IDEAL THEORY AND PRÜFER DOMAINS

FELIX GOTTI

INTEGRAL EXTENSIONS I

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 \emph{algebraic} (resp., \emph{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 \emph{integral} and the ring \( S \) is called \emph{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 \( 1, s, \ldots, s^{d-1} \). 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 \( \sum_{i=1}^n r_it_i = 1 \). 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

\[
\sum_{i=1}^n (\delta_{ij}s - c_{ij})t_i = 0,
\]
where $\delta_{ij}$ 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 (0.1) simply as $M v = 0$. 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 $\det(xI - C) \in \mathbb{R}[x]$, which is the characteristic polynomial of $C$. Hence $s$ is integral over $R$, which concludes the proof. \hfill \square

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 $s_1, \ldots, s_n \in S$ 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 1 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 1 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 2 guarantees that $R[s_1, \ldots, s_n]$ is an integral extension of $R$. \hfill \square

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 $c_0, \ldots, c_{n-1}$ are integral over $R$, and so $R[c_0, \ldots, c_{n-1}]$ is a finitely generated $R$-module by Proposition 3. Because $t$ is integral over $R[c_0, \ldots, c_{n-1}]$, the ring $R[c_0, \ldots, c_{n-1}, t]$ is also a finitely generated module over $R[c_0, \ldots, c_{n-1}]$. Hence the extension $R \subseteq R[c_0, \ldots, c_{n-1}, t]$ is finite and so integral. In particular, $t$ must be integral over $R$. Thus, $R \subseteq T$ is an integral extension. \hfill \square

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 \( R/(J \cap R) \). \( \square \)

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. 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

\[
\left( \frac{s}{m} \right)^n + \sum_{i=0}^{n-1} \frac{c_i}{m^{n-i}} \left( \frac{s}{m} \right)^i = m^{-n} \left( s^n + \sum_{i=0}^{n-1} c_is^i \right) = 0,
\]

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 \( M^{-1}R \). \( \square \)

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,

\[
s \left( s^{n-1} - \sum_{i=1}^{n-1} c_is^{i-1} \right) c_0^{-1} = 1.
\]

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 \( x^m - \sum_{i=0}^{m-1} d_ix^i \in R[x] \) having \( r^{-1} \) as a root, and so \( r^{-m} = \sum_{i=0}^{m-1} d_ir^{-i} \). After multiplying this equality by \( r^{m-1} \), we obtain that \( r^{-1} = \sum_{i=0}^{m-1} d_ir^{m-1-i} \in R \). Thus, \( R \) is a field. \( \square \)

Corollary 8. Let \( R \) be an integral domain. If the extension \( R \subseteq \text{qf}(R) \) is integral, then \( R \) is a field.

The statement of Proposition 7 is not longer true for integral extensions \( R \subseteq S \), where \( S \) is not an integral domain.
Example 9. 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 2. 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 10. 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 $R$. \hfill \Box

With notation as in Proposition 10, 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 11. 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 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
\[
s^n + \sum_{i=0}^{n-1} (m^{n-i-1} r_i) s^i = m^n \left( q^n + \sum_{i=0}^{n-1} c_i q^i \right) = 0.
\]

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. \hfill \Box

Corollary 12. 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 13. 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) $\Rightarrow$ (b): It follows from Corollary 12.

(b) $\Rightarrow$ (c): This is clear as every maximal ideal is prime.

(c) $\Rightarrow$ (a): Suppose, for the sake of a contradiction, that there exists an element $q \in \text{qf}(R) \setminus R$ 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 $1/\in I$. Let $M$ be a maximal ideal containing $I$. Observe now that $q \not\in R_M$; 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 $q \not\in R_M$. $\square$

It turns out that every UFD is integrally closed.

Proposition 14. Every UFD is integrally closed.

Proof. Let $R$ be a UFD, and take $r/s \in \text{qf}(R) \setminus \{0\}$ 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 $s \in R^*$, whence $r/s = rs^{-1} \in R$. Thus, $R$ is integrally closed. $\square$

Example 15. Since $\mathbb{Z}$ is a UFD, then it is integrally closed by Proposition 14. However, $\mathbb{Z}$ is not integrally closed in $\mathbb{C}$. Let us further show that the integral closure $R := \mathbb{Z}_\mathbb{C}$ 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 $\{1, r, \ldots, r^{n-1}\}$ 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 16. 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 a ring extension, and let $\varphi: S \rightarrow S'$ 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. $\varphi(R_S) \subseteq \varphi(R)_{S'}$.
5. The inclusion in the previous statement may be proper.

Exercise 2. 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 3. 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 4. 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 5. 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 6. 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