$$((X+k)^{p+1}-(X+k-1)^{p+1})_{\mathbf{B}} =$$

$$(p+1)k^p+\binom{p+1}{2}k^{p-1}(X^2-(X-1)^2)_{\mathbf{B}}+\binom{p+1}{3}k^{p-2}(X^3-(X-1)^3)_{\mathbf{B}}+\cdots+$$
$$\binom{p+1}{p}k(X^p-(X-1)^p)_{\mathbf{B}}+(X^{p+1}-(X-1)^{p+1})_{\mathbf{B}} = (p+1)k^p.$$

Sommando membro a membro questa uguaglianza per $k = 1,\ldots,n$ si ottiene

$$((X+n)^{p+1}-X^{p+1})_{\mathbf{B}} = (p+1)S_p(n);$$

da cui la tesi.

Nel resto di questo capitolo tratteremo gli anelli di polinomi a coefficienti in un campo. Questi sono tra gli anelli fondamentali dell'algebra.

5.3 Polinomi a coefficienti in un campo

Sia K un campo. Vogliamo studiare l'anello K[X]. Segue dalla proposizione 5.1.6 che le unità in K[X] sono le costanti non nulle, ossia i polinomi di grado 0. Inoltre i polinomi non nulli che non sono invertibili sono quelli di grado positivo: perciò un polinomio è riducibile se e solo se è costante, oppure può essere scomposto come prodotto di due polinomi di grado positivo.

Osserviamo anche che i polinomi di grado 1 sono irriducibili: se $f \in K[X]$ ha grado 1, e $f = gh$, allora $\deg(g)+\deg(h) = \deg(f) = 1$, e quindi o g o h deve avere grado 0.

Un fatto importantissimo è che K[X] è un anello euclideo: questo segue dal seguente lemma di divisione, che gioca nell'aritmetica dei polinomi lo stesso ruolo fondamentale che il lemma di divisione per gli interi ha nell'aritmetica degli interi.

(5.3.1) **Lemma di divisione per i polinomi.** Siano f e g due polinomi in K[X], con $f \neq 0$. Esistono due polinomi q ed r, con $\deg(r) <$

deg(f), tali che g = qf+r. Inoltre q ed r sono univocamente determinati da f e da g.

Ovviamente f divide g in K[X] se e solo se r = 0.

Dimostrazione. Dimostriamo prima l'unicità di q ed r. Supponiamo che g = qf+r = q'f+r', con deg(r) < deg(f) e deg(r') < deg(f). In questo caso r-r' = (q'-q)f, e quindi deg(r-r') = deg(q'-q)+deg(f) per la proposizione 5.1.5. Se q ≠ q' si avrebbe deg(q'-q) ≥ 0, e quindi deg(r-r') = deg(q'-q)+deg(f) ≥ deg(f), il che contraddice la disuguaglianza deg(r-r') ≤ max(deg(r),deg(r')) (proposizione 5.1.5).

Per dimostrare l'esistenza procediamo per induzione su deg(g). Se g = 0 allora possiamo prendere q = r = 0. Se deg(g) = 0 distinguiamo due casi. Nel caso che deg(f) = 0, f è una costante non nulla, e quindi invertibile, per la proposizione 5.1.6: poniamo allora r = 0, $q = gf^{-1}$. Se deg(f) > 0 allora si può porre q = 0, r = g.

Supponiamo ora che il lemma valga quando deg(g) < d, e assumiamo deg(g) = d. Poniamo d' = deg(f). Se d' > d prendiamo q = 0, r = g. Se d' ≤ d, chiamiamo c il quoziente tra il coefficiente direttore di g e il coefficiente direttore di f. Allora il polinomio $cX^{d-d'}f(X)$ avrà grado d e coefficiente direttore uguale al coefficiente direttore di g. Ne segue che il polinomio

$$g'(X) = g(X) - cX^{d-d'}f(X)$$

ha grado minore di d, e perciò per ipotesi induttiva esistono q' ed r in K[X] con g' = q'f+r e deg(r) < deg(f). Allora

$$g(X) = g'(X) + cX^{d-d'}f(X) = (q'(X)+cX^{d-d'})f(X) + r(X)$$

e la dimostrazione è conclusa.

Un po' di riflessione dovrebbe convincere lo studente che l'algoritmo solito per dividere un polinomio per un altro non è che una formalizzazione della dimostrazione data qui sopra.

(5.3.2) **Corollario.** L'anello K[X] è un anello euclideo.

Dimostrazione. Come funzione $\delta: K[X]\setminus\{0\} \longrightarrow \mathbb{N}$ prendiamo il grado. La condizione (a) della definizione 4.2.1 segue subito dal lemma di di-

visione, mentre la condizione (b) viene dalla formula per il grado di un prodotto (proposizione 5.1.5).

Possiamo quindi applicare tutti i teoremi che abbiamo dimostrato per gli anelli euclidei. Un vantaggio che K[X] ha rispetto a un anello euclideo qualsiasi è che, come nel caso di $\mathbb{Z}$, ogni elemento diverso da 0 è associato ad un unico elemento canonico: un intero positivo nel caso di $\mathbb{Z}$, un polinomio monico nel caso di K[X].

(5.3.3) **Proposizione**. Ogni polinomio non nullo in K[X] è associato ad un unico polinomio monico. In particolare due polinomi monici sono associati se e solo se sono uguali.

Dimostrazione. Due polinomi f e g sono associati se e solo se esiste $a \in K^*$ tale che $g = af$ (proposizione 5.1.6). Sia $f \in K[X]$, e sia c il coefficiente direttore di f. Il coefficiente direttore di af è uguale ad ac; se quindi prendiamo $a = c^{-1}$ vediamo che af è un polinomio monico. Se poi $af = g$ con $a \in K^*$, e f,g sono entrambi monici, dovremo avere $a = 1$, e perciò $f = g$.

Il teorema di scomposizione in fattori irriducibili nell'anello K[X] ha quindi una forma particolare.

(5.3.4) **Teorema**. Sia $f \in K[X]$ un polinomio di grado positivo, e sia $c \in K^*$ il coefficiente direttore di f. Allora esistono dei polinomi monici irriducibili distinti $p_1,\dots,p_r \in K[X]$ e degli interi positivi $m_1,\dots,m_r$ tali che $f = cp_1^{m_1}\dots p_r^{m_r}$. Inoltre se esistono altri polinomi monici irriducibili distinti $q_1,\dots,q_s$ e interi positivi $n_1,\dots,n_s$ tale che $f = cq_1^{n_1}\dots q_s^{n_s}$, allora $r = s$, e si possono permutare i $q_1^{n_1},\dots,q_s^{n_s}$ in maniera tale che $p_1 = q_1, \dots, p_r = q_r$, e $m_1 = n_1, \dots, m_r = n_r$.

Dimostrazione. Segue dal teorema 4.3.3 che f è associato ad un prodotto del tipo $p_1^{m1}\dots p_r^{mr}$, dove $p_1,\dots,p_r$ sono irriducibili. Sostituendo ciascun $p_1,\dots,p_r$ con il polinomio monico a cui è associato potremo assumere che i $p_1,\dots,p_r$ siano tutti monici. Esiste quindi un polinomio invertibile, ossia una costante non nulla a, tale che $f = ap_1^{m1}\dots p_r^{mr}$. Dal momento che $p_1^{m1}\dots p_r^{mr}$ è monico, perché il prodotto di polinomi monici è monico, la costante a dovrà essere il coefficiente direttore di f.

Infine se $f = cq_1^{n1},\dots,q_s^{ns}$ otteniamo dal teorema 4.3.3 che r = s, e dopo aver permutato i $q_1,\dots,q_r$ avremo che p_i è associato a q_i. Allora $p_i = q_i$ per la proposizione 5.3.3, e $m_1 = n_1, \dots, m_r = n_r$.

Come conseguenza si ha che un polinomio monico riducibile si scompone come prodotto di due polinomi monici di grado positivo.

Indaghiamo su cosa succede dividendo un polinomio f per un polinomio monico lineare. Sia $f \in K[X]$ un qualsiasi polinomio, e sia X-a, $a \in K$, un polinomio monico lineare. Possiamo scrivere $f(X) = q(X)(X-a)+r(X)$, dove r è un polinomio di grado minore di 1, ossia un polinomio costante. Sostituendo X con a otteniamo che f(a) = r. Ovviamente X-a divide f se e solo se r = 0. Abbiamo così dimostrato il fatto fondamentale che segue.

(5.3.5) **Teorema.** Il polinomio X-a divide f se e solo se f(a) = 0.

(5.3.6) **Definizione.** Un elemento $a \in K$ è detto una *radice,* o uno *zero,* di un polinomio $f \in K[X]$ se f(a) = 0.

Per il teorema 5.3.5, una definizione equivalente è che $a \in K$ è una radice di f se X-a divide f.

5.4 Radici di un polinomio

Sia K ancora un campo.

(5.4.1) **Definizione.** Sia f un polinomio non nullo a coefficienti in K, a un elemento di K. La *molteplicità* di a come radice di f, in simboli $\mu(f,a)$, è il massimo intero non negativo m tale che $(X-a)^m | f$.

Dal momento che $\deg(X-a)^m = m$ abbiamo $\mu(f,a) \leq \deg(f)$. Risulta subito dal teorema 5.3.5 che a è una radice di f se e solo se $\mu(f,a) > 0$. Una radice di un polinomio è detta *multipla* se ha molteplicità maggiore di 1, altrimenti è detta *semplice*. Un criterio per decidere se una radice è multipla verrà dato nel prossimo paragrafo.

Poniamo $m = \mu(f,a)$. Possiamo scrivere $f(X) = (X-a)^m g(X)$, perché $(X-a)^m =$ divide $g(X)$, e $g(a) \neq 0$, perché altrimenti $X-a$ dividerebbe $g(X)$, e quindi $(X-a)^{m+1}$ dividerebbe $f(X)$. Viceversa, supponiamo di avere scritto $f(X) = (X-a)^n g(X)$ con $g(a) \neq 0$; allora $(X-a)^n$ divide $f(X)$, mentre $(X-a)^k$ non può dividere $f(X)$ per nessun $k > n$. Se fosse $f(X) = (X-a)^k q(X)$ con $k > n$ avremmo anche $(X-a)^n g(X) = (X-a)^k q(X)$, da cui, semplificando per $(X-a)^n$, $g(X) = (X-a)^{k-n} q(X)$, e quindi $g(a) = 0$, contraddicendo l'ipotesi $g(a) \neq 0$. Quindi $n = m$. In altre parole, la molteplicità di a come radice di f è l'unico intero m tale che $f(X) = (X-a)^m g(X)$ per un certo polinomio $g(X)$ con $g(a) \neq 0$.

(5.4.2) **Proposizione.** Un polinomio irriducibile in K[X] ha una radice in K se e solo se ha grado 1.

Dimostrazione. Un polinomio $aX+b$ di grado 1 ha $-b/a$ come radice. Se poi $p \in K[X]$ è irriducibile e ha una radice $a \in K$, allora $(X-a) | p(X)$, e quindi $p(X)$ deve essere associato a $X-a$, ossia della forma $c(X-a)$, con $c \in K^*$.

Prendiamo un polinomio f di grado almeno 1, e sia $f = cp_1^{m_1} \dots p_r^{m_r}$ una scomposizione di f in fattori monici irriducibili. Se $a \in K$ si avrà $f(a) = cp_1(a)^{m_1} \dots p_r(a)^{m_r}$, e quindi a è una radice di f se e solo se a è una radice di uno dei p_i. Per la proposizione 5.4.2 i soli polinomi irriducibili che ammettono una radice sono quelli di primo grado. Supponiamo che $p_1, \dots, p_t$ abbiano grado 1 e che $p_{t+1}, \dots, p_r$ abbiano grado maggiore di 1. Possiamo scrivere $p_i(X) = X - a_i$ con $a_i \in K$. Perciò f avrà la forma

$$(*) \qquad f(X) = c(X-a_1)^{m_1}\dots(X-a_t)^{m_t}p_{t+1}(X)^{m_{t+1}}\dots p_r(X)^{m_r}.$$

Ovviamente $a_i \neq a_j$ se $i \neq j$, perché i p_i sono distinti. Le radici di f sono $a_1,\dots,a_t$, perché i fattori $p_{t+1},\dots,p_r$ non hanno radici. Se poniamo

$$g(X) = (X-a_1)^{m_1}\dots(X-a_{i-1})^{m_{i-1}}(X-a_{i+1})^{m_{i+1}}\dots(X-a_t)^{m_t} \\ p_{t+1}(X)^{m_{t+1}}\dots p_r(X)^{m_r}$$

abbiamo $g(a_i) \neq 0$, e $f(X) = (X-a_i)^{m_i}g(X)$. Quindi m_i è la molteplicità di a_i come radice di f. In altre parole, la molteplicità di una radice a_i di f è l'esponente con il quale $X-a_i$ appare nella scomposizione di f in fattori irriducibili.

Confrontando i gradi nell'espressione (*) abbiamo che

$$m_1+\dots+m_t+m_{t+1}\deg(p_{t+1})+\dots+m_r\deg(p_r) = \deg(f),$$

e quindi

$$m_1+\dots+m_t \leq \deg(f),$$

con uguaglianza se e solo se $t = r$. Abbiamo dimostrato il fatto seguente.

(5.4.3) **Teorema.** Siano $a_1,\dots,a_t$ le radici di un polinomio $f \in K[X]$ di grado positivo. Allora

$$\mu(f,a_1)+\dots+\mu(f,a_t) \leq \deg(f).$$

Si ha l'uguaglianza se e solo se f è un prodotto di fattori lineari.

(5.4.4) **Corollario.** Un polinomio non nullo $f \in K[X]$ ha al più deg(f) radici in K.

Dimostrazione. Se $\deg(f) \geq 1$ questo segue immediatamente dalla proposizione 5.3.3, perché $\mu(f,a_i) \geq 1$ per ciascun $i = 1,\dots,t$. Se $\deg(f) = 0$ allora f è una costante non nulla, e quindi non ha radici.

Questo è un risultato utile in molte circostanze. Diamo subito un'applicazione.

(5.4.5) **Proposizione.** Sia K un campo finito con q elementi, e sia n un intero. Allora $a^n = 1$ per ogni $a \in K^*$ se e solo se $(q-1)|n$.

In particolare $q-1$ è uguale al più piccolo intero positivo n tale che $a^n = 1$ per ogni $a \in K^*$. Nel caso particolare in cui $K = \mathbb{Z}_p$ per un primo p abbiamo che $\varphi(p) = p-1$ è in effetti il più piccolo intero positivo tale che $a^n \equiv 1 \pmod p$ per ciascun intero a non divisibile per p, come asserito dopo l'enunciato del teorema di Eulero (3.6.4).

Dimostrazione. Sappiamo che $a^{q-1} = 1$ per ogni $a \in K$ (corollario 3.6.2), e quindi se $(q-1)|n$ si ha $a^n = (a^{q-1})^{n/(q-1)} = 1$. Supponiamo ora che $a^n = 1$ per ogni $a \in K^*$. Dividiamo n per $q-1$: scriviamo $n = (q-1)d+r$, con $0 \le r < q-1$. Avremo $a^r = a^{n-(q-1)d} = a^n(a^{q-1})^{-d} = 1$, e quindi il polinomio X^r-1 ha tutti i $q-1$ elementi di K^* come radici. Ma questo non è possibile se $r > 0$, perché X^r-1 ha grado $r < q-1$.

Definiamo ora una classe importante di campi.

(5.4.6) **Definizione.** Un campo K si dice *algebricamente chiuso* se ogni polinomio in $K[X]$ di grado almeno 1 ha una radice in K.

Dalla proposizione 5.4.2 ricaviamo subito che un campo K è algebricamente chiuso se e solo se tutti i polinomi irriducibili in $K[X]$ hanno grado 1. Una condizione equivalente è che ciascun polinomio in $K[X]$ si scrive come prodotto di fattori lineari.

Segue anche dal teorema 5.4.3 che se K è algebricamente chiuso e $f \in K[X]$ ha grado positivo, con radici $a_1,\dots,a_t$, allora

$$\mu(f,a_1) + \cdots + \mu(f,a_t) = \deg(f).$$

Si dice che un polinomio in un campo algebricamente chiuso ha un numero di radici uguale al grado, se ciascuna radice viene contata con la propria molteplicità.

Osserviamo che un campo algebricamente chiuso è necessariamente infinito. Infatti se K è un campo finito con q elementi allora $a^q-a = 0$ per ogni $a \in K$ (corollario 3.6.2), e quindi il polinomio X^q-X+1 non ha radici in K. Un'altra maniera di dimostrare che un campo finito K non è algebricamente chiuso è di osservare che $K[X]$ contiene infiniti polinomi irriducibili, modificando la dimostrazione data per gli interi (teorema 1.3.7), mentre contiene solo un numero finito di polinomi lineari.

Daremo ora un solo esempio di campo algebricamente chiuso, per il momento, anche in verità ne esistono innumerevoli. Il risultato seguente porta il nome di "teorema fondamentale dell'algebra" per ragioni storiche: oggi in algebra si considerano campi (e anelli) molto più generali, e il campo complesso ha perso un po' la posizione centrale che occupava nell'algebra tradizionale. Tuttavia i numeri complessi giocano un ruolo di primissimo piano in tanti settori della matematica e delle scienze, e perciò il teorema fondamentale dell'algebra è uno dei più importanti di tutta la matematica.

(5.4.7) **Teorema fondamentale dell'algebra.** Il campo complesso $\mathbb{C}$ è algebricamente chiuso.

Sfortunatamente non conosco dimostrazioni facili di questo teorema che non usino il concetto di continuità per funzioni di più variabili reali, e in particolare il teorema che dice che una funzione continua a valori reali definita su un sottoinsieme chiuso e limitato di $\mathbb{R}^2$ ammette un minimo. La dimostrazione che segue usa questi concetti, ma è relativamente elementare. Esistono dimostrazioni che non richiedono nozioni sulle funzioni di più variabili reali, ma in compenso usano un'algebra più sofisticata.

Dimostrazione. Sia $f \in \mathbb{C}[X]$ un polinomio non costante, e cerchiamo di dimostrare che f ha una radice in $\mathbb{C}$. La dimostrazione si divide in due parti: prima facciamo vedere che esiste $z_0 \in \mathbb{C}$ tale che $|f(z)| \geq |f(z_0)|$ per ogni $z \in \mathbb{C}$, e poi concludiamo che $f(z_0) = 0$.

Sia m il grado di f. Facciamo vedere che se M è un qualsiasi numero reale positivo allora esiste un numero reale positivo R tale che se $z \in \mathbb{C}$, $|z| > R$, si ha $|f(z)| \geq M$. Innanzitutto

$$f(z) = f_0 + f_1 z + \cdots + f_m z^m = z^m \left(\frac{f_0}{z^m} + \frac{f_1}{z^{m-1}} + \cdots + \frac{f_{m-1}}{z} + f_m \right)$$

e quindi

$$|f(z)| = |z|^m \left| \frac{f_0}{z^m} + \frac{f_1}{z^{m-1}} + \cdots + \frac{f_{m-1}}{z} + f_m \right| \geq$$

$$|z|^m \left(|f_m| - \left| \frac{f_0}{z^m} + \frac{f_1}{z^{m-1}} + \cdots + \frac{f_{m-1}}{z} \right| \right) \geq$$

$$|z|^m\left(|f_m|-\left(\frac{|f_0|}{|z|^m}+\frac{|f_1|}{|z|^{m-1}}+\cdots+\frac{|f_{m-1}|}{|z|}\right)\right)$$

per la proposizione 2.6.2. Si ha

$$\lim_{\rho\to\infty}\left(\frac{|f_0|}{\rho^m}+\frac{|f_1|}{\rho^{m-1}}+\cdots+\frac{|f_{m-1}|}{\rho}\right)=0$$

e perciò esisterà un numero reale positivo R tale che se $\rho>R$ allora

$$\frac{|f_0|}{\rho^m}+\frac{|f_1|}{\rho^{m-1}}+\cdots+\frac{|f_{m-1}|}{\rho}<\frac{|f_m|}{2}$$

(ricordiamo che $f_m\neq 0$, poiché f_m ha grado m) e perciò

$$|f_m|-\left(\frac{|f_0|}{\rho^m}+\frac{|f_1|}{\rho^{m-1}}+\cdots+\frac{|f_{m-1}|}{\rho}\right)>\frac{|f_m|}{2}$$

se $\rho>R$. Possiamo anche assumere che $R^m>2M/|f_m|$: avremo allora

$$|f(z)|\geq|z|^m\left(|f_m|-\left(\frac{|f_0|}{|z|^m}+\frac{|f_1|}{|z|^{m-1}}+\cdots+\frac{|f_{m-1}|}{|z|}\right)\right)>\frac{2M}{|f_m|}\cdot\frac{|f_m|}{2}=M$$

se $|z|>R$.

Dimostriamo ora l'esistenza di z_0: per quanto appena visto esisterà un numero reale positivo R tale che $|f(z)|>|f(0)|$ se $|z|>R$. Consideriamo il disco chiuso di raggio R centrato nell'origine

$$D=\{z\in\mathbb{C}\,|\,|z|\leq R\}.$$

La funzione $|f|\colon\mathbb{C}\longrightarrow\mathbb{R}$, definita da $|f|(z)=|f(z)|$, è continua, e D è chiuso e limitato in $\mathbb{C}$, quindi esisterà un punto di minimo per $|f|$ in D, ovvero un punto $z_0\in D$ tale che $|f(z)|\geq|f(z_0)|$ per ogni $z\in D$. D'altra parte se $z\notin D$ allora $|f(z)|>|f(0)|\geq|f(z_0)|$, e quindi $|f(z)|\geq|f(z_0)|$ per ogni $z\in\mathbb{C}$.

Supponiamo ora per assurdo che $f(z_0)\neq 0$, e cerchiamo di derivare una contraddizione. Possiamo assumere che $z_0=0$. Infatti in caso contrario prendiamo il polinomio $g(X)=f(X+z_0)$, che avrà radici se e solo se f(X) ha radici. Abbiamo che $g(0)=f(z_0)\neq 0$, e $|g(z)|=|f(z+z_0)|\geq|f(z_0)|=|g(0)|$. Possiamo assumere anche che $f(0)=1$: infatti in caso contrario porremo $h(X)=f(X)/f(0)$. Allora $h(0)=f(0)/f(0)=1$, e $|h(z)|=|f(z)|/|f(0)|\geq 1$ per ogni $z\in\mathbb{C}$.

Il polinomio f(X) avrà la forma $f(X)=1+f_1X+\cdots+f_mX^m$. Sia k il più piccolo intero positivo tale che $f_k\neq 0$, e poniamo $c=f_k$. Scriviamo

$f(X) = 1+cX^k+X^{k+1}g(X)$, dove $g(X) = f_{k+1}+f_{k+2}X+\cdots+f_mX^{m-k-1}$. Sia $\omega \in \mathbb{C}$ tale che $\omega^k = -1/c$, (ω esiste per la proposizione 2.6.7), sia ρ è un numero reale con $0<\rho\le 1$. Si ha

$$f(\rho\omega) = 1+c(\rho\omega)^k+(\rho\omega)^{k+1}g(\rho\omega) = 1-\rho^k+\rho^{k+1}\omega^{k+1}g(\rho\omega).$$

Supponiamo di avere trovato un ρ tale che $\rho\cdot|\omega^{k+1}g(\rho\omega)| < 1$: allora $\rho^{k+1}|\omega^{k+1}g(\rho\omega)| < \rho^k$, e quindi

$$|f(\rho\omega)| = |1-\rho^k+\rho^{k+1}\omega^{k+1}g(\rho\omega)| \le (1-\rho^k)+\rho^{k+1}|\omega^{k+1}g(\rho\omega)| < 1,$$

che è una contraddizione, in quanto per ipotesi $|f(z)|\ge|f(0)| = 1$ per ogni $z \in \mathbb{C}$.

Ma g è limitata sul disco unitario $\{z \in \mathbb{C} \mid |z| \le |\omega|\}$, e quindi esisterà una costante reale positiva M tale che $|g(\rho\omega)| \le M$ per ogni ρ. Se prendiamo perciò ρ con $\rho < 1/|\omega|^{k+1}M$ avremo $\rho|\omega^{k+1}g(\rho\omega)| < \rho|\omega|^{k+1}M < 1$, come si desiderava.

5.5 La derivata di un polinomio

La derivata di una funzione di variabile reale viene introdotta attraverso un procedimento di passaggio al limite che non ha molto senso su un campo arbitrario. Tuttavia la derivata di una funzione polinomiale reale è ancora una funzione polinomiale, data da una formula esplicita che ha senso su un campo qualunque.

Sia K un campo.

(5.5.1) **Definizione.** Sia $f(X) = f_0+f_1X+\cdots+f_nX^n$ un polinomio a coefficienti in K. La *derivata* di f, denotata con f', oppure Df, o anche $\frac{df(X)}{dX}$, è il polinomio a coefficienti in K definito da

$$f'(X) = (Df)(X) = \frac{df(X)}{dX} = f_1+2f_2X+3f_3X^2+\cdots+nf_nX^{n-1}.$$

Più formalmente, il coefficiente di grado i di f' è $(i+1)f_{i+1}$.

C'è una profonda differenza tra la derivata di un polinomio su un

campo di caratteristica 0 e su uno di caratteristica positiva. Se K ha caratteristica 0 e a è un elemento non nullo di K, allora $na \neq 0$ per ogni intero non nullo n: se invece K ha caratteristica positiva p allora $na = 0$, con $a \in K\setminus\{0\}$, se e solo se n è divisibile per p. Quindi se K ha caratteristica 0 e f è un polinomio di grado $n > 0$, la derivata f' avrà grado n-1, perché in tale caso $nf_n \neq 0$. La stessa cosa succederà se K ha caratteristica $p > 0$ e $n = \deg(f)$ non è divisibile per p: se invece n è divisibile per p allora f' avrà grado minore di n-1. Potrà anche succedere che la derivata di f sia nulla, pur avendo f grado arbitrariamente alto: per esempio $D(X^{np}) = npX^{np-1} = 0$.

La derivata qui definita ha molte delle proprietà formali della derivata di funzioni.

(5.5.2) **Proposizione.** (a) La derivata di un polinomio costante è 0.

(b) Se $f(X) = aX^n$, allora $f'(X) = naX^{n-1}$.

(c) Se $a \in K$ e $f \in K[X]$ allora $(af)' = af'$.

(d) Se $f,g \in K[X]$ allora $(f+g)' = f'+g'$.

(e) Se $f,g \in K[X]$ allora $(fg)' = fg'+f'g$.

(f) Se $f_1,\dots,f_r \in K[X]$, allora

$$(f_1f_2\cdots f_r)' = \sum_{i=1}^{r} f_1\cdots f_{i-1}f_i'f_{i+1}\cdots f_r =$$
$$(f_1'f_2\cdots f_r)+(f_1f_2'f_3\cdots f_r)+\cdots+(f_1f_2\cdots f_r')$$

La parte (e) è chiamata *formula di Leibniz*[2].

Dimostrazione. Le parti (a), (b), (c) e (d) sono immediate. Dimostreremo la parte (e). Prima di tutto osserviamo che da (c) segue, per induzione su r, che se $f_1,\dots,f_r \in K[X]$ allora $(f_1+\cdots+f_r)' = f_1'+\cdots+f_r'$. Quindi se supponiamo di sapere che $(f_ig)' = f_i'g+f_ig'$ per ogni $i = 1,\dots,r$, e poniamo $f = f_1+\cdots+f_r$, avremo che

$$(fg)' = ((f_1+\cdots+f_r)g)' = (f_1g+\cdots+f_rg)' = (f_1g)'+\cdots+(f_rg)' =$$
$$(f_1'g+f_1g')+\cdots+(f_r'g+f_rg') = (f_1'+\cdots+f_r')g+(f_1+\cdots+f_r)g' = f'g+fg'.$$

Perciò basta dimostrare la formula quando f è un monomio. Alla stessa maniera possiamo ridurci al caso in cui anche g è un mono-

[2]Gottfried Wilhelm Leibniz (1646-1716), matematico e filosofo tedesco.

mio.

Poniamo allora $f(X) = aX^m$, $g(X) = bX^n$. Si ha

$$f'(X)g(X)+f(X)g'(X) = (maX^{m-1})(bX^n)+(aX^m)(nbX^{n-1}) =$$
$$(mab)X^{m+n-1}+(nab)X^{m+n-1} = (m+n)abX^{m+n-1} = (abX^{m+n})' = (fg)'(X).$$

La parte (f) si dimostra a partire dalla formula di Leibniz per induzione su r. Lascio i dettagli come esercizio.

Una dimostrazione più concettuale della formula di Leibniz si può dare come segue. Consideriamo K come sottocampo di $K[\sqrt{0}]$ (paragrafo 2.3), ponendo $\varepsilon = \sqrt{0}$. Possiamo pensare ad un polinomio $f \in K[X]$ come ad un polinomio a coefficienti in $K[\sqrt{0}]$. Ogni polinomio in $K[\sqrt{0}][X]$ si può scrivere in maniera unica come $f+\varepsilon g$, dove f e g hanno coefficienti in K. Dal fatto che $\varepsilon^2 = 0$ si vede subito, per induzione su k, che $\varepsilon^k = 0$ per ciascun $k \geq 2$; perciò, utilizzando il teorema del binomio (2.1.4), avremo che per ogni $n \geq 0$

$$f(X+\varepsilon) = \sum_{n\geq 0} f_n(X+\varepsilon)^n =$$
$$\sum_{n\geq 0} f_n\left(X^n+n\varepsilon X^{n-1}+\binom{n}{2}\varepsilon^2X^{n-2}+\binom{n}{3}\varepsilon^3X^{n-3}+\dots\right) =$$
$$\sum_{n\geq 0} f_n(X^n+n\varepsilon X^{n-1}) = \sum_{n\geq 0} f_nX^n+\varepsilon\sum_{n\geq 1} nf_nX^{n-1} = f(X)+\varepsilon f'(X).$$

Questo è un inizio di sviluppo in serie di Taylor. Si ha

$$f(X+\varepsilon)\,g(X+\varepsilon) = (f(X)+\varepsilon f'(X))(g(X)+\varepsilon g'(X)) =$$
$$f(X)g(X)+\varepsilon(f(X)g'(X)+f'(X)g(X))+\varepsilon^2f'(X)g'(X) =$$
$$f(X)g(X)+\varepsilon(f(X)g'(X)+f'(X)g(X)).$$

Confrontando questa formula con

$$f(X+\varepsilon)g(X+\varepsilon) = (fg)(X+\varepsilon) = f(X)g(X)+\varepsilon(fg)'(X)$$

otteniamo la formula di Leibniz.

La proposizione seguente stabilisce la connessione tra la derivata di un polinomio e le sue radice multiple.

(5.5.3) **Teorema.** Sia $f \in K[X]$, e $a \in K$ una radice di f. Allora a è una radice multipla di f se e solo se $f'(a) = 0$.

In altre parole, le radici multiple di f sono le radici di f che sono anche radici della derivata di f.

Dimostrazione. Per il teorema 5.3.5 abbiamo che f(X) è divisibile per X-a. Scriviamo $f(X) = (X-a)g(X)$ con $g \in K[X]$. La costante a è una radice multipla di f se e solo se $(X-a)^2$ divide f(X). Se X-a divide g(X) allora ovviamente $(X-a)^2$ divide f(X); se $(X-a)^2$ divide f(X) allora $(X-a)g(X) = f(X) = (X-a)^2q(X)$ per un certo $q \in K[X]$, e, semplificando, si ha $g(X) = (X-a)q(X)$. Perciò a è una radice multipla di f se e solo se X-a divide g(X), ossia se e solo se $g(a) = 0$.

Deriviamo ora entrambi i termini dell'equazione $(X-a)g(X) = f(X)$, ottenendo

$$f'(X) = ((X-a)g(X))' = (X-a)'g(X)+(X-a)g'(X) = g(X)+(X-a)g'(X)$$

Andando a sostituire a per X si ha

$$f'(a) = g(a)+(a-a)g'(a) = g(a)$$

e quindi la conclusione.

Traiamo da questo teorema una conclusione che sarà usata nel paragrafo 7.5.

(5.5.4) **Corollario.** Supponiamo che la caratteristica di K sia $p>0$, e sia n un intero positivo divisibile per p. Allora il polinomio X^n-X non ha radici multiple in K.

Dimostrazione. La derivata di X^n-X è $nX^{n-1}-1 = -1 \neq 0$, e non ammette radici.

Consideriamo ora un sottocampo $K \subset \mathbb{C}$. Siccome $\mathbb{C}$ è algebricamente chiuso ogni polinomio in K[X] si scomporrà come prodotto di fattori lineari in $\mathbb{C}[X]$. Diremo che un polinomio $f \in K[X]$ *ha radici multiple* se ha radici multiple in $\mathbb{C}$.

(5.5.5) **Proposizione.** (a) Un polinomio $f \in K[X]$ non ha radici multiple se e solo se f è relativamente primo ad f' in K[X].

(b) Un polinomio irriducibile in K[X] non ha radici multiple.

Dimostrazione. (a) Supponiamo che f ed f' siano relativamente primi in K[X], e prendiamo $s,t \in K[X]$ tali che $sf+tf' = 1$. Se a è una radice complessa di f allora $1 = s(a)f(a)+t(a)f'(a) = t(a)f'(a)$, e quindi a non è una radice di f'.

Viceversa, assumiamo che f ed f' non siano relativamente primi, e sia d un massimo comun divisore di f ed f' in K[X]. Allora d ha grado positivo, e quindi avrà una radice $a \in \mathbb{C}$. Siccome $d|f$ e $d|f'$ abbiamo che a deve essere radice sia di f che di f'.

(b) Se $f \in K[X]$ è irriducibile, allora f ha grado positivo, e, dal momento che K ha caratteristica 0, f' avrà grado deg(f)-1. Perciò $f' \neq 0$, e f' non è divisibile per f. Allora f ed f' sono relativamente primi, e quindi f non ha radici multiple.

In caratteristica 0 la conclusione del teorema 5.5.3 può essere rafforzata.

(5.5.6) **Proposizione.** Sia K un campo di caratteristica 0, $f \in K[X]$ un polinomio di grado positivo, e $a \in K$ una radice di f. Allora

$$\mu(f',a) = \mu(f,a)-1.$$

In particolare a sarà una radice di f', ossia $\mu(f',a) > 0$, se e solo se $\mu(f,a) > 1$, ossia se e solo se a è una radice multipla di f, come afferma il teorema 5.5.3. La proposizione 5.5.6 è falsa in caratteristica positiva. Per esempio, supponiamo che K abbia caratteristica $p > 0$, e poniamo $f(X) = X^{2p+1}+X^p$, $a = 0$. Si ha $\mu(f,0) = p$, mentre $f'(X) = X^{2p}$, per cui $\mu(f',0) = 2p > p-1 = \mu(f,0)-1$. In questo caso la molteplicità di a come radice di f' è maggiore della molteplicità di a come radice di f.

Dimostrazione. Poniamo $m = \mu(f,a)$. Si avrà allora

$$f(X) = (X-a)^m g(X),$$

con $g(a) \neq 0$. Derivando si ottiene

$$f'(X) = m(X-a)^{m-1}g(X)+(X-a)^m g'(X) = (X-a)^{m-1}(mg(X)+(X-a)g'(X)).$$

Se poniamo $h(X) = mg(X)+(X-a)g'(X)$ otteniamo che $h(a) = mg(a) \neq 0$, poiché siamo in caratteristica 0. Quindi la molteplicità di a come radice di f' è m-1.

Per ogni polinomio $f \in \mathbb{C}[X]$ con radici multiple si può trovare un polinomio $g \in \mathbb{C}[X]$ che ha le stesse radici di f, ma tutte semplici: la proposizione che segue sarà utilizzata nel paragrafo 5.10.

(5.5.7) **Proposizione**. Sia f un polinomio complesso di grado positivo, e chiamiamo $d \in \mathbb{C}[X]$ il massimo comun divisore di f e della sua derivata f'. Allora le radici in $\mathbb{C}$ del quoziente f/d sono le stesse radici di f, e sono tutte semplici.

Il massimo comun divisore d si calcola facilmente con l'algoritmo euclideo.

Dimostrazione. Poniamo $g = f/d$. Innanzitutto si ha $f = dg$, per cui le radici di g sono anche radici di f. Sia ora $a \in \mathbb{C}$ una radice di f di molteplicità m. Allora $\mu(f',a) = m-1$, per la proposizione 5.5.6, ossia, $(X-a)^{m-1}$ divide f'(X), ma $(X-a)^m$ non lo divide. Ciò significa che $(X-a)^{m-1}$ dividerà d(X), mentre $(X-a)^m$ non lo dividerà, ovvero $\mu(d,a) = m-1$. Ne segue che X-a deve dividere g(X) (perché altrimenti $\mu(f',a) = m-1$), mentre $(X-a)^2$ non divide g(X) (altrimenti $\mu(f,a) > m$). Questo significa precisamente che a è una radice semplice di g.

Supponiamo che K abbia caratteristica 0. Sia $f \in K[X]$ un polinomio. Indicheremo con $f^{(k)}(X)$ la derivata k-esima di f, ossia il polinomio f derivato k volte. Ovviamente $f^{(0)} = f$ e $f^{(1)} = f'$. La derivata seconda e terza si indicano anche con f'' e f'''.

Derivando in successione, otteniamo

$$f(X) = f_0+f_1X+f_2X^2+f_3X^3+\cdots,$$
$$f^{(1)}(X) = f_1+2f_2X+3f_3X^2+4f_4X^3+\cdots,$$
$$f^{(2)}(X) = 2f_2+2\cdot3f_3X+3\cdot4f_4X^2+4\cdot5f_5X^3+\cdots,$$
$$f^{(3)}(X) = 2\cdot3f_3+2\cdot3\cdot4f_4X+3\cdot4\cdot5f_5X^2+4\cdot5\cdot6f_6X^3+\cdots.$$

e, per induzione su k,

$$f^{(k)}(X) =$$
$$k!f_k+(2\cdot3\cdots(k+1))f_{k+1}X+(3\cdot4\cdots(k+2))f_{k+2}X^2+(4\cdot5\cdots(k+3))f_{k+3}X^3+\cdots.$$

In generale, il termine di grado d di $f^{(k)}$ sarà

$$(d+1)\cdot(d+2)\cdots(d+k)f_{d+k}X^d.$$

In particolare $f^{(k)}(0) = k!f_k$, e quindi

$$f_k = \frac{1}{k!}f^{(k)}(0).$$

Da qui possiamo ricavare la cosiddetta *formula di Taylor*[3] per i polinomi. Se a è un elemento di K, e poniamo

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

allora g sarà pure un polinomio. Possiamo determinare i coefficienti $g_0,g_1,g_2,\ldots$ di g derivando ripetutamente. Osserviamo che

$$g'(X) = f_1 + 2f_1(X+a)+3f_2(X+a)^2+\cdots = f'(X+a),$$

e, per induzione su k, $g^{(k)}(X) = f^{(k)}(X+a)$ per ogni $k \geq 0$. Da qui

$$g_k = \frac{1}{k!}g^{(k)}(0) = \frac{1}{k!}f^{(k)}(a).$$

Si ha ovviamente

$$f(X) = g(X-a) = g_0+g_1(X-a)+g_2(X-a)^2+\cdots,$$

da cui risulta la formula seguente, di grande importanza.

(5.5.8) **Formula di Taylor.** Sia K un campo di caratteristica 0, f un polinomio di grado n a coefficienti in K, a un elemento di K. Allora

$$f(X) = \sum_{k=0}^{n}\frac{1}{k!}f^{(k)}(a)(X-a)^k =$$

$$f(a)+\frac{1}{1!}f'(a)(X-a)+\frac{1}{2!}f''(a)(X-a)^2+\cdots+\frac{1}{n!}f^{(n)}(a)(X-a)^n.$$

Se il campo di base è il campo reale o complesso, o più in generale un campo in cui si possa parlare di *convergenza* di una serie, allora esiste una classe di funzioni, dette *funzioni analitiche*, per cui vale un analogo del teorema 5.5.8, con la differenza che in un punto possono esistere un numero infinito di derivate non nulle. Perciò una tale funzione verrà scritta come somma di una serie, detta *serie di Taylor*, la quale ha un ruolo assolutamente fondamentale in analisi.

Si può ricavare il teorema del binomio (1.2.3) dalla formula di Taylor. Sia u un intero (o più in generale, un elemento di un qualsiasi campo di caratteristica 0) e consideriamo il polinomio razionale

[3]Brook Taylor (1685-1731), matematico inglese.

$f(X) = (u+X)^n$. Si ha allora $f'(X) = n(u+X)^{n-1}$, $f''(X) = n(n-1)(u+X)^{n-2}$, e, come si vede subito per induzione su k, $f^{(k)}(X) = n(n-1)\cdots(n-k+1)(u+X)^{n-k}$ per ogni $k \leq n$. Allora

$$\frac{1}{k!} f^{(k)}(0) = \frac{n(n-1)\ldots(n-k+1)}{k!} u^{n-k} = \binom{n}{k} u^{n-k},$$

da cui, per la formula di Taylor,

$$(u+X)^n = \sum_{k=0}^{n} \binom{n}{k} u^{n-k} X^k.$$

Se v è un altro intero, allora ponendo $X = v$ nella formula sopra otteniamo precisamente il teorema del binomio.

5.6 Il teorema di interpolazione

Il *teorema di interpolazione* dice per ogni naturale n esiste un unico polinomio di grado minore di n che assume n valori preassegnati in n punti distinti.

(5.6.1) **Teorema di interpolazione.** Sia K un campo, n un intero positivo, $a_1,\ldots,a_n$ n elementi di K a due a due distinti. Se $b_1,\ldots,b_n$ sono elementi arbitrari di K, esiste un unico polinomio $f \in K[X]$ di grado minore di n, con $f(a_i) = b_i$ per ogni $i = 1,\ldots,n$.

Dimostrazione. Se f e g sono polinomi in K[X] di grado minore di n con $f(a_i) = g(b_i) = b_i$ per ogni $i = 1,\ldots,n$, allora $(f-g)(a_i) = 0$ per ogni i, e f-g è un polinomio di grado minore di n con n radici distinte. Per il corollario 5.4.4 si ha $f-g = 0$. Questo dimostra l'unicità.

Per dimostrare l'esistenza, osserviamo che il polinomio

$$\Phi_i(X) = \frac{(X-a_1)\ldots(X-a_{i-1})(X-a_{i+1})\ldots(X-a_n)}{(a_i-a_1)\ldots(a_i-a_{i-1})(a_i-a_{i+1})\ldots(a_i-a_n)}$$

ha grado n-1, ed ha la proprietà che $\Phi_i(a_i) = 1$, mentre $\Phi_i(a_j) = 0$ se $j \neq i$. Perciò il polinomio desiderato sarà