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 $\star : \mathbb{N} \times R \to R$ è tale che $\star(n, r) = \underbrace{r + r + \ldots + r}$ 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
$\boxed{\Rightarrow}$ 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 $0 = f(\alpha) = r(\alpha) \implies r = 0$ perché r ha al più grado 0.
$\boxed{\Leftarrow}$ 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
$\boxed{\Rightarrow}$ $f(x) = (x - \alpha)^2 g(x) \implies f(\alpha) = (\alpha - \alpha)^2 g(\alpha) = 0$ e $f'(\alpha) = (2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)) \mid_{x=\alpha} = 0$
$\boxed{\Leftarrow}$ Dal teorema di Ruffini sappiamo che $f(\alpha) = 0 \implies f(x) = xh(x)$. 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 $f(x) = (x - a)g(x)$ 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 $0 = f(\frac{p}{q}) = a_n(\frac{p}{q})^n + \ldots + a_1\frac{p}{q} + a_0$ 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 $0 = a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 pq^{n-1} + a_0 q^n$ 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 $\exists \alpha_1, \ldots, \alpha_{n+1}$ $n + 1$ 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. $p \nmid a_n, \quad p \mid a_0, a_1, \ldots, a_{n-1}, \quad p^2 \nmid a_0$ 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 $\bar{g_s}, \bar{h_r} \neq_A 0$. 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

Enunciato
$f(x) \in R[x]$
Dimostrazione

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 $f = y^s(a_0 + a_1 y + \dots + a_r y^r)$. 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 $f(\bar{x}, y) = y^s(u_0 + u_1 y + \dots + u_r y^r)$ 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

Polinomi simmetrici

Polinomi omogenei

I fattori di polinomi omogenei sono omogenei

Il risultante