IDEAL THEORY AND PRÜFER DOMAINS

FELIX GOTTI

Integral Extensions I

We will tacitly assume that all rings in this section are commutative with identities. Throughout this section, $R \subseteq S$ 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 $f(s) = 0$. 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 1. *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 $1, s, \dots, s^{d-1}$. 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 $\{t_1, \dots, t_n\}$ be a generating set of T as an R-module. As $1 \in T$, there are coefficients $r_1, \dots, r_n \in R$ 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

$$\sum_{i=1}^{n} (\delta_{ij} s - c_{ij}) t_i = 0, \tag{0.1}$$

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 $v := (t_1, \dots, t_n)^T$, we can write the equalities in (0.1) 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 2. *Every finite ring extension is integral.*

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

Proposition 3. *Let $R \subseteq S$ be a ring extension, and let $s_1, \dots, s_n \in S$ be integral elements over R. Hence $R[s_1, \dots, s_n]$ is a finitely generated R-module and, therefore, $R \subseteq R[s_1, \dots, s_n]$ is an integral extension.*

Proof. It follows from Theorem 1 that $R[s_1]$ is a finitely generated module over R. Assume further that $R[s_1, \dots, s_j]$ 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 $R[s_1, \dots, s_j]$, and it follows from Theorem 1 that $R[s_1, \dots, s_{j+1}]$ is a finitely generated module over $R[s_1, \dots, s_j]$. Thus, it follows by transitivity of finitely generated modules that $R[s_1, \dots, s_{j+1}]$ is a finitely generated R-module. Hence $R[s_1, \dots, s_n]$ is a finitely generated R-module by induction, and Corollary 2 guarantees that $R[s_1, \dots, s_n]$ is an integral extension of R. □

Now we prove that integrality is transitive.

Proposition 4. *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 3. 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 5. *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 6. *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. If M contains a nonzero zero-divisor of S, then the kernel J of $S \to M^{-1}S$ (that is, $J := \{s \in S : sm = 0 \text{ for some } m \in M\}$) is a nonzero ideal of S, but we can easily verify that $M^{-1}S \cong N^{-1}(S/J)$ and $M^{-1}R \cong N^{-1}((R+J)/J)$, where N is the image of M in S/J (which is a multiplicative set with no zero-divisors). Thus, there is no loss of generality in assuming that M contains no zero-divisors of S, and we do so.

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 7. *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. □

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 8. *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 3. 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 8, 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 $\text{qf}(R)$, 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 9. *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 $\text{qf}(S)$ 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 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 $r_0, \dots, r_{n-1} \in R$. 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 10. *Let R be an integral domain, and let S be a multiplicative subset of R. If R is integrally closed, so is $S^{-1}R$.*

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

Proposition 11. *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. Exercise. □

It turns out that every UFD is integrally closed.

Proposition 12. *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. $\square$

Example 13. Since $\mathbb{Z}$ is a UFD, then it is integrally closed by Proposition 12. 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 14. 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 $R \subseteq S$ 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 2. *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 3. *For an integral domain R, show that 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.*

Exercise 4. *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* $\mathbb{Z}\big[\frac{1+\sqrt{d}}{2}\big]$ *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