UNIVERSITÀ DEGLI STUDI DI ROMA TRE
FACOLTÀ DI SCIENZE M.F.N.

# Criteri di irriducibilità e poligoni di Newton

Sintesi della tesi di Laurea in Matematica
di Doriana Fulgoni
Relatore: Prof. Marco Fontana

Il problema dell'irriducibilità dei polinomi in $R[x]$, dove $R$ è un dominio a fattorizzazione unica, ha un'importanza notevole, dovuta al fatto che i polinomi irriducibili hanno un ruolo fondamentale nell'insieme di tutti i polinomi: essi hanno in $R[x]$ lo stesso ruolo che hanno i numeri primi per $\mathbb{Z}$. Pertanto per determinare una fattorizzazione in "atomi" di un polinomio occorre disporre di un metodo per stabilire se il polinomio è o non è irriducibile. A tale scopo, un semplice criterio è ciò a cui si aspira.

Uno dei più semplici criteri d'irriducibilità è stato dimostrato da Schönemann nel 1846 [**?**]:

"*Sia $p \in \mathbb{Z}$ un numero primo e $f(x) \in \mathbb{Z}[x]$ un polinomio avente la forma*

$$f(x) = \Phi(x)^e + pM(x)$$

*dove $\Phi(x)$ è un polinomio irriducibile modulo $p$ e $M(x)$ è un polinomio relativamente primo con $\Phi(x)$ modulo $p$, e $deg(M(x)) < deg(f(x))$. Allora $f(x)$ è irriducibile in $\mathbb{Q}[x]$.*"

Il più conosciuto criterio d'irriducibilità, pubblicato da Eisenstein nel 1850, è un caso particolare del criterio di Schönemann. Infatti, se $f(x)$ è monico, il criterio di Eisenstein si ricava da quello di Schönemann ponendo: $\Phi(x) = x$, $e = n = deg(f(x))$ e $pM(x) = f(x) - x^n$. Se il coefficiente direttore $a_0$ di $f(x)$ non è 1, allora moltiplicando per $a_0^{n-1}$ e sostituendo $x$ con $y = a_0 x$

si ottiene un polinomio monico $g(y) \in \mathbb{Z}[y]$ la cui irriducibilità è equivalente a quella di $f(x)$.

Un'importante applicazione del Criterio di Schönemann-Eisenstein è la dimostrazione dell'irriducibilità del polinomio ciclotomico

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1 \ ,$$

dove $p$ è un primo.

Nel 1890, Köenisberger e Netto generalizzarono il teorema di Schönemann-Eisenstein. Poi nel 1905 Bauer e Perron [**?**] estesero il criterio di Köenisberger. Tutti questi risultati verranno poi generalizzati nel 1906 da Dumas [**?**], utilizzando i poligoni di Newton, nelle sue "investigazioni generali".

L'uso del concetto dei poligoni di Newton fu usato anche da Kurschak, Rella e Ore [**?**] per ottenere alcuni criteri di irriducibilità, per lo più per polinomi a coefficienti interi. Nel 1938 MacLane [**?**] ottenne un teorema generale che includeva tutti questi criteri come casi particolari, ma dimostrato senza l'uso dei poligoni di Newton. Dalla pubblicazione dell'articolo di MacLane, l'uso dei poligoni di Newton scomparve quasi del tutto, eccetto che in pochi libri specifici. Ritroviamo questo metodo nel 1995 nell'articolo di Mott [**?**]; egli usando tale metodo rielabora in chiave moderna la dimostrazione dei criteri di Dumas, Ore e Perron e li applica per dimostrarne di nuovi. Questi suoi risultati sono meno generali di quelli di MacLane, ma più facili da applicare in certe situazioni.

Il lavoro di Mott è finalizzato allo studio di polinomi che abbiano il poligono di Newton con due segmenti (per le definizioni v. pag 15-16). Vengono considerati due casi: quello in cui i due segmenti hanno rispettivamente larghezza 1 e $n-1$ e quello in cui i due segmenti hanno rispettivamente larghezza 2 e $n-2$. Per polinomi con questa proprietà, utilizzando le congruenze modulo un primo $p$, vengono dimostrati alcuni nuovi criteri d'irriducibilità ad esempio:

" *Sia* $n > 2$ *e* $f(x) \in \mathbb{Z}[x]$ *un polinomio che ridotto modulo* 3 *assume la seguente forma:*

$$\overline{f(x)} = x^n + x^2 + 2 \ .$$

*Allora, il polinomio* $f(x)$ *non ha radici modulo* 3 *e, se* $n \equiv 3, 7 \ (mod\ 8)$*,* $f(x)$ *non possiede fattori quadratici. Se in più il poligono di Newton* $N_v(f(x))$ *ha un segmento di larghezza* 2 *ed uno di larghezza* $n-2$*, allora* $f(x)$ *è irriducibile in* $\mathbb{Q}[x]$."

Dopo aver studiato e analizzato il lavoro svolto da Mott, usando delle tecniche di dimostrazione analoghe alle sue, siamo riusciti a dimostrare alcuni criteri di irriducibilità non troppo generali, ma di facile applicazione in determinate situazioni; abbiamo cioè sviluppato il caso in cui i due segmenti hanno larghezza rispettivamente 3 e $n-3$, giungendo a dimostrare teoremi analoghi al caso "$n-2$" studiato da Mott.

Nel Capitolo 0 richiameremo, senza dimostrarli, alcuni risultati sui polinomi, Paragrafo 1, e sulle valutazioni, Paragrafo 2, che verranno utilizzati nei capitoli successivi.

Nel Capitolo 1 dopo aver introdotto il concetto di poligono di Newton, daremo una serie di risultati dovuti a Dumas, che servono a caratterizzare alcune proprietà dei poligoni di Newton rispetto ai polinomi attraverso cui vengono definiti.

Di notevole importanza, in quanto viene applicato spesso in quasi tutti i criteri successivi, sarà il Corollario 1.3 (la numerazione si riferisce alla tesi di laurea):

"*Se $f(x)$ è irriducibile in $\hat{K}[x]$, allora $N_v(f(x))$ consiste di un solo spigolo la cui larghezza è uguale al grado del polinomio $f(x)$. Conseguentemente, se $f(x)$ è monico irriducibile in $\hat{K}[x]$ allora, per ogni $i$, $0 \leqslant i \leqslant n$ :*

$$v(a_i) \geqslant \frac{v(a_n)i}{n}$$

*e in particolare*

$$v(a_i) \geqslant \min\{v(a_0), v(a_n)\} = \min\{0, v(a_n) - v(a_0)\} \quad .$$"

Osserveremo che la prima affermazione del risultato precedente non si inverte, e negli Esempi 1.8 e 1.9 (la numerazione si riferisce alla tesi di laurea) mostreremo che è possibile avere anche polinomi riducibili o irriducibili con poligoni di Newton composti di un solo spigolo ma più di un segmento. Si può avere l'inverso solo se si aggiunge un'ipotesi, come si vede dal seguente risultato:

"*Se $N_v(f(x))$ consiste di un solo segmento, allora $f(x)$ è irriducibile $\hat{K}[x]$ e conseguentemente in $K[x]$.*"

Di cui si può dare un esempio:

" *Consideriamo il seguente polinomio:*

$$f(x) = x^5 + 9x^4 + 3x^3 + 18x^2 + 27x + 3 \, .$$

*Si vede subito che $f(x)$ è irriducibile in $\mathbb{Q}[x]$ (basta utilizzare il criterio di Eisenstein), quello che vogliamo vedere è se è irriducibile in $\hat{\mathbb{Q}}[x]$. Andiamo allora a studiare il suo poligono di Newton, se sarà composto da un solo segmento, allora per il risultato precedente il polinomio sarà irriducibile in $\hat{\mathbb{Q}}[x]$ e si avrà (Corollario 1.3): $v(a_i) \geqslant \frac{v(a_n)i}{n}$. Prendiamo come valutazione quella $3-adica$, $v_3$ e disegnamo il poligono di Newton $N_{v_3}(f(x))$.*

$$\begin{array}{rcccl} v_3(a_0) & = & v_3(1) & = 0 & \Rightarrow \quad A(0,0) \\ v_3(a_1) & = & v_3(9) & = 2 & \Rightarrow \quad B(1,2) \\ v_3(a_2) & = & v_3(3) & = 1 & \Rightarrow \quad C(2,1) \\ v_3(a_3) & = & v_3(18) & = 2 & \Rightarrow \quad D(3,2) \\ v_3(a_4) & = & v_3(27) & = 3 & \Rightarrow \quad E(4,3) \\ v_3(a_5) & = & v_3(3) & = 1 & \Rightarrow \quad F(5,1) \end{array}$$

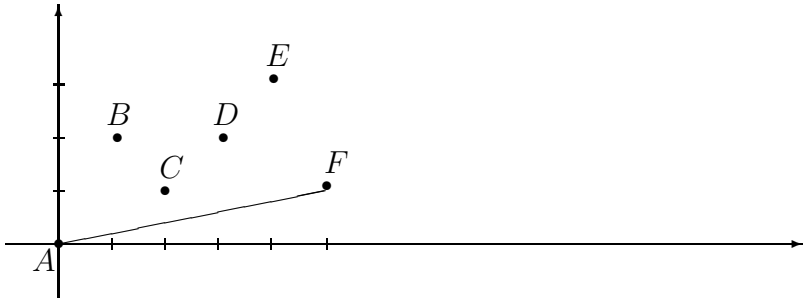


*Figura A*

*Come si vede dalla Figura A, il poligono di Newton $N_{v_3}(f(x))$ ha un solo spigolo che è anche un segmento perchè non passa per nessun altro punto dello $\mathbb{Z}$-Reticolo oltre ai suoi estremi. Inoltre si ha:*

$$\begin{aligned} 0 = v_3(a_0) &\geqslant \frac{v_3(a_5)\cdot 0}{5} = 0 \\ 2 = v_3(a_1) &\geqslant \frac{v_3(a_5)\cdot 1}{5} = 1/5 \\ 1 = v_3(a_2) &\geqslant \frac{v_3(a_5)\cdot 2}{5} = 2/5 \\ 2 = v_3(a_3) &\geqslant \frac{v_3(a_5)\cdot 3}{5} = 3/5 \\ 3 = v_3(a_4) &\geqslant \frac{v_3(a_5)\cdot 4}{5} = 4/5 \\ 1 = v_3(a_5) &\geqslant \frac{v_3(a_5)\cdot 5}{5} = 1 \end{aligned}$$

*e in particolare:*

$$v_3(a_i) \geqslant \min(0,1) = 0$$

*per ogni* $i = 0, ..., 5$."

Seguirà poi il Teorema di Dumas:

"*Se* $f(x) = g(x)h(x)$ *dove* $g(x)$ *e* $h(x)$ *sono polinomi non costanti* $\in \hat{K}[x]$, *allora il poligono di Newton* $N_v(f(x))$ *è composto di segmenti che hanno la stessa larghezza e inclinazione dei segmenti di* $N_v(g(x))$ *e* $N_v(h(x))$. *Inoltre, il grado di ogni fattore di* $f(x)$ *è la somma delle larghezze di alcuni dei segmenti di* $N_v(f(x))$."

Di cui possiamo vederne un'applicazione nel seguente esempio:
"*Consideriamo il seguente polinomio riducibile:*

$$\begin{aligned} f(x) &= g(x)h(x) = (x^2 + 6x + 4)(x^2 + 8x + 6) = \\ &= x^4 + 14x^3 + 58x^2 + 68x + 24 \in \mathbb{Q}[x] \ . \end{aligned}$$

*Esaminiamo i poligoni di Newton* $N_{v_2}(f(x))$, $N_{v_2}(g(x))$ *e* $N_{v_2}(h(x))$. *Per* $g(x)$ *avremo:*

$$\begin{array}{lllllll} v_2(a_0) & = & v_2(1) & = & 0 & \Rightarrow & A(0,0) \\ v_2(a_1) & = & v_2(6) & = & 1 & \Rightarrow & B(1,1) \\ v_2(a_2) & = & v_2(4) & = & 2 & \Rightarrow & C(2,2) \end{array}$$

*per* $h(x)$*:*

$$\begin{array}{lllllll} v_2(a_0) & = & v_2(1) & = & 0 & \Rightarrow & A(0,0) \\ v_2(a_1) & = & v_2(8) & = & 3 & \Rightarrow & D(1,3) \\ v_2(a_2) & = & v_2(6) & = & 1 & \Rightarrow & E(2,1) \end{array}$$

*Tracciamo quindi il grafico dei due poligoni di Newton:*

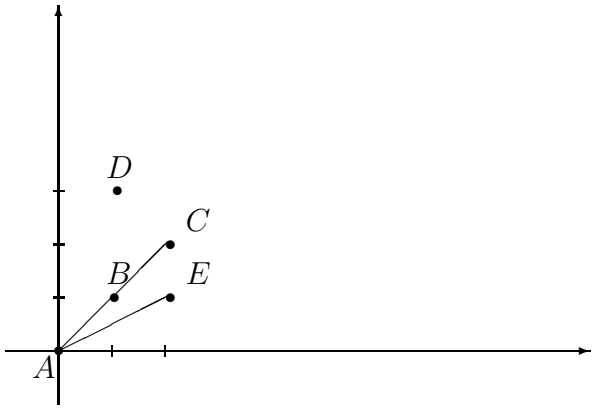


*Figura B*

*Lo spigolo $\overline{AC}$, rappresentante il poligono $N_{v_2}(g(x))$, ha larghezza 2 e inclinazione 1; lo spigolo $\overline{AE}$, rappresentante il poligono $N_{v_2}(h(x))$, ha larghezza 2 e inclinazione 1/2. Andiamo ora a disegnare il poligono $N_{v_2}(f(x))$.*

$$\begin{array}{lllll} v_2(a_0) = v_2(1) = 0 & \Rightarrow & A(0,0) \\ v_2(a_1) = v_2(14) = 1 & \Rightarrow & B(1,1) \\ v_2(a_2) = v_2(58) = 1 & \Rightarrow & C(2,1) \\ v_2(a_3) = v_2(68) = 2 & \Rightarrow & D(3,2) \\ v_2(a_4) = v_2(24) = 3 & \Rightarrow & E(4,3) \end{array}$$

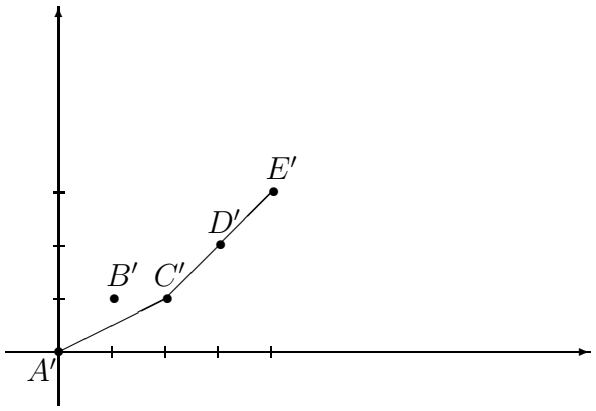


*Figura C*

*Come si vede dalle due figure, lo spigolo $\overline{A'C'}$ della Figura C corrisponde allo spigolo $\overline{AE}$ della Figura B, mentre lo spigolo $\overline{C'E'}$ della Figura C corrisponde allo spigolo $\overline{AC}$ della Figura B; infatti lo spigolo $\overline{A'C'}$ ha larghezza 2 e inclinazione 1/2, mentre lo spigolo $\overline{C'E'}$ ha larghezza 2 e inclinazione 1. Osserviamo inoltre che i due fattori di $f(x)$ sono entrambi di secondo grado, così come i due spigoli del poligono $N_{v_2}(f(x))$ hanno entrambi larghezza 2, confermando il Teorema di Dumas.*"

Successivamente daremo un'idea di come, in generale, si costruisce il poligono di Newton di un polinomio riducibile prodotto di due o più polinomi.

Nel Capitolo 2 ci occuperemo del caso in cui le valutazioni sono discrete, determinando, in modo generale, come suddividere gli spigoli del poligono di Newton in segmenti e, in particolare, quando un dato spigolo è esso stesso un segmento. Avremo ad esempio il seguente teorema:

"*Supponiamo $v(K^*) = \mathbb{Z}$ e che $(r, v(a_r)) \longleftrightarrow (s, v(a_s))$ sia uno spigolo $E$ di $N_v(f(x))$ con altezza*

$$h = v(a_s) - v(a_r)$$

*e larghezza*

$$\omega = s - r$$

*Sia* $d = MCD(h, \omega)$. *Allora gli unici punti dello* $\mathbb{Z}$*-reticolo che giacciono su* $E$ *sono i punti con la prima coordinata*

$$x_k = r + k\frac{s-r}{d} \quad dove \quad 0 \leqslant k \leqslant d$$

*Per cui, lo spigolo* $E$ *può essere suddiviso in* $d$ *segmenti ciascuno di larghezza* $(s-r)/d$. *In particolare, se* $d = 1$, *allora non ci sono punti dello* $\mathbb{Z}$*-reticolo su* $E$ *eccetto i suoi estremi, quindi* $E$ *è esso stesso un segmento di* $N_v(f(x))$."

Vediamone un'applicazione:

"*Esaminiamo il polinomio:*

$$f(x) = x^6 + 6x^5 + 15x^4 + 18x^3 + 9x^2 + 27 \in \mathbb{Q}[x]$$

*e prendiamo come valutazione quella 3-adica,* $v_3$. *Il poligono di Newton* $N_{v_3}(f(x))$ *è determinato dai seguenti punti:*

$$\begin{array}{lllll} v_3(a_0) = v_3(1) = 0 & \Rightarrow & A(0,0) \\ v_3(a_1) = v_3(6) = 1 & \Rightarrow & B(1,1) \\ v_3(a_2) = v_3(15) = 1 & \Rightarrow & C(2,1) \\ v_3(a_3) = v_3(18) = 2 & \Rightarrow & D(3,2) \\ v_3(a_4) = v_3(9) = 2 & \Rightarrow & E(4,2) \\ v_3(a_6) = v_3(27) = 3 & \Rightarrow & F(6,3) \end{array}$$

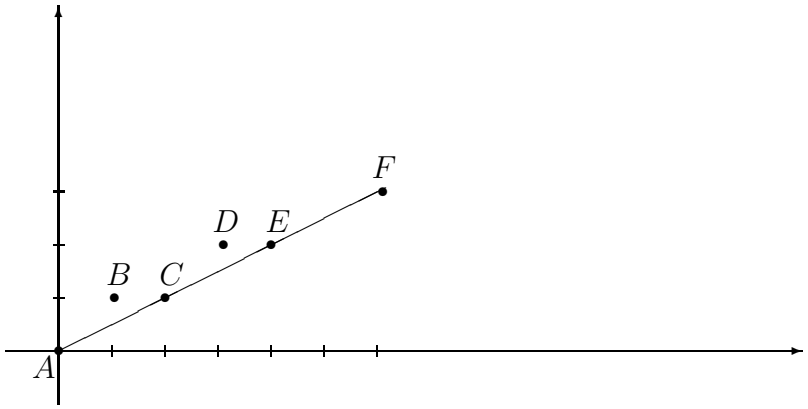


*Figura D*

*Osserviamo che il poligono di Newton* $N_{v_3}(f(x))$ *ha un solo spigolo formato da* 3 *segmenti, ognuno di larghezza* 2. *Infatti lo spigolo* $\overline{AF}$ *ha altezza* 3 *e*

*larghezza* 6*, quindi per il teorema precedente i segmenti di cui è composto devono avere larghezza uguale a* $2 = 6/3$*, inoltre saranno* $3 = MCD(3, 6)$*. Aggiungiamo che i punti dello* $\mathbb{Z}$*-reticolo che dividono lo spigolo in segmenti devono avere l'ascissa uguale a*

$$x_k = 0 + k\frac{6}{3} \quad dove \quad 0 \leqslant k \leqslant 2 \ ,$$

*infatti lo spigolo passa per i punti* $(2, 1)$ *e* $(4, 2)$*.*

Il Capitolo 3 conterrà i risultati pricipali di questa tesi: considereremo, infatti, polinomi con il poligono di Newton con due soli segmenti. Dai risultati dei capitoli precedenti seguirà che se il polinomio fosse riducibile dovrebbe avere due fattori, uno di grado uguale alla larghezza del primo segmento e l'altro di grado uguale alla larghezza del secondo segmento. Quindi, se con altri metodi, riusciremo ad escludere fattori di quel grado, allora potremo concludere che il polinomio considerato è irriducibile. Suddivideremo quindi il capitolo in tre paragrafi: nel primo considereremo il caso in cui il poligono di Newton ha due segmenti, uno di larghezza 1 e l'altro di larghezza $n - 1$. In questo caso il polinomio in questione o è irriducibile o ha due fattori, uno lineare ed uno di grado $n - 1$. Abbiamo considerato in un primo momento polinomi in $R[x]$, dove $R$ è un $UFD$, sviluppando il seguente teorema:

"*Sia* $R$ *un* $UFD$ *con campo dei quozienti* $K$*. Sia* $n > 2$ *e*

$$f(x) = x^n + a_1x^{n-1} + ... + a_n \ \in R[x]$$

*dove* $a_n = p_1^{e_1} \cdot ... \cdot p_m^{e_m} \cdot u$ *dove ogni* $p_i$ *è un elemento primo di* $R$ *e* $u \in U(R)$*. Supponiamo* $MCD(a_1, p_1, ..., p_m) = 1$ *e che il poligono di Newton* $N_{v_{p_1}}(f(x))$ *consista di esattamente due segmenti, uno di larghezza* 1 *e l'altro di larghezza* $n - 1$*. Supponiamo inoltre che per ogni* $p_j$ *con* $j \geqslant 2$*,* $N_{v_{p_j}}(f(x))$ *abbia un segmento di larghezza* 1*. Se* $f(u') \neq 0$ *per ogni* $u' \in U(R)$*, allora* $f(x)$ *è irriducibile in* $K[x]$*.*"

Nel seguente esempio applicheremo il risultato precedente:

" *Sia* $R = \mathbb{Z}[i]$*, consideriamo in* $R[x]$ *il seguente polinomio:*

$$f(x) = x^4 + (3 + 2i)x^3 - 345 + 152i$$

*Studiamone i coefficienti:* $a_1 = 3 + 2i$*, la sua norma è* 13*, quindi è un elemento primo di* $R$*;* $a_4 = -345 + 152i = (2 + 3i)^2 \cdot (5 + 2i)^2$*, la norma dei suoi fattori è rispettivamente* 13 *e* 29*, quindi sono entrambi elementi primi di* $R$*. Se consideriamo la valutazione p-adica con* $p = 2 + 3i$ *otteniamo:*

$$\begin{array}{rcccccl} v_p(a_0) & = & v_p(1) & = & 0 & \Rightarrow & A(0,0) \\ v_p(a_1) & = & v_p(3+2i) & = & 0 & \Rightarrow & B(1,0) \\ v_p(a_4) & = & v_p(2+3i) & = & 2 & \Rightarrow & C(4,2) \end{array}$$

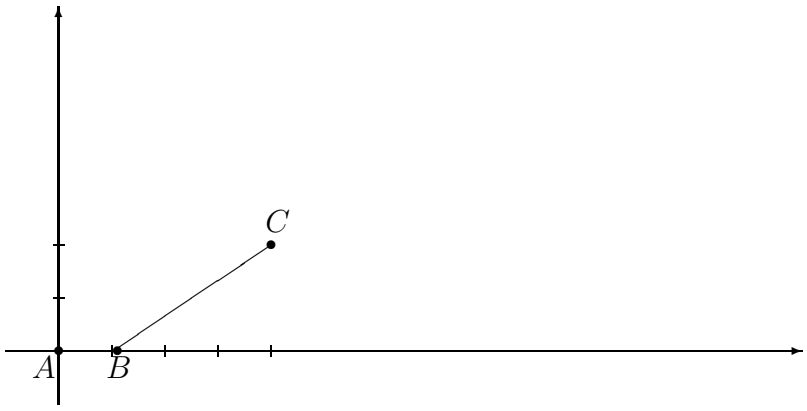


*Figura E*

*Quindi siamo nelle ipotesi del teorema precedente, dobbiamo verificare soltanto che* $f(u) \neq 0$ *per ogni* $u \in U(R)$. *Ora* $U(R) = \{\pm 1, \pm i\}$ *quindi andiamo a calcolarci* $f(u)$ *con* $u \in \{\pm 1, \pm i\}$*:*

$$\begin{aligned} f(1) &= -341 + 154i \neq 0 \\ f(-1) &= -347 + 150i \neq 0 \\ f(i) &= -342 + 152i \neq 0 \\ f(-i) &= -346 + 155i \neq 0\ . \end{aligned}$$

*Pertanto* $f(x)$ *è irriducibile in* $\mathbb{Q}[i][x]$.

Considereremo in seguito polinomi in $\mathbb{Z}[x]$. In questo ambito un modo per escludere fattori lineari consiste nell'escluderli in $\mathbb{Z}_q[x]$ per qualche primo $q$. Questo metodo è usato, ad esempio, nel "VII Teorema di Perron" (la numerazione si riferisce a quella dell'articolo originale [**?**]):

" *Supponiamo* $n > 2$ *e*

$$\begin{aligned} f(x) =& x^n + \alpha_1 x^{n-1} + p_1^{\left[\frac{e_1}{n-1}\right]+1} \cdot p_2^{\left[\frac{e_2}{n-1}\right]+1} \cdot \ldots \cdot p_m^{\left[\frac{e_m}{n-1}\right]+1} \cdot \alpha_2 x^{n-2} \\ &+ p_1^{\left[\frac{2e_1}{n-1}\right]+1} \cdot p_2^{\left[\frac{2e_2}{n-1}\right]+1} \cdot \ldots \cdot p_m^{\left[\frac{2e_m}{n-1}\right]+1} \cdot \alpha_3 x^{n-3} + \ldots \\ &+ p_1^{e_1} \cdot \ldots \cdot p_m^{e_m} u \quad \in \mathbb{Z}[x] \end{aligned}$$

*dove* $u \in U(\mathbb{Z})$. *Se*

$$\begin{aligned} 1 &= MCD(n-1, e_1) = MCD(n-1, e_2) = \ldots = MCD(n-1, e_m) = \\ &= MCD(\alpha_1, p_1 \ldots p_m) \end{aligned}$$

*e se* $\pm 1$ *non sono radici di* $f(x)$, *allora* $f(x)$ *è irriducibile in* $\mathbb{Q}[x]$."

Vediamo un esempio:

"*consideriamo il seguente polinomio:*

$$f(x) = x^6 + 11x^5 + 105x^4 + 315x^3 + 1575x^2 + 4725x + 4725$$

*osserviamo che:*

$$\begin{aligned} a_6 &= 3^3 \cdot 5^2 \cdot 7 \\ a_1 &= 11 \\ n-1 &= 5 \\ 105 &= 3 \cdot 5 \cdot 7 \\ 315 &= 3^2 \cdot 5 \cdot 7 \\ 1575 &= 3^2 \cdot 5^2 \cdot 7 \\ 4725 &= 3^3 \cdot 5^2 \cdot 7 \ . \end{aligned}$$

*Inoltre:*

$$\begin{aligned} &MCD(11, 3 \cdot 5 \cdot 7) = 1 \\ &MCD(5,3) = MCD(5,2) = MCD(5,1) = 1 \ . \\ &f(1) \neq 0 \neq f(-1) \end{aligned}$$

*Possiamo allora applicare il teorema precedente e affermare quindi che $f(x)$ è irriducibile in $\mathbb{Q}[x]$.*"

Nel secondo paragrafo dell'ultimo capitolo considereremo poligoni di Newton con due segmenti, uno di larghezza 2 e un di larghezza $n-2$. Si tratta in questo caso di eliminare la possibilità di fattori quadratici. Questo caso è stato studiato da Mott [**?**] nell'ambito dei polinomi a coefficienti interi, usando la riduzione modulo un primo $p$. Riporteremo i suoi risultati, non generali come quelli di MacLane, ma interessanti perchè di facile applicazione in determinati casi. Ad esempio menzioniamo il Teorema 3.2.5 (la numerazione si riferisce alla tesi di laurea):

" *Supponiamo $f(x) \in \mathbb{Z}[x]$ sia un polinomio che ridotto modulo* 3 *assume la seguente forma:*

$$\overline{f(x)} = x^n + 2x^2 + 2$$

*dove $n > 2$ è pari. Allora $f(x)$ non possiede fattori quadratici. Se in più $n \neq 4$ e il poligono di Newton $N_v(f(x))$ ha un segmento di larghezza* 2 *ed uno di larghezza $n-2$, allora $f(x)$ è irriducibile in $\mathbb{Q}[x]$.*"

Verrà applicato per ottenere il seguente esempio, il quale fornisce una ampia classe di polinomi irriducibili:

"*Sia* $n > 4$ *e*

$$f(x) = x^n + 2p^k x^2 + 2p^{e+k} \ ,$$

*dove* $p$ *è un primo,* $k$ *ed* $e$ *sono numeri positivi tali che:*

1) $p \equiv 1 \ (mod\ 3)$
2) $(n-2)k > 2e$
3) $MCD(e, n-2) = 1$
4) $n$ *è pari.*

*Allora* $f(x)$ *è irriducibile in* $\mathbb{Q}[x]$.
*La condizione su* $p$ *implica che* $f(x) \equiv x^n + 2x^2 + 2 \ (mod\ 3)$. *Inoltre le condizioni su* $k$ *e su* $e$ *implicano che* $N_{v_p}(f(x))$ *possiede un segmento di larghezza* $n-2$ *da* $(0,0)$ *a* $(n-2,k)$ *ed un segmento di larghezza* $2$ *da* $(n-2,k)$ *a* $(n, e+k)$. *Essendo* $n$ *pari possiamo applicare il Teorema 3.2.5 per il quale* $f(x)$ *risulta irriducibile.*"

Nel terzo paragrafo proveremo ad affrontare il caso in cui il poligono di Newton ha due segmenti, uno di larghezza 3 ed uno di larghezza $n-3$. In questo caso si tratta di eliminare la possibilità di fattori cubici. Svilupperemo il caso nell'ambito dei polinomi a coefficienti interi usando le stesse tecniche di dimostrazione usate da Mott. Arriveremo così a risultati analoghi al caso precedente, che come quelli di Mott, non sono spinti verso la massima generalità, ma da un punto di vista pratico sono facili da applicare. Uno dei teoremi che dimostreremo in questo ambito è ad esempio il seguente:

" *Supponiamo* $n > 3$ *e* $f(x) \in \mathbb{Z}[x]$ *un polinomio che ridotto modulo* 3 *assume la forma:*

$$\overline{f(x)} = x^n + x^3 + 2 \ .$$

*Se* $n \equiv 6, 8, 10, 16 \ (mod\ 26)$, *allora* $f(x)$ *non possiede fattori cubici. Se inoltre* $N_v(f(x))$ *possiede un segmento di larghezza* 3 *ed uno di larghezza* $n-3$, *allora* $f(x)$ *è irriducibile in* $\mathbb{Q}[x]$."

Mettiamolo in pratica nel seguente esempio:

"*Consideriamo il seguente polinomio:*

$$f(x) = x^8 + 6x^7 + 12x^6 + 24x^4 - 2x^3 + 24x + 8 \in \mathbb{Z}[x] \ .$$

*Osserviamo innanzi tutto che*

$$f(x) \equiv x^8 + x^3 + 2 \ (mod\ 3)$$

*e che*

$$n \equiv 8 \ (mod\ 26) \ ,$$

*quindi per il teorema precedente* $f(x)$ *non possiede fattori cubici. Consideriamo ora la valutazione* $2-$*adica,* $v_2$*, e disegnamo il poligono di Newton* $N_{v_2}(f(x))$*. I punti del diagramma di Newton sono:*

$$\begin{array}{rcrcrcl} v_2(a_0) & = & v_2(1) & = & 0 & \Rightarrow & A(0,0) \\ v_2(a_1) & = & v_2(6) & = & 1 & \Rightarrow & B(1,1) \\ v_2(a_2) & = & v_2(12) & = & 2 & \Rightarrow & C(2,2) \\ v_2(a_4) & = & v_2(24) & = & 3 & \Rightarrow & D(4,3) \\ v_2(a_5) & = & v_2(-2) & = & 1 & \Rightarrow & E(5,1) \\ v_2(a_7) & = & v_2(24) & = & 3 & \Rightarrow & F(7,3) \\ v_2(a_8) & = & v_2(8) & = & 3 & \Rightarrow & G(8,3) \end{array}$$

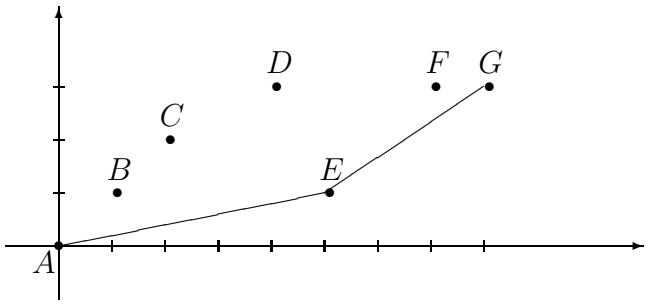


*Figura F*

*Dalla Figura F si vede subito che* $N_{v_2}(f(x))$ *ha due segmenti, uno di larghezza* $5$ *e uno di larghezza* $3$*, quindi per il teorema precedente* $f(x)$ *è irriducibile in* $\mathbb{Q}[x]$*.*"

# Bibliografia


[Ab] Abhyankar, S.S., *Algebraic Geometry for Scientists and Engineers*, Math. Survey No. 35, Amer. Math. Soc. Providence, RI, 1990.

[Ar] Artin, E., *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.

[Bo1] Bourbaki, N.,*Commutative Algebra*, Addison-Wesley, Reading MA, 1972.

[Bo2] Bourbaki, N., *General Topology*, Springer-Verlag, New York, 1989.

[Ch] Childs, L., *Algebra, Un'introduzione concreta*, ETS Editrice, Pisa, 1989.

[Do] Dorwort, H.L., Irreducibility of polynomials, *Amer. Math. Monthly* 42 (1935), 369-381.

[Du] Dumas, G., Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels, *J. Math. Pures Appl.* (6) vol. 2, (1906), 191-258.

[Fo1] Fontana, M. e Gabelli, S., *Insiemi, numeri e polinomi*, CISU, Roma, 1989.

[Fo2] Fontana, M., *Anelli ...*, Secondo ciclo di lezioni del corso di algebra, Dipartimento di Matematica, Istituto *Guido Castelnuovo*, Università di Roma *La Sapienza*, 1989.

[Ke] Kelly, J.B., On factorization of polynomials, *Amer. Math. Monthly* 60 (1953), 375-379.

[ML] MacLane, S, The Schönemann-Eisenstein irreducibility criteria in terms of prime ideals, *Trans. Amer. Math. Soc.* 43 (1938), 226-239.

[Mi] Mignotte, M., *Mathematics for Computer Algebra*, Springer-Verlag, New York, 1992.

[Mo] Mott, J.L., Eisenstein-Type Irreducibility Criteria. *Zero-dimensional commutative rings (Knoxville, TN, 1994)*, 307-329, Lecture Notes in Pure and Appl. Math., 171, *Dekker, New York*, 1995.

[Or] Ore, O., A note on factorization of polynomials, *Revista de Ciencias Lima* 41 (1939), 587-592.

[Pe] Perron, O., Über eine Anwendung der Idealtheorie auf die Frage nach der Irreduzibilität algebraischen Gleichengen, *Math. Ann.* 60 (1905), 448-458.

[Po] Pohst, M. and Zassenhaus, H., *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989.

[Re] Reiner, I., *Maximal Orders*, Academic Press, New York, 1975.

[Sw] Swan, R., Factorization of polynomials over finite fields, *Pacific J. Math.* 12 (1962), 1099-1106.

[VW1] Van der Waerden, B.L., *Modern Algebra*, vol. 1, Ungar, New York, 1953.

[VW2] Van der Waerden, B.L., *Modern Algebra*, vol. 2, Ungar, New York, 1953.

[We] Weiss, E., *Algebraic Number Theory*, McGraw-Hill, Nrw York, 1963.

La bibliografia si riferisce all'intera Tesi di Laurea.