Università degli Studi Roma Tre
Corso di Laurea in Matematica

Stefania Gabelli e Florida Girolami

Anelli di polinomi

Appunti per i corsi di ALGEBRA

Settembre 2004

INDICE

Anelli di polinomi

1. Costruzione di anelli di polinomi.

Nel seguito considereremo sempre anelli commutativi e unitari e diremo che un tale anello è un *dominio* (o *dominio integro*, o *dominio di integrità*) se non possiede divisori dello zero.

Ricordiamo che un *divisore dello zero*, o uno *zero-divisore*, di un anello commutativo A è un elemento non nullo a tale che $ab = 0$ per qualche elemento non nullo $b \in A$.

Consideriamo l'insieme

$$A^{\mathbf{N}} := \{(c_0, c_1, \dots, c_k, \dots\dots) ; c_k \in A\}$$

delle successioni di elementi di A.

Per definizione, si ha che,

$$(a_0, a_1, \dots, a_k, \dots\dots) = (b_0, b_1, \dots, b_k, \dots\dots)$$

se e soltanto se $a_i = b_i$, per ogni $i \geq 0$.

Definiamo in $A^{\mathbf{N}}$ le operazioni di addizione e moltiplicazione rispettivamente con:

$$(a_0, a_1, \dots, a_k, \dots\dots) + (b_0, b_1, \dots, b_k, \dots\dots) = (a_0+b_0, a_1+b_1, \dots, a_k+b_k, \dots\dots),$$

$$(a_0, a_1, \dots, a_k, \dots\dots)(b_0, b_1, \dots, b_k, \dots\dots) = (a_0b_0, a_0b_1+ a_1b_0, \dots, \Sigma_{i+j=k}\, a_ib_j, \dots\dots).$$

Si verifica facilmente che, rispetto a queste operazioni, $A^{\mathbf{N}}$ è un anello commutativo unitario; lo zero di $A^{\mathbf{N}}$ è la successione nulla $(0, 0, \dots, 0, \dots\dots)$ e la sua unità è la successione $(1, 0, \dots, 0, \dots\dots)$.

Una successione $(c_0, c_1, \dots, c_k, \dots\dots)$ di elementi di A si dice *quasi ovunque nulla* se esiste un intero $n \geq 0$ tale che $c_m = 0$ per ogni $m \geq n$. Questo equivale a dire che $c_k \neq 0$ al più per un numero finito di interi k.

Denotiamo con P_A l'insieme delle successioni quasi ovunque nulle di elementi di A:

$$P_A := \{(c_0, c_1, \dots, c_k, \dots\dots) ; c_k \in A, c_k \neq 0 \text{ al più per un numero finito di interi } k\}.$$

Si verifica facilmente che somme, differenze e prodotti di successioni quasi ovunque nulle sono ancora successioni quasi ovunque nulle. Dunque P_A è un sottoanello di $A^{\mathbf{N}}$. Inoltre, se

$$\underline{c} := (c, 0, \dots, 0, \dots\dots), \text{ per ogni } c \in A,$$

l'applicazione

$$A \longrightarrow P_A \quad \text{definita da} \quad c \longrightarrow \underline{c} := (c, 0, \dots, 0, \dots\dots)$$

è un omomorfismo iniettivo di anelli; dunque l'insieme delle successioni

$$\{\underline{c} := (c, 0, \dots, 0, \dots\dots) ; c \in A\}$$

costituisce un sottoanello di P_A isomorfo a A.

Posto

$$X := (0, 1, 0, \dots, 0, \dots\dots),$$

risulta:

$$(c_0, c_1, \dots, c_n, 0, \dots\dots) = \underline{c}_0 + \underline{c}_1 X + \dots + \underline{c}_n X^n .$$

Quindi, identificando A con la sua immagine in P_A, ovvero identificando c con $\underline{c}$, gli elementi dell'anello P_A si possono scrivere come espressioni formali del tipo

$$f(X) := c_0 + c_1 X + \dots + c_n X^n , \ n \geq 0, \ c_k \in A \text{ per } k = 0, \dots, n .$$

Per evidenziare questo fatto, si usa indicare l'anello P_A con $A[X]$.

Notiamo che

$$(c_0, c_1, \dots, c_n, 0, \dots\dots) = c_0 + c_1 X + \dots + c_n X^n = 0$$

se e soltanto se $c_0 = c_1 = \dots = c_n = 0$. Questa proprietà si esprime dicendo che X è una *indeterminata* su A.

L'espressione:

$$f(X) := c_0 + c_1 X + \dots + c_n X^n$$

si dice un *polinomio* nell'indeterminata X con *coefficienti* $c_0, \dots, c_n$. Il polinomio che ha tutti i coefficienti nulli si identifica con lo zero di A e si dice il *polinomio nullo*.

L'anello $A[X]$ si chiama allora l'*anello dei polinomi a coefficienti in* A (o *su* A) *nell'indeterminata* X.

Se $f(X) := c_0 + c_1 X + \dots + c_n X^n$ e $c_n \neq 0$, si dice che $f(X)$ ha *grado* n e si scrive $\deg(f(X)) = n$. Inoltre c_n si dice il *coefficiente direttore* di $f(X)$ e $c_n X^n$ si dice il *termine direttore* di $f(X)$.

Il grado del polinomio nullo non è definito. I polinomi di grado 0 si identificano con gli elementi non nulli di A. Gli elementi di A si chiamano i *polinomi costanti* o semplicemente le *costanti* di $A[X]$.

Per come sono definite le operazioni in P_A, se

$$f(X) := a_0 + a_1 X + \dots + a_n X^n \quad \text{e} \quad g(X) := b_0 + b_1 X + \dots + b_m X^m$$

sono due polinomi di gradi n e m rispettivamente, $m \geq n$, risulta:

$$f(X) + g(X) = (a_0+b_0) + (a_1+b_1)X + \dots + (a_n+b_n)X^n + b_{n+1}X^{n+1} + \dots + b_m X^m ,$$
$$f(X)g(X) = (a_0b_0) + (a_0b_1+a_1b_0)X + \dots + (\Sigma_{i+j=k}\, a_i b_j)X^k + \dots + (a_n b_m)X^{n+m} .$$

Inoltre, se $f(X)$ e $g(X)$ sono tali che $f(X) + g(X) \neq 0$ e $f(X)g(X) \neq 0$, si ha:

$$\deg(f(X) + g(X)) \leq \max\{\deg(f(X)), \deg(g(X))\} \ ;$$
$$\deg(f(X)g(X)) \leq \deg(f(X)) + \deg(g(X)).$$

Proposizione 1.1 (Principio di Uguaglianza tra Polinomi). Siano $f(X), g(X) \in A[X]$ due polinomi non nulli. Allora $f(X) = g(X)$ se e soltanto se $f(X)$ e $g(X)$ hanno stesso grado e tutti i coefficienti uguali.

Dimostrazione. Segue dal fatto che $f(X) = g(X)$ se e soltanto se $f(X) - g(X) = 0$, ovvero il polinomio $f(X) - g(X)$ ha tutti i coefficienti nulli.

Proposizione 1.2. Se A è un dominio, allora $A[X]$ è un dominio e vale l'uguaglianza:

$$\deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X)) \qquad \textit{(formula del grado)}.$$

Dimostrazione. Siano $f(X), g(X) \in A[X]$ due polinomi non nulli, di gradi n e m rispettivamente. Poiché A è un dominio e a_n e b_m sono diversi da zero, risulta $a_n b_m \neq 0$ e dunque $f(X)g(X) \neq 0$. Ne segue che $A[X]$ è un dominio e inoltre $\deg(f(X)g(X)) = n+m$.

Se A non è integro, l'anello $A[X]$ non è integro e non vale quindi la formula del grado. Ad esempio, il prodotto dei polinomi non nulli $2X$ e $3X$ di $\mathbf{Z}_6[X]$ è il polinomio nullo, dunque il prodotto dei polinomi di primo grado $2X+1$ e $3X+1$ è il polinomio di primo grado $5X+1$.

Il fatto che, se A è un anello commutativo unitario (rispettivamente un dominio), anche $A[X]$ è un anello commutativo unitario (rispettivamente un dominio), ci permette di definire, per induzione su n, l'anello dei *polinomi in* n *indeterminate* $X_1, \ldots, X_n$ su A ponendo

$A_0 := A$ e $A_i = A_{i-1}[X_i] = ((\ldots((A[X_1])[X_2]) \ldots)[X_{i-1}])[X_i]$ per $i = 1, \ldots, n$.

L'anello A_n si indica con $A[X_1, \ldots, X_n]$; i suoi elementi si scrivono come espressioni

$$f(X_1, \ldots, X_n) := \Sigma c_{k_1 \ldots k_n} X_1^{k_1} \ldots X_n^{k_n},$$

dove $c_{k_1 \ldots k_n} \in A$ e $0 \leq k_1 + \ldots + k_n \leq m$ per m opportuno (con la convenzione che $X_i^0 = 1$ per $i = 1, \ldots, n$).

Per costruzione, essendo X_i una indeterminata su A_{i-1}, si ha che $f(X_1, \ldots, X_n) = 0$ se e soltanto se tutti i coefficienti $c_{k_1 \ldots k_n}$ sono nulli; ovvero gli elementi $X_1, \ldots, X_n$ non soddisfano alcuna relazione algebrica su A. Questa condizione si esprime anche dicendo che $X_1, \ldots, X_n$ sono *indeterminate (algebricamente) indipendenti* su A.

Osserviamo che, per le proprietà commutativa e distributiva, per ogni $i = 1, \ldots, n$, si può scrivere

$$f(X_1, \ldots, X_n) = f_0 + f_1 X_i + \ldots + f_{n_i} X_i^{n_i},$$

dove, per $k = 0, \ldots, n_i$, f_k è un polinomio in cui non compare l'indeterminata X_i. Per questo fatto, possiamo considerare $f(X_1, \ldots, X_n)$ come un polinomio nell'indeterminata X_i a coefficienti nell'anello $B_i := A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ e in questo modo identificare $A[X_1, \ldots, X_n]$ con $B_i[X_i]$.

Il *grado* del polinomio non nullo $f(X_1, \ldots, X_n)$ *rispetto all'indeterminata* X_i è il suo grado come elemento di $B_i[X_i]$.

Un polinomio di $A[X_1, \ldots, X_n]$ del tipo $cX_1^{k_1} \ldots X_n^{k_n}$ si dice un *monomio*. Se $m(X) := cX_1^{k_1} \ldots X_n^{k_n}$ è un monomio non nullo, il suo grado rispetto all'indeterminata X_i è k_i. Il *grado totale* (o semplicemente *grado*) di $m(X)$ si definisce come $k_1 + \ldots + k_n$. Un polinomio non nullo è somma di monomi e il suo *grado* si definisce come il massimo grado dei monomi suoi addendi. Un polinomio si dice *omogeneo* se tutti i suoi termini hanno lo stesso grado.

Per semplicità di notazione, si usa anche porre

$$\mathbf{X} := (X_1, \ldots, X_n) \quad \text{e} \quad A[\mathbf{X}] := A[X_1, \ldots, X_n] .$$

Allo stesso modo, se $k := (k_1, \ldots, k_n)$ si pone

$$\mathbf{X}^k := X_1^{k_1} \ldots X_n^{k_n} \quad \text{e} \quad c_k := c_{k_1 \ldots k_n} .$$

In questo contesto, la n-pla $k := (k_1, \ldots, k_n)$ si dice un *multiindice*.

Questa convenzione ha il vantaggio di poter scrivere un polinomio di $A[\mathbf{X}]$ come

$$f(\mathbf{X}) = \Sigma c_k \mathbf{X}^k ,$$

in analogia con il caso dei polinomi in una indeterminata.

Poiché un polinomio può avere più termini dello stesso grado, per completare l'analogia è talvolta utile ordinare linearmente i monomi di $A[\mathbf{X}]$; per questo basta ordinare linearmente i multiindici. Ad esempio, si può usare l'*ordine lessicografico* , indicato con $<_{lex}$ e definito da

$$(k_1, \ldots, k_n) = (h_1, \ldots, h_n) \Leftrightarrow k_i = h_i \text{ per } i = 1, \ldots, n ;$$

$(k_1, \ldots, k_n) <_{lex} (h_1, \ldots, h_n) \Leftrightarrow$

per il più piccolo intero s tale che $k_s \neq h_s$, si ha che $k_s < h_s$.

Notiamo che, nell'ordine lessicografico, si ha

$$X_n < X_n^2 < X_n^3 < \ldots < X_{n-1} < X_{n-1}^2 < \ldots < X_1 < \ldots$$

$$X_{j+1} < X_1^{k_1} \ldots X_j^{k_j} , \text{ se } (k_1, \ldots, k_j) \neq (0, \ldots, 0) .$$

Per questo motivo viene usato talvolta anche un altro ordinamento, detto *ordine lessicografico inverso* e indicato con $<_{revlex}$. Questo consiste nell'ordinare lessicograficamente le n-ple $(k_n, k_{n-1}, \ldots, k_1)$ e più precisamente è definito nel seguente modo:

$$(k_1, \ldots, k_n) = (h_1, \ldots, h_n) \Leftrightarrow k_i = h_i \text{ per } i = 1, \ldots, n ;$$

$(k_1, \ldots, k_n) <_{revlex} (h_1, \ldots, h_n) \Leftrightarrow$

per il più grande intero s tale che $k_s \neq h_s$, si ha che $k_s < h_s$.

Nell'ordine lessicografico inverso, risulta

$$X_1 < X_1^2 < X_1^3 < \ldots < X_{n-1} < X_{n-1}^2 < \ldots < X_n < \ldots$$

$$X_1^{k_1} \ldots X_j^{k_j} < X_{j+1} , \text{ se } (k_1, \ldots, k_j) \neq (0, \ldots, 0) .$$

In particolare l'ordinamento lessicografico inverso non è l'ordinamento opposto dell'ordinamento lessicografico.

Una volta ordinati i monomi di $A[\mathbf{X}]$, se $f(\mathbf{X}) \neq 0$, il massimo monomio $c_m \mathbf{X}^m$ di $f(\mathbf{X})$ si dice il *monomio direttore* (o anche il *termine direttore*) di $f(\mathbf{X})$ (rispetto all'ordinamento scelto) e il suo coefficiente c_m si dice il *coefficiente direttore* di $f(\mathbf{X})$. Inoltre, il multiindice $m = (m_1, \ldots, m_n)$ si dice il *multigrado* di $f(\mathbf{X})$ (rispetto all'ordinamento scelto).

Ricordiamo che, se A è un dominio, si può costruire un campo, unico a meno di isomorfismi, con la proprietà di essere il più piccolo campo contenente una copia isomorfa di A. Questo campo si chiama il *campo dei quozienti* di A e si indica con $Qz(A)$. I suoi

elementi sono le classi di equivalenza dell'insieme $A\times A^*$ rispetto alla relazione di equivalenza ε definita da:

$$(a,b)\ \varepsilon\ (a',b') \Leftrightarrow ab' = a'b\ .$$

Si usa indicare la classe di (a,b) rispetto a ε con a/b, in modo da poter scrivere

$$Qz(A) := \{a/b\ ;\ a, b \in A\ ,\ b \neq 0\}.$$

Le operazioni in $Qz(A)$ sono definite da:

$$a/b + c/d = (ad + cb)/bd \quad \text{e} \quad (a/b)(c/d) = ac/bd.$$

Se A è contenuto in un campo K, allora ogni elemento non nullo di A ha un inverso in K. In questo caso risulta $Qz(A) = \{xy^{-1}\ ;\ x, y \in A\ ,\ y \neq 0\}$.

Il campo dei quozienti dell'anello di polinomi $K[\mathbf{X}] := K[X_1, \ldots, X_n]$ a coefficienti nel campo K è il campo

$$K(\mathbf{X}) := K(X_1, \ldots, X_n) := \{f(\mathbf{X})/g(\mathbf{X})\ ;\ f(\mathbf{X}), g(\mathbf{X}) \in K[\mathbf{X}]\ ,\ g(\mathbf{X}) \neq 0\}\ .$$

Esso si dice il *campo delle funzioni razionali nelle indeterminate* $X_1, \ldots, X_n$ a coefficienti in K (o su K).

Se A è un dominio, il campo dei quozienti di $A[\mathbf{X}] := A[X_1, \ldots, X_n]$ è il campo delle funzioni razionali su $Qz(A)$. Ad esempio, il campo dei quozienti sia di $\mathbf{Z}[\mathbf{X}]$ che di $\mathbf{Q}[\mathbf{X}]$ è $\mathbf{Q}(\mathbf{X})$.

ESERCIZI

1. Ordinare i seguenti monomi di $\mathbf{Q}[\mathbf{X}]$ secondo l'ordine lessicografico e l'ordine lessicografico inverso:

$$\frac{1}{3}X_1X_2^2X_3^6X_5^8\ ,\quad -\frac{7}{5}X_2^3X_3X_4X_5\ ,\quad \frac{2}{9}X_1X_2^4X_3X_4X_5\ ,\quad -\frac{3}{13}X_4^{21}X_5^3\ ,\quad 7X_1X_2^4X_3X_4^2X_5^3\ .$$

2. Determinare il grado totale e i multigradi rispetto agli ordinamenti lessicografico e lessicografico inverso dei seguenti polinomi di $\mathbf{Q}[\mathbf{X}]$:

(a) $f(X) = \frac{2}{5}X_1^2X_2^3X_3^2X_5^8 - \frac{1}{13}X_2^3X_3X_4X_5 + \frac{2}{7}X_1X_2^4X_3X_4X_5^4$;

(b) $g(X) = -\frac{3}{8}X_2^3X_3^5X_4^2X_6 + \frac{1}{10}X_1^4X_2X_5^2 - 7X_6^{15} + 4X_2^5X_5$.

3. Indichiamo con $mdeg(f)$ il multigrado del polinomio non nullo $f(\mathbf{X})$ di $A[\mathbf{X}]$ rispetto all'ordinamento lessicografico. Mostrare che, se A è un dominio e $f(\mathbf{X})$, $g(\mathbf{X})$ sono due polinomi non nulli di $A[\mathbf{X}]$, allora

$$mdeg(f(\mathbf{X})+g(\mathbf{X})) \leq_{lex} \max\{mdeg(f(\mathbf{X})),\ mdeg(g(\mathbf{X}))\}\ ;$$

$$mdeg(f(\mathbf{X})g(\mathbf{X})) \leq_{lex} mdeg(f(\mathbf{X}))+mdeg(g(\mathbf{X})).$$

Dimostrare inoltre che formule analoghe valgono per l'ordinamento lessicografico inverso.

4. Mostrare che, se A è un dominio, il campo dei quozienti di $A[\mathbf{X}] := A[X_1, \ldots, X_n]$ è il campo delle funzioni razionali su $Qz(A)$, ovvero

$Qz(A[\mathbf{X}]) = Qz(A)(\mathbf{X}) := \{f(\mathbf{X})/g(\mathbf{X})\ ;\ f(\mathbf{X}), g(\mathbf{X}) \in Qz(A)[\mathbf{X}]\ ,\ g(\mathbf{X}) \neq 0\}$.

2. Funzioni polinomiali.

Il fatto di poter scrivere un polinomio su A come una espressione formale nell'indeterminata X ci permette di associare a tale polinomio una funzione da A in A.

Precisamente, sia $f(X) := c_0 + c_1X + \ldots + c_nX^n \in A[X]$. Se $\alpha \in A$, poniamo

$$f(\alpha) := c_0 + c_1\alpha + \ldots + c_n\alpha^n .$$

L'elemento $f(\alpha)$ sta in A e si dice il *valore* del polinomio $f(X)$ calcolato in α.

Per ogni $f(X) \in A$, si può allora considerare la funzione $\varphi_f : A \longrightarrow A$ che ad ogni elemento $\alpha \in A$ associa il valore di $f(X)$ in α. Ovvero

$$\varphi_f : A \longrightarrow A , \quad \alpha \longrightarrow f(\alpha) , \text{ per ogni } \alpha \in A .$$

Ad ogni elemento c di A corrisponde la funzione che assume valore costante c su tutto A. In questo modo, agli elementi di A, ovvero ai polinomi costanti, vengono associate le funzioni costanti e questo giustifica la terminologia.

Le funzioni definite come sopra si chiamano le *funzioni polinomiali* su A.

Poiché A è un anello, si verifica facilmente che l'insieme A^A di tutte le funzioni da A in A costituisce a sua volta un anello rispetto alle operazioni di addizione e moltiplicazione definite rispettivamente da

$$(\varphi+\psi)(\alpha) = \varphi(\alpha) + \psi(\alpha) \quad \text{e} \quad (\varphi\,\psi)(\alpha) = \varphi(\alpha)\,\psi(\alpha) , \text{ per ogni } \alpha \in A .$$

Lo zero di A^A è la funzione nulla e, se 1 è l'unità di A, l'unità di A^A è la funzione costante che assume valore 1 su tutto A.

Proposizione 2.1. L'applicazione $A[X] \longrightarrow A^A$ che ad ogni polinomio a coefficienti in A associa la corrispondente funzione polinomiale è un omomorfismo di anelli. Dunque le funzioni polinomiali su A costituiscono un sottoanello di A^A.

Dimostrazione. E' immediato constatare che alla somma di polinomi $f(X) + g(X)$ resta associata la somma $\varphi_f + \varphi_g$ delle funzioni polinomiali corrispondenti ad $f(X)$ e $g(X)$ e, analogamente, al prodotto di polinomi $f(X)g(X)$ corrisponde il prodotto di funzioni polinomiali $\varphi_f\,\varphi_g$.

Per la proposizione precedente, con abuso di notazione, porremo talvolta

$$\varphi_f + \varphi_g = (f+g)(X) , \quad \varphi_f\,\varphi_g = (fg)(X) \quad \text{e} \quad \varphi_f \circ \varphi_g = (f \circ g)(X) = f(g(X)) .$$

In generale, l'omomorfismo sopra definito non è iniettivo. Ad esempio, se $A = \{a_1, \ldots, a_n\}$ è un anello finito, al polinomio non nullo $(X-a_1)\ldots(X-a_n)$ corrisponde la funzione nulla. Tuttavia, vedremo nel seguito che, se A è infinito, l'anello dei polinomi su A e quello delle funzioni polinomiali su A sono isomorfi; ovvero due funzioni polinomiali sono uguali (cioè assumono lo stesso valore su ogni elemento di A) se e soltanto se i polinomi che le definiscono sono uguali (cioè hanno coefficienti uguali). Questo fatto ci sarà particolarmente utile nello studio dei polinomi a coefficienti numerici (cf. Proposizione 4.4).

Quanto precede si estende senza difficoltà all'anello dei polinomi $A[\mathbf{X}] := A[X_1, \ldots, X_n]$ per $n \geq 2$.

Se $f(\mathbf{X}) := \Sigma c_{k_1 \ldots k_n} X_1^{k_1} \ldots X_n^{k_n} \in A[\mathbf{X}]$ e $\alpha = (\alpha_1, \ldots, \alpha_n) \in A^n$, il *valore* del polinomio $f(\mathbf{X})$ calcolato in α è l'elemento di A definito da

$$f(\alpha) := \Sigma c_{k_1 \ldots k_n} \alpha_1^{k_1} \ldots \alpha_n^{k_n} .$$

Ogni $f(\mathbf{X}) \in A[\mathbf{X}]$, definisce allora la *funzione polinomiale* $\varphi_f : A^n \longrightarrow A$ che ad ogni elemento $\alpha \in A^n$ associa il valore di $f(\mathbf{X})$ in α. Ovvero

$$\varphi_f : A^n \longrightarrow A , \quad \alpha \longrightarrow f(\alpha) , \text{ per ogni } \alpha \in A^n .$$

L'insieme delle funzioni polinomiali su A^n è un sottoanello dell'anello di tutte le funzioni da A^n in A ed è isomorfo ad $A[\mathbf{X}]$ se A è infinito. Quest'ultimo fatto si può dimostrare per induzione su n una volta provato il caso $n = 1$.

ESERCIZI

1. Determinare in $\mathbf{Q}[X]$ i polinomi $f(X)+g(X)$, $f(X)g(X)$ e $f(g(X))$ nei seguenti casi:

(a) $f(X) = 1 - 3X + X^2$; $g(X) = 2 + 3X - 7X^3$;

(b) $f(X) = 1 - X^4$; $g(X) = 2 + X^2$.

2. Mostrare che, se A è un anello (commutativo unitario), l'insieme di tutte le funzioni da A^n in A costituisce un anello (commutativo unitario) rispetto alle operazioni di somma e moltiplicazione definite rispettivamente da

$$(\varphi + \psi)(\alpha) = \varphi(\alpha) + \psi(\alpha) \quad \text{e} \quad (\varphi \psi)(\alpha) = \varphi(\alpha) \psi(\alpha) , \text{ per ogni } \alpha \in A^n .$$

Mostrare inoltre che, anche se A è un campo, tale anello non è mai un dominio.

3. Costruire due polinomi differenti di $A[X]$ che assumano stessi valori su A nel caso in cui $A = \mathbf{Z}_3$, $\mathbf{Z}_5$.

4. Costruire un polinomio di $\mathbf{Z}_2[X]$ tale che $f(0) = a$, $f(1) = b$, per ogni coppia (a,b) di elementi di $\mathbf{Z}_2$. Dedurre che ogni funzione da $\mathbf{Z}_2$ a $\mathbf{Z}_2$ è polinomiale.

5. Costruire un polinomio di $\mathbf{Z}_3[X]$ tale che $f(0) = 2$, $f(1) = 1$, $f(2) = 0$.

6. Sia p un numero primo. Mostrare che ogni funzione da $\mathbf{Z}_p$ a $\mathbf{Z}_p$ è polinomiale. (Sugg. Se a_1 , …, a_p sono gli elementi di $\mathbf{Z}_p$, allora, per ogni $i = 1, \ldots, p$ e $c \in \mathbf{Z}_p$, il polinomio

$$f_i(X) := c(X - a_1) \ldots (X - a_{i-1})(X - a_{i+1}) \ldots (X - a_p)$$

è tale che $f_i(a_j) = 0$ per $j \neq i$: inoltre il valore $f_i(a_i)$ può essere controllato dalla scelta di c.)

3. Divisibilità tra polinomi. Algoritmo della divisione.

L'assenza di zero-divisori permette di costruire per i domini una Teoria della Divisibilità del tutto analoga a quella esistente nel dominio degli interi relativi $\mathbf{Z}$. In questo contesto siamo interessati a sviluppare questa teoria per gli anelli di polinomi in una indeterminata a coefficienti in $\mathbf{Z}$ o in un campo K ; la terminologia è però del tutto generale.

Sia R un dominio e siano $a, b \in R$. Si dice che b *divide* a in R, e si scrive $b|a$, se esiste un elemento $c \in R$ tale che $a = bc$. In tal caso b si dice anche un *divisore* o un *fattore* di a in R. Lo zero di R è diviso da ogni elemento di R e divide soltanto se stesso. Un divisore di 1 si dice un elemento *invertibile*, o una *unità*, di R. In altre parole, un elemento $u \in R$ è invertibile in R se esiste $v \in R$ tale che $uv = 1$. Gli elementi invertibili di R formano un gruppo moltiplicativo che si indica con $U(R)$. Due elementi a, b di R si dicono *associati* in R se esiste una unità u di R tale che $a = ub$.

D'ora in poi, A denoterà sempre un dominio e dunque anche gli anelli di polinomi su A saranno domini.

Osserviamo che, se $g(X)$ è un divisore di $f(X)$ in $A[X]$, per la formula del grado (Proposizione 1.2), deve essere $\deg(g(X)) \leq \deg(f(X))$. Questo fatto ci permette di dimostrare subito la seguente Proposizione.

Proposizione 3.1. Gli elementi invertibili di $A[X]$ sono tutti e soli gli elementi invertibili di A. In particolare, se K è un campo, gli elementi invertibili di $K[X]$ sono tutte e sole le costanti non nulle.

Dimostrazione. Il prodotto di due polinomi $f(X)$ e $g(X)$ entrambi non nulli ha grado uguale alla somma dei due gradi $\deg(f(X))$ e $\deg(g(X))$ (Proposizione 1.2) e coefficiente direttore uguale al prodotto dei coefficienti direttori di $f(X)$ e di $g(X)$. Pertanto il prodotto $f(X)g(X)$ può essere 1 soltanto quando entrambi i fattori sono costanti, ciascuno invertibile in A.

Corollario 3.2. I polinomi $f(X)$ e $g(X)$ sono associati in $A[X]$ se e soltanto se $f(X) = ug(X)$, dove u è un elemento invertibile di A. In particolare due polinomi associati hanno lo stesso grado.

Dimostrazione. Segue dalla Proposizione 3.1. e dalla formula del grado (Proposizione 1.2.).

Esempi.

1. Poiché $U(\mathbf{Z}) = \{1, -1\}$, allora $U(\mathbf{Z}[X]) = \{1, -1\}$. Inoltre i polinomi $f(X)$ e $g(X)$ sono associati in $\mathbf{Z}[X]$ se e soltanto se $g(X) = \pm f(X)$.

2. Se K è un campo, $U(K) = K^* := K \setminus \{0\}$. Dunque $U(K[X]) = K^*$ e i polinomi $f(X)$ e $g(X)$ sono associati in $K[X]$ se e soltanto se $g(X) = cf(X)$, dove $c \in K^*$ è una costante non nulla.

3. Se A non è un dominio, ci possono essere in $A[X]$ polinomi invertibili che hanno grado positivo. Ad esempio in $\mathbf{Z}_4[X]$ risulta $(2X+1)(2X+1) = 1$.

Teorema 3.3 (Algoritmo della divisione tra polinomi). Se $f(X)$, $g(X) \in A[X]$ sono due polinomi non nulli e il coefficiente direttore di $g(X)$ è invertibile, esistono e sono univocamente determinati, due polinomi $q(X)$, $r(X) \in A[X]$ tali che:

$$f(X) = g(X)q(X) + r(X) \quad \text{e} \quad r(X) = 0 \text{ oppure } \deg(r(X)) < \deg(g(X)) .$$

In questo caso $q(X)$ si dice il *quoziente della divisione* di $f(X)$ per $g(X)$ e $r(X)$ si dice il *resto* della divisione.

Dimostrazione. Se $\deg(f(X)) < \deg(g(X))$, basta prendere $q(X) := 0$ e $r(X) := f(X)$. Pertanto d'ora in avanti supporremo che $\deg(f(X)) \geq \deg(g(X))$.

Sia $n := \deg(f(X))$ e $k := \deg(g(X))$ e siano a_n e b_k i coefficienti direttori di $f(X)$ e $g(X)$ rispettivamente. Essendo b_k invertibile e $n \geq k$, possiamo considerare il polinomio $q_1(X) := a_n b_k^{-1} X^{n-k}$; allora il polinomio $g(X)q_1(X)$ ha termine direttore $b_k X^k \left(a_n b_k^{-1}\right) X^{n-k} = a_n X^n$. Avendo $f(X)$ e $g(X)q_1(X)$ lo stesso termine direttore, il polinomio $f_1(X) := f(X) - g(X)q_1(X)$ o è nullo, oppure ha grado minore di n e risulta $f(X) = g(X)q_1(X) + f_1(X)$.

Ripetendo il procedimento con $f_1(X)$ al posto di $f(X)$, otterremo un polinomio $f_2(X) := f_1(X) - g(X)q_2(X)$ che è nullo oppure ha grado minore di quello di $f_1(X)$. Inoltre risulterà $f(X) = g(X)(q_1(X) + q_2(X)) + f_2(X)$. Dopo un numero finito m di passi otterremo un polinomio $q(X) := q_1(X) + q_2(X) + \ldots + q_m(X)$ di $A[X]$ tale che il polinomio $f(X) - g(X)q(X)$ o è nullo oppure ha grado minore di $k = \deg(g(X))$. A questo punto, basta porre $r(X) := f(X) - g(X)q(X)$. Questo prova l'esistenza.

Per dimostrare l'unicità, supponiamo che

$$f(X) = g(X)\, q_1(X) + r_1(X) = g(X)q_2(X) + r_2(X) ,$$

dove $r_1(X) = 0$ oppure $\deg(r_1(X)) < \deg(g(X))$ ed inoltre $r_2(X) = 0$ oppure $\deg(r_2(X)) < \deg(g(X))$. Sottraendo si ottiene

$$g(X)[q_2(X) - q_1(X)] = r_1(X) - r_2(X) .$$

Essendo $g(X)$ non nullo, risulta $r_1(X) - r_2(X) = 0$ se e soltanto se $q_2(X) - q_1(X) = 0$. Ma, se fosse $r_1(X) - r_2(X) \neq 0$, almeno un polinomio tra $r_1(X)$ e $r_2(X)$ sarebbe necessariamente non nullo ed inoltre, per la formula del grado, si avrebbe:

$$\deg(r_1(X) - r_2(X)) = \deg(g(X)) + \deg(q_2(X) - q_1(X)) \geq \deg(g(X)) ;$$

in contraddizione con l'ipotesi su $r_1(X)$ e $r_2(X)$ (ognuno di essi o è nullo oppure è di grado inferiore a quello di $g(X)$) .

Esempi.

4. Sia $f(X) := 3X^3 - 2X^2 + 2X + 2$ e $g(X) := X^2 - X + 1$. Allora $q_1(X) = 3X$ e $f_1(X) := f(X) - g(X)q_1(X) = X^2 - X + 2$. Dunque $q_2(X) = 1$ e $f_2(X) := f_1(X) - g(X)q_2(X) = 1$. Ne segue che $q(X) := q_1(X) + q_2(X) = 3X + 1$ e $r(X) = := f(X) - g(X)q(X) = 1$. In conclusione, $f(X) = (3X+1)g(X) + 1$.

Se K è un campo, per il Teorema precedente, è sempre possibile effettuare la divisione col resto tra due polinomi non nulli di $K[X]$. Inoltre se F è un sottocampo di K e $f(X)$ e $g(X)$ sono due polinomi non nulli di $F[X]$, per l'unicità del quoziente e del resto si ha che $g(X)$ divide $f(X)$ in $F[X]$ se e soltanto se lo divide in $K[X]$.

Un polinomio non nullo $f(X) \in A[X]$ si dice *monico* se il suo coefficiente direttore è uguale a 1. Notiamo che, se il coefficiente direttore u di $f(X)$ è invertibile in A, allora $u^{-1}f(X)$ è l'unico polinomio monico associato a $f(X)$ in $A[X]$. Se in particolare K è un campo, ogni polinomio di $K[X]$ è associato a un (unico) polinomio monico di $K[X]$.

Teorema 3.4 (Esistenza e unicità del massimo comune divisore in K[X]). Sia K un campo e siano $f(X), g(X) \in K[X]$ due polinomi non nulli. Allora esiste un unico polinomio monico $d(X)$ tale che:

1) $d(X)$ divide $f(X)$ e $g(X)$;
2) ogni divisore comune di $f(X)$ e $g(X)$ divide $d(X)$.

Inoltre esistono due polinomi $h(X), k(X) \in K[X]$ tali che

$$d(X) = h(X)f(X) + k(X)g(X) \qquad (\textit{identità di Bezout per i polinomi}).$$

Tale polinomio monico $d(X)$ si chiama il *massimo comune divisore* di $f(X)$ e $g(X)$ e si scrive $d(X) = MCD(f(X), g(X))$.

Dimostrazione. Sia

$$I := \{\lambda(X)f(X) + \mu(X)g(X) ;\ \lambda(X), \mu(X) \in K[X],\ \lambda(X)f(X) + \mu(X)g(X) \neq 0\}.$$

I contiene sia $f(X)$ che $g(X)$ perchè, per esempio, $f(X) = 1f(X) + 0g(X)$. I gradi dei polinomi appartenenti ad I formano un insieme non vuoto di interi non negativi, dunque, per il Principio del Buon Ordinamento dei numeri naturali, esiste un polinomio $m(X)$ di grado minimo in I. Mostriamo che ogni tale polinomio $m(X)$ soddisfa le proprietà 1) e 2).

Chiaramente ogni divisore comune di $f(X)$ e $g(X)$ divide ogni polinomio di I e quindi divide anche $m(X)$. Resta da provare che $m(X)$ divide $f(X)$ e $g(X)$. Per l'algoritmo della divisione tra polinomi, si ha che $f(X) = m(X)q(X) + r(X)$ con $r(X) = 0$ oppure $\deg(r(X)) < \deg(d(X))$; inoltre, poichè $m(X) \in I$, abbiamo che $m(X) = h(X)f(X) + k(X)g(X)$ con $h(X), k(X) \in K[X]$. Allora

$$r(X) = f(X) - m(X)q(X) = f(X) - (h(X)f(X) + k(X)g(X)) = (1 - h(X))f(X) - k(X)g(X)$$

e, se $r(X)$ fosse diverso da 0, si avrebbe $r(X) \in I$ e $\deg(r(X)) < \deg(m(X))$. Per la minimalità del grado di $m(X)$, possiamo concludere che $r(X) = 0$. Così $m(X)$ divide $f(X)$ e analogamente divide $g(X)$.

Notiamo ora che tutti i polinomi associati a $m(X)$ in $K[X]$ stanno in I e, avendo grado minimo (Corollario 3.2), soddisfano ancora le proprietà 1) e 2). Ne segue che in I c'è un unico polinomio monico $d(X)$ con queste proprietà.

Per concludere, facciamo vedere che ogni polinomio (monico) $p(X) \in K[X]$ con le proprietà 1) e 2) sta in I. Questo segue dal fatto che, essendo $m(X)$ un divisore comune

di $f(X)$ e $g(X)$, per la proprietà 2), $m(X)$ divide $p(X)$. Allora, se $p(X) = m(X)q(X)$, con $q(X) \in K[X]$, risulta

$$p(X) = m(X)q(X) = (h(X)f(X) + k(X)g(X))q(X) = (h(X)\,q(X))f(X) + (k(X)\,q(X))g(X).$$

Vogliamo ora illustrare un metodo per determinare il massimo comune divisore di due polinomi.

Lemma 3.5. Sia K un campo e siano $f(X), g(X) \in K[X]$ due polinomi non nulli. Se $f(X) = g(X)q(X) + r(X)$ con $r(X) \neq 0$, allora $MCD(f(X), g(X)) = MCD(g(X), r(X))$.

Dimostrazione. Siano $d(X) := MCD(f(X), g(X))$ e $d'(X) = MCD(g(X), r(X))$. Si verifica subito che $d(X)$ divide $r(X)$ e $d'(X)$ divide $f(X)$. Dunque, per la proprietà 2) del massimo comune divisore, $d(X)$ divide $d'(X)$ e viceversa. Ne segue che $d(X)$ e $d'(X)$ hanno uguale grado; quindi, se ad esempio $d(X) = d'(X)q(X)$, $q(X)$ deve essere una costante. Ma poiché $d(X)$ e $d'(X)$ sono monici, allora $q(X) = 1$ e $d(X) = d'(X)$.

Proposizione 3.6 (Algoritmo euclideo per il calcolo del massimo comune divisore in K[X]). Sia K un campo e siano $f(X), g(X) \in K[X]$ due polinomi non nulli. Supponiamo che:

$$f(X) = g(X)q_1(X) + r_1(X) \qquad r_1(X) = 0 \text{ oppure } \deg(r_1(X)) < \deg(g(X));$$

$$g(X) = r_1(X)q_2(X) + r_2(X) \qquad r_2(X) = 0 \text{ oppure } \deg(r_2(X)) < \deg(r_1(X));$$

$$\dots$$

$$r_i(X) = r_{i+1}(X)q_{i+2}(X) + r_{i+2}(X) \qquad r_{i+2}(X) = 0 \text{ oppure } \deg(r_{i+2}(X)) < \deg(r_{i+1}(X));$$

$$\dots\dots$$

$$r_{n-2}(X) = r_{n-1}(X)q_n(X) + r_n(X) \qquad r_n(X) = 0 \text{ oppure } \deg(r_n(X)) < \deg(r_{n-1}(X));$$

$$r_{n-1}(X) = r_n(X)q_{n+1}(X);$$

e poniamo $r_0(X) = g(X)$. Allora $d(X) := MCD(f(X), g(X))$ è il polinomio monico associato a $r_n(X)$.

Inoltre, partendo dalla penultima divisione e risalendo verso la prima, si ottiene una successione di uguaglianze:

$$r_n(X) = r_{n-2}(X) - q_n(X)r_{n-1}(X);$$

$$r_n(X) = (1 + q_n(X)q_{n+1}(X))r_{n-2}(X) + (-q_n(X))r_{n-3}(X);$$

$$\dots\dots$$

l'ultima delle quali determina esplicitamente una identità di Bézout.

Dimostrazione. Poiché $\deg(g(X)) > \deg(r_1(X)) > \deg(r_2(X)) > \cdots$, allora esiste un numero naturale n tale che $r_n(X) \neq 0$ e $r_{n+1}(X) = 0$.

Poiché $r_{n-1}(X)$ è divisibile per $r_n(X)$, si ha che il polinomio monico associato ad $r_n(X)$ è uguale a $MCD(r_n(X), r_{n-1}(X))$. Risalendo nella catena di uguaglianze, per il Lemma 3.5 si conclude che

$$r_n(X) = MCD(r_n(X), r_{n-1}(X)) = MCD(r_{n-1}(X), r_{n-2}(X)) = \ldots = MCD(f(X), g(X)).$$

Due polinomi non nulli $f(X), g(X) \in K[X]$ tali che $MCD(f(X), g(X)) = 1$ si dicono *relativamente primi* o *coprimi.*

Esempi.

5. Siano $f(X) := X^4 - X^3 - 4X^2 + 4X + 1$ e $g(X) := X^2 - X - 1$. Si ottiene

$$f(X) = g(X)(X^2 - 3) + (X - 2);$$
$$g(X) = (X - 2)(X + 1) + 1.$$

Dunque $MCD(f(X), g(X) = 1$ ed inoltre una identità di Bezout si ottiene nel seguente modo:

$$(X - 2) = f(X) - (X^2 - 3)g(X);$$
$$1 = g(X) - (X + 1)(X - 2) = g(X) - (X + 1)[f(X) - (X^2 - 3)g(X)]$$
$$= -(X + 1)f(X) + (X^3 + X^2 - 3X - 2)g(X).$$

6. Siano $f(X) := 2X^3 + X^2 + X - 1$ e $g(X) := 2X^3 - 7X^2 + 7X - 2$. Si ottiene

$$f(X) = g(X) + (8X^2 - 6X + 1);$$
$$g(X) = (8X^2 - 6X + 1)(\frac{1}{4}X - \frac{11}{16}) + (\frac{21}{8}X - \frac{21}{16});$$
$$(8X^2 - 6X + 1) = (\frac{21}{8}X - \frac{21}{16})(\frac{64}{21}X - \frac{16}{21}).$$

Allora risulta $MCD(f(X), g(X) = (X - \frac{1}{2})$ ed inoltre una identità di Bezout si ottiene nel seguente modo:

$$(8X^2 - 6X + 1) = f(X) - g(X);$$
$$(\frac{21}{8}X - \frac{21}{16}) = g(X) - (\frac{1}{4}X - \frac{11}{16})(8X^2 - 6X + 1)$$
$$= g(X) - (\frac{1}{4}X - \frac{11}{16})[f(X) - g(X)]$$
$$= -(\frac{1}{4}X - \frac{11}{16})f(X) + (\frac{1}{4}X + \frac{5}{16})g(X);$$

da cui

$$(X - \frac{1}{2}) = \frac{8}{21}(\frac{21}{8}X - \frac{21}{16}) = [-\frac{8}{21}(\frac{1}{4}X - \frac{11}{16})]f(X) + [\frac{8}{21}(\frac{1}{4}X + \frac{5}{16})]g(X).$$

Corollario 3.7. Siano K un campo e F un suo sottocampo. Siano $f(X), g(X) \in F[X]$ due polinomi non nulli. Allora il massimo comune divisore di $f(X)$ e $g(X)$ in $F[X]$ coincide con il massimo comune divisore di $f(X)$ e $g(X)$ in $K[X]$.

Dimostrazione. Segue dalla Proposizione 3.6 e dal fatto che il quoziente e il resto della divisione euclidea sono unici (Proposizione 3.3).

Il corollario precedente ci assicura che il massimo comune divisore di due polinomi a coefficienti numerici non dipende dal campo dei coefficienti.

ESERCIZI.

1. Dimostrare che, se R è un anello commutativo unitario, l'insieme $U(R)$ degli elementi invertibili di R è un gruppo moltiplicativo.

2. Dimostrare che, se R è un anello commutativo unitario, la relazione ρ su $R \setminus \{0\}$ definita da:

$$a \rho b \Leftrightarrow a \text{ e } b \text{ sono associati}$$

è una relazione di equivalenza.

3. Dimostrare che, se R è un dominio, a è associato a b in R se soltanto se a e b si dividono reciprocamente in R.

4. Dimostrare che, se A è un dominio, $U(A[X_1, \ldots, X_n]) = U(A)$, per ogni $n \geq 1$ (Sugg. Usare la Proposizione 3.1 e procedere per induzione su n).

5. Mostrare che il polinomio $2X^3 + 2X + 3$ è invertibile in $\mathbf{Z}_8[X]$, determinando esplicitamente il suo inverso.

6. Sia $f(X)$ uno dei seguenti polinomi:

$$15X \; ; \; 15X + 3 \; ; \; 6X^2 - 5X + 1 \; ; \; 6X^3 - 7X^2 - X + 2 .$$

Determinare esplicitamente tutti i divisori di $f(X)$ in $\mathbf{Z}[X]$ e $\mathbf{Q}[X]$ e ripartirli in classi di polinomi associati in $\mathbf{Z}[X]$ e $\mathbf{Q}[X]$.

7. Stabilire se le seguenti affermazioni sono vere o false in $\mathbf{Z}[X]$ e $\mathbf{Q}[X]$:

(a) $5X$ divide $3X^2$;

(b) $X - 3$ divide $X^3 - 3X^2 + X - 3$;

(c) $3(X - 3)$ divide $X^3 - 3X^2 + X - 3$.

8. Determinare il quoziente e il resto della divisione di $f(X)$ per $g(X)$ nei seguenti casi:

(a) $f(X) = 5X^6 + 2X^4 - 3X^2 - 2$, $\quad g(X) = -X^3 + 2X^2 + 5X - 7$ in $\mathbf{Z}[X]$;

(b) $f(X) = 3X^7 - 2X^5 - 3X^3 - 2X + 1$, $\quad g(X) = \frac{2}{5}X^4 - 2X^2 + \frac{1}{7}$ in $\mathbf{Q}[X]$;

(c) $f(X) = 2X^4 + 3X^3 - 3X^2 - 2X + 1$, $\quad g(X) = 4X^3 + X^2 - X + 1$ in $\mathbf{Z}_5[X]$.

9. Determinare il massimo comune divisore e una identità di Bezout per le seguenti coppie di polinomi:

(a) $f(X) = X^5 - \frac{1}{3}X^4 - \frac{1}{2}X + \frac{1}{6}$, $\quad g(X) = X^3 + \frac{2}{3}X^2 + \frac{2}{3}X - \frac{1}{3}$ in $\mathbf{Q}[X]$;

(b) $f(X) = X^4 - 1$, $\quad g(X) = X^3 - 2X^2 + X - 2$ in $\mathbf{R}[X]$;

(c) $f(X) = 2X^3 + 4X^2 + 3X + 2$, $\quad g(X) = 3X^4 + X + 4$ in $\mathbf{Z}_5[X]$;

(d) $f(X) = X^4 - 1$, $\quad g(X) = X^3 - 2X^2 + X - 2$ in $\mathbf{Z}_3[X]$.

4. Radici di polinomi.

Per ogni $\alpha \in A^n$, si può definire l'applicazione $v_\alpha : A[\mathbf{X}] \longrightarrow A$, $f(X) \longrightarrow f(\alpha)$, che ad ogni polinomio di $A[\mathbf{X}] := A[X_1, \ldots, X_n]$ associa il suo valore in α. Notiamo che, se $c \in A$ è un polinomio costante, allora $v_\alpha(c) = c$.

E' facile verificare che l'applicazione v_α è un omomorfismo di anelli; infatti risulta

$$(f+g)(\alpha) = f(\alpha)+g(\alpha) \quad \text{e} \quad (fg)(\alpha) = f(\alpha)g(\alpha).$$

Un elemento $\alpha \in A^n$ tale che $f(\alpha) = 0$ si dice una *radice* (o uno *zero*) di $f(\mathbf{X})$. Ogni elemento di A^n è trivialmente radice del polinomio nullo, mentre i polinomi costanti non nulli non hanno radici.

Studieremo particolarmente il caso dei polinomi in una indeterminata su A. E' bene osservare subito che, se $f(X) \in A[X]$ e B è un dominio tale che $A \subseteq B$, allora $f(X)$ è anche un polinomio di $B[X]$ ed esso può avere radici in B anche se non ne ha in A.

Proposizione 4.1 (Teorema del Resto, o di Ruffini). Sia $f(X) \in A[X]$ un polinomio di grado $n \geq 1$ e sia $\alpha \in A$. Allora il resto della divisione di $f(X)$ per $(X-\alpha)$ è $f(\alpha)$.

Dimostrazione. Per l'algoritmo della divisione tra polinomi (Teorema 3.3), $f(X) = (X-\alpha)q(X) + r(X)$ con $r(X) = 0$ oppure $\deg(r(X)) < 1$. Quindi $r(X)$ è un polinomio costante c. Calcolando in α si ottiene $f(\alpha) = c$.

Corollario 4.2. Sia $f(X) \in A[X]$ un polinomio di grado $n \geq 1$ e sia $\alpha \in A$. Allora α è una radice di $f(X)$ se e soltanto se $(X-\alpha)$ divide $f(X)$ in $A[X]$. Inoltre $f(X)$ ha al più n radici in A.

Dimostrazione. La prima parte segue subito dalla proposizione precedente.

Per la seconda parte, procediamo per induzione sul grado n di $f(X)$. E' evidente che se $f(X) := aX + b$ è di primo grado, esso ha al più una radice: infatti se $a\alpha + b = a\beta + b$, allora $\alpha = \beta$. Supponiamo che $f(X)$ abbia grado $n \geq 1$ e sia α una radice di $f(X)$; allora $f(X) = (X-\alpha)q(X)$ con $\deg(q(X)) = n - 1$. Per l'ipotesi induttiva, $q(X)$ ha al più $n-1$ radici in A. Ma, poichè A è un dominio, una radice di $f(X)$ è una radice di $q(X)$ oppure è l'unica radice α di $X-\alpha$. Quindi $f(X)$ ha al più n radici.

Esempi.

1. Regola di Ruffini. Sia $f(X) := c_0 + c_1X + \ldots + c_nX^n \in A[X]$ un polinomio di grado $n \geq 1$ e sia $\alpha \in A$. Per l'algoritmo della divisione tra polinomi, esistono e sono univocamente determinati due polinomi $q(X)$ e $r(X)$ tali che $f(X) = (X-\alpha)q(X) + r(X)$, dove $r(X)$ è un polinomio costante ed inoltre, per il teorema del resto, $r(X) = f(\alpha)$. Per le proprietà del grado, $q(X) := b_0 + b_1X + \ldots + b_{n-1}X^{n-1}$ è un polinomio di grado $n-1$ e, uguagliando i coefficienti dei due polinomi a primo e secondo membro dell'uguaglianza, i coefficienti di $q(X)$ soddisfano le seguenti uguaglianze:

$b_{n-1} = c_n$,
$b_k = c_{k+1} + \alpha b_{k+1}$ per $0 \le k \le n - 2$,
$f(\alpha) = c_0 + \alpha b_0$.

Pertanto $(X-\alpha)$ divide $f(X)$ se e soltanto se $c_0 = -\alpha b_0$.

Per determinare i coefficienti b_k , si usa fare ricorso alla seguente tabella:

	c_n	c_{n-1}	c_{n-2}	.....	c_1	c_0
α		αb_{n-1}	αb_{n-2}	.....	αb_1	αb_0
	$b_{n-1} = c_n$	$b_{n-2} = c_{n-1} + \alpha b_{n-1}$	$b_{n-3} = c_{n-2} + \alpha b_{n-2}$	.....	$b_0 = c_1 + \alpha b_1$	$f(\alpha) = c_0 + \alpha b_0$

2. Sia $f(X) := c_0 + c_1X + \ldots + c_nX^n \in \mathbf{Z}[X]$, $c_n \neq 0$. Se $\alpha := a/b$ è una radice razionale di $f(X)$ con a e b primi tra loro, allora a divide c_0 e b divide c_n . In particolare, se $f(X)$ è monico, le eventuali radici razionali di $f(X)$ sono intere.

Infatti, se $q(X) := b_0 + b_1X + \ldots + b_{n-1}X^{n-1}$ è il quoziente della divisione di $f(X)$ per $X - \alpha$, dalle uguaglianze ottenute nell'esercizio precedente, si ha

$$c_0 + (a/b)b_0 = 0 \text{ , da cui } ab_0 = bc_0$$

e, poiché $MCD(a, b) = 1$, allora a divide c_0 . Inoltre

$$b_k = c_{k+1} + (a/b)b_{k+1} \text{ , da cui } bb_k = bc_{k+1} + ab_{k+1} \text{ per } 0 \le k \le n - 2 .$$

Perciò b divide ab_{k+1} e, poiché $MCD(a, b) = 1$, allora b divide b_{k+1} ; in particolare, per $k = n - 2$, b divide $b_{n-1} = c_n$.

Corollario 4.3. Se $f(X)$, $g(X) \in A[X]$ sono polinomi di grado al più uguale a n e se $a_1, a_2, \ldots, a_{n+1}$ sono elementi distinti di A tali che $f(a_i) = g(a_i)$ per $i = 1, 2, \ldots, n+1$, allora $f(X) = g(X)$.

Dimostrazione. Se fosse $f(X) \neq g(X)$, allora $f(X) - g(X)$ sarebbe un polinomio non nullo di grado al più uguale ad n con almeno $n+1$ radici, in contraddizione con il Corollario 4.2.

Il seguente corollario mostra che, se A è infinito, è lecito identificare un polinomio su A con la sua corrispondente funzione polinomiale, come accennato alla fine del Paragrafo 2.

Corollario 4.4. Sia A infinito e siano $f(X)$, $g(X) \in A[X]$. Se $f(\alpha) = g(\alpha)$ per ogni $\alpha \in A$, allora $f(X) = g(X)$.

Dimostrazione. Se $f(\alpha) = g(\alpha)$ per ogni $\alpha \in A$, allora il polinomio differenza $h(X) := f(X)-g(X)$ si annulla su tutto A . Essendo A infinito, per il Corollario 4.2. $h(X)$ deve essere un polinomio costante, e quindi $h(X)$ è il polinomio nullo.

Per induzione su n , il corollario precedente si può estendere agli anelli di polinomi in n indeterminate su A.

Se $f(X) \in A[X]$ e $\alpha \in A$ è una radice di $f(X)$, per la Proposizione 4.1 e la formula del grado, esiste un intero m, compreso tra 1 e $\deg(f(X))$, tale che $(X-\alpha)^m$ divide $f(X)$ mentre $(X-\alpha)^{m+1}$ non lo divide. Se $m \geq 2$, α si dice una *radice multipla* di $f(X)$ (di *molteplicità* m), altrimenti α si dice una *radice semplice*.

Se $f(X) := c_0 + c_1X + \ldots + c_nX^n \in A[X]$, indichiamo con $f'(X)$ la *derivata formale* di $f(X)$, ovvero il polinomio $f'(X) := c_1 + 2c_2X + \ldots + nc_nX^{n-1}$.

Notiamo che $f'(X) \in A[X]$ e che nel caso numerico (più in generale in caratteristica zero) $f'(X) = 0$ se e soltanto se $f(X)$ è un polinomio costante. Tuttavia può accadere in generale che la derivata di un polinomio non costante sia il polinomio nullo. Ad esempio, se $f(X) := X^n - 1 \in \mathbf{Z}_p[X]$ e p divide n, si ha $f'(X) = nX^{n-1} = 0$.

Se $A = \mathbf{R}$ è il campo dei numeri reali, la derivata formale del polinomio $f(X)$ corrisponde alla funzione derivata della funzione reale φ_f corrispondente a $f(X)$ (Paragrafo 2). Come nel caso reale, valgono le seguenti proprietà:

$$(f+g)'(X) = f'(X) + g'(X) \; ; \; (fg)'(X) = f'(X)g(X) + f(X)g'(X) \; ;$$
$$(f\circ g)'(X) = (f'\circ g)(X)g'(X) = f'(g(X))g'(X) \; .$$

Proposizione 4.5. Sia $f(X) \in A[X]$ e sia $\alpha \in A$ una radice di $f(X)$. Allora α è una radice multipla di $f(X)$ se e soltanto se $f'(\alpha) = 0$.

Dimostrazione. Per definizione, α è una radice multipla di $f(X)$ se e soltanto se $(X-\alpha)^2$ divide $f(X)$ in $A[X]$. Se $f(X) = (X-\alpha)^2g(X)$, passando alle derivate formali si ottiene

$$f'(X) = 2(X-\alpha)g(X)+(X-\alpha)^2g'(X) \; .$$

Quindi $f'(\alpha) = 0$.

Viceversa, se $f(\alpha) = f'(\alpha) = 0$, allora $(X-\alpha)$ divide sia $f(X)$ che $f'(X)$ (Corollario 4.2). Se $f(X) = (X-\alpha)h(X)$, si ottiene $f'(X) = h(X)+(X-\alpha)h'(X)$. Poiché $(X-\alpha)$ divide $f'(X)$, ne segue che $(X-\alpha)$ divide $h(X)$ e allora $(X-\alpha)^2$ divide $f(X)$.

Corollario 4.6. Siano K un campo e $f(X) \in K[X]$. Se $f(X)$ ha una radice multipla in K, allora $\mathrm{MCD}(f(X), f'(X)) \neq 1$.

Il seguente importante teorema fu dimostrato per la prima volta in modo completo nel 1797 da C. F. Gauss nella sua Tesi di Laurea e fu pubblicato nel 1799.

Teorema 4.7 (Teorema Fondamentale dell'Algebra). Sia $f(X)$ un polinomio non costante a coefficienti numerici. Allora $f(X)$ ha una radice in $\mathbf{C}$.

Corollario 4.8. Sia $f(X)$ un polinomio a coefficienti numerici di grado $n \geq 1$. Allora

$$f(X) = u(X-\alpha_1)^{m_1}\ldots(X-\alpha_s)^{m_s}$$

dove $u, \alpha_i \in \mathbf{C}$, $u \neq 0$, $1 \leq s \leq n$ e $m_1 + \ldots + m_s = n$.

Dimostrazione. Segue dal Teorema 4.7, dal Corollario 4.2 e dalla formula del grado.

Talvolta si usa esprimere il Corollario precedente dicendo che un polinomio di grado n a coefficienti numerici ha esattamente n radici complesse "contate con la loro molteplicità".

Corollario 4.9. Sia K un campo numerico, e sia $f(X) \in K[X]$. Allora $f(X)$ ha una radice complessa multipla se e soltanto se $d(X) := MCD(f(X), f'(X)) \neq 1$ in $K[X]$. In questo caso, le radici complesse multiple di $f(X)$ sono esattamente le radici del polinomio $d(X)$.

Dimostrazione. Per il Corollario 3.7, Il polinomio $d(X)$ è anche il massimo comune divisore di $f(X)$ e $f'(X)$ in $\mathbf{C}[X]$. Possiamo allora concludere per la Proposizione 4.5 e il Teorema Fondamentale dell'Algebra.

Se $\alpha := a + bi \in \mathbf{C}$, indichiamo al solito con $\overline{\alpha}$ il *coniugato* di α, ovvero $\overline{\alpha} = a - bi$. E' immediato verificare che se $\alpha, \beta \in \mathbf{C}$, allora $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ e $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$. Inoltre $\overline{\alpha} = \alpha$ se e solo se α è un numero reale. Se $f(X) \in \mathbf{C}[X]$, denotiamo con $\overline{f}(X)$ il polinomio che si ottiene da $f(X)$ coniugando i suoi coefficienti.

Proposizione 4.10. Sia $f(X) \in \mathbf{R}[X]$. Se $\alpha \in \mathbf{C}$ è una radice di $f(X)$ di molteplicità m, allora anche $\overline{\alpha}$ è una radice di $f(X)$ di molteplicità m.

Dimostrazione. Possiamo supporre che α non sia reale. Sia $f(X) := c_0 + c_1X + \ldots + c_nX^n$. Poiché $0 = f(\alpha)$, passando ai coniugati, si ottiene

$$0 = \overline{f(\alpha)} = \overline{c_0 + c_1\alpha + \ldots + c_n\alpha^n} = \overline{c_0} + \overline{c_1\alpha} + \ldots + \overline{c_n\alpha^n} = \\ = c_0 + c_1\overline{\alpha} + \ldots + c_n(\overline{\alpha})^n$$

da cui $f(\overline{\alpha}) = 0$.

Sia k la molteplicità di $\overline{\alpha}$; allora

$$f(X) = (X - \alpha)^m(X - \overline{\alpha})^k g(X) \text{ con } g(\alpha) \neq 0 \text{ e } g(\overline{\alpha}) \neq 0.$$

Inoltre, poichè $f(X) \in \mathbf{R}[X]$, si ha che

$$f(X) = \overline{f}(X) = (X - \overline{\alpha})^m(X - \alpha)^k\overline{g}(X), \text{ con } \overline{g}(\overline{\alpha}) = \overline{g(\alpha)} \neq 0 \text{ e } \overline{g}(\alpha) = \overline{g(\overline{\alpha})} \neq 0.$$

Se $m > k$, per la legge di cancellazione, otteniamo

$$(X - \alpha)^{m-k}(X - \overline{\alpha})^k g(X) = (X - \overline{\alpha})^m\overline{g}(X)$$

e, calcolando in α, $\overline{g}(\alpha) = 0$, in contraddizione con l'ipotesi $\overline{g}(\alpha) \neq 0$.

Analogamente, se $m < k$, otteniamo

$$(X - \overline{\alpha})^k g(X) = (X - \overline{\alpha})^m (X - \alpha)^{k-m}\overline{g}(X),$$

il che non è possibile perché $g(\alpha) \neq 0$. Dunque $m = k$.

Il seguente Corollario è immediato.

Corollario 4.11. Sia $f(X) \in \mathbf{R}[X]$.

(a) Se $\deg(f(X))$ è dispari, allora $f(X)$ ha almeno una radice reale ed il numero delle sue radici reali è dispari.

(b) Se deg(f(X)) è pari, il numero delle radici reali di f(X) è pari (eventualmente nullo).

La seguente regola può essere utile per limitare il numero delle possibili radici reali di un polinomio f(X) a coefficienti reali.

Diciamo che f(X) ha una *variazione* (*di segno*) se due suoi termini consecutivi non nulli hanno segno opposto; diciamo invece che f(X) ha una *permanenza* (*di segno*) se due suoi termini consecutivi non nulli hanno segno uguale. Ad esempio, se $f(X) := X^5 - X^4 + X^3 + X - 1$, la successione dei segni dei termini non nulli di f(X) è + - + + -, dunque f(X) ha tre variazioni e una permanenenza di segno.

Proposizione 4.12 (Regola dei segni di Descartes). Sia $f(X) \in \mathbf{R}[X]$. Allora

(a) Il numero delle radici reali positive di f(X) è al più uguale al numero delle sue variazioni.

(b) Il numero delle radici reali negative di f(X) è al più uguale al numero delle variazioni del polinomio f(-X).

La dimostrazione della proposizione precedente si basa sulle proprietà analitiche delle funzioni reali polinomiali e perciò la omettiamo. Notiamo comunque che la validità della regola di Descartes può essere verificata osservando che, moltiplicando f(X) per un termine X-a, con a reale positivo, si ottiene un polinomio che ha almeno una variazione di segno in più rispetto a f(X).

Esempi.

3. Radici complesse di numeri complessi. Se $z \in \mathbf{C}$, le radici complesse del polinomio $f(X) := X^n - z$ si dicono le *radici complesse n-sime* di z. Se $z \neq 0$, allora $f'(X) = nX^{n-1}$ non ha radici in comune con f(X), quindi tali radici sono tutte distinte. Per determinarle, si possono usare le formule di De Moivre per la moltiplicazione dei numeri complessi in forma trigonometrica: se

$$z_1 = \rho_1(\cos(\theta_1) + i \operatorname{sen}(\theta_1)) \quad \text{e} \quad z_2 = \rho_2(\cos(\theta_2) + i \operatorname{sen}(\theta_2)),$$

con ρ_1, ρ_2 numeri reali positivi, allora

$$z_1 z_2 = \rho_1\rho_2(\cos(\theta_1+\theta_2) + i \operatorname{sen}(\theta_1+\theta_2));$$

notiamo che, in particolare, moltiplicando un numero complesso z per un numero complesso di modulo 1, si ottiene un numero complesso che ha lo stesso modulo di z.

Sia dunque $z := \rho(\cos(\theta) + i \operatorname{sen}(\theta))$, se $\zeta := \sigma(\cos(\varphi) + i \operatorname{sen}(\varphi))$ è radice del polinomio f(X), cioè ζ è una radice n-sima di z, deve risultare:

$$\sigma^n(\cos(n\varphi) + i \operatorname{sen}(n\varphi)) = \rho(\cos(\theta) + i \operatorname{sen}(\theta)),$$

da cui $\sigma^n = \rho$ e $n\varphi = \theta + 2k\pi$, $k \in \mathbf{Z}$, ovvero

$$\sigma = \sqrt[n]{\rho} \quad \text{e} \quad \varphi = \frac{\theta + 2k\pi}{n}.$$

Notiamo ora che, se $k \in \mathbf{Z}$ e $k = nq + r$ con $0 \le r < n$, risulta

$$\frac{\theta + 2k\pi}{n} = \frac{\theta + 2r\pi}{n} + 2q\pi$$

e dunque le funzioni trigonometriche di $\frac{\theta + 2k\pi}{n}$ e $\frac{\theta + 2r\pi}{n}$ sono le stesse. Ne segue che le radici n-sime di z si ottengono per $k = 0, 1, \ldots, n-1$ e sono:

$$\zeta_0 := \sqrt[n]{\rho}(\cos(\frac{\theta}{n}) + i\,\mathrm{sen}(\frac{\theta}{n}));$$

$$\zeta_1 := \sqrt[n]{\rho}(\cos(\frac{\theta + 2\pi}{n}) + i\,\mathrm{sen}(\frac{\theta + 2\pi}{n}));$$

$$\zeta_2 := \sqrt[n]{\rho}(\cos(\frac{\theta + 4\pi}{n}) + i\,\mathrm{sen}(\frac{\theta + 4\pi}{n}));$$

.....

$$\zeta_{n-1} := \sqrt[n]{\rho}(\cos(\frac{\theta + 2(n-1)\pi}{n}) + i\,\mathrm{sen}(\frac{\theta + 2(n-1)\pi}{n})).$$

Notiamo che questi numeri complessi si rappresentano nel piano di Gauss come i vertici di un poligono regolare di n lati con centro nell'origine e un vertice in ζ_0.

Ad esempio, le radici quadrate di $3i = 3(\cos(\frac{\pi}{2}) + i\,\mathrm{sen}(\frac{\pi}{2}))$ sono:

$$\zeta_0 := \sqrt{3}(\cos(\frac{\pi}{4}) + i\,\mathrm{sen}(\frac{\pi}{4})) = \frac{\sqrt{6}}{2} + \frac{\sqrt{6}}{2}\,i$$

$$\zeta_1 := \sqrt{3}(\cos(\frac{5\pi}{4}) + i\,\mathrm{sen}(\frac{5\pi}{4})) = -\frac{\sqrt{6}}{2} - \frac{\sqrt{6}}{2}\,i.$$

Invece le radici terze di $1 + i = \sqrt{2}(\cos(\frac{\pi}{4}) + i\,\mathrm{sen}(\frac{\pi}{4}))$ sono:

$$\zeta_0 := \sqrt[6]{2}(\cos(\frac{\pi}{12}) + i\,\mathrm{sen}(\frac{\pi}{12}));$$

$$\zeta_1 := \sqrt[6]{2}(\cos(\frac{3\pi}{4}) + i\,\mathrm{sen}(\frac{3\pi}{4}));$$

$$\zeta_2 := \sqrt[6]{2}(\cos(\frac{17\pi}{12}) + i\,\mathrm{sen}(\frac{17\pi}{12})).$$

4. Radici complesse n-sime dell'unità. Per $z := 1 = \cos(2\pi) + i\,\mathrm{sen}(2\pi)$, le formule precedenti forniscono le radici n-sime dell'unità, che sono:

$$\zeta_0 := \cos(\frac{2\pi}{n}) + i\,\mathrm{sen}(\frac{2\pi}{n});$$

$$\zeta_1 := \cos(\frac{4\pi}{n}) + i\,\mathrm{sen}(\frac{4\pi}{n});$$

$$\zeta_2 := \cos(\frac{6\pi}{n}) + i\,\mathrm{sen}(\frac{6\pi}{n});$$

.....

$$\zeta_{n-1} := \cos(2\pi) + i\,\mathrm{sen}(2\pi) = 1.$$

Per le formule di De Moivre, risulta

$$(\zeta_0)^k = \zeta_{k-1} = \cos(\frac{2k\pi}{n}) + i\,\mathrm{sen}(\frac{2k\pi}{n}), \quad \text{per } k = 1, \ldots, n .$$

Allora, posto $\xi := \zeta_0$, le radici n-sime dell'unità sono $\xi, \xi^2, \ldots, \xi^{n-1}, \xi^n = 1$.

Osserviamo anche che, se ζ è una qualsiasi radice n-sima del numero complesso z, per le formule di De Moivre, tutte le radici n-sime di z si possono scrivere come

$$\zeta\xi, \ \zeta\xi^2, \ \ldots, \ \zeta\xi^{n-1}, \ \zeta\xi^n .$$

Le radici n-sime dell'unità che non siano anche radici m-sime per qualche $m < n$, si dicono radici n-sime *primitive* dell'unità. Mostriamo ora che tali radici sono esattamente i numeri complessi $\xi^k = \cos(\frac{2k\pi}{n}) + i\,\mathrm{sen}(\frac{2k\pi}{n})$ con $1 \le k < n$ e $\mathrm{MCD}(n, k) = 1$. In particolare, se p è un numero primo, ogni radice p-sima dell'unità diversa da 1 è primitiva.

Se $\mathrm{MCD}(n, k) = d \neq 1$, si ha che $(\xi^k)^{n/d} = (\xi^{k/d})^n = 1$; dunque ξ^k è una radice m-sima dell'unità per $m := n/d < n$. Se invece $\mathrm{MCD}(n, k) = 1$ e $1 = an + bk$ è una identità di Bezout, si ha che $\xi = \xi^{(an+bk)} = \xi^{bk}$ è una potenza di ξ^k e perciò ogni radice n-sima dell'unità è anche potenza di ξ^k. Inoltre, essendo le prime n potenze di ξ tutte distinte, anche le prime n potenze di ξ^k sono tutte distinte. Infatti, se $\xi^i = \xi^{bki} \neq \xi^{bkj} = \xi^j$, deve essere $\xi^{ki} \neq \xi^{kj}$. Ne segue che possiamo scrivere le radici n-sime dell'unità come $\xi^k, \xi^{2k}, \ldots, \xi^{kn-1}, \xi^{kn} = 1$ e in particolare ξ^k è una radice n-sima primitiva.

Il numero delle radici n-sime primitive è allora il numero dei numeri naturali minori di n e primi con n. Tale numero si indica con $\varphi(n)$ e la funzione

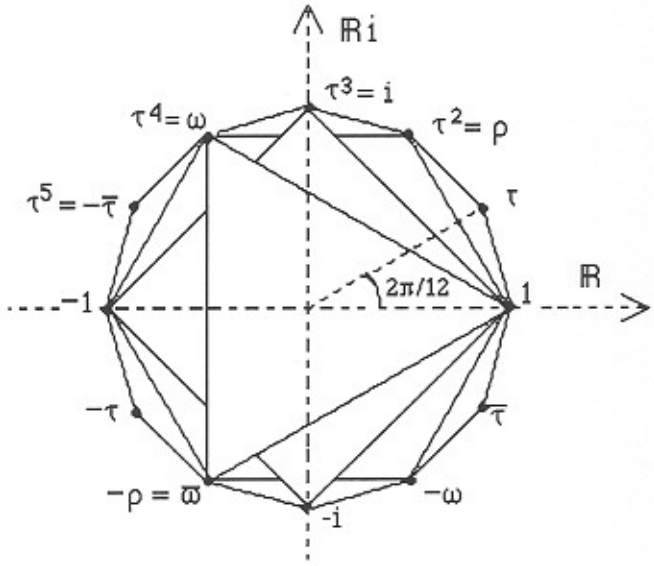
$$\mathbf{N} \longrightarrow \mathbf{N} \text{ definita da } 1 \longrightarrow 1, \ n \longrightarrow \varphi(n), \ \text{per } n \ge 2,$$

si dice la *funzione* o *indicatore di Eulero*. Se p è un numero primo, allora $\varphi(p) = p-1$.

Nel linguaggio della Teoria dei Gruppi, le radici n-sime dell'unità formano un gruppo moltiplicativo ciclico di ordine n i cui generatori sono le radici n-sime primitive.

Notiamo che le radici n-sime dell'unità rappresentano nel piano di Gauss i vertici di un poligono regolare di n-lati che abbia un vertice in 1. Inoltre, se m divide n, le radici m-sime rappresentano i vertici di un poligono regolare di m-lati che abbia ancora un vertice in 1 e sia inscritto nel primo.

Nella seguente figura, le potenze di τ sono le radici dodicesime, le potenze di $\rho := \tau^2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ sono le radici seste, le potenze di $i = \tau^3$ le radici quarte e infine le potenze di $\omega := \tau^4 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ le radici terze. Esse rappresentano rispettivamente i vertici di un dodecagono regolare, un esagono regolare, un quadrato e un triangolo equilatero con un vertice in 1.



Il polinomio a coefficienti numerici che ha per radici tutte e sole le radici n-sime primitive dell'unità si indica con $\Phi_n(X)$ e si dice l'n-simo *polinomio ciclotomico* (la parola ciclotomico deriva dal greco e significa "che taglia il cerchio"); il suo grado è $\varphi(n)$. Se p è un numero primo, si ha

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

allora, poiché le radici p-sime primitive dell'unità sono tutte quelle diverse da 1, risulta

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + 1 .$$

In generale si può dimostrare, per induzione su n, che $\Phi_n(X)$ ha coefficienti interi.

5. Radici complesse n-sime di un numero reale. La forma trigonometrica di un numero reale r positivo è $r = r(1) = r(\cos(2\pi) + i\,\mathrm{sen}(2\pi))$, mentre ogni numero reale r negativo si scrive in forma trigonometrica $r = |r|(-1) = |r|(\cos(\pi) + i\,\mathrm{sen}(\pi))$. Le radici complesse n-sime di un numero reale r si ottengono allora moltiplicando per $\sqrt[n]{|r|}$ le radici complesse n-sime di 1 o di -1, a seconda che r sia positivo o negativo. Nel primo caso, esse si dispongono nel piano di Gauss ai vertici di un poligono regolare di n lati con un vertice in $\sqrt[n]{r}$.

Le radici n-sime di -1 sono:

$$\zeta_0 := \cos(\frac{\pi}{n}) + i\,\mathrm{sen}(\frac{\pi}{n}) ;$$

$$\zeta_1 := \cos(\frac{3\pi}{n}) + i\,\mathrm{sen}(\frac{3\pi}{n}) ;$$

$$\zeta_2 := \cos(\frac{5\pi}{n}) + i\,\mathrm{sen}(\frac{5\pi}{n}) ;$$

.....

$$\zeta_{n-1} := \cos(\frac{(2n-1)\pi}{n}) + i\,\mathrm{sen}(\frac{(2n-1)\pi}{n}) .$$

Allora ad esempio, le radici terze di $-5 = 5((\cos(\pi) + i\,\mathrm{sen}(\pi))$ sono:

$$\zeta_0 := \sqrt[3]{5}\,(\cos(\frac{\pi}{3}) + i\,\mathrm{sen}(\frac{\pi}{3})) = \sqrt[3]{5}(\frac{1}{2} + \frac{\sqrt{3}}{2}i)\,;$$

$$\zeta_1 := \sqrt[3]{5}\,(\cos(\pi) + i\,\mathrm{sen}(\pi)) = -\sqrt[3]{5}\,;$$

$$\zeta_2 := \sqrt[3]{5}\,(\cos(\frac{5\pi}{3}) + i\,\mathrm{sen}(\frac{5\pi}{3})) = \sqrt[3]{5}(\frac{1}{2} - \frac{\sqrt{3}}{2}i) = \overline{\zeta_0}\,.$$

Invece le sue radici quarte sono:

$$\zeta_0 := \sqrt[4]{5}\,(\cos(\frac{\pi}{4}) + i\,\mathrm{sen}(\frac{\pi}{4})) = \sqrt[4]{5}(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i)\,;$$

$$\zeta_1 := \sqrt[4]{5}\,(\cos(\frac{3\pi}{4}) + i\,\mathrm{sen}(\frac{3\pi}{4})) = \sqrt[4]{5}(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i)\,;$$

$$\zeta_2 := \sqrt[4]{5}\,(\cos(\frac{5\pi}{4}) + i\,\mathrm{sen}(\frac{5\pi}{4})) = -\zeta_0 = \overline{\zeta_1}\,;$$

$$\zeta_3 := \sqrt[4]{5}\,(\cos(\frac{7\pi}{4}) + i\,\mathrm{sen}(\frac{7\pi}{4})) = \overline{\zeta_0} = -\zeta_1\,.$$

6. Il polinomio $f(X) := X^8 + 10X^3 + X - 4$ ha una sola variazione di segno, perciò ha al più una radice reale positiva. D'altra parte, anche il polinomio $f(-X) = X^8 - 10X^3 - X - 4$ ha una sola variazione di segno, perciò $f(X)$ ha al più una radice reale negativa. Ne segue che $f(X)$ ha almeno sei radici complesse non reali, coniugate a coppie.

Osserviamo poi che $f(X)$ ha effettivamente due radici reali; infatti $f(0) = -4 < 0$ e $f(1) = 8 > 0$. Dunque $f(X)$ ha una radice reale (positiva) e, per il Corollario 4.11 (b), ha anche un'altra radice reale (necessariamente negativa).

ESERCIZI.

1. Sia $f(X) := c_0 + c_1X + \ldots + c_nX^n \in \mathbf{Z}[X]$, $c_n \neq 0$. Dimostrare direttamente (senza usare la regola di Ruffini) che, se a/b è una radice razionale di $f(X)$, $MCD(a,b) = 1$, allora a divide c_0 e b divide c_n. In particolare, se $f(X)$ è monico, le eventuali radici razionali di $f(X)$ sono intere e dividono c_0 (Sugg. Sostituire a/b ad X e moltiplicare per b^n).

2. Sia $f(X) \in \mathbf{Z}[X]$ tale che $f(1) \neq 0$ e $f(-1) \neq 0$ e sia α una sua radice intera. Mostrare che $\dfrac{f(1)}{(1-\alpha)} \in \mathbf{Z}$ e $\dfrac{f(-1)}{(1+\alpha)} \in \mathbf{Z}$.

3. Trovare le radici razionali dei seguenti polinomi:

$$3X^4 - 8X^3 + 6X^2 - 3X - 2\ ;\ 5X^4 + 3X^3 + 3X^2 + 3X - 2\,.$$

4. Sia $f(X) := 7X^7 + 6X^6 + 5X^5 + 4X^4 + 3X^3 + 2X^2 + X + 1$. Calcolare $f(2)$ usando la regola di Ruffini.

5. Sia K un campo e sia $f(X) := a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$, $a_n \neq 0$. Mostrare che, se $\alpha \in K$ e $f(\alpha) \neq 0$, allora

$$f(X) = a_n(X-\alpha)^n + c_{n-1}(X-\alpha)^{n-1} + \ldots + c_1(X-\alpha) + f(\alpha)\,,$$

per opportuni $c_i \in K$, $i = 1, \ldots, n-1$.

6. Sia $f(X) \in \mathbf{Z}[X]$ tale che $f(1) \neq 0$, $f(-1) \neq 0$ e sia $\alpha := a/b$ una sua radice razionale, $MCD(a,b) = 1$. Mostrare che $(a-b)$ divide $f(1)$ e $(a+b)$ divide $f(-1)$ (Sugg.

Sviluppare $f(X)$ in potenze di $(X-1)$ e $(X+1)$, come nell'esercizio precedente, sostituire a/b a X e moltiplicare per b^n).

7. Stabilire se i seguenti polinomi hanno radici multiple:

$$3X^4 - 3X^3 - X^2 + 2X - 1 \; ; \quad X^4 - 3X^2 + 2 \in \mathbf{Q}[X] \; ;$$

$$X^3 + X + 3 \in \mathbf{Z}_5[X].$$

8. Determinare, nella forma $a + bi$, le radici complesse n-sime dell'unità per $n = 3, 4, 6, 8, 9$.

9. Determinare le radici complesse seconde, terze e quarte dei seguenti numeri complessi: 5, $5i$, $-7i$, $1 + i$, $1 - i$,

10. Mostrare che, se un polinomio a coefficienti reali ha i primi k termini non nulli positivi e tutti i successivi negativi, allora esso ha esattamente una radice reale (positiva).

11. Determinare il numero delle radici reali dei seguenti polinomi:

$$X^7 + X^2 + X + 1 \; ; \quad X^5 - 3X^2 - X + 1 \; ; \quad X^4 + 15X^2 + 7X - 11 \; .$$

5. Polinomi irriducibili. Teorema di fattorizzazione unica in K[X].

Ogni elemento non nullo di un dominio R è diviso in R dai suoi associati e dagli elementi invertibili di R; infatti, se $u \in U(R)$, per ogni $a \in R$, si ha $a = u(u^{-1}a)$. Se a è non nullo e non invertibile, un *divisore proprio* di a è un divisore che non è invertibile e non è associato ad a.

Un elemento non nullo e non invertibile di R si dice *riducibile* in R se ha divisori propri in R, altrimenti esso si dice *irriducibile*. In altre parole, un elemento irriducibile di R è un elemento non nullo e non invertibile i cui unici divisori sono gli elementi ad esso associati e gli elementi invertibili di R. Gli elementi irriducibili di $\mathbf{Z}$ sono esattamente i numeri primi e i loro opposti.

Lemma 5.1. Sia K un campo e sia $f(X)$ un polinomio non nullo e non invertibile di $K[X]$. Se $g(X)$ è un divisore di $f(X)$ in $K[X]$, allora $g(X)$ è un divisore proprio di $f(X)$ se e soltanto se $1 \leq \deg(g(X)) < \deg(f(X))$.

Dimostrazione. Essendo $g(X)$ un divisore di $f(X)$, si ha che $f(X) = g(X)h(X)$ con $h(X) \in K[X]$. Per definizione, $g(X)$ è un divisore proprio di $f(X)$ se e soltanto se $g(X)$ e $h(X)$ sono entrambi non invertibili in $K[X]$. Allora, essendo $U(K[X]) = K^*$, dalla formula del grado segue immediatamente che $g(X)$ è un divisore proprio di $f(X)$ se e soltanto se $1 \leq \deg(g(X)) < \deg(f(X))$.

Proposizione 5.2. Se K è un campo, un polinomio di grado $n \geq 1$ è riducibile in $K[X]$ se e soltanto se esso ha divisori non costanti di grado strettamente minore di n. In particolare ogni polinomio di grado 1 è irriducibile in $K[X]$.

Dimostrazione. Segue immediatamente dalla definizione di polinomio irriducibile e dal Lemma 5.1.

Mostriamo ora il legame esistente tra la riducibilità di un polinomio e l'esistenza di radici.

Proposizione 5.3. (a) Se $f(X) \in A[X]$ ha una radice in A e $\deg((f(X)) > 1$, allora $f(X)$ è riducibile in $A[X]$.

(b) Se K è un campo e $f(X) \in K[X]$ ha grado 2 oppure 3, allora $f(X)$ è riducibile in $K[X]$ se e soltanto se esso ha una radice in K.

Dimostrazione. (a) segue direttamente dal Corollario 4.2.

(b) segue dal Corollario 4.2. e dal fatto che, se K è un campo e $f(X)$ ha grado 2 o 3, per la formula del grado e il Corollario 5.1, esso è riducibile soltanto se ha un fattore di primo grado.

E' però importante notare che, se $\deg(f(X)) \geq 4$, $f(X) \in K[X]$ può essere riducibile in $K[X]$ senza avere radici in K.

Esempi.

1. Un polinomio non nullo e non invertibile $f(X) \in \mathbf{Z}[X]$ è irriducibile su $\mathbf{Z}$ se e soltanto se i suoi soli divisori a coefficienti interi sono $\pm 1, \pm f(X)$.

2. Il polinomio $(X^2 - 2)^2$ è riducibile in $\mathbf{Q}[X]$ e privo di radici in $\mathbf{Q}$. Il polinomio $(X^2 + 1)(X^2 + X + 1)$ è riducibile in $\mathbf{R}[X]$ e privo di radici in $\mathbf{R}$.

3. I polinomi di grado 2 di $\mathbf{Z}_2[X]$ sono

$$X^2+1 \; ; \; X^2+X+1 \; ; \; X^2 \; ; \; X^2+X \; .$$

L'unico tra questi che non ha radici in $\mathbf{Z}_2$ è $X^2 + X + 1$. Dunque esso è l'unico polinomio di grado 2 irriducibile su $\mathbf{Z}_2$.

Corollario 5.4. (a) I soli polinomi irriducibili di $\mathbf{C}[X]$ sono i polinomi di primo grado.

(b) I soli polinomi irriducibili di $\mathbf{R}[X]$ sono i polinomi di primo grado e i polinomi di secondo grado privi di radici reali.

Dimostrazione. (a) Per la Proposizione 5.2, i polinomi di primo grado di $\mathbf{C}[X]$ sono irriducibili. Viceversa, sia $f(X)$ un polinomio di $\mathbf{C}[X]$ di grado n. Per il Corollario 4.8 del Teorema Fondamentale dell'Algebra, risulta $f(X) = u(X-\alpha_1)^{m_1}\ldots(X-\alpha_s)^{m_s}$ dove $u, \alpha_i \in \mathbf{C}$, $u \neq 0$, $1 \leq s \leq n$ e $m_1 + \ldots + m_s = n$. Dunque, se $f(X)$ è irriducibile, deve essere $n = 1$.

(b) In $\mathbf{R}[X]$ i polinomi di primo grado sono irriducibili per la Proposizione 5.2 ed un polinomio di secondo grado è irriducibile se e soltanto se è privo di radici reali per la Proposizione 5.3. Sia $f(X)$ un polinomio di $\mathbf{R}[X]$ di grado $n > 2$. Per il Corollario 4.8 del Teorema fondamentale dell'Algebra, $f(X)$ si decompone in $\mathbf{C}[X]$ nel prodotto di fattori

lineari; inoltre se $\alpha \in \mathbf{C}$ è una radice di $f(X)$, per la Proposizione 4.9 anche $\overline{\alpha}$ è una radice di $f(X)$. Poiché

$$(X - \alpha)(X - \overline{\alpha}) = X^2 + (\alpha + \overline{\alpha})X + \alpha\overline{\alpha} \in \mathbf{R}[X],$$

si ha che $f(X)$ si decompone in $\mathbf{R}[X]$ nel prodotto di polinomi di grado al più uguale a due.

Nel Paragrafo successivo studieremo la riducibilità dei polinomi a coefficienti razionali. Vedremo che, per ogni $n \geq 1$, esistono polinomi di grado n irriducibili su $\mathbf{Q}$.

Se K è un campo e $p(X)$ è un polinomio irriducibile di $K[X]$, dato comunque un polinomio $f(X) \in K[X]$, si hanno soltanto due possibilità: $p(X)$ divide $f(X)$, oppure $MCD(p(X), f(X)) = 1$. Una importante conseguenza di questo semplice fatto è che un polinomio irriducibile di $\mathbf{Q}[X]$ non ha radici multiple in $\mathbf{C}$, come mostra la seguente Proposizione.

Proposizione 5.5. Sia F un campo numerico e sia $f(X) \in F[X]$ un polinomio irriducibile su F. Allora le radici complesse di $f(X)$ sono tutte semplici.

Dimostrazione. Se $f(X)$ ha una radice complessa multipla, allora $MCD(f(X), f'(X)) \neq 1$ in $\mathbf{C}[X]$ (Corollario 4.6). Allora, per il Corollario 3.7, $f(X)$ e $f'(X)$ hanno un divisore comune non costante in $F[X]$. Questo è impossibile perché $f(X)$ è irriducibile su F ed inoltre non divide $f'(X)$ perché $f'(X)$ è non nullo e di grado minore.

Terminiamo questo paragrafo mostrando che ogni polinomio di grado positivo a coefficienti in un campo K si può fattorizzare in $K[X]$ nel prodotto di una costante e polinomi monici irriducibili in modo unico, a meno dell'ordine dei fattori.

Proposizione 5.6 (Lemma di Euclide). Sia K un campo e siano $f(X), g(X) \in K[X]$ due polinomi non nulli relativamente primi. Allora, dato $h(X) \in K[X]$, se $f(X)$ divide il prodotto $g(X)h(X)$ in $K[X]$, esso divide $h(X)$ in $K[X]$.

Dimostrazione. Sia $MCD(f(X), g(X)) = 1$ e sia $1 = \alpha(X)f(X) + \beta(X)g(X)$ una identità di Bezout. Moltiplicando per $h(X)$, otteniamo $h(X) = \alpha(X)f(X)h(X) + \beta(X)g(X)h(X)$; poiché $f(X)$ divide $g(X)h(X)$, allora $f(X)$ divide $h(X)$.

Corollario 5.7 Sia K un campo. Se $p(X) \in K[X]$ è un polinomio irriducibile su K e $p(X)$ divide un prodotto di polinomi in $K[X]$, allora $p(X)$ divide almeno uno dei fattori.

Dimostrazione. Per il principio di induzione, basta provare che, se $p(X)$ divide il prodotto di due polinomi, allora ne divide almeno uno. Supponiamo che $p(X)$ divida $f(X)g(X)$ con $f(X), g(X) \in K[X]$ e che $p(X)$ non divida $f(X)$; poichè $p(X)$ è irriducibile, si ha $MCD(p(X), f(X)) = 1$. Dal Lemma di Euclide segue che $p(X)$ divide $g(X)$.

Se R è un domino, un elemento non invertibile p di R si dice un elemento *primo* se ha la seguente proprietà:

"se p divide il prodotto ab allora p divide a o/e b".

Con questa terminologia, il Corollario precedente dice che ogni polinomio irriducibile di $K[X]$ è un elemento primo.

Teorema 5.8 (Teorema di fattorizzazione unica in K[X]). Sia K un campo. Allora ogni polinomio non costante $f(X) \in K[X]$ si può fattorizzare in $K[X]$ nel prodotto di una costante e polinomi monici irriducibili. Inoltre questi polinomi sono univocamente determinati.

Dimostrazione. Sia $f(X) \in K[X]$ un polinomio di grado n e sia $c \in K$ il suo coefficiente direttore. Allora risulta $f(X) = cg(X)$, dove $g(X) = c^{-1}f(X)$ è un polinomio monico di grado n. Mostriamo, per induzione su n, che ogni polinomio monico $g(X)$ si può scrivere come prodotto di polinomi monici irriducibili.

Se $n = 1$, allora $g(X)$ è irriducibile per la Proposizione 5.2. Supponiamo poi che l'asserto sia vero per ogni k con $1 \leq k < n$. Se $g(X)$ è irriducibile non c'è niente da dimostrare. Altrimenti risulta $g(X) = h(X)k(X)$ dove $1 \leq \deg(f(X)), \deg(g(X)) < n$ (Proposizione 5.2); allora, per l'ipotesi induttiva, sia $h(X)$ che $k(X)$ si possono scrivere come prodotto di polinomi monici irriducibili e ne segue che anche $g(X)$ ha questa proprietà.

Per dimostrare l'unicità della fattorizzazione, supponiamo che sia

$$f(X) = a\, p_1(X)\, p_2(X) \dots p_r(X) = b\, q_1(X)\, q_2(X) \dots q_s(X),$$

con $a, b \in K$ e $p_1(X), \dots, p_r(X), q_1(X), \dots, q_s(X)$ polinomi monici irriducibili. Uguagliando i coefficienti, deve risultare $a = c = b$. Inoltre, $p_1(X)$ divide almeno uno dei polinomi $q_j(X)$ (Corollario 5.7) e allora, a meno di rinumerare $q_1(X), \dots, q_s(X)$, possiamo supporre che $p_1(X)$ divida $q_1(X)$. Poiché $p_1(X)$ non è costante e $q_1(X)$ è irriducibile, $p_1(X)$ e $q_1(X)$ devono essere associati; ma allora, essendo entrambi monici, deve risultare $p_1(X) = q_1(X)$.

A questo punto, per la legge di cancellazione, risulta $p_2(X) \dots p_r(X) = q_2(X) \dots q_s(X)$, e, ripetendo il ragionamento, dopo un numero finito di passi, si ottiene $r = s$ e $p_i(X) = q_i(X)$ per $i = 1, \dots, s$.

Vedremo nel seguito che un teorema analogo è vero anche per gli anelli in più indeterminate su un campo K.

Un dominio R è detto un *dominio a fattorizzazione unica* o *dominio fattoriale* (in breve, *UFD*) se soddisfa alle seguenti condizioni:

1) Ogni elemento non zero e non invertibile di R può essere fattorizzato in un prodotto di un numero finito di elementi irriducibili;

2) Se $p_1, \dots, p_r$ e $q_1, \dots, q_s$ sono due fattorizzazioni dello stesso elemento di R in elementi irriducibili, allora $r = s$ e gli elementi q_i possono essere rinumerati in modo tale che p_i e q_i siano associati per $i = 1, \dots, r$.

Si usa esprimere la proprietà 2) dicendo che la fattorizzazione in elementi irriducibili è unica, a meno dell'ordine e di elementi invertibili.

Il Teorema 5.8 ci assicura che, se K è un campo, l'anello dei polinomi $K[X]$ è un dominio a fattorizzazione unica. Infatti, se $f(X) \in K[X]$ e $p(X)$ è un suo fattore irriducibile, allora il polinomio monico associato a $p(X)$ in $K[X]$ è uno dei fattori monici irriducibili di $f(X)$.

ESERCIZI

1. Dimostrare che, se R è un dominio, ogni elemento primo di R è irriducibile.

2. Dimostrare che i numeri primi e i loro opposti sono tutti e soli gli elementi primi di $\mathbf{Z}$.

3. Mostrare che un polinomio $f(X) \in A[X]$ è irriducibile su A se e soltanto se lo sono tutti i suoi associati in $A[X]$.

4. Stabilire se i seguenti polinomi sono irriducibili su $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$:

$$6X^4 - 5X^3 - 38X^2 - 5X + 6\ ;\ X^4 - X^2 + 1\ ;\ X^4 + X + 1\ .$$

5. Fattorizzare i seguenti polinomi in fattori irriducibili su $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$:

$$15X^2 - 30\ ;\ 3X^4 - 5X^3 + 7X^2 - 15X - 6\ ;\ X^4 + 4\ ;\ X^6 + 2\ .$$

6. Dimostrare che i soli polinomi irriducibili di secondo grado in $\mathbf{Z}_3[X]$ sono:

$$X^2 + \overline{1}\ ,\ X^2 + X + \overline{1}\ ,\ X^2 + \overline{2}X + \overline{2}\ .$$

7. Stabilire se i seguenti polinomi sono irriducibili in $\mathbf{Z}_5[X]$:

$$\overline{3}X^2 + \overline{2}X + \overline{2}\ ;\ X^3 + \overline{3}X^2 + \overline{3}X + \overline{2}\ ;\ X^4 + \overline{2}X^3 + \overline{2}X^2 + \overline{2}X + \overline{1}\ .$$

6. Polinomi a coefficienti interi e razionali. Criteri di irriducibilità.

Abbiamo visto nei paragrafi precedenti che le proprietà di divisibilità di un polinomio $f(X) \in A[X]$ dipendono fortemente dall'anello A. Infatti, se A e B sono due domini tali che $A \subseteq B$, allora si ha anche $A[X] \subseteq B[X]$ e un polinomio $f(X) \in A[X]$ può avere comportamenti diversi nei due anelli di polinomi $A[X]$ e $B[X]$. Tuttavia, se $K := Qz(A)$ è il campo dei quozienti di A, c'è uno stretto legame tra le proprietà di divisibilità in $A[X]$ e quelle corrispondenti in $K[X]$. In questo paragrafo esamineremo in dettaglio il caso in cui A sia l'anello degli interi relativi $\mathbf{Z}$ (e quindi $K = \mathbf{Q}$). Nel paragrafo successivo considereremo il caso più generale in cui A sia un dominio a fattorizzazione unica.

Sia $f(X) \in \mathbf{Z}[X]$ un polinomio non nullo. Il massimo comune divisore dei coefficienti di $f(X)$ si dice il *contenuto* di $f(X)$ e si indica con $c(f)$. Se $c(f) = 1$, ovvero $f(X)$ non ha divisori costanti diversi da ± 1, allora $f(X)$ si dice *primitivo*. Un polinomio monico di $\mathbf{Z}[X]$ è senz'altro primitivo, ma è evidente che non vale il viceversa; ad esempio il polinomio $2X+1$ è primitivo ma non monico. E' evidente che i soli polinomi costanti primitivi sono 1 e -1.

Se $f(X) \in \mathbf{Q}[X]$ ha grado positivo e ha coefficienti interi, il polinomio $(c(f))^{-1}f(X)$ ha ancora coefficienti interi ed è un polinomio primitivo associato a $f(X)$ in $\mathbf{Q}[X]$. In generale, se i coefficienti di $f(X)$ non sono tutti interi e d è un denominatore comune dei suoi coefficienti, il polinomio $df(X)$ ha coefficienti interi. Dunque $f(X)$ è ancora associato in

$\mathbf{Q}[X]$ ad un unico polinomio a coefficienti interi e primitivo, che indichiamo con $f^*(X)$, tale che $f(X) = \frac{a}{b} f^*(X)$, con a e b numeri interi entrambi positivi.

Esempi.

1. Se $f(X) := 6 - 3X + 12X^2 - 15X^4$, allora $c(f) = 3$ e $f^*(X) = 2 - X + 4X^2 - 3X^4$.

2. Se $g(X) := \frac{10}{9} - \frac{5}{4}X + \frac{35}{6}X^2 - \frac{15}{2}X^4$, si ha

$$36\, g(X) = 40 - 45X + 210X^2 - 270X^4 = 5(8 - 9X + 42X^2 - 54X^4)$$

da cui $g^*(X) = 8 - 9X + 42X^2 - 54X^4$.

Poiché due polinomi di grado positivo a coefficienti in un campo K che siano associati tra loro sono entrambi riducibili o entrambi irriducibili su K, per stabilire se un polinomio $f(X) \in \mathbf{Q}[X]$ è o meno riducibile su $\mathbf{Q}$, basta allora studiare la riducibilità (su $\mathbf{Q}$) del polinomio a coefficienti interi e primitivo $f^*(X)$ associato a $f(X)$. I seguenti risultati, dovuti a Gauss, stabiliscono che, a questo scopo, basta studiare la riducibilità di $f^*(X)$ su $\mathbf{Z}$.

Ricordiamo che un polinomio $f(X)$ a coefficienti interi è irriducibile su $\mathbf{Z}$ se e soltanto se i suoi unici divisori in $\mathbf{Z}[X]$ sono ± 1, $\pm f(X)$.

Proposizione 6.1 (Lemma di Gauss). Se $f(X), g(X) \in \mathbf{Z}[X]$ sono due polinomi primitivi, allora anche $f(X)g(X)$ è un polinomio primitivo.

Dimostrazione. Siano

$$f(X) := a_0 + a_1X + \ldots + a_nX^n \text{ e } g(X) := b_0 + b_1X + \ldots + b_mX^m;$$

allora

$$f(X)g(X) = c_0 + c_1X + \ldots + c_{n+m}X^{n+m}, \text{ con } c_k = \sum_{i+j=k} a_ib_j \text{ per ogni } 0 \le k \le n+m.$$

Sia p un qualunque numero primo. Poichè $f(X)$ e $g(X)$ sono primitivi, p non divide tutti i coefficienti di $f(X)$ né divide tutti i coefficienti di $g(X)$; siano $r \le n$ e $s \le m$ i più piccoli indici tali che p non divida a_r né b_s. Il coefficiente di X^{r+s} in $f(X)g(X)$ è

$$c_{r+s} = (a_0b_{r+s} + \ldots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + \ldots + a_{r+s}b_0).$$

Poiché p divide $a_0, \ldots, a_{r-1}$, allora p divide $(a_0b_{r+s} + \ldots + a_{r-1}b_{s+1})$; analogamente, poiché p divide $b_0, \ldots, b_{s-1}$, allora p divide $(a_{r+1}b_{s-1} + \ldots + a_{r+s}b_0)$. Inoltre p non divide a_r né b_s, così che p non divide a_rb_s. Si può pertanto concludere che p non divide c_{r+s}. Questo prova che un qualunque numero primo p non divide tutti i coefficienti di $f(X)g(X)$ e allora $f(X)g(X)$ è primitivo.

Corollario 6.2. Siano $f(X), g(X) \in \mathbf{Z}[X]$ polinomi non nulli. Allora $c(fg) = c(f)c(g)$.

Dimostrazione. Siano $f(X) = c(f)f^*(X)$ e $g(X) = c(g)g^*(X)$ con $f^*(X)$ e $g^*(X)$ polinomi primitivi di $\mathbf{Z}[X]$; allora $f(X)g(X) = c(f)c(g)f^*(X)g^*(X)$, da cui, passando ai

contenuti ed essendo $f^*(X)g^*(X)$ primitivo per il Lemma di Gauss (Proposizione 6.1), si ha che $c(fg) = c(f)c(g)$.

Proposizione 6.3. Sia $f(X) \in \mathbf{Z}[X]$ un polinomio primitivo di grado positivo. Se $f(X) = g(X)h(X)$, con $g(X), h(X) \in \mathbf{Q}[X]$, allora $f(X) = g^*(X)h^*(X)$, dove $g^*(X), h^*(X)$ sono polinomi primitivi di $\mathbf{Z}[X]$ associati rispettivamente a $g(X)$ e $h(X)$ in $\mathbf{Q}[X]$.

In particolare, se $f(X)$ è irriducibile in $\mathbf{Z}[X]$, lo è anche in $\mathbf{Q}[X]$.

Dimostrazione. Siano $g(X) = \frac{a}{b}g^*(X)$ e $h(X) = \frac{c}{d}h^*(X)$ con a, b, c, d numeri interi positivi e $g^*(X)$ e $h^*(X)$ polinomi primitivi di $\mathbf{Z}[X]$. Allora, se $f(X) = g(X)h(X)$, si ha $bdf(X) = acg^*(X)h^*(X)$. Passando ai contenuti, a sinistra si ha bd, poiché $f(X)$ è primitivo; a destra si ha ac, poiché $g^*(X)h^*(X)$ è primitivo per il Lemma di Gauss (Proposizione 6.1). In definitiva, risulta $bd = ac$ da cui $\frac{a}{b}\frac{c}{d} = 1$. Si può quindi concludere che $f(X) = g^*(X)h^*(X)$.

In particolare, se $f(X)$ è riducibile su $\mathbf{Q}$, allora esiste un suo divisore $g(X)$ non costante e di grado stettamente minore (Proposizione 5.2). Poiché $g^*(X)$ ha lo stesso grado di $g(X)$, $g^*(X)$ è un divisore proprio di $f(X)$ in $\mathbf{Z}[X]$ e perciò $f(X)$ è riducibile in $\mathbf{Z}[X]$.

Corollario 6.4. (a) Un polinomio costante $c \in \mathbf{Z}[X]$ è irriducibile in $\mathbf{Z}[X]$ se e soltanto se $c = \pm p$, dove p è un numero primo.

(b) Un polinomio $f(X) \in \mathbf{Z}[X]$ di grado $n \geq 1$ è irriducibile in $\mathbf{Z}[X]$ se e soltanto se è primitivo e irriducibile in $\mathbf{Q}[X]$.

Dimostrazione. (a) Sia $c \in \mathbf{Z}$. Per la formula del grado, i divisori di c in $\mathbf{Z}[X]$ sono tutti costanti. Dunque c è irriducibile in $\mathbf{Z}[X]$ se e soltanto se i suoi unici divisori sono ± 1 e $\pm c$, ovvero $c = \pm p$, con p primo.

(b) Se $f(X)$ è primitivo, esso non ha divisori costanti diversi da ± 1. Inoltre, se $f(X)$ è irriducibile in $\mathbf{Q}[X]$, esso non ha divisori di grado positivo strettamente minore di n (Proposizione 5.2). Ne segue che i suoi soli divisori a coefficienti interi sono ± 1, $\pm f(X)$ e perciò $f(X)$ è irriducibile in $\mathbf{Z}[X]$.

Viceversa, se $f(X)$ è irriducibile in $\mathbf{Z}[X]$, esso non può avere fattori costanti diversi da ± 1. Dunque $f(X)$ è primitivo ed allora è irriducibile in $\mathbf{Q}[X]$ per la Proposizione 6.3.

Esempi.

3. Il polinomio $f(X) := 6X^2 - 5X + 1$ è primitivo e ha radici razionali 1/2 e 1/3; perciò esso si fattorizza su $\mathbf{Q}$ come $f(X) = 6(X-1/2)(X-1/3)$. Eliminando i denominatori, si ottiene una fattorizzazione in $\mathbf{Z}[X]$, cioè $f(X) = (2X-1)(3X-1)$.

4. Il polinomio $15X^2 + 6X - 5$ è primitivo e irriducibile su $\mathbf{Q}$ (perché non ha radici razionali), dunque esso è irriducibile anche su $\mathbf{Z}$.

5. Un polinomio a coefficienti interi e non primitivo può essere irriducibile in $\mathbf{Q}[X]$, anche se è sempre riducibile su $\mathbf{Z}$. Questo accade se i suoi divisori propri in $\mathbf{Z}[X]$ sono tutti costanti. Ad esempio, il polinomio $2X$ è riducibile in $\mathbf{Z}[X]$, perché 2 non è invertibile in $\mathbf{Z}$ e perciò 2 è un fattore proprio di $2X$ in $\mathbf{Z}[X]$; ma è irriducibile in $\mathbf{Q}[X]$, essendo di primo grado (Proposizione 5.2).

Corollario 6.5. Sia $p(X) \in \mathbf{Z}[X]$.

(a) Se $p(X)$ è primitivo e divide un polinomio a coefficienti interi in $\mathbf{Q}[X]$, allora lo divide anche in $\mathbf{Z}[X]$.

(b) Se $p(X)$ è irriducibile in $\mathbf{Z}[X]$ e divide un prodotto di polinomi in $\mathbf{Z}[X]$, allora divide almeno uno dei fattori.

Dimostrazione. (a) Sia $g(X) \in \mathbf{Z}[X]$ tale che $g(X) = p(X)h(X)$, con $h(X) \in \mathbf{Q}[X]$. Possiamo scrivere $g(X) = cg^*(X)$ e $h(X) = a/b\, h^*(X)$, con $g^*(X)$ e $h^*(X)$ polinomi a coefficienti interi e primitivi e $MCD(a,b) = 1$. Poiché $bcg^*(X) = ap(X)h^*(X)$, per il Lemma di Gauss (Proposizione 6.1), si ha $bc = a$; dunque, per il Lemma di Euclide, a divide c in $\mathbf{Z}$. Ma allora, poiché c divide a, risulta $b = \pm 1$ e $h(X) = \pm a\, h^*(X) \in \mathbf{Z}[X]$.

(b) Basta dimostrare che, se $p(X)$ divide il prodotto di due polinomi $f(X) := g(X)h(X)$ in $\mathbf{Z}[X]$, allora $p(X)$ divide $g(X)$ o/e $h(X)$. Il risultato seguirà per induzione sul numero dei fattori.

Se $p(X)$ è costante, allora $p(X)$ divide $c(f)$. Poiché $p(X) = \pm p$, con p primo (Corollario 6.4(a)) ed inoltre $c(f) = c(g)c(h)$ (Corollario 6.2), ne segue che $p(X)$ divide $c(g)$ o/e $c(h)$. Dunque $p(X)$ divide $g(X)$ o/e $h(X)$.

Se $\deg(p(X)) \geq 1$, allora $p(X)$ è primitivo e irriducibile su $\mathbf{Q}$ (Corollario 6.4 (b)). Ne segue che $p(X)$ divide $g(X)$ o/e $h(X)$ in $\mathbf{Q}[X]$ (Corollario 5.7); ma allora $p(X)$ divide $g(X)$ o/e $h(X)$ in $\mathbf{Z}[X]$ per il punto (a).

Siamo ora pronti per dimostrare che $\mathbf{Z}[X]$ è un dominio a fattorizzazione unica, cioè che ogni polinomio di $\mathbf{Z}[X]$ si può fattorizzare, in modo essenzialmente unico, nel prodotto di polinomi irriducibili. Un teorema analogo è stato dimostrato nel paragrafo precedente per $\mathbf{Q}[X]$ e più generalmente per un anello di polinomi in una indeterminata a coefficienti in un campo K.

Teorema 6.6 (Teorema di fattorizzazione unica in $\mathbf{Z}[X]$). Sia $f(X) \in \mathbf{Z}[X]$ un polinomio non nullo e diverso da ± 1. Allora $f(X)$ si può fattorizzare in $\mathbf{Z}[X]$ nel prodotto di numeri primi e polinomi (primitivi) irriducibili. Inoltre tale fattorizzazione è unica, a meno del segno e dell'ordine dei fattori.

Dimostrazione. Sia $f(X) \in \mathbf{Z}[X]$ un polinomio non nullo e diverso da ± 1 e poniamo $f(X) = cf^*(X)$, dove $c := c(f) \in \mathbf{Z}$ e $f^*(X)$ è un polinomio primitivo. Per il Teorema Fondamentale dell'Aritmetica, $|c|$ si fattorizza nel prodotto di numeri primi, che sono polinomi irriducibili di $\mathbf{Z}[X]$ (Corollario 6.4 (a)). Inoltre, se $f^*(X) \neq \pm 1$, $f^*(X)$ si fattorizza

nel prodotto di polinomi monici irriducibili in $\mathbf{Q}[X]$ (Teorema 5.8). Per la Proposizione 6.3, allora $f^*(X)$ si fattorizza in $\mathbf{Z}[X]$ nel prodotto di polinomi primitivi di grado positivo, ciascuno dei quali è associato in $\mathbf{Q}[X]$ a qualche fattore monico irriducibile. Ne segue che tali polinomi primitivi sono irriducibili anche in $\mathbf{Z}[X]$ (Corollario 6.4 (b)). In conclusione $f(X)$ si può fattorizzare in $\mathbf{Z}[X]$ nel prodotto di numeri primi e polinomi primitivi irriducibili.

Per mostrare l'unicità della fattorizzazione, osserviamo che, se $q(X) \in \mathbf{Z}[X]$ è un polinomio irriducibile che divide $f(X)$, allora $q(X)$ divide almeno uno dei fattori irriducibili $p(X)$ di $f(X)$ (Corollario 6.5 (b)) e quindi $q(X) = \pm p(X)$.

Diamo ora per finire alcuni criteri di sufficienza che assicurano l'irriducibilità su $\mathbf{Q}$, di un polinomio a coefficienti interi.

Teorema 6.7 (Criterio di Irriducibilità di Eisenstein). Sia $f(X) := a_0 + a_1X + \ldots + a_nX^n \in \mathbf{Z}[X]$. Se esiste un numero primo p tale che $p \nmid a_n$, $p \mid a_i$ per $0 \le i < n$ e $p^2 \nmid a_0$. Allora $f(X)$ è irriducibile su $\mathbf{Q}$.

Dimostrazione. Poniamo $f(X) = c(f)f^*(X)$ con $f^*(X)$ polinomio primitivo di $\mathbf{Z}[X]$; poiché $f(X)$ e $f^*(X)$ sono associati in $\mathbf{Q}[X]$, è sufficiente provare che $f^*(X)$ è irriducibile su $\mathbf{Q}$. Inoltre, poiché p non divide $c(f)$, i coefficienti di $f^*(X)$ soddisfano le ipotesi del Teorema. Senza perdita di generalità, possiamo allora supporre che il polinomio $f(X)$ sia primitivo; dunque, per il corollario precedente, è sufficiente provare che $f(X)$ è irriducibile in $\mathbf{Z}[X]$. Siano $g(X) := b_0 + b_1X + \ldots + b_sX^s$ e $h(X) := c_0 + c_1X + \ldots + c_tX^t$ polinomi a coefficienti in $\mathbf{Z}$ tali che $f(X) = g(X)h(X)$. Poiché $a_n = b_sc_t$ e $p \nmid a_n$, allora p non divide b_s né c_t; inoltre, poiché $a_0 = b_0c_0$, $p \mid a_0$ e $p^2 \nmid a_0$, allora p divide uno soltanto dei numeri interi b_0 e c_0. Supponiamo che p divida b_0 e non divida c_0. Sia $i \le s \le n$ il più piccolo numero intero positivo tale che $p \nmid b_i$. Poiché $a_i = b_0c_i + b_1c_{i-1} + \ldots + b_ic_0$ e p non divide b_i né c_0, allora p non divide a_i. Dalle ipotesi fatte segue che $i = n$; per cui $s = n$, ovvero $f(X)$ e $g(X)$ hanno lo stesso grado e $h(X)$ è una costante. Poiché abbiamo supposto che $f(X)$ sia primitivo, si ha che $h(X) = \pm 1$. Ne segue che $f(X)$ è irriducibile in $\mathbf{Z}[X]$ e dunque anche in $\mathbf{Q}[X]$ (Proposizione 6.3).

Proposizione 6.8. Siano F e K campi e $\varphi: F[X] \longrightarrow K[X]$ un omomorfismo di anelli che conserva il grado. Allora, se $f(X) \in F[X]$ è riducibile su F, $\varphi(f(X))$ è riducibile su K.

Dimostrazione. Poiché $f(X)$ è riducibile su F, esistono $g(X), h(X) \in F[X]$ di grado positivo tali che $f(X) = g(X)h(X)$. Allora risulta $\varphi(f(X)) = \varphi(g(X))\varphi(h(X))$ con $\varphi(g(X))$ e $\varphi(h(X))$ entrambi di grado positivo per l'ipotesi fatta su φ. Da ciò segue la riducibilità di $\varphi(f(X))$ su K.

Corollario 6.9. Siano K un campo, $\alpha \in K\backslash\{0\}$ e consideriamo le applicazioni:

$$\phi_{X+\alpha} : K[X] \longrightarrow K[X] \text{ , definita da } f(X) \longrightarrow f(X+\alpha) ;$$
$$\phi_{\alpha X} : K[X] \longrightarrow K[X] \text{ , definita da } f(X) \longrightarrow f(\alpha X).$$

Allora $f(X)$ è riducibile su K se soltanto se $f(X+\alpha)$ è riducibile su K, se soltanto se $f(\alpha X)$ è riducibile su K.

Dimostrazione. Per la proposizione 6.6, basta osservare che $\phi_{X+\alpha}$ è un automorfismo di $K[X]$ che conserva il grado, con inverso $\phi_{X-\alpha} : K[X] \longrightarrow K[X]$ definito da $f(X) \longrightarrow f(X-\alpha)$. Analogamente, $\phi_{\alpha X}$ è un automorfismo di $K[X]$ che conserva il grado, con inverso $\phi_{X/\alpha} : K[X] \longrightarrow K[X]$ definito da $f(X) \longrightarrow f(X/\alpha)$.

Esempi.

6. Per il Criterio di Irriducibilità di Eisenstein, se p è un numero primo, il polinomio $X^n - p$ è irriducibile su $\mathbf{Q}$, per ogni $n \geq 2$.

7. Irriducibilità del p-esimo polinomio ciclotomico. Sia p un numero primo. Ricordiamo che il polinomio a coefficienti interi

$$\Phi_p(X) := \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1 ,$$

le cui radici sono le radici p-sime primitive dell'unità, si dice il p-esimo polinomio ciclotomico (cf. Esempio 4.4). Mostriamo che $\Phi_p(X)$ è irriducibile su $\mathbf{Q}$.

Per il Corollario 6.7. basta provare che il polinomio $f(X) := \phi_{X+1}\left(\Phi_p(X)\right)$ è irriducibile su $\mathbf{Q}$. Risulta

$$\phi_{X+1}\left(\Phi_p(X)\right) = \frac{(X+1)^p - 1}{(X+1) - 1} =$$
$$= \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{1}X^{p-2} + \cdots + \binom{p}{p-2}X + \binom{p}{p-1} .$$

Poiché p non divide $i!(p-i)!$ per ogni $i = 1, \ldots, p-1$ e p divide $p!$, si ha che p divide il coefficiente binomiale $\binom{p}{i}$. D'altra parte, p^2 non divide $\binom{p}{p-1} = p$. Allora il polinomio $f(X)$ soddisfa le condizioni del Criterio di Irriducibilità di Eisenstein ed è per questo irriducibile.

Per stabilire la riducibiltà o meno di polinomi a coefficienti interi, si fa uso anche della riduzione dei coefficienti modulo un numero primo p. Più precisamente, sia $p \geq 2$ un numero primo fissato e si consideri l'applicazione

$\psi : \mathbf{Z}[X] \longrightarrow \mathbf{Z}_p[X]$ definita da $\psi(a_0 + a_1X + \ldots + a_nX^n) = \bar{a}_0 + \bar{a}_1X + \ldots + \bar{a}_nX^n$.

E' immediato verificare che ψ è un omomorfismo di anelli. Perciò, ponendo $\bar{f}(X) := \psi(f(X))$, se un polinomio $f(X)$ a coefficienti interi si fattorizza in $\mathbf{Z}[X]$ come $f(X) = g(X)h(X)$, allora $\bar{f}(X)$ si fattorizza in $\mathbf{Z}_p[X]$ come $\bar{f}(X) = \bar{g}(X)\bar{h}(X)$.

Teorema 6.10 (Criterio di Irriducibilità modulo p). Sia $f(X) := a_0 + a_1X + \ldots + a_nX^n \in \mathbf{Z}[X]$ un polinomio non costante e sia p un numero primo che non divide il coefficiente direttore di $f(X)$. Se $\bar{f}(X) := \bar{a}_0 + \bar{a}_1X + \ldots + \bar{a}_nX^n \in \mathbf{Z}_p[X]$ è irriducibile in $\mathbf{Z}_p[X]$, allora $f(X)$ è irriducibile in $\mathbf{Q}[X]$.

Dimostrazione. In modo analogo a quanto fatto nella dimostrazione del Teorema 6.5, possiamo supporre che il polinomio $f(X)$ sia primitivo. Poichè p non divide a_n, allora $f(X)$ e $\bar{f}(X)$ hanno lo stesso grado; in particolare $\bar{f}(X)$ non è una costante. Se $f(X)$ fosse riducibile in $\mathbf{Q}[X]$, allora, per la Proposizione 6.3, esso sarebbe riducibile in $\mathbf{Z}[X]$, cioè si avrebbe $f(X) = g(X)h(X)$ con $g(X)$ e $h(X)$ polinomi a coefficienti interi entrambi primitivi e di grado positivo, dal momento che $f(X)$ è primitivo. Allora si avrebbe anche $\bar{f}(X) = \bar{g}(X)\bar{h}(X)$ con $\deg(g(X)) = \deg(\bar{g}(X)) \geq 1$ e $\deg(h(X)) = \deg(\bar{h}(X)) \geq 1$, perché p non divide né il coefficiente direttore di $g(X)$ né quello di $h(X)$; pertanto $\bar{f}(X)$ sarebbe riducibile in $\mathbf{Z}_p[X]$.

Esempi.

8. Un polinomio $f(X) \in \mathbf{Z}[X]$ di grado 2 oppure 3 è irriducibile su $\mathbf{Q}$ soltanto se non ha radici razionali (Proposizione 5.3(b)). Riducendo i coefficienti modulo un primo p che non divide il termine noto, si ottiene un polinomio $\bar{f}(X) \in \mathbf{Z}_p[X]$ che ha stesso grado e che è dunque irriducibile in $\mathbf{Z}_p[X]$ soltanto se non ha radici in $\mathbf{Z}_p$. In conclusione, se esiste un primo p tale che $\bar{f}(X) \in \mathbf{Z}_p[X]$ non abbia radici in $\mathbf{Z}_p[X]$, allora $f(X)$ è irriducibile su $\mathbf{Q}$.

Ad esempio, riducendo modulo 3 i coefficienti del polinomio $f(X) := 5X^3 - 562X + 1400$, si ottiene il polinomio $\bar{f}(X) = \bar{2}X^3 + X + \bar{2} \in \mathbf{Z}_3[X]$, che non ha radici in $\mathbf{Z}_3$. Dunque $f(X)$ è irriducibile su $\mathbf{Q}$.

9. Il polinomio $f(X) := X^5 - 5X^4 - 6X - 1$ è irriducibile su $\mathbf{Q}$. Infatti, se fosse riducibile, avrebbe un fattore irriducibile di primo o secondo grado. Ma, riducendo i coefficienti modulo 3, si ottiene $\bar{f}(X) = X^5 + X^4 + \bar{1} \in \mathbf{Z}_3[X]$, che non ha radici in $\mathbf{Z}_3$ e dunque non ha fattori di primo grado. Inoltre $\bar{f}(X)$ non ha neanche fattori irriducibili di secondo grado, infatti i soli polinomi irriducibili di secondo grado in $\mathbf{Z}_3[X]$ sono:

$$X^2 + \bar{1}, \quad X^2 + X + \bar{1}, \quad X^2 + \bar{2}X + \bar{2},$$

(cf. Esercizio 6.6) e questi non dividono $\bar{f}(X)$.

Notiamo tuttavia che, riducendo i coefficienti modulo 2, si ottiene un polinomio riducibile in $\mathbf{Z}_2[X]$, precisamente:

$$X^5 + X^4 + \bar{1} = (X^2 + X + \bar{1})(X^3 + X + \bar{1}).$$

ESERCIZI

1. Mostrare che un polinomio $f(X) \in \mathbf{Z}[X]$ di grado 2 oppure 3 può essere riducibile su $\mathbf{Z}$ senza avere radici intere.

2. Dimostrare la seguente versione simmetrica del Criterio di Irriducibilità di Eisenstein:

Sia $f(X) := a_0 + a_1X + \ldots + a_nX^n \in \mathbf{Z}[X]$. Se esiste un numero primo p tale che $p \nmid a_0$, $p \mid a_i$ per $0 \le i < n$ e $p^2 \nmid a_n$, allora $f(X)$ è irriducibile su $\mathbf{Q}$.

3. Provare che, se $a \in \mathbf{Z}$ è privo di fattori quadratici, il polinomio $X^n - a$ è irriducibile in $\mathbf{Z}[X]$ per ogni $n \ge 1$.

4. Usando il Criterio di Irriducibilità di Eisenstein, mostrare che i seguenti polinomi sono irriducibili in $\mathbf{Q}[X]$:

$$X^3 + 6X^2 - 9X + 3 \; ; \quad 10X^4 + 15X^3 - 20X^2 - 35X - 2 \; .$$

5. Mostrare che i seguenti polinomi sono irriducibili in $\mathbf{Q}[X]$, benché non si possa applicare il Criterio di Irriducibilità di Eisenstein:

$$4X^2 + 4X - 1 \; ; \quad X^3 + X^2 + 1 \; .$$

6. Sia $f(X) := X^4 + 6X^3 + 12X^2 + 12X + 7$; determinare un numero intero α in modo tale che si possa applicare il Criterio di Eisenstein al polinomio $f(X - \alpha)$.

7. Mostrare, usando il Criterio di Irriducibilità modulo p , che i seguenti polinomi sono irriducibili in $\mathbf{Q}[X]$:

$$49X^2 + 35X + 11 \; ; \quad 124X^3 - 119X^2 + 35X + 64 \; ; \quad X^3 - 9 \; .$$

8. Fattorizzare i seguenti polinomi di $\mathbf{Z}[X]$ nel prodotto di polinomi irriducibili:

$$21X \; ; \quad 5X^2 + 10 \; ; \quad 15X^2 - 2X - 8 \; ; \quad 2X^4 - X^3 - X^2 - 2X - 1 \; ; \quad X^4 - 20X^2 + 4 \; .$$

7. Congruenze polinomiali. Costruzione di radici.

Per la formula del grado, ogni polinomio $p(X)$ di grado n a coefficienti in un campo K ha al più n radici distinte in ogni campo contenente K . Se K è un campo numerico, il Teorema Fondamentale dell'Algebra (Teorema 4.7) ci assicura che un campo in cui $p(X)$ abbia tutte le sue radici esiste, questo è infatti il campo $\mathbf{C}$ dei numeri complessi. Scopo di questo paragrafo è mostrare che, qualsiasi sia K , si può sempre costruire un campo contenente K in cui $p(X)$ abbia tutte le sue radici e quindi si fattorizzi in polinomi di primo grado.

Sia $p(X) \in K[X]$ un polinomio fissato di grado n . Diciamo che due polinomi $f(X)$ e $g(X)$ sono congrui modulo $p(X)$ e scriveremo

$$f(X) \equiv g(X) \mod p(X) \; ,$$

se $p(X)$ divide il polinomio differenza $f(X) - g(X)$. Equivalentemente,

$$f(X) \equiv g(X) \mod p(X) \iff f(X) - g(X) = h(X)p(X) \text{ per un opportuno } h(X) \in K[X] \; .$$

Indicando, in forma compatta con $(p(X))$ l'insieme dei multipli del polinomio $p(X)$, cioè

$$(p(X)) := \{h(X)p(X) \; ; \; h(X) \in K[X]\} \; ,$$

possiamo allora riformulare la definizione di congruenza modulo $p(X)$ dicendo che

$$f(X) \equiv g(X) \mod p(X) \iff f(X) - g(X) \in (p(X)) \; .$$

Osserviamo che ogni polinomio è congruo modulo $p(X)$ al resto della sua divisione per $p(X)$. Infatti, se con l'algoritmo della divisione (Teorema 3.3) si ottiene

$$f(X) = q(X)p(X) + r(X)\ ,\ \text{con}\ \ r(X) = 0\ \ \text{oppure}\ \ \deg(r(X)) < \deg(p(X)) = n\ ,$$

allora

$$f(X) - r(X) \in (p(X))\ .$$

Si verifica facilmente che la congruenza modulo $p(X)$ è una relazione di equivalenza in $K[X]$. Indicheremo la classe di equivalenza (o di congruenza) del polinomio $f(X)$ con $\overline{f(X)}$ e l'insieme quoziente di $K[X]$ rispetto a questa relazione di equivalenza con $K[X]/(p(X))$.

Per quanto appena osservato,

$$\overline{f(X)} = \{f(X) + h(X)p(X)\ ;\ h(X) \in K[X]\} =: f(X) + (p(X))$$

ed inoltre, se $r(X)$ è il resto della divisione di $f(X)$ per $p(X)$,

$$\overline{f(X)} = \overline{r(X)}\ .$$

Quindi risulta

$$K[X]/(p(X)) = \{\ \overline{r(X)} = r(X) + (p(X))\ ;\ r(X) \in K[X]\ ,\ r(X) = 0\ \text{oppure}\ \deg(r(X)) < n\}\ .$$

Notiamo che $\overline{f(X)} = \overline{0}$ se e soltanto se $p(X)$ divide $f(X)$, ovvero $f(X) \in (p(X))$; in particolare $\overline{p(X)} = \overline{0}$.

Possiamo a questo punto definire nell'insieme quoziente $K[X]/(p(X))$ due operazioni, di somma e prodotto, nel seguente modo:

$$\overline{f(X)} + \overline{g(X)} = \overline{f(X) + g(X)} \quad \text{e} \quad \overline{f(X)} \cdot \overline{g(X)} = \overline{f(X)g(X)}$$

Si può verificare senza difficoltà che queste operazioni sono ben definite, cioè non dipendono dai rappresentanti scelti. Infatti,

$$\text{se}\ \ f_1(X) \equiv f_2(X)\ \ \text{mod}\ \ p(X)\ \ \text{e}\ \ g_1(X) \equiv g_2(X)\ \ \text{mod}\ \ p(X)\ ,$$

allora

$$f_1(X) + g_1(X) \equiv f_2(X) + g_2(X)\ \ \text{mod}\ \ p(X) \quad \text{e} \quad f_1(X)g_1(X) \equiv f_2(X)g_2(X)\ \ \text{mod}\ \ p(X)\ .$$

Proposizione 7.1. Sia K un campo e $p(X) \in K[X]$ un polinomio fissato di grado $n \geq 1$. L'insieme quoziente $F := K[X]/(p(X))$ è un anello commutativo unitario rispetto alle operazioni definite da

$$\overline{f(X)} + \overline{g(X)} = \overline{f(X) + g(X)} \quad \text{e} \quad \overline{f(X)} \cdot \overline{g(X)} = \overline{f(X)g(X)}\ .$$

Inoltre, supponiamo che $p(X)$ non divida $f(X)$. Allora

se $\text{MCD}(f(X), p(X)) = 1$, $\overline{f(X)}$ è invertibile in $K[X]/(p(X))$;

se $\text{MCD}(f(X), p(X)) \neq 1$, $\overline{f(X)}$ è uno zero-divisore in $K[X]/(p(X))$.

Dimostrazione. La verifica che F è un anello commutativo è immediata. Lo zero è la classe di 0, ovvero di $p(X)$, e l'unità è la classe di 1.

Se $\text{MCD}(f(X), p(X)) = 1$ e $k(X)f(X) + h(X)p(X) = 1$ è una identità di Bezout (Teorema 3.4), allora, per come sono definite le operazioni,

$$\overline{k(X)f(X) + h(X)p(X)} = \overline{k(X)f(X)} + \overline{h(X)p(X)} = \overline{k(X)} \cdot \overline{f(X)} = \overline{1}\ ,$$

perciò $\overline{f(X)}$ è invertibile e $\overline{k(X)}$ è il suo inverso.

Se invece $MCD(f(X), p(X)) = d(X) \neq 1$, con $d(X) \neq p(X)$, allora esistono $h(X)$, $k(X) \in K[X]$ tali che $f(X) = d(X)h(X)$ e $p(X) = d(X)k(X)$. Ne segue che $f(X)k(X) = p(X)h(X)$ e perciò $\overline{f(X)k(X)} = \overline{0}$. Poiché inoltre $d(X)$ ha grado positivo, per la formula del grado, $\deg(p(X)) > \deg(k(X)) > 1$. Ne segue che $p(X)$ non può dividere $k(X)$; perciò $\overline{k(X)} \neq \overline{0}$ e $\overline{f(X)}$ è uno zero-divisore in $K[X]/(p(X))$.

Ribadiamo che, come visto nella dimostrazione della proposizione precedente, se $MCD(f(X), p(X)) = 1$, per determinare l'inverso di $\overline{f(X)}$ in $K[X]/(p(X))$ si può ricorrere ad una identità di Bezout, usando ad esempio l'algoritmo euclideo delle divisioni successive.

Esempi.

1. Sia $p(X) := X^4 - X^2 - 2 \in \mathbf{Q}[X]$. La fattorizzazione di $p(X)$ in polinomi irriducibili è $p(X) = (X^2-2)(X^2+1)$. Dunque, se $f(X)$ è un qualsiasi polinomio a coefficienti razionali, allora $MCD(f(X), p(X)) \neq 1$ se e soltanto se $f(X)$ è diviso da (X^2-2) o/e da (X^2+1) . Ne segue che $\overline{f(X)}$ è uno zero-divisore di $K[X]/(p(X))$ se e soltanto se $f(X) = (X^2-2)g(X)$, oppure $f(X) = (X^2+1)h(X)$, per opportuni $g(X), h(X) \in \mathbf{Q}[X]$ tali che (X^2+1) non divide $g(X)$ e (X^2-2) non divide $h(X)$. Altrimenti $\overline{f(X)}$ è invertibile.

La classe del polinomio $f(X) := X^4-2$ è ad esempio invertibile. Poiché inoltre l'algoritmo euclideo della divisione in $\mathbf{Q}[X]$ fornisce l'identità $X^2p(X) - (X^2-1)f(X) = -2$, allora l'inverso di $\overline{f(X)}$ in $K[X]/(p(X))$ è $\overline{\frac{1}{2}(X^2-1)}$. Possiamo anche osservare che $f(X) \equiv X^2 \mod p(X)$ e perciò, ai fini del calcolo, possiamo sostituire $f(X)$ con X^2 . Poiché $p(X) = X^2(X^2-1) - 2$, otteniamo ancora lo stesso risultato.

Proposizione 7.2. Sia K un campo e sia $p(X) \in K[X]$ un polinomio fissato di grado n . Le seguenti affermazioni sono equivalenti:

(i) $p(X)$ è un polinomio irriducibile;

(ii) $K[X]/(p(X))$ è un dominio integro;

(iii) $K[X]/(p(X))$ è un campo .

Dimostrazione. (i) $\Rightarrow$ (iii). $K[X]/(p(X))$ è un anello commutativo unitario per la Proposizione 7.1. Poiché $p(X)$ è un polinomio irriducibile, dato $f(X) \in K[X]$, se $p(X)$ non divide $f(X)$ risulta $MCD(f(X), p(X)) = 1$; Dunque, sempre per la Proposizione 7.1, se $\overline{f(X)} \neq \overline{0}$, $\overline{f(X)}$ è invertibile in $K[X]/(p(X))$. Ne segue che $K[X]/(p(X))$ è un campo.

(iii) $\Rightarrow$ (ii) è chiaro.

(ii) $\Rightarrow$ (i). Se $p(X)$ non è irriducibile, allora $p(X) = f(X)g(X)$, con $\deg(p(X)) > \deg(f(X)), \deg(g(X)) > 1$, allora $\overline{f(X)}, \overline{g(X)} \neq \overline{0}$ e $\overline{f(X)g(X)} = \overline{0}$. Perciò $K[X]/(p(X))$ ha zero-divisori.

Lemma 7.3. Sia K un campo e sia $p(X) \in K[X]$ un polinomio fissato di grado $n \geq 1$. La proiezione canonica:

$$K[X] \longrightarrow K[X]/(p(X)) \quad , \quad r(X) \longrightarrow \overline{r(X)} = r(X) + (p(X))$$

è un omomorfismo di anelli. Inoltre la sua restrizione a K è un omomorfismo iniettivo, perciò l'immagine di K in $K[X]/(p(X))$, cioè l'insieme

$$\overline{K} := \{ \bar{c} := c + (p(X)) ; c \in K\}$$

è un sottocampo dell'anello $K[X]/(p(X))$ che è isomorfo a K. Infine tale restrizione è suriettiva, cioè $\overline{K} = K[X]/(p(X))$, se e soltanto se $p(X)$ è di primo grado.

Dimostrazione. Che la proiezione canonica sia un omomorfismo di anelli segue subito dalle definizioni di somma e prodotto in $K[X]/(p(X))$. Inoltre, siano $a, b \in K$. Allora $p(X)$, avendo grado positivo, divide $a-b$ se e soltanto se $a-b = 0$. Dunque $\bar{a} = \bar{b}$ se e soltanto se $a = b$. Perciò la restrizione a K della proiezione canonica è un omomorfismo iniettivo.

Infine, se $p(X)$ è di primo grado, allora

$K[X]/(p(X)) = \{ \overline{r(X)}; r(X) \in K[X] , r(X) = 0$ oppure $\deg(r(X)) < 1\} = \{ \bar{c} ; c \in K\} = \overline{K}$.

Se invece $\deg(p(X)) \geq 2$, allora $\overline{X} \in K[X]/(p(X))$ e $\overline{X} \notin \overline{K}$, perchè $X - c$, essendo di primo grado, non può essere diviso da $p(X)$, per ogni $c \in K$. Dunque in questo caso $\overline{K}$ è propriamente contenuto in $K[X]/(p(X))$.

Per quanto appena visto, identificando K con $\overline{K}$, possiamo supporre che K sia contenuto in $K[X]/(p(X))$. In questo modo, quando $p(X)$ è irriducibile di grado maggiore di 1, $K[X]/(p(X))$ è un campo contenente propriamente K e un polinomio a coefficienti in K può anche essere letto come un polinomio a coefficienti in questo campo più grande.

Teorema 7.4. Sia K un campo e sia $p(X) \in K[X]$ un polinomio irriducibile su K di grado $n \geq 1$. Allora $p(X)$ ha una radice nel campo $F := K[X]/(p(X))$; precisamente, se α è la classe del polinomio X in F, risulta $p(\alpha) = 0$.

Dimostrazione. F è un campo perché $p(X)$ è irriducibile su F (Proposizione 7.2). Se $f(X) := c_0 + c_1X + \ldots + c_tX^t$, con $c_i \in K$, per come sono definite le operazioni in F, si ha $\overline{f(X)} = \bar{c}_0 + \bar{c}_1 \overline{X} + \ldots + \bar{c}_t \overline{X}^t$. Ponendo $\alpha := \overline{X}$ e identificando come al solito K con $\overline{K}$, allora possiamo scrivere $\overline{f(X)} = c_0 + c_1\alpha + \ldots + c_t\alpha^t = f(\alpha)$. In particolare otteniamo $0 = \overline{p(X)} = p(\alpha)$ e dunque $\alpha \in F$ è una radice di $p(X)$.

Se $r(X)$ è un polinomio di $K[X]$ di grado minore di n, oppure nullo, possiamo scrivere $r(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1}$, con $c_i \in K$. Allora, se $p(X)$ è irriducibile su K di grado n, come nella dimostrazione del teorema precedente, identificando c_i con $\overline{c_i}$ e ponendo $\alpha := \overline{X}$, otteniamo:

$$K[X]/(p(X)) = \{ \overline{r(X)} ; r(X) \in K[X] , r(X) = 0 \text{ oppure } \deg(r(X)) < n \}$$
$$= \{c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} ; c_i \in K , p(\alpha) = 0\} .$$

Per questo motivo, si usa denotare il campo $K[X]/(p(X))$ con $K(\alpha)$.

Se K è un campo numerico e γ è una qualsiasi radice complessa di $p(X)$, l'applicazione

$$K[X]/(p(X)) := K(\alpha) \longrightarrow \mathbf{C}$$

definita da

$$c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} \longrightarrow c_0 + c_1\gamma + \ldots + c_{n-1}\gamma^{n-1}$$

è un omorfismo iniettivo e perciò la sua immagine, cioè l'insieme

$$\{c_0 + c_1\gamma + \ldots + c_{n-1}\gamma^{n-1} \,;\, c_i \in K\},$$

è un sottocampo di $\mathbf{C}$. Questo campo viene ancora denotato con $K(\gamma)$.

Per determinare l'inverso del numero complesso $\beta := c_0 + c_1\gamma + \ldots + c_{n-1}\gamma^{n-1} \in K(\gamma)$, si può allora, tramite questo isomorfismo, lavorare nell'anello $K[X]$. Precisamente, si consideri il polinomio $r(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1} \in K[X]$, la cui classe in $K(\alpha)$ corrisponde a β. Poiché $p(X)$ è irriducibile di grado n, allora $r(X)$ e $p(X)$ sono coprimi e l'algoritmo della divisione euclidea ci permette di determinare due polinomi $g(X)$ e $h(X)$ tali che $g(X)r(X) + h(X)m(X) = 1$. Calcolando in γ, si ottiene che $g(\gamma)r(\gamma) = g(\gamma)\beta = 1$. Dunque $g(\gamma)$ è l'inverso di β in $K(\gamma)$.

Esempi.

2. Il polinomio $p(X) := X^2 + X + 1 \in \mathbf{Z}_2[X]$ è irriducibile su $\mathbf{Z}_2$, perché non ha radici in $\mathbf{Z}_2$. Dunque l'anello quoziente $F := \mathbf{Z}_2[X]/(p(X))$ è un campo e l'elemento $\alpha := \overline{X} \in F$ è tale che $p(\alpha) = 0$. Inoltre in $F[X]$, risulta $p(X) = (X+\alpha)(X+(1+\alpha))$.

Poiché i soli polinomi di $\mathbf{Z}_2[X]$ di grado minore di 2 sono $0, 1, X, X+1$, il campo F ha quattro elementi e possiamo scrivere

$$F = \mathbf{Z}_2(\alpha) = \{0, 1, \alpha, \alpha+1 \,;\, \alpha^2 = \alpha + 1\}.$$

Notiamo che $\alpha(\alpha+1) = \alpha^2 + \alpha = 1$.

3. Sia $p(X) := X^3 + 2X^2 + 4X + 2 \in \mathbf{Z}_5[X]$. Poiché $p(X)$ non ha radici in $\mathbf{Z}_5$, esso è irriducibile su $\mathbf{Z}_5$. Allora l'anello quoziente $F := \mathbf{Z}_2[X]/(p(X))$ è un campo e l'elemento $\alpha := \overline{X} \in F$ è tale che $p(\alpha) = 0$. Inoltre possiamo scrivere

$$F = \mathbf{Z}_2(\alpha) = \{c_0 + c_1\alpha + c_2\alpha^2 \,;\, c_i \in \mathbf{Z}_5 \,;\, p(\alpha) = 0\}.$$

Notiamo che F ha $5^3 = 125$ elementi. L'inverso di un elemento di F si può calcolare usando una identità di Bezout. Ad esempio, l'elemento $\beta := 1 + 3\alpha + \alpha^2$ di F è la classe del polinomio $1 + 3X + X^2 \in \mathbf{Z}_5[X]$. Poiché in $\mathbf{Z}_5[X]$ risulta

$$1 = -Xp(X) + (1 + 3X + X^2)(1 + 4X + X^2),$$

passando alle classi modulo $p(X)$, si ottiene che l'inverso di β in F è $1 + 4\alpha + \alpha^2$.

4. Il polinomio $p(X) := X^3 - 2$ è irriducibile su $\mathbf{Q}$; perciò l'anello quoziente $\mathbf{Q}[X]/(p(X))$ è un campo e, posto $\alpha := \overline{X}$, risulta

$$\mathbf{Q}[X]/p(X) := \mathbf{Q}(\alpha) := \{c_0 + c_1\alpha + c_2\alpha^2 \,;\, c_i \in \mathbf{Q} \,;\, \alpha^3 = 2\}.$$

Se γ è una qualsiasi radice complessa di $p(X)$, l'insieme

$$\mathbf{Q}(\gamma) := \{c_0 + c_1\gamma + c_2\gamma^2 \,;\, c_i \in \mathbf{Q}\}$$

è un sottocampo di $\mathbf{C}$ isomorfo a $\mathbf{Q}(\alpha)$.

L'inverso di $\beta := 1 + \gamma + \gamma^2$ in $\mathbf{Q}(\gamma)$ è $\gamma - 1$. Infatti il polinomio corrispondente a β in $\mathbf{Q}[X]$ è $X^2 + X + 1$. Inoltre risulta $X^3 - 2 = (X^2 + X + 1)(X - 1) - 1$ da cui, calcolando in γ, si ottiene $\beta(\gamma - 1) = 1$.

Ricordiamo che le radici complesse di $p(X)$ sono $\sqrt[3]{2}$, $\sqrt[3]{2}\xi$, $\sqrt[3]{2}\xi^2$ dove $\xi := (-1 + \sqrt{3}i)/2$ è una radice primitiva terza dell'unità (Esempio 4.5); quindi γ può assumere uno qualsiasi di questi valori.

5. Il polinomio $X^4 - 10X^2 + 1$ è irriducibile su $\mathbf{Q}$; perciò l'anello quoziente $\mathbf{Q}[X]/(p(X))$ è un campo e, posto $\alpha := \overline{X}$, risulta

$$\mathbf{Q}[X]/p(X) := \mathbf{Q}(\alpha) := \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3;\ c_i \in \mathbf{Q};\ \alpha^4 = 10\alpha^2 - 1\}.$$

Se γ è una qualsiasi radice complessa di $p(X)$, l'insieme

$$\mathbf{Q}(\gamma) := \{c_0 + c_1\gamma + c_2\gamma^2 + c_3\gamma^3;\ c_i \in \mathbf{Q}\}$$

è un sottocampo di $\mathbf{C}$ isomorfo a $\mathbf{Q}(\alpha)$.

Se $\beta := \gamma + 1$, allora il polinomio corrispondente a β è $X + 1$ e risulta

$$X^4 - 10X^2 + 1 = (X + 1)(X^3 - X^2 - 9X + 9) - 8.$$

Calcolando in γ, si ottiene che l'inverso di β in $\mathbf{Q}(\gamma)$ è $(1/8)(\gamma^3 - \gamma^2 - 9\gamma + 9)$.

Si può verificare senza difficoltà che le radici di $p(X)$ sono $\pm\sqrt{2} \pm \sqrt{3}$.

Teorema 7.6. Sia K un campo e sia $f(X) \in K[X]$ un polinomio di grado $n \geq 1$. Allora esiste un campo F contenente K in cui $f(X)$ abbia tutte le sue radici; equivalentemente

$$f(X) = c(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$$

per opportuni $\alpha_1, \ldots, \alpha_n \in F$.

Dimostrazione. Supponiamo che $f(X)$ non abbia già tutte le sue radici in K e sia $p(X)$ un fattore di $f(X)$ irriducibile su K di grado almeno 2 (Teorema 5.8). Per il Teorema 7.5, $p(X)$ ha una radice α_1 nel campo $F_1 := K[X]/(p(X)) := K(\alpha_1)$. Dunque in $F_1[X]$ si ha $f(X) = (X-\alpha_1)g(X)$, dove $\deg(g(X)) = n-1$ (Proposizione 4.1). Se $g(X)$ ha tutte le sue radici in F_1, allora $F = F_1$. Altrimenti, sia $p_1(X)$ un fattore di $g(X)$ irriducibile in $F_1[X]$ di grado almeno 2. Allora $p_1(X)$ ha una radice α_2 nel campo $F_2 := F_1[X]/(p_1(X)) = F_1(\alpha_2)$. Dunque in $F_2[X]$ si ha $f(X) = (X-\alpha_1)(X-\alpha_2)g_1(X)$, dove $\deg(g_1(X)) = n-2$.

Poiché, per motivi di grado, $f(X)$ ha al più n radici in un qualsiasi campo contenente K, al più dopo n passi, si otterrà un campo F in cui $f(X) = c(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$.

Esempi.

6. Sia $f(X) := X^4 + 2X^3 + 2X + 2 \in \mathbf{Z}_3[X]$; determiniamo un campo in cui $f(X)$ abbia tutte le sue radici. La fattorizzazione di $f(X)$ in polinomi irriducibili su $\mathbf{Z}_3$ è

$$f(X) = (X^2 + 2X + 2)(X^2 + 1).$$

Se $p(X) := X^2 + 1$ e $F_1 := \mathbf{Z}_3[X]/(p(X))$, allora $p(X)$ ha una radice α in F_1 e in $F_1[X]$ risulta $p(X) = (X+\alpha)(X+2\alpha)$. Inoltre

$$F_1 = \mathbf{Z}_3(\alpha) = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2 ; \alpha^2 = 2\} .$$

Il polinomio $q(X) := X^2 + 2X + 2$ ha radici in F_1 ; infatti è annullato da $2+\alpha$ e $2+2\alpha$. In conclusione, $f(X)$ ha tutte le sue radici in F_1 e risulta:

$$f(X) = (X+\alpha)(X+2\alpha)(X+(1+2\alpha))(X+(1+\alpha)) .$$

Notiamo che si può anche procedere considerando prima il polinomio $q(X)$. Poniamo $K_1 := \mathbf{Z}_3[X]/(q(X))$, allora $q(X)$ ha una radice β in K_1 e in $K_1[X]$ risulta $q(X) = (X+2\beta)(X+(2+\beta))$. Inoltre

$$K_1 = \mathbf{Z}_3(\beta) = \{0, 1, 2, \beta, \beta+1, \beta+2, 2\beta, 2\beta+1, 2\beta+2 ; \beta^2 = \beta+1\} .$$

Poiché in $K_1[X]$ risulta $p(X) = (X+\beta^2)(X+2\beta^2)$, il polinomio $f(X)$ ha tutte le sue radici in K_1 .

Non è difficile verificare che l'applicazione

$$F_1 \longrightarrow K_1 \quad \text{definita da} \quad c_0 + c_1\alpha \longrightarrow c_0 + c_1\beta^2$$

per ogni $c_0 , c_1 \in \mathbf{Z}_3$ è un isomorfismo di campi.

6. Sia $f(X) := X^5 + X^4 + 1 \in \mathbf{Z}_2[X]$; determiniamo un campo in cui $f(X)$ abbia tutte le sue radici. La fattorizzazione in elementi irriducibili di $f(X)$ in $\mathbf{Z}_2[X]$ è

$$f(X) = (X^2 + X + 1)(X^3 + X + 1) .$$

Se $p(X) := X^2 + X + 1$ e $F_1 := \mathbf{Z}_2[X]/(p(X))$, allora, come visto nell'esempio precedente, $p(X)$ ha una radice α in F_1 e in $F_1[X]$ risulta $p(X) = (X+\alpha)(X+(1+\alpha))$. Inoltre

$$F_1 = \mathbf{Z}_2(\alpha) = \{0, 1, \alpha, \alpha+1 ; \alpha^2 = \alpha+1\} .$$

Il polinomio $q(X) := X^3 + X + 1$ è irriducibile su F_1 , perché non ha radici in F_1 . Possiamo allora costruire il campo $F_2 := F_1[X]/(q(X))$. Il polinomio $q(X)$ ha una radice β in F_2 e in $F_2[X]$ risulta

$$q(X) = (X+\beta)(X^2 + \beta X + (1+\beta^2)) = (X+\beta)(X+\beta^2)(X+(\beta+\beta^2)) .$$

In conclusione, F_2 è un campo in cui $f(X)$ ha tutte le sue radici. Inoltre

$$F_2 = \mathbf{Z}_2(\alpha, \beta) = \{a+b\beta+c\beta^2 ; \ a, b, c \in \mathbf{Z}_2(\alpha) \ \text{e} \ \beta^3 = \beta+1\} =$$

$$\{c_{00} + c_{10}\alpha + c_{01}\beta + c_{02}\beta^2 + c_{11}\alpha\beta + c_{12}\alpha\beta^2 ; c_{ij} \in \mathbf{Z}_2 , \alpha^2 = \alpha+1 , \beta^3 = \beta+1\}$$

ha $2^6 = 64$ elementi.

Alternativamente, si può porre

$$K_1 := \mathbf{Z}_2[X]/(q(X)) = \mathbf{Z}_2(\gamma) = \{a+b\gamma+c\gamma^2 ; \ a, b, c \in \mathbf{Z}_2 \ \text{e} \ \gamma^3 = \gamma+1 \} \ \text{e}$$

$$K_2 := K_1[X]/(p(X)) = \mathbf{Z}_2(\gamma, \delta) = \{r+s\delta ; r, s \in \mathbf{Z}_2(\gamma) \ \text{e} \ \delta^2+\delta = 1\} .$$

Si verifica facilmente che l'applicazione

$$F_2 \longrightarrow K_2 \ \text{definita da} \ \Sigma c_{ij}\alpha^i\beta^j \longrightarrow \Sigma c_{ij}\delta^i\gamma^j$$

è un isomorfismo di campi.

E' importante osservare che, poiché $f(X)$ è riducibile, l'anello quoziente $\mathbf{Z}_2[X]/(f(X))$ non è un campo; nella costruzione è quindi necessario scomporre $f(X)$ in polinomi irriducibili.

ESERCIZI

1. Mostrare che la relazione di congruenza modulo un polinomio è una relazione di equivalenza in $K[X]$.

2. Sia K un campo e sia $p(X) \in K[X]$. Mostrare che, se $f(X)$ e $g(X)$ sono due polinomi differenti che hanno stesso grado $d < \deg(p(X))$, allora $\overline{f(X)} \neq \overline{g(X)}$.

3. Sia K un campo e sia $p(X) \in K[X]$. Mostrare che le operazioni di somma e prodotto definite nell'insieme quoziente $K[X]/(p(X))$ da

$$\overline{f(X)} + \overline{g(X)} = \overline{f(X)+g(X)} \quad \text{e} \quad \overline{f(X)} \cdot \overline{g(X)} = \overline{f(X)g(X)}$$

non dipendono dai rappresentanti.

4. Mostrare che, se p è un numero primo e $p(X) \in \mathbf{Z}_p[X]$ è irriducibile di grado n, allora l'anello quoziente $\mathbf{Z}_p[X]/(p(X))$ è un campo con p^n elementi.

5. Sia p un numero primo e $p(X) \in \mathbf{Z}_p[X]$ un polinomio irriducibile di grado n. Mostrare che il polinomio $p(X)$ ha tutte le sue radici nel campo $\mathbf{Z}_p[X]/(p(X))$. Precisamente, se α è una radice di $p(X)$, tutte le altre radici di $p(X)$ sono α, α^p, α^{p^2}, ... , $\alpha^{p^{n-1}}$.

6. Costruire un campo con 8 elementi e un campo con 9 elementi.

7. Sia $p(X) := X^2 + tX + 1 \in \mathbf{Z}_5[X]$. Stabilire per quali valori di $t \in \mathbf{Z}_5$ l'anello quoziente $\mathbf{Q}[X]/(p(X))$ è un campo.

8. Sia $p(X) := X^3 + 3X + t \in \mathbf{Q}[X]$. Stabilire per quali valori di $t \in \mathbf{Q}$ l'elemento α è invertibile in $K(\alpha) = \mathbf{Q}[X]/(p(X))$.

9. Sia $p(X) := X^3 + 3X + 3 \in \mathbf{Z}_5[X]$ e sia $\mathbf{Z}_5(\alpha) = \mathbf{Z}_5[X]/(p(X))$. Determinare l'inverso di α^2 e $1+\alpha$ in $\mathbf{Z}_5(\alpha)$.

10. Sia $p(X) \in \mathbf{Q}[X]$ un polinomio irriducibile su $\mathbf{Q}$ e sia γ una radice complessa di $p(X)$. Determinare l'inverso di β in $\mathbf{Q}(\gamma)$ in ognuno dei seguenti casi:

$$p(X) := X^2 - 5 \,,\ \beta := \gamma+1 \,;\quad p(X) := 4X^4 + 5X + 10 \,,\ \beta := \gamma^3+\gamma+1 \,;$$
$$p(X) := X^3 + 3X^2 + 9X + 6 \,,\ \beta := \gamma^2 \,.$$

11. Determinare un campo contenente $\mathbf{Z}_p$ in cui il polinomio $f(X)$ abbia tutte le sue radici nei seguenti casi:

$$f(X) := X^3 + 2X + 1 \,,\ p := 3, 5 \,;\quad f(X) := X^4 + 5 \,,\ p := 2, 3, 7 \,.$$

8. Anelli di polinomi su domini a fattorizzazione unica.

Ricordiamo che un dominio A si dice a fattorizzazione unica, in breve un UFD, se ogni elemento non nullo e non invertibile di A può essere fattorizzato in un numero finito di elementi irriducibili, univocamente determinati a meno dell'ordine e di elementi invertibili (Paragrafo 5).

In questo paragrafo, se non verrà specificato altrimenti, A denoterà sempre un UFD.

Nel Paragrafo 5, abbiamo provato che, se K è un campo, allora $K[X]$ è un UFD (Teorema 5.8); inoltre, sfruttando il fatto che sia $\mathbf{Z}$ che $\mathbf{Q}[X]$ sono UFD, abbiamo mostrato

nel Paragrafo 6 che anche $\mathbf{Z}[X]$ è un UFD (Teorema 6.6). Scopo di questo paragrafo è quello di estendere i metodi usati nel Paragrafo 6 per mostrare che, più generalmente, se A è un UFD, allora anche $A[X]$ è un UFD. Da questo seguirà, per induzione, che se A è un UFD, allora anche l'anello in n indeterminate $A[X_1, \ldots, X_n]$ è un UFD.

Premettiamo alcune definizioni ed alcune proprietà dei domini a fattorizzazione unica di cui faremo uso.

Ricordiamo che è possibile estendere ad un dominio qualsiasi la definizione di massimo comune divisore già data per l'anello dei polinomi a coefficienti in un campo nel Teorema 3.4; precisamente, se a e b sono due elementi non entrambi nulli di un dominio A si dice che un elemento $d \in A$ è un massimo comune divisore di a e b se d divide sia a che b ed è diviso da ogni divisore comune di a e b. E' immediato verificare che, se d e d' sono due massimi comuni divisori di a e b, allora d e d' sono associati; infatti essi si dividono reciprocamente (cf. Esercizio 3.3). Dunque, se esiste un massimo comune divisore d di a e b, esso resta definito a meno di elementi invertibili; nel seguito, mantenendo questa ambiguità, diremo che d è *il massimo comune divisore* di a e b. Diremo poi che a e b sono due elementi *coprimi* se il loro massimo comune divisore è invertibile in A.

Proposizione 8.1. Sia A un dominio a fattorizzazione unica. Allora

(a) Ogni elemento irriducibile di A è primo.

(b) Siano $a, b \in A$ e siano $a = p_1 \cdots p_r$ e $b = q_1 \cdots q_s$ fattorizzazioni in elementi irriducibili. Allora a divide b in A se e soltanto se $s \geq r$ e, con una opportuna rinumerazione dei fattori q_i di b, p_i è associato a q_i per $i = 1, \ldots, r$.

(c) Se $a, b \in A$ sono non entrambi nulli, allora esiste il loro massimo comune divisore.

Dimostrazione. (a) Sia p un elemento irriducibile di A e siano $x, y \in A$ tali che p divida xy; dunque esiste $t \in A$ tale che $at = xy$. Non potendo essere x e y entrambi invertibili, fattorizzando x o/e y in elementi irriducibili, per l'unicità della fattorizzazione, si ha che p è un fattore irriducibile di x o/e y, cioè che p divide x o/e y. Da ciò segue che p è un elemento primo.

(b) Supponiamo che a divida b in A. Allora esiste $c \in A$ tale che $ac = b$, ovvero $p_1 \cdots p_r c = q_1 \cdots q_s$. Se c è invertibile, dall'unicità della fattorizzazione segue immediatamente che $s = r$, e che, con una opportuna rinumerazione dei fattori q_i di b, p_i è associato a q_i per $i = 1, \ldots, r$; se c non è invertibile, basta fattorizzare c in elementi irriducibili e procedere in modo analogo. L'implicazione inversa è immediata.

(c) Per evitare casi banali si può supporre che a e b siano entrambi non nulli e non invertibili. Utilizzando sia i fattori irriducibili di a che quelli di b, possiamo scrivere:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \qquad \text{e} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

con $p_1, p_2, \ldots, p_r$ elementi irriducibili di A e $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_r$ interi non negativi. E' allora immediato verificare, per quanto provato in (b), che

$$d := p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)}$$

è il massimo comune divisore di a e b.

Il fatto che in un dominio a fattorizzazione unica esiste sempre il massimo comune divisore di due elementi non entrambi nulli, e quindi, per induzione, di un numero finito di elementi non tutti nulli, ci permette di porre la seguente definizione.

Sia A un dominio a fattorizzazione unica e sia $f(X) := a_0 + a_1X + \dots + a_nX^n \in A[X]$ un polinomio non nullo. Il massimo comune divisore dei coefficienti di $f(X)$, si dice il *contenuto di* $f(X)$ e si denota con $c(f)$; dunque $c(f) = MCD(a_0, a_1, \dots, a_n)$. Notiamo che, se $a \in A$, risulta $c(af) = ac(f)$.

Se $c(f)$ è un elemento invertibile di A, ovvero se due opportuni coefficienti di $f(X)$ sono coprimi, si dice che $f(X)$ è un *polinomio primitivo*. Ogni polinomio di $A[X]$ dotato di un coefficiente invertibile è primitivo; in particolare ogni polinomio monico di $A[X]$ è primitivo. E' immediato verificare che ogni polinomio associato ad un polinomio primitivo è primitivo e che un polinomio costante non nullo è primitivo se e soltanto se è invertibile.

Per ogni polinomio non nullo $f(X) \in A[X]$, possiamo allora scrivere $f(X) = c(f)f^*(X)$, dove $c(f) \in A$ e $f^*(X) \in A[X]$ è un polinomio primitivo. Tale scrittura è unica, a meno di costanti invertibili: infatti, se $f(X) = dg(X)$ con $d \in A$ e $g(X)$ un polinomio primitivo, allora si ha $c(f) = dc(g)$ e, poiché $c(g)$ è invertibile, $c(f)$ e d sono associati in A. Ne segue che anche $f^*(X)$ e $g(X)$ sono associati in $A[X]$.

A questo punto, possiamo estendere, con lievi modifiche, all'anello di polinomi $A[X]$ su un qualsiasi UFD A i risultati stabiliti per $\mathbf{Z}[X]$ nel Paragrafo A.1.6. In particolare la dimostrazione della seguente proposizione è analoga a quella della Proposizione 6.1 (Lemma di Gauss per $\mathbf{Z}[X]$); basta sostituire alla nozione di numero primo quella di elemento irriducibile ed aver presente che in un UFD le nozioni di elemento irriducibile e di elemento primo coincidono (Proposizione 8.1).

Proposizione 8.2 (Lemma di Gauss). Sia A un dominio a fattorizzazione unica. Allora il prodotto di due polinomi primitivi in $A[X]$ è un polinomio primitivo.

Dal Lemma di Gauss discende il seguente risultato che è una generalizzazione del Corollario 6.2 e si dimostra in modo analogo.

Corollario 8.3. Sia A un dominio a fattorizzazione unica e siano $f(X), g(X) \in A[X]$ polinomi non nulli. Allora $c(fg)$ e $c(f)c(g)$ sono associati.

Prima di proseguire, notiamo che, se K è il campo dei quozienti di A e

$$f(X) := \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \dots + \frac{a_n}{b_n}X^n \in K[X]$$

è un polinomio non nullo, ponendo $b := b_0b_1 \dots b_n$, il polinomio $g(X) := bf(X)$ appartiene a $A[X]$. Pertanto, se A è un UFD, in $K[X]$ risulta $f(X) = b^{-1}g(X) = b^{-1}c(g)g^*(X)$ dove $g^*(X)$ ha lo stesso grado di $f(X)$; in particolare $f(X)$ si può scrivere come prodotto di una costante e di un polinomio primitivo di $A[X]$ del suo stesso grado.

Il seguente risultato è stato dimostrato per $\mathbf{Z}[X]$ nel Corollario 6.4.

Proposizione 8.4. Siano A un un dominio a fattorizzazione unica, K il suo campo dei quozienti e $f(X) \in A[X]$ un polinomio non nullo.

(a) Se $f(X)$ è costante, esso è irriducibile in $A[X]$ se e soltanto se lo è in A.

(b) Se $f(X)$ ha grado positivo, esso è irriducibile in $A[X]$ se e soltanto se è primitivo e irriducibile in $K[X]$.

Dimostrazione. (a) Basta osservare che, per la formula del grado, ogni divisore di un polinomio costante non nullo è costante.

(b) Sia $f(X)$ di grado positivo e irriducibile in $A[X]$. Poiché $A[X]$ ed A hanno gli stessi elementi invertibili (Proposizione 3.1), ogni fattore costante di $f(X)$ è invertibile in A; dunque $f(X)$ è primitivo.

Supponiamo che $f(X)$ sia riducibile in $K[X]$, cioè che esistano in $K[X]$ due polinomi $g(X)$ e $h(X)$, entrambi di grado positivo, tali che $f(X) = g(X)h(X)$. Essendo K il campo dei quozienti di A, per quanto sopra osservato, esistono $a, b \in A$ e $r(X), s(X) \in A[X]$ tali che $ag(X) = r(X) = c(r)r^*(X)$ e $bh(X) = s(X) = c(s)s^*(X)$ con $r^*(X), s^*(X) \in A[X]$ polinomi primitivi dello stesso grado di $g(X)$ e $h(X)$ rispettivamente. Si ha pertanto che $abf(X) = c(r)c(s)r^*(X)s^*(X)$, dove per il Lemma di Gauss, $r^*(X)s^*(X)$ è un polinomio primitivo (Proposizione 8.2). Ne segue che $d := ab$ e $c(r)c(s)$ sono associati in A, cioè esiste un elemento invertibile u in A tale che $c(r)c(s) = ud$. Allora si ha che $f(X) = ur^*(X)s^*(X)$; dove i polinomi $ur^*(X)$ e $s^*(X)$ hanno entrambi grado positivo e pertanto sono divisori non banali di $f(X)$ in $A[X]$, contro l'ipotesi che $f(X)$ sia irriducibile in $A[X]$. Ne segue che $f(X)$ è irriducibile anche in $K[X]$.

Viceversa, sia $f(X)$ primitivo e irriducibile in $K[X]$ e siano $g(X), h(X) \in A[X]$ tali che $f(X) = g(X)h(X)$; essendo $f(X)$ irriducibile in $K[X]$, $g(X)$ e $h(X)$ non possono essere entrambi di grado positivo. Supponiamo che sia $g(X)$ ad avere grado zero, cioè che sia $g(X) = a \in A$; allora, poiché $f(X) = ah(X)$, a divide tutti i coefficienti di $f(X)$ e perciò a è invertibile, perché $f(X)$ è primitivo. Ne segue che $f(X)$ è irriducibile in $A[X]$.

Possiamo adesso dimostrare il risultato centrale di questo paragrafo.

Teorema 8.5 Se A è un UFD, allora $A[X]$ è un UFD.

Dimostrazione. Sia $f(X) \in A[X]$ un polinomio non nullo e non invertibile. Se $f(X)$ è di grado zero, essendo A un UFD, $f(X)$ si può fattorizzare nel prodotto di elementi irriducibili in A che sono irriducibili anche in $A[X]$ (Proposizione 8.4 (a)).

Supponiamo che $f(X)$ sia di grado positivo e consideriamolo come un elemento di $K[X]$, dove K è il campo dei quozienti di A. Per il teorema di fattorizzazione unica in $K[X]$ (Teorema 5.8), si ha $f(X) = p_1(X)\, p_2(X) \dots p_r(X)$, dove ogni $p_i(X)$ è un polinomio irriducibile di $K[X]$. Poiché K è il campo dei quozienti di A, per quanto sopra osservato, per ogni $i = 1, ..., r$, esistono $b_i, c_i \in A$ ed un polinonio $q_i(X) \in A[X]$ primitivo tali che $b_i p_i(X) = c_i q_i(X)$. Poiché $p_i(X)$ è irriducibile in $K[X]$, si ha che anche $q_i(X)$ è irriducibile in $K[X]$, perché è associato a $p_i(X)$ in $K[X]$. Ne segue che $q_i(X)$, essendo primitivo, è irriducibile in $A[X]$ (Proposizione 8.4(b)). Allora otteniamo:

$$b_1b_2\dots b_rp_1(X)p_2(X)\dots p_r(X) = b_1b_2\dots b_rf(X) = b_1b_2\dots b_rc(f)f^*(X) =$$
$$c_1c_2\dots c_rq_1(X)q_2(X)\dots q_r(X)$$

con $c(f) \in A$ e $f^*(X) \in A[X]$ un polinomio primitivo; inoltre per il Lemma di Gauss (Lemma 8.3) anche il polinomio $q_1(X)q_2(X)\dots q_r(X)$ di $A[X]$ è primitivo.

Si ha così che $b_1b_2\dots b_rc(f)$ e $c_1c_2\dots c_r$ sono associati in A e perciò $f^*(X)$ e $q_1(X)q_2(X)\dots q_r(X)$ sono associati in $A[X]$, cioè esiste un elemento invertibile $u \in A$ tale che

$$f(X) = c(f)f^*(X) = uc(f)q_1(X)\, q_2(X) \dots q_r(X)\,.$$

Poiché $uc(f) \in A$ ed A è un UFD, allora $uc(f)$ può essere fattorizzato in elementi irriducibili in A, che sono anche elementi irriducibili di $A[X]$ (Proposizione 8.4 (a)). Infine, poiché $q_1(X), q_2(X), \dots, q_r(X)$ sono irriducibili in $A[X]$, otteniamo che $f(X)$ si può fattorizzare nel prodotto di elementi irriducibili di $A[X]$.

Mostriamo ora l'unicità della fattorizzazione. Se $f(X)$ ha grado zero, non c'è niente da dimostrare, perché A è un UFD. Supponiamo che $f(X)$ abbia grado positivo e sia $f(X) = aq_1(X)q_2(X)\dots q_r(X)$, con $a \in A$ e $q_1(X), q_2(X), \dots, q_r(X)$ polinomi irriducibili di $A[X]$ di grado positivo. Poiché $q_1(X), q_2(X), \dots, q_r(X)$ sono primitivi (Proposizione 8.4 (b)), per il Lemma di Gauss anche il loro prodotto lo è. Ne segue che a e $c(f)$ sono associati in A e perciò i fattori irriducibili costanti di $f(X)$ sono univocamente determinati, a meno dell'ordine e di elementi invertibili, essendo i fattori irriducibili di $c(f)$ in A. D'altra parte, sia $p(X)$ un fattore di $f(X)$ che ha grado positivo ed è irriducibile in $A[X]$. Poiché i polinomi $q_1(X), q_2(X), \dots, q_r(X), p(X)$ sono irriducibili anche in $K[X]$ (Proposizione 8.4 (b)), per l'unicità della fattorizzazione in $K[X]$ (Teorema 5.8), possiamo supporre che, a meno dell'ordine, $p(X)$ sia associato a $q_1(X)$ in $K[X]$, ovvero che $bp(X) = cq_1(X)$, per opportuni $b, c \in A\backslash\{0\}$. Ma allora, essendo $p(X)$ e $q_1(X)$ entrambi primitivi, b e c sono associati in A e $p(X)$ e $q_1(X)$ sono associati in $A[X]$. In conclusione, i fattori di $f(X)$ che hanno grado positivo e sono irriducibili in $A[X]$ sono univocamente determinati, a meno dell'ordine e di elementi invertibili.

Corollario 8.6. Se A è un UFD, allora l'anello $A[X_1, \dots, X_n]$ dei polinomi in n indeterminate su A è un UFD.

Dimostrazione. Basta osservare che $A[X_1, \ldots, X_n] \simeq (A[X_1, \ldots, X_{n-1}])[X_n]$ (Paragrafo 1) e procedere per induzione su n, facendo uso del Teorema 8.5.

Corollario 8.7. Gli anelli di polinomi $\mathbf{Z}[X_1, \ldots, X_n]$ e $K[X_1, \ldots, X_n]$, dove K è un campo, sono UFD.

ESERCIZI

1. Mostrare che un dominio A è un UFD se e soltanto se ogni elemento non nullo e non invertibile di A può essere fattorizzato nel prodotto di un numero finito di elementi primi (Sugg. Usare il fatto che in un UFD ogni elemento irriducibile è primo (Teorema 8.1)).

2. Sia A un UFD e siano $a, b \in A$ due elementi non nulli. Verificare che, se

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{e} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

con $p_1, p_2, \ldots, p_r$ elementi irriducibili di A e $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_r$ interi non negativi, allora

$$d := p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_r^{\min(\alpha_r,\beta_r)} \quad \text{e} \quad m := p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_r^{\max(\alpha_r,\beta_r)}$$

sono rispettivamente il massimo comune divisore e il minimo comune multiplo di a e b.

3. Provare che il polinomio $f(X,Y) := X^2 + Y^2 + 1$ è irriducibile in $\mathbf{C}[X,Y]$.

4. Fattorizzare il polinomio $g(X,Y) := X^3 - Y^3$ nel prodotto di polinomi irriducibili in $\mathbf{Q}[X,Y]$.

5. Provare il seguente Criterio di Irriducibilità (Criterio di Irriducibilità di Eisenstein generalizzato):

Sia A un UFD e sia $f(X) := a_0 + a_1X + \ldots + a_nX^n \in A[X]$ un polinomio di grado $n > 1$. Se p è un elemento primo di A tale che p divide $a_0, a_1, \ldots, a_{n-1}$, p non divide a_n e p^2 non divide a_0, allora $f(X)$ è irriducibile in $A[X]$ (Sugg. Adattare la dimostrazione data per il caso $A = \mathbf{Z}$ nel Teorema 6.7).

6. Verificare che il polinomio $f(X,Y) := Y^4 - 8X^2Y^3 + 6XY^2 - 10X^2Y - 2X$ è irriducibile in $\mathbf{Q}[X,Y]$ (Sugg. Usare l'esercizio precedente).

9. Formule di interpolazione. Metodi di fattorizzazione.

Due polinomi non nulli a coefficienti in un dominio A che abbiano grado al più uguale ad n ed assumano stesso valore in $n+1$ elementi distinti di A sono uguali (Corollario 4.3); perciò, scelti $a_0, a_1, \ldots, a_n \in A$, tutti distinti, esiste al più un polinomio in $A[X]$ di grado $k \leq n$ che assume valori fissati $b_0, b_1, \ldots, b_n$ in $a_0, a_1, \ldots, a_n$. D'altra parte, se A è un campo, come mostreremo tra poco, un tale polinomio esiste. Esso infatti resta definito dalle seguenti formule, che vengono dette *Formule di Interpolazione* perché permettono anche di calcolare immediatamente i valori che il polinomio assume in ogni elemento del campo una volta noti i suoi valori $b_0, \ldots, b_n$ in $a_0, \ldots, a_n$.

Proposizione 9.1 (Formula di Interpolazione di Lagrange). Sia K un campo e siano $a_0, \ldots, a_n, b_0, \ldots, b_n \in K$, con $a_0, \ldots, a_n$ tutti distinti. Allora il polinomio

$$f(X) := \sum_{i=0}^{n} \frac{b_i(X-a_0)\cdots(X-a_{i-1})(X-a_{i+1})\cdots(X-a_n)}{(a_i-a_0)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)} \in K[X]$$

è tale che $f(a_0) = b_0$, $f(a_1) = b_1$, $\ldots$, $f(a_n) = b_n$.

Alla Formula di interpolazione di Lagrange si può aggiungere la Formula di Interpolazione di Newton, a volte più conveniente per i calcoli.

E' possibile costruire il polinomio $f(X)$ della proposizione precedente imponendo passo dopo passo le condizioni richieste nel modo seguente.

Si inizia considerando l'unico polinomio costante di $K[X]$, $\varphi_0(X) := \lambda_0$ con $\lambda_0 \in K$, che assume il valore a_0 in b_0; ovviamente deve essere $\lambda_0 = b_0$.

Per ottenere il polinomio $\varphi_1(X) \in K[X]$ di grado al più uguale a 1 che assume i valori b_0, b_1 in a_0, a_1 rispettivamente, si può pensare di aggiungere a $\varphi_0(X)$ un termine del tipo $\lambda_1(X - a_0)$ con $\lambda_1 \in K$. Perché il polinomio $\varphi_0(X) + \lambda_1(X - a_0)$ assuma in a_1 il valore b_1, si deve avere $\lambda_1 = \dfrac{b_1 - \lambda_0}{(a_1 - a_0)}$. Pertanto otteniamo

$$\varphi_1(X) := \lambda_0 + \lambda_1(X-a_0), \text{ con } \lambda_0 = b_0 \text{ e } \lambda_1 = \frac{b_1 - \lambda_0}{(a_1 - a_0)}.$$

Aggiungiamo ora a $\varphi_1(X)$ un altro termine, in modo da ottenere un polinomio $\varphi_2(X)$ di grado al più uguale a 2 con la ulteriore proprietà di assumere in a_2 il valore b_2; per non vanificare il lavoro già fatto, questo termine deve essere della forma $\lambda_2(X - a_0)(X - a_1)$. Ma perché il polinomio $\varphi_2(X) := \varphi_1(X) + \lambda_2(X - a_0)(X - a_1)$ assuma in a_2 il valore b_2, si deve avere $\lambda_2 = \dfrac{\dfrac{b_2 - \lambda_0}{(a_2 - a_0)} - \lambda_1}{(a_2 - a_1)}$; dunque il polinomio di $K[X]$ di grado al più uguale a 2 che assume in a_0, a_1, a_2 ordinatamente i valori b_0, b_1, b_2. è

$$\varphi_2(X) := \lambda_0 + \lambda_1(X-a_0) + \lambda_2(X - a_0)(X - a_1),$$

$$\text{con } \lambda_0 = b_0, \ \lambda_1 = \frac{b_1 - \lambda_0}{(a_1 - a_0)} \text{ e } \lambda_2 = \frac{\dfrac{b_2 - \lambda_0}{(a_2 - a_0)} - \lambda_1}{(a_2 - a_1)}.$$

In generale, sia $1 < k \leq n$ e sia

$$\varphi_{k-1}(X) := \lambda_0 + \lambda_1(X-a_0) + \ldots + \lambda_{k-1}(X-a_0)(X-a_1)\ldots(X-a_{k-2})$$

il polinomio di $K[X]$ di grado al più uguale a $k-1$ che assume i valori $b_0, \ldots, b_{k-1}$ in $a_0, \ldots, a_{k-1}$ rispettivamente. Allora il polinomio

$$\varphi_k(X) := \varphi_{k-1}(X) + \lambda_k(X-a_0)(X-a_1)\ldots(X-a_{k-1})$$

assume ulteriormente in a_k il valore b_k per

$$\lambda_k = \frac{\dfrac{\dfrac{b_k - \lambda_0}{(a_k - a_0)} - \lambda_1}{\cdots\cdots} - \lambda_2}{(a_k - a_{k-2})} - \lambda_{k-1}}{(a_k - a_{k-1})} .$$

Per $k = n$ si ottiene perciò il polinomio

$$f(X) = \varphi_n(X) := \lambda_0 + \lambda_1(X-a_0) + \lambda_2(X-a_0)(X-a_1) + \ldots + \lambda_n(X-a_0)(X-a_1)\ldots(X-a_{n-1}) .$$

Il polinomio $\varphi_k(X)$, che assume i valori $b_0, \ldots, b_k$ in $a_0, \ldots, a_k$, prende il nome di k-*esima funzione interpolare* di $f(X)$, per $k = 0, \ldots, n$.

Notiamo che, nelle formule precedenti, λ_k è il coefficiente di X^k in $\varphi_k(X)$. Questo prova che λ_k non dipende dall'ordine in cui si sono scelti $a_0, \ldots, a_k$. Se K è un campo numerico reale, possiamo ad esempio ordinare gli a_i in modo crescente, affinché nelle formule per determinare i coefficienti λ_i tutte le differenze a denominatore siano positive.

Si può riassumere quanto descritto nella seguente proposizione.

Proposizione 9.2 (Formula di Interpolazione di Newton). Sia K un campo e siano $a_0, \ldots, a_n, b_0, \ldots, b_n \in K$, con $a_0, \ldots, a_n$ tutti distinti. Allora il polinomio $f(X) \in K[X]$ di grado al più uguale ad n tale che $f(a_i) = b_i$ per $i = 0, \ldots, n$ si può scrivere come

$$f(X) := \lambda_0 + \lambda_1(X-a_0) + \lambda_2(X-a_0)(X-a_1) + \ldots + \lambda_n(X-a_0)(X-a_1)\ldots(X-a_{n-1}) ,$$

dove i coefficienti λ_i sono definiti per induzione nel seguente modo:

$$\lambda_0 = b_0 \; ; \quad \lambda_1 = \frac{b_1 - \lambda_0}{(a_1 - a_0)} \quad \text{e} \quad \lambda_k = \frac{\dfrac{\dfrac{b_k - \lambda_0}{(a_k - a_0)} - \lambda_1}{\cdots\cdots} - \lambda_2}{(a_k - a_{k-2})} - \lambda_{k-1}}{(a_k - a_{k-1})} , \quad \text{per } 1 < k \leq n .$$

Notiamo anche che, posto

$$f_0(X) := f(X) \quad \text{e} \quad f_i(X) := \frac{f_{i-1}(X) - f_{i-1}(a_{i-1})}{(X - a_{i-1})} , \quad \text{per } i = 1, \ldots, n ,$$

allora risulta $\lambda_i = f_i(a_i)$.

Esempi.

1. Costruiamo il polinomio di $\mathbf{Q}[X]$ di grado al più uguale a 2 che assume valori $b_0 = 0$, $b_1 = 1$, $b_2 = 2$ rispettivamente in $a_0 = 1$, $a_1 = 2$, $a_2 = 3$.

Le formule di interpolazione di Lagrange forniscono il polinomio di primo grado:

$$f(X) = \frac{(X-1)(X-3)}{(2-1)(2-3)} + \frac{2(X-1)(X-2)}{(3-1)(3-2)} = X - 1 .$$

2. Costruiamo il polinomio di $\mathbf{Q}[X]$ di grado al più uguale a 2 che assume valori $b_0 = 0$, $b_1 = 1$, $b_2 = -2$ rispettivamente in $a_0 = 1$, $a_1 = 2$, $a_2 = 3$.

Le formule di interpolazione di Lagrange forniscono il polinomio di secondo grado:

$$f(X) = \frac{(X-1)(X-3)}{(2-1)(2-3)} - \frac{2(X-1)(X-2)}{(3-1)(3-2)} = -2X^2 + 7X - 5 .$$

Se invece vogliamo usare le formule di Newton, otteniamo:

$$\lambda_0 = 0 , \ \lambda_1 = 1 , \ \lambda_2 = 0 .$$

Da cui ancora:

$$f(X) = (X-1) - 2(X-1)(X-2) = -2X^2 + 7X - 5.$$

3. Costruiamo il polinomio di $\mathbf{Q}[X]$ di grado al più uguale a 3 che assume valori $b_0 = 1$, $b_1 = -1$, $b_2 = 1$, $b_3 = 0$ rispettivamente in $a_0 = 0$, $a_1 = 1$, $a_2 = -1$, $a_3 = 2$.

Usando le formule di Newton otteniamo:

$$\lambda_0 = 1 , \ \lambda_1 = -2 , \ \lambda_2 = -1 , \ \lambda_3 = \frac{5}{6} .$$

Dunque il polinomio cercato è:

$$f(X) = 1 - 2X - X(X-1) + \frac{5}{6}X(X-1)(X+1) = \frac{5}{6}X^3 - X^2 - \frac{11}{6}X + 1 .$$

Se ordiniamo gli a_i in modo crescente, ponendo $a_0 = -1$, $a_1 = 0$, $a_2 = 1$, $a_3 = 2$ e, consistentemente, $b_0 = 1$, $b_1 = 1$, $b_2 = -1$, $b_3 = 0$, otteniamo lo stesso polinomio. Infatti risulta

$$\lambda_0 = 1 , \ \lambda_1 = 0 , \lambda_2 = -1 , \lambda_3 = \frac{5}{6} ,$$

da cui

$$f(X) = 1 - (X+1)X + \frac{5}{6}(X+1)X(X-1) = \frac{5}{6}X^3 - X^2 - \frac{11}{6}X + 1 .$$

Le formule di interpolazione possono essere usate per determinare i fattori irriducibili di un polinomio a coefficienti razionali; il seguente metodo è dovuto a Kronecker.

Ricordiamo che ogni polinomio a coefficienti in $\mathbf{Q}$ si può scrivere come prodotto di una costante per un polinomio a coefficienti interi e primitivo. Sia dunque $f(X) \in \mathbf{Z}[X]$ un polinomio primitivo di grado $n \geq 2$. Se $f(X)$ non è irriducibile in $\mathbf{Q}[X]$, per la formula del grado e la Proposizione 6.3, esso ha un fattore primitivo $g(X) \in \mathbf{Z}[X]$ di grado $s \leq n/2$. Per stabilire se $f(X)$ ha effettivamente un tale fattore, procediamo nel modo seguente.

Supponiamo che $g(X)$ sia un polinomio di grado s che divida $f(X)$ in $\mathbf{Z}[X]$ e consideriamo $s+1$ interi $a_0, \ldots, a_s$. Allora, se $f(X) = g(X)h(X)$, valutando in a_i otteniamo $f(a_i) = g(a_i)h(a_i)$; perciò $g(a_i)$ deve dividere $f(a_i)$ in $\mathbf{Z}$, per $i = 0, \ldots, s$. Ora, $f(a_i)$ ha un numero finito di divisori e, per ogni $(s+1)$-pla di interi $(b_0, \ldots, b_s)$, con b_i che divide $f(a_i)$, le formule di interpolazione forniscono un unico polinomio $k(X) \in \mathbf{Q}[X]$ tale che

$k(a_i) = b$; perciò $g(X)$ è tra i polinomi a coefficienti interi che è possibile ottenere in questo modo. Tali polinomi sono un numero finito e, per stabilire quali tra essi dividono $f(X)$ in $\mathbf{Z}[X]$, si può usare l'algoritmo della divisione in $\mathbf{Q}[X]$; in particolare, i divisori di $f(X)$ vanno cercati tra i polinomi il cui coefficiente direttore divide il coefficiente direttore di $f(X)$.

In conclusione, tutti i divisori di $f(X)$ in $\mathbf{Z}[X]$ si ottengono con un numero finito di verifiche.

E' anche utile ricordare che ci sono soltanto due polinomi associati a un divisore $g(X)$ di $f(X)$ in $\mathbf{Z}[X]$, precisamente $g(X)$ e $-g(X)$; perciò ci si può limitare a considerare i polinomi il cui coefficiente direttore è positivo. Non è difficile verificare poi che, se $g(X)$ è determinato dalla $(s+1)$-pla $(b_0 , \ldots, b_s)$, allora $-g(X)$ è determinato dalla $(s+1)$-pla $(-b_0 , \ldots, -b_s)$.

Esempi.

4. Sia $f(X) := X^4 + X^2 + 1$. Se $f(X)$ è riducibile, esso ha un fattore al più di secondo grado. Se poniamo $a_0 = -1$, $a_1 = 0$, $a_2 = 1$, risulta $f(a_0) = 3$, $f(a_1) = 1$, $f(a_2) = 3$. Quindi, se $g(X) \in \mathbf{Z}[X]$ è un polinomio di grado al più uguale a due che divide $f(X)$, può risultare soltanto $g(a_0) = \pm 1 , \pm 3$, $g(a_1) = \pm 1$, $g(a_2) = \pm 1, \pm 3$. Inoltre

$$g(X) = \lambda_0 + \lambda_1(X-a_0) + \lambda_2(X-a_0)(X-a_1) =$$
$$\lambda_0 + \lambda_1(X+1) + \lambda_2(X+1)X = (\lambda_0 + \lambda_1) + (\lambda_1 + \lambda_2)X + \lambda_2X^2 ;$$

dove, per la Formula di Newton,

$$\lambda_0 = g(a_0) , \ \lambda_1 = g(a_1) - g(a_0) , \ \lambda_2 = \frac{g(a_0) + g(a_2)}{2} + g(a_1) .$$

Osserviamo ora che, poiché $f(X)$ è monico, il coefficiente direttore di $g(X)$ può essere soltanto uguale a ± 1 . Ma poiché, quando $\lambda_2 = 0$, $\lambda_1 = g(a_1) - g(a_0)$ non può assumere questi valori, $g(X)$ deve essere di secondo grado con coefficiente direttore $\lambda_2 = \pm 1$. Dunque, i soli valori da prendere in considerazione per la terna $(g(a_0) , g(a_1) , g(a_2))$ sono:

$$\pm(1, 1, -1) , \ \pm(1, -1, -1) , \pm(3, 1, -3) , \pm(3, -1, -3) , \pm(1, -1, 3) , \pm(3, -1, 1) ,$$

che forniscono, per la terna $(\lambda_0 , \lambda_1 , \lambda_2)$, rispettivamente i valori

$$\pm(1, 0, 1) , \pm(1, -2, -1) , \pm(3, -2, 1) , \pm(3, -4, -1) , \pm(1, -2, 1) , \pm(3, -4, 1) ,$$

a cui corrispondono i polinomi di $\mathbf{Z}[X]$ con coefficiente direttore positivo:

$$1 + X + X^2 ; 1 + 3X + X^2 ; 1 - X + X^2 ; 1 + 5X + X^2 ; -1 - X + X^2 ; -1 - 3X + X^2 .$$

Si verifica subito che risulta:

$$f(X) = (1 + X + X^2)(1 - X + X^2) .$$

Il metodo di fattorizzazione appena illustrato si può anche applicare per determinare i fattori irriducibili di un polinomio a coefficienti in un dominio a fattorizzazione unica con un numero finito di elementi invertibili.

Infatti, siano A un tale dominio e K il suo campo dei quozienti. Analogamente al caso in cui $A = \mathbf{Z}$, se $f(X), g(X) \in A[X]$ e $g(X)$ divide $f(X)$ in $A[X]$, allora, per ogni $a \in A$, $g(a)$ divide $f(a)$ in A . Poiché ogni elemento di A ha un numero finito di associati, i

divisori di $f(a)$ sono in numero finito. Allora, fissati $s+1$ interi $a_0, \ldots, a_s$, le $(s+1)$-ple di interi $(b_0, \ldots, b_s)$, con b_i che divide $f(a_i)$, sono in numero finito e, per ognuna di esse, le formule di interpolazione forniscono un unico polinomio $k(X) \in K[X]$ tale che $k(a_i) = b_i$. Dunque i divisori $g(X)$ di $f(X)$ di grado al più uguale ad s sono tra i polinomi a coefficienti in A ottenuti in questo modo e si possono determinare in un numero finito di passi.

Esempi.

5. Se A è un dominio a fattorizzazione unica con un numero finito di elementi invertibili, i polinomi in n indeterminate a coefficienti in A si possono fattorizzare con un numero finito di passi usando il metodo di Kronecker.

Infatti, come abbiamo appena visto, tale metodo si può applicare al caso di una indeterminata. Inoltre, procedendo per induzione su n, sia $A_1 := A[X_1, \ldots, X_{n-1}]$. Se $f(X) \in A[X_1, \ldots, X_n]$, risulta

$$f(X) = g_0(X_1, \ldots, X_{n-1}) + g_1(X_1, \ldots, X_{n-1})\, X_n + \ldots + g_n(X_1, \ldots, X_{n-1})\, X_n^m ,$$

dove $g_i(X_1, \ldots, X_{n-1}) \in A_1$, $0 \le i \le m$. Poiché A_1 è ancora un dominio a fattorizzazione unica ed i suoi elementi invertibili sono quelli di A (cf. Esercizio 3.4), allora $f(X)$ si può ancora fattorizzare con un numero finito di passi usando il metodo di Kronecker.

In pratica, scriviamo $f(X) = f_1(X_1, \ldots, X_{n-1}) f^*(X_n)$, dove $f_1(X_1, \ldots, X_{n-1}) := c(f) := \mathrm{MCD}(g_0(X_1, \ldots, X_{n-1}), \ldots, g_n(X_1, \ldots, X_{n-1})) \in A_1$ e $f^*(X_n) \in A_1[X_n]$ è un polinomio primitivo. Allora $f^*(X)$ non ha fattori irriducibili di grado zero in X_n ed inoltre i suoi fattori possono essere determinati con un numero finito di passi. Possiamo poi ripetere il procedimento per fattorizzare $f_1(X_1, \ldots, X_{n-1})$ in A_1. Precisamente, poniamo $A_2 := A[X_1, \ldots, X_{n-2}]$ e, considerando $f_1(X_1, \ldots, X_{n-1})$ come un polinomio nell'indeterminata X_{n-1} a coefficienti in A_2, scriviamo $f_1(X_1, \ldots, X_{n-1}) = f_2(X_1, \ldots, X_{n-2}) f_1^*(X_1, \ldots, X_{n-1})$, dove $f_2(X_1, \ldots, X_{n-2}) = c(f_1) \in A_2$ e $f_1^*(X_1, \ldots, X_{n-1}) \in A_2[X_{n-1}]$ è primitivo, cioè non ha fattori di grado zero in X_{n-1}. Procediamo poi come prima per fattorizzare $f_1^*(X_1, \ldots, X_{n-1})$ e $f_2(X_1, \ldots, X_{n-2})$. Dopo un numero finito di passi, otteniamo una fattorizzazione completa di $f(X)$ in fattori irriducibili.

Tale metodo si può applicare anche per fattorizzare un polinomio in n indeterminate a coefficienti in $\mathbf{Q}$, ricordando che ogni tale polinomio si può scrivere, come nel caso $n = 1$, come una costante per un polinomio primitivo a coefficienti in $\mathbf{Z}$.

ESERCIZI

1. Mostrare, usando il metodo di Kronecker, che il polinomio $X^4 + X + 1$ è irriducibile su $\mathbf{Q}$.

2. Usando il metodo di Kronecker, fattorizzare in polinomi irriducibili su $\mathbf{Q}$ i polinomi

$$X^5 + X^4 + X^2 + X + 2 \; ; \quad 3X^4 + 5X^2 - 1 .$$

3. Usando il metodo di Kronecker, fattorizzare in polinomi irriducibili il polinomio

$$X^3 + Y^3 + Z^3 - X^2(Y+Z) - Y^2(X+Z) - Z^2(X+Y) + 2XYZ \in \mathbf{Z}[X, Y, Z] .$$

10. Polinomi simmetrici e funzioni simmetriche. Il discriminante di un polinomio.

Sia A un dominio e K il suo campo dei quozienti. Per $n \geq 1$, poniamo al solito $\mathbf{X} := (X_1, \ldots, X_n)$ e $A[\mathbf{X}] := A[X_1, \ldots, X_n]$. Il campo dei quozienti di $A[\mathbf{X}]$ è il campo $K(\mathbf{X})$ delle funzioni razionali a coefficienti in K.

Per ogni $\sigma \in \mathbf{S}_n$, consideriamo l'applicazione $\varphi_\sigma : K(\mathbf{X}) \longrightarrow K(\mathbf{X})$ definita da $\varphi_\sigma(f(X_1, \ldots, X_n)) := f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. Si verifica facilmente che φ_σ è un automorfismo $K(\mathbf{X})$ e che l'insieme $\Sigma := \{\varphi_\sigma ; \sigma \in \mathbf{S}_n\}$ è un sottogruppo di $\mathrm{Aut}(K(\mathbf{X}))$ isomorfo a $\mathbf{S}_n$.

La funzione razionale $f(X_1, \ldots, X_n) \in K(\mathbf{X})$ si dice una *funzione simmetrica* se $\varphi_\sigma(f(X_1, \ldots, X_n)) = f(X_1, \ldots, X_n)$, per ogni $\sigma \in \mathbf{S}_n$, ovvero se essa rimane invariata per una qualsiasi permutazione delle indeterminate $X_1, \ldots, X_n$. Il sottoinsieme di $A[\mathbf{X}]$ costituito dai polinomi simmetrici è un sottoanello di $A[\mathbf{X}]$ ed è detto *l'anello dei polinomi simmetrici* su A. Non è difficile infatti verificare che somme, differenze e prodotti di polinomi simmetrici sono ancora polinomi simmetrici. Il campo dei quozienti dell'anello dei polinomi simmetrici su A è il sottocampo di $K(\mathbf{X})$ costituito dalle funzioni simmetriche.

Esempi.

1. Ogni polinomio di $A[X]$ è simmetrico; infatti l'unica permutazione sull'insieme $\{X\}$ è l'identità.

2. Il polinomio $X + Y - X^3Y^3$ è simmetrico, mentre il polinomio $X + XY$ non lo è.

3. I polinomi di $A[\mathbf{X}]$ del tipo $p_k(X) := X_1^k + X_2^k + \ldots + X_n^k$, $k \geq 1$, sono simmetrici. Essi vengono chiamati *polinomi di Newton.*

4. Il polinomio $D(\mathbf{X}) := \prod_{1 \leq i < j \leq n}(X_i - X_j)^2$ è un polinomio simmetrico in $X_1, \ldots, X_n$. Per convincersene, basta osservare che, permutando le indeterminate, al più cambia il segno di qualche fattore $(X_i - X_j)$.

Di particolare interesse sono i seguenti polinomi simmetrici in $X_1, \ldots, X_n$, detti *polinomi simmetrici elementari* (o *funzioni simmetriche elementari*):

$$s_1 := s_1(\mathbf{X}) := \Sigma_{i=1,\ldots,n} X_i ;$$

$$s_2 := s_2(\mathbf{X}) := \Sigma_{1 \leq i_1 < i_2 \leq n} X_{i_1} X_{i_2} ;$$

$$\ldots\ldots\ldots$$

$$s_r := s_r(\mathbf{X}) := \Sigma_{1 \leq i_1 < \ldots < i_r \leq n} X_{i_1} X_{i_2} \ldots X_{i_r} ;$$

$$\ldots\ldots\ldots$$

$$s_n := s_n(\mathbf{X}) := X_1 \ldots X_n .$$

I polinomi simmetrici elementari in $X_1, \ldots, X_{n-1}$ si ottengono da $s_1, \ldots, s_n$ ponendo $X_n = 0$. Infatti, se indichiamo con $s'_1, \ldots, s'_{n-1}$ i polinomi simmetrici elementari in $X_1, \ldots, X_{n-1}$, notiamo che valgono le *relazioni ricorsive*:

$$s_1 = s'_1 + X_n \ ;$$
$$s_2 = s'_2 + X_n s'_1$$
$$\ldots\ldots\ldots$$
$$s_r = s'_r + X_n s'_{r-1}$$
$$\ldots\ldots\ldots$$
$$s_{n-1} = s'_{n-1} + X_n s'_{n-2}$$
$$s_n = X_n s'_{n-1} \ .$$

Esempi.

5. Se $n = 1$, l'unico polinomio simmetrico elementare è il polinomio $s_1 := X$.

Se $n = 2$, i polinomi simmetrici elementari in X_1, X_2 sono:

$$s_1 := X_1 + X_2 \ \text{ e } \ s_2 := X_1 X_2 \ .$$

Se $n = 3$, i polinomi simmetrici elementari in X_1, X_2, X_3 sono:

$$s_1 := X_1 + X_2 + X_3 \ , \ s_2 := X_1X_2 + X_1X_3 + X_2X_3 \ , \ s_3 := X_1X_2X_3 \ .$$

L'importanza dei polinomi simmetrici elementari risiede nel fatto che, come dimostreremo tra poco, ogni polinomio simmetrico di $A[\mathbf{X}]$ si può esprimere come un polinomio in $s_1, \ldots, s_n$ ed inoltre $s_1, \ldots, s_n$ sono *algebricamente indipendenti* su A, cioè $f(s_1, \ldots, s_n) \neq 0$ per ogni polinomio non nullo $f(X_1, \ldots, X_n) \in A[\mathbf{X}]$. In questo modo, l'anello dei polinomi simmetrici su A risulta essere isomorfo all'anello dei polinomi $A[\mathbf{X}]$. Infatti l'applicazione $A[X_1, \ldots, X_n] \longrightarrow A[s_1, \ldots, s_n]$ definita da $f(X_1, \ldots, X_n) \longrightarrow f(s_1, \ldots, s_n)$ è un omomorfismo di anelli suriettivo, il cui nucleo è costituito dai polinomi $f(X_1, \ldots, X_n)$ tali che $f(s_1, \ldots, s_n) = 0$. Perciò $s_1, \ldots, s_n$ sono algebricamente indipendenti su A se e soltanto se questa applicazione ha nucleo zero, ovvero è un isomorfismo.

Notiamo però che, se $n \geq 2$, l'anello dei polinomi simmetrici $A[s_1, \ldots, s_n]$ è propriamente contenuto in $A[\mathbf{X}]$, perché in questo caso esistono polinomi non simmetrici.

Proposizione 10.1. I polinomi simmetrici elementari in n indeterminate su A sono algebricamente indipendenti su A.

Dimostrazione. Procediamo per induzione sul numero n delle indeterminate.

Se $n = 1$, allora l'unico polinomio simmetrico elementare è il polinomio $s_1 := X_1$ e non c'è niente da dimostrare. Supponiamo che l'asserzione sia vera per $n-1$ indeterminate e mostriamola vera per n indeterminate.

Se $s_1, \ldots, s_n$ fossero algebricamente dipendenti su A, esisterebbe un polinomio non nullo $f(\mathbf{Y}) := f(Y_1, \ldots, Y_n)$ a coefficienti in A tale che $f(s_1, \ldots, s_n) = 0$. Supponiamo che $f(\mathbf{Y})$ abbia grado minimo possibile e scriviamolo come un polinomio in Y_n:

$$f(\mathbf{Y}) = f_0(Y_1, \ldots, Y_{n-1}) + f_1(Y_1, \ldots, Y_{n-1})Y_n + \ldots + f_m(Y_1, \ldots, Y_{n-1})Y_n^m \ .$$

Il polinomio $f_0(Y_1, \ldots, Y_{n-1})$ è non nullo, altrimenti $f(\mathbf{Y})$ sarebbe divisibile per Y_n e $s_1, \ldots, s_n$ annullerebbero il polinomio $f(\mathbf{Y})/Y_n$ che ha grado minore di quello di $f(\mathbf{Y})$.

Poiché

$$f(s_1, \ldots, s_n) = f_0(s_1, \ldots, s_{n-1}) + f_1(s_1, \ldots, s_{n-1})s_n + \ldots + f_m(s_1, \ldots, s_{n-1})s_n^m = 0 ,$$

e X_n divide s_n, allora, ponendo $X_n = 0$, otteniamo

$$f(s_1, \ldots, s_n) = f_0(s_1, \ldots, s_{n-1}) = 0 .$$

Indicando con $s'_1, \ldots, s'_{n-1}$ i polinomi simmetrici elementari in $X_1, \ldots, X_{n-1}$ e usando le formule ricorsive, abbiamo

$$f_0(s_1, \ldots, s_{n-1}) = f_0(s'_1, \ldots, s'_{n-1}) + X_n h(s'_1, \ldots, s'_{n-1}) = 0 ,$$

da cui, ancora per $X_n = 0$, otteniamo $f_0(s'_1, \ldots, s'_{n-1}) = 0$, contro l'ipotesi induttiva.

Facciamo ora vedere che ogni polinomio simmetrico si può esprimere come un polinomio nei polinomi simmetrici elementari. Osserviamo intanto che un polinomio $\varphi(s_1, \ldots, s_n)$ in $s_1, \ldots, s_n$ su A è senz'altro un polinomio simmetrico in $X_1, \ldots, X_n$, perché lo sono $s_1, \ldots, s_n$ e i polinomi simmetrici su A formano un sottoanello di $A[\mathbf{X}]$. Dunque $A[s_1, \ldots, s_n]$ è contenuto nell'anello dei polinomi simmetrici.

Poiché s_i è omogeneo di grado i in $X_1, \ldots, X_n$, se $cs_1^{k_1} \ldots s_n^{k_n}$, $c \neq 0$, è un termine di $\varphi(s_1, \ldots, s_n)$, il suo grado totale in $X_1, \ldots, X_n$ è $k := k_1 + 2k_2 + \ldots + nk_n$. L'intero k si chiama il *peso del termine* $cs_1^{k_1} \ldots s_n^{k_n}$ e *il peso del polinomio* $\varphi(s_1, \ldots, s_n)$ si definisce come il massimo peso dei suoi termini. E' evidente che il grado in $X_1, \ldots, X_n$ del polinomio $\varphi(s_1, \ldots, s_n)$ non è superiore al suo peso.

Teorema 10.2 (Teorema Fondamentale sulle Funzioni Simmetriche). Ogni polinomio simmetrico $f(\mathbf{X}) \in A[X_1, \ldots, X_n]$ di grado k si può esprimere in modo unico come un polinomio di peso k nei polinomi simmetrici elementari $s_1, \ldots, s_n$ a coefficienti in A.

Dimostrazione. Procediamo per doppia induzione sul numero n delle indeterminate e sul grado k del polinomio.

Se $n = 1$, allora l'unico polinomio simmetrico elementare è il polinomio $s_1 := X_1$ e non c'è niente da dimostrare. Supponiamo che il teorema sia vero per tutti i polinomi in $n-1$ indeterminate. Per dimostrare che esso è vero per n indeterminate, procediamo per induzione sul grado di $f(\mathbf{X})$. Se questo grado è zero, il teorema è vero banalmente. Supponiamo allora che esso sia vero se il grado di $f(\mathbf{X})$ è al più $k-1$ e dimostriamolo vero se il grado è k.

Sia $f(\mathbf{X}) \in A[X_1, \ldots, X_n]$ di grado k. Possiamo scrivere:

$$f(\mathbf{X}) = f_0(X_1, \ldots, X_{n-1}) + f_1(X_1, \ldots, X_{n-1})X_n + \ldots + f_m(X_1, \ldots, X_{n-1})X_n^m ,$$

dove i polinomi $f_i(X_1, \ldots, X_{n-1})$ hanno grado al più uguale a k, per $i = 0, \ldots, m$.

Se $f(\mathbf{X})$ è simmetrico, anche i polinomi $f_i(X_1, \ldots, X_{n-1})$ sono simmetrici. Perciò, indicando con $s'_1, \ldots, s'_{n-1}$ i polinomi simmetrici elementari in $X_1, \ldots, X_{n-1}$, per l'ipotesi induttiva, si ha che ogni $f_i(X_1, \ldots, X_{n-1})$ si può esprimere come un polinomio $\varphi_i(s'_1, \ldots,$

s'_{n-1}) di peso (in $s'_1, \ldots, s'_{n-1}$) uguale al suo grado, che è al più uguale a k. Perciò otteniamo che

$$f(\mathbf{X}) = \varphi_0(s'_1, \ldots, s'_{n-1}) + \varphi_1(s'_1, \ldots, s'_{n-1})X_n + \ldots + \varphi_m(s'_1, \ldots, s'_{n-1})X_n^m ,$$

dove i polinomi $\varphi_i(s'_1, \ldots, s'_{n-1})$ hanno peso al più uguale a k.

Usando le relazioni ricorsive

$$s'_1 = s_1 - X_n , \quad s'_j = s_j - X_n s'_{j-1} \text{ per } j = 2, \ldots, n-1 ,$$

possiamo esprimere $\varphi_i(s'_1, \ldots, s'_{n-1})$ come un polinomio in $s_1, \ldots, s_{n-1}, X_n$. Notiamo che in questo modo risulta:

$$\varphi_0(s'_1, \ldots, s'_{n-1}) = \varphi_0(s_1, \ldots, s_{n-1}) + X_n\psi(s_1, \ldots, s_{n-1}, X_n)$$

e dunque

$$f(\mathbf{X}) = \varphi_0(s_1, \ldots, s_{n-1}) + \psi_1(s_1, \ldots, s_{n-1})X_n + \ldots + \psi_m(s_1, \ldots, s_{n-1})X_n^r .$$

Consideriamo ora il polinomio simmetrico

$$f_1(\mathbf{X}) := f(\mathbf{X}) - \varphi_0(s_1, \ldots, s_{n-1}) .$$

Poiché $\varphi_0(s_1, \ldots, s_{n-1})$ ha peso al più uguale a k (in $s_1, \ldots, s_{n-1}, s_n$), esso ha grado al più uguale a k. Dunque $f_1(\mathbf{X})$ ha grado al più uguale a k. Inoltre, $f_1(\mathbf{X})$ è diviso da X_n e perciò, essendo simmetrico, esso è diviso da ogni indeterminata X_i. Ne segue che

$$f_1(\mathbf{X}) = (X_1 \ldots X_n)g(\mathbf{X}) = s_n g(\mathbf{X}) ,$$

dove $g(\mathbf{X})$ è un polinomio simmetrico di grado al più uguale a $k-n < k$. Per l'ipotesi induttiva, allora $g(\mathbf{X})$ si può esprimere come un polinomio di peso $k-n$ nei polinomi simmetrici elementari $s_1, \ldots, s_n$ e dunque anche $f(\mathbf{X}) = \varphi_0(s_1, \ldots, s_{n-1}) + s_n g(\mathbf{X})$ si può esprimere come un polinomio nei polinomi simmetrici elementari $s_1, \ldots, s_n$. Questo polinomio ha peso al più uguale a k, perché sia $\varphi_0(s_1, \ldots, s_{n-1})$ che $s_n g(\mathbf{X})$ hanno peso al più uguale a k; ma allora esso ha peso esattamente uguale a k, altrimenti $f(\mathbf{X})$ avrebbe grado minore di k.

Per finire, l'espressione di $f(\mathbf{X})$ come un polinomio nei polinomi simmetrici elementari è unica perché $s_1, \ldots, s_n$ sono algebricamente indipendenti su A e allora, se $\varphi(s_1, \ldots, s_n) = \psi(s_1, \ldots, s_n)$, il polinomio differenza $\varphi(\mathbf{Y}) - \psi(\mathbf{Y})$ deve essere il polinomio nullo.

Corollario 10.3. Se F è un campo, il campo delle funzioni simmetriche su F è $F(s_1, \ldots, s_n)$ ed è isomorfo al campo delle funzioni razionali $F(X_1, \ldots, X_n)$.

Dimostrazione. Il campo delle funzioni simmetriche su F è il sottocampo di $F(X_1, \ldots, X_n)$ formato dalle funzioni razionali $f(\mathbf{X})/g(\mathbf{X})$ dove $f(\mathbf{X})$ e $g(\mathbf{X})$ sono polinomi simmetrici su F e $g(\mathbf{X}) \neq 0$. Per il teorema precedente, $f(\mathbf{X})/g(\mathbf{X}) = \varphi(s_1, \ldots, s_n)/\psi(s_1, \ldots, s_n) \in F(s_1, \ldots, s_n)$. Infine, poiché $s_1, \ldots, s_n$ sono algebricamente indipendenti su F, i campi $F(X_1, \ldots, X_n)$ e $F(s_1, \ldots, s_n)$ sono isomorfi.

Esempi.

6. La dimostrazione del Teorema 10.2 è costruttiva e fornisce un metodo per esprimere effettivamente un polinomio simmetrico in funzione dei polinomi simmetrici elementari. Ad esempio, consideriamo il polinomio

$$f(X_1, X_2, X_3) := X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2 \in F[\mathbf{X}] .$$

Ponendo $X_3 = 0$, otteniamo il polinomio

$$f(X_1, X_2, 0) = X_1^2X_2 + X_2^2X_1 = X_1X_2(X_1 + X_2) = s'_1s'_2 ,$$

dove $s'_1 = X_1 + X_2$ e $s'_2 = X_1X_2$. Passando di nuovo a tre indeterminate, consideriamo il polinomio $f(X_1, X_2, X_3) - s_1s_2$, dove $s_1 = X_1 + X_2 + X_3$ e $s_2 = X_1X_2 + X_1X_3 + X_2X_3$. Otteniamo

$$f(X_1, X_2, X_3) - s_1s_2 = - 3X_1X_2X_3 = -3s_3 ,$$

Perciò

$$f(X_1, X_2, X_3) = s_1s_2 - 3s_3 .$$

7. Le relazioni tra i polinomi di Newton e i polinomi simmetrici elementari su F sono date dalle cosidette *formule di Newton*:

$$s_1 = p_1 ;$$

$$2s_2 = - p_2 + p_1s_1 ;$$

$$3s_3 = p_3 - p_2s_1 + p_1s_2 ;$$

$$\cdots\cdots$$

$$ns_n = (-1)^n(p_n - p_{n-1}s_1 + \ldots + p_1s_{n-1}) .$$

e, per $k > n$,

$$p_k - p_{k-1}s_1 + p_{k-2}s_2 - \ldots + (-1)^n p_{k-n}s_n = 0 .$$

Queste relazioni ci permettono di ricavare i polinomi di Newton in funzione dei polinomi simmetrici elementari e viceversa. In particolare, otteniamo che $F(s_1, \ldots, s_n) = F(p_1, \ldots, p_n)$ e che anche $p_1, \ldots, p_n$ sono algebricamente indipendenti su F.

Ad esempio, per $k = 2$, si ottiene $p_2(\mathbf{X}) := X_1^2 + X_2^2 + \ldots + X_n^2 = s_1^2 - 2s_2$.

8. Dato un campo F, il *determinante di Vandermonde* in n indeterminate su F è il polinomio $V(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ ottenuto calcolando il determinante della matrice

$$A := (X_i^j)_{1\le i\le n,\ 0\le j\le n-1} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \end{pmatrix} .$$

Non è difficile mostrare che risulta $V(X_1, \ldots, X_n) = \prod_{1\le i<j\le n}(X_i - X_j)$ e dunque

$$D(\mathbf{X}) := \prod_{1\le i<j\le n}(X_i - X_j)^2 = V(\mathbf{X})^2.$$

Questa osservazione ci permette di calcolare il polinomio simmetrico $D(\mathbf{X})$ in funzione dei polinomi di Newton e quindi dei polinomi simmetrici elementari. Infatti si ha

$$D(\mathbf{X}) = V(\mathbf{X})^2 = |A|^2 = |A|\,|{}^tA| = |A\,{}^tA| = \begin{vmatrix} n & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & \cdots & p_{2n-2} \end{vmatrix} .$$

Ad esempio per $n = 2$ si ottiene:

$$D(X_1, X_2) := 2p_2 - p_1^2 = s_1^2 - 4s_2 .$$

In generale però l'espressione del polinomio simmetrico $D(\mathbf{X})$ in funzione dei polinomi simmetrici elementari è piuttosto complicata. Già per $n = 3$, si ottiene

$$D(X_1, X_2, X_3) = s_1^2 s_2^2 - 4s_2^3 - 4s_1^3 s_3 - 27s_3^2 + 18s_1 s_2 s_3 .$$

Introduciamo ora una indeterminata T su $A[\mathbf{X}]$ e cosideriamo l'anello $A[X_1, \ldots, X_n, T] = A[\mathbf{X}][T]$. Il polinomio

$$g(\mathbf{X}, T) := (T-X_1)(T-X_2)\ldots(T-X_n) \in A[\mathbf{X}][T]$$

si dice il *polinomio generale* di grado n su A. Sviluppando i prodotti, si ottiene

$$g(\mathbf{X}, T) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \ldots + (-1)^n s_n ;$$

dunque i polinomi simmetrici elementari di $A[\mathbf{X}]$ sono (a meno del segno) i coefficienti i questo polinomio. Precisamente, il coefficiente di T^k è $(-1)^{n-k} s_{n-k}$, per $k = 1, \ldots, n$. In particolare,

$$g(\mathbf{X}, T) \in A[s_1, \ldots, s_n][T] .$$

Dal momento che le funzioni simmetriche elementari sono algebricamente indipendenti su A, il polinomio generale di grado n su A è un polinomio di grado n i cui coefficienti sono indeterminate su A. Ogni polinomio monico di grado n su A si ottiene assegnando valori specifici in A a $s_1, \ldots, s_n$.

Consideriamo in particolare il caso in cui F sia un campo numerico. Sia $f(T) := a_n T^n + a_{n-1} T^{n-1} + a_{n-2} T^{n-2} + \ldots + a_0 \in F[T]$ e siano $\alpha_1, \ldots, \alpha_n$ le sue radici complesse (non necessariamente tutte distinte). Allora, in $\mathbf{C}[T]$, risulta $f(T) = a_n(T-\alpha_1)\ldots(T-\alpha_n)$ e perciò il polinomio $(a_n)^{-1} f(T)$ si ottiene dal polinomio generale $g(\mathbf{X}, T)$ su F sostituendo $\alpha_1, \ldots, \alpha_n$ a $X_1, \ldots, X_n$. Ne segue che i coefficienti di $(a_n)^{-1} f(T)$ sono le funzioni simmetriche elementari calcolate nelle radici $\alpha_1, \ldots, \alpha_n$ (indipendentemente dall'ordine scelto per esse). Precisamente, valgono le relazioni

$$(a_n)^{-1} a_k = (-1)^{n-k} s_{n-k}(\alpha_1, \ldots, \alpha_n) .$$

Poiché per il Teorema 10.2 ogni funzione simmetrica è una funzione razionale in $s_1, \ldots, s_n$, allora il valore di ogni funzione simmetrica calcolata nelle radici di $f(T)$ si può esprimere come funzione razionale dei coefficienti di $f(T)$ ed in particolare è un elemento del campo F.

Il polinomio simmetrico $D(\mathbf{X}) := \prod_{1\le i<j\le n}(X_i-X_j)^2$ considerato nell'Esempio 10.4 si dice il *discriminante* del polinomio generale $g(\mathbf{X}, T)$ di grado n. Se $f(T)$ è un particolare polinomio di grado n a coefficienti numerici, il *discriminante* di $f(T)$ è il valore del polinomio $D(\mathbf{X})$ calcolato nelle radici complesse $\alpha_1, \ldots, \alpha_n$ di $f(T)$ e si indica con $D(f)$. Ovvero

$$D(f) := D(\alpha_1, \ldots, \alpha_n) := \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2 ,$$

Notiamo che tutti i polinomi associati a $f(T)$ su F hanno le stesse radici e perciò anche lo stesso discriminante; ci possiamo dunque limitare a considerare polinomi monici.

Dalla definizione segue che il discriminante del polinomio $f(T)$ è nullo se e soltanto se $f(T)$ ha radici multiple. Dunque il discriminante di un polinomio irriducibile su F è non nullo (Proposizione 5.5). Inoltre, il discriminante del polinomio $f(T)$, essendo una funzione simmetrica delle radici, è esprimibile in funzione dei coefficienti e in particolare appartiene al campo di definizione di $f(T)$.

Osserviamo che tutte queste considerazioni si estendono senza difficoltà al caso in cui F sia un campo qualsiasi. Infatti, come visto nel Paragrafo 7, ogni polinomio a coefficienti in F ha tutte le sue radici in un opportuno campo contenente F.

Per semplificare il calcolo del discriminante, si può trasformare il polinomio monico $f(T) := T^n + a_{n-1}T^{n-1} + a_{n-2}T^{n-2} + \ldots + a_0$ in un altro polinomio che abbia alcuni coefficienti nulli e stesso discriminante. Particolarmente utile, anche per il calcolo delle radici, è la cosiddetta *forma ridotta* del polinomio $f(T)$, che si ottiene da $f(T)$ con la trasformazione $T = X - a_{n-1}/n$ (detta *trasformazione di F. Viète*). In questo modo, si ottiene un polinomio $\tilde{f}(X)$ in cui il termine di grado $n-1$ è zero. E' evidente che α è una radice di $f(T)$ se e soltanto se $\beta := \alpha - a_{n-1}/n$ è una radice di $\tilde{f}(X)$. Perciò $f(T)$ e la sua forma ridotta $\tilde{f}(X)$ hanno stesso discriminante.

Esempi.

9. Sia $f(X) := X^2 + bX + c \in \mathbf{Q}[X]$. Se α_1, α_2 sono le radici di $f(X)$, allora risulta

$$b = -s_1(\alpha_1, \alpha_2) = -(\alpha_1+\alpha_2) , \quad c = s_2(\alpha_1, \alpha_2) = \alpha_1\alpha_2 \quad \text{e} \quad D(f) = D(\alpha_1, \alpha_2) = b^2 - 4c .$$

10. Sia $f(T) := T^3 + a_2T^2 + a_1T + a_0 \in \mathbf{Q}[T]$. Se $\alpha_1, \alpha_2, \alpha_3$ sono le radici di $f(T)$, allora risulta:

$$a_2 = -s_1(\alpha_1, \alpha_2, \alpha_3) = -(\alpha_1+\alpha_2+\alpha_3) ,$$
$$a_1 = s_2(\alpha_1, \alpha_2, \alpha_3) = \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 ,$$
$$a_0 = -s_3(\alpha_1, \alpha_2, \alpha_3) = -\alpha_1\alpha_2\alpha_3 .$$

Con la posizione $T = X - a_2/3$ si ottiene la forma ridotta di $f(T)$:

$$\tilde{f}(X) := X^3 + pX + q ,$$

dove $p := a_1 - a_2^2/3$ e $q := a_0 - a_1a_2/3 + 2a_2/27$.

Le radici di $\tilde{f}(X)$ sono $\beta_i := \alpha_i - a_2/3$, per $i = 1, 2, 3$ e inoltre risulta:

$$s_1(\beta_1, \beta_2, \beta_3) = 0 , \quad s_2(\beta_1, \beta_2, \beta_3) = p , \quad s_3(\beta_1, \beta_2, \beta_3) = -q ,$$

da cui, usando l'espressione calcolata nell'Esempio 10.8, si ottiene

$$D(f) = D(\tilde{f}) = D(\beta_1, \beta_2, \beta_3) = -4p^3 - 27q^2 .$$

Mostriamo ora che il discriminante di un polinomio $f(X)$ può essere calcolato tramite i valori che il polinomio derivato assume nelle radici $\alpha_1, \ldots, \alpha_n$ di $f(X)$.

Proposizione 10.4. Sia $f(X) \in F[X]$ un polinomio monico di grado n e siano $\alpha_1, \ldots, \alpha_n$ le sue radici. Allora risulta

$$D(f) = (-1)^{n(n-1)/2} \prod_{1 \le i \le n} f'(\alpha_i) .$$

Dimostrazione. Poiché $f(X) = (X-\alpha_1)\ldots(X-\alpha_n)$, allora si ha

$$f'(X) = \sum_{1 \le k \le n} (X-\alpha_1)\ldots(X-\alpha_{k-1})(X-\alpha_{k+1})\ldots(X-\alpha_n) ;$$

da cui

$$f'(\alpha_i) = (\alpha_i-\alpha_1)\ldots(\alpha_i-\alpha_{k-1})(\alpha_i-\alpha_{k+1})\ldots(\alpha_i-\alpha_n) ,$$

per ogni $i = 1, \ldots, n$. Infine

$$D(f) := D(\alpha_1, \ldots, \alpha_n) := \prod_{1 \le i < j \le n} (\alpha_i-\alpha_j)^2 =$$
$$(-1)^{n(n-1)/2} \prod_{i \ne j} (\alpha_i-\alpha_j) = (-1)^{n(n-1)/2} \prod_{1 \le i \le n} f'(\alpha_i) .$$

Esempi.

11. Sia $f(X) := X^p - 1 \in \mathbf{Q}[X]$, dove $p \ne 2$ è un numero primo. Se ξ è una radice primitiva p-sima dell'unità, le radici di $f(X)$ sono $\xi, \xi^2, \ldots, \xi^p = 1$ (Esempio 4.4). Poiché $f'(X) = pX^{p-1}$, risulta

$$D(f) = (-1)^{(p-1)/2} \prod_{1 \le i \le p} p\xi^{i(p-1)} = (-1)^{(p-1)/2}\, p^p \xi^N ,$$

per un opportuno $N \ge 1$. Osserviamo ora che, poiché $D(f) \in \mathbf{Q}$, anche

$$\xi^N = (-1)^{(p-1)/2} D(f)/p^p \in \mathbf{Q} .$$

Allora $\xi^N = 1$ e

$$D(f) = (-1)^{(p-1)/2} p^p .$$

12. Il risultante di due polinomi. Dati due polinomi non nulli a coefficienti in un campo (numerico) F

$$f(X) := a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0 \quad \text{e} \quad g(X) := b_m X^m + b_{m-1}X^{n-1} + \ldots + b_0 ,$$

con $n > 0$, poniamo

$$R(f, g) := b_m{}^n \quad \text{se} \quad m = 0 .$$

Altrimenti, se $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_m$ sono le radici di $f(X)$ e $g(X)$ rispettivamente, poniamo

$$R(f, g) := a_n{}^m b_m{}^n \prod_{1 \le i \le n,\ 1 \le j \le m} (\alpha_i - \beta_j) .$$

$R(f, g)$ si dice il *risultante* di $f(X)$ e $g(X)$ e si può far vedere che esso è il determinante della seguente matrice quadrata di ordine $n+m$, detta *matrice di J. Sylvester* (cf. [Van der Waerden, Modern Algebra, Par. 82]).

$$\begin{pmatrix} a_0 & a_1 & \dots & a_n & 0 & 0 & \dots & & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & 0 & \dots & 0 \\ 0 & 0 & a_0 & a_1 & \dots & a_n & 0 & 0 \dots & 0 \\ \dots & & & & & & & & \\ 0 & 0 & 0 \dots & & \dots & 0 & 0 & a_0 \; a_1 \dots & a_n \\ b_0 & b_1 & \dots & b_m & 0 & 0 & \dots & & 0 \\ 0 & b_0 & b_1 & \dots & b_m & 0 & 0 \dots & & 0 \\ \dots & & & & & & & & \\ 0 & 0 & 0 \dots & & & \dots & 0 & 0 \; b_0 \; b_1 \dots & b_m \end{pmatrix}$$

In particolare, $R(f, g) \in F$. E' evidente che $R(f, g) = 0$ se e soltanto se $f(X)$ e $g(X)$ hanno qualche radice in comune. Inoltre si verifica subito che $R(f, g) = (-1)^{nm} R(g, f)$.

Osserviamo che, poiché $g(X) = b_m(X-\beta_1)\dots(X-\beta_m)$, allora risulta $g(\alpha_i) = b_m(\alpha_i-\beta_1)\dots(\alpha_i-\beta_m)$ e si ha

$$R(f, g) := a_n^m \prod_{1\le i\le n} g(\alpha_i) .$$

Se $f(X)$ è monico, dalla Proposizione 10.4, otteniamo allora che il discriminante di $f(X)$ è, a meno del segno, il risultante di $f(X)$ e della sua derivata $f'(X)$, perché

$$D(f) = (-1)^{n(n-1)/2} \prod_{1\le i\le n} f'(\alpha_i) = (-1)^{n(n-1)/2} R(f, f') .$$

Questa espressione ci fornisce un metodo per calcolare il discriminante di un polinomio usando l'algoritmo della divisione euclidea. Infatti non è difficile verificare che, se $f(X) = g(X)q(X) + r(X)$, con $r(X) \neq 0$ e $\deg(r(X)) = d$, allora

$$R(g, f) = a_n^{m-d} R(g, r) .$$

Sia ad esempio $f(X) := X^2 + bX + c$. Allora $f'(X) = 2X + b$ e

$$f(X) = f'(X)(X/2 + a/4) + (b - a^2/4) .$$

Posto $r := (b-a^2/4)$, si ottiene

$$D(f) = -R(f, f') = -R(f', f) = -2^2 R(f', r) = -4r = a^2 - 4b .$$

ESERCIZI

1. Verificare che somme, differenze e prodotti di polinomi simmetrici sono ancora polinomi simmetrici.

2. Verificare che la corrispondenza $\mathbf{S}_n \longrightarrow \mathrm{Aut}(K(\mathbf{X}))$ definita da $\sigma \longrightarrow \varphi_\sigma$, per ogni $\sigma \in \mathbf{S}_n$, è un omomorfismo iniettivo di gruppi.

3. Mostrare che un polinomio omogeneo di grado k si può esprimere come un polinomio nei polinomi simmetrici elementari i cui termini abbiano tutti peso uguale a k.

4. Calcolare il determinante di Vandermonde in n indeterminate e verificare che risulta $V(X_1, \dots, X_n) = \prod_{1\le i<j\le n}(X_i-X_j)$.

5. Stabilire se i seguenti polinomi in X, Y, Z sono simmetrici e, in caso affermativo, esprimerli in funzione dei polinomi simmetrici elementari:

$$X^2Y + Y^2Z + Z^2X ;$$

$$(X + Y)(X + Z)(Y + Z) ;$$
$$X^3Y + Y^3Z + Z^3X - XY^3 - YZ^3 - ZX^3 ;$$
$$X^3Y^3 + Y^3Z^3 + Z^3X^3 .$$

6. Sia $f(X) = X^3 - X + 1 \in \mathbf{Q}[X]$ e siano ρ, σ, τ le sue radici, con $\rho \in R$. Mostrare che $\sigma + \tau = -\rho$ e $\sigma\tau = -1/\rho$.

7. Mostrare che un polinomio $f(X) \in F[X]$ è irriducibile su F se e soltanto se la sua forma ridotta è irriducibile su F (Sugg. Usare la Proposizione 6.5).

8. Siano $f(X), g(X) \in F[X]$ due polinomi non costanti di grado uguale a n e m rispettivamente e sia $f(X) = g(X)q(X) + r(X)$, con $r(X) \neq 0$ e $\deg(r(X)) = d$. Mostrare che

$$R(f, g) = (-1)^{nm} R(g, f) \quad \text{e} \quad R(g, f) = a_n^{m-d} R(g, r) .$$

9. Siano $f(X), g(X) \in F[X]$ due polinomi monici non costanti. Mostrare che

$$D(fg) = D(f)D(g)R(f, g)^2 .$$

10. Sia $f(X)$ uno dei seguenti polinomi:

$$X^2 + X + 1 , \quad X^3 - X^2 + 1 , \quad X^3 - 2X + 1 , \quad X^4 + X + 1 .$$

Determinare $D(f)$ usando la matrice di Sylvester di $f(X)$ e $f'(X)$.

11. Sia $f(X) := X^3 + pX + q$. Determinare $D(f)$ con l'algoritmo euclideo della divisione, come descritto nell'Esempio 10.12.

11. Formule risolutive per le quazioni di terzo e quarto grado.

Metodi generali per la risoluzione delle equazioni polinomiali di terzo grado del tipo $X^3 + pX = q$, con p, q interi positivi, furono trovati per la prima volta attorno al 1515 da Scipione del Ferro, che tuttavia non li rese noti. Successivamente, le formule risolutive furono riscoperte da Niccolò Fontana, detto Tartaglia, che le comunicò a Gerolamo Cardano a condizione che questi le mantenesse segrete. Tuttavia Cardano, convinto della loro importanza, e venuto a conoscenza del fatto che esse erano già state dimostrate da Scipione del Ferro, le rese note pubblicandole nel suo libro *Ars Magna* del 1545. Inoltre Cardano estese il metodo di Tartaglia per risolvere anche le equazioni del tipo $X^3 = pX + q$ e $X^3 + q = pX$ (ricordiamo che all'epoca si operava soltanto con i numeri positivi mentre i numeri negativi, benché già noti, venivano usati principalmente con il significato di *debiti*). Successivamente, Raffaele Bombelli ripubblicò queste formule con l'aggiunta di alcuni commenti esemplificativi nel secondo capitolo del suo libro *Algebra*, nel 1572.

Come visto nel Paragrafo 10, non è restrittivo considerare un'equazione di terzo grado a coefficienti numerici della forma

$$f(X) := X^3 + pX + q = 0$$

(Esempio 10.10).

Le formule risolutive di Tartaglia-Cardano si basano sull'identità algebrica

$$(u+v)^3 = u^3 + v^3 + 3uv(u+v) ,$$

che rispecchia la possibilità di scomporre geometricamente un cubo in due cubi più piccoli e tre parallelepipedi uguali.

Ponendo $X = u+v$ si ottiene

$$(u+v)^3 + p(u+v) + q = (3uv+p)(u+v) + u^3 + v^3 + q = 0 .$$

Osserviamo allora che certamente $x = u_0+v_0$ è una radice dell'equazione se sono soddisfatte le due uguaglianze

$$3u_0v_0 + p = 0 \quad \text{e} \quad u_0^3 + v_0^3 + q = 0 .$$

Per determinare u_0 e v_0 con queste proprietà, dobbiamo risolvere il sistema

$$uv = -p/3 \; ; \; u^3 + v^3 = - q ,$$

da cui

$$u^3v^3 = (-p/3)^3 = -p^3/27 \; ; \; u^3 + v^3 = - q .$$

Queste ultime relazioni ci dicono che u^3 e v^3 debbono essere radici dell'equazione di secondo grado

$$r(Z) := Z^2 + qZ - p^3/27 = 0 ,$$

detta *equazione risolvente* dell'equazione cubica. Dunque possiamo porre

$$u^3 = - q/2 + \sqrt{q^2/4 + p^3/27} \; , \; v^3 = - q/2 - \sqrt{q^2/4 + p^3/27} ,$$

dove $\sqrt{z}$ indica uno qualsiasi dei due numeri complessi il cui quadrato è z.

Se ξ è una radice terza primitiva dell'unità e u_0 e v_0 sono due qualsiasi numeri complessi tali che

$$u_0^3 = - q/2 + \sqrt{q^2/4 + p^3/27} \quad \text{e} \quad v_0^3 = - q/2 - \sqrt{q^2/4 + p^3/27} ,$$

allora u può assumere i valori $u_0 , u_0\xi , u_0\xi^2$ e v può assumere i valori $v_0 , v_0\xi , v_0\xi^2$ (Esempi 4.4 e 4.5). Infine, tenendo conto che deve risultare $uv = -p/3$, otteniamo che le radici del polinomio $f(X)$ sono

$$\alpha_1 = u_0 + v_0 \; , \; \alpha_2 = \xi u_0 + \xi^2 v_0 \; , \; \alpha_3 = \xi^2 u_0 + \xi v_0 .$$

Se i coefficienti di $f(X)$ sono reali, come stabilito dal Corollario 4.11, $f(X)$ avrà tutte radici reali oppure una radice reale e due radici complesse coniugate. Questo dipende dal segno del discriminante

$$D(f) = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = - 4p^3 - 27q^2$$

(Esempio 10.10).

Tale discriminante è nullo se e soltanto se $f(X)$ ha radici multiple; inoltre si verifica subito che $f(X)$ ha una sola radice ρ di molteplicità 3 (necessariamente reale), ovvero $f(X) = (X - \rho)^3$, se e soltanto se $\rho = 0$, cioè $p = q = 0$.

Supponiamo quindi che p e q non siano entrambi nulli e poniamo per comodità $q := -2a$ e $p := 3b$. Allora l'equazione di terzo grado diventa

$$f(X) := X^3 + 3bX - 2a = 0 ,$$

la cui risolvente è

$$r(Z) := Z^2 - 2aZ - b^3 = 0 .$$

Il discriminante di $r(Z)$ è $D(r) = 4(a^2+b^3) = -D(f)/27$ e le radici di $r(Z)$ sono

$$\alpha := a + \sqrt{a^2 + b^3} \quad \text{e} \quad \beta := a - \sqrt{a^2 + b^3} \ .$$

Se $D(f) = D(r) = 0$, allora risulta $\alpha = \beta = a \in \mathbf{R} \setminus \{0\}$ e le radici di $f(X)$ sono

$$\rho := \sqrt[3]{\alpha} + \sqrt[3]{\beta} = 2\sqrt[3]{a} \ ;$$

$$\sigma = \tau := (\xi + \xi^2)\sqrt[3]{a} = -\sqrt[3]{a} = -\rho/2 \ .$$

In particolare esse sono tutte reali (e due sono coincidenti).

Se $D(f) < 0$, allora $D(r) > 0$ e perciò α e β sono numeri reali. In questo caso $f(X)$ ha una radice reale e due radici non reali (complesse coniugate). Infatti risulta:

$$\rho := \sqrt[3]{\alpha} + \sqrt[3]{\beta} \in \mathbf{R} \ ,$$

$$\sigma := \sqrt[3]{\alpha}\,\xi + \sqrt[3]{\beta}\,\xi^2 = -1/2[(\sqrt[3]{\alpha} + \sqrt[3]{\beta}) + \sqrt{3}(\sqrt[3]{\alpha} - \sqrt[3]{\beta})i] \ ,$$

$$\tau := \sqrt[3]{\alpha}\,\xi^2 + \sqrt[3]{\beta}\,\xi = -1/2[(\sqrt[3]{\alpha} + \sqrt[3]{\beta}) - \sqrt{3}(\sqrt[3]{\alpha} - \sqrt[3]{\beta})i] \ .$$

Se $D(f) > 0$, allora $f(X)$ ha tre radici reali distinte. Infatti, in questo caso $D(r) < 0$ e perciò α e β non sono numeri reali; dunque non sono reali neanche le loro radici cubiche. Se $\alpha_0^3 = \alpha$ e $\beta_0^3 = \beta$, senza perdere generalità, possiamo supporre che $\rho = \alpha_0 + \beta_0$ sia una radice reale di $f(X)$. Poiché α_0 e β_0 hanno somma e prodotto reali $(\alpha_0\beta_0 = -p/3)$, allora essi sono numeri complessi coniugati, come radici dell'equazione di secondo grado a coefficienti reali $Y^2 - \rho Y - p/3 = 0$. Poiché anche ξ e ξ^2 sono numeri complessi coniugati, lo sono anche le coppie $\xi\alpha_0$, $\xi^2\beta_0$ e $\xi^2\alpha_0$, $\xi\beta_0$. Ne segue che le radici di $f(X)$

$$\rho = \alpha_0 + \beta_0 \ , \quad \sigma = \xi\alpha_0 + \xi^2\beta_0 \ , \quad \tau = \xi^2\alpha_0 + \xi\beta_0$$

sono tutte reali.

In quest'ultimo caso tuttavia le formule di Tartaglia-Cardano forniscono un'espressione delle radici di $f(X)$ che non è sempre possibile ridurre a forma reale. Per questo motivo, il caso in cui $D(f) > 0$ venne denominato *casus irriducibilis*. Tale caso, appena accennato nel libro di Cardano, fu discusso a fondo da Bombelli. Dalla necessità di considerare radici quadrate di numeri negativi per risolvere un'equazione di questo tipo ebbe origine il calcolo con i numeri complessi.

Esempi.

1. Nel suo libro *Algebra*, Bombelli, usando le formule di Tartaglia-Cardano, risolve l'equazione $X^3 = 15X + 4$ trovando la soluzione

$$\sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} \ .$$

Egli tuttavia osserva che l'equazione data non è "impossibile", avendo come soluzione 4. Notiamo che questa equazione ha tre radici reali, precisamente 4, $-2+\sqrt{3}$, $-2-\sqrt{3}$, ma Bombelli prende in considerazione soltanto la radice razionale perché all'epoca il calcolo algebrico simbolico non era ancora sufficientemente sviluppato ed i radicali venivano all'atto pratico approssimati con frazioni (nello stesso libro di Bombelli ad esempio viene illustrato un metodo per approssimare i radicali quadratici con frazioni continue).

Tentando di dare significato all'espressione radicale trovata, Bombelli, usando ingegnosamente i metodi algebrici conosciuti a quel tempo, trova che

$$\sqrt[3]{2 + \sqrt{-121}} = 2 + \sqrt{-1} \quad \text{e} \quad \sqrt[3]{2 - \sqrt{-121}} = 2 - \sqrt{-1} ,$$

da cui ricava

$$\sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = (2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4 .$$

La quantità $\sqrt{-1}$ permetteva dunque di arrivare alla corretta soluzione dell'equazione, ma non era necessario attribuirle un significato proprio, perché essa non compariva più nel risultato finale; bisognò aspettare più di un secolo perché i numeri complessi fossero pienamente accettati dalla comunità matematica.

L'espressione *numero immaginario* fu usato per la prima volta da R. Descartes nel suo *Discorso sul Metodo* (1637), mentre il termine *numero complesso* sembra sia dovuto a F. Gauss, che per primo definì rigorosamente i numeri complessi e ne studiò le proprietà.

2. Sia $f(X) := (X-1)(X-2)(X+3) = X^3 - 7X + 6$. Le formule di Tartaglia-Cardano forniscono la soluzione

$$\sqrt[3]{\frac{1}{2}(-6 + \sqrt{\frac{-400}{27}})} + \sqrt[3]{\frac{1}{2}(-6 - \sqrt{\frac{-400}{27}})} ,$$

che deve evidentemente essere uguale a 1 , 2 , oppure -3 .

3. Formule di Viéte. Nel *casus irriducibilis* un'equazione di terzo grado si può risolvere anche usando metodi trigonometrici. Le *formule di F. Viéte*, pubblicate postume nel 1615, sono basate sulle formule trigonometriche per la triplicazione dell'angolo:

$$\cos(\lambda) = 4 \cos^3(\lambda/3) - 3 \cos(\lambda/3)$$

(Esercizio 11.1).

Se r è un arbitrario numero reale positivo, moltiplicando per $2r^3$ e ponendo

$$A := 2r \cos(\lambda/3) \quad \text{e} \quad B := 2r \cos(\lambda) ,$$

tali formule diventano:

$$A^3 - 3r^2A - r^2B = 0 ,$$

da cui A è radice dell'equazione di terzo grado $X^3 - 3r^2X - r^2B = 0$, dove $|B| \leq 2r$.

Notiamo ora che, se il polinomio $f(X) := X^3 + pX + q$ (con $q \neq 0$, per evitare casi banali) ha discriminante positivo, allora p deve essere negativo. Infatti, se $D(f) = -4p^3 - 27q^2 > 0$, allora deve essere $-p^3 > 27/4\, q^2 > 0$. Esiste pertanto un numero positivo r tale che $p = -3r^2$.

A questo punto, se $|q| \leq 2r^3$, possiamo anche porre $q = -r^2B = -2r^3 \cos(\lambda)$. In questo modo, come visto sopra, una radice di $f(X)$ è $A := 2r \cos(\lambda/3)$.

Le relazioni

$$r = \sqrt{-\frac{p}{3}} \quad \text{e} \quad \cos(\lambda) = -\frac{q}{2r^3} .$$

ci permettono di determinare l'angolo λ e dunque le radici di $f(X)$, che sono:

$$\rho := A := \sqrt{\frac{-4p}{3}}\cos(\lambda/3)\,;\quad \sigma := \sqrt{\frac{-4p}{3}}\cos(\lambda/3 + 2\pi/3)\,;\quad \tau := \sqrt{\frac{-4p}{3}}\cos(\lambda/3 + 4\pi/3)\,.$$

Ad esempio, se $f(X) := X^3 - 3X + 1$, otteniamo $\cos(\lambda) = -1/2$, da cui $\lambda = 2\pi/3 + 2k\pi$ oppure $\lambda = 4\pi/3 + 2k\pi$. Le radici di $f(X)$ sono perciò:

$\rho := 2\cos(2\pi/9) = \xi + \xi^8$, $\sigma := 2\cos(8\pi/9) = \xi^4 + \xi^5$, $\tau := 2\cos(4\pi/9) = \xi^2 + \xi^7$,

dove ξ è una radice primitiva nona dell'unità.

Fu Ludovico Ferrari, un discepolo di Cardano, a dimostrare per primo che l'equazione generale di quarto grado può essere risolta per mezzo di radici quadrate e cubiche; le sue formule risolutive furono pubblicate per la prima volta da Cardano nell'*Ars Magna*.

L'idea di Ferrari è stata quella di usare la formula del quadrato del trinomio, che egli dimostrava geometricamente,

$$(u + v + z)^2 = (u + v)^2 + 2uz + 2vz + z^2.$$

Consideriamo l'equazione di quarto grado a coefficienti reali, che al solito possiamo supporre in forma ridotta

$$f(X) := X^4 + aX^2 + bX + c = 0\,.$$

Introducendo una indeterminata ausiliaria t su $\mathbf{R}$, abbiamo

$$f(X) = (X^2 + \frac{a}{2} + t)^2 + bX + c - (\frac{a^2}{4} + 2tX^2 + at + t^2)\,.$$

Quindi l'equazione $f(X) = 0$ si riduce a

$$(X^2 + \frac{a}{2} + t)^2 = 2tX^2 - bX + (\frac{a^2}{4} + at + t^2 - c)\,.$$

Dando un opportuno valore a t, si può ora fare in modo che il secondo membro di questa uguaglianza sia anche esso un quadrato. Per determinare tale valore, basta imporre che sia nullo il discriminante del polinomio

$$g_t(X) := 2tX^2 - bX + (\frac{a^2}{4} + 2at + t^2 - c)\,,$$

ovvero che sia

$$D(g_t) = b^2 - 4(2t)(\frac{a^2}{4} + 2at + t^2 - c) = -(8t^3 - 8at^2 + (2a^2 - 8c)t - b^2) = 0\,.$$

L'equazione cubica ausiliaria

$$8Y^3 - 8aY^2 + (2a^2 - 8c)Y - b^2 = 0$$

può essere risolta ponendola in forma ridotta ed usando le formule di Tartaglia-Cardano. Se t_0 è una sua soluzione, il polinomio $g_{t_0}(X)$ ha l'unica radice doppia $\frac{b}{4t_0}$ e perciò

$$g_{t_0}(X) = 2t_0(X - \frac{b}{4t_0})^2\,.$$

Per $t = t_0$, otteniamo allora l'equazione

$$(X^2 + \frac{a}{2} + t_0)^2 = 2t_0(X - \frac{b}{4t_0})^2\,,$$

che si riduce alle due equazioni quadratiche

$$X^2 + \frac{a}{2} + t_0 = \pm \sqrt{2t_0}\,(X - \frac{b}{4t_0}) .$$

Risolvendole, otteniamo in questo modo le quattro radici di $f(X)$.

Esempi.

4. Per illustrare il metodo di Ferrari, Cardano risolve nell'*Ars Magna* l'equazione

$$X^4 + 6X^2 + 36 = 60X .$$

Aggiungendo $6X^2$ a entrambi i membri, egli ottiene prima

$$(X^2 + 6)^2 = 6X^2 + 60X .$$

Poi, usando l'identità

$$(X^2 + 6 + t)^2 = (X^2 + 6)^2 + 2tX^2 + 12t + t^2 ,$$

ottiene

$$(X^2 + 6 + t)^2 = (6X^2 + 60X) + (2tX^2 + 12t + t^2) = (2t + 6)X^2 + 60X + (12t + t^2) .$$

A questo punto, per ridurre il secondo membro ad un quadrato, egli impone

$$(2t + 6)(12t + t^2) = 30^2 ,$$

equivalentemente

$$t^3 + 15t^2 + 36t = 450 ,$$

che è possibile risolvere usando le formule di Tartaglia-Cardano.

Illustriamo ora un altro metodo per risolvere l'equazione di quarto grado, dovuto a R. Descartes.

Imponiamo che l'equazione di quarto grado in forma ridotta

$$f(X) := X^4 + aX^2 + bX + c = 0$$

sia il prodotto di due equazioni di secondo grado. Poiché il coefficiente di X^3 è nullo, otteniamo

$$f(X) = (X^2 + kX + l)(X^2 - kX + m) ,$$

dove k , l , m sono indeterminati.

Uguagliando i coefficienti, si ha

$$l + m - k^2 = a$$
$$k(m - l) = b$$
$$lm = c$$

Dalle prime due equazioni, ricaviamo

$$2m = k^2 + a + b/k$$
$$2l = k^2 + a - b/k$$

e sostituendo nella terza

$$k^6 + 2ak^4 + (a^2 - 4c)k^2 - b^2 = 0 ,$$

da cui, ponendo $Z = k^2$

$$r(Z) := Z^3 + 2aZ^2 + (a^2 - 4c)Z - b^2 = 0 .$$

Il polinomio $r(Z)$ si dice la *risolvente cubica* di $f(X)$.

Le soluzioni di $r(Z)$ forniscono i possibili valori di k^2 ; una volta noti questi valori è possibile determinare anche l e m . Le radici di $f(X)$ a questo punto si ottengono risolvendo le due equazioni di secondo grado

$$X^2 + kX + l = 0 \quad \text{e} \quad X^2 - kX + m = 0 .$$

Esempi.

4. Sia $f(X) := X^4 - 2X^2 + 8X - 3$. La risolvente cubica di $f(X)$ è

$$r(Z) := Z^3 - 4Z^2 + 16Z - 64 = (Z - 4)(Z^2+16) ,$$

da cui si ottiene ad esempio $Z = k^2 = 4$ e $k = \pm 2$. Ne segue che

$$l + m = 2 \quad \text{e} \quad \pm 2(m - l) = 8 ;$$

perciò

$$k = 2 , \; l = -1 , \; m = 3 \quad \text{oppure} \quad k = -2 , \; l = 3 , \; m = -1 .$$

Infine

$$f(X) = (X^2 + 2X - 1)(X^2 - 2X + 3) .$$

Notiamo che i tre valori possibili di k^2 sono determinati dai possibili modi di scomporre il polinomio di quarto grado $f(X)$ nel prodotto di due polinomi di secondo grado. Infatti, siano $\alpha_1 , \alpha_2 , \alpha_3 , \alpha_4$ le radici di $f(X)$, allora due di esse saranno radici del polinomio $X^2 + kX + l$ e le altre due saranno radici del polinomio $X^2 - kX + m$. Supponiamo ad esempio che sia

$$X^2 + kX + l = (X - \alpha_1)(X - \alpha_2) \quad \text{e} \quad X^2 - kX + m = (X - \alpha_3)(X - \alpha_4) .$$

In questo caso, si ha

$$-(\alpha_1 + \alpha_2) = k \quad \text{e} \quad -(\alpha_3 + \alpha_4) = -k ,$$

da cui

$$-(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = k^2 .$$

Dunque una radice della risolvente cubica $r(Z)$ è

$$u := -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = (\alpha_1 + \alpha_2)^2 .$$

Osserviamo che lo stesso valore si ottiene supponendo che

$$X^2 + kX + l = (X - \alpha_3)(X - \alpha_4) \quad \text{e} \quad X^2 - kX + m = (X - \alpha_1)(X - \alpha_2) .$$

In modo analogo si vede che le altre due radici di $r(Z)$ sono

$$v := -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = (\alpha_1 + \alpha_3)^2 ,$$
$$w := -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) = (\alpha_1 + \alpha_4)^2 .$$

Dunque

$$r(Z) = (Z - u)(Z - v)(Z - w) .$$

Dalle relazioni

$$u = (\alpha_1 + \alpha_2)^2 ,$$
$$v = (\alpha_1 + \alpha_3)^2 ,$$
$$w = (\alpha_1 + \alpha_4)^2 ,$$
$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$$

ricaviamo

$$(\alpha_1 + \alpha_2) = \sqrt{u} = -(\alpha_3 + \alpha_4) ,$$
$$(\alpha_1 + \alpha_3) = \sqrt{v} = -(\alpha_2 + \alpha_4) ,$$
$$(\alpha_1 + \alpha_4) = \sqrt{w} = -(\alpha_2 + \alpha_3) ,$$

dove con $\sqrt{z}$ si indica uno qualsiasi dei due numeri complessi il cui quadrato è z, ed infine possiamo esprimere le radici di $f(X)$ in funzione di quelle di $r(Z)$:

$$\alpha_1 = 1/2(\sqrt{u} + \sqrt{v} - (\alpha_2 + \alpha_3)) = 1/2(\sqrt{u} + \sqrt{v} + \sqrt{w}) ,$$
$$\alpha_2 = 1/2(\sqrt{u} - \sqrt{w} - (\alpha_1 + \alpha_3)) = 1/2(\sqrt{u} - \sqrt{v} - \sqrt{w}) ,$$
$$\alpha_3 = 1/2(\sqrt{v} - \sqrt{u} - (\alpha_1 + \alpha_4)) = 1/2(- \sqrt{u} + \sqrt{v} - \sqrt{w}) ,$$
$$\alpha_4 = 1/2(\sqrt{w} - \sqrt{u} - (\alpha_1 + \alpha_3)) = 1/2(- \sqrt{u} - \sqrt{v} + \sqrt{w}) .$$

L'impossibilità di trovare formule radicali per la risoluzione dell'equazione generale di quinto grado su $\mathbf{Q}$ è stata dimostrata da P. Ruffini e indipendentemente da N. Abel nei primi anni del 1800. Il problema di determinare quali particolari equazioni a coefficienti razionali di grado superiore a quattro siano risolubili per radicali è stato risolto da E. Galois nel 1831. Una delle conseguenze della sua teoria è che, per ogni $n \geq 5$, esiste un polinomio di grado n a coefficienti razionali le cui radici non si posono esprime come funzioni radicali dei coefficienti.

ESERCIZI

1. Dimostrare le formule trigonometriche per la triplicazione dell'angolo

$$\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$$

(Sugg. Usare le formule di De Moivre per la potenza di un numero complesso espresso in forma trigonometrica).

2. Sia $f(X) := X^3 + pX + q$ e siano ρ, σ, τ le radici di $f(X)$. Usando le formule di Tartaglia-Cardano, mostrare direttamente che $D(f) = (\rho-\sigma)^2(\rho-\tau)^2(\sigma-\tau)^2 = -(4p^3+27q^2)$. (Sugg. Usare il fatto che, se ξ è una radice primitiva terza dell'unità, allora $\xi(1-\xi^2)(1-\xi)^2 = 3i\sqrt{3}$).

3. Mostrare direttamente che, se $f(X)$ è un polinomio di terzo grado su $\mathbf{Q}$ con una sola radice reale, allora $D(f) < 0$.

4. Calcolare il discriminante dei seguenti polinomi di terzo grado su $\mathbf{Q}$:

$X^3 - 2$; $X^3 + 27X - 4$; $X^3 - 21X + 17$; $X^3 + X^2 - 2X - 1$; $X^3 + X^2 - 2X + 1$.

5. Sia $f(X) := X^3 + aX + 2 \in \mathbf{Q}[X]$. Mostrare che $f(X)$ ha 3 radici reali se e soltanto se $a \leq -3$.

6. Sia p un numero primo e sia $f(X) := X^3 - 2pX + p$. Mostrare che $f(X)$ è irriducibile su $\mathbf{Q}$ ed ha tre radici reali. Determinare inoltre le sue radici usando le formule di Tartaglia-Cardano.

7. Determinare le radici razionali dei seguenti polinomi su $\mathbf{Q}$ usando le formule di Tartaglia-Cardano:

$$X^3 + 9X - 10 \; ; \quad X^3 + 6X - 20 \; ; \quad X^3 + 6X - 7 \; .$$

8. Risolvere la seguente equazione di quarto grado su $\mathbf{Q}$ usando le formule di L. Ferrari:

$$X^4 + 2X^2 - 2X - 1 = 0 \; .$$

9. Verificare che un polinomio di quarto grado su un campo F in forma ridotta e la sua risolvente cubica hanno lo stesso discriminante.

10. Calcolare il discriminante dei polinomi $X^4 + aX^2 + c$, $X^4 + bX + c \in F[X]$.

11. Sia $f(X) \in \mathbf{R}[X]$ un polinomio di quarto grado su un campo F. Mostrare che

(a) se $D(f) > 0$, allora le radici di $f(X)$ sono tutte reali o tutte non reali;

(b) se $D(f) < 0$, allora le radici di $f(X)$ sono due reali e due non reali.

12. Sia $f(X) \in \mathbf{R}[X]$ un polinomio di quarto grado e sia $r(Z)$ la sua risolvente cubica. Mostrare che $f(X)$ ha esattamente due radici non reali se e soltanto se $r(Z)$ ha la stessa proprietà.