Algebra 3

Matteo Varbaro, studio 943, email: varbaro@dima.unige.it

Ricevimento: bussare alla porta o accordarsi via email

Motivazioni

Alla fine del corso, tra le altre cose, sapremo risolvere in modo algoritmico problemi come i seguenti:

Problema 1

Dato un sistema di equazioni polinomiali, decidere se ha soluzioni, ed eventualmente dire quante sono. Per esempio, il seguente sistema di equazioni polinomiali

$$\begin{cases} Y^4 + X^3 - 1 = 0 \\ X^4 - X^2Y^3 + Y^5 - 1 = 0 \end{cases}$$

ha soluzioni? Quante?

Problema 2

Come si passa da una rappresentazione parametrica polinomiale a quella cartesiana? Ad esempio, se

$$X = \{(t^2 + t^3, t^4) : t \in \mathbb{C}\} \subseteq \mathbb{C}^2$$

vorremmo trovare un insieme di polinomi $T \subseteq \mathbb{C}[X, Y]$ tale che

$$X = \{(a, b) \in \mathbb{C}^2 : F(a, b) = 0 \ \forall \ F \in T\}.$$

Operazioni fra ideali

In questo corso: "anello" = "anello commutativo e unitario"

Definizione/Proposizione

Siano I, J ideali di un anello A. I seguenti insiemi sono ideali di A:

- $I \cap J$ (intersezione insiemistica);
- $I + J = \{a + b : a \in I, b \in J\}$;
- $IJ = \{a_1 b_1 + a_2 b_2 + \ldots + a_n b_n : n \in \mathbb{N}, a_i \in I, b_i \in J\}$.

Osservazione

$IJ \subseteq I \cap J$:

Operazioni fra ideali

Osservazione

Se I, J, K sono ideali di un anello A, allora

- $I + J = J + I = (I \cup J)$;
- $IJ = JI$;
- $(I + J) + K = I + (J + K)$;
- $(IJ)K = I(JK)$;
- $(I + J)K = IK + JK$.

Osservazione (dipende dal Lemma di Zorn)

Sia I un ideale proprio di un anello A. Allora esiste un ideale massimale $\mathfrak{m}$ di A tale che $I \subseteq \mathfrak{m}$.

Operazioni fra ideali

Osservazione

Se $I_1, \ldots, I_n$ sono ideali di un anello A tali che $\cap_{i=1}^n I_i \subseteq \mathfrak{p}$ per qualche ideale primo $\mathfrak{p}$ di A, allora $\exists\ i \in \{1, \ldots, n\}$ tale che $I_i \subseteq \mathfrak{p}$.

Proposizione

Siano I, J ideali di un anello A. Allora:

- $(I + J)(I \cap J) \subseteq IJ$;
- Se I e J sono coprimi (cioè $I + J = A$), allora $I \cap J = IJ$;
- Se $I_1, \ldots, I_n$ sono ideali di A a due a due coprimi (cioè $I_i + I_j = A$ per ogni $i \neq j$), allora $\cap_{i=1}^n I_i = \prod_{i=1}^n I_i$.

Operazioni fra ideali

Teorema cinese dei resti

Se $I_1, \ldots, I_n$ sono ideali di un anello A a due a due coprimi, allora

$$\cap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i \quad \text{e} \quad A/\cap_{i=1}^{n} I_i \cong \prod_{i=1}^{n} A/I_i$$

Operazioni fra ideali

Remind da Algebra 2 (ideale generato da . . .)

Dato un anello A, *l'ideale generato da un sottoinsieme* $T \subseteq A$ è l'ideale di A più piccolo contenente T, e viene denotato con (T).
Dati elementi $a_1, \ldots, a_n$ di A, l'ideale di A generato da $a_1, \ldots, a_n$ (cioè da $\{a_1, \ldots, a_n\}$) è l'ideale

$$(a_1, \ldots, a_n) = \{\textstyle\sum_{i=1}^{n} x_i a_i : x_1, \ldots, x_n \in A\}$$

Operazioni fra ideali

Un altro ideale importante è l'ideale "colon": Dato un ideale I di un anello A e $a \in A$ definiamo il seguente insieme:

$$I : a = \{x \in A : xa \in I\}$$

Esercizio

Verificare che $I : a$ è un ideale di A contenente I. Inoltre $I : a = I$ se e solo se $\overline{a}$ è un NZD (Non Zero Divisore) di A/I.

Operazioni fra ideali

Definizione

Dato un ideale I di un anello A e un sottoinsieme $J \subseteq A$, l'ideale colon $I : J$ è $I : J = \{x \in A : xa \in I \ \forall \ a \in J\}$.

Esercizio

Se I è un ideale di A, allora:

- $K \subseteq J \implies I : J \subseteq I : K$;
- $I : J = I : (J)$ per ogni sottoinsieme $J \subseteq A$;
- Se $J = (a_1, \ldots, a_n)$, $I : J = \cap_{i=1}^{n} (I : a_i)$.

Remind da Algebra 2 (Emmy Noether)

Un anello A è *Noetheriano* se ogni ideale I di A è finitamente generato, cioè esistono $a_1, \ldots, a_n \in A$ tali che $I = (a_1, \ldots, a_n)$.

Le seguenti sono condizioni equivalenti:

1. A è Noetheriano;
2. per ogni successione debolmente crescente di ideali di A $I_1 \subseteq I_2 \subseteq \ldots I_n \subseteq \ldots$ esiste $n_0 \in \mathbb{N}$ tale che $I_n = I_{n_0}\ \forall\ n \geq n_0$;
3. ogni famiglia non vuota di ideali di A ha un elemento massimale (nella famiglia).

L'equivalenza fra (2) e (3) vale in generale per insiemi parzialmente ordinati. Il punto (2) si può formulare come: "ogni successione debolmente crescente di ideali di A è definitivamente costante" o "non esiste una successione infinita strettamente crescente di ideali di A".

Esempio

Un PID è Noetheriano: infatti ogni suo ideale è generato da un elemento.

Esercizio

Se A è un anello Noetheriano, allora A/I è un anello Noetheriano per ogni ideale I di A.

Osservazione

Se A è Noetheriano, per ogni sottoinsieme T di A esistono $a_1, \ldots, a_n \in T$ tali che $(T) = (a_1, \ldots, a_n)$.

Esercizio

Se A è un anello Noetheriano e $f : A \to A$ è un omomorfismo di anelli surgettivo, allora f è un isomorfismo.

Osservazione

Un sottoanello di un anello Noetheriano può non essere Noetheriano. Ad esempio $A = \mathbb{Q}[X, Y]$, $B = \{a + Xf : f \in A\}$.

- B è un sottoanello di A tale che $\mathbb{Q}[X] \subseteq B$ e $Y \notin B$.
- $(X) \subset (X, XY) \subset (X, XY, XY^2) \subset \ldots$ è una successione infinita strettamente crescente di ideali di B.
- A è Noetheriano per il teorema della base di Hilbert...

Teorema della base (David Hilbert)

Per un anello A sono fatti equivalenti:

1. A è Noetheriano.
2. $A[X]$ è Noetheriano.

Dimostrazione. (2) $\implies$ (1): immediato perché $A \cong A[X]/(X)$.

(1) $\implies$ (2): per assurdo, sia $I \in A[X]$ un ideale non finitamente generato. Costruiamo la seguente successione di polinomi $\{f_n\}_{n\in\mathbb{N}}$:

- f_0 un polinomio di grado minimo di I.
- $\forall\ n \in \mathbb{N}$, f_{n+1} un polinomio di grado minimo di $I \setminus (f_0, \ldots, f_n)$.

Per ogni $n \in \mathbb{N}$, sia $a_n \in A$ il coefficiente direttivo di f_n e $d_n \in \mathbb{N}$ il grado di f_n. Sia $I = (a_i : i \in \mathbb{N})$ l'ideale di A generato dagli a_i.

Essendo A Noetheriano, esiste $n \in \mathbb{N}$ tale che $I = (a_1, \ldots, a_n)$...

Corollario

Se K è un campo, $K[X_1, \ldots, X_n]$ è Noetheriano.

Remind da Algebra 2

Dato un anello A, un elemento $a \in A \setminus U(A)$ si dice **irriducibile** se:

$$a = xy \text{ con } x, y \in A \implies x \in U(A) \text{ o } y \in U(A).$$

Un dominio A si dice **UFD** se:

- $\exists$ Per ogni $0 \neq a \in A \setminus U(A)$ esistono $a_1, \ldots, a_n \in A$ elementi irriducibili tali che $a = a_1 \cdots a_n$.
- ! Se $a_1, \ldots, a_n$ e $b_1, \ldots, b_m$ sono elementi irriducibili di A tali che $a_1 \cdots a_n = b_1 \cdots b_m$, allora $n = m$ e, a meno di riordinare, $(a_i) = (b_i)$ per ogni $i = 1, \ldots, n$.

Dato un elemento non nullo a di un dominio A, se (a) è un ideale primo allora a è irriducibile. Il viceversa vale se A è un UFD. In generale, il fatto che i concetti "essere un elemento irriducibile" e "generare un ideale primo" coincidano è equivalente a "!" in A. D'altro canto, "$\exists$" in A è immediata se A è Noetheriano.

Ricordiamo che in un UFD esistono i concetti di massimo comune divisore **MCD** e di minimo comune multiplo **mcm**.

Definizione

Se A è un UFD e $f \in A[X]$, il **contenuto** di f è $c(f) = \mathrm{MCD}(a_0, \ldots, a_n) \in A$ dove $f = \sum_{i=0}^{n} a_i X^i$ con $a_i \in A$.

Definizione

Se A è un UFD, $f \in A[X]$ si dice **primitivo** se $c(f) = 1$.

Lemma di Gauss (uno dei tanti)

Sia A un UFD, e $f, g \in A[X]$. Allora $c(fg) = c(f)c(g)$. In particolare se f e g sono primitivi lo è anche fg.

Dimostrazione. Prima supponiamo che sia $f = \sum_{i=0}^{n} a_i X^i$ che $g = \sum_{i=0}^{m} b_i X^i$ siano primitivi, cioè che $\mathrm{MCD}(a_0, \ldots, a_n) = \mathrm{MCD}(b_0, \ldots, b_m) = 1$. Vogliamo provare che fg è primitivo, cioè che $\mathrm{MCD}(c_0, \ldots, c_{m+n}) = 1$ dove $c_k = \sum_{i+j=k} a_i b_j$...

Campo delle frazioni di un dominio

Sia A un dominio, e $S = A \setminus \{0\}$. Denotiamo con $\mathrm{Frac}(A)$ l'insieme quoziente $(A \times S)/\sim$ dove $(a, s) \sim (b, t) \iff at = bs$. Denoteremo la classe di (a, s) con a/s.

Definizione/Proposizione

Le applicazioni $+/\cdot : \mathrm{Frac}(A) \times \mathrm{Frac}(A) \to \mathrm{Frac}(A)$ date da $a/s + b/t = (at + bs)/st$ e $a/s \cdot b/t = ab/st$ sono ben definite, e rendono $\mathrm{Frac}(A)$ un campo con $0 = 0/1$ e $1 = 1/1$.

Notazione

Se A è un dominio, denoteremo $\mathrm{Frac}(A[X_1, \ldots, X_n])$ con $A(X_1, \ldots, X_n)$.

Il seguente teorema a volte è anch'esso chiamato Lemma di Gauss

Teorema

Se A è un UFD, allora $A[X]$ è un UFD.

Dimostrazione: ($\exists$). Sia $0 \neq f \in A[X]$, $f \notin U(A[X]) = U(A)$. Vogliamo provare che f ammette una fattorizzazione in elementi irriducibili. Ragioniamo per induzione su $n = \deg(f)$. . . . . .

(!). Basta provare che, dato $f = \sum_{i=0}^{n} a_i X^i \in A[X]$:

$$f \text{ irriducibile} \implies (f) \subseteq A[X] \text{ ideale primo}$$

Se $n = 0$ ok perché A è un UFD:

Se $n > 0$, allora $c(f) = 1$:

Scrivendo $f = \sum_{i=0}^{n} a_i/1 X^i \in K[X]$ dove $K = \mathrm{Frac}(A)$, allora f è irriducibile anche in $K[X]$: se $f = gh$ con $g = \sum_{i=0}^{m} b_i/s_i X^i$ e $h = \sum_{i=0}^{k} c_i/t_i X^i$, siano $s = s_1 \cdots s_m$, $t = t_1 \cdots t_k$ .....

Siccome $K[X]$ è un PID, in particolare un UFD, e f è irriducibile in $K[X]$, allora genera un ideale primo in $K[X]$, perciò in $A[X]$. $\square$

Corollario

Se K è un campo, allora $K[X_1, \ldots, X_n]$ è un UFD.

L'anello di polinomi a coefficienti in un campo K

Abbiamo appena finito di dire che $S = K[X_1, \ldots, X_n]$ è un UFD. In particolare, se $f, g \in S$, esistono MCD(f, g) e mcm(f, g), ma come si calcolano? Se $n = 1$ S è un dominio euclideo, quindi c'è l'algoritmo euclideo, ma se $n > 1$ S non è nemmeno un PID... Fattorizzare f e g in irriducibili non è una buona idea...

In generale, siano I e J ideali di S. Poiché, per il teorema della base, S è Noetheriano, $I = (f_1, \ldots, f_v)$ e $J = (g_1, \ldots, g_w)$. È immediato osservare che, scrivendo $[k] = \{1, \ldots, k\}$ se $k \in \mathbb{N}$:

$$I + J = (f_1, \ldots, f_v, g_1, \ldots, g_w) \quad \text{e} \quad IJ = (f_i g_j : i \in [v], j \in [w])$$

Anche $I \cap J$ e $I : J$, essendo ideali di S, sono finitamente generati, ma calcolarne i generatori non è immediato: trovare un algoritmo per farlo sarà uno degli scopi di questo corso...

Esercizio (Ideali principali: $v = w = 1$, $f = f_1$, $g = g_1$)

$I \cap J = (\text{mcm}(f, g))$ e $I : J = (f / \text{MCD}(f, g))$.

Comunque, non avendo un algoritmo per calcolare MCD e mcm, per ora non sappiamo calcolare in maniera efficiente neppure l'intersezione e il colon di ideali principali.

Esercizio

1. $IJ \subseteq (\mathrm{mcm}(f_i, g_j) : i \in [v], j \in [w]) \subseteq I \cap J$.
2. $I : J \supseteq \bigcap_{j=1}^{w} (f_i / \mathrm{MCD}(f_i, g_j) : i \in [v])$.

Esercizio

Verificare che $I \cap J \supsetneq (\mathrm{mcm}(f_i, g_j) : i \in [v], j \in [w])$ se $S = \mathbb{Q}[X, Y]$, $I = (X^2, Y^2)$, $J = ((X + Y)^2)$.

Definizione

Dato un anello A, un A-**modulo** è un gruppo Abeliano $(M, +)$ dotato di un' operazione $A \times M \to M$, $(a, m) \mapsto am$, tale che:

1. $a(m_1 + m_2) = am_1 + am_2$ per ogni $a \in A, m_1, m_2 \in M$.
2. $(ab)m = a(bm)$ per ogni $a, b \in A, m \in M$.
3. $(a + b)m = am + bm$ per ogni $a, b \in A, m \in M$.
4. $1_A m = m$ per ogni $m \in M$.

Proprietà

1. $0_A m = 0_M$ per ogni $m \in M$.
2. $a0_M = 0_M$ per ogni $a \in A$.
3. $(-a)m = a(-m) = -am$ per ogni $a \in A, m \in M$.

Esempi

1. Se K è un campo, K-moduli $=$ K-spazi vettoriali.
2. $\mathbb{Z}$-moduli $=$ gruppi Abeliani.
3. A è un A-modulo in maniera ovvia.
4. A^n è un A-modulo in maniera naturale per ogni $n \in \mathbb{N}$.

Osservazioni

È possibile dare . . .

1. una struttura di A-modulo ad ogni gruppo Abeliano M?
2. più strutture di A-modulo ad un dato gruppo Abeliano M?
3. ad A una struttura di A-modulo diversa da quella ovvia?

Definizione

Un A-**sottomodulo** di un A-modulo M è un sottogruppo $N \subseteq M$ tale che $an \in N$ per ogni $a \in A, n \in N$.

Esempi

1. Se K è un campo, K-sottomoduli $=$ K-sottospazi vettoriali.
2. $\mathbb{Z}$-sottomoduli $=$ sottogruppi.
3. Gli A-sottomoduli di A sono gli ideali di A.

Definizione/Proposizione

Se N è un A-**sottomodulo** di un A-modulo M, il gruppo quoziente M/N è naturalmente un A-modulo con l'operazione

$$A \times M/N \longrightarrow M/N$$
$$(a, \overline{m}) \mapsto a\overline{m} := \overline{am}$$

Esercizio

Se $\mathcal{F}$ è una famiglia di A-sottomoduli di un A-modulo M, $\cap_{N\in\mathcal{F}} N$ è un A-sottomodulo di M.

Definizione

Se T è un sottoinsieme di un A-modulo M, **l'A-sottomodulo di M generato da T** è l'A-sottomodulo $\langle T\rangle$ di M più piccolo contenente T. Cioè, se $\mathcal{F}$ è la famiglia degli A-sottomoduli di M contenenti T, $\langle T\rangle = \cap_{N\in\mathcal{F}} N$. Se $\langle T\rangle = M$ diciamo che T è un **sistema di generatori di M**.

Definizione

Un A-modulo M è **finitamente generato (f.g.)** se ammette un sistema di generatori finito.

Osservazione

Se T è un sottoinsieme di A, l'A-sottomodulo di A generato da T altro non è che l'ideale di A generato da T: $\langle T \rangle = (T)$.

Esercizio

Se $m_1, \ldots, m_n \in M$, $\langle m_1, \ldots, m_n \rangle = \{\sum_{i=1}^{n} a_i m_i : a_1, \ldots, a_n \in A\}$.

Definizione

Dati due A-moduli M, N, una funzione $\phi : M \to N$ è un **omomorfismo di A-moduli** se:

1. $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$ per ogni $m_1, m_2 \in M$, cioè ϕ è un omomorfismo di gruppi.
2. $\phi(am) = a\phi(m)$ per ogni $a \in A, m \in M$.

Chiamiamo **isomorfismo di A-moduli** un omomorfismo di A-moduli $\phi : M \to N$ bigettivo. Se esiste un isomorfismo di A-moduli da M ad N scriviamo $M \cong N$.

Osservazione

Se $\phi : M \to N$ è un isomorfismo di A-moduli la funzione inversa $\phi^{-1} : N \to M$ è anch' essa un omomorfismo di A-moduli.

Proprietà

Se $\phi : M \to N$ è un omomorfismo di A-moduli abbiamo:

1. $\mathrm{Ker}(\phi) \subseteq M$ è un A-sottomodulo di M.
2. $\mathrm{Im}(\phi) \subseteq N$ è un A-sottomodulo di N.
3. $M/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi)$ (I teorema di isomorfismo per moduli).

Esempio

Se $a \in A$, la moltiplicazione $a\cdot : M \to M$, $m \mapsto am$ è un omomorfismo di A-moduli

Definizione

Diciamo che degli elementi $m_1, \ldots, m_n$ di un A-modulo M sono:

- **linearmente indipendenti (l.i.)** se: dati $a_1, \ldots, a_n \in A$ tali che $\sum_{i=1}^{n} a_i m_i = 0$ si ha $a_i = 0 \ \forall \ i \in [n]$.
- una **base di** M se sono sia l.i. che un sistema di generatori di M.

Gli A-moduli che ammettono una base si chiamano **liberi**.

Esercizio

- A^n è libero con base $e_1, \ldots, e_n$.
- Se M è un A-modulo libero f.g., $M \cong A^n$.

Contrariamente a quanto succede per gli spazi vettoriali, non tutti gli A-moduli sono liberi:

Differenze principali con gli spazi vettoriali

Contrariamente a quanto succede se A è un campo ...

- non è detto che, se $m_1, \ldots, m_n$ sono elementi l.i. di un A-modulo M, uno di essi sia combinazione A-lineare degli altri.
- non è detto che un elemento $m \neq 0$ di un A-modulo M sia l.i..

Almeno si ha:

Proposizione

Se $m_1, \ldots, m_k$ è una base di un A-modulo M e $n_1, \ldots, n_h$ sono un sistema di generatori di M, allora $h \geq k$. In particolare, due basi di un A-modulo libero f.g. hanno la stessa cardinalità.

Dimostrazione: Scriviamo $m_i = \sum_{j=1}^{h} a_{ij} n_j$ e $n_r = \sum_{s=1}^{k} b_{rs} m_s$.
Per assurdo sia $h < k$: siano $U = (u_{ij})$ e $V = (v_{ij})$ le matrici $k \times k$ con entrate in A così definite:

$u_{ij} = a_{ij}$ se $j \leq h$ e 0 altrimenti, e $v_{ij} = b_{ij}$ se $i \leq h$ e 0 altrimenti.

Se $W = (w_{ij}) = UV$ ...

Definizione

Sia M un A-modulo. Dato un A-sottomodulo $N \subseteq M$ e un sottoinsieme $L \subseteq M$, denotiamo con $N : L$ l'ideale di A

$$N : L = \{a \in A : am \in N \ \forall \ m \in L\} \subseteq A$$

Osservazioni

Sia M un A-modulo. Dato un A-sottomodulo $N \subseteq M$ allora:

- $L \subseteq P \implies N : P \subseteq N : L$;
- $N : L = N : \langle L \rangle$ per ogni sottoinsieme $L \subseteq M$;
- Se $L = \langle m_1, \ldots, m_n \rangle$, allora $N : L = \cap_{i=1}^{n} (N : m_i)$.
- $N : L = \overline{0} : \frac{N + \langle L \rangle}{N}$.

L'ultima delle osservazioni precedenti dice che, in qualche modo, il caso in cui $N = 0$ include il caso generale.

Definizione

Sia A un anello e M un A-modulo, e $m \in M$. L'**annullatore di** M è l'ideale $\mathrm{Ann}(M) = 0 : M \subseteq A$, mentre l'**annullatore di** m è l'ideale $\mathrm{Ann}(m) = 0 : m \subseteq A$.

Definizione/Proposizione

Sia A un dominio e M un A-modulo. Il sottoinsieme di M $T(M) = \{m \in M : \mathrm{Ann}(m) \neq 0\}$ è un A-sottomodulo di M, e si chiama il **modulo di torsione di** M.

Se A è un dominio, diciamo che un A-modulo M è **di torsione** se $M = T(M)$, e che è **privo di torsione** se $T(M) = 0$.

Osservazioni

Sia A un dominio e M un A-modulo finitamente generato, allora:

- M è di torsione $\iff$ $\mathrm{Ann}(M) \neq 0$:
- Se M è libero, allora M è privo di torsione:
- Il viceversa è falso: sia $A = \mathbb{Q}[X, Y]$ e $M = (X, Y)\ldots$

In generale un ideale di un dominio A è privo di torsione ma, se non è principale, non è mai libero...

Definizione

Un modulo M su un anello A è Noetheriano se ogni A-sottomodulo N di M è finitamente generato.

Lo stesso argomento usato per gli anelli prova che le seguenti sono condizioni equivalenti:

1. M è Noetheriano;
2. per ogni successione deb. crescente $N_1 \subseteq N_2 \subseteq \ldots N_n \subseteq \ldots$ di A-sottomoduli di M esiste $n_0 \in \mathbb{N}$ tale che $N_n = N_{n_0}\ \forall\ n \geq n_0$;
3. ogni famiglia non vuota di A-sottomoduli di M ha un elemento massimale (nella famiglia).

Osservazione

Un anello A è Noetheriano se e solo se A è Noetheriano come A-modulo.

Proprietà

Dato un anello A e $\phi : M \to N$ un omomorfismo di A-moduli:

- se ϕ è iniettivo, M è Noetheriano $\Leftarrow$ N è Noetheriano. In altre parole, un A-sottomodulo di un A-modulo Noetheriano è Noetheriano;
- se ϕ è surgettivo, M è Noetheriano $\Rightarrow$ N è Noetheriano. In altre parole, un quoziente di un A-modulo Noetheriano è Noetheriano;

Teorema

Se N è un A-sottomodulo di un A-modulo M:

$$M \text{ è Noetheriano} \iff N \text{ e } M/N \text{ sono Noetheriani}$$

Dimostrazione: Sia $M_1 \subseteq M_2 \subseteq \ldots M_n \subseteq \ldots$ una successione debolmente crescente di A-sottomoduli di M ...

Teorema

Sia A un anello Noetheriano. Un A-modulo M è Noetheriano $\iff$ è finitamente generato.

Dimostrazione: "$\implies$" è ovvio, per il viceversa prima proviamo per induzione su $n \in \mathbb{N}$ che $M = A^n$ è Noetheriano ...

Corollario

Sia K un campo e $S = K[X_1, \ldots, X_n]$. Un S-modulo M è Noetheriano se e solo se è finitamente generato.

Quando A è un PID, si ha un teorema di struttura per moduli f.g. analogo a quello per i gruppi abeliani f.g. (che corrispondono ai moduli f.g. sul PID $\mathbb{Z}$): Ogni A-modulo M f.g. ammette una **quasi-base**, cioè un sistema di generatori $m_1, \ldots, m_n$ tali che, dati $a_1, \ldots, a_n \in A$, $\sum_{i=1}^{n} a_i m_i = 0 \implies a_i m_i = 0 \ \forall\ i = 1, \ldots, n$.

Più precisamente abbiamo:

Teorema di struttura per moduli f.g. su un PID

Sia A un PID e M un A-modulo f.g. Allora

$$M \cong A^r \oplus \left(\bigoplus_{i=1}^{s} A/(p_i^{m_i})\right) \text{ con } p_i \in A \text{ irriducibile per ogni } i.$$

Tale scrittura è unica a meno di riordinare i fattori.

Teorema

Sia A un PID. Se M è un A-modulo f.g. privo di torsione, allora M è libero.

Dimostrazione: Procediamo per induzione sul numero n di generatori di M.

Se $n = 1 \ldots$

Se $n > 1$, siano $m_1, \ldots, m_n$ n generatori di M e definiamo $t_1 := m_1$. Se $M/\langle t_1 \rangle$ ha torsione, allora esiste $t \in M \setminus \langle t_1 \rangle$ e $a \in A$ tale che $at \in \langle t_1 \rangle$, cioè $at = bt_1$ per qualche $b \in A$. Osserviamo:

- $a \notin U(A)$:

- Possiamo supporre $\mathrm{MCD}(a, b) = 1$:

Poiché A è un PID, esistono $c, d \in A$ tali che $ca + db = 1$. Quindi $t_1 = cat_1 + dbt_1 = act_1 + dat = a(ct_1 + dt)$. Quindi $t_1 = at_2$ dove $t_2 := ct_1 + dt \in M$. Osserviamo:

- $t_2, m_2, \ldots, m_n$ generano M:
- $\langle t_1 \rangle \subsetneq \langle t_2 \rangle$:

Lemma 1

Sia A un PID. Se M è un A-modulo f.g., allora esiste un unico $n \in \mathbb{N}$ tale che $M \cong A^n \oplus T(M)$.

Dimostrazione: Osserviamo che $M/T(M)$ è privo di torsione:

Essendo M f.g., anche $M/T(M)$ è f.g., dunque $M/T(M) \cong A^n$ per qualche $n \in \mathbb{N}$ grazie al teorema precedente. Inoltre n è unico:

Sia $\overline{m_1}, \ldots, \overline{m_n}$ una base di $M/T(M)$, e $M' = \langle m_1, \ldots, m_n \rangle \subseteq M$. Osserviamo che $M' \cong M/T(M) \cong A^n$ e che $M = M' \oplus T(M)$:

Grazie al lemma precedente per dimostrare il teorema di struttura per moduli f.g. su un PID **basta considerare moduli di torsione**.

Se A è un PID e M è un A-modulo f.g. di torsione, $\exists\ a \in A^*$ t.c.

$$\mathrm{Ann}(M) = (a).$$

Sia $a \sim p_1^{m_1} \cdots p_r^{m_r}$ la fattorizzazione in potenze di irr. distinti di a.

Lemma 2

Sia A un PID e M un A-modulo f.g. di torsione come sopra. Allora esistono A-sottomoduli $M_i \subseteq M$, per $i = 1, \ldots, r$, tali che

$$\mathrm{Ann}(M_i) = (p_i^{m_i}), \quad M = \bigoplus_{i=1}^{r} M_i.$$

Dimostrazione: Per ogni $i = 1, \ldots, r$, sia M_i il nucleo della moltiplicazione per $p_i^{m_i}$ su M. Osserviamo che $\mathrm{Ann}(M_i) = (p_i^{m_i})$:

Se $a_i = a/p_i^{m_i}$ si ha $a_i M \subseteq M_i$.

D'altra parte la moltiplicazione per a_i su M_i è bigettiva:

In particolare la moltiplicazione per a_i su M_i è surgettiva, dunque $a_i M \supseteq a_i M_i = M_i$. Quindi $M_i = a_i M$.

Poiché $\mathrm{MCD}(a_1, \ldots, a_r) = 1$, $M = M_1 + \ldots + M_r$:

Essendo la moltiplicazione per a_i su M_i iniettiva, $M = \bigoplus_{i=1}^{r} M_i$:

Per concludere la dimostrazione del teorema di struttura è quindi sufficiente dimostrarlo per A-moduli f.g. M con $\mathrm{Ann}(M) = (p^k)$ dove p è un elemento irriducibile di A e $k \in \mathbb{N}$.

Proposizione

Sia A un PID e M un A-modulo f.g. con $\mathrm{Ann}(M) = (p^k)$ dove p è un elemento irriducibile di A e $k \in \mathbb{N}$. Allora esistono (unici) numeri naturali $k = h_1 \geq \ldots \geq h_n \geq 1$ tali che $M \cong \bigoplus_{i=1}^{n} A/(p_i^{h_i})$.

Dimostrazione: Ragioniamo per induzione sul minimo numero s di generatori $m_1, \ldots, m_s$ di M:

se $s = 1$ allora $M \cong A/\mathrm{Ann}(m_1)$ e $\mathrm{Ann}(m_1) = \mathrm{Ann}(M) = (p^k)$.

Se $s > 1$, comunque esiste $i = 1, \ldots, s$ tale che $\mathrm{Ann}(m_i) = (p^k)$:

Consideriamo $N = M/\langle m_i \rangle$. Osserviamo che $\mathrm{Ann}(N) = (p^h)$ per qualche $h \leq k$ e che N è generato da $s - 1$ elementi.

Per induzione esistono $x_1, \ldots, x_n \in N$ tali che $N = \bigoplus_{j=1}^{n} \langle x_j \rangle$.

Siano $\mathrm{Ann}(x_j) = (p^{l_j})$ $(l_j \leq h \leq k)$ e $y_j \in M$ tali che $\overline{y_j} = x_j$.
Quindi $p^{l_j} y_j = p^t a m_i$ per qualche $a \in A$ e $t \in \mathbb{N}$ tali che $\mathrm{MCD}(a, p) = 1 \ldots$

Essendo $\mathrm{MCD}(a,p)=1$, $p^{k-t-1+l_j}y_j = p^{k-1}am_i \neq 0$.

Dunque $l_i \leq t$, e se $y_j' = y_j - p^{t-l_j}am_i$ si ha $p^{l_j}y_j' = 0$.

Essendo che $\overline{y_j'} = \overline{y_j} = x_j$ in $N = M/\langle m_i \rangle$, possiamo supporre che $\mathrm{Ann}(y_j) = \mathrm{Ann}(\overline{y_j}) = (p^{l_j})$, cioè che $\langle y_j \rangle \cong \langle \overline{y_j} \rangle \ldots$.

Sia K un campo algebricamente chiuso, V un K-spazio vettoriale di dimensione finita e $\phi : V \to V$ un endomorfismo di V. Vogliamo trovare una base di V tale che la matrice associata a ϕ sia diagonale a blocchi, con blocchi della forma, per qualche $\lambda \in K$,

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \dots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & \lambda & 1 \\ 0 & \dots & \dots & \dots & 0 & \lambda \end{pmatrix}$$

Osserviamo che V è un $K[X]$-modulo ponendo:

$$f \cdot v := f(\phi)v \quad \forall\, f \in K[X], v \in V.$$

Osservazioni

1. Un sistema di generatori di V come K-spazio vettoriale è anche un sistema di generatori di V come $K[X]$-modulo. In particolare, V è un $K[X]$-modulo f.g.
2. I $K[X]$-sottomoduli di V sono esattamente i K-sottospazi $W \subseteq V$ tali che $\phi(W) \subseteq W$.
3. V è un $K[X]$-modulo di torsione.

Essendo $K[X]$ un PID, esistono $v_1, \ldots, v_m \in V$, $f_1, \ldots, f_m \in K[X]$ irriducibili e interi positivi $r_1, \ldots, r_m$ tali che

$$V = \bigoplus_{i=1}^{m} \langle v_i \rangle, \quad \mathrm{Ann}(v_i) = (f_i^{r_i}).$$

Poiché K è algebricamente chiuso, $f_i = X - \lambda_i$ per qualche $\lambda_i \in K$.

Osserviamo che $\dim_K \langle v_i \rangle = r_i$.

Lemma

Gli elementi $u_{i,k} = f_i^{k-1} \cdot v_i$, $k = 1, \ldots, r_i$, sono una base di $\langle v_i \rangle$ come K-spazio vettoriale.

Dimostrazione: ...

Osserviamo che $u_{i,k} = f_i^{k-1} \cdot v_i = f_i \cdot (f_i^{k-2} \cdot v_i) = f_i \cdot u_{i,k-1}$. Quindi

$$\phi(u_{i,h}) = X \cdot u_{i,h} = u_{i,h+1} + \lambda_i u_{i,h} \text{ per ogni } h = 1, \ldots, r_i - 1.$$

Inoltre $\phi(u_{i,r_i}) = X \cdot u_{i,r_i} = f_i \cdot u_{i,r_i} + \lambda_i u_{i,r_i} = \lambda_i u_{i,r_i}$.

Concludiamo: $u_{i,j}$ con $i \in [m], j \in [r_i]$ è la base che volevamo!

Se M è un A-modulo finitamente generato, diciamo da elementi $m_1, \ldots, m_n$, abbiamo un omomorfismo surgettivo di A-moduli

$$\begin{aligned} \phi : A^n &\longrightarrow M \\ e_i &\mapsto m_i \end{aligned}$$

Se A è Noetheriano, anche A^n è Noetheriano, perciò $U = \mathrm{Ker}(\phi) \subseteq A^n$ sarà finitamente generato, diciamo da elementi $v_1 = \sum_{j=1}^{n} a_{1j} e_j, \ldots, v_m = \sum_{j=1}^{n} a_{mj} e_j \ \ldots$

Dunque abbiamo associato ad un A-modulo M f.g. su un anello Noetheriano una matrice $X = (a_{ij}) \in \mathrm{M}_{m,n}(A)$. In altre parole

Corollario

Ogni A-modulo finitamente generato su un anello Noetheriano è isomorfo a $A^n / \mathrm{Im}(\psi_X)$ dove ψ_X è l'omomorfismo di A-moduli $A^m \to A^n$ associato a una matrice $X = (a_{ij}) \in \mathrm{M}_{m,n}(A)$:

$$\psi_X : A^m \longrightarrow A^n$$

$$f_i \mapsto \sum_{j=1}^{n} a_{ij} e_j$$

($f_1, \ldots, f_m$ è una base di A^m e $e_1, \ldots, e_n$ è una base di A^n).

Algebre

Definizione

Dato un anello A, una A-**algebra** è una coppia (B, ϕ) dove B è un anello e $\phi : A \to B$ è un omomorfismo unitario di anelli.
L'omomorfismo ϕ si dice **strutturale**, e spesso sarà sottointeso.

Alternativamente:

Definizione

Dato un anello A, una A-**algebra** è un anello B che è anche un A-modulo con un operazione $* : A \times B \to B$ tale che $a * (b_1 b_2) = (a * b_1) b_2$ per ogni $a \in A, b_1, b_2 \in B$.

Esempi

- Un anello A è un A-algebra con omomorfismo strutturale id_A.
- Se A è un sottoanello di un anello B tale che $1_A = 1_B$, B è un A-algebra con l'inclusione come omomorfismo strutturale.
- $K[X_1, \ldots, X_n]$ è una K-algebra con l'inclusione come omomorfismo strutturale.
- $\mathbb{C}$ è una $\mathbb{R}$-algebra con l'inclusione come omomorfismo strutturale.
- $\mathbb{R}^2$ non è una $\mathbb{R}$-algebra con l'immersione $h : \mathbb{R} \to \mathbb{R}^2$ data da $h(x) = (x, 0)$ come omomorfismo strutturale.

Altri esempi

- Ogni anello A è una $\mathbb{Z}$-algebra con omomorfismo strutturale:
- Dato un anello A e un suo ideale I, A/I è un A-algebra con omomorfismo strutturale $\pi : A \to A/I$, $\pi(a) = \overline{a}$.
- Se A è un dominio, $\mathrm{Frac}(A)$ è una A-algebra con omomorfismo strutturale $A \to \mathrm{Frac}(A)$ dato da $a \mapsto a/1$.

Definizione

Se $B = (B, \phi)$ è una A-algebra, $C \subseteq B$ è una A-sottoalgebra di B se C è un sottoanello di B e $\mathrm{Im}(\phi) \subseteq B$.

Definizione

Se $B = (B, \phi)$ e $C = (C, \psi)$ sono A-algebre, $f : B \to C$ è un **omomorfismo di A-algebre** se f è un omomorfismo unitario di anelli *tale che $f \circ \phi = \psi$, o equivalentemente tale che f sia un omomorfismo di A-moduli*.

Osservazione

Se A è un sottoanello di B e di C con $1_B = 1_A = 1_C$, $f : B \to C$ è un omomorfismo di A-algebre se e solo se f è un omomorfismo unitario di anelli unitari tale che...

Osservazione

Se $B = (B, \phi)$ è una A-algebra e $I \subseteq B$ è un ideale, B/I è naturalmente una A-algebra con omomorfismo strutturale...

D'ora in poi, $A \subseteq B$ anelli $= A$ sottoanello dell'anello B con $1_A = 1_B$.

In tal caso, B verrà considerata come A-algebra con l'inclusione come omomorfismo strutturale.

Se A è un anello, l'anello di polinomi $R = A[X_1, \ldots, X_n]$ è una A-algebra f.g. e, come A-modulo, è libero con base numerabile:

$$(X^{\underline{\alpha}})_{\underline{\alpha} \in \mathbb{N}^n}, \quad X^{\underline{\alpha}} = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \ \forall \ \underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n.$$

Il fatto che l'insieme dei monomi sia una base di R come A-modulo è una conseguenza del principio di identità dei polinomi: dati polinomi di R $f = \sum_{\underline{\alpha} \in \mathbb{N}^n} a_{\underline{\alpha}} X^{\underline{\alpha}}$ e $g = \sum_{\underline{\alpha} \in \mathbb{N}^n} b_{\underline{\alpha}} X^{\underline{\alpha}}$:

$$f = g \iff a_{\underline{\alpha}} = b_{\underline{\alpha}} \ \forall \ \underline{\alpha} \in \mathbb{N}^n,$$

che a sua volta dipende dalla definizione formale: i polinomi sono funzioni $\mathbb{N}^n \to A$ a supporto finito, equivalentemente sottoinsiemi finiti $X \subseteq \mathbb{N}^n \times A$ con fibre $X_{\underline{\alpha}} = \{(\underline{\alpha}, a) \in X\}$ di cardinalità al più 1 $\forall \ \underline{\alpha} \in \mathbb{N}^n$.

Esempio

Il polinomio $X^3 + 4X^2Y^2 - Y^5 \in \mathbb{Z}[X, Y]$ corrisponde a:

- $f : \mathbb{N}^2 \to \mathbb{Z}$ con $f(3,0) = 1$, $f(2,2) = 4$, $f(0,5) = -1$ e $f(a,b) = 0 \ \forall \ (a,b) \in \mathbb{N}^2 \setminus \{(3,0), (2,2), (0,5)\}$.
- $\{((3,0),1), ((2,2),4), ((0,5),-1)\} \subseteq \mathbb{N}^2 \times \mathbb{Z}$.

Proprietà universale dell'anello di polinomi

Siano B una A-algebra e $b_1, \ldots, b_n \in B$. Allora esiste un unico omomorfismo di A-algebre $A[X_1, \ldots, X_n] \xrightarrow{\phi} B$ tale che $\phi(X_i) = b_i$.

Dimostrazione: (!) Siccome ϕ è omomorfismo di anelli, $\phi(X^{\underline{\alpha}}) = b_1^{\alpha_1} \cdots b_n^{\alpha_n} =: \underline{b}^{\underline{\alpha}}$ per ogni $\underline{\alpha} \in \mathbb{N}^n$:

Poiché ϕ è omomorfismo di A-algebre $\phi_{|A}$ è l'omomorfismo strutturale $A \xrightarrow{h} B$, quindi $\phi\left(\sum_{\underline{\alpha} \in \mathbb{N}^n} a_{\underline{\alpha}} X^{\underline{\alpha}}\right) = \sum_{\underline{\alpha} \in \mathbb{N}^n} h(a_{\underline{\alpha}}) \underline{b}^{\underline{\alpha}}$.

($\exists$): Basta provare che $\phi\left(\sum_{\underline{\alpha}\in\mathbb{N}^n} a_{\underline{\alpha}} X^{\underline{\alpha}}\right) = \sum_{\underline{\alpha}\in\mathbb{N}^n} h(a_{\underline{\alpha}}) \underline{b}^{\underline{\alpha}}$ è un omomorfismo di A-algebre.

L'unica proprietà che rimane da verificare è che $\phi(fg) = \phi(f)\phi(g)$ per ogni $f = \sum_{\underline{\alpha}\in\mathbb{N}^n} r_{\underline{\alpha}} X^{\underline{\alpha}}, g = \sum_{\underline{\alpha}\in\mathbb{N}^n} s_{\underline{\alpha}} X^{\underline{\alpha}} \in A[X_1, \ldots, X_n]$: ...

Definizione

Se B è una A-algebra e $b_1, \ldots, b_n \in B$, se ϕ è l'unico omomorfismo di A-algebre $A[X_1, \ldots, X_n] \to B$ tale che $\phi(X_i) = b_i$, $A[b_1, \ldots, b_n] := \mathrm{Im}(\phi)$ si chiama la A-**sottoalgebra di** B **generata da** $b_1, \ldots, b_n$.

Osservazione

$A[b_1, \ldots, b_n]$ è il più piccolo sottoanello di B contenente $h(A)$ e $b_1, \ldots, b_n$, dove $A \xrightarrow{h} B$ è l'omomorfismo strutturale di B.

Come A-modulo, $A[b_1, \ldots, b_n]$ è generato dai monomi $b_1^{\alpha_1} \cdots b_n^{\alpha_n}$ con $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$.

Definizione

Diciamo che B è una A-algebra finitamente generata se esistono $b_1, \ldots, b_n \in B$ tali che $B = A[b_1, \ldots, b_n]$.

Algebre

Esempi

- $\mathbb{Z}[i]$ è una $\mathbb{Z}$-sottoalgebra di $\mathbb{C}$.
- $\mathbb{Q}[\sqrt{2}]$ è una $\mathbb{Q}$-sottoalgebra di $\mathbb{R}$.
- $\mathbb{R}[i]$ è una $\mathbb{R}$-sottoalgebra di $\mathbb{C}$.
- $\mathbb{Q}[t^3, t^4, t^5]$ è una $\mathbb{Q}$-sottoalgebra di $\mathbb{Q}[t]$.
- $\mathbb{Z}[1/2]$ e $\mathbb{Z}[2/3]$ sono $\mathbb{Z}$-sottoalgebre di $\mathbb{Q}$.
- $\mathbb{C}[t^3 + s^3, t^4 + s^4, t^5 + s^5]$ è una $\mathbb{C}$-sottoalgebra di $\mathbb{C}[s, t]$.
- $\mathbb{C}[1/s, 1/t, 1/(s + t)]$ è una $\mathbb{C}$-sottoalgebra di $\mathbb{C}(s, t)$.
- $\mathbb{Z}[X, 1/X] = \mathbb{Z}[X][1/X]$ è una $\mathbb{Z}$-sottoalgebra di $\mathbb{Z}(X)$ (o una $\mathbb{Z}[X]$-sottoalgebra di $\mathbb{Z}(X)$).

Altri esempi

- $\mathbb{C}$ è una $\mathbb{R}$-algebra finitamente generata.
- $A[X_1, \ldots, X_n]$ è una A-algebra finitamente generata.
- $\mathbb{R}$ non è una $\mathbb{Q}$-algebra finitamente generata.

Esercizi

- Se $a, b \in \mathbb{Z}$ sono tali che $\mathrm{MCD}(a, b) = 1$, $\mathbb{Z}[a/b] = \mathbb{Z}[1/b]$.
- Se $X/Y, 1/Y \in \mathbb{Q}(X, Y)$, $\mathbb{Q}[X, Y, X/Y] \subsetneq \mathbb{Q}[X, Y, 1/Y]$.
- $\mathbb{Q}(X)$ non è una $\mathbb{Q}[X]$-algebra finitamente generata. In generale, se A è un UFD con infiniti elementi irriducibili (non associati), $\mathrm{Frac}(A)$ non è una A-algebra finitamente generata.
- Se $A \subseteq B \subseteq C$ sono anelli tali che B è f.g. come A-algebra e C è f.g. come B-algebra, allora C è f.g. come A-algebra.

Proposizione

Ogni A-algebra f.g. B è isomorfa, come A-algebra, a $A[X_1, \ldots, X_n]/I$ per qualche ideale $I \subseteq A[X_1, \ldots, X_n]$. In particolare, se A è Noetheriano, ogni A-algebra f.g. è un anello Noetheriano.

Dimostrazione: Siano $b_1, \ldots, b_n \in B$ tali che $B = A[b_1, \ldots, b_n]$ e $A[X_1, \ldots, X_n] \xrightarrow{\phi} B$ l'omom. di A-algebre definito da $\phi(X_i) = b_i$...

Definizione

L'ideale $I \subseteq A[X_1, \ldots, X_n]$ si dice l'ideale di definizione, o di presentazione, o delle relazioni, di B.

Esempi

- $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$.
- $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[X]/(X^2-2)$, $\mathbb{Q}[i\sqrt{2}] \cong \mathbb{Q}[X]/(X^2+2)$.
- $\mathbb{C} = \mathbb{R}[i] \cong \mathbb{R}[X]/(X^2+1)$.
- $\mathbb{Q}[t^3, t^4, t^5] \cong \mathbb{Q}[X,Y,Z]/(X^3-YZ, Y^2-XZ, Z^2-X^2Y, ???)$.
- $\mathbb{Z}[1/2] \cong \mathbb{Z}[X]/(2X-1)$.
- $\mathbb{C}[t^3+s^3, t^4+s^4, t^5+s^5] \cong \mathbb{C}[X,Y,Z]/(f)$ dove

$$\begin{aligned} f = \quad & 2X^{10} - 10X^6Y^3 - 50X^2Y^6 + 120X^3Y^4Z \\ & -60X^4Y^2Z^2 + 8X^5Z^3 + 36Y^5Z^2 \\ & -80XY^3Z^3 + 30X^2YZ^4 + 4Z^6 \end{aligned}$$

Cosa che sapremo fare (algoritmicamente) alla fine del corso:

Problema

Sia K un campo, $S = K[X_1, \ldots, X_n]$, $f_1, \ldots, f_s \in S$ e $B = K[f_1, \ldots, f_s] \subseteq S$.

- Calcolare l'ideale delle relazioni di B.
- Dato $f \in S$, decidere se $f \in B$, e in caso affermativo determinare $F \in K[Y_1, \ldots, Y_s]$ tale che $F(f_1, \ldots, f_s) = f$.
- Stessi problemi rimpiazzando S con $\mathrm{Frac}(S) = K(X_1, \ldots, X_n)$.

All'inizio del corso abbiamo osservato che un sottoanello di un anello Noetheriano può non essere Noetheriano. In quell'esempio avevamo $C = A[X, Y]$, $B = \{a + Xf : a \in A, f \in C\} \subseteq C$ e $A = \mathbb{Q} \subseteq B$. In particolare, in questo esempio $A \subseteq B \subseteq C$ sono anelli con A Noetheriano, C f.g. come A-algebra, ma B non f.g. come A-algebra...

Lemma di Artin-Tate

Siano $A \subseteq B \subseteq C$ anelli. Se:

1. A è Noetheriano.
2. C è finitamente generata come A-algebra.
3. C è finitamente generato come B-modulo.

Allora B è finitamente generata come A-algebra.

Dimostrazione: Siano $c_1, \ldots, c_n \in C$ tali che $C = A[c_1, \ldots, c_n]$ e $x_1, \ldots, x_m \in C$ generatori di C come B-modulo. Scriviamo:

- $c_i = \sum_{j=1}^{m} b_{ij} x_j$ con $b_{ij} \in B$ $(\forall\ i \in [n])$;
- $x_r x_s = \sum_{k=1}^{m} b_{rsk} x_k$ con $b_{rsk} \in B$ $(\forall\ r, s \in [m], r \leq s)$;
- $B_0 = A[b_{ij}, b_{rsk} : i \in [n], j, r, s, k \in [m], r \leq s]$.

B_0 è una A-sottoalgebra Noetheriana di B...

Osserviamo che $x_1, \ldots, x_m \in C$ generano C anche come B_0-modulo:

Dunque C è un B_0-modulo Noetheriano, e perciò $B \subseteq C$ è finitamente generato come B_0-modulo...

Algebre

Sia $(\Gamma, +)$ un monoide commutativo. Una **struttura Γ-graduata** di un anello A è una collezione $\{A_\gamma\}_{\gamma\in\Gamma}$ di sottogruppi (additivi) di A tali che:

1. $A = \bigoplus_{\gamma\in\Gamma} A_\gamma$.
2. $A_\gamma A_\delta \subseteq A_{\gamma+\delta}$ per ogni $\gamma, \delta \in \Gamma$.

In tal caso diciamo che $A = \bigoplus_{\gamma\in\Gamma} A_\gamma$ è un **anello Γ-graduato**.

Esempi

1. Ogni anello A ammette una struttura Γ-graduata ponendo $A_0 = A$ e $A_\gamma = 0$ per ogni $0 \neq \gamma \in \Gamma$.
2. $R = A[X]$ è $\mathbb{N}$-graduato ponendo, per ogni $d \in \mathbb{N}$, $R_d = \{aX^d : a \in A\}$:
3. $R = A[X_1, \ldots, X_n]$ è $\mathbb{N}^n$-graduato ponendo, per ogni $\underline{\alpha} \in \mathbb{N}^n$, $R_{\underline{\alpha}} = \{aX^{\underline{\alpha}} : a \in A\}$:

Se $A = \bigoplus_{\gamma\in\Gamma} A_\gamma$ è un anello Γ-graduato, $a \in A$ si dice **omogeneo di grado** γ se $a \in A_\gamma$; in tal caso scriveremo $\deg(a) = \gamma$.

In generale, ogni $a \in A$ si scrive in maniera unica come somma finita $a = \sum_{\gamma\in\Gamma} a_\gamma$ con $a_\gamma \in A_\gamma$, che si dice **la componente omogenea** di a di grado γ.

Esercizio

Se $A = \bigoplus_{\gamma\in\Gamma} A_\gamma$ è un anello Γ-graduato, $1 \in A_0$.

Osservazioni

Sia $A = \bigoplus_{\gamma \in \Gamma} A_\gamma$ un anello Γ-graduato. Allora:

1. A_0 è un sottoanello di A con $1_{A_0} = 1_A$:
2. A è un A_0-algebra.
3. A_γ è un A_0-modulo per ogni $\gamma \in \Gamma$:

Definizione

R è una A-algebra Γ-graduata se $R = \bigoplus_{\gamma \in \Gamma} R_\gamma$ con $R_0 = A$.

Struttura $\mathbb{N}$-graduata dell'anello di polinomi

Sia $R = A[X_1, \ldots, X_n]$. Il supporto di $f = \sum_{\underline{\alpha} \in \mathbb{N}^n} a_{\underline{\alpha}} X^{\underline{\alpha}} \in R$ è

$$\mathrm{supp}(f) = \{\underline{\alpha} \in \mathbb{N}^n : a_{\underline{\alpha}} \neq 0\} \subseteq \mathbb{N}^n.$$

Diciamo che $g \in R$ è omogeneo di grado $d \in \mathbb{N}$ se

$$|\underline{\alpha}| = \alpha_1 + \ldots + \alpha_n = d \text{ per ogni } \underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathrm{supp}(g).$$

Se $R_d = \{g \in R : g \text{ è omogeneo di grado } d\}$, $R = \bigoplus_{d \in \mathbb{N}} R_d$ è una A-algebra $\mathbb{N}$-graduata.

Esercizio: strutture $\mathbb{N}$-graduate non-standard dell'anello di polinomi

Sia $R = A[X_1, \ldots, X_n]$. Dato $\underline{w} \in \mathbb{N}^n$, per ogni $d \in \mathbb{N}$ poniamo

$$R_d = \{g \in R : \underline{\alpha} \cdot {}^t\underline{w} = d \ \forall\ \underline{\alpha} \in \mathrm{supp}(g)\}.$$

Allora $R = \bigoplus_{d \in \mathbb{N}} R_d$ è una A-algebra $\mathbb{N}$-graduata.

Algebre

Se $I \subseteq A = \bigoplus_{\gamma\in\Gamma} A_\gamma$ si ha $\bigoplus_{\gamma\in\Gamma} I \cap A_\gamma \subseteq I$.

Definizione

Sia $A = \bigoplus_{\gamma\in\Gamma} A_\gamma$ un anello Γ-graduato. Un ideale $I \subseteq A$ si dice Γ-omogeneo se $\bigoplus_{\gamma\in\Gamma} I \cap A_\gamma = I$.

Proposizione

Sia $A = \bigoplus_{\gamma\in\Gamma} A_\gamma$ un anello Γ-graduato. Dato un ideale $I \subseteq A$ sono fatti equivalenti:

1. I è Γ-omogeneo.
2. $a = \sum_{\gamma\in\Gamma} a_\gamma \in I \implies a_\gamma \in I \ \forall\ \gamma \in \Gamma$.
3. I è generato da elementi omogenei.

Dimostrazione: (1) $\iff$ (2) è una tautologia. (2) $\implies$ (3):

(3) $\implies$ (2): Sia $I = (T)$ dove $T \subseteq A$ è un insieme di elementi omogenei. Se $f \in I$, esistono $x_1, \ldots, x_n \in T$, $a_1, \ldots, a_n \in A$, t.c.

$$f = \sum_{i=1}^{n} a_i x_i.$$

Sia $\gamma \in \Gamma$ e poniamo $\deg(x_i) = \delta_i \in \Gamma$. Per provare $f_\gamma \in I$ poniamo

$$X(\gamma, i) = \{\alpha \in \Gamma : \alpha + \delta_i = \gamma\} \subseteq \Gamma \qquad \forall\ i \in [n] \ldots$$

Se K è un campo, l'anello di polinomi $S = K[X_1, \ldots, X_n]$ ha due strutture graduate importanti:

1. Quella $\mathbb{N}$-graduata: $\deg(X_i) = 1 \in \mathbb{N} \ \forall \ i \in [n]$.
2. Quella $\mathbb{N}^n$-graduata: $\deg(X_i) = e_i \in \mathbb{N}^n \ \forall \ i \in [n]$.

Chiameremo gli ideali $\mathbb{N}$-omogenei di S semplicemente **ideali omogenei**, e quelli $\mathbb{N}^n$-omogenei **ideali monomiali**.

Osservazione

Un ideale $I \subseteq S$ è monomiale se e solo se è generato da un insieme (finito) di monomi $X^{\underline{\alpha}}$.

Esercizio

Sia $A = \bigoplus_{\gamma \in \Gamma} A_\gamma$ un anello Γ-graduato. Siano I e J ideali Γ-omogenei di A:

- $I \cap J$ è un ideale Γ-omogeneo di A.
- IJ è un ideale Γ-omogeneo di A.
- Se Γ è cancellativo ($\gamma + \alpha = \gamma + \beta \implies \alpha = \beta \ \forall \ \alpha, \beta, \gamma \in \Gamma$), $I : J$ è un ideale Γ-omogeneo di A.

Osservazione

$\mathbb{N}$ e $\mathbb{N}^n$ sono cancellativi.

Corollario

L'intersezione, il prodotto e il colon fra ideali monomiali (omogenei) di $K[X_1, \ldots, X_n]$ è un ideale monomiale (omogeneo).

Proposizione

Sia Γ cancellativo, e $A = \bigoplus_{\gamma \in \Gamma} A_\gamma$ un anello Γ-graduato. Se A è Noetheriano, allora A_γ è un A_0-modulo finitamente generato per ogni $\gamma \in \Gamma$.

Dimostrazione: Consideriamo l'ideale $I = (A_\gamma) \subseteq A$. Poiché A è Noetheriano, esistono $x_1, \ldots, x_n \in A_\gamma$ tali che $I = (x_1, \ldots, x_n)$. Vediamo che $x_1, \ldots, x_n$ genero A_γ come A_0-modulo:

Algebre

Definizione

Un monoide commutativo $(\Gamma, +)$ si dice privo di opposti se, per ogni $0 \neq \gamma \in \Gamma$ si ha $\gamma + \delta \neq 0 \ \forall \ \delta \in \Gamma$.

Osservazione

$\mathbb{N}$ e $\mathbb{N}^n$ sono privi di opposti.

Lemma

Sia Γ privo di opposti e $A = \bigoplus_{\gamma \in \Gamma} A_\gamma$ un anello Γ-graduato. Allora $\mathfrak{m} = \bigoplus_{\gamma \in \Gamma^*} A_\gamma$ è un ideale omogeneo di A e $A/\mathfrak{m} \cong A_0$.

Dimostrazione: Che $\mathfrak{m}$ sia un gruppo additivo è ovvio, quindi basta provare che, per ogni $x \in \mathfrak{m}$ e $a \in A$, $xa \in \mathfrak{m}$. Scriviamo $x = \sum_{\gamma \in \Gamma^*} x_\gamma$ e $a = \sum_{\delta \in \Gamma} a_\delta \ldots$

Sia $\phi : A \to A_0$ la funzione definita da $\phi(a) = a_0$ (componente omogenea di grado 0). Osserviamo che ϕ è un omomorfismo surgettivo di anelli con $\mathfrak{m} = \mathrm{Ker}(\phi)$:

Concludiamo grazie al primo teorema di isomorfismo per anelli.

Algebre

Definizione

Dato un ideale I di un anello A, un insieme di generatori $T \subseteq A$ si dice minimale se $(T \setminus \{t\}) \neq I$ per ogni $t \in T$.

Esempi

- Se $A = \mathbb{Z}$, l'insieme di generatori $\{2, 4\}$ dell'ideale dei numeri pari non è minimale.
- Se $A = \mathbb{Q}[X, Y, Z]$, $X - Y, X - Z, Y - Z$ non è un sistema di generatori minimale di $I = (X - Y, X - Z, Y - Z)$.
- Se $A = \mathbb{Q}[X]$, entrambi gli insiemi $\{X^2, X^2 + X\}$ e $\{X\}$ sono insiemi di generatori minimali di $I = (X)$.

Teorema

Sia Γ privo di opposti e $A = \bigoplus_{\gamma\in\Gamma} A_\gamma$ un anello Γ-graduato con $A_0 = K$ un campo. Supponiamo che A sia Noetheriano. Dato un ideale Γ-omogeneo $I \subseteq A$ si ha:

1. I non può essere generato da meno di $\dim_K(I/\mathfrak{m}I)$ elementi (dove $\mathfrak{m} = \bigoplus_{\gamma\in\Gamma^*} A_\gamma$).
2. Se Γ è cancellativo, ogni sistema minimale di generatori omogenei di I ha la stessa cardinalità, cioè $\dim_K(I/\mathfrak{m}I)$.

Dimostrazione: Riguardo a (1), siano $x_1, \ldots, x_r$ un sistema di generatori di I. Allora $\overline{x_1}, \ldots, \overline{x_r}$ generano l'$A/\mathfrak{m}$-spazio vettoriale $I/\mathfrak{m}I$, dunque è chiaro che $r \geq \dim_K(I/\mathfrak{m}I)$.

Per (2), siano $x_1, \ldots, x_n$ un sistema minimale di generatori omogenei di I: come prima $\overline{x_1}, \ldots, \overline{x_n}$ generano l'$A/\mathfrak{m}$-spazio vettoriale $I/\mathfrak{m}I$, vogliamo provare che sono linearmente indipendenti:

Quindi $\overline{x_1}, \ldots, \overline{x_n}$ sono una base di $I/\mathfrak{m}I$, dunque $n = \dim_K(I/\mathfrak{m}I)$.

Esempi

- Se $S = K[X_1, \ldots, X_n]$, l'ideale $\mathfrak{m} = (X_1, \ldots, X_n) \subseteq S$ non può essere generato da meno di n elementi.

- L'ideale $(X + Y, X^2 + Y^2)$ di $\mathbb{Q}[X, Y]$ non è principale.

Algebre

Teorema

Sia $A = \bigoplus_{d \in \mathbb{N}} A_d$ un anello $\mathbb{N}$-graduato. Sono fatti equivalenti:

1. A_0 è un anello Noetheriano e A è una A_0-algebra f.g.
2. A è un anello Noetheriano.

Dimostrazione: "(1) $\Rightarrow$ (2)" vale in generale per A_0-algebre.

Riguardo a "(2) $\Rightarrow$ (1)", se $\mathfrak{m} = \bigoplus_{d \in \mathbb{N}^*} A_d$ si ha $A/\mathfrak{m} \cong A_0$, dunque A_0 è Noetheriano. Siano $x_1, \ldots, x_n$ dei generatori omogenei di $\mathfrak{m}$. Vogliamo provare che $A = A_0[x_1, \ldots, x_n]$: ...

Algebre

Ideali monomiali

Per il resto delle slides, K sarà un campo e $S = K[X_1, \ldots, X_n]$.
Ricordiamo che S è dotato di una struttura $\mathbb{N}^n$-graduata ponendo

$$S_{\underline{\alpha}} = \{\lambda X^{\underline{\alpha}} : \lambda \in K\} \quad \forall\, \underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \qquad (X^{\underline{\alpha}} := X_1^{\alpha_1} \cdots X_n^{\alpha_n}).$$

Gli ideali $\mathbb{N}^n$-graduati di S si chiamano **ideali monomiali**. Sia $\mathrm{Mon}(S) := \{X^{\underline{\alpha}} : \underline{\alpha} \in \mathbb{N}^n\}$ l'insieme dei monomi di S e, dato $f = \sum_{\underline{\alpha} \in \mathbb{N}^n} \lambda_{\underline{\alpha}} X^{\underline{\alpha}} \in S$, $\mathrm{supp}(f) := \{X^{\underline{\alpha}} : \lambda_{\underline{\alpha}} \neq 0\} \subseteq \mathrm{Mon}(S)$.

Definizione/Proposizione

Dato un ideale $I \subseteq S$ sono fatti equivalenti:

1. I è monomiale.
2. Se $f \in I$, $\mathrm{supp}(f) \subseteq I$.
3. Esiste un insieme $T \subseteq \mathrm{Mon}(S)$ tale che $I = (T)$.

Osservazione

$\mathrm{Mon}(S)$ è una base di S come K-spazio vettoriale che è chiusa rispetto alla moltiplicazione.

Osservazione

Sia $f = \sum_{i=1}^{m} f_i \in S$, con $f_i \in S$, e $u \in \mathrm{Mon}(S)$.

1. $\mathrm{supp}(f) \subseteq \bigcup_{i=1}^{m} \mathrm{supp}(f_i)$.
2. $\mathrm{supp}(uf) = \{uv : v \in \mathrm{supp}(f)\}$.

Lemma

Sia $T \subseteq \mathrm{Mon}(S)$, $I = (T)$ e $f \in S$. Allora

$$f \in I \iff \forall\, v \in \mathrm{supp}(f)\ \exists\, u \in T : u|v.$$

Consideriamo l'ordine parziale su $\mathrm{Mon}(S)$ dato dalla divisibilità:

$$\forall\ u, v \in \mathrm{Mon}(S), u \leq v \iff u|v.$$

Lemma

Se $T \subseteq \mathrm{Mon}(S)$, per ogni $v \in T$ esiste $u \in T$ minimale in T (cioè non diviso da altri elementi di T) tale che $u|v$.

Dimostrazione: Sia $T(v) = \{t \in T : t|v\} \subseteq T$ ....

Lemma

Se $T \subseteq \mathrm{Mon}(S)$ il sottoinsieme $T_0 \subseteq T$ degli elementi minimali in T è finito.

Dimostrazione: Sia $I = (T) \subseteq S$. ...

Ideali monomiali

Ricapitolando, $I \subseteq S$ è un ideale monomiale se e solo se I è generato da un insieme finito di monomi $u_1, \ldots, u_m$.

Inoltre il sistema di generatori $u_1, \ldots, u_m$ è minimale se e solo se non esistono $i \neq j$ tali che $u_i | u_j$.

Il sistema minimale di generatori monomiali $u_1, \ldots, u_m$ di I è univocamente determinato da I, e verrà denotato con $M(I)$.

Inoltre, un ideale monomiale $I \subseteq S$ non può essere generato da meno di $m = |M(I)|$ polinomi, ed ogni sistema minimale di generatori omogenei di I ha cardinalità uguale ad m.

Infine, dato $f \in S$, si ha $f \in I \iff \forall\, v \in \mathrm{supp}(f)\ \exists\, u \in M(I) : u | v$

Ideali monomiali

Osservazione

Siccome $X_i \in S$ è irriducibile $\forall\ i \in [n]$, dati $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ e $\underline{\beta} = (\beta_1, \ldots, \beta_n)$ si ha:

- $\mathrm{MCD}(X^{\underline{\alpha}}, X^{\underline{\beta}}) = X_1^{\min\{\alpha_1,\beta_1\}} \cdots X_n^{\min\{\alpha_n,\beta_n\}}$.
- $\mathrm{mcm}(X^{\underline{\alpha}}, X^{\underline{\beta}}) = X_1^{\max\{\alpha_1,\beta_1\}} \cdots X_n^{\max\{\alpha_n,\beta_n\}}$.

Proposizione

Siano $I = (u_1, \ldots, u_r)$ e $J = (v_1, \ldots, v_s)$ ideali monomiali con $u_i, v_j \in \mathrm{Mon}(S)$. Si ha:

1. $I \cap J = (\mathrm{mcm}(u_i, v_j) : i \in [r], j \in [s])$.
2. $I : J = \bigcap_{j=1}^{s} (u_i / \mathrm{MCD}(u_i, v_j) : i \in [r])$.

Dimostrazione:

Ideali monomiali

Definizione

Se $f = f_1^{a_1} \cdots f_v^{a_v}$ con f_i irriducibili, $a_i > 0$, e $(f_i) \neq (f_j)$ se $i \neq j$, definiamo $\mathrm{sqfree}(f) := f_1 \cdots f_v$.

Osservazione

Se $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ e $u = X^{\underline{\alpha}}$, $\mathrm{sqfree}(u) = \prod_{i \in F} X_i$ dove $F = \{i \in [n] : \alpha_i > 0\} \subseteq [n]$.

Definizione

Se $F \subseteq [n]$, denotiamo con $X^F := \prod_{i \in F} X_i \in \mathrm{Mon}(S)$ e $\mathfrak{p}_F := (X_i : i \in F) \subseteq S$.

Ideali monomiali

Osservazione

Se $F \subseteq [n]$, $\mathfrak{p}_F \subseteq S$ è un ideale primo. Inoltre, se $u \in \mathrm{Mon}(S)$, $u \in \mathfrak{p}_F \iff \mathrm{MCD}(u, \mathrm{X}^F) \neq 1$.

Di conseguenza, se $F_1, \ldots, F_m \subseteq [n]$ e $u \in \mathrm{Mon}(S)$,

$$u \in \bigcap_{i=1}^{m} \mathfrak{p}_{F_i} \iff \mathrm{MCD}(u, \mathrm{X}^{F_i}) \neq 1 \ \forall \ i \in [m]$$

Teorema

Se $I = (u_1, \ldots, u_m) \subseteq S$ è un ideale monomiale generato da monomi $u_1, \ldots, u_m$, sia $V := \{F \subseteq [n] : I \subseteq \mathfrak{p}_F\}$. Allora

$$(\mathrm{sqfree}(u_1), \ldots, \mathrm{sqfree}(u_m)) = \bigcap_{F \in V} \mathfrak{p}_F$$

Dimostrazione:

Diciamo che $f \in S$ è **squarefree** se $f = \mathrm{sqfree}(f)$.

Esempio

Se $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $X^{\underline{\alpha}}$ è squarefree se e solo se $\alpha_i \leq 1 \ \forall \ i \in [n]$.

Proposizione

Se $I \subseteq S$ è un ideale monomiale, allora:

1. I è massimale se e solo se $I = (X_1, \ldots, X_n)$.
2. I è primo se e solo se esiste $F \subseteq [n]$ tale che $I = \mathfrak{p}_F$.
3. I è radicale se e solo se I è generato da monomi squarefree.

Dimostrazione:

Ideali monomiali

Sia $G = (K^*)^n$ il **toro algebrico**. Dato $\underline{\lambda} = (\lambda_1, \ldots, \lambda_n) \in G$, consideriamo l'omomorfismo di K-algebre $\phi_{\underline{\lambda}} : S \to S$ dato da $\phi_{\underline{\lambda}}(X_i) = \lambda_i X_i$, e l'applicazione

$$\rho : G \times S \to S, \quad \rho(\underline{\lambda}, f) = \underline{\lambda} \cdot f = \phi_{\underline{\lambda}}(f)$$

Osservazione

ρ è un'azione e $\phi_{\underline{\lambda}}(I) = I$ per ogni $\underline{\lambda} \in (K^*)^n$ e per ogni ideale monomiale $I \subseteq S$.

Esercizio

Se K è infinito e $0 \neq f \in S$, esiste $\underline{\lambda} \in (K^*)^n$ tale che $f(\underline{\lambda}) \neq 0$.

Teorema

Se K è infinito, per un ideale $I \subseteq S$ sono equivalenti:

1. I è monomiale.
2. $\phi_{\underline{\lambda}}(I) = I$ per ogni $\underline{\lambda} \in (K^*)^n$.

Dimostrazione: (1) $\implies$ (2) lo abbiamo già osservato.

Per (2) $\implies$ (1), sia $f \in I$: proveremo che $\mathrm{supp}(f) \subseteq I$ per induzione su $|\mathrm{supp}(f)|$. Se $|\mathrm{supp}(f)| = 1$ è ovvio.

Altrimenti sia $X^{\underline{\alpha}} \in \mathrm{supp}(f)$ e $f = \mu X^{\underline{\alpha}} + g$ con $\mu \in K^*$ e $g \in S$ con $X^{\underline{\alpha}} \notin \mathrm{supp}(g)\ldots$

Ideali monomiali

Domanda

Come fare i calcoli in maniera efficace in S/I? In analogia con $K[X]/(f)$, vorremmo descrivere una base come K-spazio vettoriale e un efficiente algoritmo di moltiplicazione in $S/I\ldots$

Teorema di Macaulay per ideali monomiali

Sia $I \subseteq S$ un ideale monomiale, e $B = \{\overline{X^{\underline{\alpha}}} \in S/I : X^{\underline{\alpha}} \notin I\}$. Allora B è una base di S/I come K-spazio vettoriale, e la moltiplicazione è data da:

$$\overline{X^{\underline{\alpha}}}\overline{X^{\underline{\beta}}} = \begin{cases} \overline{X^{\underline{\alpha}+\underline{\beta}}} & \text{se } \overline{X^{\underline{\alpha}+\underline{\beta}}} \in B \\ \overline{0} & \text{se } \overline{X^{\underline{\alpha}+\underline{\beta}}} \notin B \end{cases}$$

Dimostrazione:

Esempi

1. Se $I = (X^2, XY^2, Y^3) \subseteq S = K[X, Y]$ allora i monomi non in I sono $1, X, Y, XY, Y^2$ e le loro classi sono una base di S/I come K-spazio vettoriale. In particolare $\dim_K S/I = 5$.
2. Se $I = (X^2, XY^2, Y^3) \subseteq S = K[X, Y, Z]$ allora i monomi non in I sono $1, X, Y, XY, Y^2$ ed ogni monomio ottenuto da questi moltiplicando per una potenza di Z. In particolare S/I è un K-spazio vettoriale di dimensione infinita.

Radicale di un ideale

Definizione

Dato un ideale I di un anello A, il radicale di I è definito come

$$\sqrt{I} = \{a \in S : \text{ esiste } n \in \mathbb{N} \text{ tale che } a^n \in I\}$$

Osservazione

Per ogni ideale $I \subseteq A$, $\sqrt{I}$ è un ideale di A.

Proposizione

Dato un ideale I di un anello A, $\sqrt{I}$ è l'ideale radicale di A più piccolo contenente I. In particolare, $I \subseteq \sqrt{I}$, vale l'uguale se e solo se I è radicale, e $\sqrt{\sqrt{I}} = \sqrt{I}$.

Dimostrazione:

Radicale di un ideale

Esercizio

Sia $A = K[X, Y, Z, W]$ e $I = (XZ, XW + YZ, YW) \subseteq A$. Provare che $\sqrt{I} = (XY, XZ, YZ, YW)$.

Radicale di un ideale

Definizione

Se I, J sono ideali di un anello A, allora

1. $I \subseteq J \implies \sqrt{I} \subseteq \sqrt{J}$.
2. $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J} = \sqrt{IJ}$.
3. $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I + J}$.
4. $\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I + J}$.

Esempio

In (3) l'inclusione può essere stretta: ad esempio si prendano $I = (X^2 + XY), J = (Y)$ in $K[X, Y]$.

Radicale di un ideale

Osservazione

Se I è un ideale di $S = K[X_1, \ldots, X_n]$, $f \in I \implies \text{sqfree}(f) \in \sqrt{I}$.
Quindi $I = (f_1, \ldots, f_m) \implies \sqrt{I} \supseteq (\text{sqfree}(f_1), \ldots, \text{sqfree}(f_m))$.

Teorema

Se I è un ideale monomiale di $S = K[X_1, \ldots, X_n]$, generato da monomi $u_1, \ldots, u_m$, allora $\sqrt{I} = (\text{sqfree}(u_1), \ldots, \text{sqfree}(u_m))$.

Dimostrazione:

Radicale di un ideale

Proposizione

Se $I = (f)$ un ideale principale di $S = K[X_1, \ldots, X_n]$. Allora $\sqrt{I} = (\text{sqfree}(f))$.

Dimostrazione:

Domanda

È possibile calcolare sqfree(f) algoritmicamente?

Vediiamolo nel caso in cui $S = K[X]$: se $f = \sum_{i=0}^{n} \lambda_i X^i \in K[X]$, denotiamo la sua derivata formale con

$$f' = \sum_{i=1}^{n} i\lambda_i X^{i-1} \in K[X]$$

Osservazione

Sia $f = \sum_{i=0}^{n} \lambda_i X^i \in K[X]$. Allora:

1. Se K ha caratteristica 0, $f' = 0 \iff \lambda_i = 0 \ \forall \ i \neq 0$.
2. Se K ha caratteristica p, $f' = 0 \iff \lambda_i = 0 \ \forall \ i \not\equiv 0 \ (p)$.

Ricordiamo che se A è un anello di caratteristica p, dove p è un numero primo, la funzione $F : A \to A$ definita da $F(a) = a^p$ è un omomorfismo di anelli, chiamato **endomorfismo di Frobenius**. Si ha che A è ridotto se e solo se F è iniettivo.

Definizione

Un anello di caratteristica p, dove p è un numero primo, si dice **perfetto** se l'endomorfismo di Frobenius è bigettivo.

Esercizio

Sia A un anello perfetto di caratteristica p. Se A è Noetheriano, tutti i nonzero divisori di A sono invertibli.

Diremo che ogni campo di caratteristica 0 è perfetto.

Esempi

1. Un campo finito è perfetto.
2. Un campo algebricamente chiuso è perfetto.
3. $\mathbb{Z}_p(X)$ è un campo non perfetto.

Radicale di un ideale

Osservazione

Se K è un campo perfetto di caratteristica $p > 0$ e $f \in K[X]$, allora $f' = 0$ se e solo se esiste $g \in K[X]$ tale che $f = g^p$.

Lemma

Sia K un campo e $0 \neq f \in K[X]$.

1. Se $\mathrm{MCD}(f, f') = 1$, allora (f) è un ideale radicale.
2. Se K è perfetto, $\mathrm{MCD}(f, f') = 1 \iff (f)$ è radicale.

Dimostrazione:

Teorema

Sia K un campo, $f \in K[X]$ e $f = \prod_{i=1}^{s} g_i^{a_i}$ la fattorizzazione in potenze di irriducibili distinti ($a_i > 0$).

1. Se K ha caratteristica 0, $\mathrm{MCD}(f, f') = \prod_{i=1}^{s} g_i^{a_i - 1}$.
2. Se K è perfetto di caratteristica $p > 0$,
$$\mathrm{MCD}(f, f') = \prod_{a_i \equiv 0 \ (p)} g_i^{a_i} \prod_{a_i \not\equiv 0 \ (p)} g_i^{a_i - 1}$$
.
3. Se K ha caratteristica 0 o $p > \deg(f)$ ed è perfetto,
$$\mathrm{sqfree}(f) = f / \mathrm{MCD}(f, f')$$

Radicale di un ideale

Dimostrazione: