L’anello dei polinomi

Sia R un anello commutativo con identità. È possibile costruire un anello commutativo unitario, che si denota con R[x], che contiene R (come sottoanello) e un elemento x non appartenente ad R, i cui elementi risultano essere espressioni del tipo:
$f = a_0+a_1x+\ldots+a_nx^n$, dove $n\in\mathbb{N}$ e $a_0,a_1,...a_n\in R$,
ed inoltre, posto $a_i = 0$, per ogni $i > n$, gli elementi a_0, a_1, $...a_n$, a_{n+1}, … risultano essere univocamente determinati. Tale anello **R[x]** è detto **anello dei polinomi nella indeterminata x a coefficienti in R**, ciascun suo elemento $f = a_0+a_1x+\ldots+a_nx^n$ viene detto *polinomio*, e gli elementi a_i ($i\in\mathbb{N}$) si dicono i *coefficienti* di f.
Dati dei polinomi $f = a_0+a_1x+\ldots+a_nx^n$ e $g = b_0+b_1x+\ldots+b_mx^m$, risulta dunque f = g se, e solo se, $a_i = b_i$ per ogni $i\in\mathbb{N}$; si noti inoltre che è possibile, quando opportuno, supporre n = m, in quanto è sufficiente aggiungere eventualmente ulteriori termini a coefficiente nullo.

Applicando le note proprietà delle operazioni in un anello commutativo (associatività, commutatività, ditributività e le regole del prodotto tra potenze), e raccogliendo i coefficienti relativi ai termini in cui compare la stessa potenza di x, si ha che le operazioni di somma e prodotto in R[x] possono essere così descritte. Siano $f = a_0+a_1x+\ldots+a_nx^n$ e $g = b_0+b_1x+\ldots+b_mx^m$ e sia n maggiore o uguale ad m. Per calcolare la somma tra f e g si può supporre che sia n = m, aggiungendo eventualmente coefficienti $b_j = 0$ (per ogni j compreso tra m + 1 ed n). Allora

$$f + g =(a_0+a_1x+\ldots+a_nx^n)+(b_0+b_1x+\ldots+b_nx^n) = (a_0+b_0)+(a_1+b_1)x+\ldots+(a_n+b_n)x^n$$

Il prodotto tra f e g si ottiene nel modo che segue:

$$fg = (a_0+a_1x+\ldots+a_nx^n)(b_0+b_1x+\ldots+b_mx^m) = c_0 + c_1x + \ldots +c_{m+n}x^{n+m},$$

dove $c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2}+ \ldots a_{i-1}b_i + a_ib_0$, per ogni i che varia da 0 ad m + n.
Gli elementi di R, che sono detti *polinomi costanti*, sono i polinomi che hanno i coefficienti $a_i = 0$ per ogni $i > 0$. Lo zero di R[x] è il polinomio costante 0_R; l’identità è il polinomio costante 1_R.

Grado di un polinomio. Sia $f = a_0+a_1x+\ldots+a_tx^t$ un polinomio non nullo di R[x]. Se n è il massimo dell'insieme (non vuoto e finito) $\{m \in \mathbb{N}: a_m \neq 0\}$, n è detto *grado di f* (in simboli: $n = \delta(f)$) ed è possibile scrivere :

$$f = a_0+a_1x+\ldots+a_nx^n \quad (a_n \neq 0).$$

a_n è detto il *coefficiente direttivo* (o *parametro direttore*) di f; se $a_n = 1$ il polinomio f si dice *monico.* Al polinomio nullo si attribuisce per definizione grado uguale a $-\infty$ (meno infinito); le costanti non nulle sono tutti e soli i polinomi di grado 0.

Prop.1 *Siano R un anello commutativo unitario,* $f = a_0+a_1x+\ldots+a_nx^n$ *e* $g = a_0+a_1x+\ldots+a_mx^m$ *polinomi di R[x]. Allora:*

i) $\delta(f+g) \leq max\{\delta(f),\delta(g)\}$;

ιι) $\delta(fg) \leq \delta(f)+\delta(g)$;

iii) se R è un dominio di integrità, allora $\delta(fg) = \delta(f)+\delta(g)$ *(regola di addizione dei gradi).*

N.B. In questo enunciato si intendono adottate le ovvie convenzioni: $(-\infty)+(-\infty) = -\infty$; $(-\infty)+n = -\infty$; $-\infty < n$, per ogni $n \in \mathbb{N}$.

Dim. L'enunciato è banalmente vero se f o g sono nulli. Si può allora supporre $f \neq 0$, $g \neq 0$, ed $n = \delta(f)$, $m = \delta(g)$ (con $n,m \in \mathbb{N}$).

i) Se $n = \max\{n,m\}$, risulta $f+g = (a_0+b_0)+(a_1+b_1)x+\ldots+(a_n+b_n)x^n$, per cui $\delta(f+g) \leq n$.

ii) Da $fg = a_0b_0+(a_0b_1+a_1b_0)x+\ldots+a_nb_mx^{n+m}$ segue che il massimo degli indici dei coefficienti eventualmente non nulli è n+m, relativo al coefficiente a_nb_m ; allora $\delta(fg) \leq n+m$.

iii) Se R è un dominio d'integrità, da $a_n \neq 0$ e $b_m \neq 0$ segue $a_nb_m \neq 0$; pertanto, ragionando come in ii), $\delta(fg) = n+m = \delta(f)+\delta(g)$.

Corollario 2 *Sia R un anello commutativo unitario. R è un dominio d'integrità se, e solo se, R[x] è un dominio d'integrità.*

Dim. Se R[x] è un dominio d'integrità, tale è anche R, che è un sottoanello di R[x]. Viceversa, sia R un dominio d'integrità, e siano f,g polinomi non nulli di R[x], cioè tali che $\delta(f) \geq 0$, $\delta(g) \geq 0$. Allora, per la iii) della prop.1, si ha $\delta(fg) = \delta(f) +\delta(g) \geq 0+0 = 0$, e fg non è nullo.

Corollario 3 *Se R è un dominio d'integrità, gli elementi invertibili di R[x] sono tutti e soli gli elementi invertibili di R; in particolare, se F è un campo, gli elementi invertibili di F[x] sono tutte e sole le costanti non nulle.*

Dim. Se un elemento di R è invertibile, è invertibile in R[x], poiché, come già osservato, l'unità di R e quella di R[x] coincidono. Viceversa, se f è un polinomio invertibile di R[x], esiste un polinomio g tale che fg = 1. Per la regola di addizione dei gradi risulta $\delta(fg) = \delta(f) + \delta(g) = \delta(1) = 0$, dunque $\delta(f) = \delta(g) = 0$, e f e g sono elementi invertibili di R.

Osservazione 4 Si noti che, alla luce del corollario 3, è evidente che, anche nell'ipotesi che R[x] sia un dominio di integrità, **R[x] non è mai un campo**, essendo i suoi elementi invertibili tra i polinomi di grado 0. Più in generale si può dimostrare che, qualunque sia R, il polinomio $x \in R[x]$ non è mai invertibile.

Teorema 5 (Divisione euclidea fra polinomi a coefficienti in un campo) *Sia F un campo, e sia F[x] l'anello dei polinomi nell'indeterminata x a coefficienti in F. Siano $f,g \in F[x]$, con $g \neq 0$. Allora esistono e sono univocamente determinati $q,r \in F[x]$ tali che*

$$f = gq+r;$$
$$\delta(r) < \delta(g).$$

(q ed r sono detti rispettivamente quoziente e resto della divisione di f per g).

Dim. Esistenza: Se f = 0, essendo $0 = 0 \cdot g + 0$, basta porre q = 0, r = 0. Sia allora $f \neq 0$, e si ponga

$$\delta(f) = n,$$
$$\delta(g) = m,$$
$$f = a_0+a_1x+\ldots+a_nx^n,$$
$$g = b_0+b_1x+\ldots+b_mx^m.$$

Si ragionerà per induzione su n, usando la seconda forma del principio di induzione.
Se n = 0, $f = a_0$ è un elemento di F. Se m = 0, anche $g = b_0$ è un elemento invertibile di F, e $a_0 = (a_0b_0^{-1})b_0+0$: basta porre allora $q = a_0b_0^{-1}$, r = 0. Se invece è m > 0, $a_0 = 0 \cdot g + a_0$, e q = 0 ed $r = a_0$ hanno le proprietà richieste.
Supposto dunque n > 0, si supponga l'asserto vero per ogni polinomio $h \neq 0$ di grado $\delta(h) < n$.

Se $n < m$, $f = 0 \cdot g + f$, per cui $q = 0$ ed $r = f$ hanno le proprietà richieste; se $n \geq m$, il polinomio

$$h = f - a_n b_m^{-1} x^{n-m} g = (a_0 + a_1 x + \ldots + a_n x^n) - (a_n b_m^{-1} b_0 x^{n-m} + \ldots a_n b_m^{-1} b_{m-1} x^{n-1} + a_n x^n)$$

è un polinomio di grado $\delta(h) < n$. Per ipotesi di induzione, o se $h = 0$, esistono allora q_1 e r_1 in $F[x]$ tali che

$$h = f - a_n b_m^{-1} x^{n-m} g = q_1 \cdot g + r_1 \text{ , con } \delta(r_1) < \delta(g).$$

Allora

$$f = a_n b_m^{-1} x^{n-m} g + q_1 \cdot g + r_1 = (a_n b_m^{-1} x^{n-m} + q_1) \cdot g + r_1,$$

e basta porre $q = a_n b_m^{-1} x^{n-m} + q_1$ ed $r = r_1$.

Unicità: Si supponga $f = gq + r = gq_1 + r_1$, con $\delta(r) < \delta(g)$, $\delta(r_1) < \delta(g)$; allora $(q - q_1)g = r_1 - r$. Se $q \neq q_1$, $\delta((q - q_1)g) = \delta(r_1 - r) < \delta(g)$; ma è pure $\delta((q - q_1)g) = \delta(q - q_1) + \delta(g) \geq \delta(g)$, e dalla contraddizione segue $q = q_1$, $r = r_1$, come si voleva.

Osservazione 6 La dimostrazione del teorema precedente è di tipo costruttivo, propone cioè un algoritmo che permette di calcolare effettivamente il quoziente e il resto della divisione tra due polinomi. A tal proposito, si faccia riferimento agli esempi a pag.226 del testo consigliato (Facchini, *Algebra e Matematica Discreta*).

Osservazione 7 Se sostituiamo al concetto di grado di un polinomio quello di valore assoluto di numero relativo, risulta chiara l'analogia tra l'algoritmo della divisione euclidea tra polinomi a coefficienti in un campo e quello tra numeri interi che vale in $\mathbb{Z}$, che qui ricordiamo:

Algoritmo della divisione euclidea in $\mathbb{Z}$ *Siano $m,n \in \mathbb{Z}$, $n \neq 0$. Allora esistono e sono univocamente determinati $q,r \in \mathbb{Z}$ (detti rispettivamente quoziente e resto della divisione di m per n) tali che*

$$m = nq + r \text{ con } 0 \leq r < |n|.$$

La validità in F[x] dell'algoritmo della divisione euclidea permette, come si vedrà in seguito, di stabilire ulteriori analogie tra l'anello degli interi e quello dei polinomi a coefficienti in un campo.

Fattorizzazione nell'anello dei polinomi a coefficienti in un campo

Sia F un campo, e siano f, g∈F[x]. Diremo che *f divide g* (o che *f è un divisore di g*, o ancora che *g è un multiplo di f*) se esiste h∈F[x] tale che

$$g = f \cdot h.$$

Se f divide g, useremo la scrittura $f \mid g$. Se $f \neq 0$, f divide g se, e solo se, il resto della divisione di g per f è nullo.
I polinomi invertibili di F[x], ovvero le costanti non nulle a∈F\{0}, sono tutti e soli i divisori di 1; più in generale, se a∈F\{0}, a divide ogni polinomio f∈F[x], potendo scriversi $f = a^{-1}(af)$.

Se f∈F[x]\{0}, si dirà *polinomio associato* ad f ogni polinomio della forma af (con a∈F\{0}). I polinomi associati ad f sono divisori di f, essendo f = $= a^{-1}(af)$; si noti inoltre che polinomi associati hanno lo stesso grado.

Le costanti non nulle e i polinomi associati ad f si dicono *divisori impropri* (o *banali*) di f; tutti gli altri eventuali divisori di f sono detti *propri* (o *non banali*).

Un polinomio f ∈F[x]\{0} si dice *irriducibile* se:
i) $\delta(f) > 0$;
ii) $f = hk \Rightarrow \delta(h)=0, \delta(k)=\delta(f)$ oppure $\delta(k)=0, \delta(h)=\delta(f)$.

La proprietà i) equivale a richiedere che f non sia invertibile; la ii) può essere espressa equivalentemente richiedendo che f non possa scriversi come prodotto di polinomi entrambi di grado strettamente minore di quello di f, o ancora che gli unici divisori di f siano quelli impropri. Ne segue più evidente l'analogia tra i polinomi irriducibili di F[x] e i numeri primi di $\mathbb{Z}$: questi ultimi sono elementi p non nulli non invertibili (ovvero, diversi da +1 e da –1) i cui unici divisori siano +1, -1(gli elementi invertibili), p e –p. p e –p

possono vedersi come gli associati di p, essendo della forma ap, con a elemento invertibile di $\mathbb{Z}$. Alla luce di quanto evidenziato, il teorema che segue, del quale si omette la dimostrazione, può leggersi come analogo del Teorema Fondamentale dell'Aritmetica:

Teorema 8 (Fattorizzazione unica nell'anello dei polinomi a coefficienti in un campo) *Siano F un campo, f un polinomio non nullo e non invertibile di F[x]. Allora f o è irriducibile o è prodotto di fattori irriducibili. Tale fattorizzazione è essenzialmente unica, nel senso che, se* $f = p_1p_2\ldots p_r = q_1q_2\ldots q_s$ *(dove* $p_1,\ldots,p_r,q_1,\ldots,q_s$ *sono polinomi irriducibili), allora r = s e si possono riordinare i fattori in modo che sia* p_i *associato a* q_i*, per ogni i =* $1,\ldots,r$.

Radici di un polinomio. Teorema di Ruffini.

Sia $f = a_0+a_1x+\ldots+a_nx^n$ un polinomio a coefficienti in un campo F. Si dice *applicazione polinomiale* determinata da f l'applicazione:

$$\bar{f} : c \in F \rightarrow f(c) = a_0+a_1c+\ldots+a_nc^n \in F.$$

Si osservi che, se $f,g \in F[x]$, risulta $(f+g)(c) = f(c)+g(c)$, $(fg)(c) = f(c)g(c)$, per ogni $c \in F$.
È opportuno notare che le applicazioni polinomiali determinate dagli elementi di F sono applicazioni costanti, e che polinomi distinti possono determinare la stessa applicazione polinomiale: basta considerare, ad esempio, i polinomi $f = x^3$ e $g = x^3+x^2-x$ a coefficienti in $\mathbb{Z}_2$. Infatti $f(\bar{0}) = \bar{0}^3 = \bar{0}$, $g(\bar{0}) = \bar{0}^3+\bar{0}^2-\bar{0} = \bar{0}$, e quindi $f(\bar{0}) = g(\bar{0}) = \bar{0}$; $f(\bar{1}) = \bar{1}^3 = \bar{1}$, $g(\bar{1}) = \bar{1}^3+\bar{1}^2-\bar{1} = \bar{1}$, e quindi $f(\bar{1}) = g(\bar{1}) = \bar{1}$: ne segue $f(\bar{c}) = g(\bar{c})$, per ogni $\bar{c} \in \mathbb{Z}_2$, e $\bar{f} = \bar{g}$.

Un elemento $c \in F$ si dice una *radice* di f (o una *soluzione dell'equazione f(x) = 0*) se $f(c) = 0$.
Di immediata verifica sono le seguenti proposizioni:

Proposizione 9 *Ogni polinomio di primo grado a coefficienti in un campo F ammette una radice in F.*

Dim. Sia $f = ax+b \in F[x]$ un polinomio di primo grado. Poichè F è un campo, a è invertibile in F e l'elemento $-a^{-1}b$ è radice di f, essendo:
$a(-a^{-1}b)+b = -b+b = 0$.

Proposizione 10 *Sia F un campo, e siano f, g, h ∈ F[x]. Se f = gh, un elemento c∈F è radice di f se, e solo se, g(c) = 0 oppure h(c) = 0.*

Dim. Se c è radice di f, da $0 = f(c) = g(c)h(c)$ segue che almeno uno dei due fattori g(c) o h(c) è nullo, essendo F privo di divisori dello zero. Viceversa, se g(c) = 0 oppure h(c) = 0, risulta ovviamente $f(c) = g(c)h(c) = 0$.

L'esistenza di radici per f è legata all'esistenza per f di fattori di primo grado. Vale infatti il seguente

Teorema 11 (Teorema di Ruffini) *Siano F un campo, f∈F[x], c∈F. Allora c è radice di F se, e solo se, il polinomio x-c divide f.*

Dim. Sia c una radice di f. Per l'algoritmo della divisione esistono $q, r \in F[x]$ tali che $f = (x-c)q + r$, con $\delta(r) < \delta(x-c) = 1$. Essendo $\delta(r) \leq 0$, $r \in F$, sicchè risulta $0 = f(c) = (c-c)q(c) + r = r$. Ne segue che $f = (x-c)q$, cioè che $(x-c) \mid f$. Viceversa, se (x-c) divide f, da $f = (x-c)q$, per un opportuno polinomio q, segue $f(c) = (c-c)q(c) = 0 \cdot q(c) = 0$, e c è radice di f.

Corollario 12 *Un polinomio f a coefficienti in un campo F ammette in F una radice se, e solo se, ammette in F[x] un fattore di primo grado.*

Dim. Se f ammette una radice $c \in F$, per il Teorema di Ruffini è divisibile per x-c. Viceversa, sia $f = (a_0+a_1x)q$; allora l'elemento $c = -a_1^{-1}a_0$ risulta radice di f, poichè è radice del suo fattore a_0+a_1x.

Il Teorema di Ruffini ammette la seguente generalizzazione, della quale si omette la dimostrazione:

Teorema 13 *Siano F un campo, $f \in F[x]$, $c_1, c_2, \ldots, c_n$ n radici distinte di F. Allora f è divisibile per $(x-c_1)(x-c_2)\ldots(x-c_n)$ (ovvero esiste $g \in F[x]$ tale che $f = (x-c_1)(x-c_2)\ldots(x-c_n)g$).*

Corollario 14 *Un polinomio f di grado n ≥ 0 a coefficienti in un campo F ha al più n radici distinte.*

Dim. Per il Teorema 13, se f ammette m radici distinte $c_1, c_2,\ldots,c_m$, esiste $g \in F[x]$ tale che $f = (x-c_1)(x-c_2)\ldots(x-c_n)g$. Poichè il grado di un prodotto è uguale alla somma dei gradi dei fattori, ed avendo ogni fattore $x-c_i$ grado 1 (per i = 1, 2,…,m), da $n = m+\delta(g)$ segue $m \leq n$.

Polinomi irriducibili

In questa sezione si evidenzieranno alcune condizioni necessarie e/o sufficienti per l'irriducibilità di un polinomio a coefficienti in un campo F.

Prop.15 *Siano F un campo, f un polinomio non nullo di F[x]. Allora:*
i) se $\delta(f) = 1$, f è irriducibile;
ii) se $\delta(f) = n > 1$ e f è irriducibile, f non possiede radici in F;
iii) se $\delta(f) = 2$ oppure $\delta(f) = 3$, f è irriducibile se, e solo se, f non possiede radici in F.

Dim. i) Segue dalla definizione, non potendosi scrivere f, per la regola di addizione dei gradi, come prodotto di fattori entrambi di grado strettamente minore di quello di f.
ii) Se f ammettesse una radice c in F, per il teorema di Ruffini il polinomio x-c di grado 1 dividerebbe f, ed esisterebbe un polinomio g in F[x] di grado n-1 tale che f = (x-c)g: ciò contraddice l'irriducibilità di f.
iii) Se f è irriducibile, per la ii) non possiede radici. Viceversa, f non ammetta radici in F e, per assurdo, f non sia irriducibile. Poichè $\delta(f) > 0$, f ammette una decomposizione in fattori entrambi di grado strettamente minore di quello di f. Essendo $\delta(f) = 2$ o $\delta(f) = 3$, dalla regola di addizione dei gradi segue che almeno uno di questi fattori ha grado 1; ma ciò implica (cfr. cor.10) che f ha una radice, contro l'ipotesi.

Osservazione 16 Si noti che in generale la ii) della prop.12 non si inverte, potendo esistere polinomi di grado maggiore di uno non irriducibili e privi di radici (si pensi, ad esempio, al polinomio $x^4-4 = (x^2-2)(x^2+2) \in \mathbb{Q}[x]$, che

non ammette radici in $\mathbb{Q}$, non esistendo numeri razionali il cui quadrato sia 2 o –2). Dunque in generale per un polinomio di grado maggiore di 1 **non sono equivalenti** le proprietà "**essere irriducibile**" e "**essere privo di radici**"; esse si equivalgono solo (cfr.iii) della prop.12) quando il grado del polinomio è 2 o 3.

Nelle proposizioni che seguono, delle quali si omette la dimostrazione, si caratterizzano i polinomi irriducibili a coefficienti in alcuni campi notevoli:

Prop.17 *I polinomi irriducibili dell'anello dei polinomi $\mathbb{C}[x]$ (dove $\mathbb{C}$ è il campo dei numeri complessi) sono tutti e soli i polinomi di grado 1.*

Prop.18 *Sia f un polinomio a coefficienti nel campo $\mathbb{R}$ dei numeri reali. Allora f è irriducibile se, e solo se, f ha grado 1 oppure $f = ax^2+bx+c$ ha grado 2 e discriminante $\Delta(f) < 0$ (dove discriminante di f è il numero $\Delta(f) = b^2-4ac$).*

Si osservi in particolare che, se $f= ax^2+bx+c \in \mathbb{R}[x]$ ha grado 2 e discriminante $\Delta(f) \geq 0$, la formula risolutiva delle equazioni di II grado consente di determinarne le radici c_1 e c_2 (eventualmente coincidenti), e risulta $f = a(x – c_1)(x – c_2)$.

Per i polinomi a coefficienti nel campo $\mathbb{Q}$ dei numeri razionali non esiste una caratterizzazione analoga; esistono tuttavia delle condizioni sufficienti ad assicurare l'irriducibilità di polinomi a coefficienti razionali, e che permettono di dedurre l'esistenza in $\mathbb{Q}[x]$ di polinomi irriducibili di grado n, per ogni $n \in \mathbb{N}^*$. A tal proposito si ricorda il seguente criterio di irriducibilità:

Prop.19 (Criterio di Eisenstein) *Sia $f = a_0+a_1x+\ldots+a_nx^n$ un polinomio di $\mathbb{Q}[x]$, e siano $a_0,a_1,\ldots,a_n$ numeri interi. Se esiste un numero primo p tale che:*
i) p divide $a_0,a_1,\ldots,a_{n-1}$;
ii) p non divide a_n;
iii) p^2 non divide a_0,
allora f è irriducibile in $\mathbb{Q}[x]$.

Osservazione 20 Dal criterio di Eisenstein segue in particolare che, se p è un numero primo e $n \in \mathbb{N}$, il polinomio $f = x^n-p$ è irriducibile in $\mathbb{Q}[x]$,

verificando p rispetto ad f le ipotesi del criterio. Dunque in $\mathbb{Q}[x]$ il grado dei polinomi irriducibili può essere comunque elevato.

La proposizione che segue, pur non fornendo condizioni di irriducibilità, può essere utile nella determinazione delle radici razionali di un polinomio a coefficienti interi; sappiamo che ciò equivale a determinare eventuali fattori di grado 1.

Prop.21 *Sia* $f = a_0+a_1x+\ldots+a_nx^n$ *un polinomio di* $\mathbb{Q}[x]$ *, e siano* $a_0,a_1,\ldots,a_n$ *numeri interi. Se* $\frac{r}{s}$ *è una radice razionale di f, con r, s coprimi, allora s divide* a_n *e r divide* a_0*. In particolare, se* $a_n = \pm 1$*, f ammette in* $\mathbb{Q}$ *solo radici intere.*

Esempio: Le eventuali radici razionali del polinomio $f = 2+x^2-x^3$ devono essere intere, e dividere 2: sono da ricercarsi dunque nell'insieme {+1,-1,+2,-2} dei divisori di 2. Poichè nessuno di questi interi è radice di f, f è privo di radici in $\mathbb{Q}$. In particolare, poichè f ha grado 3, ciò equivale (cfr. Prop.12 iii)) all' essere f irriducibile in $\mathbb{Q}$ [x].

Massimo Comun Divisore tra polinomi a coefficienti in un campo

Sia F un campo ed f e g siano polinomi a coefficienti in F. Un polinomio $d \in F[x]$ è un massimo comun divisore tra f e g (in simboli: un M.C.D.(f,g)) se:

1. $d \mid f$ e $d \mid g$;
2. se $h \mid f$ e $h \mid g$, allora $h \mid d$.

ovvero se d è un divisore comune di f e g, diviso da tutti i divisori comuni di f e g.
Così come in $\mathbb{Z}$ l'algoritmo delle divisioni successive permette di determinare un massimo comun divisore tra due qualsiasi interi non

entrambi nulli, l'qanalogo algoritmo, applicato a due polinomi non entrambi nulli, permette di individuare nell'ultimo resto non nullo un M.C.D. tra i due polinomi considerati.
Nell'anello degli interi, una volta individuato un M.C.D. d tra due interi non entrambi nulli a e b, si è osservato che tutti i M.C.D. si ottenevano moltiplicando d per gli elementi invertibili di $\mathbb{Z}$, vale a dire 1 e –1. Continua a valere la stessa osservazione nell'anello dei polinomi F[x]. Infatti, se d è un M.C.D. tra due polinomi non entrambi nulli a coefficienti in F, tutti e soli i M.C.D. di tale coppia di polinomi si ottengono moltiplicando d per gli elementi invertibili di F[x] (e quindi, come già osservato, per gli elementi non nulli di F). Pertanto, se d è un M.C.D. dei polinomi f e g, tutti e soli i M.C.D. tra f e g sono del tipo $a \cdot d$ con a elemento non nullo di F. In particolare, se c è il parametro direttore del polinomio d, il polinomio $c^{-1} \cdot d$ è l'unico M.C.D. monico tra f e g.