Lecture 5, IIII

Lemma 3.23: Consider ring extensions $R \subset S \subset T$. If $R \subset S$ and $S \subset T$ (1)
are integral, so is $R \subset T$.

Proof: Let $t \in T$. Then there is $f = X^n + s_{n-1}X^{n-1} + \dots + s_1 X + s_0 \in S[X]$ with
$f(t) = 0$. Let $S' := R[s_0, \dots, s_{n-1}] \subset S$. Since $R \subset S$ is integral, each s_i
is integral over $R \rightsquigarrow S'$ f.g. R-module by Cor 3.20.
Since t integral over S' ($s_i \in S'$) $\Rightarrow S'[t]$ f.g. S'-module by Cor 3.20
$\Rightarrow S'[t]$ f.g. R-module (S' f.g. R-module)
$\Rightarrow t$ integral over R by Thm 3.19. $\square$

3.4 Ring of integers is integrally closed

Def 3.24: $R \subset S$ a ring extension. Say that R is <u>integrally closed</u> in S if
$R^{int,S} = R$, i.e. if $\alpha \in S$ integral over $R \Rightarrow \alpha \in R$.

Lemma 3.25: The integral closure of R in S is integrally closed in S.

Proof:
Note: $R' := R^{int,S}$ is contained in S and $R \subset R'$ is integral.
So, if $\alpha \in S$ integral over R' $\Rightarrow$ integral over R by Lemma 3.23.
$\rightarrow \alpha \in R'$.
$\rightarrow R'$ integrally closed.
$\square$

Ex 3.26:
a) $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$
b) $\mathbb{Z}[i] = \mathbb{Z}^{int, \mathbb{Q}(i)}$ is integrally closed in $\mathbb{Q}(i)$.
c) $\mathcal{O}_L = \mathbb{Z}^{int,L}$ ring of integers in a number field L is integrally closed in L.

Def 3.27: Let R be an integral domain. The <u>field of fractions</u> (or <u>quotient field</u>) of R is

$$Q(R) := \left\{ \frac{r}{r'} \;\middle|\; r, s \in R, r' \neq 0 \right\}$$ with the obvious addition and multiplication

$$\left(\text{Formally: } Q(R) = \{(r_1, r_1') \mid r_1, r_1' \in R, r_1' \neq 0\}/\sim \text{ with } (r_1, r_1') \sim (r_2, r_2') \text{ iff } r_1 r_2' = r_1' r_2 \right)$$

Ex 3.28:

a) $Q(\mathbb{Z}) = \mathbb{Q}$

b) $Q(\mathbb{Z}[i]) = \mathbb{Q}(i)$: $(a+bi)^{-1} = \dfrac{1}{a^2+b^2} + \dfrac{1}{a^2+b^2} \cdot i \in \mathbb{Q}(i)$

c) $Q(K[X]) = \left\{ \frac{f}{g} \;\middle|\; f, g \in K[X], g \neq 0 \right\}$: <u>rational function field</u>

Remark 3.29: The map $R \to Q(R)$, $r \mapsto \frac{r}{1}$, is injective.
$Q(R)$ is the smallest field containing R.

Def 3.30: R an integral domain, $K := Q(R)$.
The <u>integral closure</u> (or <u>normalization</u>) of R is $R^{\mathrm{int},K}$.
R is <u>integrally closed</u> (or <u>normal</u>) if $R^{\mathrm{int},K} = R$.

Lemma 3.31: Let R be an integral domain and L an algebraic extension of $K := Q(R)$. Let $S := R^{\mathrm{int},L}$. Then

a) For every $\alpha \in L$ there is $d \in R \setminus \{0\}$ such that $d\alpha \in S$.

b) $Q(S) = L$.

c) S is integrally closed.

$$\begin{tikzcd}
R^{\mathrm{int},L} = S \arrow[r, hook] & L = Q(S) \\
R \arrow[r, hook] \arrow[u, hook, "\text{integral}"] & K = Q(R) \arrow[u, hook, dotted, "\text{algebraic}"']
\end{tikzcd}$$

<u>Proof:</u> Since $K \subseteq L$ algebraic, there is

$$f := X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in K[X]$$

with $f(\alpha) = 0$, i.e.

$$\alpha^n + a_1 \alpha^{n-1} + \dots + a_{n-1}\alpha + a_n = 0$$

Since $K = Q(R)$, there is $d \in R$ such that $da_i \in R \ \forall i$ (common denominator).

Multiply above by d^n:

$$0 = d^n\alpha^n + d^n a_1 \alpha^{n-1} + \dots + d^n a_{n-1}\alpha + d^n a_n$$

$$= (d\alpha)^n + a_1 d (d\alpha)^{n-1} + \dots + a_{n-1} d^{n-1} (d\alpha) + a_n d^n$$

$\rightsquigarrow$ $d\alpha$ integral over R $\rightsquigarrow$ $d\alpha \in S$.

Clearly $Q(S) \subset L$. Above shows $L \subset Q(S)$, so $L = Q(S)$.

By Lemma 3.25, $S = R^{\mathrm{int}, L}$ is integrally closed in L. Since $L = Q(S)$, S is integrally closed. $\square$

<u>Cor</u> 3.32: Rings of integers are integrally closed. $\square$

3.5 Integrality of minimal polynomial, norm, trace

Let R be an integrally closed domain, $K = Q(R)$, $L \supseteq K$ a finite extension.

<u>Lemma</u> 3.33: $\alpha \in L$ is integral over R iff $p_{\alpha,K}$ has coefficients in R.

<u>Proof:</u> If p_α has coefficients in R, then α is integral.

Conversely, let α be integral. Then

$$\alpha^n + r_1\alpha^{n-1} + \dots + r_{n-1}\alpha + r_n = 0, \text{ for some } r_i \in R.$$

Let α' be another root of p_α (in some splitting field).

Then $K[\alpha]$ and $K[\alpha']$ are both stem fields of p_α

$\rightsquigarrow$ $\exists \sigma: K[\alpha] \xrightarrow{\sim} K[\alpha']$ with $\sigma(\alpha) = \alpha'$

Applied to equation above: $(\alpha')^n + r_1 (\alpha')^{n-1} + \dots + r_{n-1}(\alpha') + r_n = 0$

$\Rightarrow \alpha'$ integral over R.

As integral elements form a ring by Cor 3.21 $\rightsquigarrow$ all coefficients of p_α are integral over R.

Coeffs of p_α are in K, they are integral over $R \Rightarrow$ coeffs in R since R integrally closed. $\rightsquigarrow p_\alpha \in R[X]$

$\square$

<u>Cor</u> 3.34: Suppose $K \subseteq L$ separable. If $\alpha \in L$ integral over R then:

a) χ_α has coefficients in R

b) α integral over R then $N_{L|K}(\alpha), Tr_{L|K}(\alpha) \in R$.

<u>Proof</u>: $\chi_\alpha = p_\alpha^d$ by Prop 2.31 $\Rightarrow \chi_\alpha \in R[X]$ by Lemma 3.33

$N_{L|K}(\alpha)$ and $Tr_{L|K}(\alpha)$ are coefficients of χ_α by Lemma 2.26 $\Rightarrow$ both $\in R$.

$\square$

3.6 Ring of integers is finitely generated

Let R be a ring

<u>Def</u> 3.35: An R-module V is <u>noetherian</u> if every submodule of V is finitely generated.

<u>Prop</u> 3.36: The following are equivalent:

a) V is noetherian

b) Every ascending chain of submodules of V eventually becomes stationary:

$$0 = V_0 \subseteq V_1 \subseteq V_2 \subseteq \dots \rightsquigarrow V_i = V_{i+1} \quad \forall i \geq N$$

c) Every non-empty set of submodules of M has a maximal element

<u>Proof</u>:

a⇒b: Let $V' := \sum_{i \in I} V_i$, a submodule of V.

By assumption, V' is finitely generated, so $V' = R \cdot \{v_1, \dots, v_n\}$

⇝ There is N such that $v_j \in V_N \; \forall j$

⇝ $V_i = V_{i+1} \; \forall i \geq N$.

b⇒c: Let $S \neq \emptyset$ be a set of submodules.

Choose $V_1 \in S$. If V_1 not maximal in S, there is $V_2 \in S$, $V_1 \subsetneq V_2$.

If V_2 not maximal ...... ⇝ ascending chain

⇝ becomes stationary, say at V_N

⇝ V_N is a maximal element.

c⇒a: Let $U \subseteq V$ be a submodule. Need to show: U is f.g.

Let $S :=$ set of all finitely generated submodules of U.

$S \neq \emptyset$ since $0 \in S$

⇝ S contains a maximal element U'.

$U' = R \cdot \{v_1, \dots, v_n\}$. If $U' \neq U$ ⇝ $\exists v \in U \setminus U'$

⇝ $\{v_1, \dots, v_n, v\} \in S$ ↯ to U' maximal

⇒ $U' = U$

⇒ U f.g.

□

Lemma 3.37: If U is a submodule of V, then:

a) the abelian group V/U is naturally an R-module with $r \cdot \bar{v} := \overline{r \cdot v}$.

b) $\{$submodules of V containing $U\} \xleftrightarrow{1:1} \{$submodules of $V/U\}$.

Proof: Straightforward.

□

Lemma 3.38: U a submodule of V. Then V noetherian iff both U and V/U noetherian.

Proof: ⇒ clear.

$\Leftarrow$: Claim: $V' \subseteq V''$ submodules of V with $V'+U/U = V''+U/U$ and $V' \cap U = V'' \cap U$
Then $V' = V''$.

Let $v'' \in V''$. Then there is $v' \in V'$ s.t. $v' + U = v'' + U \Rightarrow v' - v'' \in U$
$\Rightarrow v' - v'' \in V'' \cap U = V' \cap U \subset V'$
$\Rightarrow v'' \in V'$.

Now, suppose there is an ascending chain of submodules of V. The image of this chain in V/U becomes stationary since V/U noetherian. The intersection of the chain with U becomes stationary since U noetherian $\Rightarrow$ The chain itself becomes stationary by claim. $\square$

3.39

Def: A morphism $f: V \to W$ of R-modules V, W is a map such that
$$f(v+v') = f(v+v')$$
$$f(rv) = r f(v).$$

3.40

Lemma: Kernel, image, isomorphism theorem as for vector spaces. $\square$

3.41

Def: R is called noetherian if noetherian as R-module, i.e. every ideal is f.g.

3.42

Prop: If R is noetherian then every f.g. R-module is noetherian.

Proof: By induction on the minimum number of generators for V.
If $n = 1 \rightsquigarrow V = R \cdot \{v\} \to f: R \to V$, $1 \mapsto v$, is surjective
$\Rightarrow R/I \simeq V$ as R-modules, $I = \ker f$

Since R noetherian, so is R/I, hence V.

If $n > 1$: $V = R \cdot \{v_1, \dots, v_n\}$. Then $U := R \cdot \{v_1, \dots, v_n\}$ noetherian by induction.
Also V/U, noetherian since generated by one element, v_n.
$\overset{\text{Lemma}}{\Rightarrow}$ V noetherian. $\square$

Ex 3.43:

a) Every principal ideal domain is noetherian
$\rightarrow K, K[X], \mathbb{Z}, \dots$

b) $K[X_1, X_2, \dots]$ infinitely many vars is not noetherian,
has the submodule $I = (X_1, X_2, \dots)$ which is not f. g

Prop 3.44: If R is noetherian, it has a maximal ideal. $\square$

Remark 3.45: Also holds if R not noetherian! (Zorns Lemma)

Without proof (but possible with your knowledge):

Thm 3.46 **(Hilbert Basis Theorem)**: If R is noetherian, then every f.g. R-algebra is noetherian. $\square$

Now, back to business:

Thm 3.47: Let R be integrally closed and noetherian, $K := Q(R)$.
Let L be a finite separable extension of K.
Then $S := R^{\text{int}, L}$ is a finitely generated R-module and a noetherian ring.

Proof: Let $\{\alpha_1, \dots, \alpha_n\}$ be a K-basis of L. By Lemma 3.31 there is
$d \in R \setminus \{0\}$ s.t. $d\alpha_i \in S \; \forall i$. Then $\{d\alpha_1, \dots, d\alpha_n\}$ is still a K-basis of L.
Can thus assume $\alpha_i \in S \; \forall i$
The trace form on $K \subseteq L$ is non-degenerate by Corollary 2.43
$\Rightarrow$ The K-basis $\{\alpha_1, \dots, \alpha_n\}$ of L has a dual basis $\{\alpha_1', \dots, \alpha_n'\}$,
i.e. $Tr_{L|K}(\alpha_i \alpha_j') = \delta_{ij}$.
Let $\alpha \in S$. Then $\alpha = \sum_{j=1}^{n} \beta_j \alpha_j'$ with $\beta_i \in K$.

Since $\alpha_i, \alpha \in S \rightsquigarrow \alpha\alpha_i \in S$.

$\rightsquigarrow Tr_{L|K}(\alpha\alpha_i) \in R$ by Cor 3.34.

Hence
$$R \ni Tr_{L|K}(\alpha\alpha_i) = Tr_{L|K}\left(\sum_{j=1}^{n} \beta_j \alpha_j' \alpha_i\right) = \sum_{j=1}^{n} \beta_j \delta_{ij} = \beta_j$$

$\Rightarrow \alpha \in R\cdot\{\alpha_1', \dots, \alpha_n'\}$

$\Rightarrow S \subseteq R\cdot\{\alpha_1', \dots, \alpha_n'\} \rightsquigarrow S$ submodule of a f.g. R-module

$\rightsquigarrow S$ f.g. R-module since R noetherian.

By Hilbert's Basis Theorem: S is noetherian. $\square$

<u>Corollary</u> 3.48: Every ring of integers $\mathcal{O}_L$ is a finitely generated $\mathbb{Z}$-module and a noetherian ring. $\square$

<u>3.7 Ring of integers is free</u>

Note: $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$, every element of the for $a+bi$ with unique $a,b \in \mathbb{Z}$

<u>Def</u> 3.49: Let V be an R-module. A subset $\{v_i\}_{i\in I} \subseteq V$ is <u>linearly independent</u> if whenever
$$\sum_{i\in I} r_i v_i = 0 \Rightarrow r_i = 0 \ \forall i$$

A <u>basis</u> of V is a linearly independent generating set.

V is called <u>free</u> if it has a basis

<u>Note</u>: V free $\Rightarrow$ every $v \in V$ is of the form $\sum_{i\in I} r_i v_i$ with unique $r_i \in R$.

<u>Ex</u> 3.50:

a) R itself is a free R-module.
So is $R^{(I)} := \bigoplus_{i\in I} R = \{(r_i)_{i\in I} \mid \underset{\text{all but finitely many } r_i = 0.}{r_i \in R}\}$

In fact:
V free $\Leftrightarrow V \simeq R^{(I)}$ for some I.

b) Ever K-vector space is a free K-module.