Lecture 15: Bilinear forms

Wednesday, May 2, 2018 11:02 AM

<u>Lemma</u>. A: integral domain, integrally closed with field of fractions F.

E/F is an algebraic extension. B: integral closure of A in E.

Then $E = (A\setminus\{0\})^{-1} B$.

<u>Pf.</u> $\forall \alpha \in E$, $\exists f_i \in F$ s.t. $\alpha^n + f_{n-1}\alpha^{n-1} + \cdots + f_1 \alpha + f_0 = 0$.

Since F is the field of fractions of A, $\exists a_i \in A$ s.t. $a_n \neq 0$ and

$a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, which implies

$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + \cdots + a_0 a_n^{n-1} = 0$; and so $a_n \alpha \in B$. Therefore

$\alpha \in a_n^{-1} B \subseteq (A\setminus\{0\})^{-1} B$. ∎

Recall a few results from linear algebra:

Suppose V is a finite dimensional vector space over F. Let $\{v_1, \ldots, v_n\}$

be an F-basis. Then for any $v \in V$, $\exists!\ (c_1, \ldots, c_n) \in F^n$ s.t.

$\sum_{i=1}^n c_i v_i = v$. We let $|v\rangle_{\mathcal{B}} = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$ and $\langle v|_{\mathcal{B}} = [c_1 \cdots c_n]$.

For a linear map $T: V \to V$, let $[T]_{\mathcal{B}} \in M_n(F)$ s.t. its i^{th}

column is $|T v_i\rangle_{\mathcal{B}}$. And we get $|Tv\rangle_{\mathcal{B}} = [T]_{\mathcal{B}} |v\rangle_{\mathcal{B}}$ and

$\langle Tv|_{\mathcal{B}} = \langle v|_{\mathcal{B}} [T]_{\mathcal{B}}^{t}$.

Lecture 15: Bilinear forms

Saturday, May 5, 2018 1:27 PM

- $f: V \times V \to F$ is called a <u>bilinear form</u> if

$$f(cv + c'v', w) = c f(v,w) + c' f(v', w) \quad \text{and}$$

$$f(v, cw + c'w') = c f(v,w) + c' f(v', w).$$

- Let $[f]_{\mathcal{B}} := [f(v_i, v_j)] \in M_n(F)$. Then

$$f(v,w) = \langle v|_{\mathcal{B}} \, [f]_{\mathcal{B}} \, |w\rangle_{\mathcal{B}}.$$

- f is called <u>non-degenerate</u> if one of the following equivalent properties hold:

(1) $f(v, V) = 0 \implies v = 0$

(2) $\det [f]_{\mathcal{B}} \neq 0$

(3) $f(V, w) = 0 \implies w = 0$

(1) $\Rightarrow$ (2). It is enough to show $[f]_{\mathcal{B}}$ does not have a right kernel. Suppose $\langle v|_{\mathcal{B}}$ is in the right kernel of $[f]_{\mathcal{B}}$. Then $\forall w \in V$, $f(v,w) = \langle v|_{\mathcal{B}} [f]_{\mathcal{B}} |w\rangle_{\mathcal{B}} = 0$. Hence $v = 0$.

(2) $\Rightarrow$ (1) $f(v, V) = 0 \Rightarrow \forall w \in V, \langle v|_{\mathcal{B}} [f] \, |w\rangle_{\mathcal{B}} = 0 \Rightarrow \langle v|_{\mathcal{B}} [f]_{\mathcal{B}} = 0$

$\Rightarrow \langle v|_{\mathcal{B}} = 0 \Rightarrow v = 0$.

Similarly (2) $\Leftrightarrow$ (3). ∎

Lecture 15: Bilinear forms

Saturday, May 5, 2018 1:42 PM

<u>Lemma</u>. Suppose f is a non-degenerate bilinear form. Then

$$T_f : V \to V^*, \quad (T_f(v))(w) := f(v,w)$$

is an F-vector space isomorphism.

<u>Pf.</u> <u>$T_f(v) \in V^*$</u>. $\quad (T_f(v))(cw + c'w') = f(v, cw + c'w')$

$$= c\, f(v,w) + c' f(v,w')$$

$$= c\, (T_f(v))(w) + c' (T_f(v))(w').$$

<u>T_f is linear</u>. $\quad (T_f(cv + c'v'))(w) = f(cv + c'v', w)$

$$= c\, f(v,w) + c' f(v',w)$$

$$= c\, (T_f(v))(w) + c' (T_f(v'))(w).$$

<u>T_f is injective</u>. $\quad T_f(v) = 0 \Rightarrow \forall w \in V,\ (T_f(v))(w) = 0$

$$\Rightarrow f(v,w) = 0 \quad \forall w \in V \Rightarrow v = 0.$$

<u>T_f is surjective</u>. $\quad \dim V = \dim V^*$ and T_f is inject.

(and linear). ■

<u>Lemma</u>. f: non-degenerate bilinear form; $W \subseteq V$ subspace;

$W^\perp := \{v \in V \mid f(v, W) = 0\}$. Then

$$0 \to (V/W)^* \to V^* \to W^* \to 0 \quad \text{and} \quad 0 \to W^\perp \to V \to V/W^\perp \to 0$$

are isomorphic S.E.S.; in particular $\dim W + \dim W^{\perp} = \dim V$.

This proof was not presented during lecture.

__Pf.__ Since $0 \to W \to V \to V/W \to 0$ is a S.E.S.,

$$\begin{tikzcd}
0 \arrow[r] & (V/W)^{*} \arrow[r] & V^{*} \arrow[r] & W^{*} \arrow[r] & 0 \\
0 \arrow[r] & W^{\perp} \arrow[r] & V \arrow[r] \arrow[u, "\wr\, T_f"] & V/W^{\perp} \arrow[r] & 0
\end{tikzcd}$$

is a S.E.S..

For any $\omega' \in W^{\perp}$ and $\omega \in W$, $\big(T_f(\omega')\big)(\omega) = f(\omega', \omega) = 0$

$\Rightarrow T_f(W^{\perp}) \subseteq (V/W)^{*}$.

Let $\overline{T_f} : V/W^{\perp} \to W^{*}$, $\overline{T_f}(v + W^{\perp})(\omega) := f(v, \omega)$.

One can see that $\overline{T_f}$ is a well-defined linear map and the following is a commuting diag.

$$\begin{tikzcd}
0 \arrow[r] & (V/W)^{*} \arrow[r] & V^{*} \arrow[r] & W^{*} \arrow[r] & 0 \\
0 \arrow[r] & W^{\perp} \arrow[r] \arrow[u, "T_f|_{W^{\perp}}"] & V \arrow[r] \arrow[u, "\wr\, T_f"] & V/W^{\perp} \arrow[r] \arrow[u, "\overline{T_f}"] & 0
\end{tikzcd}$$

It is easy to see that $T_f|_{W^{\perp}}$ and $\overline{T_f}$ are injective; and so by dimension comparison, they are also surjective. In particular,

$$\dim W^{\perp} = \dim (V/W)^{*} = \dim V/W = \dim V - \dim W. \quad \blacksquare$$

__Corollary__. In the above setting $(W^{\perp})^{\perp} = W$.

Lecture 15: Dual basis

Tuesday, May 8, 2018 10:54 PM

Pf. Clearly $(W^\perp)^\perp \supseteq W$. By the previous lemma

$\dim (W^\perp)^\perp + \dim W^\perp = \dim V = \dim W^\perp + \dim W$. And so $\dim W = \dim (W^\perp)^\perp$. ∎

Proposition. Suppose $f: V \times V \to F$ is a non-degen. bilinear form.

Suppose $\mathcal{B} := \{v_1, \ldots, v_n\}$ is an F-basis of V. Then $\exists\, \omega_1, \ldots, \omega_n \in V$

such $f(\omega_i, v_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$. $\{\omega_1, \ldots, \omega_n\}$ is an F-basis

of V and it is called the dual basis of V.

Pf. We construct ω_i's recursively. Since $\langle v_1 \rangle^\perp \neq V$, $\exists\, \omega_1 \in V$ s.t.

$f(\omega_1, v_1) = 1$. Suppose $\omega_1, \ldots, \omega_k$ have been already constucted. Then

since $v_{k+1} \notin \langle v_1, \ldots, v_k \rangle$, by the previous corollary

$$\langle v_1, \ldots, v_k \rangle^\perp \not\subseteq \langle v_{k+1} \rangle^\perp.$$

Hence $\exists\, \omega_{k+1} \in \langle v_1, \ldots, v_k \rangle^\perp$ s.t. $f(\omega_{k+1}, v_{k+1}) = 1$. And $\omega_1, \ldots, \omega_n$

satisfy $f(\omega_i, v_j) = \delta_{ij}$. Thus $\omega = \sum c_i \omega_i$ implies $c_j = f(\omega, v_j)$.

In particular ω_i's are linearly independent; and claim follows. ∎

Corollary. In the above setting

$$v = \sum f(v, v_j)\, \omega_j = \sum f(\omega_i, v)\, v_i . \qquad \square$$

Lecture 15: Integral closure; Noetherian

Wednesday, May 2, 2018 12:31 AM

Theorem. A: integral domain, integrally closed, with field of fractions F

E/F : finite separable extension;

B : integral closure of A in E;

$\Rightarrow \exists\, e_1,\ldots,e_n \in E$ s.t. $B \subseteq Ae_1 + \cdots + Ae_n$; in particular if A is Noetherian, then B is a Noetherian A-mod. (; and so B is a Noetherian ring as well.)

Pf of theorem. Suppose $\{e_1,\ldots,e_n\} \subseteq E$ is an F-basis of E. By a lemma $E = (A\setminus\{0\})^{-1}B$; so $e_i = \frac{b_i}{a_i}$ for some $b_i \in E$ and $a_i \in A \subseteq F$.

Hence $\{b_1,\ldots,b_n\} \subseteq B$ is an F-basis of E. Since E/F is a finite separable extension, $f: E\times E \to F$, $f(e,e') := T_{E/F}(ee')$ is a symmetric non-degenerate bilinear form. By a result proved earlier $\exists$ an F-basis $\{e_1,\ldots,e_n\}$ of E s.t. $f(e_i, b_j) = \delta_{ij}$. And so for any $b \in B$, $b = \sum_{j=1}^{n} T_{E/F}(bb_j)\, e_j$. On the other hand $T_{E/F}(bb_j) = \sum_{\sigma \in \mathrm{Hom}_F(E,\bar{F})} \sigma(bb_j) \in F$; and bb_j is integral over A implies $\sigma(bb_j)$ is integ. over A. Therefore $T_{E/F}(bb_j) \in F$ is integral over A. Since A is integrally closed, $T_{E/F}(bb_j) \in A$.

Lecture 15: Noetherian; integral closure

Wednesday, May 2, 2018 12:49 AM

Hence $B \subseteq \sum_{i=1}^{n} Ae_i$.

If A is Noetherian, any f.g. A-mod is a Noeth. A-mod. Hence $\sum_{i=1}^{n} Ae_i$ is a Noetherian A-mod. And so B is a Noeth. A-mod; this implies B is a Noetherian ring as well. ■

<u>Corollary</u>. Let $k/\mathbb{Q}$ be a finite extension, $\mathcal{O}_k$ be the integral closure of $\mathbb{Z}$ in k. Then $\mathcal{O}_k \simeq \mathbb{Z}^{[k:\mathbb{Q}]}$ as an additive group; in particular it is Noetherian and finitely gener. ring.

<u>Pf</u>. By the mentioned theorem $\mathcal{O}_k$ is a finitely generated $\mathbb{Z}$-module. And it is a torsion-free abelian group, as $\mathcal{O}_k \subseteq k$ has char. $\underline{0}$. Hence $\mathcal{O}_k \simeq \mathbb{Z}^d$. By another lemma $(\mathbb{Z}\setminus\{0\})^{-1}\mathcal{O}_k = k$; and so $(\mathbb{Z}\setminus\{0\})^{-1}\mathbb{Z}^d \simeq k$ as $\mathbb{Q}$-vector space, which implies $d=[k:\mathbb{Q}]$. ■

<u>Exercise</u>. Deduce $|N_{k/\mathbb{Q}}(a)| = |\mathcal{O}_k / a\mathcal{O}_k|$ for $a \in \mathcal{O}_k \setminus \{0\}$.