Capitolo G21:
Polinomi

G21:0.01 Questo capitolo è dedicato alla introduzione della nozione di polinomio su un campo. I polinomi sono entità matematiche che risultano utili per un gran numero di sviluppi formali e nella risoluzione effettiva di molti problemi e che si possono manipolare abbastanza facilmente. Tuttavia per definire i polinomi in modo versatile e in modo formalmente soddisfacente, si rende necessario un discorso un poco elaborato.
Vanno considerati gli insiemi di polinomi collegati ad un campo ben determinato. Se si procede su un piano costruttivo si possono utilizzare pienamente solo il campo dei razionali $\mathbb{Q}_{fld}$ ed alcune sue estensioni costruttive (campi algebrici, campo dei reali costruibili). Per presentare le proprietà e la portata dei polinomi, tuttavia, conviene introdurre queste entità in relazione a un campo qualsiasi, cioè in relazione ad un insieme di entità che possono essere composte mediante certe operazioni, chiedendo solo che elementi ed operazioni del campo godano di determinate proprietà formali.

G21:A.. I polinomi e le operazioni di somma e prodotto

G21:A.01 Ricordiamo che in algebra per campo si intende un insieme munito delle operazioni di addizione, sottrazione, moltiplicazione e divisione, chiaramente definite nel caso dei numeri razionali e in generale caratterizzate dal fatto di godere 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, elemento neutro per la somma, e un numero uno, elemento neutro per il prodotto.
Le entità costituenti un campo, potendo essere sottoposte alle accennate operazioni, possono essere chiamate **entità numeriche** o **numeri** *tout court*.
In seguito si introdurranno campi costruibili che ampliano $\mathbb{Q}_{fld}$ definendo i meccanismi che consentono di individuare i loro numeri e di eseguire le relative operazioni. Si introduce invece il campo dei numeri reali con una definizione assiomatica e facendo riferimento all'intuizione per associarlo alla retta reale. Si introduce in seguito il campo dei numeri complessi per ampliare il campo reale in relazione ad una esigenza computazionale molto forte, la piena risolubilità delle equazioni polinomiali. Si possono inoltre definire altri campi di rilevante utilità in ambito discreto, in particolare i campi di classi di resti.
La possibilità di fare riferimento alla nozione generale e astratta di campo, prescindendo dai processi che conducono ad un campo specifico presenta rilevanti vantaggi, in quanto consente di definire costruzioni di tipo generale, prescindendo dalle elaborazioni effettive necessarie alla loro concretizzazione, e questo consente di trattare in modo unificato una vasta gamma di risultati strutturali e di metodi computazionali, realizzando notevoli economie di pensiero e di organizzazione delle conoscenze.

G21:A.02 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 fra polinomi godono di proprietà molto simili a quelle delle operazioni omologhe sul campo; la divisione fra 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 più elaborati di quelli richiesti dalle operazioni su un campo.

G21:A.03 Definiamo come **polinomio in una variabile su un campo** $\mathbb{F}$ ogni sequenza finita di elementi di $\mathbb{F}$ che cominciamo con lo scrivere nella forma neutra $P = \langle a_0, a_1, ..., a_n \rangle$ e per la quale chiediamo che se $n \geq 1$ sia $a_n \neq 0$.
Le componenti della sequenza si dicono **coefficienti** del polinomio; talora 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 $a_0 = 0$, unità di $\mathbb{F}$, si dice **polinomio nullo** ed il polinomio con $n = 0$ e $a_0 = 1$, unità del campo, viene chiamato **polinomio unità**.
Si dice **grado del polinomio** $P = \langle a_0, a_1, ..., a_n \rangle$ l'intero n se esso è positivo oppure se $n = 0$ ed $a_0 \neq 0$; inoltre al polinomio nullo si attribuisce 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 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 $\{\mathbb{F} \longmapsto \mathbb{F}\}$ che vengono loro associate.

G21:A.04 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 useremo 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

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

Ad esempio il polinomio $P = \langle 2, -1.5, -1, 1.25 \rangle$ è individuato dalla espressione canonica
$P(x) = 2x^0 - \frac{3}{2}x - x^2 + \frac{5}{4}x^3$
Questa scrittura fornisce le stesse informazioni della sequenza da cui siamo partiti e, come vedremo, consente di controllare più agevolmente varie elabborazioni sui polinomi; si tende quindi con identificarla con il polinomio stesso.
Una espressione canonica si può interpretare come una espressione da calcolare facendo agire su elementi di $\mathbb{F}$ le operazioni del campo $\mathbb{F}$; 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 processo 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 $\{\mathbb{F} \longmapsto \mathbb{F}\}$ che chiamiamo **funzione associata al polinomio**. Complessivamente le funzioni associate ai polinomi su un campo sono dette **funzioni polinomiali**.

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.

G21:A.05 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 indicati essplicitamente o 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 $\{\mathbb{F} \longmapsto \mathbb{F}\}$.
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.

G21:A.06 Il problema della struttura e dell'equivalenza fra espressioni polinomiali in generale non è semplice. 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 approfondire questioni relative ai linguaggi generati da [[grammatiche formali]] e alle tecniche della [[manipolazione simbolica]]).
Preliminarmente osserviamo che il segno di sommatoria consente una scrittura concisa di un'espressione canonica:

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

Alcune semplici varianti equivalenti di un'espressione canonica sono delle sue evidenti semplificazioni. Un termine a_0x^0 si semplifica in a_0, un termine a_1x^1 si può sostituire con a_1x, ogni termine $1x^i$ con x^i e ogni sottoespressione $+0x^j$ si può trascurare *sic et simpliciter*. Si hanno quindi equivalenze le seguenti, che per semplicità presentiamo 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 ad equivalenze poco chiare a prima vista. Ad esempio il polinomio $P = \langle 2, -1.5, 0, 1.25\rangle$, oltre ad essere individuato dalla espressione canonica

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

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 il cui coefficiente è 0 (che non influisce sul calcolo) e da altre espressioni equivalenti come $\frac{5}{4}x^3 - \frac{3}{2}x + 2$ e $\frac{x}{4}(x^2 - 6) + 2$.

G21:A.07 L'insieme dei polinomi sul campo $\mathbb{F}$ identificati mediante loro espressioni polinomiali nella indeterminata x si denota tradizionalmente con la scrittura $\mathbb{F}\mathbf{[}x\mathbf{]}$.

$\mathbb{F}[x]$ viene munito 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 $\cdot$. Le definizioni si servono delle espressioni canoniche dei polinomi usate 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** dei polinomi P e Q il polinomio $P+Q$ dato dalla espressione semicanonica $(P+Q)(x) = \sum_{i=0}^{g}(a_i + b_i)$ 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

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

Ad esempio la somma dei polinomi $P(x) = 4x^3+12x-4$ e $Q(x) = x^2+3x-1$ di grado rispettivamente 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.

G21:A.08 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.
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 $4x^5 - 3x_2^3 x$, $-3x^3 + 2x + 4x^5$ e tutte le altre 3 espressioni nelle quali i tre termini sono permutati diversamente.
Altre equivalenze delle espressioni polinomiali provengono dalla associatività della somma: ad esempio sono espressioni equivalenti alle precedenti $x - 3x^3 + 6x^5 + x - 2x^5$ e $(2x + 2x^3 + 2x^5) + (2x^5 - 5x^3)$.

G21:A.09 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 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 fra due polinomi P e Q la somma di P e l'opposto di Q: $P - Q := P + (-Q)$. Ad esempio se $P(x) = 3 - x + x^3$ e $Q(x) = 2x + x^2 + x^3$ si ha $P(x) - Q(x) = 3 - 2x - x^2$.
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, rispettivamente, 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 relazioni come $\mathbb{F}_{\leq n}[x] = \mathbb{F}_{<n}[x] \dot\cup \mathbb{F}_n[x]$ $\mathbb{F}_{\leq n}[x] = \mathbb{F}_{<n+1}[x]$ e $\mathbb{F}[x] = \mathbb{F}_{<n}[x] \dot\cup \mathbb{F}_{\geq n}[x]$.
Dalle considerazioni precedenti segue che la quaterna $\langle \mathbb{F}_{<n}[x], +, -, 0\rangle$ è un gruppo abeliano e che per ogni naturale n la quaterna $\langle \mathbb{F}_{<n}[x], +, -, 0\rangle$ è un suo sottogruppo proprio.

G21:A.10 Definiamo come **prodotto** dei polinomi $P(x) = \sum_{i=0}^{n} a_i x^i$ e $Q(x) = \sum_{j=0}^{m} b_i x^i$ diversi dal polinomio nullo il polinomio denotato con $P \cdot Q$ individuato dalla espressione $(P \cdot Q)(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} \left(a_i b_j x^{i+j}\right)$.
Ad esempio $(x^3 + 2x - 4) \cdot (-x^2 + 2x - 3) = -x^5 + 2x^4 - 5x^3 + 12x^2 - 14x + 12$
Per il grado del polinomio prodotto di due polinomi non nulli quindi

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

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

L'operazione di prodotto di due polinomi va chiarita. Per questo può essere utile organizzare il suo calcolo con una matrice 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

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

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

G21:A.11 Si dimostra che il prodotto di due polinomi è un'operazione binaria commutativa: 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 prodotto riguardano le stesse sequenze di addendi.

Si dimostra anche che il prodotto di polinomi è un'operazione associativa e distributiva rispetto alla somma. Per questo consideriamo anche il polinomio $R(x) = \sum_{l=0}^{r} c_q x^q$ e supponiano che sia $c_l = 0$ per $l > r$.
Per la associatività si trova che sia $(P(x)Q(x))R(x)$ che $P(x)(Q(x)R(x))$ portano all'espressione

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

Per la distributività si constata che

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

e si osserva che questa e la commutatività comportano

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

Da queste proprietà seguono altre equivalenze fra le espressioni polinomiali: ad esempio sono equivalenti le espressioni presentate con le uguaglianze seguenti:

$$(x^3-2x+4)(x^2-5x+2) \qquad (2-5x+x^2)(4-2x+x^3) \qquad 8+16x-6x^2+5x^4+x^5$$

$$[(x^2-6)(2x^2-4x+2)](x^3-5x) = (2x^4-4x^3-11x^2+24x-12)(x^3-5x)$$
$$= 2x^-4x^6-21x^5+4x^4-43x^3-120x^2+60x =$$
$$(x^2-6)[2x^5-4x^4-8x^3+20x^2-10x] = (x^2-6)[(2x^2-4x+2)(x^3-5x)]$$

$$[(x^2+3x-1)+(3x^2-4)](x^3-2x^2) = (x^5+x^4-7x^3+2x^2)+(3x^5-6x^4-4x^3+8x^2)$$
$$= 4x^5-5x^4-11x^3+10x^2 = (4x^2+3x-5)(x^3-2x^2)$$

G21:A.12 Due polinomi si dicono **proporzionali** se uno si ottiene dall'altro moltiplicandolo per un elemento di $\mathbb{F}$ diverso da zero, cioè per un polinomio costante non nullo. Ad 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 fra polinomi è evidentemente una equivalenza. Una classe di equivalenza è costituita dal solo polinomio nullo; le altre classi di equivalenza di polinomi si dicono anche **raggi di polinomi**; una seconda classe è costituita da tutti i polinomi di grado 0, cioè si identifica con $\mathbb{F}_{nz}$.
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 contenuta in un insieme di polinomi di un dato grado 1, 2, 3, ...
In ogni classe di proporzionalità di polinomi c'è 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. Ad 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 sono chiamati **monomi monici**, naturalmente.

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 (0 -1). Dei polinomi si possono quindi considerare le combinazioni lineari: 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 gli elementi del campo c_j.

G21:A.13 Spesso accade di individuare un polinomio come espressione costruita con combinazioni lineari e prodotti di altri polinomi. Queste espressioni possono essere sviluppate servendosi delle proprietà delle operazioni binarie fino ad arrivare ad 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 di forma particolare. 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, ovvero sse presentano la stessa espressione canonica. 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.

Alcune uguaglianze fra polinomi equivalenti sono ampiamente utilizzate in molti sviluppi della matematica e in varie dlle 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.

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

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

$x^2 - a^2 = (x-a)(x+a)$ $\quad$ $x^3 - a^3 = (x-a)(x^2+ax+a^2)$ $\quad$ $x^4 - a^4 = (x-a)(x^3+ax2+a^2x+a^3)$

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

G21:A.14 Le definizioni delle operazioni di somma, sottrazione e prodotto di due polinomi sono motivate dal il 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 polinimio 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 alcune 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 $x = 0$.
Le proprietà dei polinomi generici si possono ricondurre a quelle dei corrispondenti polinomi monici. Si osserva inoltre che per elevati valori della $|x|$ prevale il termine relativo alla massima potenza e nel caso dei polinomi monici sono utili le considerazioni precedenti sopra x^{2k} e x^{2k+1}.
Il comportamento per valori generici della variabile non si può descrivere in modo altrettanto semplice e richiede considerazioni specifiche spesso non semplici che possono richiedere sia il ricorso a considerazioni algebriche non semplici, sia l'utilizzo di strumenti di calcolo numerico e di calcolo automatico.

G21:A.15 I polinomi hanno numerose applicazioni e vengono ampiamenmte manipolati con strumenti software, in particolare nell'ambito dei maggiori sistemi per il calcolo numerico-simbolico-grafico come [[Maple]], [[Mathematica]] e [[Matlab]] (v.a. [[CAS]], Computer Algebra Systems).
Per tutti questi strumenti e sistemi software sono stati sviluppati metodi di calcolo effettivo ed algoritmi riguardanti le elaborazioni su polinomi altamente sofisticati.

G21:A.16 Ha interesse considerare complessivamente la successione dei polinomi $\langle n \in \mathbb{N} :| x^n \rangle$ che presentano i gradi uguali ai rispettivi indici.
Si incontrano varie altre utili successioni di polinomi 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 $x(x+1)\cdots(x+n-1)$.

G21:A.17 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 $a_0 = 1$. 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]].
Si verifica che l'anello $\mathbb{F}[x]$ è un dominio di integrità (cioè privo di divisori dello zero).
L'insieme dei polinomi sopra il campo $\mathbb{F}$ si può considerare uno spazio vettoriale su $\mathbb{F}$ (v. G40:). Tutti i polinomi di grado inferiore ad 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

(quali teoremi della divisione, MCD, fattorizzazione,...) si possono riesprimere in forme analoghe per i polinomi.

G21:B.. La divisione tra polinomi

G21:B.01 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 ed 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 $deg(Q(x)) = deg(N(x)) - deg(D(x))$.

Dim.: I polinomi $Q(x)$ e $R(x)$ si chiamano, rispettivamente, **quoziente** e **resto** della divisione $\dfrac{N(x)}{D(x)}$ fra **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 $Q(x) = 0$ e $R(x) = N(x)$.
Per i casi in cui $deg(N(x)) \geq deg(D(x))$ serviamoci delle espressioni $N(x) = \sum_{i=0}^{n} a_i x^i$ e $D(x) = \sum_{i=0}^{m} b_i x^i$ con $0 \leq m = deg(D(x)) \leq n = deg(N(x))$. e procediamo per induzione sulla differenza dei gradi fra 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 richiesto 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 $D(x)(Q(x) - Qol(x)) = \overline{R}(x) - R(x)$; dato che $deg(\overline{R}(x) - R(x)) < deg(D(x))$, questa uguaglianza è accettabile solo se $Q(x) - Qol(x) = 0$ e $\overline{R}(x) - R(x)$ ∎

G21:B.02 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 $Q_i(x)$.

G21:B.03 Esercizio Verificare che le seguenti quaterne di polinomi soddisfano l'uguaglianza $N(x) = D(x)Q(x) + R(x)$:
$N(x) = x^5 - 3x^3 + 5x + 4 \quad , \quad D(x) = x^3 + 1 \quad , \quad Q(x) = x^2 - 3 \quad , \quad R(x) = -x^2 + 5x + 7$
$N(x) = x^3 + 1 \quad , \quad D(x) = x + 1 \quad , \quad Q(x) = x^2 - x + 1 \quad , \quad R(x) = 0$
$N(x) = 3x^4 + 4x^3 - 5x^2 - 6 \quad , \quad D(x) = 2x^2 + 1 \quad , \quad Q(x) = 3x^2/2 + 2x - 13/4 \quad , \quad R(x) = -2x - 11/4$

G21:B.04 Se $R(x) = 0$ si ha $N(x) \in \mathbb{F}[x] \cdot D(x)$ e si dice che $N(x)$ è **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 $D(x) \nmid N(x)$.
Ad 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 sé stesso e per ogni polinomio di grado 0, cioè per ogni polinomio costante. Si dicono **divisori banali** del 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.
Un polinomio $P(x) \in \mathbb{F}_{\geq 1}(x)$ si dice **irriducibile** sse è privo di divisori non banali.
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 deteminazione 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.

G21:B.05 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 $D(x) \nmid F(x)$, $D(x) \nmid G(x)$ e per ogni polinomio $Q(x)$ tale che $Q(x) \nmid F(x)$ e $Q(x) \nmid G(x)$ si ha $Q(x) \nmid D(x)$.

Contrariamente a quanto accade ai numeri interi, due polinomi hanno più di un massimo comun divisore: ad esempio $4x^2 - 1$ e $6x^2 - x - 5$ hanno come massimo comun divisore in $\mathbb{Q}$ il polinomio $2x - 1$ e tutti gli altri polinomi proporzionali ad esso della forma $qx - q$ con $q \in \mathbb{Q}_{nz}$, polinomi ciascuno dei quali è divisore di tutti gli altri.
Risulta opportuno definire la funzione MCD che a due polinomi associa l'unico polinomio monico che sia divisore di entrambi e che abbia il grado massimo.
Ad esempio $MCD(4x^2 - 1, 6x^2 - 12x + 6) = x - \dfrac{1}{2}$.

Due polinomi privi di divisori non banali comuni si dicono **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 non banali comuni. Se si vuole l'unico massimo comun divisore monico, cioè il polinomio fornito da MCM basta limitarsi ai divisori non banali monici.

G21:B.06 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 (non nulli) 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 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 non nullo 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.

G21:B.07 Teorema Vale l'**identità di Bézout**: Se $D(x) = MCD(F(x), G(x))$ allora in $\mathbb{F}[x]$ si trovano $H(x)$ ed $L(x)$ tali che $D(x) = F(x) \cdot H(x) + G(x) \cdot L(x)$.

G21:C.. Radici di un polinomio

G21:C.01 Sia $P(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$; un elemento $\alpha \in \mathbb{F}$ si dice che è una **radice** o uno **zero** del polinomio $P(x)$ sse la corrispondente funzione polinomiale calcolata in corrispondenza di α vale 0, ovvero sse si ha $P(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0$.
Si dice **equazione polinomiale** associata al 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 α del campo è radice del polinomio $P(x)$ sse sostituendo alla indeterminata x il valore α nell'equazione associata questa risulta **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 non nullo, 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 ad 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. Ad 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 $x^2 + 1$ sul 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 queli algebrici a quelli numerici aapprossimati.

G21:C.02 Teorema di Ruffini 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.:

G21:C.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: $P(-1) = 0$ 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 $Q(x) = x^{n-1} - x^{n-2} + x^{n-3} - \cdots + (-1)^n x + (-1)^{n-1}$.