# Math 210B Lecture 26 Notes

Daniel Raban

March 13, 2019

## 1 Integral Extensions and Integral Closure

### 1.1 Towers of integral extensions

**Proposition 1.1.** *Let $B = A[\beta_1, \dots, \beta_n]$. The following are equivalent.*

1. *$B$ is integral over $A$.*
2. *Each $\beta_i$ is integral over $A$.*
3. *$B$ is finitely generated as an $A$-module.*

*Proof.* (1) $\implies$ (2): This is by definition.

(2) $\implies$ (3): Recall the lemma that if $B$ is a finitely generated $A$-module and $M$ is a finitely generated $B$-module, then $M$ is a finitely generated $A$-module. So it is enough to show (by recursion) that $A[\beta_1, \dots, \beta_{j+1}]$ is finitely generated over $A[\beta_1, \dots, \beta_j]$ for all $0 \leq j \leq k - 1$. So we reduce to the case $B = A[\beta]$, where $\beta$ is integral over $A$. By a proposition from last time, $B$ is finitely generated over $A$.

(3) $\implies$ (1): $B$ is a faithful $B$-module, and it is finitely generated over $A$. Take $\beta \in B$. Then $B$ is an $A[\beta]$-submodule of $B$ that is faithful and finitely generated over $A$, so $\beta$ is integral over $A$ (by the same proposition from last time). $\square$

**Proposition 1.2.** *If $B/A$ and $C/B$ are integral, then so is $C/A$.*

*Proof.* Let $\gamma \in C$. There exists a monic $f \in B[x]$ with $\gamma$ as a root. Let $B'$ be the $A$-subalgebra of $B$ generated by the coefficients of $f$. By the previous proposition, $B'$ is finitely generated as an $A$-module. Then $B'[\gamma]/B'$ is integral, so $B[\gamma]$ is finitely generated as a $B'$ module. Then $B'[\gamma]$ is finitely generated as an $A$-module. Thus, $\gamma$ is integral over $A$. So $C$ is integral over $A$. $\square$

## 1.2 Integral closure

**Definition 1.1.** The **integral closure** of $A$ in $B$ is the subset of elements in $B$ integral over $A$.

**Proposition 1.3.** *The integral closure of $A$ in $B$ is an $A$-subalgebra of $B$.*

*Proof.* Look at $A[\alpha, \beta]$, where $\alpha, \beta \in B$ are integral over $A$. This is integral over $A$. So $\alpha - \beta$ and $\alpha\beta$ are integral over $A$. $\square$

**Example 1.1.** The integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$.

**Example 1.2.** The integral closure of $\mathbb{Z}$ in $\mathbb{Z}[x]$ is $\mathbb{Z}$.

**Example 1.3.** The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$.

**Definition 1.2.** The **ring of integers** $O_K$ of a number field $K$ is the integral closure of $\mathbb{Z}$ in $K$.

**Remark 1.1.** Integral closure as we have defined it is not absolute. It is relative to the larger ring $B$.

**Definition 1.3.** A domain $A$ is **integrally closed** if it is its own integral closure in its quotient field.

**Example 1.4.** $\mathbb{Z}$ is integrally closed.

**Example 1.5.** Any field is integrally closed.

So this is not the same notion as algebraically closed.

**Proposition 1.4.** *Let $A$ be an integrally closed domain (resp. UFD). Let $K = Q(A)$, and let $L/K$ be a field extension. If $\beta \in L$ is integral over $A$ with minimal polynomial $f \in K[x]$, then $f \in A[x]$.*

*Proof.* Let $A$ be integrally closed. Let $g \in A[x]$ be monic, having $\beta$ as a root. Then $f \mid g$ in $K[x]$. Every root of $g$ in $\overline{K}$ (algebraic closure) is integral over $A$. In $\overline{K}[x]$, $f(x) = \prod_{i=1}^{n}(x - \beta_i)$, where the $\beta_i$ are integral over $A$. So all coefficients of $f$ are integral over $A$ and are in $K$. So $f \in A[x]$, as $A$ is integrally closed.

Let $A$ be a UFD. There exists a $d \in K$ such that $df \mid g$ (since $A$ is a $UFD$). $f$ is monic, so $d \in A$. $g$ is monic, so $d \in A^{\times}$. So $f \in A[x]$. $\square$

**Corollary 1.1.** *UFDs are integrally closed.*

*Proof.* Let $A$ be a UFD, and let $a \in K = Q(A)$ be integral over $A$. $x - a \in K[x]$ is the minimal polynomial. By the proposition, $x - a \in A[x]$. So $a \in A$. $\square$

**Example 1.6.** $\mathbb{Z}[\sqrt{17}]$ is not integrally closed. $\alpha = (1+\sqrt{17})/2$ satisfies $x^2 - x - 4$. So $\mathbb{Z}[\sqrt{17}]$ is not a UFD.

**Proposition 1.5.** *The integral closure of an integral domain $A$ in an integrally closed extension $B/A$ is integrally closed.*

*Proof.* Let $\overline{A}$ be the integral closure of $A$ in $B$. Let $Q = Q(\overline{A})$ be the quotient field of $\overline{A}$. Let $\alpha \in Q$ be integral over $\overline{A}$. $\overline{A}[\alpha]/\overline{A}$ is integral (by a previous proposition). Also, $\overline{A}/A$ is integral, so $\overline{A}[\alpha]/A$ is integral. So $\alpha$ is integral over $A$, and $\alpha \in B$, so $\alpha \in \overline{A}$. $\square$

**Example 1.7.** Let $\overline{\mathbb{Z}}$, the algebraic integers, be the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. Then $\overline{\mathbb{Z}}$ is integrally closed.

**Example 1.8.** Let $K \subseteq \overline{\mathbb{Q}}$ be a number field. Then the ring of integers, $O_K = \overline{Z} \cap K$, is integrally closed.

**Proposition 1.6.** *Let $A$ be an integrally closed domain with quotient field $K$. Let $L$ be an algebraic extension of $K$. Then the integral closure of $B$ of $A$ in $L$ has quotient field $L$.*

$$\begin{tikzcd}
L \arrow[dd, dash] \arrow[dr, dash] & \\
& B \arrow[dd, dash] \\
K \arrow[dr, dash] & \\
& A
\end{tikzcd}$$

*In fact, if $\beta \in L$, then $\beta = b/d$ with $b \in B$, $d \in A$.*

*Proof.* Let $\beta \in L$ be a root of $f = \sum_{i=0}^{n} a_i x_i \in K[x]$, where $a_n = 1$. Let $d \in A \setminus \{0\}$ be such that $df \in A[x]$. Consider $g = d^N f(d^{-1}x) = \sum_{i=0}^{n} d^{n-i} a_i x^i \in A[x]$ is monic, and $g(d\beta) = 0$. So $d\beta \in B$. Since $b := d\beta \in B$, $\beta = b/d$. $\square$

**Theorem 1.1.** *Let $d > 1$ be squarefree.*

$$O_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4. \end{cases}$$

*Proof.* Let $\alpha = a + b\sqrt{d} \in O_{\mathbb{Q}(\sqrt{d})}$, where $a, b \in \mathbb{Q}$. If $b = 0$, then $a \in \mathbb{Z}$. If $b \neq 0$, then $\alpha$ has a minimal polynomial $f = x^2 - 2ax + (a^2 - b^2 d)$. $\alpha$ is integral, so $f \in \mathbb{Z}[x]$. So $2a \in \mathbb{Z}$. We have 2 cases:

1. If $a \in \mathbb{Z}$, then $b^2 d \in \mathbb{Z}$. This implies $b \in \mathbb{Z}$, since $d$ is squarefree.

2. If $a \notin \mathbb{Z}$, then $2a = a', 2b = b' \in \mathbb{Z}$, where $a', b'$ are odd. Then $a^2 - b^2 - d = \frac{(a')^2 - (b')^2 d}{4} \in \mathbb{Z}$. So $(a')^2 \equiv (b')^2 d \pmod 4$. The only squares in $\mathbb{Z}/4\mathbb{Z}$ are 0 and 1. So $f \equiv 1 \pmod 4$. In this case, check that $\frac{1+\sqrt{d}}{2}$ is integral. $\square$