Lecture 22: Finite & integral extensions of rings, II.

1) Integral closures, cont'd.
2) Noether normalization lemma.

Refs: [AM], Sec 5.3; [E], Sec 4.2

1.0) Recap.

A is comm've ring, B is an A-algebra. Recall (Sec 2 of Lec 21) the integral closure of A in B:
$\overline{A}^B = \{b \in B \mid b \text{ is integral over } A\}$, A-subalgebra in B.

1.1) Normal domains.

Let A be a domain.

Definition:
i) The normalization of A is $\overline{A}^{\operatorname{Frac}(A)}$, integral closure of A in its fraction field $\operatorname{Frac}(A)$.
ii) A is normal if A coincides w. its normalization.

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

In particular, any ring of algebraic integers ($\overline{\mathbb{Z}}^K$, where K is a finite field extension of $\mathbb{Q}$, Sec 2 in Lec 21) is a normal domain.

Exercise: Let K be a finite field extension of $\mathrm{Frac}(A)$. Prove that $\mathrm{Frac}(\bar{A}^K)=K$ (hint: for any algebraic (over $\mathrm{Frac}(A)$) $\alpha\in K$ $\exists\, a\in A$, $a\neq 0$, s.t. $a\alpha$ is integral over A).

2) UFD $\Rightarrow$ normal: let A be UFD & $\frac{a}{b}\in \mathrm{Frac}(A)$ w. coprime $a,b\in A$. Need to show: $\frac{a}{b}$ is integral over A $\Rightarrow$ $\frac{a}{b}\in A$ i.e. b is invertible. Let $f(x)=x^k+c_{k-1}x^{k-1}+\ldots+c_1x+c_0$ $(c_i\in A)$ be s.t. $f(\frac{a}{b})=0 \Rightarrow 0=b^kf(\frac{a}{b})=a^k+\sum_{i=0}^{k-1}c_ia^ib^{k-i}$. The sum is divisible by b. So $a^k \vdots b$. Since a & b are coprime, this implies that b is invertible.

1.2) Algebraic integers in $\mathbb{Q}(\sqrt{d})$.

Proposition: Let d be a square-free integer, and $K=\mathbb{Q}(\sqrt{d})$. Then

$$\bar{\mathbb{Z}}^K=\begin{cases}\mathbb{Z}[\sqrt{d}] & \text{if } d\equiv 2 \text{ or } 3 \bmod 4\\ \{a+b\sqrt{d}\mid a,b\in\mathbb{Z} \text{ or } a,b\in\frac{1}{2}+\mathbb{Z}\} & \text{if } d\equiv 1 \bmod 4.\end{cases}$$

Proof: We need to understand when $\beta=a+b\sqrt{d}\in\mathbb{Q}(\sqrt{d})$ $(a,b\in\mathbb{Q})$, 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 $f(\bar\beta)=\overline{f(\beta)}$. So 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 $\mathbb{Z}$. But $\mathbb{Z}$ is UFD, hence normal. So 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. $\square$

Using Proposition and 1) from Section 1.1, we get

Corollary: i) $\mathbb{Z}[\sqrt{d}]$ is normal $\Leftrightarrow d\equiv 2$ or $3 \bmod 4$.
If $d\equiv 1 \bmod 4$, then the normalization of $\mathbb{Z}[\sqrt{d}]$ is $\{a+b\sqrt{d}\mid a,b\in\mathbb{Z} \text{ or } a,b\in\mathbb{Z}+\frac{1}{2}\}$.

ii) $\mathbb{Z}[\sqrt{-5}]$ is normal but not UFD.

2) Noether normalization lemma

Recall that a finitely generated field extension is a finite ext'n of a purely transcendental one. Here's an analog for rings.

Theorem (Noether). Let $\mathbb{F}$ be a field, A a fin. generated $\mathbb{F}$-algebra. Then $\exists$ inclusion $\mathbb{F}[x_1,\dots x_m] \hookrightarrow A$ s.t. A is finite over $\mathbb{F}[x_1,\dots x_m]$ (for some $m \geqslant 0$).

We'll only prove this when $\mathbb{F}$ is infinite, where a proof is easier. For a general case, see [E], Lemma 13.2 & Theorem 13.3.

Key lemma: Assume $\mathbb{F}$ is infinite, $F \in \mathbb{F}[x_1,\dots x_n]$ be nonzero. The $\exists$ $\mathbb{F}$-linear combinations $y_1,\dots,y_{n-1}$ of variables $x_1 \dots x_n$ s.t. $\mathbb{F}[x_1,\dots x_n]/(F)$ is finite over $\mathbb{F}[y_1,\dots,y_{n-1}]$.

Proof of lemma:

$F = f_0 + \dots + f_k$, f_i is homogeneous of $\deg = i$, $f_k \neq 0$.

Special case: $a := f_k(0,\dots,0,1) \neq 0$. Note that a is the coeff't of x_n^k in F, & $F = a x_n^k + \sum_{i=0}^{k-1} g_i(x_1,\dots x_{n-1}) x_n^i$, where $g_i \in \mathbb{F}[x_1,\dots x_{n-1}]$, Replacing F w. $a^{-1}F$, can assume f_k is monic as an element in $\mathbb{F}[x_1,\dots x_{n-1}][x_n]$. Example 2 in Sec 1.2 of Lec 21, $\mathbb{F}[x_1,\dots x_n]/(F)$ is finite over $\mathbb{F}[x_1,\dots x_{n-1}]$ and we set $y_i := x_i$.

General case: $f_k \neq 0$ & $\mathbb{F}$ is infinite $\Rightarrow f_k(a_1,\dots a_n) \neq 0$ for some $a_i \in \mathbb{F}$. Pick invertible $\varphi \in Mat_{n\times n}(\mathbb{F})$ s.t.

$\varphi\begin{pmatrix}0\\ \vdots \\ 0\\ 1\end{pmatrix} = \begin{pmatrix}a_1\\ \vdots \\ a_n\end{pmatrix}$. Consider $F^{\varphi} = F\circ\varphi$ as a function $\mathbb{F}^n \to \mathbb{F}$ (polynomial obtained from F by linear change of variables). Then $f_k^{\varphi}(0,\dots,0,1) = f_k(a_1,\dots a_n) \neq 0$. So

$\mathbb{F}[x_1,\dots x_n]/(F^{\varphi})$ is finite over $\mathbb{F}[x_1,\dots,x_{n-1}]$, hence

$\wr\uparrow \varphi^{-1}$, linear change of variables.

$\mathbb{F}[x_1,\dots x_n]/(F)$ is finite over $\mathbb{F}[y_1,\dots y_{n-1}]$ w.

$\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix} := \varphi^{-1}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$ $\square$

Proof of Thm: Pick <u>minimal possible</u> m s.t. $\exists\ \varphi: \mathbb{F}[x_1,\dots x_m] \to A$ s.t. A is finite over $\mathbb{F}[x_1,\dots,x_m]$. This makes sense b/c A is finitely generated, hence a quotient of $\mathbb{F}[x_1,\dots x_n]$ for some n. It remains to prove the following:

Claim: φ is injective.

Proof of claim:

Assume the contrary: $\exists\ F\in\ker\varphi$, $F\neq 0$. By Key Lemma $\mathbb{F}[x_1,\dots x_m]/(F)$ is finite over $\mathbb{F}[y_1,\dots y_{m-1}]$ & A is finite over $\mathbb{F}[x_1,\dots x_m]/(F)$ (b/c φ factors through $\mathbb{F}[x_1,\dots x_m]/(F)$). By Lemma 1 in Section 1.3 in Lecture 21 A is finite over $\mathbb{F}[y_1,\dots,y_{m-1}]$. Contradiction w. choice of m. $\square$

Important corollary: Let A be a fin. gen'd $\mathbb{F}$-algebra. If A is a field, then $\dim_{\mathbb{F}} A < \infty$.

Proof: By Thm, $\mathbb{F}[x_1, \dots x_m] \hookrightarrow A$ s.t. A is finite over $\mathbb{F}[x_1, \dots x_m]$. Need to show $m=0$. Assume the contrary. Since A is a field, the image of x_1 is invertible, so $\mathbb{F}[x_1, \dots x_m] \hookrightarrow A$ extends to $\mathbb{F}[x_1, \dots x_m] \hookrightarrow \mathbb{F}[x_1^{\pm 1}, x_2, \dots, x_m] \xrightarrow{\tau} A$. The homomorphism τ is injective (if $\tau(x_1^{-i} f) = 0$, then $\tau(f) = 0$). Note that A is finitely generated over $\mathbb{F}[x_1, \dots, x_m]$ & $\mathbb{F}[x_1, \dots, x_m]$ is Noetherian $\Rightarrow$ $\mathbb{F}[x_1^{\pm 1}, x_2, \dots x_m]$ is a finitely generated $\mathbb{F}[x_1, \dots x_m]$-module.

But this is not true: the $\mathbb{F}[x_1, \dots, x_m]$-submodule generated by $x_1^{-d_i} F_i$, $i = 1, \dots, \ell$ is contained in $x_1^{-d} \mathbb{F}[x_1, \dots x_m]$, w. $d = \max(d_i)$, a proper subset of $\mathbb{F}[x_1^{\pm 1}, x_2, \dots x_n]$. Contradiction w. $m > 0$. $\square$

Exercise: Let $\mathbb{F}$ be algebraically closed. Prove that $\forall$ max. ideal $\mathfrak{m} \subset \mathbb{F}[x_1, \dots x_n]$ $\exists$ $(a_1, \dots a_n) \in \mathbb{F}^n \mid \mathfrak{m} = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$.

Remark: Important Corollary is an elegant statement but its usefulness for us is that we'll use it to prove Hilbert's Nullstellensatz in Lec 23 (it's sometimes called "weak Nullstellensatz).