Algebra 2

Riccardo Zanotto

18 luglio 2017

Indice

1 Anelli e ideali

1.1 Definizioni

Definizione 1.1 (Anello)**.** Un insieme A è detto *anello* se è dotato di due operazioni $(A, +, \cdot)$ tali che

- $(A, +)$ è un gruppo commutativo, con elemento neutro 0_A
- $\cdot$ è associativo
- Esiste un elemento $1 \in A$ tale che $1 \cdot a = a \cdot 1 = a \forall a \in A$
- $\forall x, y, z \in A$ vale $x \cdot (x + z) = xy + xz$ e $(y + z) \cdot x = yx + zx$

Inoltre se il prodotto è commutativo, A è detto *anello commutativo*

Osservazione. In generale $0 \neq 1$, altrimenti $A = 0$ è l'anello banale, poiché $a = a \cdot 1 = a \cdot 0 = 0$

Esempio.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con le operazioni usuali sono anelli commutativi
- Le matrici $n \times n$ sono un anello non commutativo

Definizione 1.2 (Unità)**.** Un elemento $a \in A$ si dice *unità* se $\exists b \in A$ tale che $ab = 1$.
Si indica con A^* l'insieme delle unità, o elementi invertibili.

Definizione 1.3 (Divisore di 0)**.** Un elemento $a \in A$ si dice *divisore di* 0 se $\exists b \in A$ tale che $ab = 0$.
Si indica con $\mathcal{D}(A)$ l'insieme dei divisori di 0.
Se $D(A) = 0$, allora l'anello è detto *dominio.*

Definizione 1.4 (Nilpotente)**.** Un elemento $a \in A$ si dice *nilpotente* se $\exists n \in \mathbb{N}$ tale che $a^n = 0$.
Si indica con $N(A)$ l'insieme degli elementi nilpotenti, che è detto nilradicale.
Se $N(A) = 0$, l'anello A è detto *ridotto.*

Esempio. Prendiamo $A = \mathbb{Z}/n\mathbb{Z}$ con $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Allora i nilpotenti sono tutti e soli gli elementi del tipo $p_1^{b_1} \cdots p_k^{b_k}$ cpn $b_i > 0$. I divisori di 0 sono gli m tali che $\gcd(m, n) > 1$.

Proposizione 1.1. *La somma di un nilpotente ed un invertibile è ancora invertibile.*

Dimostrazione.
Detto $a \in A^*$ e $b \in N(A)$, consideriamo $a^{-1}(a + b) = 1 - x$ e osserviamo che x è ancora nilpotente.
Detto n l'indice di nilpotenza di x, vale $(1 - x)(1 + x + \cdots + x^{n-1}) = 1 - x^n = 1$ cioè $1 - x$ è invertibile; ma allora anche $a(1 - x) = a + b$ è invertibile. $\square$

Consideriamo ora dei sottoinsiemi particolari di un anello, che saranno fondamentali nello studio delle proprietà degli anelli, in quanto corrispettivi della nozione di sottogruppo.

Definizione 1.5 (Ideale)**.** Un sottoinsieme $I \subset A$ di un anello è detto *ideale* se è un sottogruppo di $(A, +)$ ed è chiuso rispetto alla moltiplicazione per elementi di A, ovvero $x \in A, i \in I \Longrightarrow xi \in I$.

Esempio.

- In $\mathbb{Z}$ un ideale è formato ad esempio da tutti i multipli di 5.
- In $\mathbb{Z}[x]$ tutti i polinomi che non hanno termine noto formano un ideale.

Osserviamo che se $S \subset A$, è facile costruire un ideale I che contenga S; in particolare $(S) = \left\{ \sum_{i=1}^{k} a_i s_i \mid a_i \in A, s_i \in S \right\}$ si dice *ideale generato da* S.
Se S è finito, allora (S) è *finitamente generato*.

Definizione 1.6 (Principale)**.** Un ideale $I \subset A$ è detto *principale* se $\exists a \in A$ per cui $I = (a)$.

Definizione 1.7 (Primo)**.** Un ideale $I \subset A$ è detto *primo* se $ab \in I \Longrightarrow a \in I \vee b \in I$.
L'insieme di tutti gli ideali primi $Spec(A)$ è detto *spettro* di A.

Definizione 1.8 (Primario)**.** Un ideale $I \subset A$ è detto *primario* se $ab \in I \Longrightarrow a \in I \vee b^n \in I$ per qualche $n \in \mathbb{N}$.

Definizione 1.9 (Massimale)**.** Un ideale $I \subset A$ è detto *massimale* se $I \neq A$ e non esiste nessun ideale $J \neq A$ tale che $I \subset J$.

Esempi, esempi, esempi!!!

Esercizio 1.1. Se ogni ideale di A è primo, allora A è un campo.

1.2 Prime proprietà

Vediamo ora alcune proprietà degli ideali, che saranno gli oggetti più studiati. Iniziamo col vedere che questi oggetti esistono realmente.

Proposizione 1.2. *Sia A un anello non banale. Allora esiste sempre un ideale massimale $\mathfrak{m} \subset A$.*

Dimostrazione.
Sia $\Sigma = \{I \mid I \subsetneq A\}$ ordinato con l'inclusione. Osserviamo che $(0) \in \Sigma$.
Prendiamo una catena $\{I_j\}_{j \in J}$ e consideriamo $I = \bigcup_{j \in J} I_j$; dimostriamo che I è un ideale.
Infatti se $x, y \in I$ vuol dire che $x \in I_h$ e $y \in I_k$ per qualche indice; supponiamo senza perdita di generalità che $I_h \subset I_k$. Allora $x \in I_k$, perciò $x + y \in I_k \subset I$.
La verifica che $ai \in I \forall a \in A, i \in I$ è banale.
Inoltre I è proprio, poiché $1 \notin I_j \forall j$, per cui $1 \not\ni I$. Perciò I è un maggiorante della catena che avevamo considerato. Concludiamo usando il lemma di Zorn su Σ, perciò esiste un ideale massimale. $\square$

Osservazione. Dato un elemento $a \notin A^*$, si dimostra che esiste un massimale $\mathfrak{m}$ con $a \in \mathfrak{m}$, prendendo $\Sigma = \{I \mid I \subsetneq A, a \in I\}$.

Proposizione 1.3. *Dato un anello A, il nilradicale si può esprimere come* $N(A) = \bigcap_{P \text{ primi}} P$.

Dimostrazione.

$\subset$ Dato $a \in N(A)$, allora $a^n = 0 \in P$ per ogni ideale P. Ma se P è primo, $0 = a^n = a \cdot a^{n-1}$, per cui o $a \in P$, o $a^{n-1} \in P$. Procedendo così ottengo in ogni caso che $a \in P$.

$\supset$ Dato un $a \notin N(A)$, voglio trovare un P primo per cui $a \notin P$.
Sia $\Sigma = \{I \text{ ideale proprio} | a^n \notin I \forall n \in \mathbb{N}\}$ ordinato con l'inclusione.
Data una catena $\{I_j\}_{j \in J}$, considero $I = \bigcup_{j \in J} I_j$ e vale ovviamente $a^n \notin I$.
Inoltre $\Sigma \neq \emptyset$ poiché essendo a non nilpotente, $(0) \in \Sigma$.
Per il lemma di Zorn, esiste allora un elemento $P \in \Sigma$ massimale; osserviamo che P è un ideale, e voglio mostrare che è primo.
Siano $x, y \notin P$. Allora $(P, x) = P + (x) \supsetneq P$, per cui $(P, x) \notin \Sigma$, ovvero $a^n \in P + (x)$; analogamente $a^m \in P + (y)$.
Questo vuol dire che $a^n = kx + p_1, a^m = hy + p_2$, perciò $a^{m+n} = khxy + p_1 hy + p_2 kx + p_1 p_2 \in P + (xy)$, per cui $P + (xy) \notin \Sigma$.
Ma allora $xy \notin P$, altrimenti $P + (xy) = P \in \Sigma$.

□

Costruiamo ora alcune operazioni tra ideali che risulteranno utili in seguito...

- Data una famiglia arbitraria di ideali $\{I_j\}_{j \in J}$, allora $\bigcap I_j$ è un ideale.
- Dati due ideali I_1, I_2, si definisce la somma $I_1 + I_2 = (I_1, I_2) = \{i_1 + i_2 \mid i_1 \in I_1, i_2 \in I_2\}$, ovvero l'ideale generato da $I_1 \cup I_2$.
  In generale $\sum I_j = (\bigcup I_j)$.
- Dati due ideali I_1, I_2, si definisce il prodotto $I_1 \cdot I_2 =$
  $= \left\{\sum x_j^{(1)} x_j^{(2)} \mid x_j^{(1)} \in I_1, x_j^{(2)} \in I_2\right\}$
- Dati due ideali I, J, si definisce $I : J = \{a \in A \mid aJ \subset I\}$
- Dato un ideale I, si definisce radicale $\sqrt{I} = \{a \in A \mid \exists n \in \mathbb{N} a^n \in I\}$

Per quest'ultima operazione non è banale il fatto che si ottenga un altro ideale, ma si può dimostrare nella seguente

Proposizione 1.4. *Dato un ideale I, il suo radicale $\sqrt{I}$ è un ideale.*

Dimostrazione.
Vediamo intanto che se $a \in \sqrt{I}$, allora $a^n \in I$ per un qualche n, per cui $(ka)^n = k^n a^n \in I \forall k \in A$, cioè $ka \in \sqrt{I}$.
Siano ora $a, b \in I$, cioè $a^n \in I$ e $b^m \in I$ per certi interi. Dimostriamo che

$(a+b)^{n+m} \in I$.

$$\begin{aligned}(a+b)^{m+n} &= \sum_{k=0}^{m+n} \binom{n+m}{k} a^k b^{m+n-k} \\ &= \sum_{k=0}^{n} \binom{n+m}{k} a^k b^{m+n-k} + \sum_{k=n+1}^{m+n} \binom{n+m}{k} a^k b^{m+n-k}\end{aligned}$$

Osserviamo che nella prima sommatoria $m + n - k \geq m$, per cui possiamo raccogliere b^m; analogamente nella seconda $k \geq n$, per cui raccogliamo a^n. Ma allora abbiamo una combinazione lineare di a^n e b^m che stanno entrambi in I, per cui tutta la somma sta in I. □

Definiamo ora un ideale particolare:

Definizione 1.10 (Radicale di Jacobson)**.** $J(A) = \bigcap_{\mathfrak{m} \subset A} \mathfrak{m}$

Proposizione 1.5. $x \in J(A) \iff \forall y \in A \;\; 1 - xy \in A^*$

Dimostrazione.

$\Longleftarrow$ Se $x \notin J(A)$, allora $\exists \mathfrak{m}$ massimale tale che $x \notin \mathfrak{m}$, perciò l'ideale $(\mathfrak{m}, x) \supset \mathfrak{m}$ conincide con tutto l'anello A.
Allora $A \ni 1 = m + xy$ con $m \in \mathfrak{m}$ e $y \in A$, ovvero $1 - xy \in \mathfrak{m}$ da cui $1 - xy \in A^*$, perché altrimenti $\mathfrak{m} = A$.

$\Longrightarrow$ Se $\alpha = 1 - xy \notin A^*$, allora esiste un $\mathfrak{m}$ ideale massimale tale che $\alpha \in \mathfrak{m}$. Ma allora $x \notin \mathfrak{m}, y \notin \mathfrak{m}$, altrimenti si avrebbe $1 \in \mathfrak{m}$ e perciò $\mathfrak{m} = A$. Dunque $x \notin J(A) \subset \mathfrak{m}$.

□

Definizione 1.11 (Anello locale)**.** Dato un anello A, se esiste un unico ideale $\mathfrak{m}$ massimale, allora A è detto *locale* e di solito si indica con $(A, \mathfrak{m})$

Esempio. L'anello $\mathbb{Z}/p^n\mathbb{Z}$ è locale: gli unici ideali propri sono (p^i) con $i = 1, .., n-1$ e in particolare l'unico ideale massimale è (p)

Definizione 1.12. Dato un anello A e due ideali $I, J \subset A$, si dice che I e J sono *comassimali* o *coprimi* se $I + J = A$

Proposizione 1.6. *Siano $I, J \subset A$ due ideali comassimali, allora $I \cap J = IJ$*

Dimostrazione.
Osserviamo intanto che l'inclusione $I \cap J \supset IJ$ è vera sempre.
Dimostriamo allora che se $\alpha \in I \cap J$, allora $\alpha \in IJ$. Infatti essendo I, J comassimali esistono $i \in I, j \in J$ tali che $1 = i + j$.
Ma allora $\alpha = \alpha \cdot 1 = \alpha \cdot i + \alpha \cdot j$ ed entrambi i termini appartengono all'ideale IJ. □

Osservazione. Il viceversa non è in generale vero: se consideriamo come anello $K[x, y]$ e prendiamo gli ideali $(x), (y)$, vale chiaramente $(x) \cap (y) = (xy)$, ma ad esempio nell'ideale $(x) + (y)$ non troviamo le costanti.

Esempio. Su $\mathbb{Z}$, osserviamo che $(a) + (b) = (\gcd(a, b))$ mentre $(a) \cap (b) = (\operatorname{lcm}(a, b))$. Vediamo poi che se $\gcd(a, b) = 1$ allora $\operatorname{lcm}(a, b) = a \cdot b$, che è esattamente la proposizione.

Lemma 1.7 (di scansamento)**.**

a) Siano A un anello, P un ideale primo, $I_1, \ldots, I_n$ ideali. Vale

$$\bigcap I_i \subset P \Longrightarrow \exists j \mid I_j \subset P$$

Inoltre se $\bigcap I_i = P$ vale anche $I_j = P$.

b) Siano A un anello, $I \subset A$ un ideale, $P_1, \ldots, P_n$ ideali primi. Vale

$$I \subset \bigcup P_i \Longrightarrow \exists j \mid I \subset P_j$$

Dimostrazione.

a) Dimostriamo che $\forall i \;\; I_i \not\subset P \Longrightarrow \bigcap I_i \not\subset P$.
L'ipotesi ci fornisce allora per ogni i un elemento $x_i \in I_i$ e $x_i \notin P$.
Ma allora $x_1 \cdots x_n \in \prod I_i \subset \bigcap I_i$, ma $x_1 \cdots x_n \notin P$ poiché prodotto di elementi che non stanno in un ideale primo.
Infine se $P = \bigcap I_i$, allora $I_i \supset \bigcap I_i = P$, e in particolare $P \subset I_j$, dove I_j è l'ideale tale che $I_j \subset P$ che abbiamo appena dimostrato esistere, da cui $P = I_j$.

b) Dimostriamo per induzione su n che $\forall i \;\; I \not\subset P_i \Longrightarrow I \not\subset \bigcup P_i$.
Il caso $n = 1$ è banale, dimostriamo il passo induttivo $n - 1 \to n$.
Per ipotesi induttiva vale che $I \not\subset \bigcup_{i \neq k} P_i \quad \forall k$, ovvero $\exists x_k \in I$ per cui $x_k \notin \bigcup_{i \neq k} P_i$.
Osserviamo che se per un qualche k, $x_k \notin P_k$, allora la tesi segue poiché $\bigcup P_i = P_k \cup \bigcup_{i \neq k} P_i$.
Supponendo per assurdo $x_i \in P_i \quad \forall i$, consideriamo $\alpha = \displaystyle\sum_{i=1}^{n} \prod_{j \neq i} x_j = x_2 \cdots x_n + x_1 x_3 \cdots x_n + \cdots + x_1 \cdots x_{n-1}$.
Chiaramente $\alpha \in I$; inoltre $P_i \ni \alpha - x_i(\ldots) = \prod_{j \neq i} x_j \notin P_i$ perché prodotto di fattori che non stanno in P_i. Assurdo.

$\square$

1.3 Quozienti e omomorfismi

Cominciamo ad entrare nel vivo della teoria degli anelli, e vediamo quali sono le relazioni che sussistono tra anelli diversi, e qual è la struttura e l'utilità degli anelli quozienti.

Definizione 1.13 (Omomorfismo)**.** Dati due anelli A, B, una funzione $f : A \to B$ si dice *omomorfismo di anelli* se valgono le seguenti proprietà:

- $f(a + b) = f(a) + f(b)$
- $f(ab) = f(a)f(b)$

- $f(1_A) = 1_B$

Osservazione. Esiste un unico omomorfismo di anelli $f : \mathbb{Z} \to \mathbb{Z}$, ed è l'identità. Infatti $\mathbb{Z}$ è un gruppo ciclico e fissando l'immagine di 1 si fissa l'omomoerfismo.

Definizione 1.14. Si chiama *nucleo* dell'omomorfismo l'ideale $ker(f) = \{a \in A \mid f(a) = 0\}$.
Si dice *immagine* dell'omomorfismo il sottoanello $Im(f) = \{b \in B \mid \exists a \in A\ f(a) = b\}$

Come per i gruppi, possiamo definire una relazione d'equivalenza su A:
Fissato un ideale I, diciamo che $a \equiv b \pmod I$ se $a - b \in I$.
Le classi di equivalenza sono i laterali, che sono della forma $a + I$; l'insieme dei laterali è detto quoziente e si indica con ${}^{A}\!/_{I}$.

Proposizione 1.8. *Il quoziente* ${}^{A}\!/_{I}$ *ha una struttura di anello con le operazioni indotte da* A*:*

- $(a + I) + (b + I) = (a + b) + I$
- $(a + I)(b + I) = ab + I$

Possiamo allora definire un'importante mappa, la proiezione al quoziente:

$$\begin{aligned} \Pi : A &\to {}^{A}\!/_{I} \\ a &\mapsto a + I \end{aligned}$$

In particolare osserviamo che se $J \subset A$ è un ideale di A, allora $\Pi(J) = {}^{J}\!/_{I}$ è un ideale di ${}^{A}\!/_{I}$. Perciò vale la seguente

Proposizione 1.9. *Esiste una corrispondenza biunivoca tra gli ideali di* ${}^{A}\!/_{I}$ *e gli ideali* $A \supset J \supset I$*. Tale bigezione è data da* $\Pi^{-1}(L) = \{b \in A \mid \Pi(b) \in L\}$

Vi sono inoltre i fondamentali teoremi di omomorfismo, analoghi a quelli sui gruppi

Teorema 1.10.

1) Sia $f : A \to B$ *un omomorfismo. Allora* $A/ker(f) \cong Im(f)$

2) Data una catena di ideali $I \subset J \subset A$ *vale*

$$ {}^{{}^{A}\!/_{I}}\!\Big/_{{}^{J}\!/_{I}} \cong {}^{A}\!/_{J} $$

Dimostrazione.

1) Chiamiamo $I = ker(f)$; sia $\varphi : {}^{A}\!/_{I} \to Im(f)$ definita da $\varphi(a + I) = f(a)$.
Si osserva banalmente che φ è un omomorfismo.
Supponiamo che $\varphi(a + I) = \varphi(b + I)$, ma allora $f(a) = f(b)$ ovvero $f(a - b) = 0$ e $a - b \in I$; quindi φ è iniettiva.
Inoltre è chiaramente surgettiva, perciò è un isomorfismo.

2) Definiamo $f : {}^{A}\!/_{I} \to A/J$ come $f([b]_I) = [b]_J$, ed è una buona definizione in quanto se $[b_1]_I = [b_2]_I$ allora $b_1 - b_2 \in I \subset J$. Vediamo subito che è surgettiva.
Per il punto 1), basta dimostrare che $ker(f) = {}^{J}\!/_{I}$; ma questo si vede subito in quanto $f([b]_I) = 0 \iff b \in J$, perciò $ker(f) = \{j + I \mid j \in J\} = {}^{J}\!/_{I}$.

□

Osserviamo ora che ci sono delle ben precise relazioni tra le proprietà dell'ideale I e quelle dell'anello quoziente ${}^{A}\!/_{I}$. In particolare vale

Proposizione 1.11.

- *l'ideale I è massimale* $\iff$ ${}^{A}\!/_{I}$ *è un campo*
- *l'ideale I è primo* $\iff$ ${}^{A}\!/_{I}$ *è un dominio*
- *l'ideale I coincide con* $\sqrt{I}$ $\iff$ ${}^{A}\!/_{I}$ *è ridotto*
- *l'ideale I è primario* $\iff$ $N({}^{A}\!/_{I}) = D({}^{A}\!/_{I})$

Teorema 1.12 (cinese del resto)**.** *Sia A un anello e $I_1, \dots, I_n$ ideali a coppie coprimi. Allora vale* ${}^{A}\!/_{I_1 \times \cdots \times I_n} \cong A/I_1 \times \cdots \times A/I_n$

Dimostrazione.
Consideriamo l'omomorfismo di proiezione $\varphi : A \to A/I_1 \times \cdots \times A/I_n$ che manda a in $([a]_{I_1}, \dots, [a]_{I_n})$. Dimostriamo che è surgettiva.
Prendiamo $(a_1, \dots, a_n) \in A/I_1 \times \cdots \times A/I_n$; poiché gli ideali sono a coppie comassimali, $\forall i, j$ esistono $\alpha_i^{(j)} \in I_i, \alpha_j^{(i)} \in I_j$ tali che $\alpha_i^{(j)} + \alpha_j^{(i)} = 1$.
Costruiamo $L_i = \prod_{j \neq i} a_j^{(i)}$ e poi $a = \sum a_i L_i$.
Allora vediamo che $\varphi(a) = (a_1, \dots, a_n)$, poiché $L_i \equiv 0 \pmod{I_j}$ se $j \neq i$, mentre $L_i \equiv \prod(1 - \alpha_i^{(j)}) \equiv 1 \pmod{I_i}$.
Osserviamo che $\ker\varphi = \bigcap I_i$. Dimostriamo che $\bigcap I_i = \prod I_i$; per induzione, basta che $(I_n, \prod_{i \leq n-1} I_i) = (1)$.
Ma allora prendiamo $L_n \in \prod_{i \leq n-1} I_i$ e vediamo che vale $L_n \equiv 1 \pmod{I_n}$. □

Osservazione. Se come anello consideriamo $\mathbb{R}[x]$ e come ideali quelli generati da polinomi di primo grado $I_i = (x - a_i)$, vediamo che gli L_i sono proprio i polinomi interpolanti di Lagrange.

1.4 Ideali contratti ed estesi

Siano A, B due anelli e $f : A \to B$ un omomorfismo. Prendiamo poi $I \subset A$ e $J \subset B$ ideali.

Definizione 1.15.

- L'ideale contratto di J è $J^c = f^{-1}(J) = \{a \in A \mid f(a) \in J\}$
- L'ideale esteso di I è $I^e = (f(I)) = \{\sum b_i f(a_i) \mid a_i \in I\}$ cioè l'ideale generato dall'immagine di I

Vale la seguente proprietà

Proposizione 1.13.

1. *J^c è un ideale $\forall J \subset B$ ideale.*
2. *se f è surgettiva, allora $f(I)$ è un ideale.*

Dimostrazione.

1. Siano $a, b \in J^c$, allora $f(a), f(b) \in J$; ma allora $J \ni f(a)+f(b) = f(a+b)$ cioè $a + b \in J^c$. Inoltre se $c \in A$, $J \ni f(c)f(a) = f(ca)$ cioè $ca \in J^c$
2. Vale banalmente $f(I) \subset (f(I))$; prendiamo ora $b \in I^e$ ovvero $b = \sum b_i f(a_i)$. Poiché f è surgettiva, esistono $c_i \in A$ tali che $b_i = f(c_i)$ $\forall i$. Allora $b = f\left(\sum c_i a_i\right) \in f(I)$.

□

Esercizio 1.2. Valgono le uguaglianze $I^{ece} = I$ e $J^{cec} = J$

Proposizione 1.14. *La contrazione di un ideale primo è primo.*

Dimostrazione.
Sia $J \subset B$ un ideale primo; supponiamo $ab \in J^c$, ovvero $f(ab) \in J$. Ciò vuol dire $f(a)f(b) \in J$, ed essendo primo abbiamo $f(a) \in J$ oppure $f(b) \in J$, cioè $a \in J^c$ o $b \in J^c$ □

1.5 Esercizi svolti

Problema 1.1. Se A è un anello finito, allora $A = D(A) \cup A^*$

Problema 1.2. Dato un anello A e un ideale $I \subset A$ tale che $\forall x \notin I \;\; x \in A^*$, dimostrare che A è locale e I è il suo massimale.

Problema 1.3. Dato un anello A in cui ogni ideale primo è principale, allora ogni ideale è principale (A è un PIR).

Problema 1.4. $D(A)$ è unione di ideali primi; inoltre $D(A) = \bigcup \sqrt{\operatorname{Ann}(a)}$

Problema 1.5. Se $\sqrt{I}$ è massimale, allora I è primario.

2 Anelli di polinomi

2.1 Polinomi in una variabile

Sia A un anello e consideriamo l'anello di polinomi $A[x]$.
Prendiamo il morfismo di inclusione $i : A \hookrightarrow A[x]$, siano $I \subset A, J \subset A[x]$ e studiamo I^e, J^c. Si vede subito che vale

Proposizione 2.1.

- $J^c = J \cup A$
- $I^e = I[x]$

Vale inoltre la importante

Proposizione 2.2. *Dato $I \subset A$ ideale,* ${}^{A[x]}\!\big/_{I[x]} \cong \left({}^{A}\!\big/_{I}\right)[x]$

Dimostrazione.
Consideriamo $\varphi : A[x] \to \left({}^{A}\!\big/_{I}\right)[x]$ tale che $\varphi\left(\sum a_i x^i\right) = \sum \pi(a_i)x^i$ dove π è la proiezione al quoziente.
È chiaramente surgettiva; inoltre $ker\varphi$ è esattamente $I[x]$, perciò il risultato segue dal primo teorema di omomorfismo. $\square$

Corollario. *Se $I \subset A$ è primo, allora $I^e = I[x]$ è primo in $A[x]$*

Infatti, se ${}^{A}\!\big/_{I}$ è dominio, anche $\left({}^{A}\!\big/_{I}\right)[x]$ è dominio; ma questo è esattamente ${}^{A[x]}\!\big/_{I[x]}$, perciò $I[x]$ è primo.

Detto $R = A[x]$ con A anello, cerchiamo di identificare $N(R), D(R)$ e R^*.

Proposizione 2.3. *Sia $f = \sum a_i x^i \in R$. Allora*

1. $f \in R^* \iff a_0 \in A^*$ *e* $a_1, \dots, a_n \in N(A)$
2. $f \in N(R) \iff a_i \in N(A)\ \forall i$
3. $f \in D(R) \iff \exists a \in A$ *tale che* $af = 0$

Dimostrazione.

2, $\Leftarrow$ Detti m_i gli indici di nilpotenza di a_i, si vede facilmente che $f^{m_1+\dots+m_n+1} = 0$

1, $\Leftarrow$ Usando la freccia appena dimostrata di 2, sappiamo che $g(x) = a_1x + \dots + a_nx^n \in N(R)$; ma allora $f = a_0 + g$ è somma di un invertibile e un nilpotente, quindi è ancora invertibile.

1, $\Rightarrow$ Sia $g = \sum b_i x^i$ di grado m tale che $fg = 1$; guardando il termine noto sappiamo $a_0b_0 = 1$ perciò a_0 e b_0 sono invertibili.
Considerando poi i termini di grado maggiore abbiamo $0 = a_nb_m$ e $0 = a_nb_{m-1} + a_{n-1}b_m$, da cui moltiplicando la seconda per a_n otteniamo $a_n^2b_{m-1} = 0$. Continuando così ricaviamo $a_n^{r+1}b_{m-r} = 0$; se prendiamo $r = m$ abbiamo $a_n^{m+1}b_0 = 0$ ed essendo b_0 invertibile, abbiamo a_n nilpotente.
Riapplichiamo ora questo ragionamento a $f - a_nx^n$ che è ancora invertibile.

2, $\Rightarrow$ Se f è nilpotente, anche $xf \in N(R)$; ma allora $1 + xf \in R^*$ e per la 1 si deve avere $a_0, \dots, a_n \in N(A)$.

$\square$

2.2 Ideali monomiali

Prendiamo ora un campo k e consideriamo l'anello $A = k[x_1, \ldots, x_n]$.
Diamo una notazione per rendere le scritture più compatte: chiamiamo $X = (x_1, \ldots, x_n)$ e se $\alpha = (a_1, \ldots, a_n)$ allora X^α indica il monomio $x_1^{a_1} \cdots x_n^{a_n}$.
In generale un $f \in k[X]$ si scrive come $f = \sum c_\alpha X^\alpha$ con $c_\alpha \in k$, e la somma è finita.

Definizione 2.1. Un ideale $I \subset A$ è detto *monomiale* se $\exists E \in \mathbb{N}^n$ tale che $I = (X^\alpha, \alpha \in E)$

Proposizione 2.4. *Dato un ideale I monomiale, $f = \sum c_\beta X^\beta \in I$ se e solo se $X^\beta \in I \; \forall \beta$*

Dimostrazione.
Una freccia è ovvia. Se invece $f \in I$, allora $f = \sum_{\alpha \in E} P_\alpha(X) X^\alpha$ con $P_\alpha(X) = \sum d_{\gamma,\alpha} X^\gamma$ con i $d \in k$. Quindi $\sum c_\beta X^\beta = f = \sum d_{\gamma,\alpha} X^{\alpha+\gamma}$, perciò ogni X^β è della forma $X^{\alpha+\gamma}$ ovvero $X^\beta \in I$ □

Osserviamo che agli ideali monomiali corrispondono in maniera ovvia certi sottoinsiemi di $\mathbb{N}^n$ grazie alla mappa $X^\alpha \mapsto (a_1, \ldots, a_n)$.

Definizione 2.2. Un sottoinsieme non vuoto $E \subset \mathbb{N}^n$ si dice $\mathcal{E}$-sottoinsieme se $\forall \alpha \in E, \forall \beta \in \mathbb{N}^n$ anche $\alpha + \beta$ sta in E.
$F \subset E$ si dice *frontiera* di E se $\forall \alpha \in E \;\; \exists \gamma \in F, \beta \in \mathbb{N}^n$ tali che $\alpha = \gamma + \beta$

Lemma 2.5 (Dickson)**.** *Ogni $\mathcal{E}$-sottoinsieme E ha una frontiera finita.*

Dimostrazione.
Facciamo una induzione su n.
Se $n = 1$, allora $E \subset \mathbb{N}$; ma poiché $\mathbb{N}$ è ben ordinato, la frontiera è semplicemente $\min(E)$.
Passo induttivo $n \Rightarrow n + 1$: $E \subset \mathbb{N}^{n+1}$.
Consideriamo la proiezione $\Pi : \mathbb{N}^{n+1} \to \mathbb{N}^n$ che ignora l'ultima coordinata. Allora $\Pi(E)$ è ancora un $\mathcal{E}$-sottoinsieme: infatti $\Pi(\alpha) + \gamma = \Pi(\alpha + (\gamma, 0))$.
Per ipotesi induttiva $\Pi(E)$ ha una frontiera finita $\hat{F} = \{\hat{\gamma}_1, \ldots, \hat{\gamma}_k\}$. Siano $\gamma_i \in E$ tali che $\Pi(\gamma_i) = \hat{\gamma}_i$, e $\tilde{F} = \{\gamma_i\}$.
Prendiamo $\bar{a}$ il massimo delle componenti $n+1$-esime dei γ_i, e per ogni $a < \bar{a}$ poniamo $E_a = E \cap \left(\mathbb{N}^n \times \{a\}\right)$.
Si vede che $\Pi(E_a)$ è ancora un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$ e quindi ha frontiera finita $\hat{F}_a = \{\gamma_{a,1}, \ldots, \gamma_{a,k_a}\}$; rimontiamo questo insieme in E: $F_a = \{(\gamma_{a,i}, a) \mid i = 1, \ldots, k_a\}$.
Allora la frontiera di E è $F = \tilde{F} \cup \left(\bigcup_{a<\bar{a}} F_a\right)$.
Sia infatti $\alpha = (a_1, \ldots, a_n, a_{n+1}) \in E$; se $a_{n+1} \geq \bar{a}$, allora esiste un $\beta \in \tilde{F}$ tale che $\alpha - \beta \in \mathbb{N}^{n+1}$; se $a_{n+1} < \bar{a}$, allora $\alpha \in E_{a_{n+1}}$ per cui $\exists \gamma \in F_{a_{n+1}}$ per cui $\alpha - \gamma \in \mathbb{N}^{n+1}$. □

Corollario. *Ogni ideale monomiale è finitamente generato*

Proposizione 2.6. *Dato un $\mathcal{E}$-sottoinsieme $E \subset \mathbb{N}^n$, esiste un'unica frontiera di cardinalità minima.*

Dimostrazione.
Siano $F = \{a_1, \dots, a_k\}$ e $G = \{b_1, \dots, b_k\}$ due frontiere minimali di E; allora $E = \bigcup(a_i + \mathbb{N}^n) = \bigcup(b_i + \mathbb{N}^n)$.
In particolare per ogni i esiste un $j = \eta(i)$ tale che $a_i \in b_j + \mathbb{N}^n$. Se η non fosse surgettiva, allora G non sarebbe minimale. Quindi $\eta : \{1, \dots, k\} \to \{1, \dots, k\}$ è una permutazione.
Analogamente esiste una permutazione ϵ tale che $b_i \in a_{\epsilon(i)} + \mathbb{N}^n$. Ma allora $a_i + \mathbb{N}^n \subset b_{\eta(i)} + \mathbb{N}^n \subset a_{\epsilon(\eta(i))} + \mathbb{N}^n$; poiché F è frontiera minimale, deve essere $\epsilon \circ \eta = \mathrm{id}$ e allora $a_i = b_{\eta(i)}$, cioè F e G sono lo stesso insieme. $\square$

Vediamo ora alcune operazioni tra ideali monomiali. Siano $I = (m_1, \dots, m_k)$ e $J = (n_1, \dots, n_h)$; allora

- $I + J = (m_1, \dots, m_k, n_1, \dots, n_h)$
- $I \cap J = \big(\mathrm{lcm}(m_i, n_j)\big)$
- $I : m = \left(\frac{m_i}{\gcd(m_i, m)}\right)$

Ricordiamo inoltre il seguente ed utile lemma:

Lemma 2.7. *Se I è un ideale monomiale, m e n due monomi coprimi, allora* $(I, mn) = (I, m) \cap (I, n)$

Dimostrazione.
L'inclusione $(I, mn) \subset (I, m) \cap (I, n)$ è banale. Se ora $v \in (I, m) \cap (I, n)$ un monomio, o $v \in I$ (e allora il lemma è vero), oppure $v \notin I$ e perciò $m \mid v$ e $n \mid v$; essendo $(m, n) = 1$, vale $mn \mid v$. $\square$

Infine enunciamo alcune caratterizzazioni di ideali monomiali:

Proposizione 2.8. *Sia I un ideale monomiale. Allora*

- *I è primo $\iff$ $I = (x_{i_1}, \dots, x_{i_k})$, ovvero è generato da variabili*
- *I è radicale $\iff$ I è generato da prodotti di variabili squarefree*
- *I è primario $\iff$ $I = (x_{i_1}^{k_1}, \dots, x_{i_s}^{k_s}, m_1, \dots, m_t)$ con $m_i \in k[x_{i_1}, \dots, x_{i_s}]$*
- *I è irriducibile $\iff$ $I = (x_{i_1}^{k_1}, \dots, x_{i_s}^{k_s})$*

2.3 Riduzione di polinomi

Cerchiamo ora di trovare un modo di fare la divisione di polinomi anche in più variabili, generalizzando il procedimento in una variabile: se dobbiamo dividere $f(x)$ per $g(x)$, dividiamo intanto il termine di grado massimo di $f(x)$ per il termine di grado massimo di $g(x)$.
Il primo problema è dunque decidere qual è il termine di grado massimo di un polinomio in più variabili, e questo si può fare in diversi modi; partiamo dunque dalla seguente definizione.

Definizione 2.3. Una relazione d'ordine $<$ su $\mathbb{N}^n$ è detto *ordinamento monomiale* se:

- $<$ è totale
- $<$ è un buon ordinamento, ovvero se ogni sottoinsieme non vuoto ha minimo
- $<$ rispetta la somma, ovvero se $\alpha < \beta$ anche $\alpha+\gamma < \beta+\gamma$ per ogni $\gamma \in \mathbb{N}^n$

Vi sono diversi ordinamenti monomiali possibili, i più usati sono i seguenti:

- $\texttt{lex}$: $\alpha <_L \beta \iff$ la prima coordinata non nulla di sinistra di $\beta - \alpha$ è positiva.
- $\texttt{deg} - \texttt{lex}$: $\alpha <_{DL} \beta \iff |\alpha| < |\beta|$, oppure $|\alpha| = |\beta|$ e $\alpha <_L \beta$.
- $\texttt{deg} - \texttt{rev} - \texttt{lex}$: $\alpha <_{DRL} \beta \iff |\alpha| < |\beta|$ oppure $|\alpha| = |\beta|$ e la prima cooordinata non nulla da destra di $\beta - \alpha$ è negativa.

Fissato ora un ordinamento monomiale $<$, possiamo parlare di multigrado e termine di testa: dato un polinomio $f = \sum c_\alpha X^\alpha$, posso considerare

- $\mathrm{Deg}_<(f) = \max\{\alpha \in \mathbb{N}^n \mid c_\alpha \neq 0\}$ il multigrado
- $\mathrm{lt}(f) = c_\delta X^\delta$ dove $\delta = \mathrm{Deg}_<(f)$ è il termine di testa, o "leading term"

Siamo ora pronti a fare la divisione:

Definizione 2.4. Dati $f, g, h \in A = k[x_1, \dots, x_n]$ diciamo che $f = \sum t_\alpha$ *riduce* ad h modulo g, e scriviamo $f \xrightarrow{g} h$ se $\exists \alpha$ per cui $\mathrm{lt}(g) \mid t_\alpha$ e $h = f - \dfrac{t_\alpha}{\mathrm{lt}(g)} \cdot g$

Esempio. Conti...

Quello che ci interessa davvero però è ridurre modulo molti polinomi, perciò introduciamo la seguente notazione

Definizione 2.5. Dati $f, f_1, \dots, f_s \in A$ diciamo che f riduce ad h modulo $F = \{f_1, \dots, f_s\}$ e scriviamo $f \xrightarrow{F}_* h$ se esistono $i_1, \dots, i_k$ e polinomi $h_1, \dots, h_{k-1}$ tali che $f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} \dots \xrightarrow{f_{i_k}} h$
Diciamo inoltre che h è *ridotto* rispetto ad F se non posso fare altre riduzioni, ovvero o $h = 0$ oppure per ogni termine t di h vale che $\mathrm{lt}(f_i) \nmid t$

Ispirandoci al processo di riduzione, possiamo definire un algoritmo di divisione nella maniera seguente

Data: $f, f_1, \dots, f_s$; $<$
Result: $f = \sum u_i f_i + r$, con r ridotto modulo $\{f_1, \dots, f_s\}$ e
$\mathrm{Deg}_<(f) \geq \max(\mathrm{Deg}_<(r), \mathrm{Deg}_<(u_i f_i))\ \forall i$
$u_i = 0, r = 0, h = f$;
while $h \neq 0$ **do**
  if $\exists i$ *tale che* $\mathrm{lt}(f_i) \mid \mathrm{lt}(h)$ **then**
    scegli j il minimo indice per cui vale la divisibilità;
    $u_j = u_j + \dfrac{\mathrm{lt}(h)}{\mathrm{lt}(f_j)}$;
    $h = h - \dfrac{\mathrm{lt}(h)}{\mathrm{lt}(f_j)} \cdot f_j$;
  else
    $r = r + \mathrm{lt}(h)$;
    $h = h - \mathrm{lt}(h)$;
  end
end

Algorithm 1: Algoritmo di divisione

È facile vedere che quest'algoritmo termina, poiché $\mathrm{Deg}(h)$ diminuisce ad ogni passaggio.
Inoltre osserviamo che se $f \xrightarrow{F}_* 0$, allora $f \in (f_1, \dots, f_s)$.
Esempi...

2.4 Basi di Gröbner

Introduciamo ora un oggetto molto importante nello studio degli ideali di polinomi.

Definizione 2.6. Dato un ideale $I \subset k[x] = A$ e un ordinamento monomiale $<$, definiamo $\mathrm{Lt}(I) = (\mathrm{lt}(f) \mid f \in I)$ l'ideale dei leading term di I.
L'insieme $G = \{g_1, \dots, g_k\}$ è detta *base di Gröbner* dell'ideale I se vale $\mathrm{Lt}(G) = (\mathrm{lt}(g_1), \dots, \mathrm{lt}(g_k)) = \mathrm{Lt}(I)$

Osservazione. Una base di Gröbner esiste sempre; infatti $\mathrm{Lt}(I)$ è un ideale monomiale, perciò è generato da $\hat{g}_1, \dots, \hat{g}_k$.
Allora basta rimontare questi monomi su I, ovvero prendere dei polinomi per cui $\mathrm{lt}(g_i) = \hat{g}_i$, e poi $G = \{g_1, \dots, g_k\}$ è una base di Gröbner.

Vediamo ora una caratterizzazione importante delle basi di Gröbner, che avrà molti corollari utili.

Teorema 2.9. *Sia $I \subset k[x_1, \dots, x_n]$ un ideale e $G = \{g_1, \dots, g_k\} \subset I$; allora sono fatti equivalenti:*

1. *G è una base di Gröbner di I*
2. *$f \in I \iff f \xrightarrow{G}_* 0$*
3. *$f \in I \iff f = \sum h_i g_i$ con $\mathrm{Deg}\, f \geq \mathrm{Deg}(h_i g_i)$*

Dimostrazione.

$1 \Rightarrow 2$ Facciamo l'algoritmo di divisione $f \xrightarrow{G}_* r$.
Se $r = 0$, allora $f = \sum h_i g_i$, ovvero $f \in I$.
Sia poi $f \in I$, ma allora anche $r = f - \sum h_i g_i \in I$. Se $r \neq 0$, si avrebbe $\text{lt}(r) \in \text{Lt}(I) = \text{Lt}(G)$; tuttavia r è ridotto, ovvero nessuno dei suoi monomi sta in $\text{Lt}(G)$, tantomeno il suo termine di testa; perciò abbiamo $r = 0$.

$3 \Rightarrow 1$ Dimostriamo che $\text{Lt}(I) \subset (\text{lt}(g_1), \ldots, \text{lt}(g_k))$, poiché l'altra inclusione vale sempre.
Sia $f \in I$, allora $f = \sum h_i g_i$ con $\text{Deg}\, f \geq \text{Deg}(h_i g_i)$; dato che vale anche $\text{Deg}(f) \leq \max(\text{Deg}(h_i g_i))$, esisterà un j per cui $\text{Deg}(f) = \text{Deg}(h_j g_j)$. Ma allora $\text{lt}(g_j) \mid \text{lt}(h_j g_j) \mid \text{lt}(f)$, perciò $\text{lt}(f) \in \text{Lt}(G)$.

$\square$

Ecco alcuni corollari immediati, ma importantissimi:

Corollario. *Per ogni polinomio $f \in A$, se G è base di qualche ideale, nella riduzione $f \xrightarrow{G}_* r$ il resto è unico.*

Teorema 2.10. *Ogni ideale $I \subset k[x_1, \ldots, x_n]$ è finitamente generato, o equivalentemente ogni successione di ideali $I_1 \subset I_2 \subset \ldots$ si stabilizza.*

Unicità della base minimale??

Mostriamo ora un metodo per costruire una base di Gröbner partendo da dei generatori di un ideale.
Per fare questo dobbiamo introdurre una nuova operazione tra polinomi, che permette di trovare nuovi termini di testa.

Definizione 2.7. Siano $f, g \in A$, con $\text{Deg}\, f = (a_1, \ldots, a_n)$ e $\text{Deg}\, g = (b_1, \ldots, b_n)$; considero $\gamma = (\max(a_1, b_1), \ldots, \max(a_n, b_n))$ e definisco

$$S(f, g) = \frac{X^\gamma}{\text{lt}(f)} \cdot f - \frac{X^\gamma}{\text{lt}(g)} \cdot g$$

come *S-polinomio* di f e g.

Esempio. Se $f = xy^2 + x, g = x^2y + y$ e considero il $\texttt{deg} - \texttt{lex}$, allora $S(f, g) = xf - yg = x^2 - y^2$

Proposizione 2.11. *Dato un insieme $G = \{g_1, \ldots, g_k\}$, questo è una base di Gröbner se e solo se $S(g_i, g_j) \xrightarrow{G}_* 0$ per goni coppia i, j*

Allora possiamo scrivere un algoritmo che, partendo da un insieme di generatori, calcoli una base di Gröbner semplicemente prendendo tutti i possibili S-polinomi.

input : $F = \{f_1, \dots, f_s\}$
output: $G = \{g_1, \dots, g_t\}$ base di Gröbner di I
$G = F, t = s$
$B = \{(i, j) \mid 1 \leq i < j \leq s\}$
while $B \neq \emptyset$ **do**
  scegli un $(i, j) \in B$
  $S(g_i, g_j) \xrightarrow{G}_* h$ ridotto
  if $h \neq 0$ **then**
    $t = t + 1, g_t = h$
    $G = G \cup \{g_t\}$
    $B = B \cup \{(i, t) \mid 1 \leq i < t\}$
  end
  $B = B \setminus \{(i, j)\}$
end

Algorithm 2: Algoritmo di Buchberger

Questo algoritmo termina, poiché ad ogni passo si ingrandisce G, ovvero si ha una catena $\mathrm{Lt}(G_1) \subset \mathrm{Lt}(G_2) \subset \dots$; ma dato che ogni ideale è finitamente generato, ad un certo punto questa catena si stabilizza, ovvero non aggiungo più elementi a G.

Esempio. Consideriamo $I = (f_1, f_2) = (xy^2 + x, x^2y + y)$, e calcoliamone una base.

Teorema 2.12 (Eliminazione)**.** *Sia $I \subset k[x_1, \dots, x_n]$ un ideale e G una base di Gröbner di I secondo l'ordinamento* `lex`*. Consideriamo $I_k = I \cap k[x_{k+1}, \dots, x_n]$ il k-esimo ideale di eliminazione e $G_k = G \cap k[x_{k+1}, \dots, x_n]$.*
Allora G_k è una base di Gröbner di I_k

Osserviamo che $k[x_1, \dots, x_n]/_I$ è uno spazio vettoriale su k, generato dai resti nella divisione per I.

Proposizione 2.13. *Sia $I \subset k[x_1, \dots, x_n]$ un ideale; sono fatti equivalenti*

1. $\dim_k k[x_1, \dots, x_n]/_I$ *è finita*
2. $\forall i \; \exists h_i \in I$ *tali che* $\mathrm{lt}(h_i) = x_i^{s_i}$
3. *Presa $G = \{g_1, \dots, g_t\}$ una base di Gröbner, $\forall i \; \exists g_h \in G$ tali che* $\mathrm{lt}(g_h) = x_i^{s_i}$

Dimostrazione.

$3 \Rightarrow 2$ Ovvio

$2 \Rightarrow 3$ Allora per ogni i, $x_i^{s_i} \in \mathrm{Lt}(I)$, perciò esiste un elemento di base g_h per cui $\mathrm{lt}(g_h) \mid x_i^{s_i}$, da cui anche $\mathrm{lt}(g_h)$ è una potenza pura.

$1 \Rightarrow 2$ Se la dimensione è m finito, vuol dire che, fissato un i, esistono c_j non tutti nulli per cui $\sum c_j x_i^j = 0$; perciò risollevando abbiamo $\sum c_j x_i^j \in I$ che ha termine di testa potenza pura.

$3 \Rightarrow 1$ Gli elementi del quoziente possono essere visti come i resti delle riduzioni $f \xrightarrow{G}_* r$ con $f \in k[x_1, \dots, x_n]$; ma allora $r = \sum c_\alpha X^\alpha$ e $X^\alpha \notin \mathrm{Lt}(I)$ e poiché in $\mathrm{Lt}(I)$ ci sono tutte le potenze pure, $\mathrm{lt}(r)$ ha ciascuno degli esponenti boundato, perciò i possibili monomi di testa sono finiti, e questi sono proprio una base per lo spazio vettoriale quoziente.

□

Definizione 2.8. Un ideale I che soddisfa una delle condizioni precedenti è detto 0-dimensionale.

2.5 Risoluzione dei sistemi di equazioni polinomiali

In questo capitolo studieremo i sistemi del tipo

$$\begin{cases} f_1 = 0 \\ \vdots \\ f_k = 0 \end{cases}$$

dove $f_i \in k[x_1, \dots, x_n]$, con k algebricamente chiuso, e vogliamo trovarne le soluzioni.
Osserviamo che se tutti gli f_i hanno grado 1, questo sistema è esattamente un problema dell'algebra lineare, che sappiamo risolvere triangolando la matrice associata.
Cominciamo intanto con un paio di oggetti molto importanti:

Definizione 2.9. Dato $I \subset k[X]$, la *varietà affine* di I è $V(I) = \{\alpha \in k^n \mid f(\alpha) = 0 \; \forall f \in I\}$.
Dato $W \subset k^n$, l'*ideale* di W è $\mathcal{I}(W) = \{f \in k[X] \mid f(\alpha) = 0 \; \forall \alpha \in W\}$

Osservazione. Le cose con i x^n e le inclusioni

Un altro strumento fondamentale per indagare i sistemi polinomiali è la matrice di Sylvester, e in particolare il suo determinante

Definizione 2.10. Siano $f, g \in R[x]$ con R dominio; scriviamo $f = \sum^m a_i x^i$ e $g = \sum^n b_i x^i$.
La *matrice di Sylvester* è la seguente matrice $(m+n) \times (m+n)$:

$$\mathrm{Syl}(f,g) = \begin{pmatrix} a_m & a_{m-1} & & \cdots & & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_m & & \cdots & & & a_1 & a_0 & \cdots & 0 \\ \vdots & & \ddots & & & & & & & \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & \cdots & a_2 & a_1 & a_0 \\ b_n & \cdots & & b_1 & b_0 & & \cdots & & & \\ \vdots & & & & & & & & & \\ 0 & & & & & b_n & & & & b_0 \end{pmatrix}$$

Il *risultante* di f, g è $\mathrm{Ris}(f,g) = \det \mathrm{Syl}(f,g)$

Osservazione. Se uno tra f e g è una costante, ovvero ha grado 0, la matrice di Sylvester è diagonale.

Proposizione 2.14.

- $\operatorname{Ris}(f,g) \in R$
- $\operatorname{Ris}(g,f) = (-1)^{mn} \operatorname{Ris}(f,g)$
- $\operatorname{Ris}(af,g) = a^n \operatorname{Ris}(f,g)$ *se* $a \in R$

Dimostriamo ora alcune proprietà importanti del risultante.
Consideriamo il polinomio $f_m(x) = \prod(x - z_i)$ dove $z_1, \dots, z_m$ sono incognite; se espandiamo il prodotto, abbiamo $f_m(x) = \sum a_i^{(m)} x^i$ dove i coefficienti sono i polinomi simmetrici elementari.

Lemma 2.15. *Dato* $g = \sum b_i x^i \in R[x]$*, vale*

$$\operatorname{Ris}(f_m, g) = g(z_m) \operatorname{Ris}(f_{m-1}, g)$$

Dimostrazione.
Consideriamo la matrice $\operatorname{Syl}(f_m, g)$, e facciamo le seguenti operazioni elementari: moltiplichiamo la colonna i per z_m^{n+m-i} e sommiamola all'ultima colonna.

Dopo queste operazioni l'ultima colonna diventa esattamente $\begin{pmatrix} z_m^{n-1} f_m(z_m) \\ \vdots \\ f_m(z_m) \\ z_m^{m-1} g(z_m) \\ \vdots g(z_m) \end{pmatrix}$,

ma poichè $f_m(z_m) = 0$, possiamo riscriverla come $g(z_m) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ z_m^{m-1} \\ \vdots 1 \end{pmatrix}$.

Dato che le operazioni elementari non cambiano il determinante, possiamo calcolare $\operatorname{Ris}(f_m, g)$ usando questa matrice con l'ultima colonna modificata, che chiamiamo A; in particolare $\operatorname{Ris}(f_m, g) = g(z_m) \cdot \det A$. Se consideriamo quest'uguaglianza come tra polinomi in z_m, vediamo che a sinistra il grado è al più n (infatti ogni $a_i^{(m)}$ è lineare in z_m), mentre a destra almeno n (c'è infatti il polinomio g di grado n valutato in z_m); ciò vuol dire che il grado è esattamente n, ed in particolare $\det A$ è indipendente da z_m.
Allora per calcolare $\det A$ possiamo porre $z_m = 0$, perciò espandendo rispetto all'ultima colonna abbiamo $\det A = 1 \cdot \det B$, dove B è il minore delle prime $m+n-1$ righe e $m+n-1$ colonne; osserviamo che $B = \operatorname{Syl}(f_{m-1}, g)$ in quanto vale proprio $a_{i-1}^{(m-1)}(z_1, \dots, z_{m-1}) = a_i^{(m)}(z_1, \dots, z_{m-1}, 0)$. □

Come immediata conseguenza di questo lemma otteniamo il seguente

Teorema 2.16. *Siano* $f(x) = a_m \prod(x - \alpha_i)$ *e* $g(x) = b_n \prod(x - \beta_i)$*. Allora vale*

$$\begin{aligned} \operatorname{Ris}(f,g) &= (-1)^{mn} b_n^m \prod f(\beta_i) \\ &= a_m^n \prod g(\alpha_i) \\ &= a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j) \end{aligned}$$

Vediamo ora come il risultante sia un indicatore dei fattori comuni a f e g

Proposizione 2.17. *Dati $f, g \in R[x]$, esistono $A, B \in R[x]$ tali che $\deg A < \deg g$, $\deg B < \deg f$ e $\mathrm{Ris}(f, g) = Af + Bg$*

Dimostrazione.

□

Teorema 2.18 (Estensione)**.** *Sia $I = (f_1, \dots, f_s) \subset k[x_1, \dots, x_n]$ e $I_1 = I \cap k[x_2, \dots, x_n]$ il primo ideale di eliminazione; supponiamo $k = \bar{k}$. Scriviamo $f_i = g_i(x_2, \dots, x_n) \cdot x_1^{n_i} + \bar{f}_i$ con $\deg_{x_1} \bar{f}_i < n_i$.*
Sia $\alpha \in V(I_1)$ tale che $\alpha \notin V(g_1, \dots, g_s)$; allora esiste un $a \in k$ tale che $(a, \alpha) \in V(I)$.

Teorema 2.19 (Nullstellensatz)**.** *Sia k algebricamente chiuso e $I \subset k[x_1, \dots, x_n]$ un ideale. Valgono*

- *forma debole: $V(I) = \emptyset \iff I = (1)$*
- *forma forte: $\mathcal{I}(V(I)) = \sqrt{I}$*

3 Moduli

Introduciamo ora una nuova struttura algebrica che generalizza il concetto di spazio vettoriale, con il quale ha alcune somiglianze ma anche profonde differenze.

3.1 Definizioni

In tutto questo paragrafo A sarà un anello con unità.

Definizione 3.1. Dato un insieme M diciamo che è un A-*modulo* se $(M, +)$ è un gruppo abeliano, ed esiste una funzione $\cdot : A \times M \to M$ che soddisfa le seguenti proprietà:

- $(a + b) \cdot m = a \cdot m + b \cdot m$
- $a \cdot (m + n) = a \cdot m + a \cdot n$
- $a \cdot (b \cdot m) = (ab) \cdot m$
- $1 \cdot m = m$

Ovvero stiamo dotando un gruppo additivo di un prodotto per scalare, esattamente come uno spazio vettoriale; tuttavia essendo gli scalari elementi di un anello, spesso non si possono invertire.
In particolare, se A è un campo, allora un A-modulo è esattamente uno spazio vettoriale.

Osservazione. $0_A \cdot m = 0_M$ e $a \cdot 0_M = 0_M$

Esempio. $M = A$ è un A-modulo.
Se $A = \mathbb{Z}$, gli A-moduli sono i gruppi abeliani.
$A[x]$ è un A-modulo.

Definizione 3.2. $N \subset M$ è sottomodulo di M se $(N,+) < (M,+)$ e $\forall a \in A, n \in N$ si ha $an \in N$

Se I è un ideale di A, M è un A-modulo, possiamo definire il sottomodulo $I \cdot M = \{\sum a_i m_i \mid a_i \in I, m_i \in M\}$.
Inoltre, se $M_1, M_2 \subset M$ sono sottomoduli, posso considerare la somma $M_1 + M_2 = \{m_1 + m_2 \mid m_1 \in M_1, m_2 \in M_2\}$.
Osserviamo che se ho una famiglia $\{M_i\}$ di sottomoduli, allora l'intersezione $\bigcap M_i$ è ancora un sottomodulo.

Definizione 3.3. Dato un sottoinsieme $S \subset M$, il sottomodulo generato è $\langle S \rangle = \{\sum a_i s_i \mid a_i \in A, s_i \in S\}$

Andiamo ora a vedere come viene modificato il concetto di base rispetto agli spazi vettoriali.

Definizione 3.4.

- S si dice *insieme di generatori* di M se $\langle S \rangle = M$, ovvero ogni $m \in M$ si scrive come $m = \sum a_i s_i$.
  Se M ammete un insieme di generatori di cardinalità finita, si dice che M è *finitamente generato.*
- $S \subset M$ si dice *libero* se i suoi elementi sono linearmente indipendenti, ovvero $\sum a_i s_i = 0 \Rightarrow a_i = 0 \forall i$.
- Un insieme di generatori che è anche libero si dice *base* di M.

Osserviamo che, al contrario degli spazi vettoriali, non tutti i moduli ammettono una base.
Ad esempio, $\mathbb{Z}/n\mathbb{Z}$ come $\mathbb{Z}$-modulo non ha una base: se g è un suo generatore (ad esempio 1), abbiamo $n \cdot g = 0$, ma $n \neq 0$ in $\mathbb{Z}$; tuttavia se lo consideriamo come $\mathbb{Z}/n\mathbb{Z}$-modulo, 1 è anche libero, perciò $\{1\}$ è una base.
Considerando inoltre $A^n = A \times \cdots \times A$ come A-modulo, in analogia agli spazi vettoriali, questo ha per base i vettori coordinati.

Definizione 3.5. Un A-modulo è detto *libero* se ammette una base.

Definizione 3.6. Un'applicazione $f : M \to N$ dove M, N sono A-moduli è detta *omomorfismo* se soddisfa

- $f(m + n) = f(m) + f(n)$
- $f(a \cdot m) = a \cdot f(m)$

Possiamo inoltre definire nella solita maniera $\ker f$ e $\operatorname{Im} f$, che sono *entrambi* sottomoduli.

Definizione 3.7. Sia M un A-modulo e $N \subset M$ un sottomodulo; poichè $N \trianglelefteq M$ come gruppi additivi, esiste il gruppo quoziente ${M}/{N}$.
Posso ora metterci una struttura di A-modulo, ponendo $a \cdot (m + N) = am + N$, che è una buona definizione in quanto $aN \subset N$.
Questo modulo è detto *quoziente* di M per N.

In analogia a gruppi e anelli, abbiamo i vari teoremi di omomorfismo.

Teorema 3.1. *Siano* M, N *due* A*-moduli, e* $f : M \to N$ *un omomorfismo di moduli. Allora* $\operatorname{Im} f \cong {}^{M}\!\diagup_{\ker f}$

Dimostrazione.
Abbiamo intanto l'isomorfismo $\varphi : {}^{M}\!\diagup_{\ker f} \to \operatorname{Im} f$ come gruppi dato da $\varphi(m + \ker f) = f(m)$.
Osserviamo ora che $\varphi(a \cdot (m + \ker f)) = \varphi(am + \ker f) = f(am) = af(m) = a\varphi(m + \ker f)$, cioè φ è anche omomorfismo di A-moduli. $\square$

Teorema 3.2. *Siano* $M_1, M_2 \subset M$ *due sottomoduli. Allora vale* ${}^{M_1 + M_2}\!\diagup_{M_2} \cong {}^{M_1}\!\diagup_{M_1 \cap M_2}$

Osservazione. Se prendo un ideale $I \subset A$ e M un A-modulo, allora ${}^{M}\!\diagup_{IM}$ ha la struttura di ${}^{A}\!\diagup_{I}$-modulo.
Infatti $(a + I)(m + IM) = am + aIM + Im + IIM = am + IM$ è ben definita.