Il discriminante, introdotto qui per polinomi quadratici e cubici, può essere definito per polinomi di grado qualunque (paragrafo 9.4). La sua proprietà distintiva è di essere nullo precisamente quando il polinomio ha una radice multipla.

5.9 Polinomi reali

Abbiamo già visto quali sono i polinomi irriducibili in $\mathbb{C}[X]$: per il teorema fondamentale dell'algebra sono solo i polinomi di grado 1. Sul campo reale la situazione non è molto più complicata.

(5.9.1) **Teorema.** Un polinomio reale di grado positivo si scompone come prodotto di fattori lineari e quadratici con discriminante negativo.

In particolare, esso è irriducibile se e solo se è lineare oppure quadratico con discriminante negativo.

Preliminarmente, definiamo il *coniugato* di un polinomio complesso $f \in \mathbb{C}[X]$ come il polinomio complesso che ha come coefficienti i coniugati dei coefficienti di f:

$$\bar{f}(X) = \bar{f}_0 + \bar{f}_1 X + \bar{f}_2 X^2 + \bar{f}_3 X^3 \dots .$$

Il polinomio f è reale se e solo se $\bar{f} = f$. Lascio come esercizio la verifica del fatto che, come per i numeri complessi, il coniugato di una somma è la somma dei conigati, e il coniugato di un prodotto è il prodotto dei coniugati, ossia $\overline{f+g} = \bar{f} + \bar{g}$ e $\overline{fg} = \bar{f}\bar{g}$. Da qui segue per induzione su r che se $f_1, \dots, f_r$ sono polinomi complessi allora $\overline{f_1+\dots+f_r} = \bar{f}_1+\dots+\bar{f}_r$ e $\overline{f_1 \cdots f_r} = \bar{f}_1 \cdots \bar{f}_r$.

Dimostrazione. Sia f un polinomio reale di grado positivo. Siano $u_1, \dots, u_s$ le radici reali di f, $\alpha_1, \dots, \alpha_t$ le radici non reali, $m_1, \dots, m_s$, $n_1, \dots, n_t$ le loro molteplicità. Scomponiamo f come

$$f(X) = c(X-u_1)^{m_1} \dots (X-u_s)^{m_s} (X-\alpha_1)^{n_1} \dots (X-\alpha_t)^{n_t}.$$

Coniugando si ottiene

$$\bar{f}(X) = c(X-\bar{u}_1)^{m1}\dots(X-\bar{u}_s)^{ms}(X-\bar{\alpha}_1)^{n1}\dots(X-\bar{\alpha}_t)^{nt} =$$
$$c(X-u_1)^{m1}\dots(X-u_s)^{ms}(X-\bar{\alpha}_1)^{n1}\dots(X-\bar{\alpha}_t)^{nt}.$$

Perciò se α_i è una radice non reale di f, allora il coniugato $\bar{\alpha}_i$ è pure una radice. Inoltre se $\bar{\alpha}_i = \alpha_j$ vediamo dall'uguaglianza sopra che $\bar{\alpha}_i$ ha molteplicità n_j come radice di f. Possiamo riassumere così.

(5.9.2) **Proposizione.** Se f è un polinomio reale e α una radice complessa di f, allora il coniugato $\bar{\alpha}$ è pure una radice di f, e la sua molteplicità è uguale alla molteplicità di α.

Quindi in particolare il numero di radici non reali di f è pari, ed esse si divideranno in $r = t/2$ coppie di numeri complessi coniugati. Riordiniamo gli α_i cosicché $\alpha_1, \dots, \alpha_r$ stiano in r coppie distinte. Allora le radici di f sono $\alpha_1, \dots, \alpha_r, \bar{\alpha}_1, \dots, \bar{\alpha}_r$, e

$$f(X) = c(X-u_1)^{m1}\dots(X-u_s)^{ms}(X-\alpha_1)^{n1}(X-\bar{\alpha}_1)^{n1}\dots(X-\alpha_t)^{nt}(X-\bar{\alpha}_t)^{nt}.$$

Ma per ciascun $i = 1, \dots, r$ si ha

$$g_i(X) \stackrel{\text{def}}{=} (X-\alpha_i)(X-\bar{\alpha}_i) = X^2-(\alpha_i+\bar{\alpha}_i)X+|\alpha_i|^2,$$

e $\alpha+\bar{\alpha}$, $|\alpha|^2$ sono entrambi reali. Perciò g_i è un polinomio reale quadratico, il cui discriminante sarà negativo, perché le sue radici non sono reali, e

$$f(X) = c(X-u_1)^{m1}\dots(X-u_s)^{ms}g_1(X)^{n1}\dots g_r(X)^{nr}.$$

Da notare che dalla dimostrazione del teorema 5.9.1 vediamo che i fattori lineari di un polinomio reale corrispondono alle sue radici reali, mentre i fattori quadratici corrispondono alle coppie di radici non reali coniugate.

(5.9.3) **Corollario.** Un polinomio reale di grado dispari ha almeno una radice reale.

Dimostrazione. Un polinomio di grado dispari non può essere prodotto di polinomi di grado 2, e quindi nella sua scomposizione in fattori irriducibili di ı interverrà almeno un polinomio lineare.

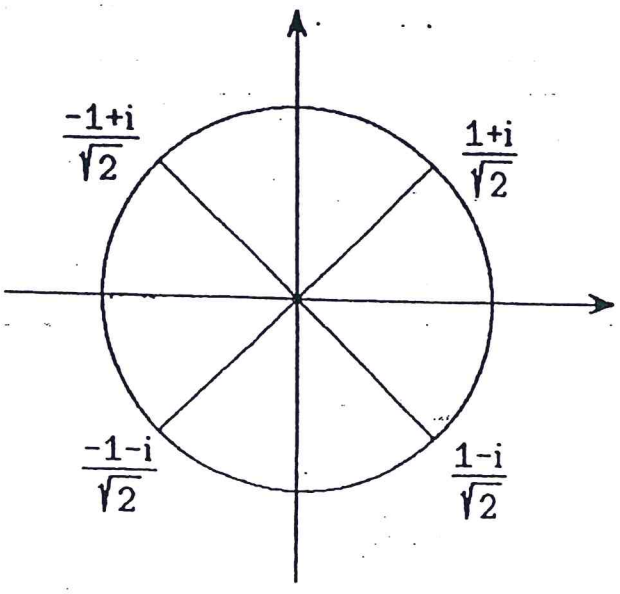
Questo corollario si dimostra facilmente per via analitica. Infatti se $f \in \mathbb{R}[X]$ è un polinomio di grado dispari, che potremo supporre monico, allora $\lim_{x\to+\infty} f(x) = +\infty$ e $\lim_{x\to-\infty} f(x) = -\infty$, e quindi f dovrà assumere sia valori negativi che positivi. Ma un ben il noto teorema studiato in analisi dice che se una funzione continua su un intervallo ammette sia valori positivi che negativi, allora si annulla in qualche punto.

Esistono dimostrazioni del teorema fondamentale dell'algebra basate solo su questo fatto, ma le tecniche di algebra richieste vanno oltre quelle trattate in queste note.

(5.9.4) **Esempio.** Consideriamo il polinomio reale X^4+1. Esso non ha radici reali, e quindi non avrà fattori reali lineari. Le radici complesse di X^4+1 sono le radici quarte di -1. Se z è una radice quarta di -1, allora $z^8 = 1$, per cui z è anche una radice ottava di 1. Inoltre se $z^8 = 1$, allora $(z^4)^2 = 1$, per cui $z^4 = 1$ oppure $z^4 = -1$. Per il teorema 2.6.6 ci saranno 8 radici ottave di 1, di cui quattro saranno radici quarte di 1. Le rimanenti quattro saranno le radici di X^4+1. Se poniamo

$$\omega = \cos(\pi/4) + i\sin(\pi/4) = \frac{1+i}{\sqrt{2}},$$

allora le radici ottave di uno sono $1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7$, mentre le radici quarte di 1 sono $1, \omega^2 = i, \omega^4 = -1, \omega^6 = -i$.



Le radici di X^4+1 sono perciò $\alpha = (1+i)/\sqrt{2}$, $\bar{\alpha} = (1-i)/\sqrt{2}$, $\beta = (-1+i)/\sqrt{2}$, $\bar{\beta} = (-1-i)/\sqrt{2}$. Ciascuna di queste sarà una radice semplice di X^4+1, perché altrimenti X^4+1 non potrebbe avere quattro radici distinte. Ricaviamo così una scomposizione

$$X^4+1 = (X-\alpha)(X-\bar{\alpha})(X-\beta)(X-\bar{\beta}) =$$
$$(X^2-(\alpha+\bar{\alpha})X+\alpha\bar{\alpha})(X^2-(\beta+\bar{\beta})X+\beta\bar{\beta}) = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).$$

5.10 Il numero di radici reali di un polinomio reale

Esistono vari metodi per stimare il numero radici reali di un polinomio reale in un dato intervallo. Noi ne tratteremo due, il primo più semplice da applicare, ma che dà solo un limite superiore sul numero di radici, il secondo più elaborato, che fornisce tuttavia il numero preciso di radici.

Sia $f \in \mathbb{R}[X]$ un polinomio reale non nullo, e siano a, b numeri reali con $a < b$. Desideriamo conoscere quante radici f abbia nell'intervallo chiuso

$$[a,b] = \{x \in \mathbb{R} \mid a \le x \le b\}.$$

Sia $a_0,a_1,a_2,\ldots$ una successione finita di numeri reali non tutti nulli. Eliminiamo dalla successione i numeri nulli, e sostituiamo ad ogni numero positivo il simbolo + e ad ogni numero negativo il simbolo −. Chiamiamo questa successione di simboli + e − la *successione dei segni* di $a_0,a_1,a_2,\ldots$. Il *numero di cambiamenti di segno* nella successione $a_0,a_1,a_2,\ldots$ sarà per definizione il numero di volte che nella successione dei segni di $a_0,a_1,a_2,\ldots$ si passa da un + ad un −, o viceversa.

Consideriamo la successione di numeri reali $f(a)$, $f'(a)$, $f''(a)$, ... , $f^{(n)}(a)$, dove $n = \deg(f)$. Questi numeri non possono essere tutti nulli, perché altrimenti f sarebbe nullo, per la formula di Taylor (5.5.8). Indichiamo con $Z_a(f)$ il numero di cambiamenti di segno di questa successione.

(5.10.1) **Teorema di Fourier[10]–Budan[11].** Siano a e b numeri re-

ali con $a<b$. Supponiamo che a e b non siano radici del polinomio reale non nullo f. Il numero di radici di f nell'intervallo [a,b] non è maggiore di $Z_a(f) - Z_b(f)$.

Se $a = 0$, allora $f^{(k)}(0) = k!f_k$, per la formula di Taylor (5.5.8), e quindi $Z_0(f)$ è il numero di cambiamenti di segno nella successione dei coefficienti di f.

Vediamo cosa succede per a molto grande. Come abbiamo visto nel paragrafo 5.5, il termine di grado d di $f^{(k)}$ è $(d+1)(d+2)\cdots(d+k)f_{d+k}X^d$. Questo significa che $f^{(k)}$ ha grado n-k, e il suo coefficiente direttore è $(n-k)(n-k+1)\cdots n\,f_n$, ossia uguale al prodotto di una costante positiva per il coefficiente direttore di f.

(5.10.2) **Lemma.** Dato un polinomio reale g di grado $d \geq 0$ con coefficiente direttore g_d, esiste un numero reale positivo M tale che g(x) e g_d hanno lo stesso segno per ogni $x > M$.

Dimostrazione. Questo segue dal teorema della permanenza del segno, perché

$$\lim_{x\to+\infty} \frac{g(x)}{x^d} = \lim_{x\to+\infty} \frac{g_0+g_1x+\cdots+g_dx^d}{x^d} =$$
$$\lim_{x\to+\infty} \left(g_0\frac{1}{x^d}+g_1\frac{1}{x^{d-1}}+\cdots+g_{d-1}\frac{1}{x}+g_d\right) = g_d.$$

Vediamo così che esiste un M tale che per tutti i $b > M$ $f^{(k)}(b)$ ha lo stesso segno di f_n, cosicché tutti i numeri f(b), f'(b), ... , $f^{(n)}(b)$ hanno stesso segno, e quindi $Z_b(f) = 0$. Deduciamo da questo, e dal teorema di Fourier-Budan, il fatto seguente.

(5.10.3) **Regola dei segni di Cartesio**[12]. Il numero di radici positive di un polinomio reale non è maggiore del numero di cambiamenti di segno nella successione dei suoi coefficienti.

---

[10] Charles Fourier (1768-1830), matematico francese.
[11] Ignoro chi sia Budan.
[12] René Descartes (1595-1650), italianizzato in Cartesio, matematico e filosofo francese.

Cominciamo ora la dimostrazione del teorema di Fourier-Budan. L'osservazione chiave è che se prendiamo la successione f(a), f'(a), f''(a), ... , $f^{(n)}(a)$, e gli togliamo il primo elemento, otteniamo la successione f'(a), f''(a), ... , $f^{(n)}(a)$, che è la successione analoga per il polinomio f', che ha grado deg(f)-1. Potremo dimostrare il teorema per induzione sul grado una volta che abbiamo trovato una relazione tra la radici del polinomio f e le radici della sua derivata f'. Una tale relazione è fornita dal risultato che segue.

(5.10.4) **Teorema di Rolle**[13]. Se u e v sono due radici reali di f con $u < v$, allora esiste un numero reale x, con $u < x < v$, tale che $f'(x) = 0$.

In altre parole: tra due radici di f si trova sempre una radice di f'.

Questo è un caso particolare del teorema di Rolle studiato in analisi, che dice che se una funzione continua dall'intervallo chiuso [u,v] ad $\mathbb{R}$ ha derivata all'interno di [u,v], e f(u) = f(v), allora esiste x con $u < x < v$ tale che $f'(x) = 0$. La dimostrazione consiste nell'osservare che f deve avere un punto di minimo oppure un punto di massimo all'interno di [a,b], e che in un tale punto la derivata deve essere nulla.

Dimostrazione di 5.10.1. Procederemo per induzione sul grado di f. Se deg(f) = 0, allora f è costante e non nulla, non ha radici, e $Z_a(f) = 0$ per ogni a. Il teorema è banalmente verificato.

Supponiamo che deg(f) > 0, e che il teorema valga per polinomi di grado deg(f)-1. Dal momento che f' ha grado deg(f)-1, il teorema varrà per f'. Siano $u_1,\dots,u_r$ le radici di f' contenute in [a,b], sistemate in ordine crescente (ovvero $a \le u_1 < u_2 < \cdots < u_r \le b$). Il teorema di Rolle ci dice questo: nell'intervallo chiuso $[u_i,u_{i+1}]$, con $i = 1,\dots,r-1$, non può esserci più di una radice di f. Infatti, se α e β fossero radici di f con $u_i \le \alpha < \beta \le u_{i+1}$, ci sarebbe una radice di f' tra α e β. Lo stesso ragionamento si applica agli intervalli $[a,u_1]$ e $[u_r,b]$, che pure non possono contenere più di una radice di f.

Abbiamo così r+1 intervalli chiusi $[a,u_1]$; $[u_1,u_2]$, ... , $[u_{r-1},u_r]$, $[u_r,b]$, la cui unione è tutto [a,b], e ciascuno dei quali contiene al più una radice di f. Ovviamente questo implica che f può avere al più

[13]Michel Rolle (1652-1719), matematico francese.

r+1 radici nell'intervallo [a,b].

La successione f'(a), f''(a), ... , $f^{(n)}(a)$ è ottenuta dalla successione f(a), f'(a), f''(a), ... , $f^{(n)}(a)$ togliendo il primo elemento, e perciò $Z_a(f) = Z_a(f')+1$, se f(a) ha lo stesso segno di $f^{(k)}(a)$, dove $f^{(k)}(a)$ è il primo degli f'(a), f''(a), ... ad essere diverso da 0, oppure $Z_a(f) = Z_a(f')$, in caso contrario. Analogamente $Z_b(f) = Z_b(f')$ oppure $Z_b(f) = Z_a(f')+1$. Perciò $Z_a(f)-Z_b(f) = Z_a(f')-Z_b(f')$ oppure $Z_a(f)-Z_b(f) = Z_a(f')-Z_b(f')+1$. Faremo vedere ora che se f ha r+1 radici in [a,b], allora $Z_b(f) = Z_b(f')$ e $Z_a(f) = Z_a(f')+1$, e quindi $Z_a(f)-Z_b(f) = Z_a(f')-Z_b(f')+1$. Dal momento che, per ipotesi induttiva, $r \le Z_a(f')-Z_b(f')$, questo implica che in ogni caso $r+1 \le Z_a(f)-Z_b(f)$, e quindi il numero di radici di f in [a,b] non sarà superiore a $Z_a(f)-Z_b(f)$, come si voleva.

Se f ha r+1 radici in [a,b], ciascuno degli r+1 intervalli chiusi $[a,u_1]$, $[u_1,u_2]$, ... , $[u_{r-1},u_r]$, $[u_r,b]$ dovrà contenerne una, e nessuna radice potrà stare in più di uno di questi intervalli. Perciò $f'(a) \neq 0$: in caso contrario $a = u_1$, e quindi la radice di f contenuta in $[a,u_1] = \{u_1\}$ dovrebbe essere uguale ad u_1, mentre $u_1 \in [u_1,u_2]$. Supponiamo per esempio che $f'(a) > 0$. Allora $f'(x) > 0$ per ogni x con $a \le x < u_1$, perché una funzione continua che non si annulla in un intervallo deve avere sempre lo stesso segno. Se ne deduce che f deve essere crescente sull'intervallo $[a,u_1]$. Dal momento che f ha una radice all'interno di $[a,u_1]$, vediamo che f(a) deve essere negativo. Analogamente si constata che se $f'(a) < 0$, allora $f(a) > 0$. In ogni caso vediamo che $Z_a(f) = Z_a(f')+1$.

Allo stesso modo, dovremo avere $f'(b) \neq 0$. Se $f'(b) > 0$ allora f sarà crescente nell'intervallo $[u_r,b]$, e quindi $f(b) > 0$, perché f ha una radice in $[u_r,b]$, e se $f'(b) < 0$ allora $f(b) < 0$. In ogni modo $Z_b(f) = Z_b(f')$, e questo conclude la dimostrazione del teorema.

Il *metodo di Sturm* [14], che verrà illustrato ora, permette di calcolare con precisione il numero di radici che un polinomio reale ha in un determinato intervallo dell'asse reale, invece di dare solo un limite superiore, come il metodo di Fourier-Budan; tuttavia i calcoli da effettuare sono assai più complessi.

Prendiamo un polinomio reale f non costante, e due numeri reali $a,b \in \mathbb{R}$, con $a < b$. Vogliamo calcolare il numero di radici di f nell'in-

[14] Jacques Charles François Sturm (1803-1855), matematico francese.

tervallo chiuso $[a,b] = \{x \in \mathbb{R} \mid a \le x \le b\}$. Se d è il massimo comun divisore di f e f', allora per la proposizione 5.5.7 il quoziente f/d avrà le stesse radici di f, ma tutte semplici. Assumeremo perciò che f abbia radici semplici.

(5.10.5) **Definizione.** Sia f un polinomio reale di grado positivo con radici semplici. Una *successione di Sturm* per il polinomio f nell'intervallo [a,b] è una successione $f_0, f_1, \ldots, f_r$ di polinomi reali con le proprietà seguenti.

(a) $f_0 = f$, $f_1 = f'$.

(b) f_r non si annulla in nessun punto dell'intervallo [a,b].

(c) Per ciascun $i = 1, \ldots, r-1$ si ha $f_{i-1} = q_i f_i - f_{i+1}$ per un certo polinomio reale q_i.

Una successione di Sturm esiste sempre, e può essere calcolata facilmente mediante una versione leggermente modificata dell'algoritmo euclideo. Poniamo $f_0 = f$, $f_1 = f'$. Sia f_2 l'opposto del resto della divisione di f_0 per f_1, f_3 l'opposto del resto della divisione di f_1 per f_2, se f_2 è diverso da 0, f_4 l'opposto del resto della divisione di f_2 per f_3, se f_3 è diverso da 0, eccetera. In generale f_i sarà l'opposto del resto della divisione di f_{i-2} per f_{i-1}. Ci fermeremo quando otterremo un polinomio che non si annulla mai nell'intervallo [a,b]. Il grado di f_i si abbassa ogni volta, perciò prima o poi dovremo raggiungere 0 come resto. Esattamente come nel caso dell'algoritmo euclideo, si vede che se m è l'intero più grande per cui $f_m \neq 0$, allora f_m è un massimo comun divisore di f e di f'. Per la proposizione 5.5.5, f ed f' sono relativamente primi, per cui f_m deve essere una costante non nulla, ed in particolare f_m non si annulla in nessun intervallo. Naturalmente per ottenere una successione di Sturm può non essere necessario continuare ad effettuare divisioni fino ad ottenere una costante: per esempio, se un certo f_r risultasse uguale a X^2+1, potremmo essere sicuri che questo f_r non si annullerà su nessun intervallo, e quindi ci fermeremmo.

Sia f un polinomio reale di grado positivo con radici semplici, e siano a e b numeri reali con $a < b$. Supponiamo che né a né b siano radici di f. Sia $f_0, f_1, \ldots, f_r$ una successione di Sturm per f, e per ciascun numero reale x chiamiamo $W_x(f)$ il numero di cambiamenti di

segno della successione $f_0(x)$, $f_1(x)$, ... , $f_r(x)$ (questo numero $W_x(f)$ dipenderà in generale dalla successione di Sturm che abbiamo scelto).

(5.10.6) **Teorema di Sturm.** Sia f un polinomio reale di grado positivo con radici semplici., e siano a e b due numeri reali, con $a<b$, $f(a) \neq 0$, $f(b) \neq 0$. Allora il numero di radici reali di f nell'intervallo [a,b] è uguale a $W_a(f)-W_b(f)$.

Dimostrazione. Siano x_1, Osserviamo che se $]x,y[$ è un intervallo aperto, e nessuno dei polinomi f_i ha uno zero in $]x,y[$, allora $f_i(t)$ ha lo stesso segno per ogni $t \in]x,y[$, e quindi $W_t(f)$ è costante su $]x,y[$. Supponiamo ora che $x \in]a,b[$ sia una radice di qualche polinomio f_i. Siano y ed y' numeri reali sufficientemente vicini ad x, con $y<x<y'$. Per concludere la dimostrazione basta far vedere che se x non è una radice di f, allora $W_y(f) = W_{y'}(f)$, mentre se x è una radice di f allora $W_y(f) = W_{y'}(f)+1$.

Notiamo prima di tutto che due funzioni successive della successione $f_0,f_1,\ldots,f_r$ non possono annullarsi nello stesso punto di [a,b]. Se fosse infatti $f_{i-1}(x) = f_i(x) = 0$, con $x \in [a,b]$, avremmo anche $f_{i+1}(x) = q_i(x)f_i(x)-f_{i-1}(x) = 0$, $f_{i+2}(x) = q_{i+1}(x)f_{i+1}(x)-f_i(x) = 0$, e così via, fino a concludere che $f_r(x) = 0$, in contraddizione con la condizione (c) della definizione 5.10.5.

Prendiamo ora un punto $x \in [a,b]$ tale che $f_i(x) = 0$ per qualche $i \geq 0$. Se $i>0$, allora $f_{i-1}(x) = q_i(x)f_i(x)-f_{i+1}(x) = -f_{i+1}(x)$, e quindi $f_{i-1}(x)$ e $f_{i+1}(x)$ avranno segno opposto. Se y è sufficientemente vicino ad x, allora $f_{i-1}(y)$ e $f_{i+1}(y)$ avranno lo stesso segno di $f_{i-1}(x)$ e di $f_{i+1}(x)$, rispettivamente, dimodoché nella successione $f_{i-1}(y)$, $f_i(y)$, $f_{i+1}(y)$ ci sarà un solo cambiamento di segno, qualunque sia il segno di $f_i(y)$. Supponiamo ora che $i = 0$, ossia che x sia una radice di f. Allora $f'(x) \neq 0$, perché per ipotesi x non può essere una radice doppia di f. Se $f'(x)>0$ allora f è crescente in un intorno di x; quindi se prendiamo y sufficientemente vicino ad x, avremo $f(y)<0$ se $y<x$, e $f(y)>0$ se $y>x$. Se $f'(x)<0$ succederà il contrario: in ogni caso, la successione $f(y)$, $f'(y)$ avrà un cambiamento di segno quando $y<x$ e nessun cambiamento se $y>x$. Questo implica la tesi.

Il lemma 5.10.2 dice che se M è un reale positivo abbastanza

grande allora $W_M(f)$ è uguale al numero di cambiamenti di segno nella successione dei coefficienti direttori degli elementi di una successione di Sturm di f. Indicheremo questo numero con $W_{+\infty}(f)$. Analogamente, se g è un polinomio reale non nullo il segno di $g(-M)$ è uguale al segno del coefficiente direttore di g se g ha grado pari, e al suo opposto se g ha grado dispari. Perciò $W_{-M}(f)$ è il numero di cambiamenti di segno nella successione di numeri reali ottenuta da una successione di Sturm prendendo il coefficiente direttore di ogni polinomio di grado pari, e l'opposto del coefficiente direttore per ogni polinomio di grado dispari. L'intero $W_{-M}(f)$ verrà indicato con $W_{-\infty}(f)$.

(5.10.7) **Corollario.** Il numero di radici reali di un polinomio reale f con radici semplici è $W_{-\infty}(f)-W_{+\infty}(f)$.

Come esempio, consideriamo il polinomio $f(X) = X^n+pX+q$, dove n è un intero con $n \geq 3$, p e q sono reali, $p \neq 0$. Si ha $f'(X) = nX^{n-1}+p$, e

$$X^n+pX+q = \frac{1}{n}X(nX^{n-1}+p)-(\frac{n-1}{n}pX-q).$$

La radice di $\frac{n-1}{n}pX-q$ è $\alpha = nq/(1-n)p$, per cui il resto della divisione di $f'(X)$ per $\frac{n-1}{n}pX-q$ è

$$f'(\alpha) = n(nq/(1-n)p)^{n-1}+p = \frac{(1-n)^{n-1}p^n+n^nq^{n-1}}{(1-n)^{n-1}p^{n-1}}.$$

Poniamo $\delta = (1-n)^{n-1}p^n+n^nq^{n-1}$. Se $\delta = 0$ allora f ed f' non sono relativamente primi, e f avrà perciò una radice multipla. Supporremo quindi $\delta \neq 0$. Come successione di Sturm prenderemo

$$f_0(X) = X^n+pX+q,$$

$$f_1(X) = nX^{n-1}+p,$$

$$f_2(X) = \frac{n-1}{n}pX-q,$$

$$f_3(X) = -\frac{(1-n)^{n-1}p^n+n^nq^{n-1}}{(1-n)^{n-1}p^{n-1}}.$$

Dal corollario 5.10.7 è facile allora dedurre quante radici reali abbia f. Per esempio, assumiamo che n sia dispari e che p sia negativo. Il numero di radici reali di f dipende dal segno di $\delta = (1-n)^{n-1}p^n+n^nq^{n-1}$:

se $\delta > 0$ allora $W_{-\infty}(f) = 2$ e $W_{+\infty}(f) = 1$, per cui f avrà una sola radice reale, mentre se $\delta < 0$ allora $W_{-\infty}(f) = 3$ e $W_{+\infty}(f) = 0$, e perciò f avrà tre radici reali.

5.11 Polinomi razionali

I polinomi irriducibili razionali sono enormemente più difficili da studiare dei polinomi irriducibili reali o complessi. In verità non è assolutamente possibile classificare i polinomi irriducibili in $\mathbf{Q}[X]$ come si fa in $\mathbf{R}[X]$ e $\mathbf{C}[X]$. In questa sezione ci limiteremo a dimostrare qualche risultato importante, scalfendo appena la superficie di questa vasta teoria.

Cominciamo col dare un metodo per calcolare tutte le radici razionali di un polinomio razionale.

(5.11.1) **Proposizione.** Sia f un polinomio intero non nullo, e sia $a \in \mathbf{Q}$ una radice di f. Se $a = r/s$ con r ed s interi relativamente primi, allora r divide il coefficiente costante di f, e s divide il coefficiente direttore.

Dimostrazione. Poniamo $f(X) = f_0+f_1X+\dots+f_mX^m$ con $f_m \neq 0$. Allora $0 = f(a) = f_0+f_1(r/s)+f_2(r/s)^2+\dots+f_m(r/s)^m$, e perciò, moltiplicando per s^m,

$$f_0s^m + f_1rs^{m-1} + f_2r^2s^{m-2} + \dots + f_mr^m = 0.$$

Siccome r divide $f_1rs^{m-1}+f_2r^2s^{m-2}+\dots+f_mr^m$ avremo che r dividerà anche f_0s^m. Siccome r è relativamente primo ad s si avrà $r|f_0$, come si voleva (corollario 1.4.5).

Per vedere che $s|f_m$ si ragiona in maniera analoga.

(5.11.2) **Corollario.** Una radice razionale di un polinomio monico intero è intera.

Osserviamo che il corollario 5.11.2 applicato al polinomio X^n-d di-

mostra il lemma 2.3.8.

Dimostrazione. Il denominatore s di una radice razionale di un polinomio monico intero f divide il coefficiente direttore di f, che è 1, per la proposizione 5.11.1, e quindi $s = \pm 1$.

Supponiamo di voler trovare tutte le radici di un polinomio razionale non nullo f di grado m. Moltiplicando per il minimo comun divisore dei denominatori di $f_0,\dots,f_m$ potremo supporre che f sia un polinomio intero.

Assumiamo innanzitutto che $f_0 \neq 0$. Allora se r/s è una radice razionale di f, con r ed s interi relativamente primi, r dividerà f_0, mentre s dividerà f_m. Siccome sia f_0 che f_m sono interi non nulli, avranno un numero finito di divisori, e quindi ci saranno solo un numero finito di possibilità per r ed s. Possiamo anche assumere $s>0$.

Se invece $f_0 = 0$, chiamiamo i il minimo intero positivo tale che $f_i \neq 0$. Potremo allora scrivere

$$f(X) = f_iX^i+\dots+f_mX^m = X^i(f_i+\dots+f_mX^{m-i}).$$

Le radici di f sono 0, più le radici di $f_i+\dots+f_mX^{m-i}$, che si potranno trovare col procedimento appena descritto.

Svilupperemo ora una teoria che può essere considerata un generalizzazione della proposizione 5.11.1 a fattori irriducibili non lineari. Per esempio, il corollario 5.11.2 dice che se un polinomio intero monico è divisibile per un polinomio della forma X-a, con $a \in \mathbb{Q}$, allora a è intero. Ebbene, faremo vedere che se un polinomio monico razionale f di grado arbitrario divide un polinomio intero monico allora f è intero.

(5.11.3) **Definizione.** Un polinomio razionale si dice *primitivo* se è intero e non nullo, e se il massimo comun divisore dei suoi coefficienti è 1.

Per esempio un polinomio intero monico è primitivo.

(5.11.4) **Proposizione.** Ogni polinomio razionale non nullo è associato in $\mathbb{Q}[X]$ ad un polinomio primitivo.

Dimostrazione. Sia $f \in \mathbb{Q}[X]$ un polinomio non nullo di grado m, e siano $f_0,\dots,f_m$ i suoi coefficienti. Moltiplicando per il minimo comun divisore dei denominatori di $f_0,\dots,f_m$ potremo supporre che f sia un polinomio intero. Se chiamiamo d il massimo comun divisore di $f_0,\dots,f_m$ abbiamo che $f_0/d,\dots,f_m/d$ sono relativamente primi: infatti se un intero positivo e divide $f_0/d,\dots,f_m/d$ abbiamo che de divide $f_0,\dots,f_m$, e quindi $de \le d$. Questo implica $e = 1$. Perciò il polinomio f/d, che è associato ad f, è primitivo.

(5.11.5) **Lemma.** Il prodotto di due polinomi primitivi è primitivo.

Dimostrazione. Siano f e g due polinomi primitivi, e supponiamo che il loro prodotto fg non sia primitivo. Esisterà perciò un primo p che divide tutti i coefficienti di fg. Sia m il più grande numero naturale tale che p non divide f_m, n il più grande numero naturale tale che p non divide g_n. Consideriamo

$$(fg)_{m+n} = \sum_{i+j=m+n} f_i g_j.$$

Se $i+j = m+n$ e $i>m$ allora f_i è divisibile per p, e quindi $p \mid f_i g_j$, mentre se $i<m$ allora $j>n$, e g_j è divisibile per p, quindi di nuovo $p \mid f_i g_j$. Allora $(fg)_{m+n}$ è la somma di $f_m g_n$, che non è divisibile per p, e di altri termini che sono divisibili per p. Ne segue che $(fg)_{m+n}$ non è divisibile per p, che è una contraddizione.

(5.11.6) **Teorema.** Se f è un polinomio primitivo e g è un polinomio razionale tale che fg è intero, allora g è intero.

Dimostrazione. Possiamo ovviamente assumere che $g \neq 0$. Sia g' un polinomio primitivo associato a g, che esiste per il lemma 5.11.4., e poniamo $g = (r/s)h$, ossia $sg = rg'$, con r ed s interi relativamente primi, $s>0$. Allora $sfg = rfg'$. Dal momento che fg è intero abbiamo che s divide tutti i coefficienti di rfg', e, dal momento che s è relativamente primo ad r, s dividerà tutti i coefficienti di fg'. Ma fg' è primitivo, per il lemma 5.11.5, e quindi $s = 1$. Ne segue che $g = rg'$ è un polinomio intero.

Questo teorema può essere usato per dimostrare la proposizione 5.11.1. Infatti avremo che se r/s è una radice di un polinomio razionale f, con r ed s interi relativamente primi, allora sX-r = s(X-(r/s)) divide f(X) in $\mathbb{Q}[X]$, e sX-r è un polinomio primitivo. Ricaviamo dal teorema che f(X) = (sX-r)g(X), dove g è un polinomio intero di grado m-1. Perciò $f_0 = -rg_0$ e $f_m = sg_{m-1}$, e quindi $r|f_0$ e $s|f_m$.

Ricaviamo anche da questo che se d è un intero e r/s è una radice di un polinomio intero f, con r ed s interi relativamente primi, allora sd-r divide f(d). Questo fornisce un ulteriore criterio per decidere per se un dato numero razionale r/s può essere una radice.

(5.11.7) **Corollario.** Se un polinomio monico razionale f divide un polinomio monico intero allora f è intero.

Dimostrazione. Sia f' un polinomio primitivo associato ad f, e sia g un polinomio monico intero tale che f|g. Allora f'|g, ed esiste $q \in \mathbb{Q}[X]$ tale che f'q = g. Per il teorema 5.11.6 q è intero, e in particolare avrà il coefficiente direttore intero. Siccome il coefficiente direttore di g, che è 1, è il prodotto del coefficiente direttore di f' e di quello di q, il coefficiente direttore di f' deve essere ±1. Ne segue che f' oppure -f' è monico: per la proposizione 5.3.3 dovremo avere f = f' oppure f = -f'. In ogni caso f è intero.

(5.11.8) **Lemma di Gauss**[15]. Un polinomio intero di grado possitivo è irriducibile in $\mathbb{Q}[X]$ se e solo se è il prodotto di due polinomi interi di grado positivo.

Un polinomio intero monico di grado positivo è irriducibile se e solo se è il prodotto di due polinomi interi monici di grado positivo.

Dimostrazione. Ovviamente se un polinomio è il prodotto di due polinomi interi di grado positivo allora non è irriducibile. Supponiamo che $f \in \mathbb{Z}[X]$ non sia irriducibile come polinomio razionale, e sia g un polinomio di grado maggiore di 0 e minore di deg(f) che divide f. Possiamo assume che g sia primitivo, per la proposizione 5.11.4. Allora f = gh con $h \in \mathbb{Q}[X]$, e per il teorema 5.11.6 il polinomio h è pure

[15] Carl Friedrich Gauss (1777-1855), sommo matematico tedesco. Lo stesso degli interi gaussiani.

intero. Se f è monico, e chiamiamo a e b i coefficienti direttori di g ed h rispettivamente, allora ab = 1, e quindi a = b = 1 oppure a = b = -1. Nel primo caso g ed h sono monici, nel secondo -g e -h lo sono, e f = (-g)(-h).

Dimostriamo ora un criterio di irriducibilità che permette di dare moltissimi esempi di polinomi razionali irriducibili.

(5.11.9) **Criterio di irriducibilità di Eisenstein**[16]. Sia

$$f(X) = f_0 + f_1X + \cdots + f_mX^m$$

un polinomio intero di grado $m > 0$. Supponiamo che esista un primo p che non divide f_m, che divide $f_0,\ldots,f_{m-1}$, e tale che p^2 non divida f_0. Allora f è irriducibile in $\mathbf{Q}[X]$.

(5.11.10) **Corollario.** Se n è un intero positivo, esiste un polinomio razionale irriducibile di grado n.

Dimostrazione. Se p è un primo il polinomio X^n+p è irriducibile, per il criterio di Eisenstein.

Dimostrazione di 5.11.9. Supponiamo per assurdo che f non sia irriducibile. Per il lemma di Gauss esisteranno g ed h in $\mathbf{Z}[X]$ di grado positivo tale che f = gh. Avremo allora $f_0 = g_0h_0$, e quindi p dividerà g_0 oppure h_0, ma non entrambi, poiché f_0 non è divisibile per p^2. Diciamo per esempio che p divide g_0 ma non h_0. Facciamo vedere per induzione su k che p divide g_k per ogni $k < m$. Se assumiamo che p divida g_i per ogni $i < k$, si avrà

$$f_k = g_kh_0 + g_{k-1}h_1 + \cdots + g_1h_{k-1} + g_0h_k$$

e quindi $p \mid g_kh_0$, poiché p divide f_k. Siccome p non divide h_0 concludiamo che p divide g_k, come volevamo. Ma questa è una contraddizione: dal momento che il grado di g è minore di m vediamo che il coefficiente direttore di g è divisibile per p, e quindi anche il coefficiente direttore di f dovrebbe essere divisibile per p, il che è falso.

Talora il criterio di Eisenstein può essere applicato in maniera in-

[16]Ferdinand Gotthold Max Eisenstein (1823-1852), matematico tedesco.

diretta. Prendiamo un polinomio $f \in \mathbb{Z}[X]$, e un intero a. Consideriamo il polinomio

$$g(X) = f(X+a) = f_0 + f_1(X+a) + f_2(X+a)^2 + \cdots$$

che è pure in $\mathbb{Z}[X]$, ed ha lo stesso grado di f(X). Ovviamente $f(X) = g(X-a)$, e se f_1 e $f_2 \in \mathbb{Z}[X]$ si ha $(f_1 f_2)(X+a) = f_1(X+a)f_2(X+a)$. Perciò il polinomio f è irriducibile se e solo se f(X+a) è irriducibile. Può capitare che il criterio di Eisenstein non si applichi ad f(X), ma si applichi ad f(X+a). Diamo un esempio importante.

(5.11.11) **Proposizione**. Sia p un primo. Il polinomio

$$X^{p-1}+X^{p-2}+ \cdots +X^2+X+1$$

è irriducibile in $\mathbb{Q}[X]$.

Dimostrazione. Poniamo $f(X) = X^{p-1}+X^{p-2}+ \cdots +X^2+X+1$. Per la proposizione 2.1.5 abbiamo $(X-1)f(X) = X^p-1$. Sostituendo X con X+1 e applicando il teorema del binomio (2.1.4) otteniamo

$$Xf(X+1) = (X+1)^p - 1 = \left(X^p + \binom{p}{1}X^{p-1} + \binom{p}{2}X^{p-2} + \cdots + \binom{p}{p-1}X + 1\right) - 1 =$$

$$X\left(X^{p-1} + \binom{p}{1}X^{p-2} + \binom{p}{2}X^{p-3} + \cdots + \binom{p}{p-1}\right)$$

e quindi, semplificando,

$$f(X+1) = X^{p-1} + \binom{p}{1}X^{p-2} + \binom{p}{2}X^{p-3} + \cdots + \binom{p}{p-1}.$$

Per il lemma 1.7.7 sappiamo che $\binom{p}{k}$ è divisibile per p per ogni $k = 1,\cdots,p-1$, mentre p^2 non divide $\binom{p}{p-1} = p$. Possiamo perciò concludere dal criterio di Eisenstein che f(X+1) è irriducibile, e quindi che f(X) è irriducibile.

Poniamo $\omega = \cos(2\pi/p) + i\sin(2\pi/p)$, e ricordiamo (teorema 2.6.6) che le radici p-esime dell'unità in $\mathbb{C}$ sono $1, \omega, \omega^2, \ldots, \omega^{p-1}$. Osserviamo che dalla scomposizione

$$(X-1)(X^{p-1}+X^{p-2}+\cdots+X^2+X+1) = X^p-1$$

segue che tutte le radici p-esime di 1 in $\mathbb{C}$ sono radici del polinomio $X^{p-1}+X^{p-2}+ \cdots +X^2+X+1$, eccetto 1. Perciò questo ha p-1 radici distin-

te in $\mathbb{C}$, che sono $\omega, \omega^2, \ldots, \omega^{p-1}$.

Un altro metodo per mostrare l'irriducibilità di un polinomio intero è la riduzione modulo un primo, che verrà discussa nel prossimo paragrafo.

5.12 Polinomi irriducibili su campi finiti

Sia K un campo finito. Per ogni intero positivo n esiste un polinomio irriducibile di grado n su K, (vedi corollario 5.14.3, teorema 7.6.6). In questo paragrafo ci limiteremo a dare qualche esempio di polinomio irriducibile su campi finiti, e a contare il numero di polinomi irriducibili di grado 2 e 3 su un campo finito qualsiasi. Nel paragrafo 5.14 utilizzeremo una tecnica più sofisticata per dare una formula per il numero di polinomi irriducibili di grado n su un campo finito qualunque.

(5.12.1) **Proposizione.** Sia K un campo finito.

(a) Se la caratteristica di K è diversa da 2 allora esiste un elemento $c \in K$ tale che il polinomio X^2-c è irriducibile.

(b) Se la caratteristica di K è 2 allora esiste un elemento $c \in K$ tale che il polinomio X^2+X+c è irriducibile.

Dimostrazione. Abbiamo visto (proposizione 2.4.3) che se la caratteristica di K non è 2 allora K contiene un elemento c che non è un quadrato in K. Questo è equivalente a dire che X^2-c non ha radici, ossia che è irriducibile (proposizione 5.8.1).

Assumiamo che la caratteristica di K sia 2. Allora vogliamo far vedere che esiste un $c \in K$ tale che X^2+X+c non ha radici, ossia tale che $c \neq a^2+a$ per ogni $a \in K$. Per fare questo imitiamo la dimostrazione della proposizione 2.4.3: consideriamo la funzione $f: K \longrightarrow K$ definita da $f(a) = a^2+a$, e mostriamo che non è suriettiva. Per far ciò osserviamo che per ogni $a,b \in K$ si ha

$$(a+b)^2 = a^2+2ab+b^2 = a^2+b^2,$$

e quindi