MATH200C, LECTURE 13

GOLSEFIDY

Getting Noetherian condition for some integral closures.

In the previous lecture we were proving the following result.

Theorem 1. *Suppose A is an integrally closed integral domain. Suppose F is a field of fractions of A, and E/F is a finite separable field extension. Let B be the integral closure of A in E. Then there are $e_1, \ldots, e_n \in E$ such that*

$$B \subseteq Ae_1 + \cdots + Ae_n. \tag{1}$$

In particular, if A is Noetherian, then B is Noetherian.

We have already pointed out how to deduce that B is Noetherian if A is. We have also proved a few lemmas. Let us recall a few of them.

Lemma 2. *Suppose E/F is a finite separable field extension. Then*

(1) $|\mathrm{Embed}_F(E, \overline{F})| = [E : F]$ where $\overline{F}$ is an algebraic closure of F and $\mathrm{Embed}_F(E, \overline{F})$ is the set of F-embeddings of E into $\overline{F}$.

(2) $\mathrm{Tr}_{E/F}(a) := \sum_{\sigma \in \mathrm{Embed}_F(E,\overline{F})} \sigma(a) = \mathrm{Tr}(l_a)$ where $l_a : E \to E, l_a(e) := ae$ is viewed as an F-linear map; in particular, $\mathrm{Tr}_{E/F}(E) \subseteq F$.

Lemma 3. *Suppose E/F is a finite separable field extension. Then $h(e, e') := \mathrm{Tr}_{E/F}(ee')$ is a non-degenerate symmetric bilinear form.*

Lemma 4. *Suppose V is a finite-dimensional F-vector space, and $h : V \times V \to F$ is a non-degenerate F-bilinear map. Suppose $\{v_1, \ldots, v_n\}$ is an F-basis of V. Then there is a dual basis $\{w_1, \ldots, w_n\}$ with respect to h; that means it is an F-basis and for any i, j we have*

$$h(v_i, w_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

The last needed lemma is the following:

Lemma 5. *Suppose A is an integral domain, F is its field of fractions, E/F is an algebraic extension, and B is the integral closure of A in E. Then $E = (A \setminus \{0\})^{-1}B$.*

Proof. Let $\beta \in E$. Then β satisfies an equation with coefficients in F; that means

$$\beta^n + c_{n-1}\beta^{n-1} + \cdots + c_1\beta + c_0 = 0$$

for some $c_i \in F$. Taking a common denominator for c_i's, we find $a \in A$ such that $a_i := ac_i \in A$. Then

$$a\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0 = 0.$$

After multiplying both sides by a^{n-1}, we get

$$(a\beta)^n + a_{n-1}(a\beta)^{n-1} + \cdots + a^{n-2}a_1(a\beta) + a^{n-1}a_0 = 0,$$

which means $a\beta$ is integral over A. Hence $a\beta \in B$ and $\beta = \frac{a\beta}{a} \in (A\setminus\{0\})^{-1}B$. □

Proof of Theorem 1. Let $\{\beta_1, \ldots, \beta_n\}$ be an F-basis of E. By the previous lemma, there is $a \in A$ such that $b_i := a\beta_i \in B$. Since $a \in A \subseteq F$, $\{b_1, \ldots, b_n\}$ is an F-basis of E. Let $\{e_1, \ldots, e_n\}$ be a dual basis of E with respect to the bilinear form $h(x, y) := \mathrm{Tr}_{E/F}(xy)$. Hence for any $b \in B$ there are $c_i \in F$ such that

$$b = c_1e_1 + \cdots + c_ne_n;$$

this implies $h(b, b_i) = h(c_1e_1 + \cdots + c_ne_n, b_i) = \sum_j c_jh(e_j, b_i) = c_i$. On the other hand, $h(b, b_j) = \sum_{k=1}^n \sigma(bb_j)$ where $\{\sigma_1, \ldots, \sigma_n\}$ are all the F-embeddings of E into an algebraic closure $\overline{F}$ of F. As $bb_j \in B$, they are integral over A; and so are $\sigma_k(bb_j)$. Thus $h(b, f_j)$ is integral over A, and it is in F. As A is integrally closed, we deduce that $h(b, b_j) \in A$. Altogether, we get

$$b \in Ae_1 + \cdots + Ae_n;$$

and claim follows. □

Corollary 6. *As an additive group $\mathscr{O}_k$ is isomorphic to $\mathbb{Z}^{[k:\mathbb{Q}]}$.*

Proof. Since $\mathbb{Z}$ is integrally closed, we can apply Theorem 1 and deduce that

$$\mathscr{O}_k \subseteq \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$$

for some $e_i \in k$. This implies that $\mathscr{O}_k$ is a subgroup of a torsion-free finitely generated abelian group. Hence $\mathscr{O}_k$ is a finite rank abelian group; say $\mathscr{O}_k \simeq \mathbb{Z}^d$. Since $(\mathbb{Z} \setminus \{0\})^{-1}\mathscr{O}_k = k$, we deduce that $d = [K : \mathbb{Q}]$; and claim follows. □

Valuation rings

We start with a technical definition and theorem; and then deduce many important results.

Definition 7. *An integral domain A is called a valuation ring if for any element α of its field of fractions F, either $\alpha \in A$ or $\alpha^{-1} \in A$.*

Example 8. *Let $A := \{\frac{m}{n} |\, m, n \in \mathbb{Z}, 2 \nmid n\}$; then A is a valuation ring. More generally if D is a UFD and $p \in D$ is irreducible, then $D_{\langle p\rangle} := \{\frac{a}{b} |\, a, b \in D, p \nmid b\}$ is a valuation ring.*

In your homework assignment you will see the definition of a valuation; and you will see that a ring is a valuation ring if and only if there is a valuation v of F and $A = \{a \in F | v(a) \geq 0\}$.

Proposition 9. *Suppose A is a valuation ring and F is its field of fractions. Then*

(1) A is a local ring.
(2) If $A \subseteq A' \subseteq F$, then A' is a valuation ring.
(3) A is integrally closed.

Proof. (1) Let $\mathfrak{m} := A \setminus A^{\times}$. For $a \in \mathfrak{m}$ and $b \in A$, clearly $ab \in \mathfrak{m}$ (if the product of two elements has an inverse, then both of them have).

If $a, b \in \mathfrak{m} \setminus \{0\}$, then either $\frac{a}{b} \in A$ or $\frac{b}{a} \in A$. This implies that either $(1 + \frac{a}{b}) \in A$ or $(1 + \frac{b}{a}) \in A$; and so either $a(1 + \frac{b}{a}) \in \mathfrak{m}$ or $b(1 + \frac{a}{b}) \in \mathfrak{m}$. In either case, we deduce that $a + b \in \mathfrak{m}$. Hence $\mathfrak{m}$ is an ideal of A. Therefore it is the unique maximal ideal as its complement consists of units.

(2) is clear.

(3) Suppose $\alpha \in F$ is integral over A. And suppose to the contrary that α is not in A. Hence $\alpha^{-1} \in A$ and

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

for some $a_i \in A$. Therefore

$$\alpha = -(a_{n-1} + a_{n-2}\alpha^{-1} + \cdots + a_0\alpha^{-(n-1)}) \in A$$

which is a contradiction. $\square$

Note. As you can see in the above argument, if A is a subring of a field F and $\alpha \in F$, then α is integral over A if and only if $\alpha \in A[\alpha^{-1}]$.

The following is our main technical theorem on this subjection.

Theorem 10. *Suppose Ω is an algebraically closed field, A_0 is an integral domain, and $\theta_0 : A_0 \to \Omega$ is a ring homomorphism. Suppose A_0 is a subring of a field F. Let*

$$\Sigma := \{(B, \theta) |\ A \subseteq B \subseteq F \text{ intermediate ring }, \theta \text{ ring hom}, \ \theta|_{A_0} = \theta_0\}.$$

We say $(B, \theta) \preceq (B', \theta')$ if $B \subseteq B'$ and $\theta'|_B = \theta$. Then Σ has a maximal element (B, θ), B is a valuation ring, its unique maximal ideal is $\ker \theta$, and F is the field of fractions of B.

Let's make a remark on why it is important to have a good understanding of $\mathrm{Hom}(A, \Omega)$. Suppose A is a finitely generated F-algebra; that implies that $A \simeq F[x_1, \ldots, x_n]/\mathfrak{a}$. Then there is a bijection between $\mathrm{Hom}_F(A, \Omega)$ and

$$\{\phi \in \mathrm{Hom}_F(F[x_1, \ldots, x_n], \Omega) |\ \mathfrak{a} \subseteq \ker \phi\}.$$

On the other hand, there is a bijection between F-algebra homomorphism $\phi : F[x_1, \ldots, x_n] \to \Omega$ and Ω^n; to any point $p \in \Omega^n$, we can associate the evaluation at p map ϕ_p; and any homomorphism is of this form. So we get a bijection between $\mathrm{Hom}_F(A, \Omega)$ and

$$\{p \in \Omega^n |\ \forall f \in \mathfrak{a}, f(p) = 0\}.$$

So have a good understand of $\mathrm{Hom}(A, \Omega)$ helps us understand common zeros of a family of polynomials.

Proof of Theorem 10. **Claim 1.** *Existence of a maximal element.*

Proof of Claim 1. It is clear that $(\Sigma, \preceq)$ is a non-empty POSet ($(A_0, \theta_0) \in \Sigma$). To show that it has a maximal, by Zorn's lemma, it is enough to show any chain $\mathscr{C} := \{(B_i, \theta_i)\}_{i \in I}$ in Σ has an upper bound.

Let $B := \bigcup_{i \in I} B_i$ and $\theta : B \to \Omega, \theta(b) := \theta_i(b)$ if $b \in B_i$. For $b, b' \in B$, there are $i, j \in I$ such that $b \in B_i$ and $b' \in B_j$. Since $\mathscr{C}$ is a chain, without loss of generality we can and will assume that $B_i \subseteq B_j$. Hence $b, b' \in B_j$, which implies that $b + b', bb' \in B_j \subseteq B$. Thus B is a subring of F.

If $b \in B_i \cap B_j$, then again as $\mathscr{C}$ is a chain without loss of generality we can and will assume that $(B_i, \theta_i) \preceq (B_j, \theta_j)$; and so $\theta_j | B_i = \theta_i$, which implies that $\theta_i(b) = \theta_j(b)$. Hence θ is well-defined.

If $b, b' \in B$, then as we discussed above, there is $i \in I$ such that $b, b' \in B_i$. Hence $\theta(b + b') = \theta_i(b + b') = \theta_i(b) + \theta_i(b') = \theta(b) + \theta(b')$, and $\theta(bb') = \theta_i(bb') = \theta_i(b)\theta_i(b') = \theta(b)\theta(b')$. Therefore θ is a ring homomorphism.

So (B, θ) is an upper bound of $\mathscr{C}$; thus by Zorn's lemma, Σ has a maximal element.

Claim 2. *Suppose (B, θ) is a maximal element of Σ. Then B is a local ring and $\mathfrak{m} := \ker\theta$ is it unique maximal ideal.*

Note. At each step, we try to extend θ; and then use the maximality condition to get the desired property.

Proof of Claim 2. Since $B/\ker\theta$ can be embedded into Ω, it is an integral domain. Hence $\ker\theta$ is a prime ideal of B. As B is a subring of F, we get that $B_{\ker\theta} \subseteq F$. Since $\theta(B \setminus \ker\theta) \subseteq \Omega^\times$, by the universal property of localization, there is $\widehat{\theta} : B_{\ker\theta} \to \Omega$ such that $\widehat{\theta}(\frac{b}{1}) = \theta(b)$. Hence $(B_{\ker\theta}, \widehat{\theta}) \in \Sigma$ and $(B, \theta) \preceq (B_{\ker\theta}, \widehat{\theta})$. Since (B, θ) is maximal in Σ, we deduce that $B = B_{\ker\theta}$. Therefore B is a local ring and $\ker\theta$ is its unique maximal ideal.

Claim 3. *For any $\alpha \in F$, either $\alpha \in B$ or $\alpha^{-1} \in B$.*

To prove this claim, again we would like to extend θ to either $B[\alpha]$ or $B[\alpha^{-1}]$, and then use maximality of B to deduce the desired result. That means we have to find a ring homomorphism $\widehat{\theta} : B[\alpha] \to \Omega$ such that $\widehat{\theta}|_B = \theta$; in particular, $\ker\widehat{\theta} \supseteq \ker\theta =: \mathfrak{m}$. Hence $\mathfrak{m}[\alpha]$ needs to be a proper ideal of $B[\alpha]$. So we start with the following subclaim.

Subclaim. *For any $\alpha \in F^\times$, either $\mathfrak{m}[\alpha] \neq B[\alpha]$ or $\mathfrak{m}[\alpha^{-1}] \neq B[\alpha^{-1}]$.*

Proof of Subclaim. Suppose to the contrary that $1 \in \mathfrak{m}[\alpha] \cap \mathfrak{m}[\alpha^{-1}]$. So there are $c_i, c'_i \in \mathfrak{m}$ such that $1 = c_0 + c_1\alpha + \cdots + c_n\alpha^n$, and $1 = c'_0 + c'_1\alpha^{-1} + \cdots + c'_m\alpha^{-m}$; and suppose m and n are smallest possible positive integers with these properties. Without loss of generality we can and will assume that $n \geq m$. Then

$$\begin{aligned}
1 = c'_0 + c'_1\alpha^{-1} + \cdots + c'_m\alpha^{-m} &\Rightarrow (1 - c'_0) = c'_1\alpha^{-1} + \cdots + c'_m\alpha^{-m} \\
(\text{since } B \text{ is local, } 1 + \mathfrak{m} \subseteq B^\times) &\Rightarrow 1 = (1 - c'_0)^{-1}(c'_1\alpha^{-1} + \cdots + c'_m\alpha^{-m}) \\
(\text{for some } c''_i \in \mathfrak{m}) &\Rightarrow 1 = c''_1\alpha^{-1} + \cdots + c''_m\alpha^{-m} \\
&\Rightarrow \alpha = c''_1 + \cdots + c''_m\alpha^{-(m-1)}.
\end{aligned}$$

Hence

$$
\begin{aligned}
1 =& c_0 + c_1\alpha + \cdots + c_n\alpha^n \\
=& c_0 + c_1\alpha + \cdots + c_n\alpha^{n-1}(\alpha) \\
=& c_0 + c_1\alpha + \cdots + c_n\alpha^{n-1}(c''_1 + \cdots + c''_m\alpha^{-(m-1)}) = \quad c'''_0 + c'''_1\alpha + \cdots + c'''_{n-1}\alpha^{n-1},
\end{aligned}
$$

for some $c'''_i \in \mathfrak{m}$ which contradicts minimality of n.

Proof of Claim 3. By Subclaim, without loss of generality we can and will assume that $\mathfrak{m}[\alpha]$ is a proper ideal of $B[\alpha]$. Hence there is a maximal ideal $\mathfrak{m}'$ of $B[\alpha]$ that contains $\mathfrak{m}$ as a subset. Therefore $\mathfrak{m}' \cap B \supseteq \mathfrak{m}$; and as $\mathfrak{m}$ is a maximal ideal, we deduce that $B \cap \mathfrak{m}' = \mathfrak{m}$. Thus $B/\mathfrak{m}$ can be embedded into $B[\alpha]/\mathfrak{m}'$; and $B[\alpha]/\mathfrak{m}' = k(\mathfrak{m})[\overline{\alpha}]$ where $k(\mathfrak{m})$ is the copy of $B/\mathfrak{m}$ in $B[\alpha]/\mathfrak{m}'$ and $\overline{\alpha} := \alpha + \mathfrak{m}'$. Since $k(\mathfrak{m})[\overline{\alpha}]$ is a field extension of $k(\mathfrak{m})$, we deduce that it is a finite extension. Hence the embedding of $k(\mathfrak{m})$ in Ω can be extended to an embedding of $k(\mathfrak{m})[\overline{\alpha}]$ into Ω. Overall we get the following commuting diagram:

$$
\begin{tikzcd}
B \arrow[r, hook] \arrow[d] \arrow[dd, bend right, "\theta"'] & B[\alpha] \arrow[d] \\
B/\mathfrak{m} \arrow[r, hook] \arrow[d, hook] & B[\alpha]/\mathfrak{m}' \arrow[dl, hook, dashed] \\
\Omega &
\end{tikzcd}
$$

And s we get an extension of θ to $B[\alpha]$. Therefore by the maximality of (B, θ), we deduce that $\alpha \in B$; and claim follows. $\square$