Lecture 11: Finite & integral extension of rings, II

1) Finite and integral algebras, cont'd
2) Integral closure.

Ref: [AM], Sections 5.1, 5.3

1) Finite and integral algebras.

Last time, we have stated the following theorem.

Thm: Let B be an A-algebra. TFAE
(a) B is integral and finitely generated A-algebra.
(b) B is finite over A.

We've proved (a) $\Rightarrow$ (b) & our first task now is to prove (b) $\Rightarrow$ (a). Then we deduce some corollaries of the theorem parallel to those in the case of field extensions.

1.1) Caley-Hamilton type lemma

This is the most essential ingredient in proving (b) $\Rightarrow$ (a).

Lemma: Let M be a finitely generated A-module, $I \subset A$ an ideal, $\varphi: M \to M$ A-linear map s.t. $\varphi(M) \subset IM$. Then there is a polynomial $f(x) \in A[x]$ of the form

(*) $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ with $a_k \in I^k$ $\forall k$

s.t. $f(\varphi) = 0$.

Proof: Note that M upgrades to an $A[x]$-module w. x acting by φ. Pick generators $m_1,\dots m_n \in M$. We have elements $a_{ij} \in I$, $i=1,\dots n$ s.t.

$$(1) \qquad x m_i = \sum_{j=1}^{n} a_{ij} m_j$$

Form the matrix $X = xI - (a_{ij}) \in Mat_n(A[x]) \rightsquigarrow det(X) \in A[x]$. Note that $det(X)$ is a polynomial $f(x)$ satisfying $(*)$ (exercise: hint – use that $det(X) = \sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} x_{i\sigma(i)}$ & $x_{ij} \in \delta_{ij} x + I$). Also note that $det(X)$ acts by $f(\varphi)$ on M. So it's enough to show that $det(X)$ acts by 0.

Let $\vec{m} = (m_1,\dots m_n)$ viewed as a column vector. Then $X\vec{m} = \vec{0}$ by (1). Consider the "adjoint" matrix $X' = (x'_{ij})$ w. $x'_{ij} = (-1)^{i+j} \cdot det$ (the matrix obtained from X by removing row #i & column #j) so that $X'X = det(X) \cdot Id$. Then $X\vec{m} = \vec{0} \Rightarrow det(X)\vec{m} = X'X\vec{m} = \vec{0} \Rightarrow$

$$(2) \qquad f(\varphi) m_i = det(X) m_i = 0 \quad \forall i.$$

Since $m_1,\dots m_n$ span the A- (and hence $A[x]$-) module M, (2) $\Rightarrow f(\varphi)m = det(X)m = 0 \quad \forall\, m \in M$. This finishes the proof $\square$

Rem: Caley-Hamilton lemma in Linear algebra is the claim that for a finite dimensional vector space V & a linear operator $\varphi: V \to V$ we have $\chi(\varphi) = 0$, where χ is the characteristic polynomial. It's proved similarly to the lemma above.

1.2) Proof of (b) $\Rightarrow$ (a) Let B be a finite A-algebra. It's finitely generated as an A-algebra b/c module generators are algebra generators. It remains to show that $\forall b \in B$ is integral over A. In Lemma we take $M := B$, $\varphi: M \to M$, $m \mapsto bm$, $I = A$. 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.

1.2) 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 $B \rightsquigarrow \exists\, b_0, \ldots b_{k-1} \in B$ s.t. $\gamma^k - b_{k-1}\gamma^{k-1} - \ldots - b_0 = 0$. So γ is integral over $A[b_0, \ldots b_{k-1}] \subset B$. 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 $A[b_0, \dots b_{k-1}]$ so $A[b_0, \dots b_{k-1}, \gamma]$ is finite over A. By (b) $\Rightarrow$ (a) of Thm, γ is integral over A and we are done. $\square$

2) Integral closure.

2.1) Definition & basic properties

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 B 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.

2.2) Rings of algebraic integers.

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.

Example: Let $K=\mathbb{Q}$. Then $\overline{\mathbb{Z}}^{\mathbb{Q}}=\mathbb{Z}$. Indeed, assume $\frac{a}{b}\in\overline{\mathbb{Z}}^{\mathbb{Q}}$ ($\frac{a}{b}\in\mathbb{Z}$, $GCD(a,b)=1$) $\Rightarrow \exists!\ f(x)=x^n+c_{n-1}x^{n-1}+\ldots+c_0$ w. $c_i\in\mathbb{Z} \mid f(\frac{a}{b})=0 \Leftrightarrow$ $a^n+c_{n-1}a^{n-1}b+\ldots+c_0b^n=0 \Rightarrow a^n \vdots b \Rightarrow [GCD=1]\ b=\pm1 \Rightarrow \frac{a}{b}\in\mathbb{Z}$.

Let's consider a special case $K=\mathbb{Q}(\sqrt{d})$ w. square-free d (= d not divisible by p^2 $\forall$ prime p).

Proposition: Let d be a square-free integer, and $K=\mathbb{Q}(\sqrt{d})$. Then
$$\overline{\mathbb{Z}}^K=\begin{cases}\mathbb{Z}[\sqrt{d}] & \text{if } d\equiv 2 \text{ or } 3 \bmod 4\\ \{a+b\sqrt{d} \mid a,b\in\mathbb{Z} \text{ or } a,b\in\frac{1}{2}+\mathbb{Z}\} & \text{if } d\equiv 1 \bmod 4.\end{cases}$$

Proof: We need to understand when $\beta=a+b\sqrt{d}$ ($a,b\in\mathbb{Q}$), is integral over $\mathbb{Z}$.

Claim: TFAE

(i) β is integral over $\mathbb{Z}$,

(ii) $2a,\ a^2-b^2d\in\mathbb{Z}$.

Proof of Claim: Set $\bar\beta := a - b\sqrt{d}$. Note that $\beta+\bar\beta = 2a$, $\beta\bar\beta = a^2-b^2d \in \mathbb{Q}$. So $(x-\beta)(x-\bar\beta) = x^2-2ax+(a^2-b^2d)$, hence (ii) $\Rightarrow$ (i).

Now assume (i). Note that $\beta \mapsto \bar\beta$ is a ring homomorphism $\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$. So for $f(x) \in \mathbb{Z}[x]$ we have $f(\bar\beta) = \overline{f(\beta)}$. Hence if $f(\beta)=0$, then $f(\bar\beta)=0$. In particular, if β is integral over $\mathbb{Z}$, then $\bar\beta$ is integral. By Proposition 1 of Section 2 of Lecture 9, $\beta+\bar\beta, \beta\bar\beta \in \mathbb{Q}$ are integral over $\mathbb{Z}$. By Example, elements of $\mathbb{Q}$ integral over $\mathbb{Z}$ are integers. (ii) follows. $\square$

Now we get back to the proof of Proposition. The following claim is elementary Number theory.

Exercise If $d \equiv 2$ or $3 \bmod 4$, then (ii) $\Leftrightarrow$ $a, b \in \mathbb{Z}$; if $d \equiv 1 \bmod 4$, then (ii) $\Leftrightarrow$ either $a, b \in \mathbb{Z}$ or $a, b \in \mathbb{Z}+\frac{1}{2}$.

Claim & exercise finish the proof of Proposition. $\square$

Remark: The rings of algebraic integers are the most important integral closures. The reason: 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 $p \equiv 1 \bmod 4$ 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 $\mathbb{Q}(\sqrt{d})$.

• Let $K = \mathbb{Q}(\sqrt[p]{1})$. If $\overline{\mathbb{Z}}^K$ is UFD, then Fermat Last theorem holds for deg p.

2.3) Normal domains.

Let A be a domain.

Definition:

A is normal if it coincides with its integral closure in the fraction field $\mathrm{Frac}(A)$.

Special cases:

1) L is a field, $A \subset L$ is a subring. Claim: $\bar{A}^L$ is normal. Indeed, $\bar{A}^L$ is integr. closed in L & $\mathrm{Frac}(\bar{A}^L) \subset L \Rightarrow$ $\bar{A}^L$ closed in $\mathrm{Frac}(\bar{A}^L)$.

In particular, any ring of algebraic integers is a normal domain. As a concrete example, for square-free d, $\mathbb{Z}[\sqrt{d}]$ is normal iff $d \equiv 2$ or $3 \bmod 4$ (for $d \equiv 1 \bmod 4 \Rightarrow \mathbb{Z}[\sqrt{d}] \subsetneq$ its int. closure in $\mathbb{Q}(\sqrt{d})$).

2) UFD $\Rightarrow$ normal. The argument is similar to the case of $\mathbb{Z}$ & is left as exercise.