# Lecture 21: Finite & integral extension of rings, I.

1) Finite and integral algebras.
2) Integral closure.

Ref: [AM], Section 5.1.

## 1) Finite and integral algebras.

In what follows $A$ is a commutative ring & $B$ is a commutative $A$-algebra.

The concepts of finite & integral $A$-algebras (and related results) generalize the concepts of finite & algebraic field extensions (and related results). They are important for Algebraic Number theory: the rings of algebraic integers arise as integral (and finite) $\mathbb{Z}$-algebras, these will be defined later (w. some motivation).

### 1.1) Main definitions.

Recall (Sec 1 of Lec 6) that $B$ is finitely generated (as an $A$-algebra) if $\exists\, b_1, \dots b_n \in B$ (generators) s.t. $\forall b \in B\ \exists\, F \in A[x_1, \dots x_n] \mid b = F(b_1, \dots b_n)$.

**Definition:** We say that $B$ is finite over $A$ if it is a finitely generated $A$-module.

In particular, finite $\Rightarrow$ finitely generated but not vice versa: $A[x]$ is finitely generated as an $A$-algebra but is not finite.

**Definition:** Let $B$ be a commutative $A$-algebra.

- $b \in B$ is **integral** over $A$ if $\exists$ monic (i.e. leading coeff $= 1$) $f \in A[x] \,|\, f(b) = 0$.
- $B$ is **integral** over $A$ if $\forall\, b \in B$ is integral (over $A$).

**Exercise:** If $B$ is integral over $A$ & $C$ is a quotient of $B$, then $C$ is integral over $A$.

**Rem:** If $A \hookrightarrow B$ we can view $A$ as a subring of $B$. We call $B$ an extension of $A$ and talk about finite/integral extensions.

## 1.2) Examples

1) Let $A := K$, $B := L$ be fields. Here any homomorphism from $A$ is injective), so $L$ is a field extension of $K$. "$L$ is finite over $K$" is the usual notion from the study of field extensions. And $L$ is integral over $K$ iff $L$ is algebraic over $K$: if $\ell \in L$ & $g \in K[x]$ are s.t. $g(\ell) = 0$ (i.e. $\ell$ is algebraic over $K$) & $g = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ w. $a_n \neq 0$, then set $f = a_n^{-1} g$, it's monic and satisfies $f(\ell) = 0$. So $\ell$ is integral.

2) Let $f(x) \in A[x]$ be a monic polynomial. Then $\bar{x} := x + (f) \in B := A[x]/(f)$ is integral$/A$. Also note that $B$ is finite over $A$ (generated by $1, \bar{x}, \ldots \bar{x}^{d-1}$ for $d := \deg f$).

Below we'll see that $B$ in 2) is integral over $A$.

## 1.3) Finite vs integral.

Reminder: for field extensions: finite $\Leftrightarrow$ [algebraic & finitely generated (as a field extension)].

This generalizes to the ring setting.

**Thm:** Let $B$ be an $A$-algebra. TFAE.

(a) $B$ is integral and finitely generated $A$-algebra.

(b) $B$ is finite over $A$.

The proof of (a) $\Rightarrow$ (b) is based on the following lemma. Note that if $A_1$ is an $A$-algebra & $A_2$ is an $A_1$-algebra, then $A_2$ is also an $A$-algebra: the homomorphism $A \to A_2$ is the composition $A \to A_1 \to A_2$.

**Lemma 1:** Suppose $A_1$ is finite over $A$ & $A_2$ is finite over $A_1$. Then $A_2$ is finite over $A$.

*Proof:* Have $a_1, \dots, a_k \in A_1$ & $b_1, \dots b_\ell \in A_2$ s.t. $A_1 = \operatorname{Span}_A(a_1, \dots a_k)$, $A_2 = \operatorname{Span}_{A_1}(b_1, \dots, b_\ell)$.

Exercise: $A_2 = \operatorname{Span}_A(a_j b_i \mid i = 1, \dots, \ell, j = 1, \dots k)$ $\square$

**Notation:** For an $A$-algebra $B$ & $b_1, \dots b_k \in B$ we write $A[b_1, \dots b_k]$ for the $A$-subalgebra of $B$ generated by $b_1, \dots b_k$.

Proof of (a) $\Rightarrow$ (b): say $B$ is generated by some elements $b_1, \dots b_k$ as an $A$-algebra. We induct on $k$.

Base: $k=1$: $B$ is generated by $b$ as $A$-algebra. $b$ is integral over $A$, let $f \in A[x]$ be monic s.t. $f(b)=0$. Then the unique $A$-algebra homomorphism $A[x] \to B$ w. $x \mapsto b$ factors as $A[x] \twoheadrightarrow A[x]/(f) \to B$. Since $b$ generates $B$, have $A[x] \twoheadrightarrow B \Rightarrow A[x]/(f) \twoheadrightarrow B$. By Example 2 above, $A[x]/(f)$ is fin. gen'd $A$-module $\Rightarrow B$ is fin. gen'd $A$-module.

Step: $B$ is generated by $b_2, \dots b_k$ ($k-1$ el'ts) over $\tilde{A} := A[b_1]$. By inductive assumption, $B$ is finite over $\tilde{A}$. Now we apply Lemma 1 (to $A_1 = \tilde{A}$, $A_2 = B$) to finish the proof. $\square$

To prove (b) $\Rightarrow$ (a) we will need a lemma, a special case of the lemma in Sec 1.1 in Lec 20 (w. $I := A$ there).

**Lemma 2:** Let $M$ be an finitely generated $A$-module, $\varphi: M \to M$ $A$-linear map. Then $\exists$ monic $f(x) \in A[x]$ s.t. $f(\varphi)=0$.

Proof of (b) $\Rightarrow$ (a): Let $B$ be a finite $A$-algebra. It's fin. gen'd as an $A$-algebra b/c module generators are algebra generators. We need to show that $\forall b \in B$ is integral over $A$. In Lemma 2 we take $M := B$, $\varphi: M \to M$, $m \mapsto bm$. We conclude: $\exists$ monic polynomial $f \in A[x]$ s.t. $f(\varphi) = 0 \Rightarrow 0 = f(\varphi)1 = f(b) \Rightarrow b$ is integral over $A$. $\square$

Exercise: Under the assumptions of Thm, if $A$ is Noetherian, then $B$ is Noetherian.

## 1.4) Consequences of Thm.

Corollary 1: i) If $f(x) \in A[x]$ is monic, then $A[x]/(f(x))$ is integral over $A$.

ii) If $B$ is an $A$-algebra & $\alpha \in B$ is integral over $A$, then $A[\alpha]$ is integral over $A$.

Proof: exercise.

Corollary 2 (transitivity of integral algebras): If $B$ is an $A$-algebra integral over $A$, and $C$ is a $B$-algebra integral over $B$, then $C$ is an integral $A$-algebra.

Note that this corollary generalizes the transitivity of algebraic field extensions. The proof is similar to that case.

Proof: Take $\gamma \in C$; it's integral over $B \rightsquigarrow \exists\, b_0, \dots b_{k-1} \in B$ s.t. $\gamma^k - b_{k-1}\gamma^{k-1} - \dots - b_0 = 0$. Let $A[b_0, \dots b_{k-1}]$ denote the $A$-subalgebra of $B$ generated by $b_0, \dots b_{k-1}$. So $\gamma$ is integral over $A[b_0, \dots b_{k-1}] \subset B$. But $b_0, \dots b_{k-1}$ are integral over $A$. We use $(a) \Rightarrow (b)$ of Thm to show that $A[b_0, \dots b_{k-1}]$ is finite over $A$, while $A[b_0, \dots b_{k-1}, \gamma] \subset C$ is finite over $A[b_0, \dots b_{k-1}]$.

Using Lemma 1, we see that $A[b_0, \dots b_{k-1}, \gamma]$ is finite over $A$.

By (b) ⇒ (a) of Thm, $\gamma$ is integral over $A$ and we are done. $\square$

## 2) Integral closure.

**Proposition 1:** Let $B$ be an $A$-algebra. If $\alpha, \beta \in B$ are integral over $A$, then so are $\alpha+\beta$, $\alpha\beta$, $a\alpha$ $(\forall a \in A)$.

*Proof:* Consider subalgebras $A[\alpha] \subset A[\alpha,\beta] \subset B$, $A[\alpha]$ is integral over $A$, $A[\alpha,\beta]$ is integral over $A[\alpha]$ thx to Cor 1.

By Corollary 2, $A[\alpha,\beta]$ is integral over $A$. Since $\alpha\beta$, $\alpha+\beta$, $a\alpha \in A[\alpha,\beta]$, they are integral over $A$. $\square$

**Corollary/definition:** The elements in $B$ integral over $A$ form an $A$-subalgebra of $A$ called the integral closure of $A$ in $B$.

We'll denote the integral closure by $\bar{A}^B$.

**Example:** If $A = K \subset B = L$ are fields, then $\bar{K}^L$ is the algebraic closure of $K$ in $L$.

**Proposition 2:** The integral closure of $\bar{A}^B$ in $B$ is $\bar{A}^B$.

Proof: apply Corollary 2, left as exercise.

**Definition:** Let $K$ be a finite field extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in $K$ is called the ring of algebraic integers in $K$.

Remark: The rings of algebraic integers are the most important integral closures. The reason is they are of crucial importance for Number theory as they appear in various classical number theoretic questions, e.g.

- the claim that a prime $p$ is the sum of two squares if $p \equiv 1 \mod 4$ is proved using Gaussian integers, $\mathbb{Z}[\sqrt{-1}]$, in particular using that it's a UFD.
- integer solutions to $a^2 - db^2 = \pm 1$ are closely related to invertible elements in the ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$.
- The unique factorization property of the ring of algebraic integers in $\mathbb{Q}(\sqrt[p]{1})$ implies the Fermat Last theorem for deg $p$.