$ and $\lambda \mapsto N_\lambda$ be two functors from a small category Λ to ((R-mod)), and $\{\theta_\lambda\colon M_\lambda \to N_\lambda\}$ a natural transformation. Show

$$\varinjlim \mathrm{Coker}(\theta_\lambda) = \mathrm{Coker}(\varinjlim M_\lambda \to \varinjlim N_\lambda).$$

Show that the analogous statement for kernels can be false by constructing a counterexample using the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
\mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \to & \mathbb{Z}/\langle 2\rangle & \to & 0 \\
\downarrow{\scriptstyle\mu_2} & & \downarrow{\scriptstyle\mu_2} & & \downarrow{\scriptstyle\mu_2} & & \\
\mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \to & \mathbb{Z}/\langle 2\rangle & \to & 0
\end{array}$$

Answer: By (6.8), the cokernel is a direct limit, and by (6.14), direct limits commute; thus, the asserted equation holds.

To construct the desired counterexample using the given diagram, view its rows as expressing the cokernel $\mathbb{Z}/\langle 2\rangle$ as a direct limit over the category Λ of (6.8). View the left two columns as expressing a natural transformation $\{\theta_\lambda\}$, and view the third column as expressing the induced map between the two limits. The latter map is 0, so its kernel is $\mathbb{Z}/\langle 2\rangle$. However, $\operatorname{Ker}(\theta_\lambda) = 0$ for $\lambda \in \Lambda$; so $\varinjlim \operatorname{Ker}(\theta_\lambda) = 0$. □

7. Filtered direct limits

Exercise **(7.2)**. — Let R be a ring, M a module, Λ a set, M_λ a submodule for each $\lambda \in \Lambda$. Assume $\bigcup M_\lambda = M$. Assume, given λ, $\mu \in \Lambda$, there is $\nu \in \Lambda$ such that M_λ, $M_\mu \subset M_\nu$. Order Λ by inclusion: $\lambda \le \mu$ if $M_\lambda \subset M_\mu$. Prove that $M = \varinjlim M_\lambda$.

Answer: Let us prove that M has the UMP characterizing $\varinjlim M_\lambda$. Given homomorphisms $\beta_\lambda\colon M_\lambda \to P$ with $\beta_\lambda = \beta_\nu|M_\lambda$ when $\lambda \le \nu$, define $\beta\colon M \to P$ by $\beta(m) := \beta_\lambda(m)$ if $m \in M_\lambda$. Such a λ exists as $\bigcup M_\lambda = M$. If also $m \in M_\mu$ and M_λ, $M_\mu \subset M_\nu$, then $\beta_\lambda(m) = \beta_\nu(m) = \beta_\mu(m)$; so β is well defined. Clearly, $\beta\colon M \to P$ is the unique set map such that $\beta|M_\lambda = \beta_\lambda$. Further, given $m, n \in M$ and $x \in R$, there is ν such that $m, n \in M_\nu$. So $\beta(m+n) = \beta_\nu(m+n) = \beta(m)+\beta(n)$ and $\beta(xm) = \beta_\nu(xm) = x\beta(m)$. Thus β is R-linear. Thus $M = \varinjlim M_\lambda$. □

Exercise **(7.3)**. — Show that every module M is the filtered direct limit of its finitely generated submodules.

Answer: Every element $m \in M$ belongs to the submodule generated by m; hence, M is the union of all its finitely generated submodules. Any two finitely generated submodules are contained in a third, for example, their sum. So the assertion results from (7.2) with Λ the set of all finite subsets of M. □

Exercise **(7.4)**. — Show that every direct sum of modules is the filtered direct limit of its finite direct subsums.

Answer: Consider an element of the direct sum. It has only finitely many nonzero components. So it lies in the corresponding finite direct subsum. Thus the union of the subsums is the whole direct sum. Now, given any two finite direct subsums, their sum is a third. Thus the finite subsets of indices form a directed partially ordered set Λ. So the assertion results from (7.2). □

Exercise **(7.6)**. — Keep the setup of (7.5). For each $n \in \Lambda$, set $N_n := \mathbb{Z}/\langle n\rangle$; if $n = ms$, define $\alpha_n^m\colon N_m \to N_n$ by $\alpha_n^m(x) := xs \pmod{n}$. Show $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$.

Answer: For each $n \in \Lambda$, set $Q_n := M_n/\mathbb{Z} \subset \mathbb{Q}/Z$. If $n = ms$, then clearly Diagram (7.5.1) induces this one:

$$\begin{array}{ccc} N_m & \xrightarrow{\alpha_n^m} & N_n \\ {\scriptstyle \gamma_m}\big\downarrow \simeq & & {\scriptstyle \gamma_n}\big\downarrow \simeq \\ Q_m & \xhookrightarrow{\eta_n^m} & Q_n \end{array}$$

where η_n^m is the inclusion. Now, $\bigcup Q_n = \mathbb{Q}/\mathbb{Z}$ and $Q_n,\, Q_{n'} \subset Q_{nn'}$. So (7.2) yields $\mathbb{Q}/\mathbb{Z} = \varinjlim M_n$. Thus $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$. □

Exercise **(7.9)**. — Let R be a filtered direct limit of rings R_λ. Show $R = 0$ if and only if $R_\lambda = 0$ for some λ. Show R is a domain if R_λ is a domain for every λ.

Answer: If $R_\lambda = 0$, then $1 = 0$ in R_λ; so $1 = 0$ in R as $\alpha_\lambda\colon R_\lambda \to R$ carries 1 to 1 and 0 to 0; hence, $R = 0$ by (1.1). Conversely, assume $R = 0$. Then $1 = 0$ in R. So $\alpha_\lambda 1 = 0$ for any given λ. Hence, by (7.8)(3) with $\mathbb{Z}$ for R, there is α_μ^λ such that $\alpha_\mu^\lambda 1 = 0$. But $\alpha_\mu^\lambda 1 = 1$. Thus $1 = 0$ in R_μ, and so $R_\mu = 0$ by (1.1).

Suppose every R_λ is a domain. Given $x, y \in R$ with $xy = 0$, we can lift x, y back to $x_\lambda, y_\lambda \in R_\lambda$ for some λ by (7.8)(1) and (7.1)(1). Then $x_\lambda y_\lambda$ maps to $0 \in R$. Hence, by (7.8)(3), there is a transition map α_μ^λ with $\alpha_\mu^\lambda(x_\lambda y_\lambda) = 0$ in R_μ. However, $\alpha_\mu^\lambda(x_\lambda y_\lambda) = \alpha_\mu^\lambda(x_\lambda)\alpha_\mu^\lambda(y_\lambda)$, and R_μ is a domain. Hence either $\alpha_\mu^\lambda(x_\lambda) = 0$ or $\alpha_\mu^\lambda(y_\lambda) = 0$. Therefore, either $x = 0$ or $y = 0$. Thus R is a domain. □

Exercise **(7.11)**. — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, and $N \subset M$ a submodule. For each λ, let $\alpha_\lambda\colon M_\lambda \to M$ be the insertion, and set $N_\lambda := \alpha_\lambda^{-1} N \subset M_\lambda$. Prove that $N = \varinjlim N_\lambda$.

Answer: The given functor $\lambda \mapsto M_\lambda$ induces a functor $\lambda \mapsto N_\lambda$, and the insertions $\alpha_\lambda\colon M_\lambda \to M$ induce maps $\beta_\lambda\colon N_\lambda \to N$. So there is a map $\beta\colon \varinjlim N_\lambda \to N$ with $\beta\alpha_\lambda = \beta_\lambda$. By (7.10), $\varinjlim N_\lambda \to M$ is injective; so β is too. Further, for any $m \in M$, there is an $m_\lambda \in M_\lambda$ such that $m = \alpha_\lambda m_\lambda$, and if $m \in N$, then $m_\lambda \in N_\lambda$ since $N_\lambda := \alpha_\lambda^{-1} N$. Thus β is surjective, so an isomorphism. □

Exercise **(7.13)**. — Let Λ and Λ' be small categories, $C\colon \Lambda' \to \Lambda$ a functor. Assume Λ' is filtered. Assume C is *cofinal*; that is,

(1) given $\lambda \in \Lambda$, there is a map $\lambda \to C\lambda'$ for some $\lambda' \in \Lambda'$, and
(2) given $\psi, \varphi\colon \lambda \rightrightarrows C\lambda'$, there is $\chi\colon \lambda' \to \lambda_1'$ with $(C\chi)\psi = (C\chi)\varphi$.

Let $\lambda \mapsto M_\lambda$ be a functor from Λ to $\mathcal{C}$ whose direct limit exists. Show that

$$\varinjlim_{\lambda' \in \Lambda'} M_{C\lambda'} = \varinjlim_{\lambda \in \Lambda} M_\lambda;$$

more precisely, show that the right side has the UMP characterizing the left.

Answer: Let P be an object of $\mathcal{C}$. For $\lambda' \in \Lambda'$, take maps $\gamma_{\lambda'}\colon M_{C\lambda'} \to P$ compatible with the transition maps $M_{C\lambda'} \to M_{C\mu'}$. Given $\lambda \in \Lambda$, choose a map $\lambda \to C\lambda'$, and define $\beta_\lambda\colon M_\lambda \to P$ to be the composition

$$\beta_\lambda\colon M_\lambda \longrightarrow M_{C\lambda'} \xrightarrow{\gamma_{\lambda'}} P.$$

Let's check that β_λ is independent of the choice of $\lambda \to C\lambda'$.

Given a second choice $\lambda \to C\lambda''$, there are maps $\lambda'' \to \mu'$ and $\lambda' \to \mu'$ for some $\mu' \in \Lambda'$ since Λ' is filtered. So there is a map $\mu' \to \mu_1'$ such that the compositions $\lambda \to C\lambda' \to C\mu' \to C\mu_1'$ and $\lambda \to C\lambda'' \to C\mu' \to C\mu_1'$ are equal since C is cofinal. Therefore, $\lambda \to C\lambda''$ gives rise to the same β_λ, as desired.

Clearly, the β_λ are compatible with the transition maps $M_\kappa \to M_\lambda$. So the β_λ induce a map $\beta\colon \varinjlim M_\lambda \to P$ with $\beta\alpha_\lambda = \beta_\lambda$ for every insertion $\alpha_\lambda\colon M_\lambda \to \varinjlim M_\lambda$. In particular, this equation holds when $\lambda = C\lambda'$ for any $\lambda' \in \Lambda'$, as required. □

Exercise **(7.14)**. — Show that every R-module M is the filtered direct limit over a directed set of finitely presented modules.

Answer: By (5.19), there is a presentation $R^{\oplus\Phi_1} \xrightarrow{\alpha} R^{\oplus\Phi_2} \to M \to 0$. For $i = 1, 2$, let Λ_i be the set of finite subsets Ψ_i of Φ_i, and order Λ_i by inclusion. Clearly, an inclusion $\Psi_i \hookrightarrow \Phi_i$ yields an injection $R^{\oplus\Psi_i} \hookrightarrow R^{\oplus\Phi_i}$, which is given by extending vectors by 0. Hence (7.2) yields $\varinjlim R^{\oplus\Psi_i} = R^{\oplus\Phi_i}$.

Let $\Lambda \subset \Lambda_1 \times \Lambda_2$ be the set of pairs $\lambda := (\Psi_1, \Psi_2)$ such that α induces a map $\alpha_\lambda\colon R^{\oplus\Psi_1} \to R^{\oplus\Psi_2}$. Order Λ by componentwise inclusion. Clearly, Λ is directed. For $\lambda \in \Lambda$, set $M_\lambda := \mathrm{Coker}(\alpha_\lambda)$. Then M_λ is finitely presented.

For $i = 1, 2$, the projection $C_i\colon \Lambda \to \Lambda_i$ is surjective, so cofinal. Hence, (7.13) yields $\varinjlim_{\lambda\in\Lambda} R^{\oplus C_i\lambda} = \varinjlim_{\Psi_i\in\Lambda_i} R^{\oplus\Psi_i}$. Thus (6.17) yields $\varinjlim M_\lambda = M$. □

8. Tensor Products

Exercise **(8.6)**. — Let R be a domain. Set $K := \mathrm{Frac}(R)$. Given a nonzero submodule $M \subset K$, show that $M \otimes_R K = K$.

Answer: Define a map $\beta\colon \mathfrak{a} \times K \to K$ by $\beta(x, y) := xy$. It is clearly R-bilinear. Given any R-bilinear map $\alpha\colon \mathfrak{a}\times K \to P$, fix a nonzero $z \in \mathfrak{a}$, and define an R-linear map $\gamma\colon K \to P$ by $\gamma(y) := \alpha(z, y/z)$. Then $\alpha = \gamma\beta$ as

$$\alpha(x, y) = \alpha(xz, y/z) = \alpha(z, xy/z) = \gamma(xy) = \gamma\beta(x, y).$$

Clearly, β is surjective. So γ is unique with this property. Thus the UMP implies that $K = \mathfrak{a} \otimes_R K$. (Also, as γ is unique, γ is independent of the choice of z.)

Alternatively, form the linear map $\varphi\colon \mathfrak{a}\otimes K \to K$ induced by the bilinear map β. Since β is surjective, so is φ. Now, given any $w \in \mathfrak{a}\otimes K$, say $w = \sum a_i \otimes x_i/x$ with all x_i and x in R. Set $a := \sum a_i x_i \in \mathfrak{a}$. Then $w = a \otimes (1/x)$. Hence, if $\varphi(w) = 0$, then $a/x = 0$; so $a = 0$ and so $w = 0$. Thus φ is injective, so bijective. □

Exercise **(8.8)**. — Let R be a ring, R' an R-algebra, M, N two R'-modules. Show there is a canonical R-linear map $\tau\colon M \otimes_R N \to M \otimes_{R'} N$.

Let $K \subset M \otimes_R N$ denote the R-submodule generated by all the differences $(x'm) \otimes n - m \otimes (x'n)$ for $x' \in R'$ and $m \in M$ and $n \in N$. Show $K = \mathrm{Ker}(\tau)$. Show τ is surjective, and is an isomorphism if R' is a quotient of R.

Answer: The canonical map $\beta'\colon M\times N \to M\otimes_{R'} N$ is R'-bilinear, so R-bilinear. Hence, by (8.3), it factors: $\beta' = \tau\beta$ where $\beta\colon M \times N \to M \otimes_R N$ is the canonical map and τ is the desired map.

Set $Q := (M \otimes_R N)/K$. Then τ factors through a map $\tau'\colon Q \to M \otimes_{R'} N$ since each generator $(x'm) \otimes n - m \otimes (x'n)$ of K maps to 0 in $M \otimes_{R'} N$.

By (8.7), there is an R'-structure on $M \otimes_R N$ with $y'(m \otimes n) = m \otimes (y'n)$, and so by (8.5)(1), another one with $y'(m\otimes n) = (y'm) \otimes n$. Clearly, K is a submodule for each structure, so Q is too. But on Q the two structures coincide. Further, the canonical map $M \times N \to Q$ is R'-bilinear. Hence the latter factors through $M \otimes_{R'} N$, furnishing an inverse to τ'. So $\tau'\colon Q \xrightarrow{\sim} M \otimes_{R'} N$. Hence $\mathrm{Ker}(\tau)$ is equal to K, and τ is surjective.

Finally, suppose R' is a quotient of R. Then every $x' \in R'$ is the residue of some $x \in R$. So each $(x'm) \otimes n - m \otimes (x'n)$ is equal to 0 in $M \otimes_R N$ as $x'm = xm$ and $x'n = xn$. Hence $\operatorname{Ker}(\tau)$ vanishes. Thus τ is an isomorphism. $\square$

Exercise **(8.13)**. — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, and M a module.
(1) Use (8.11) to show that $(R/\mathfrak{a}) \otimes M = M/\mathfrak{a}M$.
(2) Use (1) to show that $(R/\mathfrak{a}) \otimes (R/\mathfrak{b}) = R/(\mathfrak{a} + \mathfrak{b})$.

Answer: To prove (1), view $R/\mathfrak{a}$ as the cokernel of the inclusion $\mathfrak{a} \to R$. Then (8.11) implies that $(R/\mathfrak{a}) \otimes M$ is the cokernel of $\mathfrak{a} \otimes M \to R \otimes M$. Now, $R \otimes M = M$ and $x \otimes m = xm$ by (8.5)(2). Correspondingly, $\mathfrak{a} \otimes M \to M$ has $\mathfrak{a}M$ as image. The assertion follows. (Caution: $\mathfrak{a} \otimes M \to M$ needn't be injective; if it's not, then $\mathfrak{a} \otimes M \neq \mathfrak{a}M$. For example, take $R := \mathbb{Z}$, take $\mathfrak{a} := \langle 2 \rangle$, and take $M := \mathbb{Z}/\langle 2 \rangle$; then $\mathfrak{a} \otimes M \to M$ is just multiplication by 2 on $\mathbb{Z}/\langle 2 \rangle$, and so $\mathfrak{a}M = 0$.)

To prove (2), apply (1) with $M := R/\mathfrak{b}$. Note $\mathfrak{a}(R/\mathfrak{b}) = (\mathfrak{a} + \mathfrak{b})/\mathfrak{b}$. Hence

$$R/\mathfrak{a} \otimes R/\mathfrak{b} = (R/\mathfrak{b})\big/((\mathfrak{a} + \mathfrak{b})/\mathfrak{b}).$$

The latter is equal to $R/(\mathfrak{a} + \mathfrak{b})$ by (4.8). $\square$

Exercise **(8.14)**. — Let k be a field, M and N nonzero vector spaces. Prove that $M \otimes N \neq 0$.

Answer: Since k is a field, M and N are free; say $M = k^{\oplus \Phi}$ and $N = k^{\oplus \Psi}$. Then (8.11) yields $M \otimes N = k^{\oplus(\Phi \times \Psi)}$ as $k \otimes k = k$ by (8.5)(2). Thus $M \otimes N \neq 0$. $\square$

Exercise **(8.16)**. — Let $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ be a linear functor. Show that F always preserves finite direct sums. Show that $\theta(M)\colon M \otimes F(R) \to F(M)$ is surjective if F preserves surjections and M is finitely generated, and that $\theta(M)$ is an isomorphism if F preserves cokernels and M is finitely presented.

Answer: The first assertion follows immediately from the characterization of finite direct sum in terms of maps (4.15), since F preserves the stated relations.

The second assertion follows from the first via the second part of the proof of Watt's Theorem (8.15), but with Σ and Λ finite. $\square$

Exercise **(8.20)**. — Let X be a variable, ω a complex cubic root of 1, and $\sqrt[3]{2}$ the real cube root of 2. Set $k := \mathbb{Q}(\omega)$ and $K := k[\sqrt[3]{2}]$. Show $K = k[X]/\langle X^3 - 2 \rangle$ and then $K \otimes_k K = K \times K \times K$.

Answer: Note ω is a root of $X^2 + X + 1$, which is irreducible over $\mathbb{Q}$; hence, $[k : \mathbb{Q}] = 2$. But the three roots of $X^3 - 2$ are $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. Therefore, $X^3 - 2$ has no root in k. So $X^3 - 2$ is irreducible over k. Thus $k[X]/\langle X^3 - 2 \rangle \xrightarrow{\sim} K$.

Note $K[X] = K \otimes_k k[X]$ as k-algebras by (8.19). So (8.5)(2) and (8.10) and (8.13)(1) yield

$$\begin{aligned} k[X]/\langle X^3 - 2 \rangle \otimes_k K &= k[X]/\langle X^3 - 2 \rangle \otimes_{k[X]} (k[X] \otimes_k K) \\ &= k[X]/\langle X^3 - 2 \rangle \otimes_{k[X]} K[X] = K[X]/\langle X^3 - 2 \rangle. \end{aligned}$$

However, $X^3 - 2$ factors in K as follows:

$$X^3 - 2 = \big(X - \sqrt[3]{2}\big)\big(X - \omega\sqrt[3]{2}\big)\big(X - \omega^2\sqrt[3]{2}\big).$$

So the Chinese Remainder Theorem, (1.12), yields

$$K[X]/\langle X^3-2\rangle = K\times K\times K,$$

because $K[X]/\langle X-\omega^i\sqrt[3]{2}\rangle \xrightarrow{\sim} K$ for any i by (1.6). □

9. Flatness

Exercise **(9.7)**. — Let R be a ring, R' a flat algebra, and P a flat R'-module. Show that P is a flat R-module.

Answer: Cancellation (8.10) yields $\bullet\otimes_R P = (\bullet\otimes_R R')\otimes_{R'} P$. But $\bullet\otimes_R R'$ and $\bullet\otimes_{R'} P$ are exact. Hence, $\bullet_R P$ is too. Thus P is R-flat. □

Exercise **(9.8)**. — Let R be a ring, M a flat module, and R' an algebra. Show that $M\otimes_R R'$ is a flat R'-module.

Answer: Cancellation (8.10) yields $(M\otimes_R R')\otimes_{R'}\bullet = M\otimes_R\bullet$. Therefore, $(M\otimes_R R')\otimes_{R'}\bullet$ is exact. Thus $M\otimes_R R'$ is R'-flat. □

Exercise **(9.9)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume that $R/\mathfrak{a}$ is R-flat. Show that $\mathfrak{a}=\mathfrak{a}^2$.

Answer: Take the short exact sequence $0\to\mathfrak{a}\to R\to R/\mathfrak{a}\to 0$, and tensor it with $R/\mathfrak{a}$. Then the flatness of $R/\mathfrak{a}$ yields the exactness of this sequence:

$$0\to\mathfrak{a}\otimes_R(R/\mathfrak{a})\to R\otimes_R(R/\mathfrak{a})\xrightarrow{\alpha}(R/\mathfrak{a})\otimes_R(R/\mathfrak{a})\to 0.$$

The left-hand term is equal to $\mathfrak{a}/\mathfrak{a}^2$ by (8.13). By the same token, α is bijective. Hence $\mathfrak{a}/\mathfrak{a}^2=0$. Thus $\mathfrak{a}=\mathfrak{a}^2$. □

Exercise **(9.13)**. — Let R be a ring, R' an algebra, M and N modules. Show that there is a canonical map

$$\sigma\colon \operatorname{Hom}_R(M,N)\otimes_R R'\to\operatorname{Hom}_{R'}(M\otimes_R R', N\otimes_R R').$$

Assume R' is flat over R. Show that if M is finitely generated, then σ is injective, and that if M is finitely presented, then σ is an isomorphism.

Answer: Simply put $R':=R$ and $P:=R'$ in (9.13), put $P:=N\otimes_R R'$ in the second equation in (8.10), and combine the two results. □

Exercise **(9.17)** (*Equational Criterion for Flatness*). — Show that Condition (9.16)(4) can be reformulated as follows: For every relation $\sum_i x_iy_i=0$ with $x_i\in R$ and $y_i\in M$, there are $x_{ij}\in R$ and $y'_j\in M$ such that

$$\textstyle\sum_j x_{ij}y'_j = y_i \text{ for all } i \text{ and } \sum_i x_{ij}x_i=0 \text{ for all } j. \qquad \textbf{(9.17.1)}$$

Answer: Assume (9.16)(4) holds. Let $e_1,\dots,e_m$ be the standard basis of R^m. Given a relation $\sum_1^m x_iy_i=0$, define $\alpha\colon R^m\to M$ by $\alpha(e_i):=y_i$ for each i. Set $k:=\sum x_ie_i$. Then $\alpha(k)=0$. So (9.16)(4) yields a factorization $\alpha\colon R^m\xrightarrow{\varphi}R^n\xrightarrow{\beta}M$ with $\varphi(k)=0$. Let $e'_1,\dots,e'_n$ be the standard basis of R^n, and set $y'_j:=\beta(e'_j)$ for each j. Let (x_{ij}) be the $n\times m$ matrix of φ; that is, $\varphi(e_i)=\sum x_{ji}e'_j$. Then $y_i=\sum x_{ji}y'_j$. Now, $\varphi(k)=0$; hence, $\sum_{i,j}x_{ji}x_ie'_j=0$. Thus (9.17.1) holds.

Conversely, given $\alpha\colon R^m\to M$ and $k\in\operatorname{Ker}(\alpha)$, write $k=\sum x_ie_i$. Assume (9.17.1). Let $\varphi\colon R^m\to R^n$ be the map with matrix (x_{ij}); that is, $\varphi(e_i)=\sum x_{ji}e'_j$.

Then $\varphi(k) = \sum x_i x_{ji} e'_j = 0$. Define $\beta\colon R^n \to M$ by $\beta(e'_j) := y'_j$. Then $\beta\varphi(e_i) = y_i$; hence, $\beta\varphi = \alpha$. Thus (9.16)(4) holds. □

Exercise **(9.20)**. — Let R be a domain, M a module. Prove that, if M is flat, then M is *torsion free*; that is, $\mu_x\colon M \to M$ is injective for all nonzero $x \in R$. Prove that, conversely, if R is a PID and M is torsion free, then M is flat.

Answer: Since R is a domain, $\mu_x\colon R \to R$ is injective. So if M is flat, then $\mu_x \otimes M\colon R \otimes M \to R \otimes M$ is injective too. But $R \otimes M = M$ by (8.5).

Conversely, assume R is a PID and M is torsion free. Let $\mathfrak{a}$ be a nonzero ideal, say $\mathfrak{a} = \langle x \rangle$. Define $\alpha\colon R \to \mathfrak{a}$ by $\alpha(y) := xy$. Then α is injective as R is a domain and $x \neq 0$. Further, α is surjective as $\mathfrak{a} = \langle x \rangle$. So α is bijective.

Consider the composition

$$\beta\colon M = R \otimes M \xrightarrow{\alpha\otimes M} \mathfrak{a} \otimes M \to M.$$

Clearly, $\beta = \mu_x$. So β is injective since M is torsion free. Hence $\mathfrak{a} \otimes M \to M$ is injective too. So M is flat by the Ideal Criterion (9.18). □

10. Cayley–Hamilton Theorem

Exercise **(10.6)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a}$ is finitely generated and satisfies $\mathfrak{a} = \mathfrak{a}^2$. Prove there is a unique idempotent e such that $\langle e \rangle = \mathfrak{a}$.

Answer: By (10.3) with $\mathfrak{a}$ for M, there is $e \in \mathfrak{a}$ such that $(1-e)\mathfrak{a} = 0$. In other words, for all $x \in \mathfrak{a}$, we have $(1-e)x = 0$, or $x = ex$. Thus $\mathfrak{a} = \langle e \rangle$ and $e = e^2$.

Suppose also $\mathfrak{a} = \langle f \rangle$ and $f = f^2$. Say $e = fx$ and $f = ey$. Then

$$e = fx = f^2x = fe = e^2y = ey = f.$$ □

Exercise **(10.10)**. — Let A be a local ring, $\mathfrak{m}$ the maximal ideal, M a finitely generated A-module, and $m_1, \dots, m_n \in M$. Set $k := A/\mathfrak{m}$ and $M' := M/\mathfrak{m}M$, and write m'_i for the image of m_i in M'. Prove that $m'_1, \dots, m'_n \in M'$ form a basis of the k-vector space M' if and only if $m_1, \dots, m_n$ form a *minimal generating set* of M (that is, no proper subset generates M), and prove that every minimal generating set of M has the same number of elements.

Answer: By (10.9), reduction mod $\mathfrak{m}$ gives a bijective correspondence between generating sets of M as an A-module, and generating sets of M' as an A-module, or equivalently by (4.5), as an k-vector space. This correspondence preserves inclusion. Hence, a minimal generating set of M corresponds to a minimal generating set of M', that is, to a basis. But any two bases have the same number of elements. □

Exercise **(10.11)**. — Let A be a local ring, k its residue field, M and N finitely generated modules. (1) Show that $M = 0$ if and only if $M \otimes_A k = 0$. (2) Show that $M \otimes_A N \neq 0$ if $M \neq 0$ and $N \neq 0$.

Answer: Let $\mathfrak{m}$ be the maximal ideal. Then $M \otimes k = M/\mathfrak{m}M$ by (8.13)(1). So (1) is nothing but a form of Nakayama's lemma (10.8).

In (2), $M \otimes k \neq 0$ and $N \otimes k \neq 0$ by (1). So $(M \otimes k) \otimes (N \otimes k) \neq 0$ by (8.14) and (8.8). But $(M \otimes k) \otimes (N \otimes k) = (M \otimes N) \otimes (k \otimes k)$ by the associative and commutative laws. Finally, $k \otimes k = k$ by (8.13)(1) or by (8.8) and the unitary law. □

Exercise **(10.14)**. — Let G be a finite group acting on a domain R, and R' the ring of invariants. Show every $x \in R$ is integral over R', in fact, over the subring R'' generated by the elementary symmetric functions in the conjugates gx for $g \in G$.

Answer: Given an $x \in R$, form $F(X) := \prod_{g\in G}(X - gx)$. Then the coefficients of $F(X)$ are the elementary symmetric functions in the conjugates gx for $g \in G$; hence, they are invariant under the action of G. So $F(x) = 0$ is a relation of integral dependence for x over R', in fact, over its subring R''. □

Exercise **(10.16)**. — Let k be a field, $P := k[X]$ the polynomial ring in one variable, $f \in P$. Set $R := k[X^2] \subset P$. Using the free basis $1, X$ of P over R, find an explicit equation of integral dependence of degree 2 on R for f.

Answer: Write $f = f_e + f_o$, where f_e and f_o are the polynomials formed by the terms of f of even and odd degrees. Say $f_o = gX$. Then the matrix of μ_f is $\left(\begin{smallmatrix} f_e & gX^2 \\ g & f_e \end{smallmatrix}\right)$. Its characteristic polynomial is $T^2 - 2f_eT + f_e^2 - f_o^2$. So the Cayley–Hamilton Theorem (10.1) yields $f^2 - 2f_ef + f_e^2 - f_o^2 = 0$. □

Exercise **(10.21)**. — Let $R_1, \dots, R_n$ be R-algebras that are integral over R. Show that their product $\prod R_i$ is a integral over R.

Answer: Let $y = (y_1, \dots, y_n) \in \prod_{i=1}^n R_i$. Since R_i/R is integral, $R[y_i]$ is a module-finite R-subalgebra of R_i. Hence $\prod_{i=1}^n R[y_i]$ is a module-finite R-subalgebra of $\prod_{i=1}^n R_i$ by (4.14) and induction on n. Now, $y \in \prod_{i=1}^n R[y_i]$. Therefore, y is integral over R. Thus $\prod_{i=1}^n R_i$ is integral over R. □

Exercise **(10.23)**. — For $1 \le i \le r$, let R_i be a ring, R'_i an extension of R_i, and $x_i \in R'_i$. Set $R := \prod R_i$, set $R' := \prod R'_i$, and set $x := (x_1, \dots, x_r)$. Prove

(1) x is integral over R if and only if x_i is integral over R_i for each i;

(2) R is integrally closed in R' if and only if each R_i is integrally closed in R'_i.

Answer: Assume x is integral over R. Say $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_j \in R$. Say $a_j =: (a_{1j}, \dots, a_{rj})$. Fix i. Then $x_i^n + a_{i1}x^{n-1} + \cdots + a_{in} = 0$. So x_i is integral over R_i.

Conversely, assume each x_i is integral over R_i. Say $x_i^{n_i} + a_{i1}x_i^{n_i-1} + \cdots + a_{in_i} = 0$. Set $n := \max n_i$, set $a_{ij} := 0$ for $j > n_i$, and set $a_j := (a_{1j}, \dots, a_{rj}) \in R$ for each j. Then $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Thus x is integral over R. Thus (1) holds.

Assertion (2) is an immediate consequence of (1). □

Exercise **(10.27)**. — Let k be a field, X and Y variables. Set

$$R := k[X, Y]/\langle Y^2 - X^2 - X^3\rangle,$$

and let $x, y \in R$ be the residues of X, Y. Prove that R is a domain, but not a field. Set $t := y/x \in \mathrm{Frac}(R)$. Prove that $k[t]$ is the integral closure of R in $\mathrm{Frac}(R)$.

Answer: As $k[X, Y]$ is a UFD and $Y^2-X^2-X^3$ is irreducible, $\langle Y^2-X^2-X^3\rangle$ is prime by (2.6); however, it is not maximal by (2.24). Hence R is a domain by (2.9), but not a field by (2.16).

Note $y^2 - x^2 - x^3 = 0$. Hence $x = t^2 - 1$ and $y = t^3 - t$. So $k[t] \supset k[x, y] = R$. Further, t is integral over R; so $k[t]$ is integral over R by (2)⇒(1) of (10.20).

Finally, $k[t]$ has $\mathrm{Frac}(R)$ as fraction field. Further, $\mathrm{Frac}(R) \ne R$, so x and y

cannot be algebraic over k; hence, t must be transcendental. So $k[t]$ is normal by (10.26)(1). Thus $k[t]$ is the integral closure of R in $\mathrm{Frac}(R)$. □

11. Localization of Rings

EXERCISE **(11.2)**. — Let R be a ring, S a multiplicative set. Prove $S^{-1}R = 0$ if and only if S contains a nilpotent element.

ANSWER: By (1.1), $S^{-1}R = 0$ if and only if $1/1 = 0/1$. But by construction, $1/1 = 0/1$ if and only if $0 \in S$. Finally, since S is multiplicative, $0 \in S$ if and only if S contains a nilpotent element. □

EXERCISE **(11.4)**. — Find all intermediate rings $\mathbb{Z} \subset R \subset \mathbb{Q}$, and describe each R as a localization of $\mathbb{Z}$. As a starter, prove $\mathbb{Z}[2/3] = S^{-1}\mathbb{Z}$ where $S = \{3^i \mid i \ge 0\}$.

ANSWER: Clearly $\mathbb{Z}[2/3] \subset \mathbb{Z}[1/3]$ as $2/3 = 2 \cdot (1/3)$. But the opposite inclusion holds as $1/3 = 1 - (2/3)$. Obviously, $S^{-1}\mathbb{Z} = \mathbb{Z}[1/3]$.

Let $P \subset \mathbb{Z}$ be the set of all prime numbers that appear as factors of the denominators of elements of R in lowest terms; recall that $x = r/s \in \mathbb{Q}$ is in *lowest terms* if r and s have no common prime divisor. Let S be the multiplicative set *generated by* P, that is, the smallest multiplicative set containing P. Clearly, S is equal to the set of all products of elements of P.

First note that, if $p \in P$, then $1/p \in R$. Indeed, take an element $x = r/ps \in R$ in lowest terms. Then $sx = r/p \in R$. Also the Euclidean algorithm yields $m, n \in \mathbb{Z}$ such that $mp + nr = 1$. Then $1/p = m + nsx \in R$, as desired. Hence $S^{-1}\mathbb{Z} \subset R$. But the opposite inclusion holds because, by the very definition of S, every element of R is of the form r/s for some $s \in S$. Thus $S^{-1}\mathbb{Z} = R$. □

EXERCISE **(11.7)**. — Let R' and R'' be rings. Consider $R := R' \times R''$ and set $S := \{\,(1,1),\ (1,0)\,\}$. Prove $R' = S^{-1}R$.

ANSWER: Let's show that the projection map $\pi\colon R' \times R'' \to R'$ has the UMP of (11.5). First, note that $\pi S = \{1\} \subset R'^{\times}$. Let $\psi\colon R' \times R'' \to B$ be a ring map such that $\psi(1,0) \in B^{\times}$. Then in B,

$$\psi(1,0) \cdot \psi(0,x) = \psi\big((1,0)\cdot(0,x)\big) = \psi(0,0) = 0 \text{ in } B.$$

Hence $\psi(0,x) = 0$ for all $x \in R''$. So ψ factors uniquely through π by (1.4). □

EXERCISE **(11.8)**. — Take R and S as in (11.7). On $R \times S$, impose this relation:

$$(x,s) \sim (y,t) \quad \text{if} \quad xt = ys.$$

Prove that it is not an equivalence relation.

ANSWER: Observe that, for any $z \in R''$, we have

$$\big((1,z),\ (1,1)\big) \sim \big((1,0),\ (1,0)\big).$$

However, if $z \neq 0$, then

$$\big((1,z),\ (1,1)\big) \not\sim \big((1,0),\ (1,1)\big).$$

Thus although $\sim$ is reflexive and symmetric, it is *not* transitive if $R'' \neq 0$. □

Exercise **(11.14)**. — Let R be a ring, S a multiplicative set. Prove that

$$\operatorname{nil}(R)(S^{-1}R) = \operatorname{nil}(S^{-1}R).$$

Answer: Proceed by double inclusion. Given an element of $\operatorname{nil}(R)(S^{-1}R)$, put it in the form x/s with $x \in \operatorname{nil}(R)$ and $s \in S$ using (11.11)(1). Then $x^n = 0$ for some $n \geq 1$. So $(x/s)^n = 0$. So $x/s \in \operatorname{nil}(S^{-1}R)$. Thus $\operatorname{nil}(R)(S^{-1}R) \subset \operatorname{nil}(S^{-1}R)$.

Conversely, take $x/s \in \operatorname{nil}(S^{-1}R)$. Then $(x/s)^m = 0$ with $m \geq 1$. So there's $t \in S$ with $tx^m = 0$ by (11.13)(1). Then $(tx)^m = 0$. So $tx \in \operatorname{nil}(R)$. But $tx/ts = x/s$. So $x/s \in \operatorname{nil}(R)(S^{-1}R)$ by (11.11)(1). Thus $\operatorname{nil}(R)(S^{-1}R) \supset \operatorname{nil}(S^{-1}R)$. □

Exercise **(11.20)**. — Let R'/R be a integral extension of rings, S a multiplicative subset of R. Show that $S^{-1}R'$ is integral over $S^{-1}R$.

Answer: Given $x/s \in S^{-1}R'$, let $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ be an equation of integral dependence of x on R. Then

$$(x/s)^n + (a_{n-1}/1)(1/s)(x/s)^{n-1} + \cdots + a_0(1/s)^n = 0$$

is an equation of integral dependence of x/s on $S^{-1}R$, as required. □

Exercise **(11.21)**. — Let R be a domain, K its fraction field, L a finite extension field, and $\overline{R}$ the integral closure of R in L. Show that L is the fraction field of $\overline{R}$. Show that, in fact, every element of L can be expressed as a fraction b/a where b is in $\overline{R}$ and a is in R.

Answer: Let $x \in L$. Then x is algebraic (integral) over K, say

$$x^n + y_1x^{n-1} + \cdots + y_n = 0$$

with $y_i \in K$. Write $y_i = a_i/a$ with $a_1, \ldots, a_n, a \in R$. Then

$$(ax)^n + (aa_1)(ax)^{n-1} + \cdots + a^n a_0 = 0.$$

Set $b := ax$. Then $b \in \overline{R}$ and $x = b/a$. □

Exercise **(11.22)**. — Let $R \subset R'$ be domains, K and L their fraction fields. Assume that R' is a finitely generated R-algebra, and that L is a finite dimensional K-vector space. Find an $f \in R$ such that R'_f is module finite over R_f.

Answer: Let $x_1, \ldots, x_n$ generate R' as an R-algebra. By (11.21), we can write $x_i = b_i/a_i$ where b_i is integral over R and a_i is in R. Set $f := \prod a_i$. The x_i generate R'_f as an R_f-algebra; so the b_i do too. Hence R'_f is a finitely generated R_f-module by (10.20). □

Exercise **(11.25)**. — Let R be a ring, S and T multiplicative sets.

(1) Set $T' := \varphi_S(T)$ and assume $S \subset T$. Prove

$$T^{-1}R = T'^{-1}(S^{-1}R) = T^{-1}(S^{-1}R).$$

(2) Set $U := \{st \in R \mid s \in S \text{ and } t \in T\}$. Prove

$$T^{-1}(S^{-1}R) = S^{-1}(T^{-1}R) = U^{-1}R.$$

(3) Let $S' := \{t' \in R \mid t't \in S \text{ for some } t \in R\}$. Prove $S'^{-1}R = S^{-1}R$.

Answer: A proof like that of (11.23) shows $T^{-1}R = T'^{-1}(S^{-1}R)$. By (11.19), $T'^{-1}(S^{-1}R) = T^{-1}(S^{-1}R)$. Thus (1) holds.

As $1 \in T$, obviously $S \subset U$. So (1) yields $U^{-1}R = U^{-1}(S^{-1}R)$. Now, clearly $U^{-1}(S^{-1}R) = T^{-1}(S^{-1}R)$. Similarly, $U^{-1}R = S^{-1}(T^{-1}R)$. Thus (2) holds.

Finally, in any ring, a product is a unit if and only if each factor is a unit. So a homomorphism $\varphi\colon R \to R'$ carries S' into $R'^{\times}$ if and only if φ carries S into $R'^{\times}$. Thus $S'^{-1}R$ and $S^{-1}R$ are universal examples of R-algebras that satisfy equivalent conditions. Thus (3) holds. □

Exercise **(11.28)**. — Let R be a domain, S a multiplicative set with $0 \notin S$. Assume R is normal. Show that $S^{-1}R$ is normal.

Answer: Since $0 \notin S$, clearly $\mathrm{Frac}(S^{-1}R) = \mathrm{Frac}(R)$ owing to (11.3). Given $x \in \mathrm{Frac}(R)$ integral over $S^{-1}R$, let

$$x^n + a_1x^{n-1} + \cdots + a_n = 0$$

be an equation of integral dependence. Write $a_i = b_i/s_i$ with $b_i \in R$ and $s_i \in S$, and set $s := \prod s_i$. Then multiplying the equation by s^n, we obtain

$$(sx)^n + sa_1(sx)^{n-1} + \cdots + s^na_n = 0.$$

So since R is normal, $sx \in R$. Thus $x \in S^{-1}R$. □

12. Localization of Modules

Exercise **(12.4)**. — Let R be a ring, S a multiplicative set, and M a module. Show that $M = S^{-1}M$ if and only if M is an $S^{-1}R$-module.

Answer: If $M = S^{-1}M$, then obviously M is an $S^{-1}R$-module. Conversely, if M is an $S^{-1}R$-module, then M equipped with the identity map has the UMP that characterizes $S^{-1}M$; whence, $M = S^{-1}M$. □

Exercise **(12.5)**. — Let R be a ring, $S \subset T$ multiplicative sets, M a module. Set $T_1 := \varphi_S(T) \subset S^{-1}R$. Show $T^{-1}M = T^{-1}(S^{-1}M) = T_1^{-1}(S^{-1}M)$.

Answer: Let's check that both $T^{-1}(S^{-1}M)$ and $T_1^{-1}(S^{-1}M)$ have the UMP characterizing $T^{-1}M$. Let $\psi\colon M \to N$ be an R-linear map into an $T^{-1}R$-module. Then the multiplication map $\mu_s\colon N \to N$ is bijective for all $s \in T$ by (12.1), so for all $s \in S$ since $S \subset T$. Hence ψ factors via a unique $S^{-1}R$-linear map $\rho\colon S^{-1}M \to N$ by (12.3) and by (12.1) again.

Similarly, ρ factors through a unique $T^{-1}R$-linear map $\rho'\colon T^{-1}(S^{-1}M) \to N$. Hence $\psi = \rho'\varphi_T\varphi_S$, and ρ' is clearly unique, as required. Also, ρ factors through a unique $T_1^{-1}(S^{-1}R)$-linear map $\rho_1'\colon T_1^{-1}(S^{-1}M) \to N$. Hence $\psi = \rho_1'\varphi_{T_1}\varphi_S$, and ρ_1' is clearly unique, as required. □

Exercise **(12.6)**. — Let R be a ring, S a multiplicative set. Show that S becomes a filtered category when equipped as follows: given $s, t \in S$, set

$$\mathrm{Hom}(s,t) := \{x \in R \mid xs = t\}.$$

Given a module M, define a functor $S \to ((R\text{-mod}))$ as follows: for $s \in S$, set $M_s := M$; to each $x \in \mathrm{Hom}(s,t)$, associate $\mu_x\colon M_s \to M_t$. Define $\beta_s\colon M_s \to S^{-1}M$ by $\beta_s(m) := m/s$. Show the β_s induce an isomorphism $\varinjlim M_s \xrightarrow{\sim} S^{-1}M$.

Answer: Clearly, S is a category. Now, given $s, t \in S$, set $u := st$. Then $u \in S$; also $t \in \mathrm{Hom}(s,u)$ and $s \in \mathrm{Hom}(t,u)$. Given $x, y \in \mathrm{Hom}(s,t)$, we have $xs = t$ and $ys = t$. So $s \in \mathrm{Hom}(t,u)$ and $xs = ys$ in $\mathrm{Hom}(s,u)$. Thus S is filtered.

Further, given $x \in \mathrm{Hom}(s,t)$, we have $\beta_t \mu_x = \beta_s$ since $m/s = xm/t$ as $xs = t$. So the β_s induce a homomorphism $\beta\colon \varinjlim M_s \to S^{-1}M$. Now, every element of $S^{-1}M$ is of the form m/s, and $m/s =: \beta_s(m)$; hence, β is surjective.

Each $m \in \varinjlim M_s$ lifts to an $m' \in M_s$ for some $s \in S$ by (7.8)(1). Assume $\beta m = 0$. Then $\beta_s m' = 0$ as the β_s induce β. But $\beta_s m' = m'/s$. So there is $t \in S$ with $tm' = 0$. So $\mu_t m' = 0$ in M_{st}, and $\mu_t m' \mapsto m$. So $m = 0$. Thus β is injective, so an isomorphism. □

Exercise **(12.7)**. — Let R be a ring, S a multiplicative set, M a module. Prove $S^{-1}M = 0$ if $\mathrm{Ann}(M) \cap S \neq \emptyset$. Prove the converse if M is finitely generated.

Answer: Say $f \in \mathrm{Ann}(M) \cap S$. Let $m/t \in S^{-1}M$. Then $f/1 \cdot m/t = fm/t = 0$. Hence $m/t = 0$. Thus $S^{-1}M = 0$.

Conversely, assume $S^{-1}M = 0$, and say $m_1, \dots m_n$ generate M. Then for each i, there is $f_i \in S$ with $f_i m_i = 0$. Then $\prod f_i \in \mathrm{Ann}(M) \cap S$, as desired. □

Exercise **(12.11)**. — Let R be a ring, S a multiplicative set, P a projective module. Then $S^{-1}P$ is a projective $S^{-1}R$-module.

Answer: By (5.22), there is a module K such that $F := K \oplus P$ is free. So (12.9) yields that $S^{-1}F = S^{-1}P \oplus S^{-1}L$ and that $S^{-1}F$ is free over $S^{-1}R$. Hence $S^{-1}P$ is a projective $S^{-1}R$-module again by (5.22). □

Exercise **(12.13)**. — Let R be a ring, S a multiplicative set, M and N modules. Show $S^{-1}(M \otimes_R N) = S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} S^{-1}N = S^{-1}M \otimes_R S^{-1}N$.

Answer: By (12.12), $S^{-1}(M \otimes_R N) = S^{-1}R \otimes_R (M \otimes_R N)$. The latter is equal to $(S^{-1}R \otimes_R M) \otimes_R N$ by associativity (8.9). Again by (12.12), the latter is equal to $S^{-1}M \otimes_R N$. Thus the first equality holds.

By cancellation (8.10), $S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} (S^{-1}R \otimes_R N)$, and the latter is equal to $S^{-1}M \otimes_{S^{-1}R} S^{-1}N$ by (12.12). Thus the second equality holds.

Finally by (8.8), the kernel of the map $S^{-1}M \otimes_R S^{-1}N \to S^{-1}M \otimes_{S^{-1}R} S^{-1}N$ is generated by elements $(xm/s) \otimes (n/1) - (m/1) \otimes (xn/s)$ with $m \in M$, $n \in N$, $x \in R$, and $s \in S$. Those elements are zero because μ_s is an isomorphism on the $S^{-1}R$-module $S^{-1}M \otimes_R S^{-1}N$. Thus the third equality holds. □

Exercise **(12.24)**. — Set $R := \mathbb{Z}$ and $S = \mathbb{Z} - \langle 0 \rangle$. Set $M := \bigoplus_{n \geq 2} \mathbb{Z}/\langle n \rangle$ and $N := M$. Show that the map σ of (12.21) is not injective.

Answer: Given $m > 0$, let e_n be the nth standard basis element for some $n > m$. Then $m \cdot e_n \neq 0$. Hence $\mu_R\colon R \to \mathrm{Hom}_R(M, M)$ is injective. But $S^{-1}M = 0$, as any $x \in M$ has only finitely many nonzero components; so $kx = 0$ for some nonzero integer k. So $\mathrm{Hom}(S^{-1}M, S^{-1}M) = 0$. Thus σ is not injective. □

13. Support

Exercise **(13.3)**. — Let R be a ring, $\mathfrak{p} \in \mathrm{Spec}(R)$. Show that $\mathfrak{p}$ is a closed point — that is, $\{\mathfrak{p}\}$ is a closed set — if and only if $\mathfrak{p}$ is a maximal ideal.

Answer: If $\mathfrak{p}$ is maximal, then $\mathbf{V}(\mathfrak{p}) = \{\mathfrak{p}\}$; so $\mathfrak{p}$ is closed.

Conversely, suppose $\mathfrak{p}$ is not maximal. Then $\mathfrak{p} \subsetneqq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. If $\mathfrak{p} \in \mathbf{V}(\mathfrak{a})$, then $\mathfrak{m} \in \mathbf{V}(\mathfrak{a})$ too. So $\{\mathfrak{p}\} \neq \mathbf{V}(\mathfrak{a})$. Thus $\{\mathfrak{p}\}$ is not closed. □

Exercise **(13.10)**. — Let R be a ring, M a module, $\mathfrak{p} \in \operatorname{Supp}(M)$. Prove

$$\mathbf{V}(\mathfrak{p}) \subset \operatorname{Supp}(M).$$

Answer: Let $\mathfrak{q} \in \mathbf{V}(\mathfrak{p})$. Then $\mathfrak{q} \supset \mathfrak{p}$. So $M_\mathfrak{p} = (M_\mathfrak{q})_\mathfrak{p}$ by (11.25)(1). Now, $\mathfrak{p} \in \operatorname{Supp}(M)$. So $M_\mathfrak{p} \neq 0$. Hence $M_\mathfrak{q} \neq 0$. Thus $\mathfrak{q} \in \operatorname{Supp}(M)$. □

Exercise **(13.11)**. — Let $\mathbb{Z}$ be the integers, $\mathbb{Q}$ the rational numbers, and set $M := \mathbb{Q}/\mathbb{Z}$. Find $\operatorname{Supp}(M)$, and show that it is not Zariski closed.

Answer: Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $M_\mathfrak{p} = \mathbb{Q}_\mathfrak{p}/\mathbb{Z}_\mathfrak{p}$ since localization is exact by (12.16). Now, $\mathbb{Q}_\mathfrak{p} = \mathbb{Q}$ by (12.4) and (12.1) since $\mathbb{Q}$ is a field. If $\mathfrak{p} \neq \langle 0\rangle$, then $\mathbb{Z}_\mathfrak{p} \neq \mathbb{Q}_\mathfrak{p}$ since $\mathfrak{p}\mathbb{Z}_\mathfrak{p} \cap \mathbb{Z} = \mathfrak{p}$ by (11.15). If $\mathfrak{p} = \langle 0\rangle$, then $\mathbb{Z}_\mathfrak{p} = \mathbb{Q}_\mathfrak{p}$. Thus $\operatorname{Supp}(M)$ consists of all the nonzero primes of $\mathbb{Z}$.

Finally, suppose $\operatorname{Supp}(M) = \mathbf{V}(\mathfrak{a})$. Then $\mathfrak{a}$ lies in every nonzero prime; so $\mathfrak{a} = \langle 0\rangle$. But $\langle 0\rangle$ is prime. Hence $\langle 0\rangle \in \mathbf{V}(\mathfrak{a}) = \operatorname{Supp}(M)$, contradicting the above. Thus $\operatorname{Supp}(M)$ is not closed. □

Exercise **(13.13)**. — Prove these three conditions on a ring R are equivalent:

(1) R is reduced.
(2) $S^{-1}R$ is reduced for all multiplicatively closed sets S.
(3) $R_\mathfrak{m}$ is reduced for all maximal ideals $\mathfrak{m}$.

Answer: Assume (1) holds. Then $\operatorname{nil}(R) = 0$. But $\operatorname{nil}(R)(S^{-1}R) = \operatorname{nil}(S^{-1}R)$ by (11.14). Thus (2) holds. Trivially (2) implies (3).

Assume (3) holds. Then $\operatorname{nil}(R_\mathfrak{m}) = 0$. Hence $\operatorname{nil}(R)_\mathfrak{m} = 0$ by (11.14) and (12.2). So $\operatorname{nil}(R) = 0$ by (13.12). Thus (1) holds. □

Exercise **(13.14)**. — Let R be a ring, Σ the set of minimal primes. Prove this:

(1) If $R_\mathfrak{p}$ is a domain for any prime $\mathfrak{p}$, then the $\mathfrak{p} \in \Sigma$ are pairwise comaximal.
(2) $R_\mathfrak{p}$ is a domain for any prime $\mathfrak{p}$ and Σ is finite if and only if $R = \prod_{i=1}^n R_i$ where R_i is a domain. If so, then $R_i = R/\mathfrak{p}_i$ with $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \Sigma$.

Answer: Consider (1). Suppose $\mathfrak{p}, \mathfrak{q} \in \Sigma$ are not comaximal. Then $\mathfrak{p} + \mathfrak{q}$ lies in some maximal ideal $\mathfrak{m}$. Hence $R_\mathfrak{m}$ contains two minimal primes, $\mathfrak{p}R_\mathfrak{m}$ and $\mathfrak{q}R_\mathfrak{m}$, by (11.16). However, $R_\mathfrak{m}$ is a domain by hypothesis, and so $\langle 0\rangle$ is its only minimal prime. Hence $\mathfrak{p}R_\mathfrak{m} = \mathfrak{q}R_\mathfrak{m}$. So $\mathfrak{p} = \mathfrak{q}$. Thus (1) holds.

Consider (2). Assume $R_\mathfrak{p}$ is a domain for any $\mathfrak{p}$. Then R is reduced by (13.13). Assume, also, Σ is finite. Form the canonical map $\varphi\colon R \to \prod_{\mathfrak{p}\in\Sigma} R/\mathfrak{p}$; it is injective by (3.22), and surjective by (1) and the Chinese Remainder Theorem (1.12). Thus R is a finite product of domains.

Conversely, assume $R = \prod_{i=1}^n R_i$ where R_i is a domain. Let $\mathfrak{p}$ be a prime of R. Then $R_\mathfrak{p} = \prod (R_i)_\mathfrak{p}$ by (12.10). Each $(R_i)_\mathfrak{p}$ is a domain by (11.3). But $R_\mathfrak{p}$ is local. So $R_\mathfrak{p} = (R_i)_\mathfrak{p}$ for some i by (2.5). Thus $R_\mathfrak{p}$ is a domain. Further, owing to (2.11), each $\mathfrak{p}_i \in \Sigma$ has the form $\mathfrak{p}_i = \prod \mathfrak{a}_j$ where, after renumbering, $\mathfrak{a}_i = \langle 0\rangle$ and $\mathfrak{a}_j = R_j$ for $j \neq i$. Thus the ith projection gives $R/\mathfrak{p}_i \xrightarrow{\sim} R_i$. Thus (2) holds. □

Exercise **(13.16)**. — Let R be a ring, M a module. Prove elements $m_\lambda \in M$ generate M if and only if, at every maximal ideal $\mathfrak{m}$, their images m_λ generate $M_\mathfrak{m}$.

Answer: The m_λ define a map $\alpha\colon R^{\oplus\{\lambda\}} \to M$. By (13.15), it is surjective if and only if $\alpha_{\mathfrak m}\colon \big(R^{\oplus\{\lambda\}}\big)_{\mathfrak m} \to M_{\mathfrak m}$ is surjective for all $\mathfrak m$. But $\big(R^{\oplus\{\lambda\}}\big)_{\mathfrak m} = R_{\mathfrak m}^{\oplus\{\lambda\}}$ by (12.10). Hence (4.10)(1) yields the assertion. □

Exercise **(13.21)**. — Given n, prove an R-module P is locally free of rank n if and only if P is finitely generated and $P_{\mathfrak m} \simeq R^n_{\mathfrak m}$ holds at each maximal ideal $\mathfrak m$.

Answer: If P is locally free of rank n, then P is finitely generated by (13.20). Also, for any $\mathfrak p \in \operatorname{Spec}(R)$, there's $f \in R - \mathfrak p$ with $P_f \simeq R^n_f$; so $P_{\mathfrak p} \simeq R^n_{\mathfrak p}$ by (12.5).

As to the converse, given any prime $\mathfrak p$, take a maximal ideal $\mathfrak m$ containing it. Assume $P_{\mathfrak m} \simeq R^n_{\mathfrak m}$. Take a free basis $p_1/f_1^{k_1}, \dots, p_n/f_n^{k_n}$ of $P_{\mathfrak m}$ over $R_{\mathfrak m}$. The p_i define a map $\alpha\colon R^n \to P$, and $\alpha_{\mathfrak m}\colon R^n_{\mathfrak m} \to P_{\mathfrak m}$ is bijective, so surjective.

Assume P is finitely generated. Then (12.20)(1) provides $f \in R - \mathfrak m$ such that $\alpha_f\colon R^n_f \to P_f$ is surjective. Hence $\alpha_{\mathfrak q}\colon R^n_{\mathfrak q} \to P_{\mathfrak q}$ is surjective for every $\mathfrak q \in \mathbf D(f)$ by (12.5) and (12.16). Assume $P_{\mathfrak q} \simeq R^n_{\mathfrak q}$ if also $\mathfrak q$ is maximal. So $\alpha_{\mathfrak q}$ is bijective by (10.4). Clearly, $\alpha_{\mathfrak q} = (\alpha_f)_{(\mathfrak q R_f)}$. Hence $\alpha_f\colon R^n_f \to P_f$ is bijective owing to (13.15) with R_f for R, as desired. □

14. Krull–Cohen–Seidenberg Theory

Exercise **(14.4)**. — Let $R \subset R'$ be an integral extension of rings, and $\mathfrak p$ a prime of R. Suppose R' has just one prime $\mathfrak p'$ over $\mathfrak p$. Show (a) that $\mathfrak p' R'_{\mathfrak p}$ is the only maximal ideal of $R'_{\mathfrak p}$, (b) that $R'_{\mathfrak p'} = R'_{\mathfrak p}$, and (c) that $R'_{\mathfrak p'}$ is integral over $R_{\mathfrak p}$.

Answer: Since R' is integral over R, the localization $R'_{\mathfrak p}$ is integral over $R_{\mathfrak p}$ by (11.20). Moreover, $R_{\mathfrak p}$ is a local ring with unique maximal ideal $\mathfrak p R_{\mathfrak p}$ by (11.18). Hence, every maximal ideal of $R'_{\mathfrak p}$ lies over $\mathfrak p R_{\mathfrak p}$ by (14.3)(1). But every maximal ideal of $R'_{\mathfrak p}$ is the extension of some prime $\mathfrak q' \subset R'$ by (11.16)(2), and therefore $\mathfrak q'$ lies over $\mathfrak p$ in R. So, by hypothesis, $\mathfrak q' = \mathfrak p'$. Thus $\mathfrak p' R'_{\mathfrak p}$ is the only maximal ideal of $R'_{\mathfrak p}$; that is, (a) holds. So $R'_{\mathfrak p} - \mathfrak p' R'_{\mathfrak p}$ consists of units. Hence (11.25) and (11.6) yield (b). But $R'_{\mathfrak p}$ is integral over $R_{\mathfrak p}$; so (c) holds too. □

Exercise **(14.5)**. — Let $R \subset R'$ be an integral extension of domains, and $\mathfrak p$ a prime of R. Suppose R' has at least two distinct primes $\mathfrak p'$ and $\mathfrak q'$ lying over $\mathfrak p$. Show that $R'_{\mathfrak p'}$ is not integral over $R_{\mathfrak p}$. Show that, in fact, if y lies in $\mathfrak q'$, but not in $\mathfrak p'$, then $1/y \in R'_{\mathfrak p'}$ is not integral over $R_{\mathfrak p}$.

Answer: Suppose $1/y$ is integral over $R_{\mathfrak p}$. Say

$$(1/y)^n + a_1(1/y)^{n-1} + \cdots + a_n = 0$$

with $n \ge 1$ and $a_i \in R_{\mathfrak p}$. Multiplying by y^{n-1}, we obtain

$$1/y = -(a_1 + \cdots + a_n y^{n-1}) \in R'_{\mathfrak p}.$$

However, $y \in \mathfrak q'$, so $y \in \mathfrak q' R'_{\mathfrak p}$. Hence $1 \in \mathfrak q' R'_{\mathfrak p}$. So $\mathfrak q' \cap (R - \mathfrak p) \ne \emptyset$ by (11.15)(3). But $\mathfrak q' \cap R = \mathfrak p$, a contradiction. So $1/y$ is not integral over $R_{\mathfrak p}$. □

Exercise **(14.6)**. — Let k be a field, and X an indeterminate. Set $R' := k[X]$, and $Y := X^2$, and $R := k[Y]$. Set $\mathfrak p := (Y-1)R$ and $\mathfrak p' := (X-1)R'$. Is $R'_{\mathfrak p'}$ integral over $R_{\mathfrak p}$? Explain.

Answer: Note that R' is a domain, and that the extension $R \subset R'$ is integral as R' is generated by 1 and X as an R-module.

Suppose the characteristic is not 2. Set $\mathfrak{q}' := (X+1)R'$. Then both $\mathfrak{p}'$ and $\mathfrak{q}'$ contain $Y-1$, so lie over the maximal ideal $\mathfrak{p}$ of R. Further $X+1$ lies in $\mathfrak{q}'$, but not in $\mathfrak{p}'$. Hence $R'_{\mathfrak{p}'}$ is not integral over $R_{\mathfrak{p}}$ by (14.5).

Suppose the characteristic is 2. Then $(X-1)^2 = Y-1$. Let $\mathfrak{q}' \subset R'$ be a prime over $\mathfrak{p}$. Then $(X-1)^2 \in \mathfrak{q}'$. So $\mathfrak{p}' \subset \mathfrak{q}'$. But $\mathfrak{p}'$ is maximal. So $\mathfrak{q}' = \mathfrak{p}'$. Thus R' has just one prime $\mathfrak{p}'$ over $\mathfrak{p}$. Hence $R'_{\mathfrak{p}'}$ is integral over $R_{\mathfrak{p}}$ by (14.4). □

Exercise **(14.12)**. — Let R be a reduced ring, Σ the set of minimal primes. Prove that $\mathrm{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$ and that $R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$ for any $\mathfrak{p} \in \Sigma$.

Answer: If $\mathfrak{p} \in \Sigma$, then $\mathfrak{p} \subset \mathrm{z.div}(R)$ by (14.10). Thus $\mathrm{z.div}(R) \supset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$.

Conversely, say $xy = 0$. If $x \notin \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $y \in \mathfrak{p}$. So if $x \notin \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, then $y \in \bigcap_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. But $\bigcap_{\mathfrak{p}\in\Sigma} \mathfrak{p} = \langle 0 \rangle$ by the Scheinnullstellensatz (3.17) and (3.11). So $y = 0$. Hence if $x \notin \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, then $x \notin \mathrm{z.div}(R)$. Thus $\mathrm{z.div}(R) \subset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. Thus $\mathrm{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$.

Fix $\mathfrak{p} \in \Sigma$. Then $R_{\mathfrak{p}}$ is reduced by (13.13). Further, $R_{\mathfrak{p}}$ has only one prime, namely $\mathfrak{p}R_{\mathfrak{p}}$, by (11.16)(2). Hence $R_{\mathfrak{p}}$ is a field, and $\mathfrak{p}R_{\mathfrak{p}} = \langle 0 \rangle$. But by (12.19), $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$. Thus $R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$. □

Exercise **(14.13)**. — Let R be a ring, Σ the set of minimal primes, and K the total quotient ring. Assume Σ is finite. Prove these three conditions are equivalent:

(1) R is reduced.
(2) $\mathrm{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, and $R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$.
(3) $K/\mathfrak{p}K = \mathrm{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$, and $K = \prod_{\mathfrak{p}\in\Sigma} K/\mathfrak{p}K$.

Answer: Assume (1) holds. Then (14.12) yields (2).

Assume (2) holds. Set $S := R - \mathrm{z.div}(R)$. Let $\mathfrak{q}$ be a prime of R with $\mathfrak{q} \cap S = \emptyset$. Then $\mathfrak{q} \subset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. But Σ is finite. So $\mathfrak{q} \subset \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$ by Prime Avoidance (3.12). Hence $\mathfrak{q} = \mathfrak{p}$ since $\mathfrak{p}$ is minimal. But $K = S^{-1}R$. Therefore, by (11.16)(2), for $\mathfrak{p} \in \Sigma$, the extensions $\mathfrak{p}K$ are the only primes of K, and they all are both maximal and minimal.

Fix $\mathfrak{p} \in \Sigma$. Then $K/\mathfrak{p}K = S^{-1}(R/\mathfrak{p})$ by (12.18). So $S^{-1}(R/\mathfrak{p})$ is a field. But clearly $S^{-1}(R/\mathfrak{p}) \subset \mathrm{Frac}(R/\mathfrak{p})$. Therefore, $K/\mathfrak{p}K = \mathrm{Frac}(R/\mathfrak{p})$ by (2.3). Further, $S \subset R - \mathfrak{p}$. Hence (11.16)(2) yields $\mathfrak{p} = \varphi_S^{-1}(\mathfrak{p}K)$. Therefore, $\varphi_S^{-1}(K - \mathfrak{p}K) = R - \mathfrak{p}$. So $K_{\mathfrak{p}K} = R_{\mathfrak{p}}$ by (11.23). But $R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$ by hypothesis. Thus K has only finitely many primes, the $\mathfrak{p}K$; each $\mathfrak{p}K$ is minimal, and each $K_{\mathfrak{p}K}$ is a domain. Therefore, (13.14)(2) yields $K = \prod_{\mathfrak{p}\in\Sigma} K/\mathfrak{p}K$. Thus (3) holds.

Assume (3) holds. Then K is a finite product of fields, and fields are reduced. But clearly, a product of reduced ring is reduced. Further, $R \subset K$, and trivially, a subring of a reduced ring is reduced. Thus (1) holds. □

Exercise **(14.15)**. — Let R be a ring, $\mathfrak{p}_1 \ldots, \mathfrak{p}_r$ all its minimal primes, and K the total quotient ring. Prove that these three conditions are equivalent:

(1) R is normal.
(2) R is reduced and integrally closed in K.
(3) R is a finite product of normal domains R_i.

If so, then the R_i are equal to the $R/\mathfrak{p}_j$ up to order.

Answer: Assume (1). Then R is reduced by (13.13). Let $x \in K$ be integral over R, and $\mathfrak{m}$ any maximal ideal. Then $x/1$ is integral over $R_{\mathfrak{m}}$. So $x/1 \in R_{\mathfrak{m}}$ by hypothesis. Hence $(R[x]/R)_{\mathfrak{m}} = 0$. Therefore, $R[x]/R = 0$ by (13.12). So $x \in R$ Thus (2) holds.

Assume (2). Set $R_i := R/\mathfrak{p}_i$ and $K_i := \mathrm{Frac}(R_i)$. Then $K = \prod K_i$ by (14.13). Let R_i' be the normalization of R_i. Then $R \subset \prod R_i \subset \prod R_i'$. Further, the first extension is integral by (10.21), and the second, by (10.23); whence, $R \subset \prod R_i'$ is integral by the tower property (10.19). However, R is integrally closed in K by hypothesis. Hence $R = \prod R_i = \prod R_i'$. Thus (3) and the last assertion hold.

Assume (3). Let $\mathfrak{p}$ be any prime of R. Then $R_{\mathfrak{p}} = \prod (R_i)_{\mathfrak{p}}$ by (12.10), and each $(R_i)_{\mathfrak{p}}$ is normal by (11.28). But $R_{\mathfrak{p}}$ is local. So $R_{\mathfrak{p}} = (R_i)_{\mathfrak{p}}$ for some i by (3.5). Hence $R_{\mathfrak{p}}$ is a normal domain. Thus (1) holds. □

15. Noether Normalization

Exercise **(15.2)**. — Let $k := \mathbb{F}_q$ be the finite field with q elements, and $k[X, Y]$ the polynomial ring. Set $f := X^qY - XY^q$ and $R := k[X, Y]/\langle f\rangle$. Let $x, y \in R$ be the residues of X, Y. For every $a \in k$, show that R is not module finite over $P := k[y - ax]$. (Thus, in (15.1), no k-linear combination works.) First, take $a = 0$.

Answer: Take $a = 0$. Then $P = k[y]$. Any algebraic relation over P satisfied by x is given by a polynomial in $k[X, Y]$, which is a multiple of f. However, no multiple of f is monic in X. So x is not integral over P. By (10.15), R is not module finite over P.

Consider an arbitrary a. Since $a^q = a$, after the change of variable $Y' := Y - aX$, our f still has the same form. Thus, we have reduced to the previous case. □

Exercise **(15.3)**. — Let k be a field, and X, Y, Z variables. Set

$$R := k[X, Y, Z]\big/\langle X^2 - Y^3 - 1,\ XZ - 1\rangle,$$

and let x, y, $z \in R$ be the residues of X, Y, Z. Fix $a, b \in k$, and set $t := x + ay + bz$ and $P := k[t]$. Show that x and y are integral over P for any a, b and that z is integral over P if and only if $b \neq 0$.

Answer: To see x is integral, noice $xz = 1$, so $x^2 - tx + b = -axy$. Raising both sides of the latter equation to the third power, and using the equation $y^3 = x^2 - 1$, we obtain an equation of integral dependence of degree 6 for x over P. Now, $y^3 - x^2 - 1 = 0$, so y is integral over $P[x]$. Hence, the Tower Property, (10.19), implies that y too is integral over P.

If $b \neq 0$, then $z = b^{-1}(t - x - ay) \in P[x, y]$, and so z is integral over P by (10.20).

Assume $b = 0$ and z is integral over P. Now, $P \subset k[x, y]$. So z is integral over $k[x, y]$ as well. But $y^3 - x^2 + 1 = 0$. So y is integral over $k[x]$. Hence z is too. However, $k[x]$ is a polynomial ring, so integrally closed in its fraction field $k(x)$ by (10.26)(1). Moreover, $z = 1/x \in k(x)$. Hence, $1/x \in k[x]$, which is absurd. Thus z is not integral over P if $b = 0$. □

Exercise **(15.7)**. — Let k be a field, K an algebraically closed extension field. (So K contains a copy of every finite extension field.) Let $P := k[X_1, \dots, X_n]$ be the polynomial ring, and $f, f_1, \dots, f_r \in P$. Assume f vanishes at every zero in K^n of

$f_1, \dots, f_r$; in other words, if $(a) := (a_1, \dots, a_n) \in K^n$ and $f_1(a) = 0, \dots, f_r(a) = 0$, then $f(a) = 0$ too. Prove that there are polynomials $g_1, \dots, g_r \in P$ and an integer N such that $f^N = g_1 f_1 + \cdots + g_r f_r$.

Answer: Set $\mathfrak{a} := \langle f_1, \dots, f_r \rangle$. We have to show $f \in \sqrt{\mathfrak{a}}$. But, by the Hilbert Nullstellensatz, $\sqrt{\mathfrak{a}}$ is equal to the intersection of all the maximal ideals $\mathfrak{m}$ containing $\mathfrak{a}$. So given an $\mathfrak{m}$, we have to show that $f \in \mathfrak{m}$.

Set $L := P/\mathfrak{m}$. By the weak Nullstellensatz, L is a finite extension field of k. So we may embed L/k as a subextension of K/k. Let $a_i \in K$ be the image of the variable $X_i \in P$, and set $(a) := (a_1, \dots, a_n) \in K^n$. Then $f_1(a) = 0, \dots, f_r(a) = 0$. Hence $f(a) = 0$ by hypothesis. Therefore, $f \in \mathfrak{m}$, as desired. □

Exercise **(15.12)**. — Let R be a domain of (finite) dimension r, and $\mathfrak{p}$ a nonzero prime. Prove $\dim(R/\mathfrak{p}) < r$.

Answer: Every chain of primes of $R/\mathfrak{p}$ is of the form $\mathfrak{p}_0/\mathfrak{p} \subsetneqq \cdots \subsetneqq \mathfrak{p}_s/\mathfrak{p}$ where $0 \subsetneqq \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_s$ is a chain of primes of R. So $s < r$. Thus $\dim(R/\mathfrak{p}) < r$. □

Exercise **(15.13)**. — Let R'/R be an integral extension of rings. Prove that $\dim(R) = \dim(R')$.

Answer: Let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ be a chain of primes of R. Repeated application of Lying over, (14.3)(3), yields a chain of primes $\mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ of R' with $\mathfrak{p}_i = \mathfrak{p}'_i \cap R$ for each i. Thus $\dim(R) \le \dim(R')$.

Conversely, let $\mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ be a chain of prime ideals of R'. Set $\mathfrak{p}_i := \mathfrak{p}'_i \cap R$. Then $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ by Incomparability, (14.3)(2). Thus $\dim(R') \le \dim(R)$. Thus $\dim(R') = \dim(R)$. □

Exercise **(15.16)**. — Let k be a field, R a finitely generated k-algebra, $f \in R$ nonzero. Assume R is a domain. Prove that $\dim(R) = \dim(R_f)$.

Answer: Note that R_f is a finitely generated R-algebra since it is obtained by adjoining $1/f$. So since R is a finitely generated k-algebra, R_f is one too. Moreover, R and R_f have the same fraction field K. Hence both $\dim(R)$ and $\dim(R_f)$ are equal to $\operatorname{tr.deg}_k(K)$ by (15.10). □

Exercise **(15.17)**. — Let k be a field, $P := k[f]$ the polynomial ring in one variable f. Set $\mathfrak{p} := \langle f \rangle$ and $R := P_{\mathfrak{p}}$. Find $\dim(R)$ and $\dim(R_f)$.

Answer: In P, the chain of primes $0 \subset \mathfrak{p}$ is of maximal length by (2.6) and (2.20) or (15.10). So 0 and $\mathfrak{p}R$ are the only primes in R by (11.16). Thus $\dim(R) = 1$.

Set $K := \operatorname{Frac}(P)$. Then $R_f = K$ since, if $a/(bf^n) \in K$ with $a, b \in P$ and $f \nmid b$, then $a/b \in R$ and so $(a/b)/f^n \in R_f$. Thus $\dim(R_f) = 0$. □

16. Chain Conditions

Exercise **(16.2)**. — Let $\mathfrak{a}$ be a finitely generated ideal in an arbitrary ring. Show every set that generates $\mathfrak{a}$ contains a finite subset that generates $\mathfrak{a}$.

Answer: Say $\mathfrak{a}$ is generated by $x_1, \dots, x_r$ and also by the y_λ for $\lambda \in \Lambda$. Write $x_i = \sum_j z_j y_{\lambda_{ij}}$. Then the $y_{\lambda_{ij}}$ generate $\mathfrak{a}$. □

Exercise **(16.13)**. — Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence of R-modules, and M_1, M_2 two submodules of M. Prove or give a counterexample to this statement: if $\beta(M_1) = \beta(M_2)$ and $\alpha^{-1}(M_1) = \alpha^{-1}(M_2)$, then $M_1 = M_2$.

Answer: The statement is false: form the exact sequence

$$0 \to \mathbb{R} \xrightarrow{\alpha} \mathbb{R} \oplus \mathbb{R} \xrightarrow{\beta} \mathbb{R} \to 0$$

with $\alpha(r) := (r, 0)$ and $\beta(r, s) := s$, and take

$$M_1 := \{(t, 2t) \mid t \in \mathbb{R}\} \quad \text{and} \quad M_2 := \{(2t, t) \mid t \in \mathbb{R}\}.$$

(Geometrically, we can view M_1 as the line determined by the origin and the point $(1, 2)$, and M_2 as the line determined by the origin and the point $(2, 1)$. Then $\beta(M_1) = \beta(M_2) = \mathbb{R}$, and $\alpha^{-1}(M_1) = \alpha^{-1}(M_2) = 0$, but $M_1 \neq M_2$ in $\mathbb{R} \oplus \mathbb{R}$.) □

Exercise **(16.16)**. — Let R be a ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ ideals such that each $R/\mathfrak{a}_i$ is a Noetherian ring. Prove (1) that $\bigoplus R/\mathfrak{a}_i$ is a Noetherian R-module, and (2) that, if $\bigcap \mathfrak{a}_i = 0$, then R too is a Noetherian ring.

Answer: Any R-submodule of $R/\mathfrak{a}_i$ is an ideal of $R/\mathfrak{a}_i$. Since $R/\mathfrak{a}_i$ is a Noetherian ring, such an ideal is finitely generated as an $(R/\mathfrak{a}_i)$-module, so as an R-module as well. Thus $R/\mathfrak{a}_i$ is a Noetherian R-module. So $\bigoplus R/\mathfrak{a}_i$ is a Noetherian R-module by (16.15). Thus (1) holds.

To prove (2), note that the kernel of the natural map $R \to \bigoplus R/\mathfrak{a}_i$ is $\bigcap \mathfrak{a}_i$, which is 0 by hypothesis. So R can be identified with a submodule of the Noetherian R-module $\bigoplus R/\mathfrak{a}_i$. Hence R itself is a Noetherian R-module by (16.14)(2). So R is a Noetherian ring by (16.11). □

Exercise **(16.18)**. — Let G be a finite group acting on a domain R, and R' the subring of invariants. Let $k \subset R'$ be a field. Using (10.14), prove this celebrated theorem of E. Noether (1926): if R is a finitely generated k-algebra, then so is R'.

Answer: Say $x_1, \ldots, x_n \in R$ form a set of algebra generators. For each x_i, form the elementary symmetric functions y_{ij} in the conjugates gx_i, and let R'' be the k-subalgebra of R generated by all the y_{ij} for all i, j. Then, by (10.14), the x_i are integral over R''. Hence, R is module finite over R'' by (10.20). Now, R'' is a finitely generated k-algebra, so Noetherian by (16.10). Hence $R' \subset R$ is finite over R'' by (16.17). But R'' is a finitely generated k-algebra; hence, R is too. □

Exercise **(16.22)**. — Let k be a field, R an algebra. Assume that R is finite dimensional as a k-vector space. Prove that R is Noetherian and Artinian.

Answer: View R as a vector space, and ideals as subspaces. Now, by a simple dimension argument, any ascending or descending chain of subspaces of R stabilizes. Thus R is Noetherian by (16.5) and is Artinian by definition. □

Exercise **(16.23)**. — Let p be a prime number, and set $M := \mathbb{Z}[1/p]/\mathbb{Z}$. Prove that any $\mathbb{Z}$-submodule $N \subset M$ is either finite or all of M. Deduce that M is an Artinian $\mathbb{Z}$-module, and that it is not Noetherian.

Answer: Given $q \in N$, write $q = n/p^e$ where n is relatively prime to p. Then there is an $m \in \mathbb{Z}$ with $nm \equiv 1 \pmod{p^e}$. Hence $N \ni m(n/p^e) = 1/p^e$, and so $1/p^r = p^{e-r}(1/p^e) \in N$ for any $0 \le r \le e$. Therefore, either $N = M$, or there is a largest integer $e \ge 0$ with $1/p^e \in N$. In the second case, N is finite.

Let $M \supsetneqq N_1 \supset N_2 \supset \cdots$ be a descending chain. By what we just proved, each N_i is finite, say with n_i elements. Then the sequence $n_1 \ge n_2 \ge \cdots$ stabilizes; say $n_i = n_{i+1} = \cdots$. But $N_i \supset N_{i+1} \supset \cdots$, so $N_i = N_{i+1} = \cdots$. Thus M is Artinian.

Finally, suppose $m_1, \dots, m_r$ generate M, say $m_i = n_i/p^{e_i}$. Set $e := \max e_i$. Then $1/p^e$ generates M, a contradiction since $1/p^{e+1} \in M$. Thus M is not finitely generated, and so not Noetherian. □

Exercise **(16.24)**. — Let R be an Artinian ring. Prove that R is a field if it is a domain. Deduce that in general every prime ideal $\mathfrak{p}$ of R is maximal.

Answer: Take any nonzero element $x \in R$, and consider the chain of ideals $\langle x \rangle \supset \langle x^2 \rangle \supset \cdots$. Since R is Artinian, the chain stabilizes; so $\langle x^e \rangle = \langle x^{e+1} \rangle$ for some e. Hence $x^e = ax^{e+1}$ for some $a \in R$. If R is a domain, then we can cancel to get $1 = ax$; thus R is then a field.

In general, $R/\mathfrak{p}$ is Artinian by (16.21)(2). Now, $R/\mathfrak{p}$ is also a domain by (2.9). Hence, by what we just proved, $R/\mathfrak{p}$ is a field. Thus $\mathfrak{p}$ is maximal by (2.16). □

17. Associated Primes

Exercise **(17.6)**. — Given modules $M_1, \dots, M_r$, set $M := M_1 \oplus \cdots \oplus M_r$. Prove

$$\operatorname{Ass}(M) = \operatorname{Ass}(M_1) \cup \cdots \cup \operatorname{Ass}(M_r).$$

Answer: Set $N := M_2 \oplus \cdots \oplus M_r$. Then $N,\ M_1 \subset M$. Furthermore, $M/N = M_1$. So (17.5) yields

$$\operatorname{Ass}(N),\ \operatorname{Ass}(M_1) \subset \operatorname{Ass}(M) \subset \operatorname{Ass}(N) \cup \operatorname{Ass}(M_1).$$

So $\operatorname{Ass}(M) = \operatorname{Ass}(N) \cup \operatorname{Ass}(M_1)$. The assertion follows by induction on r. □

Exercise **(17.7)**. — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}$. Find $\operatorname{Ass}(M)$ and find two submodules $L, N \subset M$ with $L + N = M$ but $\operatorname{Ass}(L) \cup \operatorname{Ass}(N) \subsetneqq \operatorname{Ass}(M)$.

Answer: First, we have $\operatorname{Ass}(M) = \{\langle 0 \rangle, \langle 2 \rangle\}$ by (17.6) and (17.4)(2). Next, take $L := R \cdot (1,1)$ and $N := R \cdot (0,1)$. Then the canonical maps $\mathbb{Z} \to L$ and $\mathbb{Z} \to N$ are isomorphisms. Hence both $\operatorname{Ass}(L)$ and $\operatorname{Ass}(N)$ are $\{\langle 0 \rangle\}$ by (17.4)(2). Finally, $L + N = M$ because $(a,b) = a \cdot (1,1) + (b-a) \cdot (0,1)$. □

Exercise **(17.10)**. — Let R be a ring, and suppose $R_\mathfrak{p}$ is a domain for every prime $\mathfrak{p}$. Prove every associated prime of R is minimal.

Answer: Let $\mathfrak{p} \in \operatorname{Ass}(R)$. Then $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}(R_\mathfrak{p})$ by (17.9). By hypothesis, $R_\mathfrak{p}$ is a domain. So $\mathfrak{p}R_\mathfrak{p} = \langle 0 \rangle$ by (17.4). Hence $\mathfrak{p}$ is a minimal prime of R by (11.16)(2).

Alternatively, say $\mathfrak{p} = \operatorname{Ann}(x)$ with $x \in R$. Then $x/1 \ne 0$ in $R_\mathfrak{p}$; otherwise, there would be some $s \in R - \mathfrak{p}$ such that $sx = 0$, contradicting $\mathfrak{p} = \operatorname{Ann}(x)$. However, for any $y \in \mathfrak{p}$, we have $xy/1 = 0$ in $R_\mathfrak{p}$. Since $R_\mathfrak{p}$ is a domain and since $x/1 \ne 0$, we must have $y/1 = 0$ in $R_\mathfrak{p}$. So there exists some $t \in R - \mathfrak{p}$ such that $ty = 0$. Now, $\mathfrak{p} \supset \mathfrak{q}$ for some minimal prime $\mathfrak{q}$ by (3.11). Suppose $\mathfrak{p} \ne \mathfrak{q}$. Then there is some $y \in \mathfrak{p} - \mathfrak{q}$. So there exists some $t \in R - \mathfrak{p}$ such that $ty = 0 \in \mathfrak{q}$, contradicting the primeness of $\mathfrak{q}$. Thus $\mathfrak{p} = \mathfrak{q}$; that is, $\mathfrak{p}$ is minimal. □

Exercise **(17.15)**. — Let R be a Noetherian ring, M a module, N a submodule, $x \in R$. Show that, if $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Ass}(M/N)$, then $xM \cap N = xN$.

Answer: Trivially, $xN \subset xM \bigcap N$. Conversely, take $m \in M$ with $xm \in N$. Let m' be the residue of m in M/N. Then $xm' = 0$. By (17.14), $x \notin \text{z.div}(M/N)$. So $m' = 0$. So $m \in N$. So $xm \in xN$. Thus $xM \bigcap N \subset xN$, as desired. □

Exercise **(17.21)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Prove the primes minimal containing $\mathfrak{a}$ are associated to $\mathfrak{a}$. Prove such primes are finite in number.

Answer: Since $\mathfrak{a} = \operatorname{Ann}(R/\mathfrak{a})$, the primes in question are the primes minimal in $\operatorname{Supp}(R/\mathfrak{a})$ by (13.5)(3). So they are associated to $\mathfrak{a}$ by (17.17), and they are finite in number by (17.20). □

Exercise **(17.22)**. — Take $R := \mathbb{Z}$ and $M := Z$ in (17.19). Determine when a chain $0 \subset M_1 \subsetneqq M$ is acceptable, and show that then $\mathfrak{p}_2 \notin \operatorname{Ass}(M)$.

Answer: If the chain is acceptable, then $M_1 \neq 0$ as $M_1/0 \simeq R/\mathfrak{p}_1$, and M_1 is a prime ideal as $M_1 = \operatorname{Ann}(M/M_1) = \mathfrak{p}_2$. Conversely, the chain is acceptable if M_1 is a nonzero prime ideal $\mathfrak{p}$, as then $M_1/0 \simeq R/0$ and $M/M_1 \simeq R/\mathfrak{p}$.

Finally, $\operatorname{Ass}(M) = 0$ by (17.4). Further, as just observed, given any acceptable chain, $\mathfrak{p}_2 = M_1 \neq 0$. So $\mathfrak{p}_2 \notin \operatorname{Ass}(M)$. □

Exercise **(17.23)**. — Take $R := \mathbb{Z}$ and $M := Z/\langle 12\rangle$ in (17.19). Find all three acceptable chains, and show that, in each case, $\{\mathfrak{p}_i\} = \operatorname{Ass}(M)$.

Answer: An acceptable chain in M corresponds to chain

$$\langle 12\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \subset \langle a_n\rangle = \mathbb{Z}.$$

Here $\langle a_1\rangle/\langle 12\rangle \simeq \mathbb{Z}/\langle p_1\rangle$ with p_1 prime. So $a_1p_1 = 12$. Hence the possibilities are $p_1 = 2$, $a_1 = 6$ and $p_1 = 3$, $a_1 = 4$. Further, $\langle a_2\rangle/\langle a_1\rangle \simeq \mathbb{Z}/\langle p_2\rangle$ with p_2 prime. So $a_2p_2 = a_1$. Hence, if $a_1 = 6$, then the possibilities are $p_2 = 2$, $a_2 = 3$ and $p_2 = 3$, $a_2 = 2$; if $a_1 = 4$, then the only possibility is $p_2 = 2$ and $a_2 = 2$. In each case, a_2 is prime; hence, $n = 3$, and these three chains are the only possibilities. Conversely, each of these three possibilities, clearly, does arise.

In each case, $\{\mathfrak{p}_i\} = \{\langle 2\rangle, \langle 3\rangle\}$. Hence (17.19.1) yields $\operatorname{Ass}(M) \subset \{\langle 2\rangle, \langle 3\rangle\}$. For any M, if $0 \subset M_1 \subset \cdots \subset M$ is an acceptable chain, then (17.5) and (17.4)(2) yield $\operatorname{Ass}(M) \supset \operatorname{Ass}(M_1) = \{\mathfrak{p}_1\}$. Here, there's one chain with $\mathfrak{p}_1 = \langle 2\rangle$ and another with $\mathfrak{p}_1 = \langle 3\rangle$; hence, $\operatorname{Ass}(M) \supset \{\langle 2\rangle, \langle 3\rangle\}$. Thus $\operatorname{Ass}(M) = \{\langle 2\rangle, \langle 3\rangle\}$. □

18. Primary Decomposition

Exercise **(18.5)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Consider the following submodule of M:

$$\Gamma_{\mathfrak{a}}(M) := \bigcup_{n\geq 1}\{m \in M \mid \mathfrak{a}^n m = 0 \text{ for some } n \geq 1\}.$$

(1) For any decomposition $0 = \bigcap Q_i$ with Q_i $\mathfrak{p}_i$-primary, show $\Gamma_{\mathfrak{a}}(M) = \bigcap_{\mathfrak{a}\not\subset\mathfrak{p}_i} Q_i$.
(2) Show $\Gamma_{\mathfrak{a}}(M)$ is the set of all $m \in M$ such that $m/1 \in M_{\mathfrak{p}}$ vanishes for every prime $\mathfrak{p}$ with $\mathfrak{a} \not\subset \mathfrak{p}$. (Thus $\Gamma_{\mathfrak{a}}(M)$ is the set of all m whose support lies in $\mathbf{V}(\mathfrak{a})$.)

Answer: For (1), given $m \in \Gamma_{\mathfrak{a}}(M)$, say $\mathfrak{a}^n m = 0$. Given i with $\mathfrak{a} \not\subset \mathfrak{p}_i$, take $a \in \mathfrak{a} - \mathfrak{p}_i$. Then $a^n m = 0 \in Q_i$. Hence $m \in Q_i$ by (18.4). Thus $m \in \bigcap_{\mathfrak{a} \not\subset \mathfrak{p}_i} Q_i$.

Conversely, given $m \in \bigcap_{\mathfrak{a} \not\subset \mathfrak{p}_i} Q_i$, take any j with $\mathfrak{a} \subset \mathfrak{p}_j$. Now, $\mathfrak{p}_j = \operatorname{nil}(M/Q_j)$ by (18.3). So there is n_j with $\mathfrak{a}^{n_j} m \in Q_j$. Set $n := \max\{n_j\}$. Then $a^n m \in Q_i$ for all i, if $\mathfrak{a} \subset \mathfrak{p}_i$ or not. Hence $a^n m \in \bigcap Q_i = 0$. Thus $m \in \Gamma_{\mathfrak{a}}(M)$.

For (2), given $m \in \Gamma_{\mathfrak{a}}(M)$, say $\mathfrak{a}^n m = 0$. Given a prime $\mathfrak{p}$ with $\mathfrak{a} \not\subset \mathfrak{p}$, take $a \in \mathfrak{a} - \mathfrak{p}$. Then $a^n m = 0$ and $a^n \notin \mathfrak{p}$. So $m/1 \in M_{\mathfrak{p}}$ vanishes.

Conversely, given an $m \in M$ such that $m/1 \in M_{\mathfrak{p}}$ vanishes for every prime $\mathfrak{p}$ with $\mathfrak{a} \not\subset \mathfrak{p}$, consider a decomposition $0 = \bigcap Q_i$ with Q_i $\mathfrak{p}_i$-primary; one exists by (18.21). By (1), it suffices to show $m \in Q_i$ if $\mathfrak{a} \not\subset \mathfrak{p}_i$. But $m/1 \in M_{\mathfrak{p}_i}$ vanishes. So there's an $a \in R - \mathfrak{p}_i$ with $am = 0 \in Q_i$. So (18.4) yields $m \in Q_i$, as desired. □

Exercise **(18.7)**. — Let R be a ring, and $\mathfrak{p} = \langle p \rangle$ a principal prime generated by a nonzerodivisor p. Show every positive power $\mathfrak{p}^n$ is $\mathfrak{p}$-primary, and conversely, if R is Noetherian, then every $\mathfrak{p}$-primary ideal $\mathfrak{q}$ is equal to some power $\mathfrak{p}^n$.

Answer: Let's proceed by induction. Form the exact sequence

$$0 \to \mathfrak{p}^n/\mathfrak{p}^{n+1} \to R/\mathfrak{p}^{n+1} \to R/\mathfrak{p}^n \to 0.$$

Consider the map $R \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$ given by $x \mapsto xp^n$. It is surjective, and its kernel is $\mathfrak{p}$ as p is a nonzerodivisor. Hence $R/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^n/\mathfrak{p}^{n+1}$. But $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ by (17.4)(2). Hence (17.5) yields $\operatorname{Ass}(R/\mathfrak{p}^n) = \{\mathfrak{p}\}$ for every $n \geq 1$, as desired.

Conversely, $\mathfrak{p} = \sqrt{\mathfrak{q}}$ by (18.6). So $p^n \in \mathfrak{q}$ for some n; take n minimal. Then $\mathfrak{p}^n \subset \mathfrak{q}$. Suppose there is an $x \in \mathfrak{q} - \mathfrak{p}^n$. Say $x = yp^m$ for some y and $m \geq 0$. Then $m < n$ as $x \notin \mathfrak{p}^n$. Take m maximal. Now, $p^m \notin \mathfrak{q}$ as n is minimal. So (18.6) yields $y \in \mathfrak{q} \subset \mathfrak{p}$. Hence $y = zp$ for some z. Then $x = zp^{m+1}$, contradicting the maximality of m. Thus $\mathfrak{q} = \mathfrak{p}^n$. □

Exercise **(18.8)**. — Let k be a field, and $k[X, Y]$ the polynomial ring. Set $\mathfrak{a} := \langle X^2, XY \rangle$. Show $\mathfrak{a}$ is not primary, but $\sqrt{\mathfrak{a}}$ is prime. Show $\mathfrak{a}$ satisfies this condition: $ab \in \mathfrak{a}$ implies $a^2 \in \mathfrak{a}$ or $b^2 \in \mathfrak{a}$.

Answer: First, $\langle X \rangle$ is prime by (2.10). But $\langle X^2 \rangle \subset \mathfrak{a} \subset \langle X \rangle$. Hence, $\sqrt{\mathfrak{a}} = \langle X \rangle$ by (3.20). On the other hand, $XY \in \mathfrak{a}$, but $X \notin \mathfrak{a}$ and $Y \notin \sqrt{\mathfrak{a}}$; thus $\mathfrak{a}$ is not primary by (18.6). If $ab \in \mathfrak{a}$, then $X \mid a$ or $X \mid b$, so $a^2 \in \mathfrak{a}$ or $b^2 \in \mathfrak{a}$. □

Exercise **(18.9)**. — Let $\varphi\colon R \to R'$ be a homomorphism of Noetherian rings, and $\mathfrak{q} \subset R'$ a $\mathfrak{p}$-primary ideal. Show that $\varphi^{-1}\mathfrak{q} \subset R$ is $\varphi^{-1}\mathfrak{p}$-primary. Show that the converse holds if φ is surjective.

Answer: Let $xy \in \varphi^{-1}\mathfrak{q}$, but $x \notin \varphi^{-1}\mathfrak{q}$. Then $\varphi(x)\varphi(y) \in \mathfrak{q}$, but $\varphi(x) \notin \mathfrak{q}$. So $\varphi(y)^n \in \mathfrak{q}$ for some $n \geq 1$ by (18.6). Hence, $y^n \in \varphi^{-1}\mathfrak{q}$. So $\varphi^{-1}\mathfrak{q}$ is primary by (18.6). Its radical is $\varphi^{-1}\mathfrak{p}$ as $\mathfrak{p} = \sqrt{\mathfrak{q}}$, and taking the radical commutes with taking the inverse image by (3.21). The converse can be proved similarly. □

Exercise **(18.17)**. — Let k be a field, $R := k[X, Y, Z]$ be the polynomial ring. Set $\mathfrak{a} := \langle XY, X - YZ \rangle$, set $\mathfrak{q}_1 := \langle X, Z \rangle$ and set $\mathfrak{q}_2 := \langle Y^2, X - YZ \rangle$. Show that $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ holds and that this expression is an irredundant primary decomposition.

Answer: First, $XY = Y(X - YZ) + Y^2Z \in \mathfrak{q}_2$. Hence $\mathfrak{a} \subset \mathfrak{q}_1 \cap \mathfrak{q}_2$. Conversely, take $F \in \mathfrak{q}_1 \cap \mathfrak{q}_2$. Then $F \in \mathfrak{q}_2$, so $F = GY^2 + H(X - YZ)$ with $G, H \in R$. But $F \in \mathfrak{q}_1$, so $G \in \mathfrak{q}_1$; say $G = AX + BZ$ with $A, B \in R$. Then

$$F = (AY + B)XY + (H - BY)(X - ZY) \in \mathfrak{a}.$$

Thus $\mathfrak{a} \supset \mathfrak{q}_1 \cap \mathfrak{q}_2$. Thus $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ holds.

Finally, $\mathfrak{q}_1$ is prime by (2.10). Now, using (18.9), let's show $\mathfrak{q}_2$ is $\langle X, Y\rangle$-primary. Form $\varphi\colon k[X, Y, Z] \to k[Y, Z]$ with $\varphi(X) := YZ$. Clearly, $\mathfrak{q}_2 = \varphi^{-1}\langle Y^2\rangle$ and $\langle X, Y\rangle = \varphi^{-1}\langle Y\rangle$; also, $\langle Y^2\rangle$ is $\langle Y\rangle$-primary by (18.2). Thus $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ is a primary decomposition. It is irredundant as $\mathfrak{q}_1$ and $\langle X, Y\rangle$ are distinct. □

Exercise **(18.18)**. — Let $R := R' \times R''$ be a product of two domains. Find an irredundant primary decomposition of $\langle 0\rangle$.

Answer: Set $\mathfrak{p}' := \langle 0\rangle \times R''$ and $\mathfrak{p}'' := R'' \times \langle 0\rangle$. Then $\mathfrak{p}'$ and $\mathfrak{p}''$ are prime by (2.11), so primary by (17.4)(2). Obviously, $\langle 0\rangle = \mathfrak{p}' \cap \mathfrak{p}''$. Thus this representation is a primary decomposition; it is irredundant as neither $\mathfrak{p}'$ nor $\mathfrak{p}''$ can be discarded. □

Exercise **(18.25)**. — Let R be a Noetherian ring, M a finitely generated module, N a submodule. Prove $N = \bigcap_{\mathfrak{p}\in \mathrm{Ass}(M/N)} \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}})$.

Answer: Clearly $N \subset \bigcap \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}})$. To prove $N \supset \bigcap \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}})$, use (18.21): take a primary decomposition $N = \bigcap Q_i$ with Q_i is $\mathfrak{p}_i$-primary. By (18.20), then $\{\mathfrak{p}_i\} = \mathrm{Ass}(M/N)$. Further, (18.22) yields $\varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i}) \subset Q_i$ for each i (note: equality need not hold). Hence $\bigcap \varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i}) \subset \bigcap Q_i = N$, as desired. □

Exercise **(18.27)**. — Let R be a Noetherian ring, $\mathfrak{m} \subset \mathrm{rad}(R)$ an ideal, M a finitely generated module, and M' a submodule. Considering M/N, show that

$$M' = \bigcap_{n\geq 0} (\mathfrak{m}^n M + M').$$

Answer: Set $N := \bigcap_{n\geq 0} \mathfrak{m}^n(M/M')$. Then by (18.26), there is $x \in \mathfrak{m}$ such that $(1 + x)N = 0$. By (3.2), $1 + x$ is a unit since $\mathfrak{m} \subset \mathrm{rad}(R)$. Therefore, $N = (1 + x^{-1})(1 + x)N = \langle 0\rangle$. However, $\mathfrak{m}^n(M/M') = (\mathfrak{m}^n M + M')/M'$. Thus $\bigcap(\mathfrak{m}^n M + M')\big/M' = 0$, as desired. □

19. Length

Exercise **(19.2)**. — Let R be a ring, M a module. Prove these statements:

(1) If M is simple, then any nonzero element $m \in M$ generates M.
(2) M is simple if and only if $M \simeq R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and if so, then $\mathfrak{m} = \mathrm{Ann}(M)$.
(3) If M has finite length, then M is finitely generated.

Answer: Obviously, Rm is a nonzero submodule. So it is equal to M, because M is simple. Thus (1) holds.

Assume M is simple. Then M is cyclic by (1). So $M \simeq R/\mathfrak{m}$ for $\mathfrak{m} := \mathrm{Ann}(M)$ by (4.7). Since M is simple, $\mathfrak{m}$ is maximal owing to the bijective correspondence of (1.7). By the same token, if, conversely, $M \simeq R/\mathfrak{m}$ with $\mathfrak{m}$ maximal, then M is simple. Thus (2) holds.

Assume $\ell(M) < \infty$. Let $M = M_0 \supset M_1 \supset \cdots \supset M_m = 0$ be a composition series. If $m = 0$, then $M = 0$. Assume $m \geq 1$. Then M_1 has a composition series of length $m - 1$. So, by induction on m, we may assume M_1 is finitely generated. Further, M/M_1 is simple, so finitely generated by (1). Hence M is finitely generated by (16.14)(1). Thus (3) holds. □

Exercise **(19.4)**. — Let R be a Noetherian ring, M a finitely generated module. Prove that the following conditions are equivalent:

(1) M has finite length.
(2) $\mathrm{Supp}(M)$ consists entirely of maximal ideals.
(3) $\mathrm{Ass}(M)$ consists entirely of maximal ideals.

Prove that, if the conditions hold, then $\mathrm{Ass}(M)$ and $\mathrm{Supp}(M)$ are equal and finite.

Answer: If (1) holds, then (2) holds owing to (19.3). If (2) holds, then (1) holds owing to (17.19) and (19.2)(2). Finally, (17.16) and (17.20) imply that (2) and (3) are equivalent and that the last assertion holds. □

Exercise **(19.7)**. — Let k be a field, and R a finitely generated k-algebra. Prove that R is Artinian if and only if R is a finite-dimensional k-vector space.

Answer: Since k is Noetherian by (16.1) and since R is a finitely generated k-algebra, R is Noetherian by (16.10). Assume R is Artinian. Then $\ell(R) < \infty$ by (19.5). So R has a composition series. The successive quotients are isomorphic to residue class fields by (19.2)(2). These fields are finitely generated k-algebras, since R is so. Hence these fields are finite extension fields of k by the Weak Nullstellensatz. Thus R is a finite-dimensional k-vector space. The converse holds by (16.22). □

Exercise **(19.9)**. — Let k be a field, R a local k-algebra. Assume the map from k to the residue field is bijective. Given an R-module M, prove $\ell(M) = \dim_k(M)$.

Answer: If $\ell(M) = 1$, then M is simple, and so $M \cong k$ by (19.2)(2). Thus $\dim_k(M) = 1 = \ell(M)$.

If $1 < \ell(M) < \infty$, then M has a submodule M' with $M/M' \cong k$. So Additivity of Length (19.8) yields $\ell(M') = \ell(M) - 1$, and clearly $\dim_k(M') = \dim_k(M) - 1$. Hence $\ell(M') = \dim_k(M')$ by induction. So $\ell(M) = \dim_k(M)$.

If $\ell(M) = \infty$, then for every $m \geq 1$, there exists a chain of submodules,

$$M = M_0 \supsetneqq M_1 \supsetneqq \cdots \supsetneqq M_m = 0.$$

Hence $\dim_k(M) = \infty$. □

Exercise **(19.13)**. — Let R be a ring, $\mathfrak{p}$ a prime ideal, and R' a module-finite R-algebra. Show that R' has only finitely many primes $\mathfrak{p}'$ over $\mathfrak{p}$, as follows: reduce to the case that R is a field by localizing at $\mathfrak{p}$ and passing to the residue rings.

Answer: First note that, if $\mathfrak{p}' \subset R'$ is a prime lying over $\mathfrak{p}$, then $\mathfrak{p}'R'_{\mathfrak{p}} \subset R'_{\mathfrak{p}}$ is a prime lying over the maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. Hence, by (11.16)(2), it suffices to show that $R'_{\mathfrak{p}}$ has only finitely many such primes. Note also that $R'_{\mathfrak{p}}$ is module-finite over $R_{\mathfrak{p}}$. Hence we may replace R and R' by $R_{\mathfrak{p}}$ and $R'_{\mathfrak{p}}$, and thus assume that $\mathfrak{p}$ is the unique maximal ideal of R. Similarly, we may replace R and R' by $R/\mathfrak{p}$ and $R'/\mathfrak{p}R'$, and thus assume that R is a field.

There are a couple of ways to finish. First, R' is now Artinian by (19.12) or by (16.22); hence, R' has only finitely many primes by (19.10). Alternatively, every prime is now minimal by incomparability (14.3)(2). Further, R' is Noetherian by (16.10); hence, R' has only finitely many minimal primes by (17.21). $\square$

Exercise **(19.15)**. — Let R be a Noetherian ring, and M a finitely generated module. Prove the equivalence of the following four conditions:

(1) M has finite length.
(2) M is annihilated by some finite product of maximal ideals $\prod \mathfrak{m}_i$.
(3) Every prime $\mathfrak{p}$ containing $\mathrm{Ann}(M)$ is maximal.
(4) $R/\mathrm{Ann}(M)$ is Artinian.

Answer: Assume (1) holds. Let $M = M_0 \supset \cdots \supset M_m = 0$ be a composition series, and set $\mathfrak{m}_i := \mathrm{Ann}(M_{i-1}/M_i)$. Then $\mathfrak{m}_i$ is maximal by (19.2)(2). Further, $\mathfrak{m}_i M_{i-1} \subset M_i$. Hence $\mathfrak{m}_i \cdots \mathfrak{m}_1 M_0 \subset M_i$. Thus (2) holds.

If (2) holds, then (3) does too. Indeed, if $\mathfrak{p} \supset \mathrm{Ann}(M) \supset \prod \mathfrak{m}_i$, then $\mathfrak{p} \supset \mathfrak{m}_i$ for some i by (2.2) as $\mathfrak{p}$ is prime, and so $\mathfrak{p} = \mathfrak{m}_i$ as $\mathfrak{m}_i$ is maximal.

Assume (3) holds. Then $\dim(R/\mathrm{Ann}(M)) = 0$. But, by (16.7), any quotient of R is Noetherian. Hence (19.10) yields (4).

If (4) holds, then (19.11) yields (1), because M is a finitely generated $R/\mathrm{Ann}(M)$-module owing to (4.5). $\square$

20. Hilbert Functions

Exercise **(20.5)**. — Let k be a field, $k[X, Y]$ the polynomial ring. Show $\langle X, Y^2\rangle$ and $\langle X^2, Y^2\rangle$ have different Hilbert Series, but the same Hilbert Polynomial.

Answer: Set $\mathfrak{m} := \langle X, Y\rangle$ and $\mathfrak{a} := \langle X, Y^2\rangle$ and $\mathfrak{b} := \langle X^2, Y^2\rangle$. They are graded by degree. So $\ell(\mathfrak{a}_1) = 1$, and $\ell(\mathfrak{a}_n) = \ell(\mathfrak{m}_n)$ for all $n \ge 2$. Further, $\ell(\mathfrak{b}_1) = 0$, $\ell(\mathfrak{b}_2) = 2$, and $\ell(\mathfrak{b}_n) = \ell(\mathfrak{m}_n)$ for $n \ge 3$. Thus the three ideals have the same Hilbert Polynomial, namely $h(n) = n + 1$, but different Hilbert Series. $\square$

Exercise **(20.6)**. — Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus M_n$ a graded R-module. Let $N = \bigoplus N_n$ be a *homogeneous submodule*; that is, $N_n = N \cap M_n$. Assume R_0 is Artinian, R is a finitely generated R_0-algebra, and M is a finitely generated R-module. Set

$$N' := \{\, m \in M \mid \text{there is } k_0 \text{ such that } R_k m \in N \text{ for all } k \ge k_0 \,\}.$$

(1) Prove that N' is a homogeneous submodule of M with the same Hilbert Polynomial as N, and that N' is the largest such submodule.

(2) Let $N = \bigcap Q_i$ be a decomposition with Q_i $\mathfrak{p}_i$-primary. Set $R_+ := \bigoplus_{n>0} R_n$. Prove that $N' = \bigcap_{\mathfrak{p}_i \not\supset R_+} Q_i$.

Answer: Given $m = \sum m_i \in N'$, say $R_k m \subset N$. Then $R_k m_i \subset N$ since N is homogeneous. Hence $m_i \in N'$. Thus N' is homogeneous.

By (19.10) and (16.10), R is Noetherian. So N' is finitely generated by (16.17). Let $n_1, \ldots, n_r$ be homogeneous generators of N' with $n_i \in N_{k_i}$; set $k' := \max\{k_i\}$. There is k such that $R_k n_i \in N$ for all i. Given $\ell \ge k + k'$, take $n \in N'_\ell$, and write $n = \sum y_i n_i$ with $y_i \in R_{\ell - k_i}$. Then $y_i n_i \in N_\ell$ for all i. So $n \in N_\ell$. Thus $N'_\ell = N_\ell$ for all $\ell \ge k + k'$. Thus N and N' have the same Hilbert polynomial.

Say $N'' \supset N$, and both have the same Hilbert Polynomial. Then there is k_0 with $\ell(N''_k) = \ell(N_k)$ for all $k \ge k_0$. So $N''_k = N_k$ for all $k \ge k_0$. So, if $n \in N''$, then

$R_k n \in N$ for all $k \ge k_0$. Thus $N'' \subset N'$. Thus (1) holds.

To prove (2), note $0 = \bigcap(Q_i/N)$ in M/N. By (18.5),
$$\Gamma_{R_+}(M/N) = \bigcap_{\mathfrak{p}_i \not\supset R_+} (Q_i/N).$$
But clearly $\Gamma_{R_+}(M/N) = N'/N$. Thus $N' = \bigcap_{\mathfrak{p}_i \not\supset R_+} Q_i$. □

Exercise **(20.9)**. — Let k be a field, $P := k[X, Y, Z]$ the polynomial ring in three variables, $f \in P$ a homogeneous polynomial of degree $d \ge 1$. Set $R := P/\langle f\rangle$. Find the coefficients of the Hilbert Polynomial $h(R, n)$ explicitly in terms of d.

Answer: Clearly, the following sequence is exact:
$$0 \to P(-d) \xrightarrow{\mu_f} P \to R \to 0.$$
Hence, Additivity of Length, (19.8), yields $h(R, n) = h(P, n) - h(P(-d), n)$. But $P(-d)_n = P(n-d)$, so $h(P(-d), n) = h(P, n-d)$. Therefore, (20.4) yields
$$h(R, n) = \tbinom{2+n}{2} - \tbinom{2-d+n}{2} = dn - (d-3)d/2. \qquad \square$$

Exercise **(20.10)**. — Under the conditions of (20.8), assume there is a homogeneous nonzerodivisor $f \in R$ with $M_f = 0$. Prove $\deg\big(h(R, n)\big) > \deg\big(h(M, n)\big)$; start with the case $M := R/\langle f^k\rangle$.

Answer: Suppose $M := R/\langle f^k\rangle$. Set $c := k \deg(f)$. Form the exact sequence $0 \to R(-c) \xrightarrow{\mu} R \to M \to 0$ where μ is multiplication by f^k. Then Additivity of Length (19.8) yields $h(M, n) = h(R, n) - h(R, n-c)$. But
$$h(R, n) = \tfrac{e(1)}{(d-1)!} n^{d-1} + \cdots \quad \text{and} \quad h(R, n-c) = \tfrac{e(1)}{(d-1)!}(n-c)^{d-1} + \cdots .$$
by (20.8). Thus $\deg\big(h(R, n)\big) > \deg\big(h(M, n)\big)$.

In the general case, there is k with $f^k M = 0$ by (12.7). Set $M' := R/\langle f^k\rangle$. Then generators $m_i \in M_{c_i}$ for $1 \le i \le r$ yield a surjection $\bigoplus_i M'(-c_i) \twoheadrightarrow M$. Hence $\sum_i \ell(M'_{n-c_i}) \ge \ell(M_n)$ for all n. But $\deg\big(h(M'(-c_i), n)\big) = \deg\big(h(M', n)\big)$. Hence $\deg\big(h(M', n)\big) \ge \deg\big(h(M, n)\big)$. But $\deg\big(h(R, n)\big) > \deg\big(h(M', n)\big)$ by the first case. Thus $\deg\big(h(R, n)\big) > \deg\big(h(M, n)\big)$. □

Exercise **(20.15)**. — Let R be a Noetherian ring, $\mathfrak{q}$ an ideal, and M a finitely generated module. Assume $\ell(M/\mathfrak{q}M) < \infty$. Set $\mathfrak{m} := \sqrt{\mathfrak{q}}$. Show
$$\deg p_{\mathfrak{m}}(M, n) = \deg p_{\mathfrak{q}}(M, n).$$

Answer: There is an m such that $\mathfrak{m} \supset \mathfrak{q} \supset \mathfrak{m}^m$ by (3.19). Hence
$$\mathfrak{m}^n M \supset \mathfrak{q}^n M \supset \mathfrak{m}^{mn} M$$
for all $n \ge 0$. Dividing into M and extracting lengths yields
$$\ell(M/\mathfrak{m}^n M) \le \ell(M/\mathfrak{q}^n M) \le \ell(M/\mathfrak{m}^{mn} M).$$
Therefore, for large n, we get
$$p_{\mathfrak{m}}(M, n) \le p_{\mathfrak{q}}(M, n) \le p_{\mathfrak{m}}(M, nm).$$
The two extremes are polynomials in n with the same degree, say d, (but not the same leading coefficient). Dividing by n^d and letting $n \to \infty$, we conclude that the polynomial $p_{\mathfrak{q}}(M, n)$ also has degree d. □

Exercise **(20.19)**. — Derive the Krull Intersection Theorem, (18.26), from the Artin–Rees Lemma, (20.18).

Answer: In the notation of (18.26), we must prove that $N = \mathfrak{a}N$. So apply the Artin–Rees Lemma to N and the $\mathfrak{a}$-adic filtration of M; we get an m such that $\mathfrak{a}(N \cap \mathfrak{a}^m M) = N \cap \mathfrak{a}^{m+1} M$. But $N \cap \mathfrak{a}^n M = N$ for all $n \geq 0$. Thus $N = \mathfrak{a}N$. □

20. Appendix: Homogeneity

Exercise **(20.4)**. — Let R be a graded ring, $\mathfrak{a}$ a homogeneous ideal, and M a graded module. Prove that $\sqrt{\mathfrak{a}}$ and $\mathrm{Ann}(M)$ and $\mathrm{nil}(M)$ are homogeneous.

Answer: Take $x = \sum_{i \geq r}^{r+n} x_i \in R$ with the x_i the homogenous components.

First, suppose $x \in \sqrt{\mathfrak{a}}$. Say $x^k \in \mathfrak{a}$. Either x_r^k vanishes or it is the initial component of x^k. But $\mathfrak{a}$ is homogeneous. So $x_r^k \in \mathfrak{a}$. So $x_r \in \sqrt{\mathfrak{a}}$. So $x - x_r \in \sqrt{\mathfrak{a}}$ by (3.18). So all the x_i are in $\sqrt{\mathfrak{a}}$ by induction on n. Thus $\sqrt{\mathfrak{a}}$ is homogenous.

Second, suppose $x \in \mathrm{Ann}(M)$. Let $m \in M$. Then $0 = xm = \sum x_i m$. If m is homogeneous, then $x_i m = 0$ for all i, since M is graded. But M has a set of homogeneous generators. Thus $x_i \in \mathrm{Ann}(M)$ for all i, as desired.

Finally, $\mathrm{nil}(M)$ is homogeneous, as $\mathrm{nil}(M) = \sqrt{\mathrm{Ann}(M)}$ by (13.6). □

Exercise **(20.5)**. — Let R be a Noetherian graded ring, M a finitely generated graded module, Q a submodule. Let $Q^* \subset Q$ be the submodule generated by the homogeneous elements of Q. Assume Q is primary. Then Q^* is primary too.

Answer: Let $x \in R$ and $m \in M$ be homogeneous with $xm \in Q^*$. Assume $x \notin \mathrm{nil}(M/Q^*)$. Then, given $\ell \geq 1$, there is $m' \in M$ with $x^\ell m' \notin Q^*$. So m' has a homogeneous component m'' with $x^\ell m'' \notin Q^*$. Then $x^\ell m'' \notin Q$ by definition of Q^*. Thus $x \notin \mathrm{nil}(M/Q)$. Since Q is primary, $m \in Q$ by (18.4). Since m is homogeneous, $m \in Q^*$. Thus Q^* is primary by (20.3). □

Exercise **(20.9)**. — Under the conditions of (20.8), assume that R is a domain and that its integral closure $\overline{R}$ in $\mathrm{Frac}(R)$ is a finitely generated R-module.

(1) Prove that there is a homogeneous $f \in R$ with $R_f = \overline{R}_f$.

(2) Prove that the Hilbert Polynomials of R and $\overline{R}$ have the same degree and same leading coefficient.

Answer: Let $x_1, \ldots, x_r$ be homogeneous generators of $\overline{R}$ as an R-module. Write $x_i = a_i/b_i$ with $a_i, b_i \in R$ homogeneous. Set $f := \prod b_i$. Then $f x_i \in R$ for each i. So $\overline{R}_f = R_f$. Thus (1) holds.

Consider the short exact sequence $0 \to R \to \overline{R} \to \overline{R}/R \to 0$. Then $(\overline{R}/R)_f = 0$ by (12.16). So $\deg\big(h(\overline{R}/R, n)\big) < \deg\big(h(\overline{R}, n)\big)$ by (20.10) and (1). But

$$h(\overline{R}, n) = h(R, n) + h(\overline{R}/R, n)$$

by (19.8) and (20.8). Thus (2) holds. □

21. Dimension

Exercise **(21.9)**. — Let R be a Noetherian ring, and $\mathfrak{p}$ be a prime minimal containing $x_1, \ldots, x_r$. Given r' with $1 \le r' \le r$, set $R' := R/\langle x_1, \ldots, x_{r'}\rangle$ and $\mathfrak{p}' := \mathfrak{p}/\langle x_1, \ldots, x_{r'}\rangle$. Assume $\mathrm{ht}(\mathfrak{p}) = r$. Prove $\mathrm{ht}(\mathfrak{p}') = r - r'$.

Answer: Let $x'_i \in R'$ be the residue of x_i. Then $\mathfrak{p}'$ is minimal containing $x'_{r'+1}, \ldots x'_r$ by (1.7) and (2.7). So $\mathrm{ht}(\mathfrak{p}') \le r - r'$ by (21.8).

On the other hand, $R'_{\mathfrak{p}'} = R'_{\mathfrak{p}}$ by (11.19), and $R'_{\mathfrak{p}} = R_{\mathfrak{p}}/\langle x_1/1, \ldots, x_{r'}/1\rangle$ by (12.18) Hence $\dim(R'_{\mathfrak{p}'}) \ge \dim(R_{\mathfrak{p}}) - r'$ by repeated application of (21.6). So $\mathrm{ht}(\mathfrak{p}') \ge r - r'$ by (21.7.1), as required. □

Exercise **(21.11)**. — Let R be a domain. Prove that, if R is a UFD, then every height-1 prime is principal, and that the converse holds if R is Noetherian.

Answer: Let $\mathfrak{p}$ be a height-1 prime. Then there's a nonzero $x \in \mathfrak{p}$. Factor x. One prime factor p must lie in $\mathfrak{p}$ as $\mathfrak{p}$ is prime. Clearly, $\langle p\rangle$ is a prime ideal as p is a prime element. But $\langle p\rangle \subset \mathfrak{p}$ and $\mathrm{ht}(p) = 1$. Thus, $\langle p\rangle = \mathfrak{p}$.

Conversely, assume every height-1 prime is principal and assume R is Noetherian. To prove R is a UFD, it suffices to prove every irreducible element p is prime (see [**Artin**, Ch. 11, Sec. 2, pp. 392–396]).

Let $\mathfrak{p}$ be a prime minimal containing p. By Krull's Principal Ideal Theorem, $\mathrm{ht}(\mathfrak{p}) = 1$. So $\mathfrak{p} = \langle x\rangle$ for some x. Then x is prime by (2.6). And $p = xy$ for some y as $p \in \mathfrak{p}$. But p is irreducible. So y is a unit. Thus p is prime, as desired. □

Exercise **(21.12)**. — (1) Let A be a Noetherian local ring with a principal prime $\mathfrak{p}$ of height at least 1. Prove that A is a domain.

(2) Let k be a field, $P := k[[X]]$ the formal power series ring in one variable. Set $R := P \times P$. Prove that P is Noetherian and semilocal, and that P contains a principal prime $\mathfrak{p}$ of height 1, but that P is not a domain.

Answer: To prove (1), say $\mathfrak{p} = \langle x\rangle$, and let $\mathfrak{q} \subset \mathfrak{p}$ be a minimal prime. Take $y \in \mathfrak{q}$. Then $y = ax$ for some a. But $x \notin \mathfrak{q}$ since $\mathrm{ht}\,\mathfrak{p} \ge 1$. Hence $a \in \mathfrak{q}$. Thus $\mathfrak{q} = \mathfrak{q}x$. But x lies in the maximal ideal of the local ring A, and $\mathfrak{q}$ is finitely generated since A is Noetherian. Hence Nakayama's Lemma (10.8) yields $\mathfrak{q} = \langle 0\rangle$. Thus $\langle 0\rangle$ is prime, and so A is a domain.

Alternatively, as $a \in \mathfrak{q}$, also $a = a_1 x$ with $a_1 \in \mathfrak{q}$. Repeating yields an ascending chain of ideals $\langle a\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \cdots$. It must stabilize as A is Noetherian: there's a k such that $a_k \in \langle a_{k-1}\rangle$. Then $a_k = ba_{k-1} = ba_k x$ for some b. So $a_k(1 - bx) = 0$. But $1 - bx$ is a unit by (3.4) as A is local. So $a_k = 0$. Hence $y = 0$ and so $\mathfrak{q} = \langle 0\rangle$. Thus A is a domain.

As to (2), every nonzero ideal of P is of the form $\langle X^n\rangle$ by (3.8). Hence P is Noetherian. Thus R is Noetherian by (16.15).

The primes of R are of the form $\mathfrak{q} \times P$ or $P \times \mathfrak{q}$ where $\mathfrak{q}$ is a prime of P by (2.10). Further, $\mathfrak{m} := \langle X\rangle$ is the unique maximal ideal by (3.7). Hence R has just two maximal ideals $\mathfrak{m} \times P$ and $P \times \mathfrak{m}$. Thus R is semilocal.

Set $\mathfrak{p} := \langle (X, 1)\rangle$. Then $\mathfrak{p} = \mathfrak{m} \times P$. So $\mathfrak{p}$ is a principal prime. Further, $\mathfrak{p}$ contains just one other prime $0 \times P$. Thus $\mathrm{ht}(\mathfrak{p}) = 1$.

Finally, R is not a domain as $(1, 0) \cdot (0, 1) = 0$. □

Exercise **(21.13)**. — Let R be a finitely generated algebra over a field. Assume R is a domain of dimension r. Let $x \in R$ be neither 0 nor a unit. Set $R' := R/\langle x\rangle$. Prove that $r-1$ is the length of any chain of primes in R' of maximal length.

Answer: A chain of primes in R' of maximal length lifts to a chain of primes $\mathfrak{p}_i$ in R of maximal length with $\langle x\rangle \subseteq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d$. As x is not a unit, $d \geq 1$. As $x \neq 0$, also $\mathfrak{p}_1 \neq 0$. But R is a domain. So Krull's Principal Ideal Theorem yields $\operatorname{ht}\mathfrak{p}_1 = 1$. So $0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ is of maximal length in R. But R is a finitely generated algebra over a field. Hence $d = \dim R$ by (15.8). □

Exercise **(21.15)**. — Let A be a Noetherian local ring of dimension r. Let $\mathfrak{m}$ be the maximal ideal, and $k := A/\mathfrak{m}$ the residue class field. Prove that

$$r \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2),$$

with equality if and only if $\mathfrak{m}$ is generated by r elements.

Answer: By (21.5), $\dim(A)$ is the smallest number of generators of any parameter ideal. But $\mathfrak{m}$ is a parameter ideal, and the smallest number of generators of $\mathfrak{m}$ is $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ by (10.9)(2). The assertion follows. □

Exercise **(21.20)**. — Let A be a Noetherian local ring of dimension r, and $x_1, \dots, x_s \in A$ with $s \leq r$. Set $\mathfrak{a} := \langle x_1, \dots, x_s\rangle$ and $B := A/\mathfrak{a}$. Prove equivalent:

(1) A is regular, and there are $x_{s+1}, \dots, x_r \in A$ with $x_1, \dots, x_r$ a regular sop.
(2) B is regular of dimension $r-s$.

Answer: Assume (1). Then (21.19) yields $\dim_k(\mathfrak{n}/\mathfrak{n}^2) = r-s$ in its notation, as the x_i yield a basis of $\mathfrak{m}/\mathfrak{m}^2$. But $\dim_k(\mathfrak{n}/\mathfrak{n}^2) \geq \dim(B) \geq r-s$ by (21.15) and (21.6). Hence $\dim(B) = r-s$, and so B is regular. Thus (2) holds.

Assume (2). Then (21.19) yields $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq r$. But $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq r$ by (21.15). Hence $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = r$ and $\dim_k((\mathfrak{m}^2+\mathfrak{a})/\mathfrak{m}^2) = s$. Thus (1) holds. □

22. Completion

Exercise **(22.3)**. — In the 2-adic integers, evaluate the sum $1+2+4+8+\cdots$.

Answer: In the 2-adic integers, $1+2+4+8+\cdots = 1/(1-2) = -1$. □

Exercise **(22.4)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Prove the following three conditions are equivalent:

(1) $\kappa\colon M \to \widehat{M}$ is injective; (2) $\bigcap \mathfrak{a}^n M = \langle 0\rangle$; (3) M is separated.

Answer: Clearly, $\operatorname{Ker}(\kappa) = \bigcap \mathfrak{a}^n M$; so (1) and (2) are equivalent. Moreover, (2) and (3) were proved equivalent in (22.1). □

Exercise **(22.8)**. — Let A be a Noetherian semilocal ring, and $\mathfrak{m}_1, \dots, \mathfrak{m}_m$ all its maximal ideals. Prove that $\widehat{A} = \prod \widehat{A}_{\mathfrak{m}_i}$.

Answer: Set $\mathfrak{m} := \operatorname{rad}(R)$. Fix $n \geq 0$. Then $A/\mathfrak{m}^n$ is Noetherian of dimension 0; so it's Artinian by (19.15). Hence (19.14) yields

$$A/\mathfrak{m}^n = \prod_i (A/\mathfrak{m}^n)_{(\mathfrak{m}_i/\mathfrak{m}^n)}.$$

However, $(A/\mathfrak{m}^n)_{(\mathfrak{m}_i/\mathfrak{m}^n)}$ is equal to $(A/\mathfrak{m}^n)_{\mathfrak{m}_i}$ by (11.19), so to $A_{m_i}/\mathfrak{m}^n A_{m_i}$ by Exactness of Localization (12.16). Furthermore, $\mathfrak{m}^n = (\prod \mathfrak{m}_i)^n = \bigcap \mathfrak{m}_i^n$ by (1.12). Now, $\mathfrak{m}_i^n$ is $\mathfrak{m}_i$-primary by (18.11). Hence $\mathfrak{m}^n A_{m_i} = \mathfrak{m}_i^n A_{m_i}$ by (18.23). Therefore, $A/\mathfrak{m}^n = \prod_i (A_{\mathfrak{m}_i}/\mathfrak{m}_i^n A_{\mathfrak{m}_i})$. Taking inverse limits, we obtain the assertion, because inverse limit commutes with finite product by the construction of the limit. □

Exercise **(22.9)**. — Let R be a ring, M a module, $M = M_0 \supset M_1 \supset \cdots$ a filtration, and $N \subset M$ a submodule. Filter N by $N_n := N \cap M_n$. Assume $N \supset M_n$ for $n \geq n_0$ for some n_0. Prove $\widehat{N} \subset \widehat{M}$ and $\widehat{M}/\widehat{N} = M/N$ and $G(\widehat{M}\,) = G(M)$.

Answer: For each $n \geq n_0$, form this commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & N/M_{n+1} & \to & M/M_{n+1} & \to & M/N & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N/M_n & \longrightarrow & M/M_n & \longrightarrow & M/N & \to & 0 \end{array}$$

The left vertical map is surjective; the right is the identity. So the induced sequence

$$0 \to \widehat{N} \to \widehat{M} \to M/N \to 0$$

is exact by (22.6) and (22.7). Thus $\widehat{N} \subset \widehat{M}$ and $\widehat{M}/\widehat{N} = M/N$.

In particular, $\widehat{M}/\widehat{M}_n = M/M_n$ for each n. Therefore, $\widehat{M}_n/\widehat{M}_{n+1} = M_n/M_{n+1}$. Thus $G(\widehat{M}\,) = G(M)$. □

Exercise **(22.10)**. — (1) Let R be a ring, $\mathfrak{a}$ an ideal. If $G_{\mathfrak{a}}(R)$ is a domain, show $\widehat{R}$ is an domain. If also $\bigcap_{n\geq 0} \mathfrak{a}^n = 0$, show R is a domain.

(2) Use (1) to give an alternative proof that a regular local ring A is a domain.

Answer: Consider (1). Let $x, y \in \widehat{R}$ be nonzero. Since $\widehat{R}$ is separated there are positive integers r and s with $x \in \widehat{\mathfrak{a}}^{\,r} - \widehat{\mathfrak{a}}^{\,r+1}$ and $y \in \widehat{\mathfrak{a}}^{\,s} - \widehat{\mathfrak{a}}^{\,s+1}$. Let $x' \in G^r_{\widehat{\mathfrak{a}}}(\widehat{R}\,)$ and $y' \in G^s_{\widehat{\mathfrak{a}}}(\widehat{R}\,)$ denote the images of x and y. Then $x' \neq 0$ and $y' \neq 0$. Now, $G_{\widehat{\mathfrak{a}}}(\widehat{R}\,) = G_{\mathfrak{a}}(R)$ by (22.9). Assume $G_{\mathfrak{a}}(R)$ is a domain. Then $x'y' \neq 0$. Hence $x'y' \in G^{r+s}_{\widehat{\mathfrak{a}}}$ is the image of $xy \in \widehat{\mathfrak{a}}^{\,r+s}$. Hence $xy \neq 0$. Thus $\widehat{R}$ is a domain.

If $\bigcap_{n\geq 0} \mathfrak{a}^n = 0$, then $R \subset \widehat{R}$ by (22.4); so R is a domain if $\widehat{R}$ is. Thus (1) holds.

As to (2), denote the maximal ideal of A by $\mathfrak{m}$. Then $\bigcap_{n\geq 0} \mathfrak{m}^n = \langle 0 \rangle$ by the Krull Intersection Theorem (18.26), and $G_{\mathfrak{m}}(A)$ is a polynomial ring by (21.18), so a domain. Hence A is a domain, by (1). Thus (2) holds. □

Exercise **(22.12)**. — Let A be a semilocal ring, $\mathfrak{m}_1, \ldots, \mathfrak{m}_m$ all its maximal ideals, and set $\mathfrak{m} := \operatorname{rad}(A)$. Prove that $\widehat{A}$ is a semilocal ring, that $\widehat{\mathfrak{m}}_1, \ldots, \widehat{\mathfrak{m}}_m$ are all its maximal ideals, and that $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{A}\,)$.

Answer: First, (22.9) yields $\widehat{A}/\widehat{\mathfrak{m}} = A/\mathfrak{m}$ and $\widehat{A}/\widehat{\mathfrak{m}}_i = A/\mathfrak{m}_i$. So $\widehat{\mathfrak{m}}_i$ is maximal. By hypothesis, $\mathfrak{m} = \bigcap \mathfrak{m}_i$; so $A/\mathfrak{m} \subset \prod (A/\mathfrak{m}_i)$. Hence $\widehat{A}/\widehat{\mathfrak{m}} \subset \prod (\widehat{A}/\widehat{\mathfrak{m}}_i)$; so $\widehat{\mathfrak{m}} = \bigcap \widehat{\mathfrak{m}}_i$. So $\widehat{\mathfrak{m}} \supset \operatorname{rad}(\widehat{A}\,)$. But $\widehat{\mathfrak{m}} \subset \operatorname{rad}(\widehat{A}\,)$ by (22.2). Thus $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{A}\,)$.

Finally, let $\mathfrak{m}'$ be any maximal ideal of $\widehat{A}$. Then $\mathfrak{m}' \supset \operatorname{rad}(\widehat{A}\,) = \bigcap \widehat{\mathfrak{m}}_i$. Hence $\mathfrak{m}' \supset \widehat{\mathfrak{m}}_i$ for some i by (2.2). But $\widehat{\mathfrak{m}}_i$ is maximal. So $\mathfrak{m}' = \widehat{\mathfrak{m}}_i$. Thus $\widehat{\mathfrak{m}}_1, \ldots, \widehat{\mathfrak{m}}_m$ are all the maximal ideals of $\widehat{A}$, and so $\widehat{A}$ is semilocal. $\square$

Exercise **(22.15)**. — Let A be a Noetherian ring, $x \in A$, and $\widehat{x} \in \widehat{A}$ its image. Prove $\widehat{x}$ is a nonzerodivisor if x is. Prove the converse holds if A is semilocal.

Answer: Assume x is a nonzerodivisor. Then the multiplication map μ_x is injective on A. So by Exactness of Completion, the induced map $\widehat{\mu}_x$ is injective on $\widehat{A}$. But $\widehat{\mu}_x = \mu_{\widehat{x}}$. Thus $\widehat{x}$ is a nonzerodivisor.

Conversely, assume $\widehat{x}$ is a nonzerodivisor and A is semilocal. Then $\widehat{\mu}_x$ is injective on $\widehat{A}$. So its restriction is injective on the image of the canonical map $A \to \widehat{A}$. But this map is injective, as the completion is taken with respect to the Jacobson radical; further, $\widehat{\mu}_x$ induces μ_x. Thus x is a nonzerodivisor. $\square$

Exercise **(22.17)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Show that $M \mapsto \widehat{M}$ preserves surjections, and that $\widehat{R} \otimes M \to \widehat{M}$ is surjective if M is finitely generated.

Answer: The first part of the proof of (22.14) shows that $M \mapsto \widehat{M}$ preserves surjections. So (8.16) yields the desired surjectivity. $\square$

Exercise **(22.20)**. — Let R be a Noetherian ring, and $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Assume $\mathfrak{a} \subset \operatorname{rad}(R)$, and use the $\mathfrak{a}$-adic toplogy. Prove $\mathfrak{b}$ is principal if $\mathfrak{b}\widehat{R}$ is.

Answer: Since R is Noetherian, $\mathfrak{b}$ is finitely generated. But $\mathfrak{a} \subset \operatorname{rad}(R)$. Hence, $\mathfrak{b}$ is principal if $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ is cyclic by (10.9)(2). But $\mathfrak{b}/\mathfrak{a}\mathfrak{b} = \widehat{\mathfrak{b}}/(\mathfrak{a}\mathfrak{b})\widehat{\ }$ by (22.9), and $\widehat{\mathfrak{b}} = \mathfrak{b}\widehat{R}$ by (22.18)(2). Hence, if $\mathfrak{b}\widehat{R}$ is principal, then $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ is cyclic, as desired. $\square$

Exercise **(22.23)** (*Nakayama's Lemma for a complete ring*). — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Assume R is complete, and M separated. Show $m_1, \ldots, m_n \in M$ generate if their images in $M/\mathfrak{a}M$ generate.

Answer: Note that the images of $m_1, \ldots, m_n$ in $G(M)$ generate over $G(R)$. Therefore, $m_1, \ldots, m_n \in M$ generate over R by the proof of (22.22).

Alternatively, M is finitely generated over R and complete by the statement of (22.22). Since M is also separated, $M = \widehat{M}$. Hence M is also an $\widehat{R}$-module. Since R is complete, $\kappa_R \colon R \to \widehat{R}$ is surjective. Now, $\mathfrak{a}$ is closed by (22.1); so $\mathfrak{a}$ is complete; whence, $\kappa_{\mathfrak{a}} \colon \mathfrak{a} \to \widehat{\mathfrak{a}}$ is surjective too. Hence $\mathfrak{a}M = \widehat{\mathfrak{a}}M$. Thus $M/\mathfrak{a}M = M/\widehat{\mathfrak{a}}M$. So the m_i generate $M/\widehat{\mathfrak{a}}M$. But $\widehat{\mathfrak{a}} \subset \operatorname{rad}(\widehat{R})$ by (22.2). So by Nakayama's Lemma (10.9)(2), the m_i generate M over $\widehat{R}$, so also over R as κ_R is surjective. $\square$

Exercise **(22.27)**. — Let A be a Noetherian local ring, $\mathfrak{m}$ the maximal ideal. Prove (1) that $\widehat{A}$ is a Noetherian local ring with $\widehat{\mathfrak{m}}$ as maximal ideal, (2) that $\dim(A) = \dim(\widehat{A})$, and (3) that A is regular if and only if $\widehat{A}$ is regular.

Answer: First, $\widehat{A}$ is Noetherian by (22.25), and local with $\widehat{\mathfrak{m}}$ as maximal ideal by (22.8); thus (1) holds.

Second, $A/\mathfrak{m}^n = \widehat{A}/\widehat{\mathfrak{m}}^n$ by (22.9). So $d(A) = d(\widehat{A})$ by (20.13). Thus (2) holds by (21.4).

Third, $\mathfrak{m}/\mathfrak{m}^2 = \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}}^2$ by (22.9). So $\mathfrak{m}$ and $\widehat{\mathfrak{m}}$ have the same number of generators by (10.10). Thus (3) holds. $\square$

23. Discrete Valuation Rings

Exercise **(23.5)**. — Let R be a ring, M a module, and $x, y \in R$.

(1) Prove that, if x, y form an M-sequence, then, given any $m, n \in M$ such that $xm = yn$, there exists $p \in M$ such that $m = yp$ and $n = xp$.

(2) Prove the converse of (1) if R is local, and x, y lie in its maximal ideal $\mathfrak{m}$, and M is Noetherian.

Proof: Consider (1). Let n_1 be the residue of n in $M_1 := M/xM$. Then $yn_1 = 0$, but $y \notin \text{z.div}(M_1)$. Hence $n_1 = 0$. So there exists $p \in M$ such that $n = xp$. So $x(m - yp) = 0$. But $x \notin \text{z.div}(M)$. Thus $m = yp$.

Consider (2). Given $m \in M$ such that $xm = 0$, take $n := 0$. Then $xm = yn$; so there exists $p \in M$ such that $m = yp$ and $n = xp$. Repeat with p in place of m, obtaining $p_1 \in M$ such that $p = yp_1$ and $0 = xp_1$. Induction yields $p_i \in M$ for $i \geq 2$ such that $p_{i-1} = yp_i$ and $0 = xp_i$.

Then $Rp_1 \subset Rp_2 \subset \cdots$ is an ascending chain. It stabilizes as M is Noetherian. Say $Rp_n = Rp_{n+1}$. So $p_{n+1} = zp_n$ for some $z \in R$. Then $p_n = yp_{n+1} = yzp_n$. So $(1 - yz)p_n = 0$. But $y \in \mathfrak{m}$. So $1 - yz$ is a unit. Hence $p_n = 0$. But $m = y^{n+1}p_n$. Thus $m = 0$. Thus $x \notin \text{z.div}(M)$.

Given $n_1 \in M_1 := M/xM$ such that $yn_1 = 0$, take $n \in M$ with n_1 as residue. Then $yn = xm$ for some $m \in M$. So there exists $p \in M$ such that $m = yp$ and $n = xp$. Thus $n_1 = 0$. Thus $y \notin \text{z.div}(M_1)$. Thus x, y form an M-sequence. □

Exercise **(23.6)**. — Let R be a local ring, $\mathfrak{m}$ its maximal ideal, M a Noetherian module, $x_1, \ldots, x_n \in \mathfrak{m}$, and σ a permutation of $1, \ldots, n$. Assume $x_1, \ldots, x_n$ form an M-sequence, and prove $x_{\sigma 1}, \ldots, x_{\sigma n}$ do too; first, say σ transposes i and $i + 1$.

Proof: Say σ transposes i and $i + 1$. Set $M_j := M/\langle x_1, \ldots, x_j\rangle$. Then x_i, x_{i+1} form an M_{i-1}-sequence; so x_{i+1}, x_i do too owing to (23.5). So $x_1, \ldots, x_{i-1}, x_{i+1}, x_i$ form an M-sequence. But $M/\langle x_1, \ldots, x_{i-1}, x_{i+1}, x_i\rangle = M_{i+1}$. Hence $x_{\sigma 1}, \ldots, x_{\sigma n}$ form an M-sequence. In general, σ is a composition of transpositions of successive integers; hence, the general assertion follows. □

Exercise **(23.7)**. — Prove that a Noetherian local ring A of dimension $r \geq 1$ is regular if and only if its maximal ideal $\mathfrak{m}$ is generated by an A-sequence.

Answer: Assume A is regular. Given a regular sop $x_1, \ldots, x_r$, let's show it's an A-sequence. Set $A_1 := A/\langle x_1\rangle$. Then A_1 is regular of dimension $r - 1$ by (21.20). So $x_1 \neq 0$. But A is a domain by (21.21). So $x_1 \notin \text{z.div}(A)$. Further, if $r \geq 2$, then the residues of $x_2, \ldots, x_r$ form a regular sop of A_1; so we may assume they form an A_1-sequence by induction on r. Thus $x_1, \ldots, x_r$ is an A-sequence.

Conversely, if $\mathfrak{m}$ is generated by an A-sequence $x_1, \ldots, x_n$, then $n \leq \operatorname{depth}(A) \leq r$ by (23.3) and (23.4)(3), and $n \geq r$ by (21.15); thus $n = r$, and A is regular. □

Exercise **(23.9)**. — Let A be a DVR with fraction field K, and $f \in A$ a nonzero nonunit. Prove A is a maximal proper subring of K. Prove $\dim(A) \neq \dim(A_f)$.

Answer: Let R be a ring, $A \subsetneqq R \subset K$. Then there's an $x \in R - A$. Say $x = ut^n$ where $u \in A^\times$ and t is a uniformizing parameter. Then $n < 0$. Set $y := u^{-1}t^{-n-1}$. Then $y \in A$. So $t^{-1} = xy \in R$. Hence $wt^m \in R$ for any $w \in A^\times$ and $m \in \mathbb{Z}$. Thus $R = K$, as desired.

Since f is a nonzero nonunit, $A \subsetneqq A_f \subset K$. Hence $A_f = K$ by the above. So

$\dim(A_f) = 0$. But $\dim(A) = 1$ by (23.8). □

Exercise **(23.10)**. — Let k be a field, $P := k[X, Y]$ the polynomial ring in two variables, $f \in P$ an irreducible polynomial. Say $f = \ell(X, Y) + g(X, Y)$ with $\ell(X, Y) = aX + bY$ for $a, b \in k$ and with $g \in \langle X, Y\rangle^2$. Set $R := P/\langle f\rangle$ and $\mathfrak{p} := \langle X, Y\rangle/\langle f\rangle$. Prove that $R_\mathfrak{p}$ is a DVR if and only if $\ell \neq 0$. (Thus $R_\mathfrak{p}$ is a DVR if and only if the plane curve $C : f = 0 \subset k^2$ is nonsingular at $(0, 0)$.)

Answer: Set $A := R_\mathfrak{p}$ and $\mathfrak{m} := \mathfrak{p}A$. Then (12.18) and (12.4) yield

$$A/\mathfrak{m} = (R/\mathfrak{p})_\mathfrak{p} = k \quad \text{and} \quad \mathfrak{m}/\mathfrak{m}^2 = \mathfrak{p}/\mathfrak{p}^2.$$

First, assume $\ell \neq 0$. Now, the k-vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by the images x and y of X and Y in A. Clearly, the image of f is 0 in $\mathfrak{m}/\mathfrak{m}^2$. Also, $g \in (X, Y)^2$; so its image in $\mathfrak{m}/\mathfrak{m}^2$ is also 0. Hence, the image of ℓ is 0 in $\mathfrak{m}/\mathfrak{m}^2$; that is, x and y are linearly dependent. Now, f cannot generate $\langle X, Y\rangle$, so $\mathfrak{m} \neq 0$; hence, $\mathfrak{m}/\mathfrak{m}^2 \neq 0$ by Nakayama's Lemma, (10.8). Therefore, $\mathfrak{m}/\mathfrak{m}^2$ is 1-dimensional over k; hence, $\mathfrak{m}$ is principal by (10.9)(2). Now, since f is irreducible, A is a domain. Hence, A is a DVR by (23.8).

Conversely, assume $\ell = 0$. Then $f = g \in (X, Y)^2$. So

$$\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{p}/\mathfrak{p}^2 = \langle X, Y\rangle/\langle X, Y\rangle^2.$$

Hence, $\mathfrak{m}/\mathfrak{m}^2$ is 2-dimensional. Therefore, A is not a DVR by (23.9). □

Exercise **(23.11)**. — Let k be a field, A a ring intermediate between the polynomial ring and the formal power series ring in one variable: $k[X] \subset A \subset k[[X]]$. Suppose that A is local with maximal ideal $\langle X\rangle$. Prove that A is a DVR. (Such local rings arise as rings of power series with curious convergence conditions.)

Answer: Let's show that the ideal $\mathfrak{a} := \bigcap_{n\geq 0}\langle X^n\rangle$ of A is zero. Clearly, $\mathfrak{a}$ is a subset of the corresponding ideal $\bigcap_{n\geq 0}\langle X^n\rangle$ of $k[[X]]$, and the latter ideal is clearly zero. Hence (23.2) implies A is a DVR. □

Exercise **(23.12)**. — Let L/K be an algebraic extension of fields, $X_1, \dots, X_n$ variables, P and Q the polynomial rings over K and L in $X_1, \dots, X_n$.

(1) Let $\mathfrak{q}$ be a prime of Q, and $\mathfrak{p}$ its contraction in P. Prove $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{q})$.
(2) Let $f, g \in P$ be two polynomials with no common prime factor in P. Prove that f and g have no common prime factor $q \in Q$.

Answer: Since L/K is algebraic, Q/P is integral. Furthermore, P is normal, and Q is a domain. Hence we may apply the Going Down Theorem (14.9). So given any chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r = \mathfrak{p}$, we can proceed by descending induction on i for $0 \leq i \leq r$, and thus construct a chain of primes $\mathfrak{q}_0 \subsetneqq \cdots \subsetneqq \mathfrak{q}_r = \mathfrak{q}$ with $\mathfrak{q}_i \cap P = \mathfrak{p}_i$. Thus $\mathrm{ht}\,\mathfrak{p} \leq \mathrm{ht}\,\mathfrak{q}$. Conversely, any chain of primes $\mathfrak{q}_0 \subsetneqq \cdots \subsetneqq \mathfrak{q}_r = \mathfrak{q}$ contracts to a chain of primes $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r = \mathfrak{p}$, and $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$ by Incomparability, (14.3); whence, $\mathrm{ht}\,\mathfrak{p} \geq \mathrm{ht}\,\mathfrak{q}$. Hence $\mathrm{ht}\,\mathfrak{p} = \mathrm{ht}\,\mathfrak{q}$. Thus (1) holds.

Alternatively, by (15.11), $\mathrm{ht}(\mathfrak{p}) + \dim(P/\mathfrak{p}) = n$ and $\mathrm{ht}(\mathfrak{q}) + \dim(Q/\mathfrak{q}) = n$ as both P and Q are polynomial rings in n variables over a field. However, by (15.10), $\dim P/\mathfrak{p} = \mathrm{tr.deg}_K \operatorname{Frac}(P/\mathfrak{p})$ and $\dim Q/\mathfrak{q} = \mathrm{tr.deg}_L \operatorname{Frac}(Q/\mathfrak{q})$, and these two transcendence degrees are equal as Q/P is an integral extension. Thus again, (1) holds.

Suppose f and g have a common prime factor $q \in Q$, and set $\mathfrak{q} := Qq$. Then the maximal ideal $\mathfrak{q}Q_\mathfrak{q}$ of $Q_\mathfrak{q}$ is principal and nonzero. Hence $Q_\mathfrak{q}$ is a DVR by

(23.8). Thus $\operatorname{ht}(\mathfrak{q}) = 1$. Set $\mathfrak{p} := \mathfrak{q} \cap P$. Then $\mathfrak{p}$ contains f; whence, $\mathfrak{p}$ contains some prime factor p of f. Then $\mathfrak{p} \supseteq Pp$, and Pp is a nonzero prime. Hence $\mathfrak{p} = Pp$ since $\operatorname{ht}\mathfrak{p} = 1$ by (1). However, $\mathfrak{p}$ contains g too. Therefore, $p \mid g$, contrary to the hypothesis. Thus (2) holds. (Caution: if $f := X_1$ and $g := X_2$, then f and g have no common factor, yet there are no φ and ψ such that $\varphi f + \psi g = 1$.) □

Exercise **(23.14)**. — Let R be a Noetherian ring. Show that R is reduced if and only if (R_0) and (S_1) hold.

Answer: Assume (R_0) and (S_1) hold. Consider an irredundant primary decomposition $\langle 0\rangle = \bigcap \mathfrak{q}_i$. Set $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$. Then $\mathfrak{p}_i$ is minimal by (S_1), and $\mathfrak{p}_i = \mathfrak{q}_i$ by (R_0) and (18.22). So $\langle 0\rangle = \bigcap \mathfrak{p}_i = \sqrt{\langle 0\rangle}$. Thus R is reduced.

Conversely, assume R is reduced. Then $R_\mathfrak{p}$ is reduced for any prime $\mathfrak{p}$ by (13.13). So if $\mathfrak{p}$ is minimal, then $R_\mathfrak{p}$ is a field. Thus (R_0) holds. But $\langle 0\rangle = \bigcap_{\mathfrak{p}\ \text{minimal}} \mathfrak{p}$. So $\mathfrak{p}$ is minimal whenever $\mathfrak{p} \in \operatorname{Ass}(R)$ by (18.20). Thus R satisfies (S_1). □

Exercise **(23.19)**. — Prove that a Noetherian domain R is normal if and only if, given any prime $\mathfrak{p}$ associated to a principal ideal, $\mathfrak{p}R_\mathfrak{p}$ is principal.

Answer: Assume R normal. Take $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$. Then $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}(R_\mathfrak{p}/\langle x/1\rangle)$ by (17.9). So $\operatorname{depth}(R_\mathfrak{p}) = 1$. But $R_\mathfrak{p}$ is normal by (11.28). Hence $\mathfrak{p}R_\mathfrak{p}$ is principal by (23.8).

Conversely, assume that, given any prime $\mathfrak{p}$ associated to a principal ideal, $\mathfrak{p}R_\mathfrak{p}$ is principal. Given any prime $\mathfrak{p}$ of height 1, take a nonzero $x \in \mathfrak{p}$. Then $\mathfrak{p}$ is minimal containing $\langle x\rangle$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$ by (17.17). So, by hypothesis, $\mathfrak{p}R_\mathfrak{p}$ is principal. So $R_\mathfrak{p}$ is a DVR by (23.8). Thus R satisfies (R_1).

Given any prime $\mathfrak{p}$ with $\operatorname{depth}(R_\mathfrak{p}) = 1$, say $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}(R_\mathfrak{p}/\langle x/s\rangle)$ with $x \neq 0$. Then $\langle x/s\rangle = \langle x/1\rangle \subset R_\mathfrak{p}$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$ by (17.9). So, by hypothesis, $\mathfrak{p}R_\mathfrak{p}$ is principal. So $\dim(R_\mathfrak{p}) = 1$ by (23.8). Thus R also satisfies (S_2). So R is normal by Serre's Criterion, (23.17). □

Exercise **(23.20)**. — Let R be a Noetherian ring, K its total quotient ring,

$$\Phi := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{ht}(\mathfrak{p}) = 1 \,\} \quad \text{and} \quad \Sigma := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{depth}(R_\mathfrak{p}) = 1 \,\}.$$

Assuming (S_1) holds in R, prove $\Phi \subset \Sigma$, and prove $\Phi = \Sigma$ if and only if (S_2) holds.

Further, without assuming (S_1) holds, prove this canonical sequence is exact:

$$R \to K \to \textstyle\prod_{\mathfrak{p}\in\Sigma} K_\mathfrak{p}/R_\mathfrak{p}. \qquad \textbf{(23.20.1)}$$

Answer: Assume (S_1) holds. Then, given $\mathfrak{p} \in \Phi$, there exists a nonzerodivisor $x \in \mathfrak{p}$. Clearly, $\mathfrak{p}$ is minimal containing $\langle x\rangle$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$ by (17.17). Hence $\operatorname{depth}(R_\mathfrak{p}) = 1$ by (23.4)(2). Thus $\Phi \subset \Sigma$.

However, as (S_1) holds, (S_2) holds if and only if $\Phi \supset \Sigma$. Thus $\Phi = \Sigma$ if and only if R satisfies (S_2).

Further, without assuming (S_1), consider (23.20.1). Trivially, the composition is zero. Conversely, take an $x \in K$ that vanishes in $\prod_{\mathfrak{p}\in\Sigma} K_\mathfrak{p}/R_\mathfrak{p}$. Say $x = a/b$ with $a, b \in R$ and b a nonzerodivisor. Then $a/1 \in bR_\mathfrak{p}$ for all $\mathfrak{p} \in \Sigma$. But $b/1 \in R_\mathfrak{p}$ is, clearly, a nonzerodivisor for any prime $\mathfrak{p}$. Hence, if $\mathfrak{p} \in \operatorname{Ass}(R_\mathfrak{p}/bR_\mathfrak{p})$, then $\mathfrak{p} \in \Sigma$ by (23.4)(2). Therefore, $a \in bR$ by (18.25). Thus $x \in R$. Thus (23.20.1) is exact. □

Exercise **(23.21)**. — Let R be a Noetherian ring, and K its total quotient ring. Set $\Phi := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{ht}(\mathfrak{p}) = 1 \,\}$. Prove these three conditions are equivalent:

(1) R is normal.
(2) (R_1) and (S_2) hold.
(3) (R_1) and (S_1) hold, and $R \to K \to \prod_{\mathfrak{p}\in\Phi} K_{\mathfrak{p}}/R_{\mathfrak{p}}$ is exact.

Answer: Assume (1) holds. Then R is reduced by (14.15). So (23.14) yields (R_0) and (S_1). But $R_{\mathfrak{p}}$ is normal for any prime $\mathfrak{p}$ by (14.14). Thus (2) holds by (23.8).

Assume (2) holds. Then (R_1) and (S_1) hold trivially. Thus (23.20) yields (3).

Assume (3) holds. Let $x \in K$ be integral over R. Then $x/1 \in K$ is integral over $R_{\mathfrak{p}}$ for any prime $\mathfrak{p}$. Now, $R_{\mathfrak{p}}$ is a DVR for all $\mathfrak{p}$ of height 1 as R satisfies (R_1). Hence, $x/1 \in R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Phi$. So $x \in R$ by the exactness of the sequence in (3). But R is reduced by (23.14). Thus (14.15) yields (1). □

24. Dedekind Domains

Exercise **(24.5)**. — Let R be a domain, S a multiplicative set.

(1) Assume $\dim(R) = 1$. Prove $\dim(S^{-1}R) = 1$ if and only if there is a nonzero prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$.

(2) Assume $\dim(R) \geq 1$. Prove $\dim(R) = 1$ if and only if $\dim(R_{\mathfrak{p}}) = 1$ for every nonzero prime $\mathfrak{p}$.

Answer: Consider (1). Suppose $\dim(S^{-1}R) = 1$. Then there's a chain of primes $0 \underset{\neq}{\subsetneq} \mathfrak{p}' \subset S^{-1}R$. Set $\mathfrak{p} := \mathfrak{p}' \cap R$. Then $\mathfrak{p}$ is as desired by (11.16)(2).

Conversely, suppose there's a nonzero $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $0 \underset{\neq}{\subsetneq} \mathfrak{p}S^{-1}R$ is a chain of primes by (11.16)(2); so $\dim(S^{-1}R) \geq 1$. Now, given a chain of primes $0 = \mathfrak{p}'_0 \underset{\neq}{\subsetneq} \cdots \underset{\neq}{\subsetneq} \mathfrak{p}'_r \subset S^{-1}R$, set $\mathfrak{p}_i := \mathfrak{p}'_i \cap R$. Then $0 = \mathfrak{p}_0 \underset{\neq}{\subsetneq} \cdots \underset{\neq}{\subsetneq} \mathfrak{p}_r \subset R$ is a chain of primes by (11.16)(2). So $r \leq 1$ as $\dim(R) = 1$. Thus $\dim(S^{-1}R) = 1$.

Consider (2). If $\dim(R) = 1$, then (1) yields $\dim(R_{\mathfrak{p}}) = 1$ for every nonzero $\mathfrak{p}$.

Conversely, let $0 = \mathfrak{p}_0 \underset{\neq}{\subsetneq} \cdots \underset{\neq}{\subsetneq} \mathfrak{p}_r \subset R$ be a chain of primes. Set $\mathfrak{p}'_i := \mathfrak{p}_i R_{\mathfrak{p}_i}$. Then $0 = \mathfrak{p}'_0 \underset{\neq}{\subsetneq} \cdots \underset{\neq}{\subsetneq} \mathfrak{p}'_r$ is a chain of primes by (11.16)(2). So if $\dim(R_{\mathfrak{p}_i}) = 1$, then $r \leq 1$. Thus, if $\dim(R_{\mathfrak{p}}) = 1$ for every nonzero $\mathfrak{p}$, then $\dim(R) \leq 1$, as desired. □

Exercise **(24.6)**. — Let R be a Dedekind domain, S a multiplicative set. Prove $S^{-1}R$ is a Dedekind domain if and only if there's a nonzero prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$.

Answer: Suppose there's a prime nonzero $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $0 \notin S$. So $S^{-1}R$ is a domain by (11.3). And $S^{-1}R$ is normal by (11.28). Further, $S^{-1}R$ is Noetherian by (16.7). Also, $\dim(S^{-1}R) = 1$ by (24.5)(1). Thus $S^{-1}R$ is Dedekind.

The converse results directly from (24.5)(1). □

Exercise **(24.8)**. — Let R be a Dedekind domain, and $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ideals. By first reducing to the case that R is local, prove that

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}),$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}).$$

Answer: In any module over any ring, two submodules M and N are equal if their localizations $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ are equal for each maximal ideal $\mathfrak{p}$. Indeed, replacing N by $M+N$, we may assume that $M \subset N$. Then by (12.16), $(N/M)_{\mathfrak{p}} = N_{\mathfrak{p}}/M_{\mathfrak{p}} = 0$ for each $\mathfrak{p}$; whence, $N/M = 0$ by (13.12).

In the case at hand, therefore, it suffices to prove that the two equations in questions hold after localizing at each maximal ideal $\mathfrak{p}$. But localization commutes with sum and intersection by (12.15)(4), (5). So the localized equations look like the original ones, but with $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ replaced by $\mathfrak{a}_{\mathfrak{p}}$, $\mathfrak{b}_{\mathfrak{p}}$, $\mathfrak{c}_{\mathfrak{p}}$. Hence we may replace R by $R_{\mathfrak{p}}$, and thus assume that R is a DVR.

Referring to (23.1), take a uniformizing parameter t, and say $\mathfrak{a} = \langle t^i \rangle$ and $\mathfrak{b} = \langle t^j \rangle$ and $\mathfrak{c} = \langle t^k \rangle$. Then the two equations in questions are equivalent to these two:

$$\max\bigl\{i,\, \min\{j,k\}\bigr\} = \min\bigl\{\max\{i,j\},\, \max\{i,k\}\bigr\},$$
$$\min\bigl\{i,\, \max\{j,k\}\bigr\} = \max\bigl\{\min\{i,j\},\, \min\{i,k\}\bigr\}.$$

However, these two equations are easy to check for any integers i, j, k. □

Exercise **(24.12)**. — Prove that a semilocal Dedekind domain A is a PID. Begin by proving that each maximal ideal is principal.

Answer: Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the maximal ideals of A. Let's prove they are principal, starting with $\mathfrak{p}_1$. By Nakayama's lemma (10.8), $\mathfrak{p}_1 A_{\mathfrak{p}_1} \neq \mathfrak{p}_1^2 A_{\mathfrak{p}_1}$; so $\mathfrak{p}_1 \neq \mathfrak{p}_1^2$. Take $y \in \mathfrak{p}_1 - \mathfrak{p}_1^2$. The ideals $\mathfrak{p}_1^2$, $\mathfrak{p}_2$, $\ldots$, $\mathfrak{p}_r$ are pairwise comaximal because no two of them lie in the same maximal ideal. Hence, by the Chinese Remainder Theorem, (1.12), there is an $x \in A$ with $x \equiv y \bmod \mathfrak{p}_1^2$ and $x \equiv 1 \bmod \mathfrak{p}_i$ for $i \geq 2$.

The Main Theorem of Classical Ideal Theory, (24.10), yields $\langle x \rangle = \mathfrak{p}_1^{n_1} \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$ with $n_i \geq 0$. But $x \notin \mathfrak{p}_i$ for $i \geq 2$; so $n_i = 0$ for $i \geq 2$. Further, $x \in \mathfrak{p}_1 - \mathfrak{p}_1^2$; so $n_1 = 1$. Thus $\mathfrak{p}_1 = \langle x \rangle$. Similarly, all the other $\mathfrak{p}_i$ are principal.

Finally, let $\mathfrak{a}$ be any nonzero ideal. Then the Main Theorem, (24.10), yields $\mathfrak{a} = \prod \mathfrak{p}_i^{m_i}$ for some m_i. Say $\mathfrak{p}_i = \langle x_i \rangle$. Then $\mathfrak{a} = \prod x_i^{m_i}$, as desired. □

Exercise **(24.13)**. — Let R be a Dedekind domain, $\mathfrak{a}$ and $\mathfrak{b}$ two nonzero ideals. Prove (1) every ideal in $R/\mathfrak{a}$ is principal, and (2) $\mathfrak{b}$ is generated by two elements.

Answer: To prove (1), let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the associated primes of $\mathfrak{a}$, and set $S := \bigcap_i (R - \mathfrak{p}_i)$. Then S is multiplicative. Set $R' := S^{-1}R$. Then R' is Dedekind by (24.6). Let's prove R' is semilocal.

Let $\mathfrak{q}$ be a maximal ideal of R', and set $\mathfrak{p} := \mathfrak{q} \cap R$. Then $\mathfrak{q} = \mathfrak{p}R'$ by (11.16). So $\mathfrak{p}$ is nonzero, whence maximal since R has dimension 1. Suppose $\mathfrak{p}$ is distinct from all the $\mathfrak{p}_i$. Then $\mathfrak{p}$ and the $\mathfrak{p}_i$ are pairwise comaximal. So, by the Chinese Remainder Theorem, (1.12), there is a $u \in R$ that is congruent to 0 modulo $\mathfrak{p}$ and to 1 modulo each $\mathfrak{p}_i$. Hence, $u \in \mathfrak{p} \cap S$, but $\mathfrak{q} = \mathfrak{p}R'$, a contradiction. Thus $\mathfrak{p}_1 R', \ldots, \mathfrak{p}_r R'$ are all the maximal ideals of R'.

So R' is a PID by (24.12); so every ideal in $R'/\mathfrak{a}R'$ is principal. But by (12.18), $R'/\mathfrak{a}R' = S^{-1}(R/\mathfrak{a})$. Finally, $S^{-1}(R/\mathfrak{a}) = R/\mathfrak{a}$ by (11.6) because every $u \in S$ maps to a unit in $R/\mathfrak{a}$ since the image lies in no maximal ideal of $R/\mathfrak{a}$. Thus (1) holds.

Alternatively, we can prove (1) without using (24.12), as follows. The Main Theorem of Classical Ideal Theory, (24.10), yields $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$ for distinct maximal ideals $\mathfrak{p}_i$. The $\mathfrak{p}_i^{n_i}$ are pairwise comaximal. So, by the Chinese Remainder Theorem, (1.12), there's a canonical isomorphism:

$$R/\mathfrak{a} \xrightarrow{\sim} R/\mathfrak{p}_1^{n_1} \times \cdots \times R/\mathfrak{p}_k^{n_k}.$$

Next, let's prove each $R/\mathfrak{p}_i^{n_i}$ is a Principal Ideal Ring (PIR); that is, every ideal is principal. Set $S := R - \mathfrak{p}_i$. Then $S^{-1}(R/\mathfrak{p}_i^{n_i}) = R_{\mathfrak{p}_i}/\mathfrak{p}_i^{n_i}R_{\mathfrak{p}_i}$, and the latter ring is a PIR because $R_{\mathfrak{p}_i}$ is a DVR. However, $R/\mathfrak{p}_i^{n_i} = S^{-1}(R/\mathfrak{p}_i^{n_i})$ by (11.6), because every $u \in S$ maps to a unit in $R/\mathfrak{p}_i^{n_i}$ since $\mathfrak{p}/\mathfrak{p}_i^{n_i}$ is the only prime in $R/\mathfrak{p}_i^{n_i}$.

Finally, given finitely many PIRs $R_1, \ldots, R_k$, we must prove their product is a PIR. Consider an ideal $\mathfrak{b} \subset R_1 \times \cdots \times R_k$. Then $\mathfrak{b} = \mathfrak{b}_1 \times \cdots \times \mathfrak{b}_k$ where $\mathfrak{b}_i \subset R_i$ is an ideal by (1.14). Say $\mathfrak{b}_i = \langle a_i \rangle$. Then $\mathfrak{b} = \big\langle (a_1, \ldots, a_k) \big\rangle$. Thus again, (1) holds.

Consider (2). Let $x \in \mathfrak{b}$ be nonzero. By (1), there is a $y \in \mathfrak{b}$ whose residue generates $\mathfrak{b}/\langle x \rangle$. Then $\mathfrak{b} = \langle x, y \rangle$. □

25. Fractional Ideals

Exercise **(25.2)**. — Let R be a domain, M and N nonzero fractional ideals. Prove that M is principal if and only if there exists some isomorphism $M \simeq R$. Construct the following canonical surjection and canonical isomorphism:

$$\pi\colon M \otimes N \twoheadrightarrow MN \quad \text{and} \quad \varphi\colon (M : N) \xrightarrow{\sim} \operatorname{Hom}(N, M).$$

Answer: If $M \simeq R$, let x correspond to 1; then $M = Rx$. Conversely, assume $M = Rx$. Then $x \neq 0$ as $M \neq 0$. Form the map $R \to M$ with $a \mapsto ax$. It's surjective as $M = Rx$. It's injective as $x \neq 0$ and $M \subset \operatorname{Frac}(R)$.

Form the canonical $M \times N \to MN$ with $(x, y) \mapsto xy$. It's bilinear. So it induces a map $\pi\colon M \otimes N \to MN$, and clearly π is surjective.

Define φ as follows: given $z \in (M : N)$, define $\varphi(z)\colon N \to M$ by $\varphi(z)(y) := yz$. Clearly, φ is R-linear. Say $y \neq 0$. Then $yz = 0$ implies $z = 0$; thus, φ is injective.

Finally, given $\theta\colon N \to M$, fix a nonzero $n \in N$, and set $z := \theta(n)/n$. Given $y \in N$, say $y = a/b$ and $n = c/d$ with $a, b, c, d \in R$. Then $bcy = adn$. So $bc\theta(y) = ad\theta(n)$. Hence $\theta(y) = yz$. Thus, φ is surjective, as desired. □

Exercise **(25.6)**. — Let R be a domain, M and N fractional ideals. Prove that the map $\pi\colon M \otimes N \to MN$ is an isomorphism if M is locally principal.

Answer: By (13.15), we must prove that, for each maximal ideal $\mathfrak{m}$, the localized map $\pi_{\mathfrak{m}}\colon (M \otimes N)_{\mathfrak{m}} \to (MN)_{\mathfrak{m}}$ is an isomorphism. But $(M \otimes N)_{\mathfrak{m}} = M_{\mathfrak{m}} \otimes N_{\mathfrak{m}}$ by (12.13), and $(MN)_{\mathfrak{m}} = M_{\mathfrak{m}}N_{\mathfrak{m}}$ by (25.4). By hypothesis, $M_{\mathfrak{m}} = R_{\mathfrak{m}}x$ for some x. Clearly $R_{\mathfrak{m}}x \simeq R_{\mathfrak{m}}$. And $R_{\mathfrak{m}} \otimes N_{\mathfrak{m}} = N_{\mathfrak{m}}$ by (8.5)(2). Thus $\pi_{\mathfrak{m}} \simeq 1_{N_{\mathfrak{m}}}$. □

Exercise **(25.11)**. — Let R be a UFD. Show that a fractional ideal M is invertible if and only if M is principal and nonzero.

Answer: By (25.7), a nonzero principal ideal is always invertible.

Conversely, assume M is invertible. Then trivially $M \neq 0$. Say $1 = \sum m_i n_i$ with $m_i \in M$ and $n_i \in M^{-1}$. Fix a nonzero $m \in M$.

Then $m = \sum m_i n_i m$. But $n_i m \in R$ as $m \in M$ and $n_i \in M^{-1}$. Set

$$d := \gcd\{n_i m\} \in R \quad \text{and} \quad x := \textstyle\sum (n_i m/d) m_i \in M.$$

Then $m = dx$.

Given $m' \in M$, write $m'/m = a/b$ where $a, b \in R$ are relatively prime. Then

$$d' := \gcd\{n_i m'\} = \gcd\{n_i m a/b\} = a \gcd\{n_i m\}/b = ad/b.$$

So $m' = (a/b)m = (ad/b)x = d'x$. But $d' \in R$. Thus $M = Rx$. □

Exercise **(25.14)**. — Show that a ring is a PID if and only if it's a Dedekind domain and a UFD.

Answer: A PID is Dedekind by (24.2), and is a UFD by (2.20).

Conversely, let R be a Dedekind UFD. Then every nonzero fractional ideal is invertible by (25.3) and (25.13), so is principal by (25.11). Thus R is a PID.

Alternatively and more directly, every nonzero prime is of height 1 as $\dim R = 1$, so is principle by (21.11). But, by (24.10), every nonzero ideal is a product of nonzero prime ideals. Thus again, R is a PID. □

Exercise **(25.16)**. — Let R be an ring, M an invertible module. Prove that M is finitely generated, and that, if R is local, then M is free of rank 1.

Answer: Say $\alpha\colon M\otimes N \xrightarrow{\sim} R$ and $1 = \alpha(\sum m_i\otimes n_i)$ with $m_i \in M$ and $n_i \in N$. Given $m \in M$, set $a_i := \alpha(m \otimes n_i)$. Form this composition:

$$\beta\colon M = M \otimes R \xrightarrow{\sim} M \otimes M \otimes N = M \otimes N \otimes M \xrightarrow{\sim} R \otimes M = M.$$

Then $\beta(m) = \sum a_i m_i$. But β is an isomorphism. Thus the m_i generate M.

Suppose R is local. Then $R - R^\times$ is an ideal. So $u := \alpha(m_i \otimes n_i) \in R^\times$ for some i. Set $m := u^{-1}m_i$ and $n := n_i$. Then $\alpha(m \otimes n) = 1$. Define $\nu\colon M \to R$ by $\nu(m') := \alpha(m' \otimes n)$. Then $\nu(m) = 1$; so ν is surjective. Define $\mu\colon R \to M$ by $\mu(x) := xm$. Then $\mu\nu(m') = \nu(m')m = \beta(m')$, or $\mu\nu = \beta$. But β is an isomorphism. So ν is injective. Thus ν is an isomorphism, as desired. □

Exercise **(25.17)**. — Show these conditions on an R-module M are equivalent:

(1) M is invertible.
(2) M is finitely generated, and $M_{\mathfrak m} \simeq R_{\mathfrak m}$ at each maximal ideal $\mathfrak m$.
(3) M is locally free of rank 1.

Assuming the conditions, show M is finitely presented and $M \otimes \operatorname{Hom}(M, R) = R$.

Answer: Assume (1). Then M is finitely generated by (25.16). Further, say $M \otimes N \simeq R$. Let $\mathfrak m$ be a maximal ideal. Then $M_{\mathfrak m} \otimes N_{\mathfrak m} \simeq R_{\mathfrak m}$. Hence $M_{\mathfrak m} \simeq R_{\mathfrak m}$ again by (25.16). Thus (2) holds.

Conditions (2) and (3) are equivalent by (13.21).

Assume (3). Then (2) holds; so $M_{\mathfrak m} \simeq R_{\mathfrak m}$ at any maximal ideal $\mathfrak m$. Also, M is finitely presented by (13.20); so $\operatorname{Hom}_R(M, R)_{\mathfrak m} = \operatorname{Hom}_{R_{\mathfrak m}}(M_{\mathfrak m}, R_{\mathfrak m})$ by (12.21).

Consider the evaluation map

$$\operatorname{ev}(M,R)\colon M \otimes \operatorname{Hom}(M,R) \to R \quad \text{defined by} \quad \operatorname{ev}(M,R)(m,\alpha) := \alpha(m).$$

Clearly $\operatorname{ev}(M,R)_{\mathfrak m} = \operatorname{ev}(M_{\mathfrak m}, R_{\mathfrak m})$. Clearly $\operatorname{ev}(R_{\mathfrak m}, R_{\mathfrak m})$ is bijective. Hence $\operatorname{ev}(M,R)$ is bijective by (13.15). Thus the last assertions hold; in particular, (1) holds. □

26. Arbitrary Valuation Rings

Exercise **(26.3)**. — Let V be a domain. Show that V is a valuation ring if and only if, given any two ideals $\mathfrak a$ and $\mathfrak b$, either $\mathfrak a$ lies in $\mathfrak b$ or $\mathfrak b$ lies in $\mathfrak a$.

Answer: First, suppose V is a valuation ring. Suppose also $\mathfrak{a} \not\subset \mathfrak{b}$; say $x \in \mathfrak{a}$, but $x \notin \mathfrak{b}$. Take $y \in \mathfrak{b}$. Then $x/y \notin V$; else $x = (x/y)y \in \mathfrak{b}$. So $y/x \in V$. Hence $y = (y/x)x \in \mathfrak{a}$. Thus $\mathfrak{b} \subset \mathfrak{a}$.

Conversely, let $x, y \in V - \{0\}$, and suppose $x/y \notin V$. Then $\langle x\rangle \not\subset \langle y\rangle$; else, $x = wy$ with $w \in V$. Hence $\langle y\rangle \subset \langle x\rangle$ by hypothesis. So $y = zx$ for some $z \in V$; in other words, $y/x \in V$. Thus V is a valuation ring. □

Exercise **(26.4)**. — Let V be a valuation ring, $\mathfrak{m}$ its maximal ideal, and $\mathfrak{p} \subset \mathfrak{m}$ another prime ideal. Prove that $V_{\mathfrak{p}}$ is a valuation ring, that its maximal ideal $\mathfrak{p}V_{\mathfrak{p}}$ is equal to $\mathfrak{p}$, and that $V/\mathfrak{p}$ is a valuation ring of the field $V_{\mathfrak{p}}/\mathfrak{p}$.

Answer: First, set $K := \mathrm{Frac}(V_{\mathfrak{p}})$. So $K = \mathrm{Frac}(V)$. Let $x \in K - V_{\mathfrak{p}}$. Then $1/x \in V \subset V_{\mathfrak{p}}$. Thus $V_{\mathfrak{p}}$ is a valuation ring.

Second, let $r/s \in \mathfrak{p}V_{\mathfrak{p}}$ where $r \in \mathfrak{p} - \{0\}$ and $s \in V - \mathfrak{p}$. Then $s/r \notin V$, else $s = (s/r)r \in \mathfrak{p}$. Hence $r/s \in V$. Now, $(r/s)s = r \in \mathfrak{p}$, but $s \notin \mathfrak{p}$; since $\mathfrak{p}$ is prime, $r/s \in \mathfrak{p}$. Thus $\mathfrak{p}V_{\mathfrak{p}} = \mathfrak{p}$.

Third, to prove $V/\mathfrak{p}$ is a valuation ring of $V_{\mathfrak{p}}/\mathfrak{p}V_{\mathfrak{p}}$, we need only show that, whenever $x \in V_{\mathfrak{p}} - V$, then $x^{-1} \in V$. But, V is a valuation ring; hence, $x^{-1} \in V$. □

Exercise **(26.5)**. — Prove that a valuation ring V is normal.

Answer: Set $K := \mathrm{Frac}(V)$, and let $\mathfrak{m}$ be the maximal ideal. Take $x \in K$ integral over V, say $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_i \in V$. Then

$$1 + a_1x^{-1} + \cdots + a_nx^{-n} = 0. \qquad \textbf{(26.5.2)}$$

If $x \notin V$, then $x^{-1} \in \mathfrak{m}$ by (26.2). So (26.5.2) yields $1 \in \mathfrak{m}$, a contradiction. Hence $x \in V$. Thus V is normal. □

Exercise **(26.10)**. — Let K be a field, $\mathcal{S}$ the set of local subrings with fraction field K, ordered by domination. Show its maximal elements are the valuation rings.

Answer: Let V be maximal in $\mathcal{S}$. By (26.9), V is dominated by a valuation ring V' of K. By maximality, $V = V'$.

Conversely, let V be a valuation ring of K. Then V lies in $\mathcal{S}$ by (26.2). Let $V' \in \mathcal{S}$ dominate V. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the maximal ideals of V and V'. Take any nonzero $x \in V'$. Then $1/x \notin \mathfrak{m}'$ as $1 \notin \mathfrak{m}'$; so also $1/x \notin \mathfrak{m}$. So $x \in V$ by (26.2). Hence, $V' = V$. Thus V is maximal in $\mathcal{S}$. □

Exercise **(26.15)**. — Let V be a valuation ring, such as a DVR, whose value group Γ is *Archimedean*; that is, given any nonzero $\alpha, \beta \in \Gamma$, there's $n \in \mathbb{Z}$ such that $n\alpha > \beta$. Show that V is a maximal proper subring of its fraction field K.

Answer: Let R be a subring of K strictly containing V, and fix $a \in R - V$. Given $b \in K$, let α and β be the values of a and b. Then $\alpha < 0$. So, as Γ is Archimedian, there's $n > 0$ such that $-n\alpha > -\beta$. Then $v(b/a^n) > 0$. So $b/a^n \in V$. So $b = (b/a^n)a^n \in R$. Thus $R = K$. □

Exercise **(26.16)**. — Let V be a valuation ring. Show that

(1) every finitely generated ideal $\mathfrak{a}$ is principal, and

(2) V is Noetherian if and only if V is a DVR.

Answer: To prove (1), say $\mathfrak{a} = \langle x_1, \ldots, x_n \rangle$ with $x_i \neq 0$ for all i. Let v be the valuation. Suppose $v(x_1) \leq v(x_i)$ for all i. Then $x_i/x_1 \in V$ for all i. So $x_i \in \langle x_1 \rangle$. Hence $\mathfrak{a} = \langle x_1 \rangle$. Thus (1) holds.

To prove (2), first assume V is Noetherian. Then V is local by (26.2), and by (1) its maximal ideal $\mathfrak{m}$ is principal. Hence V is a DVR by (23.8). Conversely, assume V is a DVR. Then V is a PID by (23.1), so Noetherian. Thus (2) holds. □