13 Friday, March 4, 2011

Integral Extensions

$A \subset B$ domains

Definition. $b \in B$ is *integral over A* if it's a root of a monic polynomial.
$f(x) = x^n - a_1 x^{n-1} + \cdots \pm a_r$ coefficients in A

Proposition. *The following are equivalent:*

(1) b is integral over A

(2) $A[b]$ is a finite A-module

(3) There exists an $A[b]$-module M which:

- *(i) is faithful[1] as an $A[b]$-module*
- *(ii) is a finite A-module*

Proof.

(1) $\implies$ (2) Clear

(2) $\implies$ (3) Clear

(3) $\implies$ (1) Take the generators for M as an A-module, $(v_1, \ldots, v_n)$. Then $bv_i = \sum a_{ij} v_j$ for $a_{ij} \in A$. We can write this as

$$(b\mathbb{I} - A)V = 0 \qquad V = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Let C be the coefficient matrix of $(b\mathbb{I} - A)$. Then $C(b\mathbb{I} - A) = \det(b\mathbb{I} - A)\mathbb{I}$. Let $\delta := \det(b\mathbb{I} - A)$. Then $\delta V = 0$. Since M is faithful, $\delta = 0$.) Expanding δ gives $\delta = b^n - (\operatorname{tr} A) b^{n-1} + \cdots \pm \det A$ is a monic polynomial for b. The coefficients are in A, so $A[b]$ is integral.

□

Proposition. *Let A be noetherian.*

- *If B is generated as an A-algebra by elements integral over A, then every element of B is integral over A.*
- *If B is generated over A by a finite number of integral elements, then B is a finite A-module. (e.g., B integral over A and a finite type $\mathbb{C}$-algebra.)*

Proof. Take $z \in B$. Then $z \in A[b_1, \ldots, b_k]$ for b_i integral. $A[b_1, \ldots, b_k]$ is a finite A-module. Therefore $A[z]$ is contained in a finite module, so it itself is finite. □

[1] A module is faithful if for any $z \in A[b]$, $z \neq 0$, $zM \neq 0$.

Proposition (Noether Normalization)**.** *Let K be a field, and let A be a finite-type K-algebra and a domain. There exist $y_1, \ldots, y_d \in A$ algebraically independent*[2]*, and A is a finite module over $K[y_1, \ldots, y_d]$.* [3]

$$\begin{array}{ccc} A & & \operatorname{spec} A \\ \uparrow & & \downarrow \\ \mathbb{C}[y_1, \ldots, y_d] & & \mathbb{A}^d \end{array}$$

Proof. Given A generated by $x_1, \ldots, x_n$ (some finite set). Independent on n.(???) If $x_1, \ldots, x_n$ dependent, there exists a polynomial relation $f(x_1, \ldots, x_n) = 0$ of degree d. Let $h(x)$ be the degree d part of f. Then $h(0, 0, 0, \ldots, 1) =$ coefficient of x_n^d in h and in f. If the coefficient of $x_n^d \neq 0$, then $f(x)$ looks like $cx_n^d + g_{n-1}(x_1, \ldots, x_{n-1}^{d-1} + \cdots + g_0(x_1, \ldots, x_{n-1})$. If $c \neq 0$, this is a monic polynomial of which x_n is a root, and its coefficients are in the ring $K[x_1, \ldots, x_{n-1}]$. Therefore, x_n is integral over $K[x_1, \ldots, x_{n-1}]$. By induction, we get a tower of integral extensions.

If $c = 0$, then make a change of variables $x_i \mapsto x_i + u_i x_n$ (for $i < n$), $x_n \mapsto u_n x_n$. Now the coefficient of x_n^d will be $h(x_1 + u_1 x_n, \ldots, x_{n-1} + u_{n-1}x_{n-1}, u_n x_n)|_{x_1 = \cdots = x_{n-1} = 0,\ x_n = 1} = h(u_1, \ldots, u_n)$. This is non-zero for most choices of u_i.[4] $\square$

Corollary (A version of Nullstellensatz)**.** *Let K be a field, B a finite-type K-algebra that is also a field. Then B is a finite K-module.*

(It follows, without much trouble, from this that if $K = \mathbb{C}$, $B = \mathbb{C}$, too; if B is a finite field extension of $\mathbb{C}$, then $B = \mathbb{C}$.

Proof. Take $b \in B$. $\mathbb{C}[b]$ is a finite $\mathbb{C}$-module. Therefore, b is a root of an irreducible polynomial with coefficients in $\mathbb{C}$. Therefore, it is a root of a linear polynomial over $\mathbb{C}$, so $b \in \mathbb{C}$. $\square$)

Proof. Noether Normalization says B a finite module over polynomial ring $A = K[y_1, \ldots, y_d]$. If $d = 0$, then we're done. If $d > 0$, then $y_1 \in A, B$, so $\frac{1}{y_1} \in B$. Thus B is a field. But $\frac{1}{y_1}$ is not integral over $K[y_1, \ldots, y_d]$. $\square$

If A is a domain with fraction field K, then A is *integrally closed* in K if every element of K which is integral over A is an element of A.

Example. $A = \mathbb{C}[x, y]/(y^2 - x^3)$. *This is not integrally closed: Let $z = \frac{y}{x}$.*
Then $z^2 = \frac{y^2}{x^2} = \frac{x^3}{x^2} = x$.
$z^3 = \frac{y^3}{x^3} = \frac{x^3 y}{x^3} = y$.
z is a root of the monic polynomial $z^2 - x$, and of $z^3 - y$.

Theorem. *Let A be a finite-type algebra and a domain, and let K be the fraction field of A. Then the* integral closure *of A in K, the set of integral elements, is a finite A-module.*

Preview:
Given an A-module M, then $M^* := \hom_A(M, A)$ is also an A-module.

If $M \subset N$, then $M^* \supset N^*$ (in good situations).

[2] There are no polynomial relations among them.
[3] I'm still confused by this statement.
[4] For fields with finite characteristic, you'll have to make a non-linear change of variables.