1. Sistemi normali

SISTEMI NORMALI DI GENERATORI PER GLI IDEALI DI $Z[x]$

di R. FRANCI e L. TOTI RIGATELLI [1]

PREMESSA

Se I e J sono due ideali principali di $Z[x]$ possiamo agevolmente confrontarli rispetto all'inclusione confrontando i loro generatori. Tuttavia se I e J non sono principali una ispezione diretta di due dati sistemi di generatori non ci permette in generale, di confrontare gli ideali stessi. In questa nota si da un teorema di riduzione a forma normale per sistemi di generatori di ideali di $Z[x]$, ossia si definiscono certi sistemi « normali » di generatori e si dimostra che ogni ideale ammette esattamente un sistema normale di generatori e si da un procedimento « effettivo » che permette di passare da un dato sistema finito di polinomi a un sistema normale per l'ideale da esso generato. Inoltre si dimostra che alcune delle questioni principali relative agli ideali hanno soluzione « effettiva » dati i loro sistemi normali.

1. SISTEMI NORMALI

Sia J un ideale di $Z[x]$. Per ogni numero naturale n indichiamo con J_n l'insieme costituito dai coefficienti direttivi dei polinomi di grado n di J e dallo zero.

Ovviamente:

LEMMA 1. *J_n è un ideale di Z.*

LEMMA 2. *La successione degli J_n è (debolmente) crescente.*

Poichè Z è euclideo e quindi noetheriano, la successione di cui al lemma 2 è stazionaria.

Poniamo $M = \{ n : J_{n-1} \subset J_n \}$ [2] convenendo che $0 \in M$ se e solo se $J_0 \neq \{0\}$. M è ovviamente finito.

---

[1]) Lavoro eseguito nell'ambito del gruppo nazionale per le strutture algebriche e geometriche e loro applicazioni del C.N.R. Anno 1976.

[2]) Ora e nel seguito col simbolo $\subset$ intendiamo l'inclusione propria.

Indichiamo con a_n il generatore non negativo di J_n. La successione $(a_n)_{n\in\omega})$[1] si dice *segnatura* dell'ideale J. Ovviamente la segnatura di un ideale non ridotto a $\{ 0 \}$ può avere solo un segmento iniziale finito di zeri.

DEF. 1. Un polinomio di $Z[x]$ si dice *normale* se e solo se:

(i) il suo grado n è in M;

(ii) il suo coefficiente direttivo è a_n;

(iii) il suo coefficiente $i-$ esimo (per ogni $i < n$) è non negativo e minore di a_i: se $a_i \neq 0$.

LEMMA 3. *Per ogni* $n \in M$ *esiste esattamente un polinomio normale appartenente a* J *di grado* n.

Dim. Sia $n \in M$ ed a_n il generatore non negativo di J_n.

Allora esiste un polinomio in J di grado n e coefficiente direttivo a_n; sia esso $p(x) = a_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0$. Consideriamo in J un polinomio del tipo $s(x) = a_{n-1} x^{n-1} + \ldots + c_1 x + c_0$. Se $a_{n-1} \neq 0$, poichè b_{n-1}, $a_{n-1} \in Z$ esistono q_{n-1}, $r_{n-1} \in Z$ tali che $b_{n-1} = a_{n-1} q_{n-1} + r_{n-1}$ con $0 \leqslant r_{n-1} < a_{n-1}$. In $p(x) - s(x) q_{n-1} \in J$ il coefficiente del termine di grado n è a_n, quello di grado $n - 1$ è r_{n-1}. Procedendo in modo analogo si costruisce un polinomio che verifica anche la (iii).

Supponiamo adesso che esistano due polinomi $q(x), p(x) \in J$ con $p(x) \neq q(x)$ e verificanti entrambi (i), (ii), (iii). Siano $p(x) = a_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0$; $q(x) = a_n x^{n-1} + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0$. $p(x) - q(x) \in J$. Sia i il massimo indice per cui $b_i - c_i \neq 0$, allora $b_i - c_i \in J_i$ e quindi $b_i - c_i = a_i a$ con $a \in Z$, contro la (iii). Da ciò segue $p(x) = q(x)$.

TEOREMA 1. *I polinomi normali costituiscono un sistema di generatori indipendenti per* J.[2])

Dim. Sia $p(x)$ un polinomio di J, facciamo vedere innanzitutto che $p(x)$ può essere espresso come combinazione lineare di polinomi normali. Lavoriamo per induzione sul grado di $p(x)$.

Passo zero: Sia $p(x)$ di grado zero. Salvo a confondere, come faremo sistematicamente, gli elementi di Z con i polinomi di grado zero, $p(x) \in J_0$. Da cui segue l'asserto.

---

[1]) Con ω indichiamo l'insieme dei naturali.

[1]) Ovviamente nel caso che stiamo esaminando questo risultato costituisce un raffinamento del teorema della base di Hilbert.

Passo induttivo: Supponiamo adesso che ogni polinomio in J di grado minore o uguale a $n - 1$ sia esprimibile come combinazione lineare di polinomi normali. Sia $p(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0 \in J$ di grado n. Distinguiamo due casi: $n \in M$. Consideriamo il polinomio normale di grado n; sia esso $q(x) = a_n x^n + d_{n-1} x^{n-1} + \ldots + d_0$. Essendo $c_n \in J_n$ sarà per un opportuno $c \in Z$, $c_n = a_n c$. Il polinomio $p(x) - cq(x)$ è in J ed è al più di grado $n - 1$; quindi per l'ipotesi induttiva è esprimibile come combinazione lineare di polinomi normali.

$n \notin M$. Sia m il massimo grado dei polinomi normali di grado minore di n e $q(x)$ il polinomio normale di grado m. Il polinomio $q(x)\, x^{n-m}$ è in J ed è di grado n. Essendo per le ipotesi fatte $a_n = a_m$ e $c_n \in J_n$ sarà per un opportuno $c \in Z$, $c_n = a_m c$; $p(x) - c\, q(x)\, x^{n-m}$ è un polinomio di grado al più $n - 1$, quindi per l'ipotesi induttiva è combinazione lineare di polinomi normali. Resta da vedere che i polinomi normali costituiscono un sistema di generatori linearmente indipendenti. Questo risultato segue banalmente dall'osservazione che il coefficiente direttivo di ciascun polinomio normale è multiplo proprio del coefficiente direttivo del polinomio normale di grado immediatamente più alto.

Osserviamo che nei casi in cui la situazione è così semplice da suggerire un certo sistema di generatori come « naturale », questo è il sistema normale. Per esempio se J è un ideale principale, $J = (f)$ allora $\{f\}$ è il sistema normale per J. Ancora se $J \cap Z = (p)$ cioè $J = (p, f)$ con $f = x^n + b_{n-1} x^{n-1} + \ldots + b_0$ con $0 \leqslant b_i < p$ allora $\{p, f\}$ è il sistema normale per J.

2. Segnature

Def. 2. Si dice *segnatura* ogni successione di naturali decrescente rispetto alla divisibilità da un certo indice in poi. Una segnatura si dice *normale* se è decrescente rispetto alla divisibilità.

Ovviamente una segnatura è una successione stazionaria.

Sia $\mathscr{S}$ l'insieme delle segnature. Se $a = (a_n)_{n \in \omega}$, $b = (b_n)_{n \in \omega}$ sono elementi di $\mathscr{S}$ poniamo $a < b$ se e solo se: (i) a_i divide b_i per ogni $i \in \omega$: (ii) l'indice di stazionarietà di a è minore o uguale a quello di b; (iii) a_i è divisore proprio di b_i per almeno un $i \in \omega$.

E' immediato verificare che $<$ è una relazione transitiva.

La segnatura di un ideale di $Z[x]$ è una segnatura normale. Viceversa ogni segnatura normale $a = (a_n)_{n \in \omega}$ è la segnatura di un opportuno ideale J_a di $Z[x]$, per esempio dell'ideale generato da $\{a_n x^n\}_{n \in \omega}$.