

TEORIA DEI POLINOMI

Argomenti trattati: polinomi in una o più variabili, polinomi simmetrici, polinomi omogenei, teoria del risultante.

NOTAZIONE E CONVENZIONI

All'interno della presente trattazione adottiamo le seguenti convenzioni:

- Quando non diversamente specificato assumiamo che R sia un anello commutativo unitario ed anche dominio d'integrità. In particolare il fatto che R sia ID, ci permette di dire che, se $f, g \in R[x]$ allora $\deg(fg) = \deg(f) + \deg(g)$, cosa che useremo abbastanza spesso.
- Tutte le sommatorie che compaiono si intendono finite
- Con $a \mid_S b$ intendiamo che $\exists s \in S$ t.c. $b = as$

Ed useremo la seguente notazione:

- Indichiamo con Q_R il campo delle frazioni su R
- $f'(x)$ indica la derivata formale di $f(x)$, ovvero se $f(x) = \sum_i a_i x^i$ definiamo $f'(x) = \sum_i (i \star a_i) x^{i-1}$, dove $\star : \mathbb{N} \times R \rightarrow R$ è tale che $\star(n, r) = \underbrace{r + r + \dots + r}_n$ volte.
- Con \mathbb{P}_R indichiamo l'insieme dei primi in R

POLINOMI IN UNA VARIABILE

TEOREMA DI RUFFINI

Enunciato

Sia $f(x) \in R[x]$. Allora $f(\alpha) = 0 \Leftrightarrow (x - \alpha) \mid_R f(x)$

Dimostrazione

\Rightarrow Notiamo che possiamo effettuare la solita divisione euclidea tra $f(x)$ e $(x - \alpha)$ restando ad ogni passaggio in $R[x]$ in quanto $x - \alpha$ è monico. Allora si ha $\exists q(x), r(x) \in R[x]$ t.c. $f(x) = q(x)(x - \alpha) + r(x)$, con $\deg r < 1$ oppure $r = 0$. Valutando in α si ha $0 = f(\alpha) = r(\alpha) \Rightarrow r = 0$ perché r ha al più grado 0.

\Leftarrow Scriviamo $f(x) = (x - \alpha)q(x)$ e valutando in α si ha la tesi.

LEMMA DELLA DERIVATA E MOLTEPLICITÀ DELLE RADICI

Enunciato

$f(x) \in R[x]$. Allora $(x - \alpha)^2 \mid_R f(x) \Leftrightarrow f(\alpha) = 0$ e $f'(\alpha) = 0$.

Dimostrazione

\Rightarrow $f(x) = (x - \alpha)^2 g(x) \Rightarrow f(\alpha) = (\alpha - \alpha)^2 g(\alpha) = 0$ e $f'(\alpha) = (2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)) \mid_{x=\alpha} = 0$

\Leftarrow Dal teorema di Ruffini sappiamo che $f(\alpha) = 0 \Rightarrow f(x) = (x - \alpha)h(x)$. Allora $f'(x) = h(x) + (x - \alpha)h'(x)$ e $0 = f'(\alpha) = h(\alpha)$ quindi, ancora per Ruffini, abbiamo $(x - \alpha) \mid h(x)$, ovvero $(x - \alpha)^2 \mid f(x)$

MASSIMO NUMERO DI RADICI DEL POLINOMIO

Enunciato

$f(x) \neq 0 \in R[x]$, $\deg f = n$. Allora $f(x)$ ha al più n radici in R .

Dimostrazione

Ogni volta che troviamo una radice α di f , possiamo dire $f(x) = (x - \alpha)g(x)$ e abbiamo che $\deg g = \deg f - 1$, da cui la tesi.

TEOREMA DELLE RADICI IN Q_R

Enunciato

Sia R GCD, $f(x) \in R[x]$, $\deg f = n$, $f(x) = \sum_i a_i x^i$, $\alpha \in Q_R$ una sua radice. Allora, detti $p, q \in R$ t.c. $\alpha = \frac{p}{q}$, si ha che $p \mid a_0$ e $q \mid a_n$.

Dimostrazione

Sappiamo che $0 = f(\frac{p}{q}) = a_n(\frac{p}{q})^n + \dots + a_1 \frac{p}{q} + a_0$ e possiamo supporre $\frac{p}{q}$ ridotta ai minimi termini, ovvero con $(p, q) = 1$. Moltiplicando da ambo i lati per q^n si ottiene $0 = a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n$ e notiamo che q divide tutti i termini tranne $a_n p^n$ e p divide tutti i termini tranne $a_0 q^n$, quindi si ha, poiché q e p sono coprimi, $p \mid a_0$ e $q \mid a_n$.

PRINCIPIO DI IDENTITÀ DEI POLINOMI

Enunciato

$f(x) \in R[x]$, $\deg f = n$, $f(x) = \sum_i a_i x^i$. Supponiamo $\exists \alpha_1, \dots, \alpha_{n+1}$ $n+1$ radici con molteplicità di $f(x)$. Allora $f(x) \equiv 0$.

Dimostrazione

Ovvia, segue dal "Massimo numero di radici del polinomio".

STRANA DIVISIBILITÀ

Enunciato

$f(x) \in R[x]$, $a, b \in R$. Allora $(b-a) \mid_R (f(b) - f(a))$.

Dimostrazione

Effettuiamo la divisione di $f(x)$ per $(x-a)$. Si ha $\exists q(x), r(x) \in R[x]$ tali che $f(x) = (x-a)q(x) + r(x)$. Ora valutando in a si ottiene $f(a) = r(a) = r(x)$ (perché $\deg r \leq 0$) e, valutando in b si ha $f(b) = (b-a)q(b) + r(b) = (b-a)q(b) + f(a)$, e sottraendo $f(b) - f(a) = (b-a)q(b)$, quindi $(b-a) \mid_R (f(b) - f(a))$.

CRITERIO DI IRRIDUCIBILITÀ DI EISENSTEIN

Enunciato

$f(x) = \sum_i a_i x^i \in R[x]$, $\deg f = n$. Se $\exists p \in \mathbb{P}_R$ t.c. $p \nmid a_n$, $p \mid a_0, a_1, \dots, a_{n-1}$, $p^2 \nmid a_0$ allora $f(x)$ si può ridurre solo come $\beta \cdot h(x)$ con $\beta \in R$.

Dimostrazione

Supponiamo $\exists g(x), h(x) \in R[x]$ t.c. $f(x) = g(x) \cdot h(x)$. Sia $A = R/(p)$ il dominio d'integrità quoziente (perché (p) è un ideale primo). Allora abbiamo $\bar{f}(x) = \bar{a}_n x^n$. Quindi la fattorizzazione di $\bar{f} = \bar{g} \cdot \bar{h}$ implica \bar{g}, \bar{h} sono monomi (perché altrimenti il prodotto ha più termini di uno siccome A è ID). Allora abbiamo $\bar{g} = \bar{g}_s x^s$, $\bar{h} = \bar{h}_r x^r$, con $\bar{g}_s, \bar{h}_r \neq 0$. Quindi $s+r = n$ e se s oppure $r \geq 1$ si ha $p^2 \mid a_0$. Assurdo. Allora WLOG $\deg g = 0$. Ovvero $f(x) = g_0 \cdot h(x)$.

IRRIDUCIBILITÀ PER TRASLAZIONI

Enunciato

Se $f(x)$ si fattorizza come $g(x)h(x)$, allora anche $f(x+a)$ si fattorizza

Dimostrazione

Ovvia: $g(x+a)h(x+a) = f(x+a)$ e notiamo che $\deg g(x+a) = \deg g(x)$ e $\deg h(x+a) = \deg h(x)$. Può essere usato con profitto per poi usare Eisenstein sul polinomio traslato.

HENSEL LIFTING LEMMA

Qui i primi **non** indicano la derivata, ma altri polinomi.

Enunciato

$I \subseteq R$ ideale. Dati $f, g, h, s, t \in R$ tali che $f \equiv gh \pmod I$ e $sg + th \equiv 1 \pmod I$ allora $\exists g', h' \in R$ tali che $f \equiv g'h' \pmod{I^2}$, $g' \equiv g \pmod I$ e $h' \equiv h \pmod I$. Inoltre se g' e h' soddisfano le condizioni precedenti allora si ha anche $s'g' + t'h' \equiv 1 \pmod{I^2}$ per qualche $s' \equiv s \pmod I$ e $t' \equiv t \pmod I$. g', h' sono unici nel senso

che ogni altra soluzione g^* e h^* che soddisfa le condizioni sopra soddisfa anche $g^* \equiv (1+u)g' \pmod{I^2}$ e $h^* \equiv (1-u)h' \pmod{I^2}$ per qualche $u \in I$.

Dimostrazione

Sia $f - gh \equiv e \pmod{I^2}$, verifichiamo che $g' := g + te \pmod{I^2}$ e $h' := h + se \pmod{I^2}$ soddisfano le condizioni $f \equiv g'h' \pmod{I^2}$, $g' \equiv g \pmod{I}$ e $h' \equiv h \pmod{I}$. Ci riferiamo a queste tre condizioni assieme con C.

Per tutti i g', h' che soddisfano C, sia $d := sg' + th' - 1 \pmod{I^2}$, verifichiamo che $s' := (1-d)s \pmod{I^2}$ e che $t' := (1-d)t \pmod{I^2}$ soddisfano le condizioni $s'g' + t'h' \equiv 1 \pmod{I^2}$, $s \equiv s' \pmod{I}$ e $t \equiv t' \pmod{I}$.

Supponiamo che g^*, h^* siano altre soluzioni che soddisfano C. Sia $v := g^* - g'$, $w := h^* - h'$. La relazione $g^*h^* \equiv g'h' \pmod{I^2}$ implica $g'w + h'v \equiv 0 \pmod{I^2}$, siccome $v, w \in I$. Allora visto che $s'g' + t'h' \equiv 1 \pmod{I^2}$, moltiplicando entrambi i membri per v otteniamo $(s'v - t'w)g' \equiv v \pmod{I^2}$. Prendendo $u = s'v - t'w \in I$, $g^* \equiv (1+u)g' \pmod{I^2}$, in maniera simile $h^* \equiv (1-u)h' \pmod{I^2}$.

POLINOMI IN PIÙ VARIABILI

PRINCIPIO DI IDENTITÀ DEI POLINOMI

Enunciato

R di cardinalità infinita. Se $f \in R[x_1, \dots, x_n]$ è tale che $\forall a = (a_1, \dots, a_n) \in R^n \quad f(a) = 0$ allora si ha $f \equiv 0$, ovvero f è il polinomio identicamente nullo.

Dimostrazione

Mostriamo per induzione sul numero di incognite n che se $f \neq 0$ allora esiste un punto dove f non ha valore nullo. Per $n = 1$ l'abbiamo già fatto con l'analogo teorema in una variabile. Mostriamo ora il passo induttivo: supponiamo che $f \in R[x_1, \dots, x_n][x_{n+1}]$ e chiamiamo $y = x_{n+1}$ per comodità. Allora, ordinando i termini per il loro grado in y si ha $f = y^s(a_0 + a_1y + \dots + a_ry^r)$. Prendiamo il punto $\bar{x} \in R^n$ t.c. $a_0(\bar{x}) \neq 0$ e valutiamo tutti i polinomi a_k in \bar{x} , ottenendo $f(\bar{x}, y) = y^s(u_0 + u_1y + \dots + u_ry^r)$ dove $u_j = a_j(\bar{x}) \in R$. Sapendo che ora $g(y) := f(\bar{x}, y) \in R[y]$ è non nullo e che R ha cardinalità infinita so che $\exists q \in R$ t.c. $g(q) \neq 0$ allora so che il punto (\bar{x}, q) è tale che $f(\bar{x}, q) \neq 0$. Abbiamo così dimostrato ciò che volevamo.

NULLSTELLENSATZ

Lemma delle K -algebre

Enunciato

Dato K un campo, sia L una K -algebra finitamente generata su K . Se L è anche un campo, allora L è algebrico su K .

Dimostrazione

Sia $L = K[\alpha_1, \dots, \alpha_n]$. Supponiamo per assurdo che L **non** sia algebrico su K . Allora $\exists i$ t.c. α_i non è algebrico su K (se lo fossero tutti avrei L/K algebrico per torri). Consideriamo quindi $K(\alpha_i) \hookrightarrow L$ poichè L è un campo. Inoltre abbiamo $K(x) \cong K(\alpha_i)$ perché usando il morfismo che manda $x \mapsto \alpha_i$ otteniamo che ha Ker banale (altrimenti troviamo $p \in K[x]$ t.c. $p(\alpha_i) = 0$ assurdo). Adesso mostriamo che $K(x)$ **non** è finitamente generata come K -algebra: supponiamo che lo sia. Allora esistono $\{e_i\}_{i=1}^r \subset K(x)$ t.c. $\forall f(x) \in K(x) \quad f(x) = \sum_i^{\text{finite}} s_i \prod_j^{\text{finite}} e_j$ dove $s_i \in K$. Ma, scrivendo $e_i = \frac{a_i(x)}{b_i(x)}$ notiamo che necessariamente si avrebbe che ogni elemento di $K(x)$ può avere al denominatore solo elementi irriducibili che compaiono nella fattorizzazione di almeno uno dei $b_i(x)$, denominatori della base in numero finito. Mostrando ora che esistono infiniti polinomi irriducibili in $K[x]$ terminiamo la dimostrazione, ottenendo un assurdo e dovendo quindi avere che L/K è algebrico.

Supponiamo che esistano solo un numero finito di polinomi irriducibili in $K[x]$. Siano essi p_1, \dots, p_m . Consideriamo allora $S^* = (\prod_{i=1}^m p_i) + 1$. Siccome $K[x]$ è PID (e quindi UFD) abbiamo che gli elementi irriducibili sono anche primi, quindi i (p_i) sono ideali primi, ovvero sono anche massimali. O S^* è irriducibile, assurdo, oppure $S^* = \prod_{j=1}^m p_j^{\beta_j}$. Sia \bar{k} t.c. $\beta_k \geq 1$ e consideriamo $S^* \pmod{(p_k)}$. Otteniamo $0 \equiv \prod_{j=1}^m p_j^{\beta_j} \equiv S^* \equiv 1 + (\prod_{i=1}^m p_i) \equiv 1 \pmod{(p_k)}$ quindi $(p_k) = (1)$ e p_k è invertibile, contro l'ipotesi che fosse irriducibile. Abbiamo quindi l'assurdo voluto.

Nullstellensatz, forma debole

Enunciato

Sia K un campo algebricamente chiuso. Allora ogni ideale massimale nell'anello di polinomi $R = K[x_1, \dots, x_n]$ ha la forma $(x_1 - a_1, \dots, x_n - a_n)$ per qualche $a_1, \dots, a_n \in K$. Come conseguenza, una famiglia di funzioni polinomiali su K^n con nessuno zero in comune genera l'ideale unitario di R .

Dimostrazione

Se M è un ideale massimale di R , allora R/M è un campo che è finitamente generato come K -algebra. Per il lemma precedente, e poiché K è algebricamente chiuso si ha $R/M \cong K$. Quindi ogni x_i viene mappato in qualche $a_i \in K$ dalla mappa naturale $R \rightarrow R/M \cong K$, quindi M contiene l'ideale $(x_1 - a_1, \dots, x_n - a_n)$. Questo è un ideale massimale, quindi è uguale a M . Per quanto riguarda la seconda affermazione, si consideri l'ideale generato da qualche funzione polinomiale data senza zeri in comune. Se stesse in qualche ideale massimale, ovvero $(x_1 - a_1, \dots, x_n - a_n)$, allora tutte le funzioni dovrebbero avere uno zero in $(a_1, \dots, a_n) \in K^n$, contrariamente alle ipotesi. Siccome non sta in nessun ideale massimale, deve essere tutto R .

Nullstellensatz, forma forte**Enunciato**

Sia K un campo algebricamente chiuso e g e f_1, \dots, f_m siano membri di $R = K[x_1, \dots, x_n]$, visti come funzioni polinomiali su K^n . Se g si azzera sul luogo degli zeri comuni degli f_i , allora qualche potenza di g appartiene all'ideale che generano.

Dimostrazione

(*Rabinowitsch trick*: aggiungiamo un'incognita) I polinomi f_1, \dots, f_m e $x_{n+1}g - 1$ non hanno zeri comuni in K^{n+1} , quindi per il Nullstellensatz debole si ha

$$1 = p_1 f_1 + \dots + p_m f_m + p_{m+1}(x_{n+1}g - 1)$$

dove i p_i sono polinomi in x_1, \dots, x_{n+1} . Prendendo l'immagine di questa equazione attraverso l'omomorfismo $K[x_1, \dots, x_{n+1}] \rightarrow K(x_1, \dots, x_n)$ dato da $x_{n+1} \mapsto \frac{1}{g}$ troviamo che

$$1 = p_1(x_1, \dots, x_n, \frac{1}{g})f_1 + \dots + p_m(x_1, \dots, x_n, \frac{1}{g})f_m$$

Moltiplicando ora per la giusta potenza di g per cancellare i denominatori si ha la tesi.

POLINOMI SIMMETRICI

POLINOMI OMOGENEI

I FATTORI DI POLINOMI OMOGENEI SONO OMOGENEI**IL RISULTANTE**
