1

# Capitolo B33
# polinomi, funzioni razionali, calcolo letterale

## Contenuti delle sezioni



33 pagine

---

**B330.01** Questo capitolo esamina la importante nozione di polinomio, termine che viene attribuito a oggetti diversi, ma strettamente conness.
Si possono distinguere le funzioni polinomiali, funzioni numeriche che si possono calcolare agevolmente attraverso le operazioni chiamate polinomiali, ossia somma, passaggio all'opposto, differenza e prodotto.
Queste funzioni quindi sono cotrollabili attraverso le espressioni polinomiali, espressioni nelle quali compaiono operandi che possono essere sottoposti a operazioni polinomiali; sono possibili operandi innanzi tutto i numeri razionali, ma si prospetta chele operazioni polinomiali possono agire su molti altri generi di oggetti matematici, non solo numerici.
Altri possibili operandi sono le variabili e i parametri che possono assumere valori costituenti insiemi di valori numerici o più in generale insiemi di funzioni numeriche.
Lo studio delle espressioni polinomiali conduce a elaborazioni puramente formali per le quali risulta conveniente parlare di polinomi formali.
Trattando le elaborazioni si viene indotti anche a considerare i polinomi come tipi di costruzioni che si servono delle operazioni polinomiali per combinare oggetti matematici di tanti generi.

In questo capitolo vengono introdotte anche le funzioni razionali, funzioni ottenibili con la divisione tra polinomi, operazione che raramente porta a semplici polinomi.
Le funzioni razionali in effetti ampliano significativamente l'insieme delle funzioni polinomi e le modalità di trattarle attraverso le loro espressioni. Infatti si può dire che le funzioni razionali sono costruibili con le operazioni razionali, operazioni che oltre alle operazioni polinomiali includono la divisione, una operazione necessariamente parziale, sottoposta al vincolo della diversità da zero del divisore.

**B330.02** Procedendo con atteggiamento strettamente costruttivo, si dovrebbero esaminare solo le funzioni polinomiali e razionali di variabili razionali, cioè funzioni individuate da espressioni costruite con argomenti numerici, costanti e variabili, che assumono solo valori appartenenti a $\mathbb{Q}$.

Come vedremo molte delle proprietà di queste entità si generalizzano facilmente quando si consente alle costanti e alle variabili di assumere valori in insiemi strutturati più estesi di $\mathbb{Q}$, in particolare dei campi, insiemi sui quali si possono definire le quattro operazioni mantenendo buona parte delle proprietà che valgono per i numeri razionali.

Questi insiemi strutturati hanno grande importanza organizzativa generale e applicativa, in quanto numerose loro manipolazioni si possono controllare piuttosto agevolmente mediante algoritmi.

Lo studio dei campi serve anche per l'insieme dei numeri reali, numeri approssimabili quanto si vuole con numeri razionali, per l'insieme dei numeri complessi, entità numeriche esprimibili con coppie di numeri reali, e per i campi finiti basati sulle classi di resti di numeri naturali. Infatti buona parte dei risultati che si ottengono per il campo dei numeri razionali mantiene la sua validità anche per i suddetti insiemi numerici.
La nozione algebrica di campo sarà presentata in B41e, studieremo i polinomi sui reali e sui complessi in B51, mentre l'aritmetica delle classi di resti è stata introdotta in B25.

Va anche detto che sono assai chiarificanti i risultati sui polinomi che si possono estendere ad altri campi numerici come i campi algebrici e il campo dei numero reali costruibili [B38].

Inoltre va segnalato che risultano molto utili le espressioni polinomiali riguardanti elementi di strutture più generali e meno munite dei campi, come gli anelli e i semianelli, e costruzioni coinvolgenti oggetti più eleborati degli oggetti numerici come matrici, funzioni e operatori. Per queste costruzioni polinomiali, prevedibilmente, valgono proprietà più limitate di quelle ottenibili per i campi numerici, ma risulta complessivamente molto utile collegarle a quelle ottenute più elementarmente.

Nella lettura delle pagine che seguono è quindi opportuno tenere presente che le proprietà che si dimostrano hanno una portata più ampia di quella riguardante i numeri razionali: valgono anche per insiemi di entità ai quali si chiede solo di poter applicare operazioni omologhe a somme, differenze, prodotti e divisioni (parzialmente) definite suoi numeri razionali e caratterizzate da proprietà formalmente identiche.

**B330.03** I polinomi nelle loro varie accezioni, in quanto entità matematiche che si possono manipolare piuttosto facilmente sia manualmente che attraverso procedure automatiche (per le quali è stata sviluppata una articolate strumentazione consistente nei cosiddetti sistemi CAS (we)), sono ampiamente studiate da vari punti di vista e risultano utili per un gran numero di sviluppi formali e di procedimenti per la risoluzione effettiva di molti problemi.

In effetti la nozione di polinomio ha costituito da tempo una sorta di estensione di quella fondamentale di numero e si può capire come abbia potuto fornire essenziali strumenti computazionali per tutte le discipline che si avvalgono di metodi quantitativi.

Questo capitolo introduce la nozione di polinomio a partire dalle espressioni costruite con le operazioni di somma, differenza e prodotto da interpretare come funzioni di variabili razionali a valori razionali.

In tal modo le manipolazioni che si possono effettuare sulle espressioni polinomiali costituiscono i primi esempi delle elaborazioni cui si possono sottoporre espressioni formali significativamente articolate.

Lo studio delle funzioni polinomiali porta a introdurre una serie di problemi che dovranno essere affrontati anche nello studio di molte altre funzioni.

Oltre a un vero e proprio calcolo sulle espressioni, si introduce il problema della determinazione di valori particolari delle funzioni polinomiali, che si configura come problema della soluzione delle equazioni polinomiali e che si estende al problema dell'andamento complessivo delle funzioni di una variabile reale.

Anche questi problemi costituiscono esempi da generalizzare nello studio delle soluzioni di equazioni e dell'andamento complessivo di funzioni che assumono forme ben più generali delle polinomiali.

Questi problemi e, generalizzando, queste problematiche conducono naturalmente, ovvero per necessità cognitiva, ai temi dell'analisi infinitesimale a cominciare dallo studio dei limiti, delle derivate delle funzioni, alla ricerca delle loro inverse e delle loro antiderivate.

Anche queste problematiche si possono affrontare con una certa agevolezza per le funzioni polinomiali che hanno quindi fornito esempi iniziali di notevole apertura.

B330.04 Questo capitolo introduce anche le funzioni razionali; anche queste sono esaminate concretamente sui numeri razionali, ma con la prospettiva della estensione dei risultati a strutture più generali dei campi dei reali e dei complessi.

In particolare si pone il problema del dominio delle funzioni razionali, chiarendo come esso richieda di individuare le radici del polinomio denominatore.

La introduzione delle funzioni razionali costituisce il primo naturale passo dell'ampliamento che conduce all'analisi infinitesimale.

In particolare si incontra la difficoltà del problema di individuare il dominio di una funzione data attraverso un'espressione,problema inesistente per i polinomi.

Per queste funzioni si presentano algoritmi che arricchiscono in misura notevole quelli per i polinomi e che forniscono importanti strumenti per gli studi successivi, in particolare per quelli delle funzioni analitiche.

## B33 a. espressioni e funzioni polinomiali

**B33a.01** Come vedremo meglio in B41, per **campo** si intende una struttura, cioè una entità presentabile come sequenza delle forma

$$\boldsymbol{F} = \langle F, +, -, 0, {}^{-1}, 1\rangle \ ,$$

dove

- $F$ denota un insieme, il terreno del campo;
- $+$ è una operazione binaria su $F$, cioè una funzione del genere $\lceil F \times F \longmapsto F \rceil$ , commutativa e associativa detta somma;
- $0$ è un elemento di $F$ che è elemento neutro per la somma;
- "$\cdot$" è una operazione binaria su $F$ commutativa e associativa, chiamata prodotto;
- $1$ è un elemento di $F$ che è elemento neutro per il prodotto;
- $^{-1}$ è una operazione unaria su $F \setminus \{0\}$, ossia una funzione del genere $\lceil F \setminus \{0\} \triangleleft\!\!\longmapsto\!\!\triangleright F \setminus \{0\} \rceil$ , il passaggio all'inverso;
- $-$ denota una operazione unaria su $F$ tale che $\forall a, b \in F \,:\, (a+b)+(-b) = a$, chiamata cambiamento di segno;.
- vale la proprietà distributiva del prodotto rispetto alla somma:

$$\forall a, b, c \in F \,:\, (a + b) \cdot c = a \cdot c + b \cdot c$$

Si conviene di semplificare scritture come $a + (-b)$ con $a - b$ facendo assumere al segno $-$ il ruolo di rappresentatne della operazione binaria differenza.

Si conviene inoltre che nelle espressioni per il campo si dia al prodotto la precedenza sulla somma nel calcolo dell'espressione; quindi si intende che sia

$$(a + b) \cdot c \ := \ (a \cdot c) + (b \cdot c) \ .$$

**B33a.02** Le entità costituenti un campo, potendo essere sottoposte alle accennate operazioni, possono essere chiamate **entità numeriche** o semplicemente **numeri**.

Abbiamo finora incontrato due generi di campi, i campi delle classi di resti e $\mathbb{Q}_{Fld}$, il campo dei numeri razionali; per ciascuno di questi campi e tutti gli elementi e tutte le operazioni sono controllabili con algoritmi efficaci.

In seguito si introdurranno vari altri campi. Alcuni di essi ampliano $\mathbb{Q}_{Fld}$ e sono dotati di meccanismi che consentono di individuare i loro elementi e di eseguire le relative operazioni a partire da operazioni sui razionali.
Si introdurrà poi il campo dei numeri reali o con una definizione assiomatica o facendo riferimento all'intuizione per associarlo alla visualizzazione delle retta reale.

Più avanti si introdurrà il campo dei numeri complessi per ampliare il campo reale in relazione a una esigenza computazionale molto forte, la piena risolubilità delle equazioni polinomiali.

In tutti questi campi si troveranno molte proprietà dipendenti e deducibili solo dalle proprietà delle operazioni.
Emerge quindi l'opportunità di fare riferimento a una nozione generale e astratta di campo, struttura costituita da un insieme terreno munito delle operazioni suddette che godono delle proprietà sopra accennate, prescindendo del tutto dai processi che consentono di individuare gli elementi del terreno e le esecuzioni delle operazioni.
Il riferimento alla struttura astratta della specie campo presenta rilevanti vantaggi, in quanto consente di individuare costruzioni e risultati di tipo generale, possibilmente mediante formule, prescindendo

dalle elaborazioni effettive necessarie alla loro concretizzazione; questo consente di trattare in modo unificato una vasta gamma di risultati strutturali e di metodi computazionali, realizzando notevoli economie conoscitive, ossia possibilità di deduzioni e argomentazioni più nette e migliore organizzazione dei risultati e delle loro conseguenze.

In vista di questi vantaggi procederemo a sviluppare lo studio dei polinomi sopra un campo sia sul piano ben concreto dei polinomi sui numeri razionali, sia su quello più generale ma applicabile solo potenzialmente dei polinomi sopra un campo astratto.

**B33a.03** Nel seguito chiamiamo **operazioni polinomiali** o **operazioni razionali intere** le operazioni di somma, differenza, prodotto e cambiamento di segno; diciamo invece **operazioni razionali** le operazioni polinomiali e la divisione, operazione parziale inversa del prodotto.

Abbiamo visto che le operazioni razionali applicate a numeri razionali forniscono numeri razionali.
Può essere utile considerare espressioni che individuino i procedimenti di calcolo che consistono nell'applicazione di quante e quali si vogliano operazioni razionali su numeri razionali e forniscano un risultato (che deve essere un numero razionale).
Tali espressioni le denotiamo con la sigla ersnr, abbreviazione di "espressioni razionali su numeri razionali"

Nelle ersnr, oltre a numeri e operazioni razionali, possono intervenire coppie di parentesi "`(`" e "`)`" con il compito di delimitare stringhe aventi le stesse regole sintattiche e le stesse interpretazioni delle ersnr. Ciascuna di queste stringhe delimitate da parentesi, la denotiamo con $\sigma$, ha lo scopo di esprimere calcoli che vanno eseguiti indipendentemente dalle operazioni che compaiono al di fuori della $\sigma$ e che forniscono un numero razionale che sarà utilizzato da una delle operazioni che saranno effettuate nelle fasi successive della esecuzione della espressione complessiva.

Va osservato che la caratteristica delle ersnr di contenere sottoespressioni delimitate da coppie di parentesi coniugate è comune ad molti altri tipi di espressioni che abbiamo incontrate (come quelle che esprimono procedimenti che a partire da insiemi forniscono altri insiemi) o che incontreremo.

**B33a.04** Le più semplici ersnr consistono in un singolo numero razionale e sono dette **operandi elementari**; subito dopo si hanno le ersnr che coinvolgono un solo operatore e due operandi binari o un operando unario come $\left(\frac{4}{3}-\frac{3}{4}\right)$ e $\left(7\cdot\frac{1}{13}\right)$.
Si nota che ogni operatore è stato racchiuso con i propri operandi entro una cosiddetta **coppia di parentesi coniugate**; si tratta di due delimitatori che si rivelano non indispensabili per queste semplici espressioni, ma che servono per la chiara interpretazione delle ersnr più elaborate.

Queste vedono la presenza di più occorrenze di operatori e di più coppie di parentesi coniugate con il compito di stabilire la priorità rispetto alla esecuzione delle operazioni indicate.
Alcuni esempi:

$$6\cdot\left(\frac{5}{2}-\frac{7}{3}\right) \quad , \quad 1-\left(\frac{1}{2}-\frac{1}{3}\right) \quad , \quad \left(4-\frac{5}{3}\right)\cdot\left(2+\frac{3}{2}\right) .$$

La stringa delimitata da una coppia di parentesi coniugate viene detta **sottoespressione** della espressione complessiva della quale costituisce un infisso.

In talune ersnr risulta conveniente far intervenire altre costruzioni simboliche con il ruolo delle abbreviazioni di espressioni con soli operatori razionali, le potenze intere di operandi e sottoespressioni. Due semplici esempi: $\left(2^5-5^2\right)$ e $1+\left(7+\frac{23}{31}\right)^4$.

**B33a.05** Finora abbiamo incontrato espressioni con operandi numerici, ciascuna delle quali esprime un singolo processo di calcolo. È decisamente necessario aumentare la portata delle espressioni con le quali si individuano procedimenti che si servono di operazioni polinomiali o razionali in modo da renderle in grado di esprimere intere famiglie di tali elaborazioni.

Questo si ottiene facendo uso di simboli letterali ai quali si attribuisce il ruolo dei rappresentanti di insiemi di possibili valori.

Per esempio si consideri l'espressione $3 - \frac{4}{5}\,x^2$ munita della precisazione $x \in \mathbf{[}4 :: 6\mathbf{]}$; essa individua l'insieme delle coppie di valori numerici $\langle \overline{x}, \overline{y} \rangle$ ottenibili con i processi che consistono nel sostituire alla lettera $x$ uno dei numeri razionali $\overline{x}$ appartenenti all'intervallo $\mathbf{[}4 :: 6\mathbf{]}$ e nel calcolare il valore $\overline{y}$ dell'espressione puramente numerica così ottenuta. In altre parole l'espressione precedente e la specificazione $x \in \mathbf{[}4 : 6\mathbf{]}$ individuano una funzione avente come dominio l'intervallo razionale $\mathbf{[}4 :: 6\mathbf{]}$; con semplici considerazioni si trova che il codominio di questa funzione è $\Big[ -\frac{125}{5} :: -\frac{49}{5} \Big]$.
In un caso come questo si dice che $x$ denota una **variabile** ovvero una **indeterminata**, che varia (o corre) nell'insieme $\big[4 :: 6\big]$.

Si possono considerare procedimenti ed espressioni coinvolgenti una o più variabili. In questo capitolo considereremo soprattutto il caso di una sola variabile e per essa useremo la lettera $x$.
Come vedremo molte considerazioni sopra procedimenti ed espressioni riguardanti una sola variabile si possono ripetere con pochi cambiamenti per i casi delle espressioni con due o più variabili.

**B33a.06** Si osserva che una espressione come la precedente nella quale compaiono solo operazioni polinomiali ha senso per qualsiasi valore razionale della variabile. Questo discende dal fatto che le operazioni polinomiali sono definite per ogni coppia di operandi razionali.

Si hanno invece dei limiti per i valori possibili di una variabile quando compare accanto a una operazione di divisione come nella $(5 - 7x)/(x - 4)$.

In effetti risulta opportuno distinguere due tipi di procedimenti di calcolo con operandi variabili e razionali coinvolgenti operazioni razionali e conseguentemente due tipi di espressioni: **procedimenti ed espressioni polinomiali** nei quali intervengono solo operazioni polinomiali che riguardano le variabili e **procedimenti ed espressioni razionali** nei quali possono trovarsi tutte le operazioni razionali, divisione compresa.

Ci proponiamo ora di definire in modo preciso le **espressioni polinomiali sopra una variabile e numeri razionali**, che in seguito chiameremo semplicemente espressioni polinomiali.
Queste comprendono anche le ersnr. Nell'ultima parte di questo stesso capitolo incontreremo le **espressioni razionali sopra una variabile e numeri razionali**, che in breve chiameremo anche **espressioni razionali univariate**.

**B33a.07** Le espressioni polinomiali sono ampiamente utilizzate, ma una loro definizione precisa e completa richiede di chiarire molti dettagli e di effettuare varie distinzioni.
Qui trattiamo le espressioni polinomiali nella variabile che qui denoteremo sempre con la lettera $x$.

A causa dell'impegno delle precisazioni che si devono fare, risulta conveniente definire sia le espressioni polinomiali sul campo dei razionali $\mathbb{Q}$ che le espressioni polinomiali sopra un campo generico che denoteremo con $\mathbb{F}$; a rigore non daremo definizioni che valgono per tutti i campi, ma solo per quelli di maggior uso le cui caratteristiche preciseremo in seguito.

Risulta inoltre opportuno definire più insiemi di espressioni polinomiali.

Nel seguito denotiamo con ***ExprQ*** l'insieme delle espressioni che forniscono numeri razionali, denotiamo con ***ExprPln***$(\mathbb{Q}, x)$ l'insieme delle espressioni polinomiali sui razionali e nella variabile $x$ e con ***ExprPln***$(\mathbb{F}, x)$ l'insieme delle espressioni polinomiali sul campo $\mathbb{F}$ nella $x$.
Nel seguito tuttavia spesso per comodità non distingueremo i due ultimi casi e abbrevieremo le due scritture con la sola lettera ***E***.

Per procedere formalmente conviene considerare che le suddette espressioni siano stringhe su determinati alfabeti che denotiamo, risp., con $\mathbb{A}_Q$ per ***ExprQ*** e con $\mathbb{A}_{Pln}$ per ***ExprPln***$(\mathbb{Q}, x)$ e per ***ExprPln***$(\mathbb{F}, x)$.
L'alfabeto $\mathsf{A}_Q$ è costituito dai segni che consentono di esprimere gli elementi del campo, cioè dalle cifre decimali (o binarie), dal "." che precede la parte decimale, dai segni per le potenze numeriche, dai segni degli operatori polinomiali ($+$, $-$ e $\cdot$) e dal segno / in grado di esprimere le forme frazionarie.
L'alfabeto $\mathbb{A}_{Pln}$ è costituito dai segni in ***ExprQ*** dalle parentesi tonde di delimitazione delle sottoespressioni e dalla lettera della variabile $x$.
In casi più generali vengono utilizzate anche espressioni parametriche contenenti lettere che possano fornire numeri razionali: qui ci serviamo delle lettere $a$, $b$, $c$, $d$, ... .

B33a.08 Come richiesta di base della definizione di ***E*** si chiede che a tale insieme appartengano tutte le espressioni che forniscono elementi del campo, nel caso di ***ExprPln***$(\mathbb{Q}, x)$ tutte le erpnr, le espressioni per i numeri razionali (in particolare tutte le frazioni ridotte), la variabile $x$ le lettere esprimenti parametri, cioè lettere sostituibili senza restrizioni a priori, con specifici numeri razionali.

La definizione dell'insieme ***E*** prosegue con la definizione di un suo sottoinsieme chiamato l'insieme delle **espressioni polinomiali completamente parentesizzate**, in sigla epcp.
Si tratta di una cosiddetta **definizione ricorsiva**, definizione che si serve di scritture come $\mathcal{E}_1$ ed $\mathcal{E}_2$ con le quali intende rappresentare generiche espressioni polinomiali. Facciamo dunque la seguente richiesta:

se $\mathcal{E}_1$ ed $\mathcal{E}_2$ rappresentano due epcp, sono tali anche le espressioni $(\mathcal{E}_1 + \mathcal{E}_2)$, $(\mathcal{E}_1 - \mathcal{E}_2)$, $(\mathcal{E}_1 \cdot \mathcal{E}_2)$ e $(-\mathcal{E}_1)$ .

Sviluppando le costruzioni precedenti si trovano facilmente vari esempi di epcp:

$$27 \quad , \quad -\frac{134}{13} \quad , \quad (9 - x) \quad , \quad (4 \cdot x) + (x \cdot x) \quad , \quad (2 \cdot (3 \cdot 5)),\ ((2 + 3) + 5),\ (-(-(-4))),$$
$$((a + b) \cdot (c - x)),\ ((a \cdot a) - (b \cdot b)),\ (((a \cdot (x \cdot x)) + (b \cdot x)) + c) \ .$$

Questo può far sospettare un circolo vizioso, cioè una definizione che si serve di se stessa.

Questi esempi conducono subito a osservare che le epcp sono espressioni trovate sulla base di una definizione piuttosto semplice, ma presentano varie pesantezze alla lettura. Risulta quindi opportuno cercare delle loro varianti più facilmente leggibili che conducano alle stesse possibilità espressive. Come vedremo questo porta all'insieme di espressioni ***ExprPln***$(\mathbb{Q}, x)$ molto più ampio e variegato dell'insieme delle epcp.

B33a.09 Per considerare queste espressioni come rappresentazioni di procedimenti di calcolo risulta utile raffigurarle con arborescenze distese, come vedremo meglio in D30d e C14f.

Espressioni razionali completamente parentesizzate su numeri e variabili razionali

Varianti umanamente più maneggevoli delle espressioni razionali completamente parentesizzate.

Problema della correttezza di un'espressione completamente parentesizzata.

Espressioni canoniche e semicanoniche.

Espressioni canoniche e problema dell'equivalenza.

## B33 b. somma e prodotto di polinomi

**B33b.01** Si possono considerare polinomi di una o più variabili; qui ci limitiamo ai polinomi di una variabile che chiameremo semplicemente polinomi. I polinomi (di una variabile) sopra un campo $\mathbb{F}$ sono individuati da sequenze di elementi del campo e si possono comporre con operazioni che estendono in modo "naturale" quelle definite sul campo.
Le operazioni di somma, sottrazione e moltiplicazione tra polinomi godono di proprietà molto simili a quelle delle operazioni omologhe sugli elementi del campo; la divisione tra due polinomi, come per i numeri del campo, riguarda la inversione del prodotto, ma nella maggior parte dei casi individua non un solo polinomio risultato, ma due.

In effetti i polinomi su un campo costituiscono un'arricchimento piuttosto elaborato di tale campo ed è ragionevole aspettarsi che forniscano strumenti matematici di elevata utilità, ma che per essere manipolati richiedano procedimenti sensibilmente più elaborati di quelli richiesti dalle operazioni sulle scritture degli elementi del campo.

**B33b.02** Procediamo a definire gradualmente i polinomi in una variabile sul campo $\mathbb{F}$.
Per definire il polinomio che denotiamo con P cominciando con il considerare una sua rappresentazione in grado di identificarlo chiamata **sequenza dei coefficienti del polinomio**, P sequenza finita di elementi di $\mathbb{F}$ che scriviamo $\mathsf{c}(\mathsf{P}) = \langle a_0, a_1, ..., a_n \rangle$ e per la quale chiediamo che se $n \geq 1$ sia $a_n \neq 0$.

Ttalora il coefficiente $a_n$ viene detto **coefficiente direttivo del polinomio**
I polinomi relativi ad $n = 0$ si dicono **polinomi costanti** e sono evidentemente in biiezione con gli elementi del campo; in particolare il polinomio con $n = 0 \in \mathbb{Z}$ ed $a_0 = 0$, zero di $\mathbb{F}$, si dice **polinomio nullo** ed il polinomio con $n = 0$ e $a_0 = 1$, costituisce l'unità del campo, viene chiamato **polinomio unità**.

Si dice **grado del polinomio** P relativo alla $\mathsf{c}(\mathsf{P}) = \langle a_0, a_1, ..., a_n \rangle$ l'intero $n$ se esso è positivo oppure se $n = 0$ ed $a_0 \neq 0$; inoltre al polinomio nullo conviene attribuire il grado $-1$ (va però segnalato che molti non adottano questa scelta). Il grado del polinomio $P$ si denota con $deg(P)$.

Interessa considerare l'insieme di tutti i polinomi in una variabile sopra un campo munito di varie operazioni riconducibili a quelle concernenti gli elementi del campo e delle quali si studiano proprietà algebriche e ruoli computazionali.

Prima di procedere conviene però introdurre per i polinomi un tipo di scrittura meno essenziale della semplice sequenza dei suoi coefficienti, ma vantaggiosa per l'esecuzione manuale delle operazioni che riguardano i polinomi e atta a chiarire molte delle loro applicazioni, a partire dalle funzioni del genere $\lceil \mathbb{F} \longmapsto \mathbb{F} \rceil$ che vengono loro associate.

**B33b.03** I polinomi (di una variabile) vengono trattati solitamente attraverso espressioni nelle quali interviene un simbolo per il quale si possono scegliere lettere diverse che viene chiamato **indeterminata** o **variabile formale**. Per denotare l'indeterminata qui useremo sempre la lettera $x$.

Diciamo **espressione canonica** nella indeterminata $x$ del polinomio $P = \langle a_0, a_1, ..., a_n \rangle$ sul campo $\mathbb{F}$ la scrittura della forma

$$P(x) \;=\; a_0\, x^0 + a_1\, x + a_2\, x^2 + \cdots + a_n\, x^n \;.$$

Per esempio il polinomio $P = \langle_p 2, -1.5, -1, 1.25\rangle$ è individuato dalla espressione canonica

$$P(x) \;=\; 2\, x^0 - \frac{3}{2}x - x^2 + \frac{5}{4}x^3$$

Questa scrittura fornisce le stesse informazioni della sequenza da cui siamo partiti e, come vedremo, consente di controllare più agevolmente varie elaborazioni sui polinomi; si tende quindi con identificarla con il polinomio stesso.

Un'espressione canonica si può interpretare come una espressione da calcolare facendo agire su elementi di $\mathbb{F}$ le operazioni di tale campo; in essa la $x$ ha il ruolo di una variabile che può assumere come valori tutti gli elementi del campo $\mathbb{F}$. Secondo questa interpretazione l'espressione canonica del polinomio individua un procedimento di calcolo che può essere attuato per ogni valore appartenente a $\mathbb{F}$ attribuibile alla $x$.

Ad ogni polinomio su $\mathbb{F}$ nella indeterminata $x$ l'interpretazione computazionale dell'espressione canonica associa dunque una funzione del genere $\lceil\, \mathbb{F} \longmapsto \mathbb{F} \,\rceil$ che chiamiamo **funzione associata al polinomio**. Complessivamente le funzioni associate ai polinomi su un campo $\mathbb{F}$ sono dette **funzioni polinomiali sul campo** $\mathbb{F}$.

Anche la funzione polinomiale si tende a confondere con il polinomio e di solito viene individuata con la stessa espressione canonica o con una delle espressioni equivalenti che stiamo per definire.

**B33b.04** Accanto alla espressione canonica di un polinomio, in genere si possono considerare diverse altre espressioni da considerare equivalenti costruite con la stessa variabile $x$, con elementi del campo determinati indicati esplicitamente e con operandi che possono assumere più valori rappresentati da parametri letterali, con operazioni di somma, sottrazione e moltiplicazione e con coppie di parentesi ciascuna delle quali ha il compito di delimitare una sottoespressione da calcolare indipendentemente dalle valutazioni delle operazioni indicate all'esterno delle parentesi stesse.

Precisamente si considerano equivalenti alla espressione canonica tutte le espressioni di una forma opportuna che individuano la stessa funzione polinomiale del genere $\lceil\, \mathbb{F} \longmapsto \mathbb{F} \,\rceil$, cioè equivalenti per tutte le funzioni $Val_{\overline{x}}$ con $\overline{x} \in \mathbb{R}$.

Le espressioni equivalenti di un polinomio si possono ricondurre le une alle altre applicando le uguaglianze che esprimono le proprietà delle operazioni di somma, sottrazione e prodotto sugli elementi del campo.

Per molti polinomi alcune delle espressioni equivalenti alla canonica consentono di individuare alcune caratteristiche del polinomio con maggiore chiarezza della canonica. Risulta quindi utile sapere manipolare con una certa padronanza le espressioni dei polinomi; in effetti le manipolazioni simboliche sulle espressioni polinomiali costituiscono la parte basilare del cosiddetto **calcolo letterale**, termine che denota le varie tecniche per la manipolazione delle espressioni matematiche, in particolare per decisioni sulla loro equivalenza.

**B33b.05** Il problema della struttura e dell'equivalenza tra espressioni polinomiali in generale non è semplice, ma alquanto articolato.
Qui procediamo per gradi a presentare tecniche che consentono di trattare tutti i casi che ci servono, senza pretendere di essere esaurienti (cosa che richiede di servirsi di tecniche riguardanti linguaggi generati da `grammatiche formali (wi)` e la loro `manipolazione simbolica (wi)`).

Preliminarmente osserviamo che il segno di sommatoria consente una scrittura concisa di un'espressione canonica:

$$\sum_{i=0}^{n} a_i\, x^i \;:=\; a_0x^0 + a_1x^1 + \cdots + a_{n-1}x^{n-1} + a_nx^n \;.$$

Alcune semplici varianti equivalenti di un'espressione canonica sono delle sue evidenti semplificazioni. Un termine $a_0\, x^0$ si semplifica in $a_0$, un termine $a_1\, x^1$ si può sostituire con $a_1\, x$, ogni termine $1\, x^i$ con

$x^i$ e ogni sottoespressione $+0x^j$ si può trascurare *sic et simpliciter*, in quanto non ha alcuna influenza sulla valutazione del polinomio.

Si hanno quindi equivalenze come le seguenti, che per semplicità si usano presentare come uguaglianze.

$$3-2x+4x^3 \;=\; 3x^0+(-2)x^1+0x^2+4x^3 \quad , \quad x^2 \;=\; 0x^0+0x^1+1x^2 \quad , \quad 0 \;=\; 0x^0 \quad ,$$
$$\frac{2}{3}x^2-x^4 \;=\; 0x^0+0x^1+\frac{2}{3}x^2+0x^3+(-1)x^4$$

Altre equivalenze provengono dalle proprietà delle operazioni sui polinomi somma, moltiplicazione per un elemento del campo e prodotto, operazioni che introduciamo tra poco; queste proprietà applicate più volte possono portare a equivalenze a prima vista poco chiare.

Per esempio il polinomio con la sequenza di coefficienti $\langle 2,-1.5,0,1.25\rangle$ , oltre a essere individuato dalla espressione canonica

$$P(x) \;=\; 2-\frac{3}{2}\,x+0\,x^2+\frac{5}{4}\,x^3$$

può essere rappresentato dalla sua semplice variante $P(x) \;=\; 2-\frac{3}{2}x+\frac{5}{4}x^3$ ottenuta trascurando di indicare la potenza $x^2$ e da altre espressioni equivalenti come $\frac{5}{4}x^3-\frac{3}{2}x+2$ e $\frac{x}{4}\,(5\,x^2-6)+2$.

**B33b.06** L'insieme dei polinomi sul campo $\mathbb{F}$ identificati mediante loro espressioni polinomiali nella indeterminata $x$ si denota tradizionalmente con la scrittura $\mathbb{F}[x]$.

Precisiamo come $\mathbb{F}[x]$ viene munito delle due operazioni binarie somma e prodotto da intendere come estensioni funzionali, risp., delle operazioni di somma e prodotto per il campo $\mathbb{F}$ e per le quali usiamo gli stessi simboli "+" e "·".

Le definizioni si servono delle espressioni canoniche dei polinomi con una certa elasticità. Infatti è opportuno considerare come equivalente di una espressione canonica di un polinomio $P(x) \;=\; \sum_{i=0}^{n} a_i\,x^i$ ogni espressione della forma $P(x) \;=\; \sum_{i=0}^{n+h} a_i\,x^i$ con $h \;=\; 1,2,...$ e con $a_{n+1}=a_{n+2}=...=a_{n+h}:=0$.

Le espressioni canoniche dei polinomi e le loro suddette varianti le chiamiamo **espressioni semicanoniche**.

Consideriamo quindi due polinomi $P(x)=\sum_{i=0}^{n} a_i x^i$ e $Q(x)=\sum_{j=0}^{m} b_i\,x^i$ .

Si dice **somma di due polinomi** $P$ e $Q$ e si scrive $P+Q$ il polinomio dato dalla espressione semicanonica

$$(P+Q)(x) \;:=\; \sum_{i=0}^{g}(a_i+b_i) \text{ , dove } g=\max(n,m).$$

Il grado di questo polinomio somma, se $n\neq m$ è $g=\max(n,m)$, mentre se $n=m$ potrebbe essere inferiore a tale grado, in quanto potrebbe essere $a_n=-b_n$ e in questo caso potrebbe essere $a_{n-1}=-b_{n-1}$ e così via.

Quindi si può solo dire che

$$deg(P(x)+Q(x)) \;\leq\; \max(deg(P(x)),deg(Q(x)))$$

Per esempio la somma dei polinomi $P(x)=4x^3+12x-4$ e $Q(x)=x^2+3x-1$ di grado, risp., 3 e 2, è $P(x)+Q(x) \;=\; 4x^3+x^2+15x-5$ il cui grado è 3.

La somma dei due polinomi di grado 3 $S(x)=2x^3-x^2+2x+4$ e $T(x)=-2x^3+x^2+3x-1$ è $S(x)+T(x)=5x+3$ , polinomio di grado 1.

**B33b.07** Si dimostra facilmente che la somma di polinomi è un'operazione commutativa e associativa e che il polinomio nullo è l'elemento neutro per tale operazione.

Ogni polinomio della forma $cx^j$ si dice **monomio**. Ogni polinomio si può considerare come somma di monomi; ad esempio $2x - 3x^3 + 4x^5$ può essere considerato come somma dei tre monomi $2x$ di primo grado, $-3x^3$ di terzo grado e $4x^5$ di quinto grado. Per la commutatività della somma sono espressioni equivalenti della precedente come la $4x^5 - 3x^3 + 2x$, come la $-3x^3 + 2x + 4x^5$ e come tutte le altre 3 espressioni nelle quali i tre termini sono permutati diversamente.
Ogni polinomio somma di due monomi si dice **binomio**, ogni somma di tre monomi si dice **trinomio**, ogni somma di quattro polinomi si dice **quadrinomio** e così via.

Altre equivalenze delle espressioni polinomiali provengono dalla associatività della somma: per esempio sono due espressioni equivalenti $x - 3x^3 + 6x^5 + x - 2x^5$ e $(2x + 2x^3 + 2x^5) + (2x^5 - 5x^3)$ .

**B33b.08** Si dice **opposto di un polinomio** $P$ il il polinomio denotato con $-P$ i cui coefficienti sono gli elementi di $\mathbb{F}$ opposti dei rispettivi coefficienti di $P$.

In formule, l'opposto del polinomio dato dall'espressione $P(x) = \sum_{i=0}^{n} a_i\, x^i$ è il polinomio $-P(x) := \sum_{i=0}^{n} (-a_i)\, x^i$ .

Il passaggio al polinomio opposto può chiamarsi cambiamento dei segni e può considerarsi un'operazione unaria; tale operazione evidentemente è una trasformazione involutoria, cioè per ogni polinomio $P$ si ha $-(-(P)) = P$. L'unico polinomio che coincide con il proprio opposto è il polinomio nullo.

**B33b.09** Si dice **differenza tra due polinomi** $P$ e $Q$ la somma di $P$ e l'opposto di $Q$: $P - Q := P + (-Q)$.
Per esempio se $P(x) = 3 - x + x^3$ e $Q(x) = 2x + x^2 + x^3$ si ha $P(x) - Q(x) = 3 - 3x - x^2$ .

Per quanto riguarda il grado, evidentemente $deg(-(P(x)) = deg(P(x))$ e quindi si può solo dire che

$$deg(P(x) - Q(x)) \;\leq\; \max(deg(P(x)), deg(Q(x))) \;.$$

Per ogni intero naturale $n$ denotiamo, risp., con $\mathbb{F}_n[x]$ / con $\mathbb{F}_{<n}[x]$ / con $\mathbb{F}_{\leq n}[x]$ / con $\mathbb{F}_{>n}[x]$ / con $\mathbb{F}_{\geq n}[x]$ l'insieme dei polinomi sul campo $\mathbb{F}$ aventi grado uguale ad $n$ / minore di $n$ / minore o uguale ad $n$ / maggiore di $n$ / maggiore o uguale ad $n$.

Sono evidenti le relazioni

$$\mathbb{F}_{\leq n}[x] = \mathbb{F}_{<n}[x] \dot\cup \mathbb{F}_n[x] \quad , \quad \mathbb{F}_{\leq n}[x] = \mathbb{F}_{<n+1}[x] \quad \text{e} \quad \mathbb{F}[x] = \mathbb{F}_{<n}[x] \dot\cup \mathbb{F}_{\geq n}[x] \;.$$

Dalle considerazioni precedenti segue che per ogni intero positivo $n$ la quaterna $\langle \mathbb{F}_{\leq n}[x], +, -, 0\rangle$ è un gruppo abeliano e che la quaterna $\langle \mathbb{F}_{<n}[x], +, -, 0\rangle$ è un suo sottogruppo proprio.

**B33b.10** Definiamo come **prodotto di due polinomi** $P(x) = \sum_{i=0}^{n} a_i\, x^i$ e $Q(x) = \sum_{j=0}^{m} b_i\, x^i$ il polinomio denotato con $P \cdot Q$ il quale se entrambi i polinomi fattori non sono nulli viene individuato dalla espressione

$$(P \cdot Q)(x) \;=\; \sum_{i=0}^{n} \sum_{j=0}^{m} \left(a_i b_j x^{i+j}\right) \;.$$

Per esempio $(x^3 + 2x - 4) \cdot (-x^2 + 2x - 3) \;=\; -x^5 + 2x^4 - 5x^3 + 8x^2 - 14x + 12$ .
Per il grado del polinomio prodotto di due polinomi nonnulli quindi

$$deg(P(x) \cdot Q(x)) \;=\; deg(P(x)) + deg(Q(x)) \;.$$

Definiamo inoltre come prodotto di due polinomi dei quali almeno uno è nullo il polinomio nullo stesso.

Sul piano della pratica del calcolo conviene aggiungere qualche chiarimento sull'operazione di prodotto di due polinomi.
Può essere utile organizzare il suo calcolo con una matrice che si può considerare far parte delle matrici con dominio $\mathbb{N}\times\mathbb{N}$, avente le righe etichettate dai termini $a_i\,x^i$ del primo polinomio fattore, le colonne etichettate dai termini $b_j\,x^j$ del secondo fattore e ogni casella occupata dal prodotto dei termini che la caratterizzano $\;a_i\,b_j\,x^i\,x^j\;$ ; questa matrice può anche essere semplificata trascurando le potenze della variabile.

Ad esempio per i due polinomi precedenti si ha il seguente quadro

$$\begin{array}{rrrrr} -1 & 4 & -2 & 0 & -1 \\ 2 & -8 & 4 & 0 & 2 \\ -3 & 12 & -6 & 0 & -3 \\ & & & & \\ & -4 & 2 & 0 & -1 \end{array} \quad ;$$

i coefficienti delle successive potenze di $x$ del polinomio prodotto si ottengono sommando i prodotti nelle linee oblique decrescenti a partire dalla casella in basso a sinistra.

Per il prodotto di due polinomi si usa anche l'espressione

$$(P\cdot Q)(x) \;=\; \sum_{k=0}^{n+m} c_k \;,$$

dove per ogni $k=0,1,2,...,n+m$ si assume $\;c_k := \displaystyle\sum_{h=\max(0,k-m)}^{\min(k,n)} a_h\cdot b_{k-h}\;.$

Si può anche scrivere semplicemente $\;c_k=\displaystyle\sum_{h=0}^{k} a_h\,b_{k-h}$, pur di assumere che per $i>n$ sia $a_i=0$ e per $j>m$ si abbia $b_j=0$.

B33**b.11** **(1) Prop.**: Il prodotto di due polinomi è un'operazione binaria commutativa.

**Dim.**: La cosa è ovvia quando uno dei fattori è il polinomio nullo, mentre in caso contrario si fa riferimento alle due presentazioni matriciali dei due prodotti e si osserva che le due matrici sono l'una la trasposta dell'altra e che le somme che forniscono i termini del polinomio prodotto riguardano le stesse sequenze di addendi posti nelle caselle collocate sulle linee oblique discendenti delle matrici ∎

**(2) Prop.**: Il prodotto di polinomi è un'operazione associativa e distributiva rispetto alla somma.

**Dim.**: Consideriamo anche il polinomio $R(x)=\displaystyle\sum_{l=0}^{r} c_q\,x^q$ e supponiano che sia $c_l=0$ per $l>r$.

Per la associatività si trova che sia $\;\big(P(x)Q(x)\big)R(x)\;$ che $\;P(x)\big(Q(x)R(x)\big)\;$ portano all'espressione

$$\sum_{s=0}^{S} d_s\,x^s \quad \text{dove} \quad S:=n+m+r \;\text{ e }\; \text{per }\; s=0,1,...,S \;:\; d_s := \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j c_{s-i-j}\;.$$

Per la distributività si constata che

$$\begin{aligned}(P(x)+Q(x))\cdot R(x) \;&=\; \left[\sum_{i=0}^{\max(n,m)} (a_i+b_i)x^i\right]\cdot\sum_{l=0}^{r} c_l\,x^l \\ &=\; \sum_{i=0}^{n} a_i x^i\cdot\sum_{l=0}^{r} c_l x^l \;+\; \sum_{i=0}^{m} b_i\cdot\sum_{l=0}^{r} c_l x^l \;=\; P(x)\,R(x)+Q(x)\,R(x)\;;\end{aligned}$$

∎

Si osserva inoltre che distributività e commutatività comportano

$$P(x)\cdot(Q(x)+R(x)) \;=\; P(x)\cdot Q(x) \;+\; P(x)\cdot R(x)\ .$$

**B33b.12** Dalle precedenti proprietà seguono altre equivalenze tra le espressioni polinomiali: per esempio sono equivalenti le espressioni presentate con le uguaglianze seguenti:

$$(x^3-2x+4)(x^2-5x+2) \;=\; (2-5x+x^2)(4-2x+x^3) \;=\; 8-24x+14x^2-x^3-5x^4+x^5$$

$$[(x^2-6)(2x^2-4x+2)](x^3-5x) \;=\; (2x^4-4x^3-11x^2+24x-12)(x^3-5x) \;=$$

$$2x^{-}4x^6-21x^5+4x^4-43x^3-120x^2+60 \;=$$

$$(x^2-6)[2x^5-4x^4-8x^3+20x^2-10x] \;=\; (x^2-6)[(2x^2-4x+2)(x^3-5x)]$$

$$[(x^2+3x-1)+(3x^2-4)](x^3-2x^2) \;=\; (x^5+x^4-7x^3+2x^2)+(3x^5-6x^4-4x^3+8x^2) \;=$$

$$4x^5-5x^4-11x^3+10x^2 \;=\; (4x^2+3x-5)(x^3-2x^2)$$

**B33b.13** Due polinomi si dicono **polinomi proporzionali** se uno si ottiene dall'altro moltiplicandolo per uno scalare di $\mathbb{F}$ diverso dallo zero. Per esempio sono proporzionali i polinomi $F(x)=4x^2+12x-4$ e $G(x)=x^2+3x-1$, in quanto si ha $F(x)=4G(x)$.

La proporzionalità tra polinomi è evidentemente una equivalenza. Conveniamo inoltre che una classe di questa equivalenza sia costituita dal solo polinomio nullo. Una seconda classe è costituita da tutti i polinomi di grado 0, classe che si può identificare con $\mathbb{F}_{nz}$; le altre classi di equivalenza di polinomi si dicono anche **raggi di polinomi**;

Evidentemente due polinomi proporzionali hanno lo stesso grado, ossia: per ogni $c\in\mathbb{Q}_{nz}$ si ha $deg(c\cdot P(x)) = deg(P(x))$ ; in altre parole ogni raggio di polinomi è interamente contenuto in uno degli insiemi di polinomi aventi un grado fissato, cioè in $\mathbb{F}_1[\![x]\!]$, oppure in $\mathbb{F}_2[\![x]\!]$, oppure in $\mathbb{F}_3[\![x]\!]$, ... .

In ogni classe di proporzionalità di polinomi si trova esattamente un polinomio il cui coefficiente direttivo è 1; esso è detto **polinomio monico** e si può assumere come rappresentativo del raggio di polinomi cui appartiene. Per esempio sul campo dei razionali il polinomio monico proporzionale di $2x-3x^2-4x^3$ è $-\frac{1}{2}x-\frac{3}{4}x^2+x^3$. Particolari polinomi monici sono i $x^j$ per ogni $j\in\mathbb{N}$; questi opportunamente sono chiamati **monomi monici**.

La moltiplicazione di un polinomio per un elemento del campo è un caso particolare di prodotto di polinomi, caso in cui uno dei fattori ha grado 0 o -1. Quindi si possono considerare anche le combinazioni lineari dei polinomi: ad esempio se $P(x)=3x^3-x$ e $Q(x)=x^2-6x+5$, si ha $2P(x)-3Q(x)=6x^3-3x^2+16x-15$.

Un polinomio $\sum_{j=0}^{n} c_j\,x^j$ si può considerare la combinazione lineare dei monomi monici $x^j$ avente come coefficienti elementi del campo $c_j$.

**B33b.14** Un polinomio si può considerare una costruzione che si serve delle tre operazioni polinomiali di somma, prodotto e moltiplicazione per elementi di un campo $\mathbb{F}$ e di variabili su tale campo. La moltiplicazione per un elemento del campo $\mathbb{F}$ o per una variabile la chiamiamo **moltiplicazione-$\mathbb{F}$-V**
Queste costruzioni dal punto di vista algebrico si possono attribuire ai semianelli-ab, ossia ai semianelli commutativi [B41c02], strutture più generiche e meno ricche dei campi.

Anche l'insieme dei polinomi su un campo $\mathbb{F}$ munito di somma, prodotto e moltiplicazione-$\mathbb{F}$-V si può considerare un semianello-ab.

Si osserva che i polinomi in quanto costruzioni, possono agire sugli elementi di ogni semianello-ab e in particolare sopra polinomi sullo stesso campo.
Una tale costruzione può conivolgere più variabili, ma qui ci limitiamo ad una sola variabile.
Candideriamo quindi un primo polinomio che chiamiamo "compositore" $P(t)$ e un secondo polinomio $Q(x)$ che chiamiamo "componibile". Definiamo **composizione sostitutiva** di $P(t)$ sopra $Q(x)$ e denotiamo con $P(t)prsostQ(x)$ il polinomio nella variabile $x$ la cui rappresentazione canonica si ottiene sostituendo nella rappresentazione canonica di $P(x)$ ogni occorrenza della $x$ con la rappresentazione canonica di $Q(x)$.
Evidentemente si può rendere più versatile la definizione non limitando alle canoniche le rappresentazioni dei polinomi in gioco.

Esempi:

$$(2+3t-t^2)prsost(4+x^5) \;=\; 2+3(4+x^5)-(16+8x^5+x^{10}) \;=\; -2-5x^5-x^{10}\ ;$$
$$(5+4t^2-2t^3+t^4)prsost(1-x) \;=\; 8+6x+4x^2-2x^3+x^4\ .$$

Per il grado di un polinomio fornito da una composizione sostitutiva si trova facilmente che quali che siano i gradi dei polinomi in gioco abbiamo

$$deg\,(P(t)prsostQ(x)) \;=\; deg(P(t))\cdot deg(Q(x))\ \blacksquare$$

Segnaliamo anche che questa operazione di composizione può essere attribuita ai cosiddetti "polinomi formali", entità definibili come classi di equivalenza di rappresentazioni di polinomi trasformabili gli uni negli altri mediante applicazione delle uguaglianze che caratterizzano le operazioni polinomiali e le operazioni sul relativo campo.
Segnaliamo anche che i polinomi formali sono casi particolari delle serie formali di potenze [I35].

**B33b.15** Spesso accade di individuare significativamente un polinomio come espressione costruita con combinazioni lineari, prodotti, potenze e composizioni sostitutive di altri polinomi.
Queste espressioni possono essere manipolate formalmente servendosi delle proprietà delle operazioni tra polinomi ed elementi del campo binarie fino ad arrivare a una espressione canonica.

Talora invece, come vedremo, sono più utili espressioni diverse dalla canonica, in particolare prodotti di polinomi fattore aventi gradi ridotti o espressioni mediante polinomi di forma particolare. L'elaborazione di queste espressione costituisce una parte del calcolo letterale di rilevante interesse pratico.

Ovviamente due polinomi sopra un campo sono uguali sse presentano la stessa sequenza dei coefficienti, ovvero sse presentano la stessa espressione canonica. Conviene però osservare che il problema dell'uguaglianza di due polinomi forniti da espressioni elaborate può richiedere calcoli impegnativi.

**B33b.16** Alcune uguaglianze tra polinomi equivalenti sono ampiamente utilizzate in molti sviluppi della matematica e in varie delle sue applicazioni.
Presentiamo un gruppo di queste uguaglianze di facile verifica. In queste espressioni con $x_1$, $x_2$ ed $a$ denotiamo generici elementi del campo.

$(x-x_1)(x-x_2)=x^2-(x_1+x_2)x+x_1x_2 \qquad (x+a)^2=x^2+2ax+a^2 \qquad (x+a)^3=x^3+3ax^2+3a^2x+a^3$

$(x+a)^4=x^4+4ax^3+6a^2x^2+4a^3x+a^4 \qquad (x+a)^5=x^5+5ax^4+10a^2x^3+10a^3x^2+5a^4x+a^4$

$x^2-a^2=(x-a)(x+a) \qquad x^3-a^3=(x-a)(x^2+ax+a^2) \qquad x^4-a^4=(x-a)(x^3+ax^2+a^2x+a^3)$

$x(x-1)=x^2-x \qquad x(x-1)(x-2)=x^3-3x^2+2x \qquad x(x-1)(x-2)(x-3)=x^4-6x^3+11x^2-6x$

**B33b.17** Le definizioni delle operazioni di somma, sottrazione e prodotto di due polinomi sono motivate dal fatto che a queste operazioni corrispondono le operazioni omologhe per le corrispondenti funzioni polinomiali. Analogamente sono giustificati il passaggio al polinomio opposto e la moltiplicazione di un polinomio per una costante, ovvero la combinazione lineare di polinomi.

Per le funzioni polinomiali sul campo dei razionali (come per le loro estensioni al campo dei numeri reali) si possono trovare facilmente varie proprietà.

Le più semplici riguardano i monomi monici $x^n$.
Per ogni $k$ intero naturale il polinomio $x^{2k}$ di grado pari è una funzione pari che cresce illimitatamente al crescere di $|x|$; il polinomio $x^{2k+1}$ di grado dispari è invece una funzione dispari che cresce illimitatamente per $x$ crescente e decresce con valori illimitatamente negativi per $x$ sempre più piccolo. Entrambe queste funzioni polinomiali si annullano solo per $x = 0$.

È evidente che per elevati valori della $|x|$ prevale il termine dominante, quello relativo alla massima potenza della variabile.

Le proprietà dei polinomi generici in linea di principio si possono ricondurre a quelle dei corrispondenti polinomi monici.
Tuttavia nella pratica questa riconduzione spesso non è intuitiva. Il comportamento di un polinomio generico per valori non estremi della variabile non si può descrivere in modosemplice ma richiede considerazioni specifiche spesso non semplici che devono ricorrere a considerazioni algebriche non semplici e/o l'utilizzo di strumenti di calcolo numerico e di calcolo automatico.

**B33b.18** I polinomi hanno numerose applicazioni e vengono ampiamente manipolati con strumenti software, in particolare nell'ambito dei maggiori sistemi per il calcolo numerico-simbolico-grafico come `https://it.wikipedia.org/wiki/Maple`, `https://it.wikipedia.org/wiki/Mathematica`, `https://it.wikipedia.org/wiki/Magma` e `https://it.wikipedia.org/wiki/Matlab`.

Per considerazioni complessive su questi **Computer Algebra Systems** si veda `CAS (we)`.

Per tutti questi strumenti e sistemi software sono stati sviluppati metodi di calcolo effettivo e algoritmi riguardanti le elaborazioni su polinomi altamente sofisticati. A questo proposito citiamo `interpolazione di Lagrange (wi)`, `autovalori (wi)` e `metodo dei minimi quadrati (wi)`.

**B33b.19** Vedremo che risulta interessante studiare l'intera successione dei polinomi monici $\langle n \in \mathbb{N} :| x^n \rangle$ .
Più in generale molti problemi portano a esaminare successioni di polinomi che presentano i gradi uguali ai rispettivi indici, successioni della forma $\langle n \in \mathbb{N} :| p_n(x) \rangle$ con $deg(p_n(x)) = n$.
Qui ci limitiamo a citare soltanto la successione dei polinomi di Newton $(x + 1)^n$, la successione dei polinomi fattoriali decrescenti $x(x-1)\cdots(x-n+1)$, e la successione dei polinomi fattoriali crescenti $x(x+1)\cdots(x+n-1)$.

**B33b.20** Si trova facilmente che il polinomio neutro per il prodotto è il polinomio unità, cioè il polinomio costante (di grado 0) avente come unico coefficiente nonnullo $a_0 = 1$. Le proprietà trovate consentono di affermare che l'insieme di polinomi $\mathbb{F}[x]$ munito delle operazioni di somma e prodotto costituisce un `anello commutativo (wi)` [T15, T23].
Si verifica che l'anello $\mathbb{F}[x]$ è un dominio di integrità, cioè un anello.u privo di divisori dello zero [T23a].

L'insieme dei polinomi sopra il campo $\mathbb{F}$ si può considerare uno spazio vettoriale su $\mathbb{F}$ [G40].
Tutti i polinomi di grado inferiore a un dato intero positivo $M$ si possono considerare combinazioni lineari degli $M$ monomi monici 1, $x$, $x^2$, ..., $x^{M-1}$.

La struttura dell'anello dei polinomi sopra un determinato campo, presenta varie caratteristiche simili a quelle dell'anello degli interi: infatti gran parte delle definizioni e delle proprietà degli interi (come teoremi della divisione,funzione MCD, fattorizzazione,...) si possono riformulare in forme analoghe per i polinomi.

## B33 c. divisione tra polinomi

**B33c.01** Come abbiamo giaòsservato può essere utile stabilire se un polinomio di grado elevato è il prodotto di due polinomi di gradi inferiori, in quanto questi spesso risultano più facili da analizzare e manipolare. In particolare risulta più semplice la ricerca dei loro zeri e l'insieme degli zeri del polinomio prodotto è l'unione dei multiinsiemi degli zeri dei due polinomi fattori.

Accade però che i polinomi fattorizzabili sono complessivamente pochi.
Si può tuttavia ottenere una semplificazione meno vantaggiosa, ma applicabile a tutti i polinomi, con una operazione simile a quella che associa a una qualsiasi coppia di interi positivi $n$ e $d$ il quoziente e il resto relativi alla divisione $\dfrac{n}{d}$ .

**B33c.02** **Teorema** Siano $N(x)$ e $D(x)$ due polinomi in $\mathbb{F}[x]$ e sia $D(x) \neq 0$ . Esiste in $\mathbb{F}[x]$ una e una sola coppia di polinomi $\langle Q(x), R(x)\rangle$ tale che sia (i) $N(x) = D(x)\,Q(x)+R(x)$ e (ii) $deg(R(x)) < deg(D(x))$; si ha inoltre (iii) $deg(Q(x)) = deg(N(x)) - deg(D(x))$.

**Dim.:** I polinomi $Q(x)$ e $R(x)$ si chiamano, risp., **quoziente** e **resto** della divisione $\dfrac{N(x)}{D(x)}$ tra **polinomio numeratore** $N(x)$ e **polinomio denominatore** $D(x)$.

Innanzi tutto se $deg(N(x)) < deg(D(x))$ si può scrivere $N(x) = D(x)\cdot 0 + N(x)$ e quindi l'enunciato risulta verificato da $Q(x) = 0$ ed $R(x) = N(x)$.
Per i casi in cui $deg(N(x)) \geq deg(D(x))$ serviamoci delle espressioni

$$N(x) \;=\; \sum_{i=0}^{n} a_i\, x^i \;\text{ e }\; D(x) \;=\; \sum_{i=0}^{m} b_i\, x^i \quad \text{con } \; 0 \leq m = deg(D(x)) \leq n = deg(N(x))$$

e procediamo per induzione sulla differenza dei gradi tra numeratore e denominatore $d = n - m = deg(N(x)) - deg(D(x))$.
Se $d = 0$, cioè se $n = m$, la tesi è verificata da $Q(x) = \dfrac{a_n}{b_n}$ ed $R(x) = N(x) - D(x)\,\dfrac{a_n}{b_n}$.
Supponiamo allora provata l'esistenza della coppia ⟨quoziente, resto⟩ per coppie ⟨numeratore, denominatore⟩ relative a tutte le differenze di gradi minori di $d$ e proviamo l'esistenza della coppia $\langle Q(x), R(x)\rangle$ per le coppie $\langle N(x), D(x)\rangle$ relative alla differenza di gradi $n - m = d$.

Consideriamo il polinomio $M(x) := N(x) - \dfrac{a_n\, x^{n-m}}{b_n}\, D(x)$.
Dato che $a_n - \dfrac{a_n}{b_m}\, b_m = 0$, si ha $deg(M(x)) < n$.
Per l'ipotesi induttiva si può scrivere $M(x) = D(x)\,S(x) + R(x)$ con $deg(R(x)) < m$.
Si può quindi scrivere

$$N(x) \;=\; \frac{a_n x^{n-m}}{b_n} D(x) + M(x) \;=\; D(x)\left(\frac{a_n x^{n-m}}{b_n} + S(x)\right) + R(x)\ ,$$

cioè $N(x)$ si può esprimere nella forma richiesta dall'enunciato con $Q(x) = \dfrac{a_n\, x^{n-m}}{b_n} + S(x)$ .

Resta da verificare l'unicità della coppia ⟨quoziente, resto⟩.
Se $N(x) = D(x)Q(x) + R(x) = D(x)\overline{Q}(x) + \overline{R}(x)$ con $deg(R(x)), deg(\overline{R}(x)) < deg(D(x))$, si ha l'uguaglianza $D(x)\,(Q(x) - \overline{Q}(x)) = \overline{R}(x) - R(x)$. Dato che $deg(\overline{R}(x) - R(x)) < deg(D(x))$, questa uguaglianza è accettabile solo se $Q(x) - Qol(x) = 0$ e $\overline{R}(x) - R(x) = 0$ ∎

Per quoziente e resto della divisione tra i polinomi $N(x)$ e $D(x)$ useremo, risp., le notazioni

$$Qtn(N(x)/D(x)) \quad \text{e} \quad Rmnd(N(x)/D(x))\ .$$

**B33c.03** La dimostrazione precedente suggerisce anche una procedura per calcolare effettivamente il quoziente e il resto di una divisione di polinomi. Nella pratica conviene eseguire questa procedura secondo uno schema noto come **algoritmo di Euclide per quoziente e resto di due polinomi** .
La procedura applicata ai polinomi $N(x)$ e $D(x)$ richiede l'esecuzione di $n-m+1$ stadi che caratterizziamo successivamente con gli interi $n-m$, $n-m-1$, ..., 1, 0. Se si scrive $Q(x) = q_{n-m}x^{n-m} + q_{n-m-1}x^{n-m-1} + \cdots + q_1 x + q_0$, si determinano nell'ordine $q_{n-m}$, $q_{n-m-1}$, ..., $q_1$ e $q_0$. Più precisamente nello stadio $i$ si determina il coefficiente $q_i$, si dispone del polinomio $Q_i(x) = \sum_{j=i}^{n-m} q_j\, x^j$ che per $i=0$ finisce con il coincidere con $Q(x)$ e si rende disponibile il polinomio $R_i(x) := N(x) - D(x)\cdot Q_i(x)$ il cui grado è inferiore a $m+i$ e che per $i=0$ finisce con il coincidere con $R(x)$. Il coefficiente $q_i$ si ottiene dividendo per $b_m$ il coefficiente di $R_{i+1}$ della potenza $x^{m+i}$ (che potrebbe essere nullo).

L'esecuzione manuale dell'algoritmo di Euclide per quoziente e resto di polinomi prevede di operare con due colonne di polinomi: la prima riguarda $N(x)$, interpretabile come $R_{n-m+1}(x)$, e le sue riduzioni $R_i(x)$, ciascuna preceduta dal polinomio $q_i x^i D(x)$ che porta alla riduzione stessa, ultima riduzione essendo $R(x) = R_0(x)$; la seconda colonna serve solo per registrare $D(x)$ e il crescere di $Q(x)$ attraverso i successivi $Q_i(x)$.

**B33c.04** **Eserc.** Verificare che le seguenti quaterne di polinomi soddisfano l'uguaglianza $N(x) = D(x)Q(x) + R(x)$:

$N(x) = x^5 - 3x^3 + 5x + 4 \quad , \quad D(x) = x^3 + 1 \quad , \quad Q(x) = x^2 - 3 \quad , \quad R(x) = -x^2 + 5x + 7$

$N(x) = x^3 + 1 \quad , \quad D(x) = x + 1 \quad , \quad Q(x) = x^2 - x + 1 \quad , \quad R(x) = 0$

$N(x) = 3x^4 + 4x^3 - 5x^2 - 6 \quad , \quad D(x) = 2x^2 + 1 \quad , \quad Q(x) = 3x^2/2 + 2x - 13/4 \quad , \quad R(x) = -2x - 11/4$

**B33c.05** Se $R(x) = 0$ si ha $N(x) \in \mathbb{F}[x]\cdot D(x)$ e si dice che $N(x)$ è **polinomio divisibile** per $D(x)$ in $\mathbb{F}[x]$; equivalentemente si dice anche che $D(x)$ **divide** $N(x)$, che $D(x)$ è **divisore** di $N(x)$, che $N(x)$ è **multiplo** di $D(x)$; in tale caso si scrive $D(x) \nmid N(x)$.

Per esempio sono divisori del polinomio $x^4+3x^3+4x^2-3x-5$ i polinomi $x+1$, $x-1$, $x^2-1$, $x^2+3x+5$, $x^3+4x^2+8x+5$ e $x^3+2x^2+2x-5$.

Si osserva che due polinomi proporzionali sono divisori l'uno dell'altro e che viceversa se due polinomi sono divisori l'uno dell'altro allora sono proporzionali.

Accade inoltre che ogni polinomio è divisibile per se stesso e per ogni polinomio di grado 0, cioè per ogni polinomio costante. Si dicono **divisori banali di un polinomio** $P(x)$ tutti i polinomi delle forme $k$ e $k\cdot P(x)$ per ogni $k \in \mathbb{F}_{nz}$. Evidentemente di un polinomio presentano interesse effettivo solo i divisori non banali.

**B33c.06** Un polinomio $P(x) \in \mathbb{F}_{\geq 1}(x)$ si dice **polinomio irriducibile** sse è privo di divisori nonbanali.
Si osserva anche che: (i) tutti i polinomi sono divisori del polinomio nullo; (ii) l'insieme dei divisori di un qualsiasi polinomio di grado 0 è dato dall'insieme dei polinomi di grado 0; (iii) tutti i polinomi di grado 1 sono irriducibili.
Quindi presentano interesse solo i divisori non banali dei polinomi di grado maggiore o uguale a 2.

L'insieme dei multipli non banali di un polinomio $P(x) \in \mathbb{F}_{\geq 1}[x]$ è $P(x)\cdot \mathbb{F}_{\geq 1}[x]$.

Vedremo che la determinazione dei divisori di un polinomio non è un problema semplice e che tale insieme dipende dal campo sul quale viene definito l'insieme dei polinomi in esame.

**B33c.07** Consideriamo $F(x), G(x) \in \mathbb{F}[x]$.

Un polinomio $D(x) \in \mathbb{F}[x]$ si dice **massimo comun divisore** di $F(x)$ e $G(x)$ sse $D(x) \,\vdots\, F(x)$, $D(x) \,\vdots\, G(x)$ e per ogni polinomio $Q(x)$ tale che $Q(x) \,\vdots\, F(x)$ e $Q(x) \,\vdots\, G(x)$ si ha $Q(x) \,\vdots\, D(x)$ .

Contrariamente a quanto accade ai numeri interi, due polinomi hanno più di un massimo comun divisore: per esempio $4x^2 - 1$ e $6x^2 - 15x + 6$ hanno come massimo comun divisore in $\mathbb{Q}$ il polinomio $2x - 1$ e tutti gli altri polinomi proporzionali a esso, ossia polinomi della forma $2\,q\,x - q$ con $q \in \mathbb{Q}_{nz}$, polinomi ciascuno dei quali è divisore di tutti gli altri.

Risulta opportuno definire la funzione MCD$(P, Q$ che a due polinomi $P$ e $Q$ associa l'unico polinomio monico che sia divisore di entrambi e che abbia il grado massimo.

Per esempio $\mathrm{MCD}(4\,x^2 - 1\ ,\ 6\,x^2 - 15\,x + 6) \ = \ x - \dfrac{1}{2}$.

Due polinomi privi di divisori non banali comuni si dicono **polinomi coprimi**. A due tali polinomi la funzione MCD associa il polinomio unità $1x^0$.

Il massimo comun divisore si trova facilmente nel caso di due polinomi dei quali si conoscono tutti i divisori: basta considerare il prodotto di tutti i divisori nonbanali monici comuni.

**B33c.08** L'algoritmo di Euclide delle divisioni successive che garantisce l'esistenza del massimo comun divisore di due interi e consente di individuarlo, si può estendere anche ai polinomi.

Denotiamo i due polinomi (nonnulli) da esaminare con $P_1(x)$ e $P_2(x)$ e supponiamo che sia $deg(P_1) \geq deg(P_2)$.
Questo algoritmo si sviluppa in un certo numero finito di stadi successivi caratterizzati dagli interi 1, 2, ... ; nello stadio $i$ a partire dai due polinomi $P_i$ e $P_{i+1}$ si individua un nuovo polinomio della sequenza, $P_{i+2}$ come resto della divisione tra i precedenti; deve cioè essere

$$P_i(x) = P_{i+1}(x)Q_{i+1}(x) + P_{i+2}(x) \quad \text{con} \quad deg(P_i) \geq deg(P_{i+1}) > deg(P_{i+2}) \ .$$

A conclusione dello stadio $i$ se $P_{i+2}$ non è il polinomio nullo si procede allo stadio successivo, mentre in caso contrario il processo si conclude.
Dato che i gradi dei polinomi $P_{i+2}$ che si vanno trovando costituiscono una sequenza decrescente, il processo si conclude dopo un numero finito di stadi $k$ con la uguaglianza $P_k(x) = P_{k+1}(x)Q_{k+1}(x)$ e con lo stabilire che uno dei massimi comun divisori di $P_1(x)$ e $P_2(x)$ è $P_{k+1}$, ovvero l'ultimo resto nonnullo delle successive divisioni.

Si vede facilmente che $P_{k+1}(x)$ divide $P_k$, $P_{k-1}$,..., $P_2$ e $P_1$, ovvero che è un divisore dei due polinomi di partenza.
Le espressioni per i $P_i$ mostrano anche che un divisore di $P_1$ e $P_2$ divide anche $P_3$, ..., $P_k$ e $P_{k+1}$; quindi $P_{k+1}$ è uno dei massimi comuni divisori richiesti.

**B33c.09** **Teorema** (**identità di Bézout**)
Consideriamo due polinomi $F(x)$ e $G(x)$ e un $D(x) = \mathrm{MCD}(F(x), G(x))$ allora in $\mathbb{F}[x]$ si trovano i polinomi $H(x)$ ed $L(x)$ tali che $D(x) = F(x) \cdot H(x) + G(x) \cdot L(x)$.

## B33 d. espressioni polinomiali su numeri e su variabili razionali

**B33d.01** Le espressioni contenenti la $x$ alle quali si è accennato si dicono **espressioni polinomiali** sui razionali nell'indeterminata $x$.

Ad un'espressione polinomiale nella variabile $x$ che denotiamo con $\mathcal{E}(x)$ si associa la **funzione polinomiale**

$$\ulcorner\, x \in \mathbb{Q} \mapsto \mathsf{val}\big(\mathcal{E}(x)\big) \,\urcorner \in \ulcorner\, \mathbb{Q} \longmapsto \mathbb{Q} \,\urcorner \ . \tag{1}$$

Qui con $\mathsf{val}(\mathcal{E}(x)$ denotiamo il valore ottenuto eseguendo il procedimento rappresentato dalla espressione $\mathcal{E}$ sopra uno dei possibili valori della variabile $x$.

Anticipiamo che, mentre rimanendo nell'ambito di $\mathbb{Q}$ non si pongono limitazioni al dominio delle funzioni polinomiali, questo non accade per altre funzioni numeriche, per esempio per le funzioni razionali presentate in :u .

Denotiamo inoltre con $\boldsymbol{FunPln}(\mathbb{Q}, x)$ l'insieme delle funzioni polinomiali sui razionali alle quali le espressioni conducono.

La (1) individua una funzione da $\boldsymbol{ExprPln}(\mathbb{Q}, x)$ su $\boldsymbol{FunPln}(\mathbb{Q}, x)$ che diciamo **interpretazione funzionale dei polinomi**.

**B33d.02** Nel seguito del capitolo considereremo soprattutto espressioni polinomiali in una sola variabile $x$. Si possono però considerare polinomi in due, tre o più variabili, in quanto i discorsi precedenti si possono ripetere senza difficoltà per espressioni polinomiali contenenti più lettere per ciascuna delle quali si chiede possa essere rimpiazzata da opportuni valori numerici razionali (più avanti vedremo che si possono considerare altri insiemi di valori numerici).

Queste espressioni consentono di individuare insiemi piuttosto articolati di espressioni numeriche che si rivelano utili in tante circostanze.

Per esempio in geometria piana l'espressione $ax^2 + bx + c$ nelle variabili $x$, $a$, $b$ e $c$ consente di trattare l'insieme delle parabole nel piano cartesiano aventi l'asse di simmetria verticale [G50b, G50i]; nella geometria tridimensionale il volume di un generico cuboide (cioè di un parallelepipedo rettangolo) con le lunghezze dei lati espresse da tre variabili $\ell_1$, $\ell_2$ e $\ell_3$ che possono assumere arbitrari valori positivi è dato dall'espressione polinomiale $\ell_1 \cdot \ell_2 \cdot \ell_3$.

Le espressioni polinomiali in due variabili che in genere denotiamo con $x$ e $y$, come $x^2 - 2y^2 + 15\,x\,y$ o $\dfrac{3}{11}\,x^2 + y^2$ , consentono di individuare funzioni del genere $\ulcorner\, \mathbb{Q} \times \mathbb{Q} \longmapsto \mathbb{Q} \,\urcorner$.
Se denotiamo una espressione polinomiale in due variabili con $\mathcal{E}(x, y)$ si ha la funzione

$$\ulcorner\, x, y \in \mathbb{Q} \mapsto \mathsf{val}\big(\mathcal{E}(x, y)\big) \,\urcorner \ . \tag{1}$$

Le espressioni polinomiali in tre variabili che, come spesso accade, denotiamo, risp., con $x$, $y$ e $z$, come $\dfrac{1}{4}\,x^2 + y^2 - 3\,y\,z^2$, consentono di individuare funzioni del genere $\ulcorner\, \mathbb{Q}^{\times 3} \longmapsto \mathbb{Q} \,\urcorner$.
Definizioni prevedibili si possono fare per 4, 5, ... variabili.

**B33d.03** Per i simboli che si incontrano nelle espressioni polinomiali (e nelle espressioni di moltissime altre forme) si usa anche il termine **parametri**. Ai due termini vengono attribuiti significati diversi che si distinguono solo in relazione al contesto nel quale si utilizzano le espressioni in esame. Per esempio nell'espressione $ax^2 + bx + c$ si dice che $x$ è la variabile mentre $a$, $b$ e $c$ sono tre parametri quando si vuole prendere in considerazione la famiglia i cui membri sono determinati dagli indici $a$, $b$ e $c$ che variano in $\mathbb{Q}$ delle curve di $\mathbb{Q} \times \mathbb{Q}$ che sono fornite dalle funzioni $\ulcorner\, x \in \mathbb{Q} \mapsto a\,x^2 + b\,x + c \,\urcorner$ .

**B33d.04** In precedenza abbiamo introdotto discorsivamente le espressioni polinomiali sul campo $\mathbb{F}$ nella variabile $x$. In buona sostanza, per espressione polinomiale nella variabile $x$ intendiamo un'espressione costruita sulle forme frazionarie dei numeri razionali, sulla lettera $x$, su eventuali altri parametri ($a$, $b$, ...) servendosi delle composizioni di somma, differenza, prodotto e cambiamento di segno; queste sono rappresentate dai noti operatori binari infissi "+", "−", "·" e dall'operatore unario prefisso "−" i quali sono da racchiudere con i loro operandi tra due parentesi coniugate.

Si pone tuttavia anche il problema di una definizione più precisa dell'insieme $\boldsymbol{E}$ delle espressioni polinomiali che renda possibile stabilire distinzioni ed equivalenze tra polinomi. Si vuole anche che la definizione consenta di individuare meccanismi per la elaborazione manuale e automatica delle espressioni che permettano di risolvere operando solo sui simboli svariati problemi riguardanti le funzioni polinomiali e i polinomi intesi più astrattamente come entità algebriche.

Il modo più preciso per definire $\boldsymbol{E}$ consiste nel servirsi di strumenti della teoria dei linguaggi e delle grammatiche acontestuali che definiremo in C14e, C14f e C14g.
Qui ci limitiamo a un procedimento un po' intuitivo, ma non molto distante da quello ottenibile con il formalismo delle grammatiche, per giungere in fretta a conclusioni di immediata utilità.

Si procede in modo graduale iniziando con le espressioni più semplici e individuando costruzioni formali che portano ad espressioni via via più articolate. Infatti l'insieme $\boldsymbol{E}$ non si può individuare con un'espressione chiusa, ma solo con regole che permettono di decidere se una stringa costituisce una espressione polinomiale corretta o meno.

Qui procederemo individuando per prime espressioni polinomiali piuttosto semplici da definire, ma in genere appesantite da elementi ridondanti; solo successivamente individueremo espressioni più agili da maneggiare come varianti tendenzialmente più semplici delle precedenti.

**B33d.05** Tra le espressioni polinomiali occorre individuare la relazione costituita dalle coppie di espressioni che individuano le stesse funzioni polinomiali.
Si tratta della relazione canonicamente associata alla funzione di interpretazione funzionale delle espressioni polinomiali [a03]. Questa relazione è evidentemente un'equivalenza: quindi è lecito chiamare **espressioni polinomiali equivalenti** due espressioni che conducono alla stessa funzione polinomiale.

Per esempio è evidente che sono equivalenti

$$((4+x)\cdot(8-x)) \text{ e } ((8-x)\cdot(x+4)) \quad ; \quad (x-(-1/2)) \text{ e } (x+1/2)$$
$$((x+1/2)+(2\cdot x-3)) \text{ e } ((3\cdot x)-5/2)\ .$$

Questa equivalenza viene giustificata dalle uguaglianze che esprimono le proprietà delle operazioni polinomiali e delle operazioni tra numeri razionali. La prima equivalenza discende dalla commutatività della somma e del prodotto. La seconda dal carattere involutorio del meno unario. La terza dalla associatività della somma, dalla distributività di somma e prodotto e dalle regole di composizione dei numeri razionali.

Ci proponiamo quindi di ampliare le classi di equivalenza tra epcp per comprendere loro varianti più maneggevoli nel rispetto delle operazioni polinomiali e delle operazioni tra razionali.

A questo ampliamento chiediamo di soddisfare due esigenze.

(a) Data una stringa costituita da forma frazionarie, da occorrenze della variabile $x$, da operatori polinomiali, da eventuali parametri e da parentesi tonde, si deve poter decidere se essa costituisce una espressione polinomiale corretta o meno.

(2) Date due espressioni polinomiali si sappia decidere con un algoritmo se esse sono equivalenti oppure se conducano a diverse funzioni polinomiali.

Le epcp costituiscono una collezione di stringhe molto variegata destinata ad arricchirsi ulteriormente con l'aggiunta delle forme semplificate; risulta quindi opportuno dare una classificazione delle espressioni polinomiali che aiuti a tenerle sotto controllo.

B33**d.06** Nelle epcp ogni coppia di parentesi coniugate delimita una stringa che costituisce essa stessa una epcp; una di queste sottostringhe di una espressione polinomiale si dice **sottoespressione polinomiale dell'espressione**

Le epcp si possono semplificare con operazioni di riduzione che sostituiscono ogni sottoespressione polinomiale con un simbolo $R$ che si può considerare come rappresentante di una sottoespressione generica oppure come rappresentante del risultato che si può ottenere con la valutazione della sottoespressione.

Una stringa sull'alfabeto $\mathsf{A}_{pol}$ è una epcp sse con successive riduzioni del genere precedente si riduce alla generica cancellazione di coppie di parentesi coniugate ridondanti e attraverso la sostituzione di sottoespressioni con espressioni equivalenti in virtù di proprietà delle operazioni di somma, differenza, prodotto e cambiamento di segno di numeri razionali.

Procediamo a esaminare gli schemi delle semplificazioni possibili: in questi useremo lettere come $A$, $B$ e $C$ per denotare o una epcp o un'altra espressione polinomiale accettabile in virtù delle semplificazioni che stiamo definendo.

Le epcp non elementari hanno la forma $(\mathcal{C})$: le parentesi esterne possono essere cancellate in quanto la stringa $\mathcal{C}$ consente di individuare lo stesso procedimento di calcolo. Per esempio l'espressione $(A+B)$ si semplifica nella $A+B$, la $(A \cdot B)$ nella $A \cdot B$ e la $((A-B)\cdot(C+D))$ nella $(A-B)\cdot(C+D)$.

La associatività della somma consente di semplificare le espressioni $((A+B)+C)$ e $(A+(B+C))$ nella $(A+B+C)$: infatti la priorità tra le due operazioni di somma è inessenziale.

La associatività del prodotto consente di semplificare le espressioni $((A\cdot B)\cdot C)$ e $(A\cdot(B\cdot C))$ nella $(A\cdot B\cdot C)$: infatti la priorità tra le due operazioni di prodotto è inessenziale.

Dal collegamento tra operatore "-" binario e unario si può semplificare l'espressione $(A+(-B))$ nella $(A+B)$.

La $((A+B)-C)$ e $(A+(B-C))$ si possono semplificare nella $(A+B-C)$: a somma e differenza si può assegnare la stessa priorità.

La $(A-B-C)$ costituisce una semplificazione della $((A-B)-C)$, ma non della $(A-(B-C))$: in effetti la differenza non è un'operazione associativa e tra due operatori "$-$" consecutivi si conviene di assegnare la priorità a quello più a sinistra.

La $(A-B+C)$ costituisce una semplificazione della $((A-B)+C)$, ma non della $(A-(B+C))$ che non le è equivalente: in effetti tra due operatori consecutivi "$+$" e "$-$" si assegna la priorità al più a sinistra.

Un'espressione $(-(-A))$ si semplifica nella $A$ in virtù della idempotenza del cambiamento di segno.

Le espressioni $(A+0)$ e $(0+A)$ si semplificano nella $A$ grazie al fatto che 0 è elemento neutro per la somma.

Le espressioni $(A\cdot 1)$ e $(1\cdot A)$ si semplificano nella $A$ grazie al fatto che 1 è elemento neutro per il prodotto.

Le espressioni $(A\cdot 0)$ e $(0\cdot A)$ si semplificano nella $(0)$ grazie al fatto che 0 è elemento assorbente per il prodotto.

L'espressione $(A+(-A))$ e $(A-A)$ si semplificano nella $(0)$ grazie alle definizioni degli operatori "$-$" unario e binario in relazione alla somma.

**B33d.07** Un'espressione della forma $((A \cdot B) + C)$ si può semplificare nella $(A \cdot B + C)$, in quanto si conviene di assegnare al prodotto la priorità rispetto all'esecuzione sulla somma.
La priorità riguarda due operatori successivi nella stringa, indipendentemente da quale si trovi più a sinistra. Quindi un'espressione della forma $(A + (B \cdot C))$ si può semplificare nella $(A + B \cdot C)$.

Al prodotto si assegna la priorità anche rispetto alla differenza e quindi un'espressione $((A \cdot B) - C)$ si può semplificare nella $(A \cdot B - C)$ e un'espressione $(A - (B \cdot C))$ nella $(A - B \cdot C)$.

Va notato che un'espressione $((A + B) \cdot (C + D)$ non si può semplificare nella $(A + B \cdot C + D)$: questa può invece rimpiazzare $((A + (B \cdot C)) + D)$ e $(A + ((B \cdot C) + D))$.

Inoltre la $((A + B) \cdot C)$ non si può semplificare nella $(A + B \cdot C)$, che si ottiene semplificando la $(A + (B \cdot C))$ non equivalente alla prima data.

**B33d.08** Conviene introdurre le potenze intere naturali delle sottoespressioni definendo $(A^0) := 1$, $(A^1) := A$, $(A^2) := (A \cdot A)$, $(A^3) := (A \cdot (A^2)) = ((A^2) \cdot A)$, ... .

All'operatore di elevamento a potenza intera si assegna la priorità su prodotto, somma e differenza: quindi per ogni $h$ intero positivo $((A^h) \cdot B)$ si semplifica nella $(A^h \cdot B)$, $(A \cdot (B^h))$ si semplifica nella $(A \cdot B^h)$, $((A^h) + B)$ si semplifica nella $(A^h + B)$, $(A + (B^h))$ si semplifica nella $(A + B^h)$, $((A^h) - B)$ si semplifica nella $(A^h - B)$, e $(A - (B^h))$ si semplifica nella $(A - B^h)$.

Si giunge in tal modo a definire come **insieme delle espressioni polinomiali** l'insieme ottenibile dalla totalità delle epcp ampliato applicando in tutti i modi [possibili le semplificazioni precedenti ed inoltre eliminando le paremtesi coniugate che delimitano una intera espressione.

**B33d.09** Le espressioni polinomiali si possono utilmente raffigurare mediante arborescenze distese [D30D] con i nodi etichettati da elementi dell'alfabeto dei polinomi.

Queste arborescenze, oltre a costituire gli schemi visuali che determinano la sintassi delle espressioni polinomiali, costituiscono gli schemi visuali dei processi di calcolo che portano al valori delle corrispondenti funzioni polinomiali.

**B33d.10** Ad ogni espressione polinomiale corrisponde una funzione polinomiale.
Questa corrispondenza univoca è tutt'altro che biunivoca: tutte le espressioni che forniscono espressioni polinomiali equivalenti portano alla stessa funzione polinomiale.

Vediamo alcuni esempi di duetti di espressioni polinomiaali equivalenti.

(a) $(3 + x^3) + (x - 3x^2)$ e $(x - 3x^2) + (3 + x^3)$;

(b) $(3 + x^3) \cdot (x - 3x^2)$ e $(x - 3x^2) \cdot (3 + x^3)$;

(c) $(4 + x^2 + 5x^3)$ e $5x^3 - x^2 + 4$;

Due espressioni polinomiali che conducono alla stessa funzione polinomiale si dicono **espressioni polinomiali equivalenti**.

**B33d.11** Ricordiamo che si dice **monomio** una espressione razionale nella quale non compare l'operazione somma, ovvero un'espressione della forma $\pm q \cdot x^h$ con $q$ razionale e $h \in \mathbb{N}$. L'intero $h$ si dice **grado del monomio**.

Si dice **binomio** un'espressione esprimibile come somma o come differenza di due monomi; si dice **trinomio** un'espressione riconducibile alla combinazione lineare di tre monomi; si dice **quadrinomio** un'espressione riconducibile alla combinazione lineare di quattro monomi; e così via.
Ogni espressione polinomiale è equivalente a una combinazione lineare di monomi.

Si dice grado di un polinomio il grado del monomio di grado massimo cioè il grado del suo termine prevalente.

Si distinguono i polinomi dei vari gradi.

B33**d.12** Ogni espressione polinomiale si può ricondurre a una espressione canonica equivalente e questa è unica.
Si pone il problema dell'equivalenza di due espressioni polinomiali. Questo problema si può sempre risolvere: basta ricondurre entrambe alla loro canonica equivalente e constatare su di esse se le due espressioni ottenute coincidono o meno.

B33**d.13** Nella pratica l'equivalenza si decide anche con procedimenti abbreviati.

## B33 e. polinomi sopra un campo

**B33e.01** Dopo aver introdotti i polinomi sopra $\mathbb{Q}$ potremo introdurre con discorsi analoghi i polinomi sopra altri insiemi numerici individuati costruttivamente che includono propriamente $\mathbb{Q}$, come l'insieme dei numeri reali che vedremo in B42 e l'insieme dei numeri complessi che introdurremo in B50.

Le trattazioni di tutte queste collezioni di polinomi risultano molto simili, in quanto si basano sopra le operazioni polinomiali e le loro proprietà di natura algebrica (commutatività, associatività, distributività, ...) e sono poco dipendenti dalle differenze costruttive degli insiemi terreno.

Conviene quindi portare avanti anche una trattazione più generale ed astratta introducendo un insieme di polinomi sopra un insieme numerico caratterizzato solo dall'essere munito delle operazioni polinomiali (somma, sottrazione, prodotto e cambiamento di segno) caratterizzate solo da loro proprietà algebriche.
Un tale sistema insieme munito di operazioni costituisce una struttura algebrica della specie dei campi, specie che esamineremo più sistematicamente in B41c.

**B33e.02** I polinomi sono entità matematiche che si possono manipolare piuttosto semplicemente e questo fa sì che essi risultino utili per un gran numero di sviluppi computazionali e nella risoluzione di molti problemi. Tuttavia per essere definiti in modo soddisfacente, anche in relazione alla generalizzazione accennata, i polinomi richiedono un discorso un poco elaborato.

Innanzi tutto occorre dire che è opportuno considerare insiemi di polinomi ciascuno associato a un insieme di numeri che, come i numeri razionali, costituiscono un cosiddetto campo. Per campo in matematica si intende un insieme di entità (numeri o entità simili) che possono essere composti con operazioni di tipo aritmetico (addizione, sottrazione, moltiplicazione e divisione) le quali godono di proprietà come la commutatività e la associatività della addizione e della moltiplicazione e la distributività della addizione rispetto alla moltiplicazione; in un campo inoltre si devono trovare un numero zero, 0 elemento neutro per la somma, e un numero uno, 1, che sia elemento neutro per il prodotto.

Si possono considerare polinomi di una o più variabili; qui ci limitiamo ai polinomi di una variabile che chiameremo semplicemente polinomi.

I polinomi (di una variabile) sopra un campo sono costituiti da sequenze di questi numeri e si possono comporre con operazioni che estendono quelle sui numeri del campo; le operazioni di somma, sottrazione, e moltiplicazioni godono di proprietà simili a quelle delle operazioni omologhe del campo, mentre la divisione di due polinomi solo raramente individua un unico polinomio risultato.

In vista della prospettata generalizzazione nel seguito denoteremo con $F$ il terreno di un generico campo (in particolare potrebbe essere l'insieme dei numeri razionali) munito delle operazioni polinomiali e comprendente 0 e 1, il primo elemento neutrro oer l'operazione somma e il secondo elemento neutro per il prodotto.

**B33e.03** Definiamo polinomio sul campo $\mathbb{F}$ avente come terreno l'insieme $F$ una sequenza finita di elementi di $F$ che scriviamo nella forma $P = \langle a_0, a_1, ..., a_n \rangle$ e per la quale chiediamo che per ogni $n \geq 1$ sia $a_n \neq 0$.

Le componenti della sequenza si dicono coefficienti del polinomio. I polinomi relativi a $n = 0$ si dicono polinomi costanti; il polinomio con $n = 0$ e $a_0 = 0$ si dice polinomio nullo.

Si dice grado del polinomio l'intero $n$ se esso è positivo oppure se $n = 0$ ma $a_0 \neq 0$; al polinomio nullo assegnamo il grado $-1$. Il grado del polinomio $P$ si denota con $deg(P)$

Su queste sequenze si possono definire le operazioni aritmetiche e studiarne le proprietà algebriche. Conviene però introdurre per i polinomi scritture che costituiscono una complicazione per la loro definizione, ma risultano vantaggiose per l'esecuzione manuale delle operazioni e chiariscono il loro ruolo nella definizione delle funzioni del genere $\lceil K \longmapsto K \rceil$ che chiamiamo funzioni polinomiali.

**B33e.04** I polinomi (di una variabile) vengono trattati sistematicamente attraverso espressioni nelle quali interviene un simbolo per il quale spesso si sceglie la lettera $x$ e che viene chiamato **indeterminata**.

Diciamo espressione canonica nella indeterminata $x$ del polinomio $P = \langle a_0, a_1, ..., a_n \rangle$ sul campo $\mathbb{F}$ la scrittura della forma

$$P(x) \;=\; a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \;.$$

In questa scrittura la $x$ assume il ruolo di una variabile che può assumere come valori tutti gli elementi di $F$.
La scrittura precedente quindi è una rappresentazione di un processo di calcolo.
Accanto a una espressione canonica si possono considerare tutte le espressioni equivalenti, espressioni riconducibili a questa applicando le uguaglianze che estendono le proprietà delle operazioni aritmetiche degli elementi del campo.
Per esempio il polinomio $P = \langle 2, -1.5, 0, 1.25 \rangle$ è individuato dalla espressione canonica

$P(x) = 2 - \dfrac{3}{2}\,x + \dfrac{5}{4}\,x^3$ (nella quale trascuriamo di indicare la potenza $x^2$ il cui coefficiente è 0)

e dalle espressioni equivalenti $\dfrac{5}{4}x^3 - \dfrac{3}{2}x + 2$ e $\frac{x}{4}(x^2 - 6) + 2$ .

**B33e.05** In relazione alla interpretazione computazionale delle espressioni polinomiali, diciamo **funzione associata a un polinomio** $P$ la funzione che a ogni elemento $\overline{x} \in F$ associa l'elemento di $F$ ottenibile con le operazioni indicate da una delle espressioni $P(x)$ associate in seguito alla sostituzione con il valore $\overline{x}$ della indeterminata $x$.
Questa funzione può essere individuata con ciascuna delle scritture equivalenti alla sua rappresentazione canonica $P(x)$.

**B33e.06** L'insieme dei polinomi sul campo $\mathbb{F}$ forniti dalle corrispondenti espressioni polinomiali nella indeterminata $x$ si denota tradizionalmente con il simbolo $\mathbb{F}[x]$. In seguito useremo anche la notazione $\mathsf{PIn}_{\mathbb{F}}[x]$, più vicina alle notazioni qui usate per altre collezioni di funzioni definite costruttivamente.

Dotiamo $\mathbb{F}[x]$ di due operazioni binarie chiamate somma e prodotto che si possono considerare estensioni delle operazioni di somma e prodotto per il campo $\mathbb{F}$ e per le quali usiamo gli stessi simboli "+" e "·" .
Le definizioni si servono delle espressioni canoniche dei polinomi usate con una certa elasticità.
In particolare è opportuno considerare come equivalente di una espressione canonica di un polinomio $P(x) = \sum_{i=0}^{n} a_i\, x^i$ ogni espressione della forma $P(x) = \sum_{i=0}^{n+h} a_i\, x^i$ con $h = 1, 2, ...$ con $a_{n+1} = a_{n+2} = ... = a_{n+h} := 0$ . Le espressioni canoniche dei polinomi e le loro suddette varianti le chiamiamo **espressioni semicanoniche**.

Consideriamo quindi due polinomi $P(x) \;=\; \sum_{i=0}^{n} a_i\, x^i$ e $Q(x) = \sum_{j=0}^{m} b_i\, x^i$ .
Si dice somma dei polinomi $P$ e $Q$ il polinomio $P+Q$ dato dalla espressione semicanonica $(P+Q)(x) = \sum_{i=0}^{g} (a_i + b_i) x^i$ dove $g = \max(n, m)$. Il grado di questo polinomio somma, se $n \neq m$ è $g = \max(n, m)$,

mentre se $n = m$ potrebbe essere inferiore a tale grado, in quanto potrebbe essere $a_n = -b_n$ e in questo caso potrebbe essere $a_{n-1} = -b_{n-1}$ e così via. Quindi si può solo dire che

$$deg(P(x) + Q(x)) \leq \max(deg(P(x)), deg(Q(x)))$$

Per esempio la somma dei polinomi $P(x) = 4x^3 + 12x - 4$ e $Q(x) = x^2 + 3x - 1$ di grado, risp., 3 e 2, è $P(x) + Q(x) = 4x^3 + x^2 + 15x - 5$ il cui grado è 3.

La somma dei due polinomi di grado 2 $S(x) = -x^2+2x+4$ e $T(x) = x^2+3x-1$ è $S(x)+T(x) = 5x+3$ il cui grado è 1.

Si dimostra facilmente che la somma di polinomi è un'operazione commutativa e associativa e che il polinomio nullo è l'elemento neutro per la somma.

**B33e.07** Si dice **opposto di un polinomio** $P$ il il polinomio denotato con $-P$ i cui coefficienti sono gli elementi di $F$ opposti dei rispettivi coefficienti di $P$. In altre parole l'opposto del polinomio dato dall'espressione $P(x) = \sum_{i=0}^{n} a_i\, x^i$ è il polinomio $-P(x) := \sum_{i=0}^{n} -a_i\, x^i$ .
Il passaggio al polinomio opposto è una trasformazione involutoria, cioè per ogni polinomio $P$ si ha $-(-(P) = P$. L'unico polinomio che coincide con il proprio opposto è il polinomio nullo.

Si dice differenza tra due polinomi $P$ e $Q$ la somma di $P$ e l'opposto di $Q$: $P - Q := P + (-Q)$ .

**B33e.08** Si dice prodotto dei polinomi $P$ e $Q$ il polinomio denotato con $P \cdot Q$ dato dall'espressione

$$(P \cdot Q)(x) \;:=\; \sum_{i=0}^{n+m} c_i \text{ , dove per ogni } i = 0, 1, 2, ..., n+m \text{ si assume } c_i := \sum_{j=0}^{i} a_j \cdot b_{i-j} \text{ .}$$

Per il grado del polinomio prodotto quindi

$$deg\,(P(x) \cdot Q(x)) \;=\; deg(P(x)) + deg(Q(x)) \text{ .}$$

In particolare il prodotto del polinomio nullo per ogni altro polinomio è uguale al polinomio nullo.
Per esempio $(x^3 + 2x - 4) \cdot (-x^2 + 2x - 3) \;=\; -x^5 + 2x^4 - 5x^3 + 12x^2 - 14x + 12$ .

Si dimostra facilmente che il prodotto è commutativo, associativo e distributivo rispetto alla somma.
Inoltre si trova che il polinomio neutro per il prodotto è il polinomio unità, cioè il polinomio costante, ossia di grado 0, avente come unico coefficiente $a_0 = 1$.
L'insieme di polinomi $\mathbb{F}[x]$ con le operazioni di somma e prodotto e gli elementi 0 e 1 costituisce un anello commutativo unifero [B41c04].
Si verifica facilmente che l'anello $\mathbb{F}[x]$ è un dominio di integrità, ossia è privo di divisori dello zero [B41c11].

**B33e.09** Due polinomi si dicono proporzionali se uno si ottiene dall'altro moltiplicandolo per un elemento di $F$ diverso da zero, cioè per un polinomio costante nonnullo (polinomio di grado 0).
Per esempio se $G(x) = 4x^2 + 12x - 4$ e $H(x) = x^2 + 3x - 1$ si ha $G(x) = 4\,H(x)$.
Evidentemente la proporzionalità tra polinomi nonnulli è una equivalenza e due polinomi proporzionali hanno lostesso grado: dunque per ogni $c \in \mathbb{Q}_{nz}$ si ha $deg(c \cdot P(x)) = deg(P(x))$ .

In ogni classe di proporzionalità di polinomi c'è un solo polinomio il cui coefficiente direttivo è 1; esso è detto **polinomio monico**.

Dei polinomi si possono considerare le combinazioni lineari.
Quindi l'insieme dei polinomi sopra il campo $\mathbb{F}$ si può considerare uno spazio vettoriale su $\mathbb{F}$.

Tutti i polinomi di grado non superiore a un dato intero positivo $M$ si possono considerare combinazioni lineari degli $M+1$ polinomi monici 1, $x$, $x^2$, ..., $x^M$.

Spesso accade di individuare un polinomio come espressione costruita con somme e prodotti di altri polinomi. Queste espressioni possono essere sviluppate servendosi delle proprietà delle operazioni binarie fino ad arrivare a una espressione canonica.
Talora invece, come vedremo, sono più utili espressioni diverse dalla canonica, in particolare prodotti di polinomi fattore di grado ridotto o espressioni mediante polinomi appartenenti a collezioni particolari. L'elaborazione di queste espressione costituisce buona parte del calcolo letterale.

Naturalmente due polinomi sopra un campo sono uguali se e solo se presentano la stessa sequenza dei coefficienti. Questa è un'affermazione un po' banale; Conviene però osservare che il problema dell'uguaglianza di due polinomi forniti da espressioni elaborate può richiedere calcoli impegnativi.

B33e.10 La struttura dell'anello dei polinomi sopra un determinato campo, presenta qualche caratteristica simile a quella dell'anello degli interi, nel senso che gran parte delle definizioni e delle proprietà degli interi (come teoremi della divisione, MCD, fattorizzazione,...) si possono riesprimere in forme analoghe per i polinomi.

B33e.11 **Teorema** Consideriamo un campo $\mathbb{F}$ con terreno $F$ e l'anello dei polinomi nella indeterminata $x$ a coefficienti in $F$ $\mathbb{F}[x]$. Siano $N(x)$ e $D(x)$ due polinomi $\in \mathbb{F}[x]$ con $D(x) \neq 0$ . Esiste una e una sola coppia di polinomi $\langle Q(x), R(x) \rangle$ in $\mathbb{F}[x]$ tali che

$$N(x) = Q(x)D(x) + R(x), \text{ con } deg(Q(x) = deg(N(x)) - deg(D(x)) \text{ e } deg(R(x)) < deg(D(x)) \ .$$

**Dim.**: Innanzi tutto se $deg(N(x)) < deg(D(x))$ si può scrivere $N(x) = D(x) \cdot 0 + N(x)$ e quindi l'enunciato risulta verificato da $Q(x) = 0$ e $R(x) = N(x)$.
Per i casi in cui $deg(N(x)) \geq deg(D(x))$ si effettua la dimostrazione per induzione sulla differenza dei gradi $deg(N(x)) - deg(D(x))$.
Se $deg(N(x)) = deg(D(x))$
. . . .
∎

I polinomi $Q$ e $R$ si dicono, risp., quoziente e resto della divisione di $N(x)$ per $D(x)$.
Se $R(x) = 0$ si dice che $N(x)$ è divisibile per $D(x)$, o equivalentemente che $D(x)$ divide $N(x)$ o che $D(x)$ è divisore di $N(x)$in $\mathbb{F}[x]$; in tale caso si scrive $D(x) \nmid N(x)$.

Si osserva che due polinomi proporzionali sono divisori l'uno dell'altro.

Si nota anche che la dimostrazione precedente fornisce anche una procedura per calcolare effettivamente il quoziente e il resto della divisione.

Applicheremo tale procedura per determinare il MCDtra due polinomi mediante l'algoritmo di Euclide delle divisioni successive . . . . . .

B33e.12 **Eserc.** Verificare le divisioni con resto dei seguenti polinomi:
$F(x) = x^5 - 3x^3 + 5x + 4$ , $G(x) = x^3 + 1$ , $Q(x) = x^2 - 3$ , $R(x) = -x^2 + 5x + 7$ ;
$F(x) = x^3 + 1$ , $G(x) = x + 1$ , $Q(x) = x^2 - x + 1$ , $R(x) = 0$ ;
$F(x) = 3x^4 + 4x^3 - 5x^2 - 6$ , $G(x) = 2x^2 + 1$ , $Q(x) = 3x^2/2 + 2x - 13/4$ , $R(x) = -2x - 11/4$ .

B33e.13 **Teorema** Consideriamo $F(x), G(x) \in \mathbb{F}[x]$. Un polinomio $D(x) \in \mathbb{F}[x]$ è un MCDtra $F(x)$ e $G(x)$ sse $D(x) \nmid F(x)$, $D(x) \nmid G(x)$ e $\forall Q(x) \in \mathbb{F}[x]$ : $Q(x) \nmid F(x) \wedge Q(x) \nmid G(x) \implies Q(x) \nmid D(x)$

Contrariamente a quanto accade ai numeri interi, due polinomi hanno più di un MCD: per esempio $x^2-1$ e $6x^2-12x+6$ hanno come MCDin $\mathbb{Q}[x]$ il polinomio $x-1$ e tutti gli altri polinomi proporzionali a esso della forma $qx-q$ con $q \in \mathbb{Q}_{nz}$, polinomi i quali sono divisori l'uno dell'altro.

L'algoritmo di Euclide, delle divisioni successive, che ci garantisce l'esistenza del MCDtra interi, si può estendere anche ai polinomi, per cui l'ultimo resto nonnullo, nelle divisioni successive, tra due polinomi non entrambi nulli è un loro MCD.
Per convenzione si assume che il MCDdi due polinomi sia il divisore di entrambi di grado massimo e monico.

Vale l'**identità di Bézout**: Se $D(x) = \mathrm{MCD}(F(x), G(x))$ allora esistono in $\mathbb{F}[x]$ $H(x)$ ed $L(x)$ tali che $D(x) = F(x) \cdot H(x) + G(x) \cdot L(x)$.
Se $L(x) = \mathrm{MCD}(F(x), G(x))$ allora $F(x)$ e $G(x)$ sono detti **polinomi coprimi**.

## B33 f. radici di un polinomio di una variabile razionale

**B33f.01** Per molti polinomi di $\mathbb{Q}[x]$ si osservano cambiamenti di segno dei valori che assume la funzione polinomiale in relazione a valori diversi assunti dalla variabile $x$. Questo porta a ricercare valori della variabile per i quali la funzione polinomiale assume il valore zero.

Sia $P(x) = \sum_{i=0}^{n} a_i\, x^i \in \mathbb{F}[x]$ ; un elemento $\alpha \in \mathbb{F}$ si dice **radice del polinomio** o **zero del polinomio** $P(x)$ sse la corrispondente funzione polinomiale calcolata in corrispondenza di $\alpha$ vale 0, ovvero sse si ha $P(\alpha) = \sum_{i=0}^{n} a_i\, \alpha^i = 0$ .

Si dice **equazione polinomiale associata a un polinomio** $\sum_{i=0}^{n} a_i\, x^i$ l'equazione $\sum_{i=0}^{n} a_i\, x^i = 0$ .

Si dice anche che l'elemento $\alpha$ del campo è radice del polinomio $P(x)$ sse sostituendo alla indeterminata $x$ il valore $\alpha$ nell'equazione associata questa risulta essere una **equazione soddisfatta**.

Per il polinomio nullo, dato che tutti i suoi coefficienti sono nulli, si ha che ogni $\alpha \in \mathbb{F}$ è una sua radice.

Ogni polinomio di grado 0, cioè ogni polinomio costante e nonnullo, non possiede alcuna radice. Ogni polinomio di primo grado $a_1\, x + a_0$ ammette una e una sola radice, $-\dfrac{a_0}{a_1}$.

La ricerca delle radici dei polinomi è di grande importanza, in quanto a essa si riconducono le soluzioni di una grande varietà di problemi.

L'esito di una tale ricerca per molte equazioni dipende dal campo nell'ambito del quale viene posto il problema. Per esempio il polinomio $x^2 - 2 = 0$ non ammette alcuna radice quando viene considerato un polinomio sul campo dei razionali, mentre nel campo dei numeri reali ammette le due radici $\pm\sqrt{2}$.

A sua volta il polinomio $x^2 + 1$ nel campo dei reali non ammette alcuna radice, mentre nel campo dei numeri complessi ammette le due radici $\pm$i.
In genere la ricerca delle radici di un polinomio costituisce un problema non facile ed esso può essere affrontato con procedimenti diversi, da quelli algebrici a quelli numerici approssimati.

**B33f.02** Un numero $\alpha \in \mathbb{F}$ è radice del polinomio $P(x) \in \mathbb{F}[x]$ sse $P(x)$ è divisibile per il polinomio $x - \alpha$.
**Dim.**:

**B33f.03** I polinomi di grado dispari hanno almeno una radice reale.

Per il polinomio $\sum_{i=0}^{n} a_i\, x^i$ con $n > 0$ se $a_0 = 0$, allora $0 \in \mathbb{F}$ è suo zero.

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

$(x + 1)x(x - 1) = x^3 - x$.

Trovare in $\mathbb{R}[x]$ tutti gli zeri del polinomio $P(x) = x^3 - 2x^2 - 4x + 5$ sapendo che uno di essi è il numero 1.

$x_1 = 1$; $x_2 = -2$; $x_3 = 3$;

Dividere il polinomio $P(x) = x^n - 1$ per il polinomio $x - 1$.

$P(1) = 0$ quindi $P(x)$ è divisibile per $x - 1$ e il loro quoziente è $Q(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$.

Decidere se il polinomio $P(x) = x^n + 1$ è divisibile per il polinomio $x + 1$ ed eseguire la divisione con il resto.

Svolgimento: $P(-1) = 0$ sse $n$ è dispari, quindi $P(x)$ è divisibile per $x + 1$ quando $n$ è dispari e in questo caso $R(x) = 0$ e $Q(x) = x^{n-1} - x^{n-2} + x^{n-3} - \cdots + (-1)^n x + (-1)^{n-1}$.

**B33f.04** **Teorema** Se $P(x) \in \mathbb{F}[x]$, un elemento $a$ del campo $\mathbb{F}$ si dice che è una radice o uno zero di $P(x)$ sse risulta $P(a) = 0$.

Per il polinomio nullo, poiché tutti i coefficienti sono nulli, si ha che ogni $a \in K$ è una sua radice. Ogni polinomio di grado 0 non possiede radici.
Trovare in $\mathbb{R}[x]$ tutti gli zeri del polinomio $P(x) = x^3 - 2x^2 - 4x + 5$ sapendo che uno di essi è 1.
$x_1 = 1$; $x_2 = -2$; $x_3 = 3$;

Dividere il polinomio $P(x) = x^n - 1$ per il polinomio $x - 1$.

$P(1) = 0$ quindi $P(x)$ è divisibile per $x - 1$ e per il loro quoziente si ha $\dfrac{x^n - 1}{x - 1} = Q(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$ .

Decidere se il polinomio $P(x) = x^n + 1$ è divisibile per il polinomio $x + 1$ ed eseguire la divisione per opttenere quoziente e resto.
Svolgimento: $P(-1) = 0$ se e solo se $n$ è dispari, quindi $P(x)$ è divisibile per $x + 1$ quando $n$ è dispari e in questo caso $R(x) = 0$ e $Q(x) = x^{n-1} - x^{n-2} + x^{n-3} - \cdots + (-1)^n x + (-1)^{n-1}$.

## B33 g. funzioni sui razionali [1]

**B33g.01** Prima di procedere nell'esame delle funzioni polinomiali, si rende necessario introdurre varie nozioni riguardanti i sottoinsiemi di $\mathbb{Q}$ e le funzioni del genere $\lceil\, \mathbb{Q} \longrightarrow \mathbb{Q} \,\rceil$.

Le prime caratterizzazioni che conviene introdurre per queste funzioni sono collegate al fatto che esse pongono in corrispondenza due insiemi, dominio e codominio, totalmente ordinati.

Consideriamo una generica funzione $f \in \lceil\, \mathbb{Q} \longrightarrow \mathbb{Q} \,\rceil$ e denotiamo con $D$ il suo dominio e con $C$ il suo codominio:

$$D := \mathsf{dom}(f)\ ,\quad C := \mathsf{cod}(f)\ ,\quad f \in \lceil\, D \longmapsto C \,\rceil\ .$$

Se in particolare $f$ è una funzione polinomiale $D = \mathbb{Q}$.
Denotiamo inoltre con $I$ un intervallo razionale interamente contenuto in $D$.

La $f$ si dice **funzione crescente** in $I$ sse $\forall x_1, x_2 \in I\ :\ x_1 < x_2 \Longrightarrow f(x_1) < f(x_2)$.

La $f$ si dice **funzione decrescente** in $I$ sse $\forall x_1, x_2 \in I\ :\ x_1 < x_2 \Longrightarrow f(x_1) > f(x_2)$.

La $f$ si dice **funzione nondecrescente** in $I$ sse $\forall x_1, x_2 \in I\ :\ x_1 < x_2 \Longrightarrow f(x_1) \leq f(x_2)$.

La $f$ si dice **funzione noncrescente** in $I$ sse $\forall x_1, x_2 \in I\ :\ x_1 < x_2 \Longrightarrow f(x_1) \geq f(x_2)$.

La $f$ si dice **funzione monotona in senso stretto** in $I$ sse essa in $I$ è crescente oppure decrescente.

La $f$ si dice **funzione monotona [in senso lato]** in $I$ sse essa in $I$ è noncrescente oppure nondecrescente.

Evidentemente ogni funzione crescente è nondecrescente, ogni funzione decrescente è noncrescente e ogni funzione monotona in senso stretto è monotona in senso lato.
Inoltre l'insieme delle funzioni costanti è l'intersezione dell'insieme delle funzioni nondecrescenti con l'insieme delle funzioni noncrescenti.

**B33g.02** Un altro genere di caratterizzazioni delle funzioni del genere $\{\mathbb{Q} \longrightarrow \mathbb{Q} \,\rceil$ riguarda le proprietà di simmetria.

Un sottoinsieme di $\mathbb{Q}$ si dice **sottoinsieme pari di** $\mathbb{Q} \times \mathbb{Q}$ sse è invariante rispetto al cambiamento di segno, cioè sse è simmetrico rispetto al numero 0. Sono sottoinsiemi pari gli intervalli chiusi della forma $\mathbf{[}-q, q\mathbf{]}$ e gli intervalli aperti della forma $\mathbf{(}-q, q\mathbf{)}$.

Una $f \in \{\mathbb{Q} \longrightarrow \mathbb{Q} \,\rceil$ si dice **funzione pari** sse il suo dominio è un sottoinsieme pari di $\mathbb{Q}$ e $\forall q \in \mathsf{dom}(f)\ :\ f(-q) = f(q)$.

Una $f \in \{\mathbb{Q} \longrightarrow \mathbb{Q} \,\rceil$ si dice **funzione dispari** sse il suo dominio è un sottoinsieme pari di $\mathbb{Q}$ e $\forall q \in \mathsf{dom}(f)\ :\ f(-q) = -f(q)$.

Le funzioni polinomiali pari sono quelle fornite da somme di monomi di ordine pari.
Le funzioni polinomiali dispari sono quelle fornite da somme di monomi di ordine dispari.

Evidentemente il prodotto di due funzioni pari e il prodotto di due funzioni dispari sono funzioni pari. All'opposto il prodotto di una funzione pari per una funzione dispari costituisce una funzione dispari.

**B33g.03** Si dice **sottoinsieme superiormente limitato di** $\mathbb{Q}$ ogni $S \subset \mathbb{Q}\}$ tale che esiste un elemento $M$ di $\mathbb{Q}$ tale che per ogni elemento $a \in S$ sia $a < M$.

Si dice **sottoinsieme inferiormente limitato di** $\mathbb{Q}$ ogni $S \subset \mathbb{Q}\}$ tale che esiste un elemento $m$ di $\mathbb{Q}$ per il quale per ogni elemento $a \in S$ sia $m < a$.

Si dice **sottoinsieme limitato di** $\mathbb{Q}$ ogni $S \subset \mathbb{Q}\}$ che risulta sia inferiormente che superiormente limitato.

**B33g.04** Una funzione $f \in \{\mathbb{Q} \longrightarrow \mathbb{Q}\rceil$ si dice **funzione superiormente limitata** sse il suo codominio è superiormente limitato.

Una funzione $f \in \{\mathbb{Q} \longrightarrow \mathbb{Q}\rceil$ si dice **funzione inferiormente limitata** sse il suo codominio è inferiormente limitato.

Una funzione $f \in \{\mathbb{Q} \longrightarrow \mathbb{Q}\rceil$ si dice **funzione limitata** sse il suo codominio è limitato, cioè sse essa è sia superiormente che inferiormente limitata.

L'esposizione in https://www.mi.imati.cnr.it/alberto/ e https://arm.mi.imati.cnr.it/Matexp/matexp_main.php