Lecture 14: Hilbert Nullstellensatz

24 February 2021
21:45

Integral extension

Def^n: Let B be a ring & A be a subring of B then B is called an extension of A. An element $b \in B$ is said to be integral over A if $\exists$ a monic poly $f(x) \in A[x]$ s.t. $f(b) = 0$. B is said to be integral over A if $\forall x \in B$, x is integral over A.

(*) B is finite A-alg $\Rightarrow$ B is integral over A.
Converse holds if B is a f.g. A-alg.

Thm: Let $A \subseteq B$ be rings & $x \in B$. TFAE
1. x is integral over A.
2. $A[x]$ is a finite A-module
3. There exist $C \subseteq B$ subring s.t. $A[x] \subseteq C$ & C is a finite A-module.

Cor: $A \subseteq B$ rings. $x, y \in B$ integral over $A \Rightarrow x+y$ & xy are integral over A. (Pf: $A[x]$ is finite A-mod & $A[x,y]$ is finite $A[x]$-mod $\Rightarrow A[x,y]$ is finite A-mod)

Cor: $A \subseteq B$ rings. Then $\overline{A}^B = \{x \in B \mid x \text{ integral over } A\}$ is a ring. It is called the integral closure of A in B.

HW (*) B be a finite A-alg & C be a finite B-alg. Then C is a finite A-alg.

Cor: Let B be a f.g. A-alg with $\varphi: A \to B$ the str map. If B is integral over $\varphi(A)$ then B is a finite A-algebra.
In part if $A \subseteq B$, B f.g A-alg & B int over $A \Rightarrow B$ is a finite A-alg

Pf: B is gen by $b_1, \dots, b_n$ as an A-alg.

$b_1, \dots, b_n$ are int over $\varphi(A)$.

$\overset{\text{Thm}}{\Longrightarrow}$ $\varphi(A)[b_1]$ is a finite $\varphi(A)$-mod ($\because$ b_1 is int over $\varphi(A)$)

$\Rightarrow$ $\varphi(A)[b_1]$ is a finite A-mod

($\because$ b_2 is integral) $\Rightarrow$ $\varphi(A)[b_1, b_2]$ is a finite $\varphi(A)[b_1]$-mod

$\Rightarrow$ $\varphi(A)[b_1, b_2]$ is a finite $\varphi(A)$-mod

Proceeding this way we get

$B = \varphi(A)[b_1, \dots, b_n]$ is a finite $\varphi(A)$-mod

$\Rightarrow$ B is a finite A-mod.

i.e. B is a finite A-alg. ∎

Examples 1) finite field ext^n or alg ext^n are integral.

2) $\mathbb{Z}[\sqrt{3}]$ or $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt[5]{2}]$

$\mathbb{Z}[\sqrt{5}]$ is integral over $\mathbb{Z}$. $\mathbb{Z}[\frac{1}{\sqrt{2}}]$ is not integral over $\mathbb{Z}$.

$\sqrt{5}$ satisfy $X^2 - 5$.

3) $A = k[x, y, z]$, $B = \dfrac{A[W]}{(W^5 - x^2 W + yz W^3 + x)}$

B is int over A.

4) $\mathbb{Z} \subset \mathbb{Z}[\frac{1}{2}]$ $f(x) = 2x - 1$ then $f(\frac{1}{2}) = 0$.

Def^n An int domain A is called integrally closed or normal if $A = \overline{A}^{\,\mathrm{frac}(A)}$.

(*) Let $A \subseteq B$ be an integral ext^n & $S \subseteq A$ be a mult subset then $S^{-1}B$ is integral over $S^{-1}A$.

Pf: $\frac{b}{s} \in S^{-1}B$, b int over $A \Rightarrow b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$ for some $a_i \in A$.

$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \dots + \frac{a_0}{s^n} = 0 \Rightarrow \frac{b}{s}$ is int of $S^{-1}A$.

Hilbert-Nullstellensatz (Algebraic version):

Let k be a field. A finitely generated k-alg $k[x_1, \dots, x_n]$ is a field then $x_1, \dots, x_n$ are alg over k.

Note: $k \subseteq B$ be a ring ext^n with B int domain then if $x_1, \dots, x_n \in B$ are alg over k then $k[x_1, \dots, x_n]$ is a field. (From field theory)

Pf: Via induction on n.

$k[x_1]$ is a field $\Rightarrow \frac{1}{x_1} = a_0 + a_1 x_1 + a_2 x_1^2 + \dots + a_m x_1^m$ $a_i \in k$

$\Rightarrow x_1$ is int over k

$$k[x_1, \dots, x_n] \overset{?}{=} k(x_1)[x_2, \dots, x_n] \quad (\text{as } k[x_1, \dots, x_n] \text{ is a field})$$

where $k(x_1) \subseteq k[x_1, \dots, x_n]$ is the field gen by k & x_1.

By ind hyp with $k = k(x_1)$, $x_2, \dots, x_n$ are algebraic over $k(x_1)$.

So enough to show x_1 is alg over k.

Suppose not, then $k[x_1]$ is isomorphic to a poly ring.

Let $m_{x_2, k(x_1)}(Z) = Z^m + \frac{b_{m-1}(x_1)}{c_{m-1}(x_1)} Z^{m-1} + \dots + \frac{b_0(x_1)}{c_0(x_1)}$

where $b_i(x_1), c_i(x_1) \in k[x_1]$

Then x_2 is integral over $k\left[x_1, \frac{1}{a_2(x_1)}\right]$

where $a_2(x_1) = \prod_{i=0}^{m-1} c_i(x)$

Similarly $\exists\ a_i(x_1) \in k[x_1]$ s.t. x_i is integral over $k\left[x_1, \frac{1}{a_i(x_1)}\right]$. Hence

$x_2, \dots, x_n$ are integral over $k\left[x_1, \frac{1}{a(x_1)}\right]$

where $a(x_1) = \prod_{i=2}^{n} a_i(x_1)$

But $k[x_1]$ has infinitely many prime elements

Let $p(x_1)$ be a prime s.t. $p(x_1) \nmid a(x_1)$; since it is a field

Then $\frac{1}{p(x_1)} \in k[x_1, x_2, \dots, x_n]$ but

$\frac{1}{p(x_1)}$ is not integral over $k[x_1, \frac{1}{a(x_1)}]$

contradiction

to $x_2, \dots, x_n$ int over $k[x_1, \frac{1}{a(x_1)}]$

$$\left(\frac{1}{p(x_1)}\right)^m + \frac{c_{m-1}(x_1)}{a(x_1)^{i_{m-1}}}\left(\frac{1}{p(x_1)}\right)^{m-1} + \dots + \frac{c_0(x_1)}{a(x_1)^{i_0}} = 0$$

in $k(x_1)$

then $a(x_1)^i + c'_{m-1}(x_1)\, p(x_1) + \dots + c'_0(x_1)\, p(x_1)^m = 0$ in $k[x_1]$

$i = \max\{i_0, \dots, i_{m-1}\}$

$\Longrightarrow p(x_1) \mid a(x_1)^i$

$\underset{p(x_1) \text{ is prime}}{\Longrightarrow} p(x_1) \mid a(x_1)$ contra.

$\boxed{\text{Q.E.D.}}$