C1. Ideals and varieties.

17/09.

(short introductia)

0) Rings and modules.

- Ring: abelian group $(+)$ and associative mult. $(\cdot)$ distributive w.r.t. $+$

  For us, all rings will be commutative with unit 1. (mult. identity)

- Field: ring such that every elt $\neq 0$ has an inverse (mult.)

- $a \neq 0$ zero divisor means $\exists b \neq 0$ such that $a \cdot b = 0$

  Ring with zero divisor = domain.

- Modules: they are to rings what vector spaces are to fields.

  R ring; M is an R-module: - M is an abelian group

  - $R \times M \to M$ action R-linear

$$r_1(m_1+m_2) = r_1 m_1 + r_1 m_2$$

$$(r_1+r_2)m_1 = r_1 m_1 + r_2 m_2$$

$$r_1(r_2 m_1) = (r_1 r_2) m_1 \,, \quad 1(m) = m$$

- An R-mod M is finitely generated if $\exists \{m_1, \dots, m_n\} \subseteq M$ such that $\forall m \in M$: $m = \sum_{i=1}^{n} r_i m_i$, $r_i \in R$.

- Important class of modules: ideals (submodules of the ring itself).

$$I \subset R$$

Examples

- a ring is a module over itself.
- R/I is an R-mod, and also R/I-mod.
- M R-mod is free if $M \simeq \bigoplus_{i=1}^{n} R$. Not all modules are like this (compare with vect. spaces).

→ $m \in \mathbb{R}^2$ can be written as $m = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ $a_i \in R$ (similar to linear alg.)

Now, pick $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \in \mathbb{R}^2$ and consider the submodule $R \cdot \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \subseteq M = R^2$

$M' = M / \langle R \cdot \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \rangle$ is not free! $\varepsilon_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\varepsilon_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ non zero in M'

but $r_1 \varepsilon_1 + r_2 \varepsilon_2 = 0$ in M'.

- **Maps:**
  - Ring morph $\phi : A \to B$

$$\begin{cases} \phi(a \cdot b) = \phi(a) \cdot \phi(b) \\ \phi(a+b) = \phi(a) + \phi(b) \\ \phi(1) = 1 \end{cases}$$

  - M_1, M_2 fma A-mod $\Psi : M_1 \to M_2$ A-mod. morph

$$\Psi(m_1 + m_2) = \Psi(m_1) + \Psi(m_2)$$
$$\Psi(a \cdot m_1) = a\,\Psi(m_1)$$

(Important cases: $A \to A/I$ I ideal.)

- $\Psi : M_1 \to M_2$: kernel, image and cokernel ($M_2 / \Psi(M_1)$) are all A-mod.

→ do it.

Ex M2:

• Types of ideals

- I is principal if I can be generated by a single elt
- $I \neq (1)$ is prime if $f \cdot g \in I \Rightarrow f \in I$ or $g \in I$
- $I \neq (1)$ is maximal if $\nexists J$ proper ideal : $I \subsetneq J$

will be used later

- $I \neq (1)$ is primary if $f \cdot g \in I \Rightarrow f \in I$ or $g^n \in I$ (for some n)
- I is irreducible if $\nexists J_1, J_2$ such that $I = J_1 \cap J_2$, $I \subsetneq J_i$.
- I is radical if $f^m \in I \Rightarrow f \in I$ ($m \in \mathbb{N}$).

Exercise: Prove that a maximal ideal is prime.

Exercise: A local ring is a ring with a unique max. ideal $\mathfrak{m}$. Prove that is a local ring, if $f \notin \mathfrak{m}$, then f is a unit.

$\mathfrak{m}$ maximal and $ab \in \mathfrak{m}$. If $a \notin \mathfrak{m}$, then $I = \mathfrak{m} + (a) = R$

Hence $\exists m \in \mathfrak{m}$ and $t \in R$: $1 = m + ta$

$\Rightarrow b = bm + tba \in \mathfrak{m}$. □

1) Ideals and Varieties.

- k is a field. $R = k[x_1, \dots, x_n]$ pol. ring.

  Affine n-space: $\mathbb{A}^n_k = \{(a_1, \dots, a_n) \in k^n\} = \mathbb{A}^n$

  Affine variety: common zero locus of a ~~finite~~ collection of polynomials $f_i \in R$.

  $V(f_1, \dots, f_m)$ variety: $f_1 = \dots = f_m = 0$.

  → "They arise in a lot of applications".

- $V(f_1, \dots, f_m) = V(I)$ only depends on $I = (f_1, \dots, f_m)$ ideal in R.

  (If $I = (g_1, \dots, g_k)$ then ...)

Example: $I = (x^2 - y^2 - 3,\ 2x^2 + 3y^2 - 11)$

$V(I) \subseteq \mathbb{R}^2$? (2 methods).

Option 1: set $u = x^2$ $v = y^2$ then solve in u, v

Option 2: $x^2 = y^2 + 3$ so $2x^2 + 3y^2 - 11 = 0$

$\Leftrightarrow 2(y^2+3) + 3y^2 - 11 = 0$

$5y^2 + 6 - 11 = 5y^2 - 5 = 0$

So $V(I) = V(x^2 - y^2 - 3,\ y^2 - 1)$

$= V(x^2 - 2,\ y^2 - 1)$ □.

⇒ solve this kind of question systematically, i.e. find nice presentation of I. (next lecture).

- Given an ideal $J \subset R$, we have defined $V(J)$ "a geom. object".

  Conversely, given $S \subseteq \mathbb{A}^n_k$, let $I(S)$ be the set of all poly. vanishing on S.

  $I(S)$ is indeed an ideal (easy exercise !).

- Question: If $S = V(J)$ for some J, then do we have $J = I(V(J))$?

  Answer: No. $J = (x^2) \subseteq k[x]$, then $I(V(J)) = (x)$

- However, one always has: $J \subseteq I(V(J))$.

Exercise: Show that | $I_1 \subseteq I_2 \Rightarrow V(I_2) \subseteq V(I_1)$

$S_1 \subseteq S_2 \Rightarrow I(S_2) \subseteq I(S_1)$

⚠ Exercise: Show that $X = V(I(X))$ if X is a variety ($X = V(J)$).

- Natural thing to do to understand varieties, is to break them into "simpler" parts. One possibility are reducible varieties.

Def: a non-empty variety V is irred. if it is not the union of two proper subvarieties:

$V \neq V_1 \cup V_2$ for any V_i : $V_i \subsetneq V$. ⌟

$X \subset V(I(X))$ obvious

Now since $X = V(J)$

$J \subset I(X)$

$\Rightarrow V(I(X)) \subset X$

THM: $I(V)$ is prime $\Leftrightarrow$ V is irreducible.

Proof: ($\Rightarrow$) Assume $I(V)$ is prime and $V = V_1 \cup V_2$ reducible.

Let $I_1 = I(V_1)$ and $I_2 = I(V_2)$.

$\exists\, p \in V_2$ and $f \in I_1$ such that $f(p) \neq 0$

$V_1 = V(I(V_1)) = V(I_1) \longrightarrow$ (otherwise $I_1 \subseteq I_2$ and hence $V(I_2) \subseteq V(I_1)$, i.e. $V_2 \subseteq V_1$; $V(I(X)) = X$ for a variety)

$\exists\, q \in V_1$ and $g \in I_2$ such that $g(q) \neq 0$.

Now $f \cdot g \in I(V) = I(V_1 \cup V_2)$ but $f \notin I(V)$, $g \notin I(V)$ contradiction ($p \in V = V_1 \cup V_2$, $q \in V_2$, $q \notin V_1$)

($\Leftarrow$) Let $f \cdot g \in I(V)$ but $f, g \notin I(V)$.

Let $V_1 = V(I(V) + (f))$ and $V_2 = V(I(V) + (g))$.

$V_1 \cup V_2 \subseteq V$ ($\Leftarrow$): $V_1 \not\subseteq V(I(V))$ for $f \notin I(V)$; $V_2 \not\subseteq V(I(V))$

Moreover, $V \subseteq V_1 \cup V_2$ because $f \cdot g \in I(V)$.

$\forall p \in V$ $f(p) \cdot g(p) = 0$, so $f(p) = 0$ or $g(p) = 0$ (⚠ this choice may vary with p).

$\Leftarrow$ So $V = V_1 \cup V_2$, hence is reducible. □

□

Exercise. I, J ideals, then $I + J$, $I \cdot J$ and $I \cap J$ are ideals.

Show that $V(I + J) = V(I) \cap V(J)$

$V(I \cdot J) = V(I \cap J) = V(I) \cup V(J)$. ⌋

2) Noetherian rings and Hilbert basis THM.

Def: A ring is Noetherian if it contains no infinite ascending chains (infinite proper inclusions) of ideals

$$I_1 \subsetneq I_2 \subsetneq \dots$$

A module is Noetherian if it contains no ascending chain of submodules.

Lemma: A ring is Noetherian iff every ideal is finitely generated.

Proof: ($\Leftarrow$) assume all ideals are finitely generated but $\exists$

$$I_1 \subsetneq I_2 \subsetneq \dots$$

$J = \bigcup_{i=1}^{\infty} I_i$ is an ideal, so J is finitely generated

$\Rightarrow$ contradiction.

($\Rightarrow$) Suppose I is not finitely generated:

build $I_1 = (f_1)$ $I_2 = (f_1, f_2)$ for a sequence of gen...

$\Rightarrow$ contradiction.

□

Exercise: M a module. Prove that TFAE:

1. M contains no infinite ascending chains of submodules
2. Every submodule of M is finitely generated
3. Every nonempty subset Σ of submodules of M has a max element.

THM (Hilbert Basis THM): If A is a Noetherian ring, then so is $A[x]$.

Pf: $I \subset A[x]$ an ideal. To show: I is finitely generated.

$I' = (\text{ideal generated by lead coef of pol. in } I) \subset A$

$\uparrow$ finitely generated $= (g_1, \dots, g_k)$

For all g_i, $\exists\, f_i \in I$: $f_i = g_i x^{m_i} + \dots$ lower deg in x.

Set $m = \max\{x_i\}$, $I'' = (f_1, \dots, f_k)$.

Let $f \in I$. $\exists\, g \in I''$ such that $f - g$ is of deg $< m$.

M the A-module generated by $\{1, x, \dots, x^{m-1}\}$. It is $f - g$.

Hence noetherian. $\Rightarrow M \cap I$ is also noetherian.

$I \subset I'' + M \cap I$.

$\Rightarrow$ finitely gen. $\square$

Rk: If k is a field, then $k[x_1, \dots, x_n]$ is noetherian. So all ideals are finitely generated.

$\Rightarrow$ find nice generating set for an ideal makes sense.

—

3) Associated primes and primary decomposition.

[Goal: Break an ideal (variety) into simpler ones]

Exercise: • Prove that (x^2-4, y^2-1) can be written as the intersection of 4 maximal ideals in $\mathbb{R}[x,y]$.

• Prove that $(x^2-x, xy) = (x) \cap (x-1, y)$, hence is the intersection of a prime and a max. ideal.

→ both ideals are intersection of prim ideals (max is prime).

Rk: → ~~X irred variety ⇒ I(X) is prime~~

more gen.: $X = X_1 \cup \dots \cup X_r$ ~~irred~~ hope to write ~~(I)~~ as the ~~set~~ of prim ideals.

any ideal

⇒ But ~~NO!~~ $(x^2) \subsetneq k[x]$ is not the intersect of prim idals.

↳ However, in a noetherian ring, any ideal can be written as a finite intersect of irred. ideals or primary ideals (go back to definitions).

(see page 3)

Lemma: R noetherian ring, any ideal is a finite intersection of irred. ideals.

Pf: ~~Σ = set of ideals not finite int. of irred ideals~~
Let I_1 be an ideal that is not a finite int. of irred ideals.
I_1 is hence reducible: $I_1 = J_1 \cap J_2$ with both J_1, J_2 larger than I_1. If J_1, J_2 are fin. int. of irred ideals then so is I_1, so some $J_1 = I_2$ is not. We have $I_1 \subsetneq I_2$.
Repeating the construction we get $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$
ascending chain: this is not possible, so I_1 is a fin. int. ... ∎

Lemma: In a noetherian ring R, irred. ideals are primary.

Pf: I irred. let $fg \in I$ but $f \notin I$. we need to show that $g^m \in I$, equiv. $g^m = 0$ in $R/I = A$ for some m.

$$0 \subseteq \underbrace{\operatorname{ann}(g)}_{\{a \in A \mid a \cdot g = 0\}} \subseteq \operatorname{ann}(g^2) \subseteq \dots$$

ideals of A are ideals of R containing I → A is noetherian, so $\exists n : \operatorname{ann}(g^n) = \operatorname{ann}(g^{n+1})$. (*)

(0) is irreducible by assumption and $f \neq 0$ in A (i.e. $(f) \neq 0$)

so $(0) = (g^n) \cap (f)$ would imply that $(g^n) = (0)$.

To prove that $0 = (g^n) \cap (f)$, let $a \in (g^n) \cap (f)$;

$[a \in (f) \Rightarrow a \cdot g = 0$ $(fg \in I).]$ AND $a \in (g^n) \Rightarrow a = b \cdot g^n \overset{(+)}{\Rightarrow} b g^{n+1} = 0$

$\overset{(*)}{\Rightarrow} b \cdot g^n = 0 \Rightarrow a = 0$. ∎

→ Primary decompositions are generally more often used; we will see why (*)

→ Primary ideals are related to prime ideals as follows.

Def: The radical of an ideal I, denoted $\sqrt{I}$, is the set of all f such that $f^n \in I$.
└ I is said radical if $I = \sqrt{I}$.

Exercise: a) If Q is primary then $\sqrt{Q} = P$ is a prime ideal, and P is the smallest prime ideal containing Q.
Q is said to be P-primary.

b) If Q_1 and Q_2 are P-primary, so is $Q_1 \cap Q_2$

c) $I = (x^2, xy)$. Show that $\sqrt{I} = (x)$ but I is not primary.
└ "Not all ideal whose radical is prime is prime".

a) $\sqrt{Q}$ is prime: $f \cdot g \in \sqrt{Q} \Rightarrow f^m g^m \in Q \Rightarrow f^m \in Q$ or $g^{mm'} \in Q \Rightarrow f \in \sqrt{Q}$ or $g \in \sqrt{Q}$.

Let P' prime ideal such that $Q \subseteq P'$. We want to show that $\sqrt{Q} \subseteq P'$: | A prime ideal is radical and $I \subset J \Rightarrow \sqrt{I} \subset \sqrt{J}$

b) More generally, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ (Rq: int. of irred. ideals are not irred.) //

c) $\sqrt{I} = (x)$ clear. (*)

But $x \cdot y \in I$ and $x \notin I$ and $y^p \notin I$. ∎