INTRO TO MODULES AND INTEGRAL RING EXTENSIONS

FELIX GOTTI

1. A Brief Intro to Modules

Definitions and Examples. Modules over commutative rings are generalizations of vector spaces that play a fundamental role in commutative algebra and, in particular, in ideal theory. For the rest of this section, let R be a commutative ring with identity.

Definition 1. An additive abelian group M is a *module* over R (or an *R-module*) if there is an action of R on M, that is, a map $R \times M \to M$ given by $(r, m) \mapsto rm$, satisfying the following properties:

(1) $r(m_1 + m_2) = rm_1 + rm_2$ for all $r \in R$ and $m_1, m_2 \in M$,
(2) $(r_1 + r_2)m = r_1m + r_2m$ for all $r_1, r_2 \in R$ and $m \in M$,
(3) $(r_1r_2)m = r_1(r_2m)$ for all $r_1, r_2 \in R$ and $m \in M$, and
(4) $1m = m$ for all $m \in M$.

It is clear from the above definition that vector spaces are precisely modules over fields. On the other hand, it is not hard to see that there is a canonical action of $\mathbb{Z}$ over any abelian group A turning A into a $\mathbb{Z}$-module, namely, $na := a + \cdots + a$ (the addition of n copies of a) and $(-n)a := -na$ for all $n \in \mathbb{N}_0$ and $a \in A$. Also, for $n \in \mathbb{N}$, it is easy to verify that the additive abelian group R^n is an R-module over R under the action $r(a_1, \ldots, a_n) := (ra_1, \ldots, ra_n)$. Under this action, R^n is called the *free module of rank n* over R.

Let M be an R-module. A subgroup N of M is called an *R-submodule* of M if it is is closed under the action of R, that is, $rn \in N$ for all $r \in R$ and $n \in N$. One can readily prove that N is a submodule of M if and only if N is nonempty and $x + ry \in N$ for all $r \in R$ and $x, y \in N$. Every commutative ring R is an R-module over itself, and every ideal I of R is clearly an R-submodule. If N is an R-submodule of M, then the quotient group M/N is an R-module under the action $r(m + N) := rm + N$.

For R-modules M_1 and M_2, a map $\varphi\colon M_1 \to M_2$ is called an *R-module homomorphism* if φ is a group homomorphism satisfying that $\varphi(rm) = r\varphi(m)$ for all $r \in R$ and $m \in M$. In this case, $\ker \varphi$ is an R-submodule of M_1, and it follows that φ is injective if and only if $\ker \varphi = \{0\}$. When φ is bijective, it is called an *isomorphism* of R-modules. The canonical group isomorphism $M_1/\ker \varphi \cong \varphi(M_1)$ (from the First Isomorphism Theorem) is, indeed, an isomorphism of R-modules. If N_1 and N_2 are two R-submodules of M, then the subgroups $N_1 + N_2$ and $N_1 \cap N_2$ are R-submodules, and the canonical group isomorphism $(N_1 + N_2)/N_1 \cong N_2/(N_1 \cap N_2)$ (from the Second Isomorphism Theorem) is also an isomorphism of R-modules.

Finitely Generated Modules and Noetherian Modules. The R-module M is *finitely generated* if there exist $m_1, \dots, m_n \in M$ such that $M = Rm_1 + \cdots + Rm_n$. Clearly, every commutative ring R with identity is a finitely generated R-module over itself (generated by 1). In addition, quotient and so homomorphic images of finitely generated R-modules are finitely generated.

Proposition 2. *If N is an R-submodule of a finitely generated R-module M, then the quotient M/N is also a finitely generated R-module.*

Proof. Similar to the proof given for rings. □

Being finitely generated is transitive in the following sense.

Proposition 3. *Let R, S, and T be commutative rings with identities. If S is a finitely generated R-module and T is a finitely generated S-module, then T is a finitely generated R-module.*

Proof. Since S is a finitely generated R-module, we can take $s_1, \dots, s_m \in S$ such that $S = \sum_{i=1}^m Rs_i$. In addition, since T is a finitely generated S-module, we can take $t_1, \dots, t_n \in T$ such that $T = \sum_{j=1}^n St_j$. Thus, $T = \sum_{j=1}^n \big(\sum_{i=1}^m Rs_i\big)t_j = \sum_{i=1}^m \sum_{j=1}^n Rs_it_j$, whence T is a finitely generated R-module. □

An R-module M is called *Noetherian* if every R-submodule of M is finitely generated. Not every finitely generated R-module is Noetherian. For instance, although the ring $R := \mathbb{Z}[x_n : n \in \mathbb{N}]$ in countably many variables over $\mathbb{Z}$ is a finitely generated R-module, its ideal $(x_1, x_2, \dots)$ is an R-submodule that is not finitely generated.

Example 4. Let V be a finite-dimensional vector space over a field F. Then every F-submodule of V is a vector space of dimension at most $\dim V$ and, therefore, is finitely generated. As a result, V is a Noetherian F-module.

As in the case of commutative rings, one can characterize Noetherian modules as follows.

Proposition 5. *For an R-module M, the following statements are equivalent.*

(a) *M is Noetherian.*

(b) *M satisfies the ascending chain condition (ACC) on submodules: every ascending chain of R-submodules of M eventually stabilizes.*

(c) *Every nonempty set of R-submodules of M contains a maximal element (under inclusion).*

Proof. Exercise. □

As for commutative rings, quotients of Noetherian modules are Noetherian. Moreover, we have the following result.

Proposition 6. *Let M be an R-module, and let N be a submodule of M. Then M is Noetherian if and only if both N and M/N are Noetherian.*

Proof. Suppose first that M is Noetherian. Clearly, every R-submodule of N is also an R-submodule of M and, therefore, is finitely generated. Hence N is Noetherian. To verify that M/N is Noetherian, take an R-submodule S/N of M/N, where S is an R-submodule of M. Since M is Noetherian $S = Rs_1 + \cdots + Rs_k$ for some $s_1, \dots, s_k \in S$. Hence it immediately follows that $S/N = R(s_1 + N) + \cdots + R(s_k + N)$, and so S/N is finitely generated. Thus, R/N is also Noetherian.

Conversely, suppose that both N and M/N are Noetherian R-modules. Let S be an R-submodule of M, and let S' be the R-submodule $(S + N)/N$ of M/N. Since both N and M/N is Noetherian, $S \cap N = Rm_1 + \cdots + Rm_k$ and $S' = R(m_1' + N) + \cdots + R(m_\ell' + N)$ for some $m_1, \dots, m_k \in S \cap N$ and $m_1', \dots, m_\ell' \in S + N$. Indeed, we can assume that $m_1', \dots, m_\ell' \in S$. Now take $s \in S$ and write

$s + N = r_1'(m_1' + N) + \cdots + r_\ell'(m_\ell' + N)$, where $r_1', \ldots, r_\ell' \in R$. As $s - \sum_{j=1}^{\ell} r_j' m_j' \in N$, we can write $s - \sum_{j=1}^{\ell} r_j' m_j' = \sum_{i=1}^{k} r_i m_i$ for some $r_1, \ldots, r_k \in R$. Thus, $s = \sum_{i=1}^{k} r_i m_i + \sum_{j=1}^{\ell} r_j' m_j'$. Hence S can be generated by the elements $m_1, \ldots, m_k, m_1', \ldots, m_\ell'$. Since each R-submodule of M is finitely generated, we conclude that M is Noetherian. □

As a corollary of the previous proposition, we can obtain that the direct sum of finitely many Noetherian R-modules is also Noetherian.

Corollary 7. *Let $M_1, \ldots, M_n$ be R-modules. If $M_1, \ldots, M_n$ are Noetherian, then $M_1 \oplus \cdots \oplus M_n$ is Noetherian.*

Proof. It suffices to prove the statement for $n = 2$. It is clear that $M_1 \cong M_1 \oplus 0$. Also, since the projection $M_1 \oplus M_2 \to M_2$ has kernel $M_1 \oplus 0$, it follows from the First Isomorphism Theorem that $M_2 \cong (M_1 \oplus M_2)/(M_1 \oplus 0)$. Since both M_1 and M_2 are Noetherian, Proposition 6 guarantees that $M_1 \oplus M_2$ is Noetherian. □

We have pointed out before that not every finitely generated module is Noetherian. However, finitely generated modules over Noetherian rings are Noetherian, as the following proposition indicates.

Proposition 8. *Let M be a finitely generated R-module. If R is Noetherian, then M is Noetherian.*

Proof. Take $m_1, \ldots, m_k \in M$ such that $M = Rm_1 + \cdots + Rm_k$, and consider the map $\varphi\colon R^k \to M$ given by the assignment $(r_1, \ldots, r_k) \mapsto r_1 m_1 + \cdots + r_k m_k$. Clearly, φ is a surjective R-module homomorphism, and so the First Isomorphism Theorem ensures that $M \cong R^k/\ker\varphi$. Now observe that $R^k/\ker\varphi$ is a Noetherian R-module because direct sums and quotients of Noetherian modules remain Noetherian by Corollary 7 and Proposition 6, respectively. Hence M is Noetherian. □

Nakayama's Lemma. The main purpose of this section is to prove Nakayama's Lemma, which is an important result of commutative algebra that we shall be using in future lectures. Let M be an R-module. If I is an ideal of R, then

$$IM := \Big\{ \sum_{i=1}^{n} r_i m_i : r_1, \ldots, r_n \in I \text{ and } m_1, \ldots, m_n \in M \Big\}$$

is an R-submodule of M. Let us argue the following useful result, known as Nakayama's Lemma.

Lemma 9 (Nakayama's Lemma)**.** *Let R be a commutative ring with identity, and let I be an ideal of R. Then the following statements are equivalent.*

(a) *I is contained in every maximal ideal of R.*

(b) *If M is a finitely generated R-module such that $IM = M$, then $M = \{0\}$.*

(c) *If S is a submodule of a finitely generated R-module M such that $IM + S = M$, then $S = M$*

Proof. (a) ⇒ (b): Suppose that M is a finitely generated R-module such that $IM = M$. Now assume, by way of contradiction, that $M \neq \{0\}$. Write $M = Rm_1 + \cdots + Rm_n$ for $m_1, \ldots, m_n \in M$ assuming that $n \in \mathbb{N}$ is taken as smallest as possible. Since $M \neq \{0\}$, we see that $m_1 \neq 0$. As $m_1 \in M = IM$, we can take $a_1, \ldots, a_n \in I$ such that $m_1 = \sum_{i=1}^{n} a_i m_i$. Then $(1 - a_1)m_1 = \sum_{i=2}^{n} a_i m_i$. Since $a_1 \in I$ belongs to every maximal ideal, one can easily see that $1 - a_1 \in R^\times$. This implies that $n \geq 2$ and also that $a_1 = \sum_{i=2}^{n} (1 - a_1)^{-1} a_i m_i$, which contradicts the minimality of n.

(b) ⇒ (c) Let M be a finitely generated R-module, and let S be an R-submodule of M satisfying $IM + S = M$. Then M/S is also a finitely generated R-module. In addition, since $IM + S = M$, it follows that $M/S = (IM + S)/S = I(M/S)$. Therefore M/S is trivial by our hypothesis in part (b), which implies that $S = M$.

(c) $\Rightarrow$ (a) Let J be a maximal ideal of R. Then J is an R-submodule of the finitely generated R-module of R. Since $IR + J$ is an ideal of R containing the maximal ideal J, either $IR + J = R$ or $IR + J = J$. Since $J \neq R$, part (c) ensures that $IR + J \neq R$. As a result, $I + J = IR + J = J$, which implies that $I \subseteq J$. □

Localization of Modules. We can localize modules in the same way we have localized rings. Let R be a commutative ring with identity with a multiplicative subset S, and let M be an R-module. It is easy to verify that the relation on $M \times S$ defined by $(m_1, s_1) \sim (m_2, s_2)$ if there is an $s \in S$ such that $(m_1 s_2 - m_2 s_1)s = 0$ is an equivalence relation, and one denotes the class of (m, s) by m/s and the set of all equivalence classes by $S^{-1}M$. It is routine to verify that the operations

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2} \quad \text{and} \quad \frac{r}{s} \cdot \frac{m_1}{s_1} := \frac{r m_1}{s s_1},$$

where $m_1/s_1, m_2/s_2 \in S^{-1}M$ and $r/s \in S^{-1}R$, are well defined and turn $S^{-1}M$ into an $S^{-1}R$-module, which is called the *localization* M at S. In particular, $S^{-1}M$ is an R-module. As Exercise 9 indicates, localization commutes with (direct) sums, intersections, and quotients of modules. The map $\pi\colon M \to S^{-1}M$ defined by $m \mapsto m/1$ is an R-module homomorphism and has the universal property described in Proposition 10(2).

Proposition 10. *Let R be a commutative ring with identity, let S be a multiplicative subset of R, and let M be an R-module. Then the following statements hold.*

(1) *The map $\pi\colon M \to S^{-1}M$ defined by $m \mapsto m/1$ is an R-module homomorphism and $\ker \pi = \{m \in M : sm = 0 \text{ for some } s \in S\}$.*
(2) *If M' is an R-module such that, for each $s \in S$, left multiplication by s yields a bijection on M' and, in addition, $\varphi\colon M \to M'$ is an R-module homomorphism, then there is a unique R-module homomorphism $\theta\colon S^{-1}M \to M'$ such that $\varphi = \theta \circ \pi$.*
(3) *Any R-module homomorphism $\psi\colon M \to M'$ induces an $S^{-1}R$-module homomorphism $S^{-1}M \to S^{-1}M'$ via the assignment $m/s \mapsto \psi(m)/s$.*

Proof. Exercise. □

The localization of a Noetherian R-module is Noetherian.

Proposition 11. *Let R be a commutative ring with identity, and let S be a multiplicative subset of R. If M is a Noetherian R-module, then $S^{-1}M$ is also a Noetherian $S^{-1}R$-module.*

Proof. See the proof of Proposition **??**. □

2. Integral Extensions

We will tacitly assume that all rings in this lecture are commutative with identities. Throughout this lecture, $R \subseteq S$ is a ring extension, which means that R is a subring of the ring S. An element $s \in S$ is *algebraic* (resp., *integral*) over R if there exists a nonzero polynomial (resp., a monic polynomial) $f(x) \in R[x]$ such that $f(s) = 0$. Although every element of S that is integral over R is also algebraic, the converse does not hold in general; for instance, in the extension $\mathbb{Z} \subseteq \mathbb{Z}[1/2]$, the element $1/2$ is algebraic but not integral over $\mathbb{Z}$. The extension $R \subseteq S$ is called *integral* and the ring S is called *integral* over R provided that every element of S is integral over R. Observe that when R and S are fields, $R \subseteq S$ is integral if and only if S is an algebraic extension of R. We proceed to characterize integral elements.

Theorem 12. *Let $R \subseteq S$ be a ring extension. For $s \in S$, the following statements are equivalent.*

(a) *s is integral over R.*

(b) *$R[s]$ is a finitely generated R-module.*

(c) *s is contained in a subring T of S that is a finitely generated R-module.*

Proof. (a) $\Rightarrow$ (b): Since s is integral over R, there is a monic polynomial $f(x) \in R[x]$ having s as a root. Take $g(s) \in R[s]$ for some $g(x) \in R[x]$. Because $f(x)$ is monic, we can write $g(x) = q(x)f(x) + r(x)$ for $q(x), r(x) \in R[x]$ with $\deg r < d := \deg f$. Since $g(s) = r(s)$, the element $g(s)$ is a linear combination with coefficients in R of the elements $1, s, \ldots, s^{d-1}$. Hence $R[s]$ can be generated by the set $\{s^j : j \in [\![0, d-1]\!]\}$ as an R-module.

(b) $\Rightarrow$ (c): Take $T = R[s]$.

(c) $\Rightarrow$ (a): Let T be the subring described in the statement (c), and let $\{t_1, \ldots, t_n\}$ be a generating set of T as an R-module. As $1 \in T$, there are coefficients $r_1, \ldots, r_n \in R$ such that $\sum_{i=1}^n r_i t_i = 1$. Since $s \in T$, we see that $st_i \in T$ for every $i \in [\![1, n]\!]$. Hence, for each $j \in [\![1, n]\!]$, we can write $st_j = \sum_{i=1}^n c_{ij} t_i$, and so

$$\sum_{i=1}^{n} (\delta_{ij} s - c_{ij}) t_i = 0, \tag{2.1}$$

where δ_{ij} is the Kronecker delta (i.e., $\delta_{ij} = 1$ if $i = j$, and $\delta_{ij} = 0$ otherwise). After considering the $n \times n$ matrix $M := (\delta_{ij} s - c_{ij})_{i,j \in [\![1,n]\!]}$ and the vector $v := (t_1, \ldots, t_n)^T$, we can write the equalities in (2.1) simply as $Mv = 0$. By Cramer's Rule, $(\det M) t_i = 0$ for every $i \in [\![1, n]\!]$. As a result,

$$\det M = (\det M) \sum_{i=1}^{n} r_i t_i = \sum_{i=1}^{n} r_i (\det M) t_i = 0.$$

After taking C to be the matrix $(c_{ij})_{i,j \in [\![1,n]\!]}$, one obtains that s is a root of the monic polynomial $\det(xI - C) \in R[x]$, which is the characteristic polynomial of C. Hence s is integral over R, which concludes the proof. □

For a ring extension $R \subseteq S$, we say that S is *finite* over R provided that S is finitely generated as an R-module.

Corollary 13. *Every finite ring extension is integral.*

Let us show that the extension of a ring by finitely many integral elements is integral.

Proposition 14. *Let $R \subseteq S$ be a ring extension, and let $s_1, \ldots, s_n \in S$ be integral elements over R. Hence $R[s_1, \ldots, s_n]$ is a finitely generated R-module and, therefore, $R \subseteq R[s_1, \ldots, s_n]$ is an integral extension.*

Proof. It follows from Theorem 12 that $R[s_1]$ is a finitely generated R-module. Assume further that $R[s_1, \ldots, s_j]$ is a finitely generated module over R for some $j \in [\![1, n-1]\!]$. Since s_{j+1} is integral over R, it is clearly integral over $R[s_1, \ldots, s_j]$, and it follows from Theorem 12 that $R[s_1, \ldots, s_{j+1}]$ is a finitely generated module over $R[s_1, \ldots, s_j]$. Thus, it follows by transitivity of finitely generated modules that $R[s_1, \ldots, s_{j+1}]$ is a finitely generated R-module. Hence $R[s_1, \ldots, s_n]$ is a finitely generated R-module by induction, and Corollary 13 guarantees that $R[s_1, \ldots, s_n]$ is an integral extension of R. □

Now we prove that integrality is transitive.

Proposition 15. *Let $R \subseteq S$ and $S \subseteq T$ be ring extensions. If $R \subseteq S$ and $S \subseteq T$ are integral, then $R \subseteq T$ is also integral.*

Proof. Take $t \in T$. Since T is integral over S, there is a polynomial $p(x) = x^n + \sum_{i=0}^{n-1} c_i x^i \in S[x]$ for some $n \in \mathbb{N}$ having t as a root. As S is integral over R, the coefficients $c_0, \dots, c_{n-1}$ are integral over R, and so $R[c_0, \dots, c_{n-1}]$ is a finitely generated R-module by Proposition 14. Because t is integral over $R[c_0, \dots, c_{n-1}]$, the ring $R[c_0, \dots, c_{n-1}, t]$ is also a finitely generated module over $R[c_0, \dots, c_{n-1}]$. Hence the extension $R \subseteq R[c_0, \dots, c_{n-1}, t]$ is finite and so integral. In particular, t must be integral over R. Thus, $R \subseteq T$ is an integral extension. □

The integrality of an extension ring is preserved by quotients and localizations, as the following two propositions show.

Proposition 16. *Let $R \subseteq S$ be an integral ring extension, and let J be an ideal of S. Then S/J is an integral extension of $R/(J \cap R)$.*

Proof. Fix $s \in S$. As $R \subseteq S$ is an integral extension, there is a monic polynomial $x^n + \sum_{i=0}^{n-1} c_i x^i \in R[x]$ having s as a root. Setting $\bar{c}_i = c_i + J$, we see that $x^n + \sum_{i=0}^{n-1} \bar{c}_i x^i$ is a monic polynomial with coefficients in $(R+J)/J \cong R/(J \cap R)$ having $s + J$ as a root. Hence S/J is an integral extension of $R/(J \cap R)$. □

Proposition 17. *Let $R \subseteq S$ be an integral ring extension, and let M be a submonoid of $(R \setminus \{0\}, \cdot)$. Then $M^{-1}S$ is an integral extension of $M^{-1}R$.*

Proof. Take $s/m \in M^{-1}S$ with $s \in S$ and $m \in M$. Since the extension $R \subseteq S$ is integral, s is a root of a monic polynomial $x^n + \sum_{i=0}^{n-1} c_i x^i \in R[x]$. Therefore

$$\Big(\frac{s}{m}\Big)^n + \sum_{i=0}^{n-1} \frac{c_i}{m^{n-i}} \Big(\frac{s}{m}\Big)^i = m^{-n}\Big(s^n + \sum_{i=0}^{n-1} c_i s^i\Big) = 0,$$

and so s/m is a root of the monic polynomial $x^n + \sum_{i=0}^{n-1} (c_i/m^{n-i}) x^i \in M^{-1}R[x]$. As a consequence, s/m is integral over $M^{-1}R$. Hence $M^{-1}S$ is an integral extension of $M^{-1}R$. □

Proposition 18. *Let $R \subseteq S$ be an integral extension of integral domains. Then R is a field if and only if S is a field.*

Proof. First, assume that R is a field. Take $s \in S \setminus \{0\}$. As s is integral over R, there is a monic polynomial in $R[x]$ having s as a root. Assume that, among all such polynomials, $x^n - \sum_{i=0}^{n-1} c_i x^i$ has minimum degree. Hence $c_0 \in R^\times$ and, therefore,

$$s\Big(s^{n-1} - \sum_{i=1}^{n-1} c_i s^{i-1}\Big) c_0^{-1} = 1.$$

This implies that s is a unit of S. Hence S is a field.

Conversely, assume that S is a field. Take now $r \in R \setminus \{0\}$. As $r^{-1} \in S$ and S is an integral extension of R, there exists a polynomial $x^m - \sum_{i=0}^{m-1} d_i x^i \in R[x]$ having r^{-1} as a root, and so $r^{-m} = \sum_{i=0}^{m-1} d_i r^{-i}$. After multiplying this equality by r^{m-1}, we obtain that $r^{-1} = \sum_{i=0}^{m-1} d_i r^{m-1-i} \in R$. Thus, R is a field. □

Corollary 19. *Let R be an integral domain. If the extension $R \subseteq \mathrm{qf}(R)$ is integral, then R is a field.*

The statement of Proposition 18 is not longer true for integral extensions $R \subseteq S$, where S is not an integral domain.

Example 20. Let F be a field, and consider the ring $S := F[x]/(x^2)$. Observe that S is a two-dimensional vector space over F; indeed, $\{1 + (x^2), x + (x^2)\}$ is a basis of S over F. Thus, V is an integral extension of F by virtue of Corollary 13. It is clear, however, that S is not even an integral domain; for instance, $x + (x^2)$ is a nonzero zero-divisor of S.

The set $\overline{R}_S$ consisting of all elements of S that are integral over R is an integral extension of R, as we proceed to show.

Proposition 21. *Let $R \subseteq S$ be a ring extension. The set $\overline{R}_S$ is an integral extension of R, which contains every subring of S that is integral over R.*

Proof. Take $s, t \in \overline{R}_S$. Since s and t are integral over R, the ring extension $R \subseteq R[s,t]$ is integral by Proposition 14. Hence the elements $s \pm t$ and st are integral over R. As a result, $\overline{R}_S$ is a subring of S. On the other hand, it is clear that $\overline{R}_S$ contains every subring of S that is integral over R. □

With notation as in Proposition 21, the ring $\overline{R}_S$ is called the *integral closure* of R *in* S. The ring R is *integrally closed* in S if $\overline{R}_S = R$. The *integral closure* of an integral domain R, denoted by $\overline{R}$, is the integral closure of R in its field of fractions $\mathrm{qf}(R)$, and R is called *integrally closed* if $\overline{R} = R$. It turns out that the integral closure commutes with localization, as the following proposition indicates.

Proposition 22. *Let $R \subseteq S$ be a ring extension, and let M be a multiplicative subset of R. Then $M^{-1}\overline{R}_S$ is the integral closure of $M^{-1}R$ in $M^{-1}S$.*

Proof. Observe that $M^{-1}\overline{R}_S$ is the subring of $\mathrm{qf}(S)$ generated by M^{-1} and $\overline{R}_S$. As elements in both sets are integral over $M^{-1}R$, it follows that $M^{-1}\overline{R}_S$ is contained in the integral closure of $M^{-1}R$ in $M^{-1}S$. To argue the reverse inclusion, take an element $q \in M^{-1}S$ that is integral over $M^{-1}R$, and let $x^n + \sum_{i=0}^{n-1} c_i x^i$ be a polynomial with coefficients in $M^{-1}R$ having q as a root. Now take a common denominator $m \in M$ such that $q = s/m$ and $c_i = r_i/m$ for some $s \in S$ and $r_0, \ldots, r_{n-1} \in R$. After multiplying $q^n + \sum_{i=0}^{n-1} c_i q^i = 0$ by m^n, we see that

$$s^n + \sum_{i=0}^{n-1} (m^{n-i-1} r_i) s^i = m^n \Big(q^n + \sum_{i=0}^{n-1} c_i q^i \Big) = 0.$$

Hence s is a root of the monic polynomial $x^n + \sum_{i=0}^{n-1} m^{n-i-1} x^i \in R[x]$ and, therefore, $q = s/m \in M^{-1}\overline{R}_S$. As a consequence, the integral closure of $M^{-1}R$ in $M^{-1}S$ is contained in $M^{-1}\overline{R}_S$, which concludes our proof. □

Corollary 23. *Let R be an integral domain, and let S be a multiplicative subset of R. If R is integrally closed, then so is $S^{-1}R$.*

For an integral domain, being integrally closed is a local property.

Proposition 24. *For an integral domain R, the following statements are equivalent*

(a) *R is integrally closed.*

(b) *R_P is integrally closed for every prime ideal P of R.*

(c) *R_M is integrally closed for every maximal ideal M of R.*

Proof. (a) ⇒ (b): It follows from Corollary 23.

(b) ⇒ (c): This is clear as every maximal ideal is prime.

(c) ⇒ (a): Suppose, for the sake of a contradiction, that there exists an element $q \in \mathrm{qf}(R) \setminus R$ that is integral over R. Now consider the set $I := \{r \in R : rq \in R\}$. One can easily see that I is an ideal of R, which is proper because $1 \notin I$. Let M be a maximal ideal containing I. Observe now that $q \notin R_M$;

indeed, if $q = r/d$ for some $r \in R$ and $d \in R \setminus M$, then $dq = r \in R$ and so $d \in I \subseteq M$, which is not possible. Finally, the fact that q is integral over R implies that q is also integral over R_M, which contradicts that $q \notin R_M$. □

It turns out that every UFD is integrally closed.

Proposition 25. *Every UFD is integrally closed.*

Proof. Let R be a UFD, and take $r/s \in \mathrm{qf}(R) \setminus \{0\}$ to be an integral element over R, assuming that $r, s \in R$ have no common prime factors. Let $x^n - \sum_{i=0}^{n-1} c_i x^i$ be a polynomial in $R[x]$ having r/s as a root. After multiplying $(r/s)^n = \sum_{i=0}^{n-1} c_i (r/s)^i$ by s^n, one obtains $r^n = s \sum_{i=0}^{n-1} r^i s^{n-1-i}$. Therefore s divides r^n in R. This, together with the fact that R is a UFD, ensures that $s \in R^\times$, whence $r/s = rs^{-1} \in R$. Thus, R is integrally closed. □

Example 26. Since $\mathbb{Z}$ is a UFD, then it is integrally closed by Proposition 25. However, $\mathbb{Z}$ is not integrally closed in $\mathbb{C}$. Let us further show that the integral closure $R := \overline{\mathbb{Z}}_{\mathbb{C}}$ of $\mathbb{Z}$ in $\mathbb{C}$ is not even finitely generated as a $\mathbb{Z}$-module. To argue this, observe that for every $n \in \mathbb{N}$, the polynomial $p(x) = x^n + 2$ is irreducible over $\mathbb{Q}$ (by Eisenstein Criterion). Thus, taking $r \in R$ to be a root of $p(x)$, we see that $p(x)$ is the minimal polynomial of r and, therefore, the subset $\{1, r, \dots, r^{n-1}\}$ of R are integrally independent, (i.e., linearly independent over $\mathbb{Z}$).

Unlike localizations, quotients of integral domains does not preserve the property of being integrally closed.

Example 27. Since $\mathbb{Z}[x]$ is a UFD, it is integrally closed. Consider the ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}[\sqrt{5}]$ induced by the assignment $x \mapsto \sqrt{5}$. Since $x^2 - 5$ is the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}$, it follows that $\mathbb{Z}[x]/(x^2 - 5)$ is isomorphic to $\mathbb{Z}[\sqrt{5}]$, which is not integrally closed (see exercises below).

Exercises

Exercise 1. *Let M be a Noetherian R-module. Prove that any surjective R-module endomorphism of M is an isomorphism. Argue that the same does not hold if one replaces surjectivity by injectivity.*

Exercise 2. *Let R be a Noetherian ring, and let M_1 and M_2 be finitely generated R-modules. Prove that $\mathrm{Hom}_R(M_1, M_2)$ is a finitely generated R-module.*

Exercise 3. *Let R be a commutative ring with identity, and let S be a multiplicative subset of R. The set $\bar{S} := \{r \in R : \pi(r)$ is a unit of $S^{-1}R\}$ is called the* saturation *of S. Prove the following statements.*

(1) $\bar{S} = \{r \in R : rt \in S$ *for some* $t \in R\}$.
(2) $\bar{S}$ *is a multiplicative subset of R satisfying $S \subseteq \bar{S} = \bar{\bar{S}}$.*
(3) $S^{-1}R \cong \bar{S}^{-1}R$.

Exercise 4. *Let R be a commutative ring with identity, and let I and J be ideals of R. Prove that $I = J$ if and only if $IR_P = JR_P$ for every maximal ideal P of R.*

Exercise 5. *Let R be an integral domain, and let S be a multiplicative subset of R. Prove the following statements.*

(1) *If R is a UFD, then $S^{-1}R$ is a UFD.*
(2) *Suppose that S is saturated and R is atomic (i.e, every nonzero nonunit of R factors into irreducibles). If $S^{-1}R$ is a UFD, then R is a UFD.*

Exercise 6. *Prove Proposition* **??**.

Exercise 7. *Prove Proposition 10.*

Exercise 8. *Let R be a commutative ring, and let S be a multiplicative subset of R. Let M be an R-module. Let $\pi\colon M \to S^{-1}M$ be the natural map. Prove the following statements.*

(1) *For each R-submodule N of M, the set $S^{-1}N := \{n/s : n \in N \text{ and } s \in S\}$ is an $S^{-1}R$-submodule of $S^{-1}M$.*
(2) *If L is an $S^{-1}R$-submodule of $S^{-1}M$, then $\pi^{-1}(L)$ is an R-submodule of M.*
(3) *If N is an R-submodule of M, then $N \subseteq \pi^{-1}(S^{-1}N)$. Also, if $N = \pi^{-1}(L)$ for an $S^{-1}R$-submodule L of $S^{-1}M$, then $L = S^{-1}N$. In particular, every $S^{-1}R$-submodule of $S^{-1}M$ has the form $S^{-1}N$ for an R-submodule N of M.*
(4) *Deduce that there is a bijection between the set of $S^{-1}R$-submodules of $S^{-1}M$ and the set of R-submodules N of M satisfying the condition: if $sm \in N$ for some $s \in S$ and $m \in M$, then $m \in N$.*

Exercise 9. *Let R be a commutative ring with identity, let S be a multiplicative subset of R, and let M be an R-module. For any submodules M_1 and M_2 of M, prove the following statements.*

(1) $S^{-1}(M_1 + M_2) = S^{-1}M_1 + S^{-1}M_2$.
(2) $S^{-1}(M_1 \oplus M_2) = S^{-1}M_1 \oplus S^{-1}M_2$.
(3) $S^{-1}(M_1 \cap M_2) \cong S^{-1}M_1 \cap S^{-1}M_2$.
(4) $S^{-1}M \,/\, S^{-1}M_1 = S^{-1}(M/M_1)$.

Exercise 10. *Let $R \subseteq S$ be a ring extension, and let $\varphi\colon S \to S'$ be a surjective ring homomorphism. Prove the following statements.*

(1) *If $s \in S$ is integral over R, then $\varphi(s)$ is integral over $\varphi(R)$.*
(2) *There may be an element $s \in S$ that is algebraic over R such that $\varphi(s)$ is not algebraic over $\varphi(R)$.*
(3) *If $\ker\varphi \subseteq R$ and $\varphi(s)$ is integral over $\varphi(R)$ for some $s \in S$, then s is integral over R.*
(4) $\varphi(\overline{R}_S) \subseteq \overline{\varphi(R)}_{S'}$.
(5) *The inclusion in the previous statement may be proper.*

Exercise 11. *Let $R \subseteq S$ be an integral extension. Prove that for any distinct indeterminates $x_1, \ldots, x_n$ over S, the extension $R[x_1, \ldots, x_n] \subseteq S[x_1, \ldots, x_n]$ is also integral.*

Exercise 12. *Let R be a commutative ring with identity. Prove that the integral closure of R in $R[x]$ is the subring $R + N$ of $R[x]$, where N is the ideal consisting of all nilpotent elements of $R[x]$.*

Exercise 13. *Let $R \subseteq S$ be an integral ring extension. For any prime ideal Q of S, show that Q is a maximal ideal of S if and only if $Q \cap R$ is a maximal ideal of R.*

Exercise 14. *Let R be an integral domain, and let K be an algebraic extension of the field of fractions of R. Prove that K is the integral closure of R in K.*

Exercise 15. *Let d be a squarefree nonzero integer. Prove the following statements.*

(1) *The integral closure of* $\mathbb{Z}$ *in* $\mathbb{Q}(\sqrt{d})$ *is* $\mathbb{Z}[\sqrt{d}]$ *if* $d \equiv 2, 3 \pmod 4$.
(2) *The integral closure of* $\mathbb{Z}$ *in* $\mathbb{Q}(\sqrt{d})$ *is* $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *if* $d \equiv 1 \pmod 4$.
(3) *The ring* $\mathbb{Z}[\sqrt{d}]$ *is integrally closed if and only if* $d \equiv 2, 3 \pmod 4$.

Department of Mathematics, MIT, Cambridge, MA 02139
Email address: fgotti@mit.edu