Lecture 21.

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

Bonus:
1) Proof of Thm (I) in Section 1.3.
2) Cohen-Macaulay algebras.

[AM], Section 5.3; [E], Sections 4.2, 13.1, 13.3; E. Vinberg, A course in Algebra, GSM 56, Section 9.5.

1) A is comm've unital ring, B is an A-algebra. Recall (Lec 20) the integral closure $\bar{A}^B = \{b \in B \mid b \text{ is integral over } A\}$, A-subalgebra in B.

1.1) Normal domains.

Let A be a domain $\rightsquigarrow$ fraction field $\mathrm{Frac}(A) \supset A$.

Definition:
i) The <u>normalization</u> of $A := \bar{A}^{\mathrm{Frac}(A)}$, integral closure of A in $\mathrm{Frac}(A)$.
ii) A is <u>normal</u> if A coincides w. its normalization.

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 $\mathrm{Frac}(\bar{A}^L)$.

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 $f(x) = x^k + c_{k-1}x^{k-1} + \ldots + c_1 x + c_0$ $(c_i \in A)$ be s.t. $f(\frac{a}{b}) = 0 \Rightarrow 0 = b^k f(\frac{a}{b}) = a^k + \underbrace{\sum_{i=0}^{k-1} c_i a^i b^{k-i}}_{\text{divisible by } b}$
$\Rightarrow a^k \vdots b$. But $GCD(a,b) = 1 \Rightarrow b$ is invertible.

3) If A is normal $\Rightarrow A[x]$ is normal (see HW5, Problem 6)

Exercise: Let L be a field, $A_i \subset L$ normal subrings ($i \in I$). Then $\bigcap_{i\in I} A_i$ is also normal.

1.2) Example of computation of integral closure.

Want to compute the integral closure of $A = \mathbb{Z}$ ($\operatorname{Frac} A = \mathbb{Q}$), in $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ is a square-free number.

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

Lemma: TFAE

(i) β is integral over $\mathbb{Z}$

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

Proof: (ii) $\Rightarrow$ (i): $\beta^2 - (2a)\beta + (a^2 - b^2 d) = 0$, Ex 2 in Lec 20, Sect 1.1.

(i) $\Rightarrow$ (ii): $\bar{\beta} := a - b\sqrt{d}$; if for $f(x) \in \mathbb{Z}[x]$ have $f(\beta) = 0$ $\Rightarrow f(\bar{\beta}) = 0$. So $\bar{\beta}$ is also integral over $\mathbb{Z}$ $\Rightarrow$ $\beta + \bar{\beta} = 2a$, $\beta\bar{\beta} = a^2 - b^2 d \in \mathbb{Q}$ are integral over $\mathbb{Z}$. Since $\mathbb{Z}$ is UFD $\Rightarrow$ normal, i.e. all elements of $\mathbb{Q}$ integ'l over $\mathbb{Z}$ are in $\mathbb{Z}$ $\Rightarrow$ $2a,\ a^2 - b^2 d \in \mathbb{Z}$ $\square$

Exercise (elementary Number thy): 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 $a, b \in \mathbb{Z} + \frac{1}{2}$.

Corollary: i) $\mathbb{Z}[\sqrt{d}]$ is normal $\Leftrightarrow$ $d \equiv 2$ or $3 \bmod 4$.

If $d \equiv 1 \bmod 4$, then the normal'n 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.

1.3) Finiteness of integral closures.

Let A be a domain, $K = \mathrm{Frac}(A)$, $K \subset L$ finite field ext'n.
Q: Is $\bar{A}^L$ finite over A?
A: It's complicated...

Theorem: Assume that <u>one</u> of the following holds:
(I) A is Noeth'n & normal, char $K = 0$.
(II) A is a fin. gen'd algebra over a field or over $\mathbb{Z}$.
Then $\bar{A}^L$ is finite over A.
Proof under (I) will appear as a bonus.

Example: let $A = \mathbb{Z}$, L is a finite extension of $\mathbb{Q}$. The ring $\bar{A}^L$ is called <u>the ring of algebraic integers</u> in L (crucially important for Alg. Number th'y). Both (I) & (II) apply, so Thm $\Rightarrow$ $\bar{A}^L$ is finite over $\mathbb{Z}$, i.e. is a fin. gen'd abelian group. Since $\bar{A}^L$ is domain & $\mathbb{Z} \subset \bar{A}^L \Rightarrow \bar{A}^L$ is torsion-free as abelian group. So $\bar{A}^L$ is a free abelian gr'p of rank $= \dim_{\mathbb{Q}} L$, which is proved using the following exercise

Exercise: Let A be an arbitrary domain, $K = \mathrm{Frac}(A)$, L is finite field ext'n of $K \rightsquigarrow \bar{A}^L$; $S = A \setminus \{0\}$ - localizable subset $\rightsquigarrow (\bar{A}^L)_S \longrightarrow L$ (ring homom'm). Claim: this is an isomorphism.

In our example, rank of $\bar{A}^L = \dim_{\mathbb{Q}} (\bar{A}^L)_S$.

2) Noether normalization lemma ("normalization" here has nothing to do w. normalization from Section 1.1).

Reminder: let $K \subset L$ be fin. generated field extension. Then $\exists$ L' between K & L s.t

- L is finite over L'
- $L' = K(x_1,\dots,x_m)$ (field of rational functions).

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 it 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: $f_k(0,\dots,0,1) \neq 0 \iff x_n^k$ appears in f_k w. nonzero coeff't. Now view $F \in \mathbb{F}[x_1,\dots x_{n-1}][x_n]$, has leading coeff't $\neq 0$ i.e. invertible in $\mathbb{F}[x_1 \dots x_{n-1}] \Rightarrow$ class of x_n in $\mathbb{F}[x_1,\dots x_n]/(F)$ is integral over $\mathbb{F}[x_1,\dots x_{n-1}]$. By the theorem in Sect. 1.2) of

Lecture 20, $\mathbb{F}[x_1,\dots x_n]/(F)$ is finite over $\mathbb{F}[x_1,\dots x_{n-1}]$. 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 $\varphi \in \mathrm{Mat}_{n\times n}(\mathbb{F})$ 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 $\mathbb{F}^n \to \mathbb{F}$ (polyn'l 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

$$\begin{array}{l}\mathbb{F}[x_1,\dots x_n]/(F^{\varphi}) \text{ is finite over } \mathbb{F}[x_1,\dots x_{n-1}], \text{ hence}\\ \quad\wr\!\uparrow \varphi^{-1}\\ \mathbb{F}[x_1,\dots x_n]/(F) \text{ is finite over } \mathbb{F}[y_1,\dots y_{n-1}] \text{ w.}\end{array}$$

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

$\square$

Proof of Thm: Let $X = \{n \in \mathbb{Z}_{\geq 0} \mid \exists\ \mathbb{F}\text{-algebra homom'm } \mathbb{F}[x_1,\dots x_n] \longrightarrow A \text{ s.t. } A \text{ is finite over } \mathbb{F}[x_1,\dots x_n]\}$; $X \neq \emptyset$ b/c A is finitely generated & so $\mathbb{F}[x_1,\dots x_n] \twoheadrightarrow A$ for some n.

Set $m := \min X \rightsquigarrow \varphi: \mathbb{F}[x_1,\dots x_m] \longrightarrow A$ s.t. A is finite over $\mathbb{F}[x_1,\dots,x_m]$.

Claim: φ is injective.

Assume 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 Corollary 3 of Section 1.2 in Lecture 20 A is finite over $\mathbb{F}[y_1,\dots,y_{m-1}]$. Contradiction w. choice of m. $\square$

Important corollary: Let $\mathbb{F}$ be an $\overbrace{\text{infinite}}^{\text{can be removed}}$ field, 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, $\mathbb{F}[x_1,\dots x_m] \hookrightarrow A$ extends to $\mathbb{F}(x_1,\dots,x_m) \hookrightarrow A$, in particular, extends to $\mathbb{F}[x_1^{\pm 1}, x_2,\dots x_m] \hookrightarrow A$:

$$\mathbb{F}[x_1,\dots x_m] \hookrightarrow \mathbb{F}[x_1^{\pm 1}, x_2,\dots,x_m] \hookrightarrow A.$$

A is fin. gen'd over $\mathbb{F}[x_1,\dots,x_m]$ & $\mathbb{F}[x_1,\dots,x_m]$ is Noeth'n $\Rightarrow$ $\mathbb{F}[x_1^{\pm 1}, x_2,\dots x_m]$ is fin. gen'd over $\mathbb{F}[x_1,\dots,x_m]$. But this is not true: the $\mathbb{F}[x_1,\dots,x_m]$-module 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. $d=\max(d_i)$. Contradiction w. $m>0$. $\square$

Bonus 1: Proof of Theorem in Section 1.3 under assumption (I).

Proof: Let $\dim_K L = n$. Every element $\alpha \in L$ gives the K-linear operator, say, m_α, on L via multiplication. So for $\alpha \in L$ it makes sense to speak about $tr(\alpha) := tr(m_\alpha) \in K$.

Step 1: We claim that for $\alpha \in \bar{A}^L$ we have $tr(\alpha) \in A$. Let $f(x) \in A[x]$ be a monic polynomial w $f(\alpha)=0$. Choose an algebraic extension $\tilde{L}$ of L where $f(x)$ decomposes into linear factors. All eigenvalues of m_α are roots of $f(x)$, hence are integral over A. Therefore $tr(\alpha)$ – the sum of eigenvalues – is integral over A. But $tr(\alpha) \in K$ and, since A is normal, we see $tr(\alpha) \in A$.

Step 2: For $\alpha, \beta \in L$ define $(\alpha, \beta) := tr(\alpha\beta)$. This is a symmetric K-bilinear form $L \times L \to K$. We claim that since char $K = 0$, this bilinear form is nondegenerate. More precisely, for $u \in L \setminus \{0\}$ $\exists\, m \geq 0$ s.t. $(u, u^{m-1}) = tr(u^m) \neq 0$. Let $u_1 = u, u_2, \ldots u_n$ be the eigenvalues of m_u counted w. multiplicities. Then $tr(u^m) = \sum_{i=1}^n u_i^m$. If the r.h.s.'s are 0 for all m, then, thx to char $\tilde{L}$ = char $K = 0$, we get $u_1 = \ldots = u_n = 0$, which is impossible since $u \neq 0$.

Step 3: Thx to the exercise in Section 1.3, we can find a K-basis $\ell_1, \ldots \ell_n$ of L w $\ell_i \in \bar{A}^L$. Let $\ell^1, \ldots, \ell^n$ be the dual basis w.r.t. $(\cdot, \cdot)$, i.e $tr(\ell_i \ell^j) = \delta_{ij}$, it exists b/c $(\cdot, \cdot)$ is nondegenerate. Let $M := \mathrm{Span}_A (\ell^1, \ldots, \ell^n)$. Note that, for $\alpha \in \bar{A}^L$ we have $\alpha = \sum_{i=1}^n (\alpha, \ell_i) \ell^i$. We have $(\alpha, \ell_i) = tr(\alpha \ell_i) \in A$ b/c $\alpha \ell_i \in A$. So $\alpha \in M \Rightarrow \bar{A}^L \subset M$. But A is Noetherian, and M is manifestly finitely generated A-module. Hence $\bar{A}^L$ is a finitely generated A-module and we are done. □

Corollary: Theorem is also true under assumption (II) if A is a finitely generated $\mathbb{F}$-algebra & char $\mathbb{F} = 0$.

Sketch of proof: Thanks to the Noether normalization lemma we can replace A w. $\mathbb{F}[x_1, \ldots x_m]$ for some m, this doesn't change $\bar{A}^L$ (exercise). Now we are in the situation of (I) of the theorem. $\square$

For a proof of (II) w. a finitely generated algebra over an arbitrary field, see [E], Section 13.3.

Bonus 2: Cohen-Macaulay algebras.

The Noether normalization lemma, NNL, tells us that, for a finitely generated $\mathbb{F}$-algebra A, there's an embedding $\mathbb{F}[x_1,\dots x_m] \hookrightarrow A$ s.t. A is a finitely generated $\mathbb{F}[x_1\dots x_m]$-module. This invites the following:

Question: Can we choose $x_1,\dots x_m$ so that the $\mathbb{F}[x_1,\dots x_m]$-module A is "nice," e.g. free? Or projective?

Fact: If A is a projective $\mathbb{F}[x_1,\dots x_m]$-module for some choice of an embedding as in NNL, then it's projective for every such embedding.

Definition: A is called Cohen-Macaulay (CM) if the condition from Fact holds for A.

Being CM is a very nice property, perpendicular to being normal - which is another very nice property.

Example: $\mathbb{F}[x_1,\dots x_m]$ is CM (there's an obvious embedding making it into a projective $\mathbb{F}[x_1,\dots x_m]$-module).

To produce a more general family of examples we need a definition.

Definition (regular sequence). A sequence of elements $a_1,\dots a_k$ in a comm've ring A is called regular if

- the ideal $(a_1, \dots, a_k) \neq A$, and
- $\forall i = 0, \dots, k-1$, the class of a_{i+1} in $A/(a_1 \dots a_i)$ is not a zero divisor.

This definition establishes some interesting properties. For example, the order of a_i's is not important for being regular.

Fact: Let $f_1, \dots, f_k \in \mathbb{F}[x_1, \dots x_m]$ form a regular sequence. Then $\mathbb{F}[x_1, \dots, x_n]/(f_1, \dots f_k)$ is CM.

Regular sequences are studied in detail in [E], Section 17, and CM rings are studied in [E], Section 18.