Lecture 22: Hilbert basis theorem; Modules

02 November 2020
16:46

Recall:

Noetherian Rings

Prop: Let R be a commutative ring with unity. The following are equivalent:

(1) Every R-ideal is finitely generated.

(2) Every increasing chain of R-ideals is eventually constant.

i.e. $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ be a seq of R-ideals then $\exists N$ s.t. $\forall n \geq N$ $I_n = I_N$.

(3) Every non-empty collection of R-ideals has a maximal element. w.r.t inclusion

Def

Def^n A ring satisfying the above equivalent conditions is called a noetherian ring.

Examples: Fields, PID. Hilbert basis thm: R is noeth $\Rightarrow$ $R[x]$ is noeth.

(*) Localization of noetherian is noetherian.

(**) R is noeth I R-ideal then R/I is noeth.

(***) $R_1, \ldots, R_n$ noeth. $\Rightarrow$ $R_1 \times \cdots \times R_n$ is noeth.

(*) Let R be noeth ring and S be a mult. subset of R.

Let $I \subseteq S^{-1}R$ be an $S^{-1}R$-ideal.

We know that $I = S^{-1}J$ where $J = \varphi^{-1}(I)$ is an R-ideal $\varphi : R \to S^{-1}R$

But R is noeth $\Rightarrow$ $\exists\, x_1, \ldots, x_n \in J$ s.t.

$J = (x_1, \ldots, x_n)$

Claim: $I = \left(\frac{x_1}{1}, \ldots, \frac{x_n}{1}\right)$ is $S^{-1}R$.

$\alpha \in I$ then $\alpha = \frac{x}{s}$ for some $x \in J$ & $s \in R$.

But $x = r_1 x_1 + \cdots + r_n x_n$ $r_1, \ldots, r_n \in R$

$\Rightarrow$ $\alpha = \frac{x}{s} = \frac{r_1}{s}\frac{x_1}{1} + \cdots + \frac{r_n}{s}\frac{x_n}{1}$ & note $\frac{r_i}{s} \in S^{-1}R$ $\forall 1 \leq i \leq n$

Hence the claim.

Hence $S^{-1}R$ is noeth.

(*) R noeth & $J \subseteq R/I$ an ideal of R/I where I is an R-ideal.
Then $J = \tilde{J}/I$ where $\tilde{J}$ is an R-ideal containing I.
But R noeth $\Rightarrow \tilde{J} = (x_1, \dots, x_n)$ for some $x_1, \dots, x_n \in \tilde{J}$
$\Rightarrow J = (\bar{x}_1, \dots, \bar{x}_n)$. Hence R/I is noeth.

(*) $R = R_1 \times \dots \times R_n$ where R_i's are noeth and $I \subseteq R$ is an ideal. Then

$$I = I_1 \times \dots \times I_n \quad \text{where } I_j \subseteq R_j \text{ is an ideal } 1 \le j \le n$$

Since $I_1, \dots, I_n$ are f.g., hence I is f.g.
$I_j = (x_{jk} ; 1 \le k \le n_j)$ then I is gen by

$$\{ (x_{1k_1}, x_{2k_2}, \dots, x_{nk_n}) \mid 1 \le k_j \le n_j \}$$

Hence R is noeth.

<u>Ex:</u>
$$\underset{R_n}{\underset{\shortparallel}{\mathbb{Q}[X_1, X_2, \dots, X_n]}} \subseteq \underset{R_{n+1}}{\underset{\shortparallel}{\mathbb{Q}[X_1, X_2, \dots, X_{n+1}]}}$$

$R = \bigcup_{n \ge 1} R_n$ is a ring which is
$= \mathbb{Q}[X_1, X_2, \dots]$
not noetherian

Hilbert basis theorem Let R be a noetherian ring then $R[x]$ is also noetherian.

Pf: Let $I \subseteq R[X]$ be an ideal of $R[X]$.

Let $f_1(x) \in I$ be a nonzero poly of least degree n_1 and $I_1 = (f_1(x))$ be an $R[x]$-ideal

If $I_1 = I$ done.

otherwise $f_2(x) \in I \setminus I_1$ be of least degree n_2 and $I_2 = (f_1, f_2)$ be an $R[x]$-ideal and so on

$f_{i+1} \in I \setminus I_i$ be of least degree n_{i+1} & $I_{i+1} = (f_1, \dots, f_{i+1})$

Let a_i be the leading coeff of f_i and $J = (a_1, a_2, \dots)$ be a R-ideal. Since R is noetherian, $J = (a_1, \dots, a_N)$ for some $N \geq 1$.

Claim: $I = (f_1, \dots, f_N)$

Pf: If not then f_{N+1} exist and $f_{N+1} \in I \setminus I_N$

where $I_N = (f_1, \dots, f_N)$.

$f_{N+1}(x) = a_{N+1} x^{n_{N+1}} +$ lower degree terms.

$a_{N+1} \in J = (a_1, \dots, a_N) \Rightarrow \exists\, b_i \in R$ s.t.

$a_{N+1} = b_1 a_1 + \dots + b_N a_N$

Also $n_{N+1} = \deg f_{N+1} \geq \deg f_i$ for $i < N+1$

Let $g(x) = f_{N+1}(x) - b_1 x^{n_{N+1} - n_1} f_1(x) - b_2 x^{n_{N+1} - n_2} f_2(x) - \dots - b_N x^{n_{N+1} - n_N} f_N(x)$

Since $(f_1, \dots, f_N) = I_N$ and $f_{N+1} \notin I_N$

$\Rightarrow g(x) \notin I_N$. Also $g(x) \in I$

So $g(x) \in I \setminus I_{N+1}$. Also $\deg(g(x)) < n_{N+1} = \deg f_{N+1}$

contradicting the choice of f_{N+1}.

Hence the claim & R is noetherian $\blacksquare$

Note $R[X]$ is noeth $\Rightarrow$ R noeth.

Caution! Subring of noeth need not be noeth.

Example: $\mathbb{Q}[\underbrace{\pi}_{t_1}\ t_2] \subset \mathbb{C}$

Continue this way

$$R = \mathbb{Q}[t_1, t_2, \ldots] \subseteq \mathbb{C}$$

s.t. $\mathbb{Q}[t_1, t_2, \ldots, t_i] \cong \mathbb{Q}[X_1, \ldots, X_i]$

$R \cong \mathbb{Q}[t_1, t_2, \ldots]$ is not noeth.

Modules and submodules

* Given a comm ring with unity R, want to define R-modules.
* In fact if R is field then R-modules are same as R-vector spaces

Def^n: Let R be a field. A R-vector space is a $(M, +, s, R)$ where $+$ is a binary operator on M and $s: R \times M \longrightarrow M$ is a function

satisfying the following axioms

1) $(M, +)$ is an abelian group with identity 0_M.
2) $s(\alpha, x_1 + x_2) = s(\alpha, x_1) + s(\alpha, x_2)$ $\quad \forall \alpha \in R$ & $x_1, x_2 \in M$
3) $s(\alpha_1 + \alpha_2, x) = s(\alpha_1, x) + s(\alpha_2, x)$
4) $s(\alpha_1 \alpha_2, x) = s(\alpha_1, s(\alpha_2, x))$ $\quad \forall x \in M$, $\forall \alpha_1, \alpha_2 \in R$
5) $s(1, x) = x \quad \forall x \in M$.

$\alpha \in R$ & $x \in M$ then $\alpha x \in M$, $\alpha x = s(\alpha, x)$

$(\alpha_1 + \alpha_2) \cdot x = \alpha_1 x + \alpha_2 x$

$(\alpha_1 \alpha_2) x = \alpha_1 \cdot (\alpha_2 \cdot x)$

Def^n: Let R be a ring. An R-module is a $(M, +, s, R)$ where $+$ is a binary operator on M and $s: R \times M \longrightarrow M$ is a function

satisfying the following axioms

1) $(M, +)$ is an abelian group with identity 0_M.
2) $s(\alpha, x_1 + x_2) = s(\alpha, x_1) + s(\alpha, x_2)$ $\quad \forall \alpha \in R$ & $x_1, x_2 \in M$
3) $s(\alpha_1 + \alpha_2, x) = s(\alpha_1, x) + s(\alpha_2, x)$
4) $s(\alpha_1 \alpha_2, x) = s(\alpha_1, s(\alpha_2, x))$ $\quad \forall x \in M$, $\forall \alpha_1, \alpha_2 \in R$
5) $s(1, x) = x \quad \forall x \in M$.

$\alpha \in R$ & $x \in M$ then $\alpha x \in M$, $\alpha x = s(\alpha, x)$

$(\alpha_1 + \alpha_2) \cdot x = \alpha_1 x + \alpha_2 x$

$(\alpha_1 \alpha_2) x = \alpha_1 \cdot (\alpha_2 \cdot x)$

Ex: 1) R a field then R-modules are R-vs

2) $R = \mathbb{Z}$ then $M = \mathbb{Z}$ then $s: R \times M \longrightarrow M$ is the usual multi of integers then M is a R-mod.

More generally R a ring then $(R, +)$ is an R-mod. as well.

(3) $R \subseteq R'$ then any R'-mod is an R-mod.