Polinomi su un anello commutativo unitario

GIOVANNI CUTOLO

1. Definizione e terminologia essenziale

Sia A un anello commutativo unitario. Per definizione, un *anello di polinomi* a coefficienti in A nell'indeterminata x è un anello commutativo unitario $A[x]$ che verifichi le condizioni:

- (P_1) A è un sottoanello unitario di $A[x]$;[1]
- (P_2) $x \in A[x]$;
- (P_3) per ogni $f \in A[x]$ esiste una ed una sola successione $\underline{a} = (a_i)_{i\in\mathbb{N}}$ di elementi di A con la proprietà che esista $n \in \mathbb{N}$ tale che:
  - (i) $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, e
  - (ii) $a_i = 0_A$ per ogni intero $i > n$.

È possibile dimostrare, ma non lo faremo qui, che per ogni anello commutativo unitario A esiste un anello di polinomi $A[x]$ come qui specificato; vedremo più avanti che, fissato A, questi anelli di polinomi sono tutti isomorfi tra loro. Vengono chiamati *polinomi* (a coefficienti in A) gli elementi di un tale anello $A[x]$.

Lasciando fisse le notazioni per A e x appena stabilite, facciamo alcune osservazioni che dovrebbero aiutare a comprendere meglio la definizione di anello di polinomi, introducendo nel contempo un po' di terminologia.

Come mostra (P_1), gli elementi di A sono anch'essi polinomi; in questo contesto chiameremo spesso *polinomi costanti* gli elementi di A. Tra essi c'è 0_A (che è ovviamente anche lo zero di $A[x]$), chiamato anche *polinomio nullo*.

Per ogni $f \in A[x]$, la successione $\underline{a} := (a_i)_{i\in\mathbb{N}}$ descritta in (P_3) in relazione ad f viene chiamata la *successione dei coefficienti* di f e, per ciascun $i \in \mathbb{N}$, ci si riferisce talvolta ad a_i come al coefficiente di posto i (o coefficiente i-esimo) di f. Quanto richiesto al punto (ii) in (P_3) mostra che l'insieme $S_f := \{i \in \mathbb{N} \mid a_i \neq 0_A\}$ è finito (tutti gli elementi di S_f sono compresi tra 0 ed il numero che in (P_3) appare come n). Se $f \neq 0_A$ si ha ovviamente $S_f \neq \varnothing$, quindi S_f, essendo un sottoinsieme finito non vuoto di $\mathbb{N}$, ha massimo; questo massimo è chiamato il *grado* di f, denotato col simbolo νf (o anche con altri simboli, tra i quali $\nu(f)$, $\deg f$ e $\delta(f)$). Il coefficiente $a_{\nu f}$ di posto νf si chiama *coefficiente direttore* di f e verrà indicato con $\operatorname{cd} f$. In altri termini, se f è un polinomio non nullo, il grado di f è il massimo intero i tale che il coefficiente i-esimo di f non sia nullo, e questo stesso coefficiente è il coefficiente direttore di f. Ad esempio, in un anello $\mathbb{Z}[x]$ di polinomi a coefficienti in $\mathbb{Z}$ nell'indeterminata x c'è il polinomio $h = 1 + 3x - 2x^3$; la successione dei coefficienti di h è la successione $(a_i)_{i\in\mathbb{N}}$ di numeri interi definita ponendo $a_0 = 1$, $a_1 = 3$, $a_3 = -2$ e $a_i = 0$ per ogni $i \in \mathbb{N} \smallsetminus \{0, 1, 3\}$. Allora $S_h = \{0, 1, 3\}$, quindi il grado di h è 3 ed il coefficiente direttore di h è $a_3 = -2$. Un altro esempio: se $0_A \neq a \in A$ (cioè: se a è un polinomio costante non nullo) la successione $(a_i)_{i\in\mathbb{N}}$ dei coefficienti di a è quella definita da $a_0 = a$ ed $a_i = 0_A$ per ogni $i \in \mathbb{N}^*$, dunque $S_a = \{0\}$, quindi a ha grado 0 e coefficiente direttore a.

Tornando al caso generale, le definizioni appena date di grado e di coefficiente direttore per un polinomio non nullo non si possono direttamente adattare al polinomio nullo $0_A = 0_{A[x]}$ su un anello commutativo unitario A. Infatti, come si verifica immediatamente, il polinomio nullo ha la successione costante 0_A (cioè la successione $(a_i)_{i\in\mathbb{N}}$ in cui $a_i = 0_A$ per ogni $i \in \mathbb{N}$) come successione dei coefficienti. In altri termini: questo polinomio non ha coefficienti non nulli. Si conviene di estendere al polinomio nullo di $A[x]$ le definizioni di coefficiente direttore e grado ponendo $\operatorname{cd} 0_A = 0_A$ e $\nu 0_A = -\infty$, dove $-\infty$ è un simbolo, appunto, convenzionale al quale non attribuiamo uno specifico significato; richiediamo solo $-\infty \notin \mathbb{N}$ ed estendiamo a $\mathbb{N} \cup \{-\infty\}$ sia l'ordinamento che l'addizione usualmente definiti in $\mathbb{N}$, ponendo, per ogni $n \in \mathbb{N} \cup \{-\infty\}$, $-\infty \leq n$ e $(-\infty) + n = n + (-\infty) = -\infty$.

Osserviamo che, allora, i polinomi costanti sono tutti e soli i polinomi in $A[x]$ di grado minore di 1: quelli non nulli hanno grado 0, mentre il polinomio nullo è l'unico che abbia grado $-\infty$; tutti i polinomi non costanti hanno invece grado positivo. Inoltre, il polinomio nullo è l'unico polinomio con coefficiente direttore 0_A.

Riassumendo: per ogni polinomio non nullo $f \in A[x]$, la proprietà (P_3) garantisce che f si può scrivere in unico modo nella forma $\sum_{i=0}^{n} a_i x^i$ dove $n \in \mathbb{N}$, per ogni $i \in \{0, 1, 2, \ldots, n\}$ si ha $a_i \in A$ e $a_n \neq 0_A$; questo accade se si pone $n = \nu f$ e gli elementi a_i sono i primi $n+1$ termini della successione dei coefficienti di f (e quindi $a_n = \operatorname{cd} f$); i termini rimanenti della successione dei coefficienti di f sono poi tutti uguali a 0_A.[2]

Aggiungiamo ancora della terminologia: diremo che un polinomio è *monico* se e solo se il suo coefficiente direttore è 1_A. Si usa infine chiamare *termine noto* di un polinomio il suo coefficiente di posto 0.

Completiamo questa sezione introduttiva notando esplicitamente una facile conseguenza dalla proprietà (P_3). Se A è un anello commutativo unitario *non nullo* (cioè tale che $A \neq \{0_A\}$), per ogni $n \in \mathbb{N}$ il polinomio x^n ha

[1] si ricorda cosa questo significhi: A è un sottoanello di $A[x]$ e l'unità 1_A di A appartiene ad $A[x]$, quindi è anche l'unità di $A[x]$.

[2] possiamo anche aggiungere che, invece, verificano le proprietà richieste per n in (i) e (ii) di (P_3) tutti e soli i numeri naturali $n \geq \nu f$.

grado n (perché il suo coefficiente n-esimo è 1_A mentre tutti gli altri coefficienti sono uguali a 0_A), quindi $x^n \notin A$ se $n > 0$ (in particolare, $x \notin A$) e se m è un numero naturale diverso da n, allora $x^n \neq x^m$. In altri termini: se $|A| \neq 1$ le potenze di x in $A[x]$ con esponente un numero naturale sono a due a due distinte, quindi: *se A è un anello commutativo unitario non nullo, l'anello di polinomi $A[x]$ è infinito.*[3]

Approfondimenti.[4] Abbiamo un modo più preciso per chiarire la relazione che intercorre tra un polinomio e la sua successione dei coefficienti. Chiamiamo supporto di una successione $\underline{a} := (a_i)_{i\in\mathbb{N}}$ di elementi di A l'insieme $\{i \in \mathbb{N} \mid a_i \neq 0_A\}$, e indichiamo con A_ω l'insieme delle successioni di elementi di A con supporto finito. Le successioni dei coefficienti dei polinomi hanno supporto finito; abbiamo così l'applicazione $\sigma\colon A[x] \to A_\omega$ che ad ogni polinomio in $A[x]$ associa la sua successione dei coefficienti. *Questa applicazione è biettiva.* Infatti, sia $\underline{a} = (a_i)_{i\in\mathbb{N}} \in A_\omega$. Se $\{i \in \mathbb{N} \mid a_i \neq 0_A\}$ non è vuoto sia n il suo massimo, altrimenti poniamo $n = 0$. In entrambi i casi, è chiaro che il polinomio $f_{\underline{a}} := \sum_{i=0}^n a_i x^i$ ha $\underline{a}$ come successione dei coefficienti. È altrettanto chiaro che, per ogni $f \in A[x]$, se $\underline{a}$ è la successione dei coefficienti di f, allora $f = f_{\underline{a}}$. Dunque, l'applicazione $\underline{a} \in A_\omega \mapsto f_{\underline{a}} \in A[x]$ è l'inversa di σ.

Menzioniamo il fatto che una delle possibili costruzioni di un anello dei polinomi su A si ottiene proprio definendo due operazioni (di addizione e moltiplicazione) nell'insieme A_ω che rendano questo un anello commutativo unitario in cui si può immergere A, in modo che A_ω risulti un anello di polinomi ad una indeterminata a coefficienti in A.

2. Proprietà universale

La proprietà più importante degli anelli di polinomi è la seguente:

Proprietà universale per anelli di polinomi ad una indeterminata. *Sia $A[x]$ un anello di polinomi nell'indeterminata x sull'anello commutativo unitario A. Si fissino un anello commutativo unitario B ed un omomorfismo $\theta\colon A \to B$ di anelli unitari*[5] *e $b \in B$. Allora esiste uno ed un solo omomorfismo $\theta^*\colon A[x] \to B$ di anelli unitari tale che $x^{\theta^*} = b$ e θ sia la restrizione di θ^* ad A.*[6]

In altre parole, assegnati omomorfismi (di anelli commutativi unitari) come nel diagramma a sinistra (l'omomorfismo $A \hookrightarrow A[x]$ è l'immersione di A in $A[x]$) ed un arbitrario $b \in B$, esiste uno ed un solo omomorfismo θ^* che renda commutativo il diagramma a destra mandando x in b:

Diamo solo un cenno alla dimostrazione, che si può completare per esercizio. Dalla definizione di omomorfismo di anelli segue subito che θ^* non può essere altro che l'applicazione

$$\theta^*\colon \sum_{i=0}^n a_i x^i \in A[x] \longmapsto \sum_{i=0}^n a_i^\theta b^i \in B$$

(qui gli a_i rappresentano elementi di A); è da osservare che ogni elemento di $A[x]$ si scrive nella forma indicata, e segue dalla (P_3) che l'applicazione θ^* è ben definita; si può poi verificare che essa è effettivamente un omomorfismo di anelli unitari e che manda x in b. In questo modo la proprietà universale è provata.

Vediamo alcune importanti applicazioni della proprietà universale:

- *Unicità dell'anello dei polinomi, a meno di isomorfismi.* Supponiamo che $A[x]$ e $A[y]$ siano anelli di polinomi ad una indeterminata sullo stesso anello (commutativo unitario) A, con indeterminate, rispettivamente, x e y. Applichiamo la proprietà universale scegliendo come θ l'immersione $A \hookrightarrow A[y]$ e, come b, l'elemento y. Otteniamo così un (unico) omomorfismo $\alpha\colon A[x] \to A[y]$ tale che $x^\alpha = y$ e la restrizione di α ad A sia l'immersione, cioè $a^\alpha = a$ per ogni $a \in A$. Poiché anche $A[y]$ è un anello dei polinomi, possiamo ripetere la stessa costruzione scambiando i ruoli di $A[x]$ (ed x) e $A[y]$ (ed y),

  ottenendo un omomorfismo $\beta\colon A[y] \to A[x]$ tale che $y^\beta = x$ e $a^\beta = a$ per ogni $a \in A$. È facile verificare che α e β sono l'uno l'inverso dell'altro. Infatti, per ogni elemento $f = \sum_{i=0}^n a_i x^i$ di $A[x]$ si ha $f^{\alpha\beta} = (\sum_{i=0}^n a_i y^i)^\beta = \sum_{i=0}^n a_i x^i = f$ e, similmente, $g^{\beta\alpha} = g$ per ogni $g \in A[y]$. Ciò prova che α è un isomorfismo.

---

[3] segue invece facilmente da (P_1) che se A è l'anello nullo, cioè se $|A| = 1$, allora $A[x] = A$.

[4] non richiesti ai fini dell'esame.

[5] si intende con questo che θ è un omomorfismo di anelli che manda l'unità di A nell'unità di B.

[6] in queste note le immagini di elementi mediante applicazioni sono generalmente indicate con la notazione esponenziale, quindi, ad esempio, x^{θ^*} è l'immagine di x mediante θ^*.

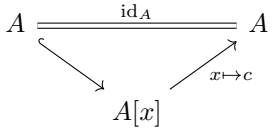
Dunque, assegnati due anelli di polinomi ad una indeterminata su A esiste un isomorfismo tra questi due anelli di polinomi che manda l'indeterminata del primo nell'indeterminata del secondo e manda in se stesso ogni elemento di A. Con le notazioni appena usate, questo isomorfismo è l'applicazione

$$\alpha\colon \sum_{i=0}^{n} a_i x^i \in A[x] \longmapsto \sum_{i=0}^{n} a_i y^i \in A[y],$$

osserviamo esplicitamente che essa manda ogni polinomio f di $A[x]$ nel polinomio di $A[y]$ che ha la stessa successione dei coefficienti di f.

Possiamo dunque dire, in modo un pò approssimativo ma efficace, che due anelli di polinomi sullo stesso anello commutativo unitario A possono solo differire per il nome dell'indeterminata; in questo senso, a meno di isomorfismi, ne esiste solo uno. Per questo motivo possiamo decidere di aver fissato, per ogni scelta di A, un anello dei polinomi $A[x]$ ad una indeterminata su A e chiamare questo *l'*anello dei polinomi ad una indeterminata su A (con l'articolo determinativo).

- L'applicazione più frequente della proprietà universale si ha per il caso in cui $B = A$ e θ è l'applicazione identica di A. In questo caso la proprietà ci dice che per ogni $c \in A$ esiste uno ed un solo omomorfismo di anelli unitari $A[x] \to A$ che manda ogni elemento di A in sé e x in c:

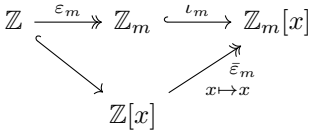


È facile descrivere esplicitamente questo omomorfismo. Per ogni $f = \sum_{i=0}^{n} a_i x^i \in A[x]$ poniamo $f(c) = \sum_{i=0}^{n} a_i c^i$. L'omomorfismo di cui stiamo parlando è allora l'applicazione:

$$f \in A[x] \longmapsto f(c) \in A,$$

che chiamiamo *omomorfismo di sostituzione*.

- Un'applicazione più specifica: per ogni intero positivo m, sia $\varepsilon_m\colon n \in \mathbb{Z} \mapsto [n]_m \in \mathbb{Z}_m$, la proiezione canonica $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_m$ (il simbolo di freccia a doppia punta ci ricorda il fatto che ε_m è un omomorfismo suriettivo). Componendo questa con l'immersione $\iota_m\colon \mathbb{Z}_m \hookrightarrow \mathbb{Z}_m[x]$ otteniamo l'omorfismo di anelli unitari[7] $\varepsilon_m\iota_m\colon n \in \mathbb{Z} \mapsto [n]_m \in \mathbb{Z}_m[x]$ (come di consueto, usiamo lo stesso simbolo, x, per l'indeterminata di diversi anelli di polinomi). La proprietà universale fornisce l'omomorfismo $\bar{\varepsilon}_m$ qui descritto:



(è facile verificare che $\bar{\varepsilon}_m$ è effettivamente suriettivo). Più esplicitamente, l'immagine mediante $\bar{\varepsilon}_m$ di $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ è il polinomio $f_m = \sum_{i=0}^{n} [a_i]_m x^i$. Per indicare questo polinomio scriveremo spesso $\sum_{i=0}^{n} \bar{a}_i x^i \in \mathbb{Z}_m[x]$; (è ovviamente essenziale indicare sempre il modulo m, per evitare ambiguità) o anche, ancora più semplicemente, $\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}_m[x]$. Si dice che f_m è *il polinomio f riguardato come polinomio a coefficienti in $\mathbb{Z}_m$* (o anche *... modulo m*). Ad esempio, se $f = 14x^3 - 3x + 1 \in \mathbb{Z}[x]$, il polinomio f riguardato come polinomio a coefficienti in $\mathbb{Z}_5$ è $\bar{4}x^3 - \bar{3}x + \bar{1} \in \mathbb{Z}_5[x]$, che possiamo anche scrivere come $-x^3 + \bar{2}x + \bar{1} \in \mathbb{Z}_5[x]$, o in infiniti altri modi.

Possiamo riferirci a quest'ultima costruzione per illustrare con qualche esempio le nozioni introdotte nella sezione precedente e vedere come grado e coefficiente direttore possono cambiare nel passaggio da un polinomio a coefficienti in $\mathbb{Z}$ al corrispondente polinomio riguardato modulo un intero positivo. Il polinomio $f = 15x^4 + 6x^2 + 2 \in \mathbb{Z}[x]$ ha grado 4 e coefficiente direttore 15. Invece f_5, cioè f riguardato come polinomio a coefficienti in $\mathbb{Z}_5$ ha grado 2 (il suo quarto coefficiente è $[15]_5 = [0]_5 = 0_{\mathbb{Z}_5}$ e coefficiente direttore $[6]_5 = [1]_5 = 1_{\mathbb{Z}_5}$, dunque f_5 è monico; possiamo scrivere $f_5 = x^2 + \bar{2} \in \mathbb{Z}_5[x]$. Invece f_3, cioè f riguardato come polinomio a coefficienti in $\mathbb{Z}_3$, ha grado 0 e si ha $f_3 = \operatorname{cd} f_3 = [2]_3 = -1_{\mathbb{Z}_3}$; dunque f_3 è un polinomio costante.

3. Grado di somme e prodotti di polinomi

Siano, ancora, A un anello commutativo unitario, e siano $f, g \in A[x]$, con successioni dei coefficienti, rispettivamente, $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}}$. Supponiamo anche $f \neq 0_A \neq g$ e poniamo $n = \nu f$, $m = \nu g$; dunque $f = \sum_{i=0}^{n} a_i x^i$ e $g = \sum_{i=0}^{m} b_i x^i$; inoltre $a_n = \operatorname{cd} f \neq 0_A$ e $b_m = \operatorname{cd} g \neq 0_A$. Allora, posto $M = \max\{n, m\}$,

$$f + g = \sum_{i=0}^{M} (a_i + b_i) x^i; \qquad f - g = \sum_{i=0}^{M} (a_i - b_i) x^i; \qquad fg = (a_0 b_0) + (a_0 b_1 + a_1 b_0) x + \cdots + (a_n b_m) x^{n+m}.$$[8]

[7] In conformità all'uso della notazione esponenziale per le immagini di elementi del dominio di un'applicazione, la composizione di applicazioni è indicata in queste note nell'ordine naturale, scrivendo a sinistra l'applicazione che agisce per prima, quindi fg piuttosto che $g \circ f$ se f e g sono applicazioni componibili. Ad esempio, $\varepsilon_m\iota_m = \iota_m \circ \varepsilon_m$

[8] più precisamente: $fg = \sum_{i=0}^{n+m} c_i x^i$, dove, per ogni i, si ha $c_i = \sum_{j=0}^{i} a_j b_{i-j} = a_0 b_i + a_1 b_{i-1} + a_2 b_{i+2} + \cdots + a_{i-1} b_1 + a_i b_0$.

Cosa possiamo dire sui gradi di questi tre polinomi? Consideriamo in primo luogo $f+g$. Nella sua espressione non appaiono potenze di x con esponente superiore a M, quindi certamente $\nu(f+g) \leq M$, e $\nu(f+g) = M$ se e solo se il coefficiente di posto M in $f+g$ (cioè $a_M + b_M$) è diverso da zero. Distinguiamo tre casi: se $n < m$ allora $M = m$ e $a_m = 0_A$, quindi $a_M + b_M = b_m \neq 0_A$. In questo caso, dunque, $\nu(f+g) = m = M$, inoltre $\operatorname{cd}(f+g) = b_m = \operatorname{cd} g$. Ad esempio: se $A = \mathbb{Z}$, $f = 2x+1$ e $g = 3x^4 + 2x + 2$ (quindi $n = 1 < m = 4$) allora $f + g = 3x^4 + 4x + 3$ ha grado $4 = m$. Similmente, se $n > m$, vediamo che $f + g$ ha grado n e coefficiente direttore $a_n = \operatorname{cd} f$. Nel terzo caso, quello in cui $n = m$, bisogna fare una distinzione ulteriore: se $a_n + b_n \neq 0_A$ abbiamo $\nu(f+g) = n = M$ e $\operatorname{cd}(f+g) = a_n + b_n$, ma se invece $a_n + b_n = 0_A$ (cioè $a_n = -b_n$) allora certamente $\nu(f+g) < n$, perché per ogni intero $i > n-1$ il coefficiente i-esimo di $f+g$ è 0_A. Possiamo riassumere così ciò che abbiamo provato sino a questo punto:

Proposizione 1. *Se A è un anello commutativo unitario e $f, g \in A[x] \smallsetminus \{0_A\}$, allora $\nu(f+g) = \max\{\nu f, \nu g\}$ a meno che $\nu f = \nu g$ e $\operatorname{cd} f = -\operatorname{cd} g$. In questo secondo caso $\nu(f+g) < \nu f = \nu g$.*

Ripetendo il ragionamento per $f - g$, oppure applicando la Proposizione 1 a f e $-g$ (perché $f - g = f + (-g)$) si ha:

Proposizione 2. *Se A è un anello commutativo unitario e $f, g \in A[x] \smallsetminus \{0_A\}$, allora $\nu(f-g) = \max\{\nu f, \nu g\}$ a meno che $\nu f = \nu g$ e $\operatorname{cd} f = \operatorname{cd} g$. In questo secondo caso $\nu(f-g) < \nu f = \nu g$.*

Vediamo qualche altro esempio, ancora in $\mathbb{Z}[x]$. Se $f = 3x^2 + x + 1$ e $g = 2x^2 + x + 2$ (quindi $n = m = 2$) allora $f - g = x^2 - 1$ ha anch'esso grado 2 (f e g hanno lo stesso grado, ma coefficienti direttori diversi); se invece $g = 3x^2 + x + 2$ allora $\nu f = \nu g$ e $\operatorname{cd} f = \operatorname{cd} g$, quindi $f - g$ non ha grado 2, infatti $f - g = -1$ ha grado 0.

Passiamo ora a considerare il grado di fg. Il ragionamento è simile: poiché nell'espressione di fg non appaiono potenze di x con esponente superiore a $n+m$ certamente $\nu(fg) \leq n+m$ e vale $\nu(fg) = n+m$ se e solo se $a_n b_m$ (il coefficiente $(n+m)$-esimo di fg) è diverso da zero. Abbiamo allora:

Proposizione 3. *Se A è un anello commutativo unitario e $f, g \in A[x] \smallsetminus \{0\}$, posto $a = \operatorname{cd} f$ e $b = \operatorname{cd} g$ si ha:*

(i) *se $ab \neq 0_A$, allora $\operatorname{cd}(fg) = ab$ e $\nu(fg) = \nu f + \nu g$. In particolare, $fg \neq 0_A$;*
(ii) *se $ab = 0_A$, allora $\nu(fg) < \nu f + \nu g$.*

Se si verifica $\nu(fg) = \nu f + \nu g$, come nel caso (i) di questa proposizione, si dice che per i polinomi f e g vale la *regola di addizione dei gradi*. Ovviamente questa regola vale sempre nel caso in cui uno tra f e g è il polinomio nullo: se, ad esempio, $f = 0_A$, allora $\nu(fg) = \nu(0_A) = -\infty = (-\infty) + \nu g = \nu f + \nu g$.

Alcune importanti conseguenze della Proposizione 3 sono:

Corollario 4. *Sia A un anello commutativo unitario e sia $f \in A[x]$. Se $\operatorname{cd} f$ è cancellabile in A allora f è cancellabile in $A[x]$ e, per ogni $g \in A[x]$, si ha $\nu(fg) = \nu f + \nu g$.*

Dimostrazione. Sia $g \in A[x] \smallsetminus \{0_A\}$ e siano $a = \operatorname{cd} f$ e $b = \operatorname{cd} g$. Poiché a è cancellabile in A, quindi non un divisore dello zero, e $b \neq 0_A$ allora $ab \neq 0_A$. Per la Proposizione 3, allora $fg \neq 0_A$ e, inoltre, $\nu(fg) = \nu f + \nu g$. La prima informazione ci dice che f non è un divisore dello zero, e quindi è cancellabile, in $A[x]$. Con questo (ricordando che la regola di addizione dei gradi vale banalmente se uno dei polinomi coinvolti è quello nullo) la dimostrazione è completa. □

Proposizione 5. *Sia A un anello commutativo unitario. Sono allora equivalenti:*

(i) *A è un dominio di integrità;*
(ii) *per ogni coppia di polinomi $A[x]$ vale la regola di addizione dei gradi (cioè: $\forall f, g \in A[x](\nu(fg) = \nu f + \nu g)$);*
(iii) *$A[x]$ è un dominio di integrità.*

Inoltre, se A è un dominio di integrità allora $\mathcal{U}(A[x]) = \mathcal{U}(A)$.[(9)]

Dimostrazione. Supponiamo che A sia un dominio di integrità, e siano $f, g \in A[x]$. Se $f = 0_A$, allora vale banalmente $\nu(fg) = \nu(0_A) = -\infty = \nu f + \nu g$. Se invece $f \neq 0_A$, allora $\operatorname{cd} f \neq 0_A$, quindi, poiché A è un dominio di integrità, $\operatorname{cd} f$ è cancellabile in A e $\nu(fg) = \nu f + \nu g$ per il Corollario 4. Abbiamo provato che (i) implica (ii).

Che (ii) implichi (iii) è ovvio: se $f, g \in A[x] \smallsetminus \{0_A\}$ e in $A[x]$ vale la regola di addizione dei gradi, allora, come per la Proposizione 3, si ha $\nu(fg) = \nu f + \nu g \geq 0$, quindi $fg \neq 0_A$; questo significa che in $A[x]$ vale la legge di annullamento del prodotto e dunque $A[x]$ è un dominio di integrità.

Anche l'implicazione (iii) $\Rightarrow$ (i) è banale: se $A[x]$ è un dominio di integrità e a e b sono elementi di $A \smallsetminus \{0_A\}$, allora $ab \neq 0_A$, perché altrimenti a sarebbe un divisore dello zero in $A[x]$.[(10)]

Resta solo da provare che $\mathcal{U}(A[x]) = \mathcal{U}(A)$ se valgono le condizioni (i), (ii) e (iii). Se $a \in \mathcal{U}(A)$ e b è l'inverso di a in A, allora $ab = 1_A = 1_{A[x]}$, quindi b è anche l'inverso di a in $A[x]$, dunque $a \in \mathcal{U}(A[x])$. Pertanto $\mathcal{U}(A) \subseteq \mathcal{U}(A[x])$.[(11)] Nell'ipotesi che A sia un dominio di integrità sia, viceversa, $f \in \mathcal{U}(A[x])$ e sia g l'inverso di f in $A[x]$. Allora $fg = 1_A$ e, ovviamente, $f \neq 0_A \neq g$. Poiché in $A[x]$ vale la regola di addizione dei gradi,

(9) ricordiamo che, per ogni anello unitario R, con $\mathcal{U}(R)$ si indica il gruppo moltiplicativo degli elementi invertibili di R.

(10) in sostanza, ciò che stiamo osservando è che i sottoanelli non nulli dei domini di integrità sono essi stessi domini di integrità.

(11) anche in questo caso l'argomentazione mostra qualcosa che vale in contesti più generali: se A è un sottoanello *unitario* di un anello unitario R, allora $\mathcal{U}(A) \subseteq \mathcal{U}(R)$.

$\nu f + \nu g = \nu(fg) = \nu(1_A) = 0$. Dunque, νf e νg sono due numeri naturali la cui somma è 0; di conseguenza $\nu f = \nu g = 0$. Ciò mostra che $f \in A$ e $g \in A$, quindi sia f che il suo inverso sono elementi di A, dunque $f \in \mathcal{U}(A)$. Abbiamo così provato anche l'inclusione $\mathcal{U}(A[x]) \subseteq \mathcal{U}(A)$; a questo punto la dimostrazione è completa. □

Vediamo così che la regola di addizione dei gradi non vale per polinomi su anelli che non siano domini di integrità, ed è importante osservare che per tali anelli può non valere neanche la conclusione finale della Proposizione 5: non è detto che i polinomi invertibili siano costanti. Se ad esempio scegliamo come A l'anello $\mathbb{Z}_4$ e poniamo $f = \bar{2}x + \bar{1} \in \mathbb{Z}_4[x]$, allora $f^2 = \bar{4}x^2 + \bar{4}x + \bar{1} = \bar{1} = 1_{\mathbb{Z}_4}$, quindi non solo $0 = \nu(f \cdot f) < \nu f + \nu f$ e non vale in questo caso la regola di addizione dei gradi, ma addirittura abbiamo $f \in \mathcal{U}(\mathbb{Z}_4[x])$ (si ha $f^{-1} = f$) pur non essendo f un polinomio costante. Quindi $\mathcal{U}(\mathbb{Z}_4[x]) \neq \mathcal{U}(\mathbb{Z}_4)$, anzi $\mathcal{U}(\mathbb{Z}_4[x]) \not\subseteq \mathbb{Z}_4$.

Un ragionamento simile a quello svolto nella dimostrazione della Proposizione 5 utilizzando la regola di addizione dei gradi mostra che i polinomi monici di grado maggiore di zero non sono mai invertibili. Ad esempio, qualunque sia l'anello commutativo unitario non nullo A, l'indeterminata x non è invertibile in $A[x]$. Infatti, se x fosse invertibile, detto g il suo inverso, avremmo $1_A = xg$ e quindi $\nu(xg) = 0$, ma, per il Corollario 4, vale per x e g la regola di addizione dei gradi, quindi $\nu(xg) = \nu x + \nu g = 1 + \nu g$, in contraddizione con quanto appena detto.[12] Di conseguenza, *qualsiasi sia l'anello commutativo unitario non nullo* A, in $A[x]$ esistono elementi non invertibili e diversi dallo zero, quindi $A[x]$ *non è un campo.*[13]

4. Divisione con resto tra polinomi

Se f e g sono due polinomi su un anello commutativo unitario A, con $g \neq 0_A$, diciamo che in $A[x]$ è possibile effettuare la divisione di f (il *dividendo*) per g (il *divisore*) se e solo se esistono $q, r \in A[x]$ (che chiamiamo rispettivamente *quoziente* e *resto*) tali che $f = gq + r$ e $\nu r < \nu g$.

Un'osservazione banale è che se, nella situazione appena descritta, $\nu f < \nu g$ allora è sicuramente possibile effettuare la divisione di f per g: basta porre $q = 0$ e $r = f$. Il teorema che segue garantisce non solo la possibilità di effettuare la divisione, ma anche l'unicità di quoziente e resto in un caso importante.

Teorema 6. *Siano A un anello commutativo unitario e $f, g \in A[x]$. Supponiamo $\operatorname{cd} g \in \mathcal{U}(A)$. Allora esiste una ed una sola coppia $(q, r) \in A[x] \times A[x]$ tale che $f = gq + r$ e $\nu r < \nu g$.*

Dimostrazione. Iniziamo a provare l'esistenza di (q, r). Come appena osservato, se $\nu f < \nu g$ una coppia con le proprietà richieste si ottiene ponendo $q = 0$ e $r = f$. Possiamo allora supporre $n := \nu f \geq m := \nu g$; osserviamo che l'ipotesi su $\operatorname{cd} g$ garantisce $\operatorname{cd} g \neq 0_A$ e quindi $n, m \in \mathbb{N}$. Ragioniamo per induzione su n, quindi supponiamo che, per ogni $h \in A[x]$ tale che $\nu h < n$, sia possibile effettuare la divisione di h per g. Siano $a = \operatorname{cd} f$ e $b = \operatorname{cd} g$. Consideriamo il polinomio $k = ab^{-1}x^{n-m}g$. È chiaro che per $ab^{-1}x^{n-m}$ e g vale la regola di addizione dei gradi, in quanto il prodotto dei coefficienti direttori di questi due polinomi è $(ab^{-1})\operatorname{cd}(g) = ab^{-1} \cdot b = a \neq 0_A$ (vedi Proposizione 3). Dunque $\nu k = \nu(ab^{-1}x^{n-m}) + \nu g = (n - m) + m = n = \nu f$ e $\operatorname{cd} k = a = \operatorname{cd} f$. Allora f e k hanno lo stesso grado, n, e lo stesso coefficiente direttore, quindi la Proposizione 2 mostra che $h := f - k$ ha grado minore di n. A questo punto l'ipotesi induttiva garantisce che è possibile effettuare la divisione di h per g, dunque esistono $q_1, r_1 \in A[x]$ tali che $h = gq_1 + r_1$ e $\nu r_1 < \nu g$. Ora, $f = k + h = ab^{-1}x^{n-m}g + gq_1 + r_1 = g(ab^{-1}x^{n-m} + q_1) + r_1$, quindi, la coppia (q, r), definita ponendo $q = ab^{-1}x^{n-m} + q_1$ e $r = r_1$, soddisfa le condizioni richieste. L'esistenza della coppia (q, r) è così provata.

Dobbiamo ora verificarne l'unicità. Siano (q, r) e $(\bar{q}, \bar{r})$ due coppie con le proprietà richieste per quoziente e resto, dunque $f = gq + r = g\bar{q} + \bar{r}$, inoltre $\nu r, \nu\bar{r} < m$. Da $gq + r = g\bar{q} + \bar{r}$ segue $g(q - \bar{q}) = \bar{r} - r$. Dalla Proposizione 2 segue $\nu(\bar{r} - r) < m$. D'altra parte, poiché $\operatorname{cd} g$ è invertibile, quindi cancellabile, vale per g e $q - \bar{q}$ la regola di addizione dei gradi, dunque $\nu\big(g(q - \bar{q})\big) = m + \nu(q - \bar{q})$. Abbiamo così $m + \nu(q - \bar{q}) = \nu(\bar{r} - r) < m$. Di conseguenza $\nu(q - \bar{q}) = -\infty$, quindi $q - \bar{q} = 0_A$, ovvero $\bar{q} = q$ e, quindi, poiché $\bar{r} - r = g(q - \bar{q}) = 0_A$, $\bar{r} = r$. L'unicità della coppia (q, r) è così dimostrata. □

Un caso molto importante è quello dei polinomi a coefficienti in un campo. Infatti, se A è un campo e $0_A \neq g \in A[x]$ allora $\operatorname{cd} g$ è invertibile, come ogni elemento non nullo di A. Dunque, in questo caso, l'ipotesi $\operatorname{cd} g \in \mathcal{U}(A)$ nel Teorema 6 può essere sostituita da $g \neq 0_A$. Abbiamo così:

Corollario 7. *Siano K un campo e $f, g \in K[x]$. Se $g \neq 0_K$ esiste una ed una sola coppia $(q, r) \in K[x] \times K[x]$ tale che $f = gq + r$ e $\nu r < \nu g$.*

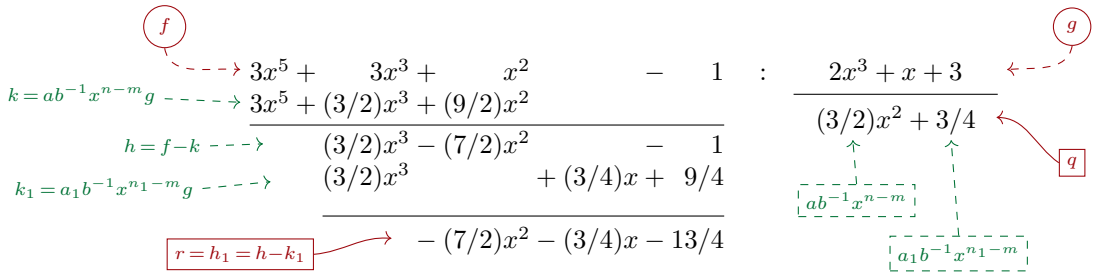
Notiamo che, con la notazione e nelle ipotesi del Teorema 6, g divide f se e solo se il resto (unicamente determinato) della divisione di f per g è 0_A.

Osserviamo poi che la dimostrazione del Teorema 6 fornisce un algorimo per il calcolo di quoziente e resto. Questo algoritmo non è altro che il procedimento comunemente insegnato anche nelle scuole per la divisione tra polinomi. Un esempio dovrebbe bastare a rendere questo punto chiaro. In $\mathbb{Q}[x]$ consideriamo i polinomi $f = 3x^5 + 3x^3 + x^2 - 1$ e $g = 2x^3 + x + 3$, e procediamo a dividere f per g. In accordo con le notazioni della dimostrazione del Teorema 6, poniamo $n = \nu f = 5$, $m = \nu g = 3$, $a = \operatorname{cd} f = 3$ e $b = \operatorname{cd} g = 2$. Abbiamo

[12] più in generale si può verificare, e si consiglia di farlo per esercizio, che lo stesso ragionamento mostra che se f è un polinomio non costante a coefficienti in un anello commutatativo unitario A e $\operatorname{cd} f$ è cancellabile in A, allora f non è invertibile in $A[x]$.

[13] Abbiamo anche accennato in una nota precedente al fatto che se A è nullo, allora anche $A[x]$ è nullo e quindi non è un campo. Dunque, qualsiasi sia l'anello commutativo unitario non nullo A, $A[x]$ non è un campo.

$ab^{-1}x^{n-m} = (3/2)x^2$ (che scriviamo sotto la linea al di sotto di g, perché sarà un addendo del quoziente) e $k = ab^{-1}x^{n-m}g = 3x^5 + (3/2)x^3 + (9/2)x^2$; seguendo la procedura descritta nella dimostrazione del teorema calcoliamo $h = f - k$. Se si avesse $\nu h < m$ allora la divisione sarebbe terminata: h sarebbe il resto, mentre il quoziente sarebbe $ab^{-1}x^{n-m}$.



Nel nostro esempio si ha invece $h = (3/2)x^3 - (7/2)x^2 - 1$, quindi $\nu h \geq m$ (in questo esempio, $\nu h = m$). La divisione va allora continuata, ripetendo la procedura dopo aver sostituito h ad f: posto $a_1 = \operatorname{cd} h$ e $n_1 = \nu h$ calcoliamo $a_1b^{-1}x^{n_1-m}$ (che scriviamo come secondo addendo del quoziente) e poi $k_1 = a_1b^{-1}x^{n_1-m}g$ e $h_1 = h - k_1$. Nel nostro esempio abbiamo $a_1 = 3/2$ e $n_1 = 3$, otteniamo dunque $a_1b^{-1}x^{n_1-m} = 3/4$, $k_1 = (3/2)x^3 + (3/4)x + 9/4$ e $h_1 = -(7/2)x^2 - (3/4)x - 13/4$. Poiché $\nu h_1 < m$ la divisione è terminata: h_1 è il resto, il quoziente è la somma $q = ab^{-1}x^{n-m} + a_1b^{-1}x^{n_1-m}$ dei suoi addendi calcolati fino a questo punto. In altri casi avremmo potuto avere ancora $h_1 \neq 0$ e $\nu h_1 \geq m$ e la divisione non sarebbe terminata qui, ma la procedura avrebbe dovuto essere ancora ripetuta, dopo aver sostituito h_1 ad f, calcolando, come nei passi precedenti, un polinomio h_2, di grado minore di νh_1, ed iterando ancora il procedimento fino ad ottenere un polinomio di grado minore di m: il resto della divisione; nello stesso tempo questo procedimento fornisce il quoziente come somma degli addendi calcolati ad ogni iterazione.

Il fatto che, nell'anello dei polinomi su un campo sia sempre possibile fare la divisione per un polinomio non nullo rende possibile, in questo caso, eseguire l'*algoritmo euclideo* delle divisioni successive per la ricerca del massimo comun divisore, esattamente allo stesso modo che nell'anello degli interi. Se K è un campo e $f, g \in K[x]$, se $g \neq 0_K$ dividiamo f per g ottenendo un quoziente q ed un resto r, se $r \neq 0_K$ dividiamo g per r ottenendo un resto r_1, se $r_1 \neq 0_K$ dividiamo r per r_1; se il resto r_2 così ottenuto non è zero dividiamo r_1 per r_2 e così via. Questo procedimento termina dopo un numero finito di passi perché i successivi resti, finché sono diversi da 0_K, hanno gradi strettamente decrescenti: $\nu g > \nu r > \nu r_1 > \nu r_2 > \cdots (\geq 0)$; dunque questa successione non può essere infinita. Così come per l'algoritmo euclideo in $\mathbb{Z}$ (ed esattamente per lo stesso motivo) l'ultimo resto non nullo è un massimo comun divisore tra f e g. E, sempre come per $\mathbb{Z}$, si può estendere l'algoritmo e dimostrare (costruttivamente) il teorema di Bézout per i polinomi su campi:

Teorema 8 (Teorema di Bézout)**.** *Sia K un campo e siano $f, g \in K[x]$. Sia d un massimo comun divisore in $K[x]$ tra f e g. Allora $\{uf + vg \mid u, v \in K[x]\}$ coincide con l'insieme dei multipli di d in $K[x]$.*

Esempio 9. In $\mathbb{Q}[x]$ consideriamo i polinomi $f = 2x^5 - x^3 + 2x^2 - 1$ e $g = x^5 + x^4 + x^3 + x^2 + x + 1$. Eseguiamo l'algoritmo euclideo per calcolare un massimo comun divisore tra f e g. La divisione di f per g fornisce quoziente 2 e resto $r = -2x^4 - 3x^3 - 2x - 3$, infatti $f = 2 \cdot g + r$. Dividendo g per r otteniamo poi $g = \big(-(1/2)x + 1/4\big) \cdot r + \big((7/4)x^3 + 7/4\big)$, qui $q_1 = -(1/2)x + 1/4$ è il quoziente e $r_1 = (7/4)x^3 + 7/4 = (7/4)(x^3 + 1)$ è il resto. La divisione successiva fornisce resto nullo, infatti $r = \big(-(8/7)x - 12/7\big)r_1$. Quindi r_1, l'ultimo resto non nullo, è un massimo comun divisore tra f e g. La teoria generale della divisibilità in monoidi commutativi ci dice che l'insieme dei massimi comuni divisori tra f e g è l'insieme dei polinomi associati a r_1; come vedremo nelle prossime sezioni questo è l'insieme di tutti i polinomi della forma cr_1 dove c è un numero razionale diverso da zero; tra questi massimi comuni divisori ne esiste dunque esattamente uno monico, precisamente $(4/7)r_1 = x^3 + 1$.

Come stabilito dal teorema di Bézout, possiamo scrivere r_1 nella forma $uf + gv$ per opportuni $u, v \in \mathbb{Q}[x]$. Possiamo calcolare una tale coppia (u, v) (ma sappiamo che ne esistono infinite) in questo modo: da $g = q_1 \cdot r + r_1$ segue $r_1 = g - q_1 r$; inoltre da $f = 2g + r$ segue $r = f - 2g$. Sostituendo questa espressione per r nell'uguaglianza precedente abbiamo $r_1 = g - q_1(f - 2g) = (-q_1)f + (1 + 2q_1)g$. Dunque, ponendo $u = -q_1 = (1/2)x - 1/4$ e $v = 1 + 2q_1 = -x + 3/2$, l'uguaglianza $r_1 = uf + gv$ è soddisfatta.

È bene tenere presente che l'algoritmo euclideo non può essere sempre utilizzato (almeno, non senza modifiche) per polinomi su anelli che non siano campi, come, ad esempio, in $\mathbb{Z}[x]$. Questo perché in questo caso non è sempre possibile effettuare la divisione tra polinomi non nulli; ad esempio, in $\mathbb{Z}[x]$ non si può dividere $2x^4 - 1$ per $3x^2 + 1$ (perché?). È possibile (ma non lo facciamo qui) verificare che *il teorema di Bézout non vale nell'anello* $\mathbb{Z}[x]$, dunque è essenziale, nel suo enunciato, richiedere che K sia un campo.

5. Applicazioni polinomiali e radici

Sia $f \in A[x]$, dove A è un anello commutativo unitario. Ricordiamo che se $f = \sum_{i=0}^{n} a_i x^i$ e $c \in A$ con $f(c)$ si indica l'elemento $\sum_{i=0}^{n} a_i c^i$ di A. L'applicazione

$$\tilde{f} \colon c \in A \longmapsto f(c) \in A$$

si chiama *applicazione polinomiale* determinata da f in A. A differenza dell'omomorfismo di sostituzione, definito nella Sezione 2, quest'applicazione non è, in generale, un omomorfismo. Osserviamo che se $f \in A$ allora $f(c) = f$ per ogni $c \in A$, quindi l'applicazione $\tilde{f}$ è costante. È per questo motivo che gli elementi di A vengono chiamati polinomi costanti (ma, attenzione!, è possibile che l'applicazione polinomiale $\tilde{f}$ sia costante anche in casi in cui il polinomio f non è costante; vedremo più avanti qualche esempio di questo tipo).

Sampre nelle stesse notazioni, diciamo che c è una *radice* di f se e solo se $f(c) = 0_A$.

Lemma 10. *Siano A un anello commutativo unitario e $f, g \in A[x]$. Allora:*

(i) *se, in $A[x]$, f divide g, ogni radice di f in A è radice di g;*
(ii) *se, in $A[x]$, f e g sono associati, f e g hanno le stesse radici in A;*
(iii) *se A è un dominio di integrità, allora le radici di fg in A sono tutti e soli gli elementi di A che sono radici di f o di g.*

Dimostrazione. (i): se $f|_{A[x]}\, g$, esiste $h \in A[x]$ tale che $g = fh$. Allora, applicando l'omomorfismo di sostituzione definito da g, abbiamo $g(c) = f(c)h(c) = 0_A h(c) = 0_A$, dunque c è radice di f.[(14)]

(ii) segue subito da (i): se f e g sono associati, f divide g e g divide f, quindi le radici di f sono radici di g e viceversa.

(iii): Per la (i), gli elementi di A che sono radici di f o di g sono radici anche di fg, multiplo di entrambi. Viceversa, se c è una radice in A di fg, allora $0_A = (fg)(c) = f(c)g(c)$. Poiché, per la Proposizione 5, $A[x]$ è un dominio di integrità, questo implica che uno tra $f(c)$ e $g(c)$ è 0_A, quindi c è radice di uno tra f e g. □

Esistono algoritmi che utilizzano questo semplice risultato per calcolare in modo efficiente valori di applicazioni polinomiali:

Teorema 11 (Teorema del resto)**.** *Sia A un anello commutativo unitario e siano $f \in A[x]$ e $c \in A$. Allora $f(c)$ è il resto della divisione di f per $x - c$.*

Dimostrazione. La prima cosa da osservare è che si può certamente effettuare la divisione di f per $x - c$, perché quest'ultimo polinomio è monico, quindi il suo coefficiente direttore è invertibile. Effettuata questa divisione, otteniamo $q, r \in A[x]$ tali che $f = (x - c)q + r$ e $\nu r < \nu(x - c) = 1$. Quest'ultima condizione equivale a dire che r è un polinomio costante, quindi $r(c) = r$. Applichiamo l'omomorfismo di sostituzione: $f(c) = \big((x - c)q + r\big)(c) = (c - c)q(c) + r(c) = 0_A q(c) + r = r$. È così provato che $f(c) = r$. □

Dal teorema del resto si ottiene immediatamente:

Teorema 12 (Teorema di Ruffini)**.** *Sia A un anello commutativo unitario e siano $f \in A[x]$ e $c \in A$. Allora c è una radice di f se e solo se $x - c$ divide f in $A[x]$.*

Dimostrazione. Per il teorema del resto, c è radice di f se e solo se il resto della divisione di f per $x - c$ è zero, cioè se e solo se $x - c$ divide f. □

Ad esempio, una conseguenza del teorema di Ruffini è:

Corollario 13. *Sia A un anello commutativo unitario e siano $f, g \in A[x]$ e $c \in A$. Supponiamo che f e g abbiano in $A[x]$ un massimo comun divisore d. Allora le radici comuni a f e g in A sono tutte e solo le radici di d in A: $\{c \in A \mid f(c) = 0_A = g(c)\} = \{c \in A \mid d(c) = 0_A\}$.*

Dimostrazione. Sia $c \in A$. Per il teorema di Ruffini, dire che c è radice di f e di g equivale a dire che $x - c$ è un divisore comune ad f e g. Per la definizione di massimo comun divisore, ciò equivale a dire che $x - c$ divide d, quindi, ancora per il teorema di Ruffini, a dire che c è radice di d. □

Per polinomi su domini di integrità vale una versione più generale del teorema di Ruffini:

Teorema 14 (Teorema di Ruffini generalizzato)**.** *Sia A un dominio di integrità unitario e siano $f \in A[x]$, $n \in \mathbb{N}^*$ e $c_1, c_2, \dots, c_n$ elementi di A a due a due distinti. Allora si ha che ciascuno degli elementi c_i è radice di f se e solo se $\prod_{i=1}^n (x - c_i)$ divide f in $A[x]$.*

Dimostrazione. Una delle due implicazioni è ovvia: se $\prod_{i=1}^n (x - c_i)$ divide f allora ciascuno degli elementi c_i è radice di f, in quanto $x - c_i$ divide f. Dimostriamo l'implicazione inversa per induzione su n. Supponiamo che gli elementi $c_1, c_2, \dots, c_n$ siano tutti radici di f. Se $n = 1$ allora $\prod_{i=1}^n (x - c_i) = x - c_1$ divide f per il teorema di Ruffini. Supponiamo allora $n > 1$ e, come ipotesi di induzione, che l'enunciato valga per insiemi di $n - 1$ elementi (distinti) di A ed arbitrari polinomi in $A[x]$. Poiché $f(c_n) = 0_A$, per il teorema di Ruffini esiste $q \in A[x]$ tale che $f = (x - c_n)q$. Sia ora i un intero tale che $1 \le i < n$. Poiché c_i è radice di f e A è un dominio di integrità, segue dal Lemma 10 (iii) che c_i è radice di uno tra $x - c_n$ e q. Ma $c_i \neq c_n$, per ipotesi, dunque $(x - c_n)(c_i) = c_i - c_n \neq 0_A$; allora c_i non è radice di $x - c_n$ e così c_i è radice di q. Dunque ciascuno degli elementi $c_1, c_2, \dots, c_{n-1}$ è radice di q. Possiamo allora applicare l'ipotesi di induzione e concludere che $\prod_{i=1}^{n-1} (x - c_i)$ divide q, quindi esiste $h \in A[x]$ tale che $q = h \prod_{i=1}^{n-1} (x - c_i)$. Allora $f = q \cdot (x - c_n) = h\big(\prod_{i=1}^{n-1} (x - c_i)\big) \cdot (x - c_n) = h \prod_{i=1}^{n} (x - c_i)$. Pertanto $\prod_{i=1}^n (x - c_i)$ divide f; la dimostrazione è così completa. □

[(14)] in alternativa, si potrebbe dedurre la (i) dal teorema di Ruffini. Come?

Il teorema di Ruffini generalizzato ha due importantissime conseguenze. La prima è una limitazione al numero di radici che un polinomio non nullo su un dominio di integrità può avere.

Teorema 15. *Sia A un dominio di integrità unitario e sia $0_A \neq f \in A[x]$. Allora il numero delle radici di f in A non supera νf.*

Dimostrazione. Se f ha esattamente n radici, siano esse $c_1, c_2, \dots, c_n$, allora f è multiplo di $g := \prod_{i=1}^{n}(x - c_i)$, per il teorema di Ruffini generalizzato, quindi $f = gq$ per opportuno $q \in A[x]$. Essendo $f \neq 0_A$ si ha anche $q \neq 0_A$. Ma $\nu g = n$ e per g e q vale la regola di addizione dei gradi (perché A è un dominio di integrità, o, in alternativa, perché g è monico, quindi ha coefficiente direttore invertibile). Quindi $\nu f = \nu g + \nu q = n + \nu q \geq n$. □

Sia per il teorema di Ruffini generalizzato che per il Teorema 15 è essenziale l'ipotesi che A sia un dominio di integrità. Consideriamo, ad esempio, il polinomio $f = \bar{2}x \in \mathbb{Z}_6[x]$. Sia $[0]_6$ che $[3]_6$ sono radici di f, quindi f ha più radici in $\mathbb{Z}_6$ di quanto sia il suo grado, che è 1. Come imposto dal teorema di Ruffini sia $x = x - [0]_6$ che $x - [3]_6$ dividono f (infatti $f = x \cdot [2]_6 = (x - [3]_6) \cdot [2]_6$), ma $x(x - [3]_6)$ non divide f, quindi la conclusione del teorema di Ruffini generalizzato non vale per f.

L'altra conseguenza del teorema di Ruffini generalizzato riguarda le applicazioni polinomiali e ci dice che nel caso dei domini di integrità infiniti ogni polinomio è identificato univocamente dalla sua applicazione polinomiale.

Teorema 16 (Principio di identità dei polinomi)**.** *Sia A un dominio di integrità infinito. Allora, per ogni $f, g \in A[x]$ si ha: $\tilde{f} = \tilde{g} \iff f = g$.*

Dimostrazione. Ovviamente $\tilde{f} = \tilde{g}$ se $f = g$. Supponiamo, viceversa, $\tilde{f} = \tilde{g}$. Allora $f(c) = g(c)$ per ogni $c \in A$. Sia $h = f - g$. Allora per ogni $c \in A$ abbiamo $h(c) = (f - g)(c) = f(c) - g(c) = 0_A$, vale a dire: ogni elemento di A è radice di h. Dunque h ha un numero infinito di radici. Ma il Teorema 15 assicura che se $h \neq 0_A$ allora il numero delle radici di h non supera νh, quindi è finito. Di conseguenza deve essere $h = 0_A$, vale a dire: $f = g$. □

È a causa del principio di identità dei polinomi che in alcuni casi vengono identificati i polinomi con le applicazioni polinomiali. Ad esempio, nei corsi di analisi matematica si definiscono i polinomi come particolari funzioni da $\mathbb{R}$ a $\mathbb{R}$, quelle che per noi sono le applicazioni polinomiali definite dai polinomi in $\mathbb{R}[x]$. Questo è lecito perché, essendo $\mathbb{R}$ un campo (quindi un dominio di integrità) infinito, il principio di identità dei polinomi assicura che i polinomi in $\mathbb{R}[x]$ corrispondono esattamente alle loro applicazioni polinomiali (in corsi di analisi più avanzati i polinomi sono definiti con riferimento al campo complesso, anziché a quello reale; il discorso è analogo: anche per il campo complesso vale il principio di identità dei polinomi). D'altra parte, non è lecito identificare polinomi ed applicazioni polinomiali in contesti in cui non valga il principio di identità dei polinomi, cioè quando l'anello A considerato sia finito oppure non sia integro.

Nel caso degli anelli finiti è certo che il principio di identità dei polinomi non può valere. Infatti, se A è un anello commutativo unitario finito, il numero delle applicazioni da A ad A, e quindi il numero delle applicazioni polinomiali in A, è finito, mentre $A[x]$ è comunque infinito. Dunque, in questo caso, è impossibile che ci sia una corrispondenza biunivoca tra polinomi e applicazioni polinomiali (ciò che il principio di identità dei polinomi afferma è che, se A è un dominio di integrità infinito, l'applicazione $f \in A[x] \mapsto \tilde{f} \in \mathrm{Map}(A, A)$ è iniettiva; ciò è impossibile nel caso che stiamo considerando ora, in cui il dominio $A[x]$ è infinito ma il codominio $\mathrm{Map}(A, A)$ è finito). Possiamo fare esempi più espliciti: il polinomio $x(x - \bar{1})(x - \bar{2}) = x^3 - x \in \mathbb{Z}_3[x]$ ha tutti gli elementi del campo $\mathbb{Z}_3$ come radici, questo significa che $\tilde{f}$ è l'applicazione costante $c \in \mathbb{Z}_3 \mapsto \bar{0} \in \mathbb{Z}_3$, ma allora $\tilde{f}$ coincide con l'applicazione polinomiale $\tilde{0}_{\mathbb{Z}_3}$ definita dal polinomio nullo, pur essendo $f \neq 0_{\mathbb{Z}_3}$. Più in generale, se se F è un campo finito, di cardinalità q, il polinomio $f = \prod_{c \in F}(x - c)$ ha grado q ed ha tutti gli elementi di F come radici, quindi $\tilde{f} = \tilde{0}_F$. È possibile dimostrare che due polinomi in $F[x]$ definiscono la stessa applicazione polinomiale se e solo se la loro differenza è un multiplo di questo polinomio f.

Anche nel caso degli anelli infiniti, che però non siano integri, il principio di identità dei polinomi può non valere. Ad esempio, se A è un anello booleano e $f = x^2 - x \in A[x]$ allora, poiché ogni elemento c di A è idempotente e quindi verifica $c^2 - c = 0_A$, ovvero $f(c) = 0_A$, tutti gli elementi di A sono radici di f. Allora $\tilde{f} = \tilde{0}_A$, anche se $f \neq 0_A$. Nel caso in cui A sia infinito, f è un esempio di polinomio di secondo grado con infinite radici.

6. Fattorizzazione

Ricordiamo che un monoide commutativo cancellativo (cioè ad elementi tutti cancellabili) si dice *fattoriale* se e solo se ogni suo elemento non invertibile è prodotto di elementi irriducibili e tali decomposizioni in irriducibili sono essenzialmente uniche.[15] Se A è un dominio di integrità unitario, allora $A^{\#} := A \setminus \{0_A\}$ è chiuso rispetto

[15] quest'ultima frase vuol dire che se $r, s \in \mathbb{N}^*$ e $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ sono elementi irriducibili tali che $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ allora $r = s$ ed esiste una permutazione $\sigma \in \mathbb{S}_r$ tale che, per ogni $i \in \{1, 2, \dots, r\}$ gli elementi p_i e q_{i^σ} siano associati. Detto in modo più facile (ma più ambiguo): il numero dei fattori nei prodotti $p_1 p_2 \cdots p_r$ e $q_1 q_2 \cdots q_s$ è lo stesso, ed i fattori nel secondo prodotto possono essere riordinati in modo che fattori corrispondenti nei due prodotti (p_1 con q_1, p_2 con q_2 etc.) siano associati tra loro. Già che ci siamo, ricordiamo anche che un elemento p si dice *irriducibile* se e solo se non è invertibile ed i suoi unici divisori sono quelli banali, cioè gli elementi invertibili e quelli associati a p. Un elemento non invertibile né irriducibile è invece *riducibile*. Due elementi a e b di un monoide commutativo S sono, per definizione, *associati* se e solo se a divide b e b divide a (in S); se poi S è anche un cancellativo si dimostra che a e b sono associati in S se e solo se $b = au$ per un opportuno elemento invertibile u di S. In ogni caso, la relazione 'essere elementi associati' è di equivalenza in S ed elementi tra loro associati hanno esattamente gli stessi divisori e gli stessi multipli.

alla moltiplicazione (questa affermazione è esattamente la legge di annullamento del prodotto: il prodotto tra due elementi di A diversi da zero è diverso da zero), quindi, con la moltiplicazione indotta da quella dell'anello, $A^\#$ è un monoide, cancellativo perché sono cancellabili in A tutti i suoi elementi. Si dice che A è un *anello fattoriale* se e solo se questo monoide $A^\#$ è fattoriale. Il motivo per cui questa nozione è importante nello studio degli anelli di polinomi è il seguente teorema, che non dimostreremo:

Teorema 17. *Se A è un anello fattoriale allora $A[x]$ è fattoriale.*

Ora, sono certamente fattoriali i campi ed è fattoriale, per il Teorema Fondamentale dell'Aritmetica, l'anello $\mathbb{Z}$ degli interi. Quindi è fattoriale $\mathbb{Z}[x]$ e, per ogni campo K, anche $K[x]$ (che, come già osservato, non può essere un campo). Dunque, sia per i polinomi a coefficienti in $\mathbb{Z}$ che per quelli a coefficienti in un campo vale un teorema di fattorizzazione essenzialmente unica in prodotto di polinomi irriducibili: ogni polinomio non invertibile e non nullo è prodotto di polinomi irriducibili e tale fattorizzazione è unica a meno dell'ordine dei fattori e della sostituzione di alcuni fattori con polinomi associati.

Nell'ipotesi che A sia fattoriale, una delle conseguenze del fatto che $A[x]$ è fattoriale è che (in analogia con ciò che accade in $\mathbb{Z}$), nota una fattorizzazione in prodotto di irriducibili di un polinomio f è facile determinare l'insieme dei divisori di f. Diamo un rapido cenno, tutto funziona come nell'aritmetica in $\mathbb{Z}$: posto $f = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$, dove ciascuno dei polinomi p_i è irriducibile, se $i \neq j$ allora p_i e p_j non sono associati e $\lambda_i \in \mathbb{N}$ per ogni i, i divisori di f sono tutti e soli i polinomi della forma $p_1^{\sigma_1} p_2^{\sigma_2} \cdots p_n^{\sigma_n}$ ed i loro associati, dove, per ogni i, valga $\sigma_i \in \mathbb{N}$ e $\sigma_i \leq \lambda_i$. Usando questa osservazione è possibile anche notare che, scelti comunque $f, g \in A[x]$, esistono un massimo comun divisore d ed un minimo comune multiplo m tra f e g, e dm è associato a fg. Infatti, escluso il caso banale in cui uno tra f e g è il polinomio nullo, f e g si possono fattorizzare nella forma $f = up_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$ e $g = vp_1^{\mu_1} p_2^{\mu_2} \cdots p_n^{\mu_n}$, dove, come sopra i p_i sono irriducibili a due a due non associati, $u, v \in \mathcal{U}(A[x]) = \mathcal{U}(A)$ e $\lambda_i, \mu_i \in \mathbb{N}$ per ogni i (notare che non è escluso che alcuni dei λ_i o μ_i siano 0). Si verifica allora che, ponendo $\sigma_i = \min\{\lambda_i, \mu_i\}$ e $\tau_i = \max\{\lambda_i, \mu_i\}$ per ogni i, si ha che $d := p_1^{\sigma_1} p_2^{\sigma_2} \cdots p_n^{\sigma_n}$ è un massimo comun divisore e $m := p_1^{\tau_1} p_2^{\tau_2} \cdots p_n^{\tau_n}$ è un minimo comune multiplo tra f e g; inoltre dm è associato a fg perché $\sigma_i + \tau_i = \lambda_i + \mu_i$ per ogni i, quindi $fg = uvdm$.

Nella pratica, è spesso molto più difficile calcolare una fattorizzazione in irriducibili di un polinomio che eseguire l'algoritmo euclideo, quindi risulta in genere conveniente questo secondo metodo quando si ricerca un massimo comun divisore tra due polinomi. È bene però notare che la discussione appena svolta mostra che anche nei casi in cui l'algoritmo euclideo non si può eseguire, come ad esempio in $\mathbb{Z}[x]$, la fattorialità garantisce comunque l'esistenza di un massimo comun divisore e di un minimo comune multiplo tra due polinomi.

Passiamo ora a discutere in maggior dettaglio le fattorizzazioni in polinomi irriducibili. Iniziamo a stabilire: quando è che due polinomi sono associati? Se A è un dominio di integrità unitario e $f \in A[x]$, i polinomi associati ad f sono tutti e soli quelli della forma uf, dove u è un polinomio invertibile in $A[x]$.[16] Come sappiamo (Proposizione 5), $\mathcal{U}(A[x]) = \mathcal{U}(A)$, quindi i polinomi associati ad f sono tutti e soli i polinomi della forma uf, dove u è un invertibile di A. In questo caso, quindi, *polinomi (non nulli) associati hanno necessariamente lo stesso grado*. Ad esempio, poiché $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$, gli associati in $\mathbb{Z}[x]$ di un $f \in \mathbb{Z}[x]$ sono f stesso (cioè $1f$) e $-f$ (cioè $(-1)f$). Se invece K è un campo $\mathcal{U}(K[x]) = \mathcal{U}(K) = K^\# := K \setminus \{0_K\}$, quindi, l'insieme di tutti i polinomi associati ad un $f \in K[x] \setminus \{0_K\}$ è $\{cf \mid 0_K \neq c \in K\}$. Se $a = \operatorname{cd} f$ si ha $\operatorname{cd}(cf) = ca$ per ogni $c \in K^\#$. Allora, qualunque sia $k \in K^\#$, il nostro polinomio f ha esattamente un associato con coefficiente direttore k, precisamente $(ka^{-1})f$ (infatti, per ogni $c \in K^\#$, abbiamo che $\operatorname{cd}(cf) = ca = k$ se e solo se $c = ka^{-1}$). Il caso più importante è quello in cui scegliamo $k = 1_K$. In questo caso ciò che otteniamo è che f ha un unico associato con coefficiente direttore 1_K, ovvero monico, precisamente $a^{-1}f$. Otteniamo così:

Proposizione 18. *Sia K un campo. In ogni classe di elementi associati di polinomi non nulli in $K[x]$ esiste uno ed un solo polinomio monico.*

Ci riferiamo a questo polinomio come al *rappresentante monico* della classe. A titolo di esempio, in $\mathbb{Q}[x]$ il polinomio monico associato a $f := 3x^2 + x - 6$ è $(1/3)f = x^2 + (1/3)x - 2$; ma anche $-6x^2 - 2x + 12$ e $(1/100)x^2 + (1/300)x - 1/50$ (e infiniti altri polinomi, tutti quelli della forma cf, dove $0 \neq c \in \mathbb{Q}$) sono associati a f. L'esistenza di un unico rappresentante monico in ogni classe di polinomi non nulli associati permette di esprimere le fattorizzazioni in irriducibili dei polinomi a coefficienti in un campo in una forma spesso più conveniente:

Proposizione 19. *Sia K un campo. Allora ogni polinomio non nullo in $K[x]$ è prodotto di un elemento di K e di polinomi monici irriducibili in $K[x]$. Tale fattorizzazione è unica a meno dell'ordine dei fattori.*

Dimostrazione. L'unicità della fattorizzazione segue dal fatto che $K[x]$ è fattoriale e dal fatto che ogni classe di polinomi associati non nulli contiene un solo rappresentante monico. L'esistenza della decomposizione è ovvia nel caso dei polinomi costanti, va provata per polinomi non costanti. Sia, allora, $f \in K[x] \setminus K$. Sia $f = p_1 p_2 \cdots p_n$ una fattorizzazione di f in prodotto di polinomi irriducibili. Per ogni $i \in \{1, 2, \ldots, n\}$ sia $a_i = \operatorname{cd}(p_i)$; allora $p_i = a_i q_i$, dove $q_i = a_i^{-1} p_i$ è associato a p_i (quindi è irriducibile) ed è monico. Posto $a = a_1 a_2 \cdots a_n$ abbiamo $f = a q_1 q_2 \cdots q_n$; questa è la decomposizione cercata. □

Si noti che, nella fattorizzazione appena descritta, $a = \operatorname{cd} f$.

[16] questo è vero se $f \neq 0_A$, perché in questo caso f è cancellabile, ma è anche banalmente vero se $f = 0_A$.

Ci vogliamo ora occupare di descrivere, per quanto possibile, la proprietà di essere o meno irriducibile per un polinomio a coefficienti in un campo. Vedremo in che modo questo proprietà è collegata alla presenza di radici. Iniziamo con una importante caratterizzazione, che, quando la trattazione è limitata ad anelli di polinomi su campi, è talvolta utilizzata per definire la nozione di polinomio irriducibile. Va tenuto ben presente che, come vedremo, questo teorema non si applica a polinomi su anelli che non siano campi.

Teorema 20. *Siano K un campo e $f \in K[x]$. Se $n = \nu f$ allora f è irriducibile in $K[x]$ se e solo se $n > 0$ e vale una delle due proprietà equivalenti:*

(a) *non esistono $g, h \in K[x]$ tali che $f = gh$ e sia g che h abbiano grado minore di n;*
(b) *non esistono $g, h \in K[x]$ tali che $f = gh$ e sia g che h abbiano grado maggiore di 0.*

Dimostrazione. Ricordiamo che f è irriducibile se e solo se, in $K[x]$, non è invertibile e non ha divisori se non quelli banali. Possiamo subito osservare che i polinomi costanti non sono irriducibili. Infatti i polinomi costanti non nulli sono invertibili per la Proposizione 5, mentre il polinomio nullo ha tutti gli elementi di $K[x] \smallsetminus K$ come divisori non banali. Abbiamo così che l'asserto è corretto nel caso in cui f sia costante: f non è irriducibile e non è vero che $n = \nu f > 0$, quindi la condizione all'enunciato non è soddisfatta. Possiamo allora assumere $f \notin K$, cioè: $n > 0$. Supponiamo dunque $n > 0$. Osserviamo che, se $g, h \in K[x]$ e $f = gh$, per la regola di addizione dei gradi (che vale perché K è un campo) si ha $\nu g + \nu h = \nu f = n$, quindi $(\nu g < n \wedge \nu h < n) \iff (\nu g > 0 \wedge \nu h > 0)$, vale a dire: (a) e (b) sono equivalenti. Se f è irriducibile, scelti comunque $g, h \in K[x]$ tali che $f = gh$, allora g è un divisore di f, quindi un divisore banale perché f è irriducibile. Allora o g è invertibile, nel qual caso $g \in K \smallsetminus \{0_K\}$ e $\nu g = 0$, oppure g è associato a f, nel qual caso $\nu g = \nu f = n$. Ciò mostra che, se f è irriducibile, sono verificate (a) e (b). Se, invece, f non è irriducibile, f ha un divisore non banale g; allora $g \neq 0_K$ (altrimenti $f = 0_K$) e g non è invertibile, quindi $\nu g > 0$, ed esiste $h \in K[x]$ tale che $f = gh$. Ovviamente $h \neq 0_K$, e h non è invertibile perché g non è associato ad f, quindi abbiamo anche $\nu h > 0$. In questo caso, dunque, non vale (b), e quindi neanche (a). □

Un'ovvia conseguenza di questa caratterizzazione è che *i polinomi di primo grado a coefficienti in un campo K sono certamente irriducibili in $K[x]$*, dal momento che i prodotti tra polinomi di grado minore di 1 sono certamente costanti.

Se, ancora, K è un campo, ogni polinomio di primo grado $ax+b \in K[x]$ ha una radice in K (precisamente $-a^{-1}b$: essendo il polinomio di grado 1 si ha $a \neq 0_K$ quindi ha senso considerare a^{-1}), dunque un polinomio f che sia divisibile per un polinomio di primo grado ha almeno una radice in K, per il Lemma 10. Viceversa, se f ha una radice allora f ha un divisore di primo grado, per il teorema di Ruffini. Dunque:

Proposizione 21. *Sia K un campo e sia $f \in K[x]$. Allora f ha radici in K se e solo se ha almeno un divisore di primo grado in $K[x]$.*

Siccome una della due implicazioni, quella stabilita dal teorema di Ruffini, vale per polinomi su anelli commutativi unitari qualsiasi, possiamo anche osservare:

Proposizione 22. *Sia A un dominio di integrità unitario e sia $f \in A[x]$. Se $\nu f > 1$ e f ha radici in A, allora f è riducibile in $A[x]$.*

Dimostrazione. Per il teorema di Ruffini, f ha un divisore h di primo grado. Allora h non è invertibile (per la Proposizione 5) e poiché, come già osservato, due polinomi in $A[x]$ che siano associati devono avere lo stesso grado, mentre $\nu h = 1 < \nu f$, allora h non è associato a f. Pertanto h è un divisore non banale di f, quindi f non è irriducibile. □

In un caso molto particolare, ma importante, vale anche il viceversa:

Proposizione 23. *Siano K un campo e f un polinomio in $K[x]$ di grado 2 o 3. Allora f è irriducibile in $K[x]$ se e solo se è privo di radici in K.*

Dimostrazione. Poiché $\nu f > 0$, certamente f non è invertibile. Se f è irriducibile allora è privo di radici, per la Proposizione 22. Viceversa, se f è riducibile allora per il Teorema 20 dobbiamo avere $f = gh$ per opportuni $g, h \in K[x]$ tali che $\nu g, \nu h < \nu f$, e naturalmente $\nu g + \nu h = \nu f$. Se $\nu f = 2$ abbiamo una sola possibilità: $\nu g = \nu h = 1$; se $\nu f = 3$ abbiamo invece due casi possibili: $\nu g = 1$ e $\nu h = 2$ oppure, viceversa, $\nu g = 2$ e $\nu h = 1$. In tutti e tre i casi, comunque, f ha un divisore di grado 1, quindi una radice. Con questo l'enunciato è dimostrato. □

Possiamo schematizzare come segue le informazioni ottenute sulle proprietà di un polinomio a coefficienti in un campo di essere o meno irriducibile ed di avere o meno radici.

Se K è un campo e $0_K \neq f \in K[x]$, posto $n = \nu f$ si ha:

$n = 0$	$\implies$	f è invertibile e privo di radici
$n = 1$	$\implies$	f è irriducibile ed ha una radice
$n \in \{2, 3\}$	$\implies$	(f è irriducibile $\iff$ f non ha radici)
$n > 3$	$\implies$	(f è irriducibile $\implies$ f non ha radici)

(Ovviamente qui per 'irriducibile' si intente 'irriducibile in $K[x]$' e per 'radice' si intende 'radice in K').

Osserviamo che l'implicazione all'ultimo rigo di questa tabella, in generale, non si inverte. Ad esempio, un polinomio di grado 4 può essere il prodotto di due polinomi irriducibili di grado 2; in questo caso il polinomio è riducibile (ovviamente ...) ma privo di radici (perché privo di divisori di primo grado; oppure per questo motivo: una radice dovrebbe necessariamente essere radice di uno dei fattori di grado due, ma essendo irriducibili questi sono privi di radici). Un esempio di questo tipo è il polinomio $(x^2+1)(x^2+2)$ in $\mathbb{Q}[x]$.

Non va poi dimenticato che tutti questi risultati valgono nel caso dei polinomi a coefficienti in un campo, ma (ad eccezione della Proposizione 22) non in casi più generali. Ad esempio, in $\mathbb{Z}[x]$ il polinomio (costante) 2 è irriducibile (non invertibile!) in $\mathbb{Z}[x]$, pur avendo grado 0; il polinomio $2x$, che è irriducibile in $\mathbb{Q}[x]$ perché $\mathbb{Q}$ è un campo e $\nu(2x)=1$, è invece riducibile in $\mathbb{Z}[x]$, perché è diviso da 2 che, in $\mathbb{Z}[x]$ non è invertibile né associato a $2x$, quindi è un divisore non banale di $2x$. Come si vede, la differenza sta nel fatto che 2 è invertibile in $\mathbb{Q}[x]$ ma non in $\mathbb{Z}[x]$. Inoltre, in $\mathbb{Z}[x]$ il polinomio di primo grado $2x+1$ è privo di radici, quindi anche la Proposizione 21 non vale per arbitrari polinomi su $\mathbb{Z}$.

7. Metodi ed esempi di fattorizzazione per polinomi su un campo

Supponiamo di voler fattorizzare un polinomio (in un fissato anello di polinomi) in prodotto di polinomi irriducibili. Per farlo abbiamo bisogno:

- di saper trovare divisori non banali dei polinomio dato, se ne esistono;
- di saper riconoscere quali tra questi divisori sono irriducibili.

Limitiamoci al caso dei polinomi su un campo. Usando la tabella nella sezione precedente, sappiamo, in linea di massima, rispondere al secondo punto nel caso di divisori di grado minore di quattro. I polinomi di grado uno sono sempre irriducibili, quelli di grado due o tre lo sono se e solo se sono privi di radici. In due casi notevoli queste informazioni sono addirittura più di quanto non sia necessario. Infatti valgono questi teoremi (che non dimostriamo) per polinomi in $\mathbb{C}[x]$ ed in $\mathbb{R}[x]$ (come di consueto, $\mathbb{C}$ indica il campo dei numeri complessi ed $\mathbb{R}$ il campo dei numeri reali).

Teorema 24. *Ogni polinomio non costante in $\mathbb{C}[x]$ ha qualche radice in $\mathbb{C}$. Di conseguenza, gli unici polinomi irriducibili in $\mathbb{C}[x]$ sono quelli di grado uno.*

Teorema 25. *Ogni polinomio irriducibile in $\mathbb{R}[x]$ ha grado minore di 3.*

Dunque, i polinomi irriducibili in $\mathbb{R}[x]$ sono precisamente quelli di grado 1 e quelli di grado 2 privi di radici. Come è noto dalle scuole superiori, un polinomio $ax^2+bx+c \in \mathbb{R}[x]$ di grado 2 ha radici in $\mathbb{R}$ se e solo se $b^2-4ac \geq 0$. Dunque, è molto facile riconoscere se un polinomio in $\mathbb{C}[x]$ o in $\mathbb{R}[x]$ è irriducibile. A proposito dei polinomi in $\mathbb{R}[x]$ vale anche questo risultato, che si può provare con metodi elementari dell'analisi (è una conseguenza del teorema di Bolzano):

Teorema 26. *Ogni polinomio di grado dispari in $\mathbb{R}[x]$ ha qualche radice in $\mathbb{R}$.*

Osserviamo che quest'ultimo teorema di potrebbe anche dedurre dal precedente, se si supponesse di aver dimostrato quello. Infatti, se f è un polinomio di grado dispari in $\mathbb{R}[x]$ e $f=p_1p_2\cdots p_r$ è una sua fattorizzazione in prodotto di polinomi irriducibili in $\mathbb{R}[x]$, allora, dal momento che ciascuno dei polinomi p_i ha grado 1 o 2, ma non tutti possono avere grado 2, altrimenti $\nu f = \sum_{i=1}^{r} \nu(p_i)$ sarebbe $2r$, che è pari, almeno uno dei fattori p_i deve avere grado 1, quindi f ha un divisore di primo grado e così ha una radice.

La situazione è molto più complessa (ed interessante) nel caso di polinomi in $\mathbb{Q}[x]$. Lo studio dei polinomi in $\mathbb{Q}[x]$ si può ridurre al caso dei polinomi a coefficienti interi. Infatti, se $f=a_0+a_1x+a_2x^2+\cdots+a_nx^n \in \mathbb{Q}[x]$, ciascuno dei coefficienti a_i sarà una frazione, che possiamo scrivere come $a_i=u_i/v_i$, dove $u_i, v_i \in \mathbb{Z}$ e $v_i \neq 0$. Se m è un multiplo comune a $v_0, v_1, \ldots, v_n$ e $m \neq 0$ allora $\bar{f} := mf \in \mathbb{Z}[x]$; poiché $m \in \mathcal{U}(\mathbb{Q}[x])$, inoltre, $\bar{f}$ è associato a f in $\mathbb{Q}[x]$. Pertanto:

Lemma 27. *Ogni polinomio $f \in \mathbb{Q}[x]$ è associato, in $\mathbb{Q}[x]$, ad un polinomio $\bar{f} \in \mathbb{Z}[x]$.*

Ora, polinomi tra loro associati hanno esattamente le stesse proprietà rispetto alla fattorizzazione. Ad esempio, i polinomi f e $\bar{f}$ di questo lemma hanno gli stessi divisori in $\mathbb{Q}[x]$, f è irriducibile in $\mathbb{Q}[x]$ se e solo se lo è $\bar{f}$, inoltre f e $\bar{f}$ hanno esattamente le stesse radici in $\mathbb{Q}$ (Lemma 10, ad esempio). In questo senso lo studio di $\bar{f}$ equivale allo studio di f. Bisogna però fare attenzione, ci stiamo riferendo a $\bar{f}$ riguardato come polinomio in $\mathbb{Q}[x]$. Detto diversamente, ci interessano le proprietà di fattorizzazione di $\bar{f}$ in $\mathbb{Q}[x]$, non in $\mathbb{Z}[x]$. Come sappiamo già da esempi visti in precedenza, anche per polinomi in $\mathbb{Z}[x]$ le proprietà di essere irriducibile in $\mathbb{Z}[x]$ o di essere irriducibile in $\mathbb{Q}[x]$ non sono equivalenti; $\bar{f}$ potrebbe essere irriducibile in $\mathbb{Q}[x]$ pur non essendolo in $\mathbb{Z}[x]$.

A differenza di quanto accade in $\mathbb{C}[x]$ ed in $\mathbb{R}[x]$, esistono in $\mathbb{Q}[x]$ polinomi irriducibili di grado arbitrariamente grande. Questo segue dal prossimo teorema, che fornisce un utile criterio sufficiente a dimostrare l'irriducibilità di alcuni polinomi.

Teorema 28 (Criterio di irriducibilità di Eisenstein)**.** *Sia $f=a_0+a_1x+a_2x^2+\cdots+a_nx^n \in \mathbb{Z}[x]$. Se esiste un primo p tale che:*

(1) *p divide $a_0, a_1, \ldots, a_{n-1}$,*

(2) *p non divide a_n,*
(3) *p^2 non divide a_0,*

allora f è irriducibile in $\mathbb{Q}[x]$.

Ad esempio, per ogni intero positivo n e per ogni primo p, il polinomio $x^n - p$ è irriducibile in $\mathbb{Q}[x]$. Infatti possiamo applicare il criterio di Eisenstein con il primo p: il coefficiente direttore del nostro polinomio, cioè 1, non è divisibile per p, ma tutti gli altri coefficienti lo sono, inoltre p^2 non divide il termine noto $-p$. Dunque le ipotesi del criterio sono soddisfatte e $x^n - p$ è irriducibile. Vediamo così che per ogni intero positivo n esistono in $\mathbb{Q}[x]$ polinomi irriducibili di grado n.

Altri esempi di polinomi la cui irriducibilità segue dal criterio di Eisenstein sono $3x^{10} - 15x^7 + 20x^5 + 5x^2 - 10$ (si può applicare il criterio ponendo $p = 5$) e $7x^4 + 6x^3 + 12x - 30$ (si può applicare il criterio ponendo $p = 2$ o anche ponendo $p = 3$). Naturalmente il fatto che non si possa applicare il criterio di Eisenstein ad un polinomio f non comporta affatto che f sia riducibile. Ad esempio, al polinomio $x^3 + 2x + 1$ non si può applicare il criterio di Eisenstein, perché nessun primo ne divide il termine noto, ma ciononostante questo polinomio è irriducibile in $\mathbb{Q}[x]$ (vedi più avanti l'Esempio 32, per una giustificazione di questo fatto).

Torniamo ora al primo dei due punti considerati all'inizio di questa sezione: in che modo possiamo cercare divisori di un polinomio? Il metodo più semplice, quando è applicabile, è quello fornito dal teorema di Ruffini. Se di un polinomio f conosciamo una radice c allora f è divisibile per $x - c$. Dividendo f per $x - c$ otteniamo un polinomio f_1 tale che $f = (x - c)f_1$. Se stiamo ricercando una fattorizzazione in irriducibili di f basterà allora trovare una fattorizzazione in irriducibili di f_1 ed aggiungere a questa il fattore $x-c$. Ad esempio, $f = x^3-1 \in \mathbb{Q}[x]$ ha chiaramente 1 come radice; possiamo allora dividere f per $x - 1$ ottenendo il quoziente $x^2 + x + 1$, allora $f = (x-1)(x^2+x+1)$. Poiché x^2+x+1 non ha radici in $\mathbb{Q}$ (non ne ha neanche in $\mathbb{R}$) ed ha grado due, x^2+x+1 è irriducibile in $\mathbb{Q}[x]$ per la Proposizione 23; dunque la fattorizzazione ottenuta è la fattorizzazione in irriducibili monici di f in $\mathbb{Q}[x]$.

La ricerca di radici (in $\mathbb{Q}$) di polinomi in $\mathbb{Q}[x]$ è semplificata enormemente da questo semplice risultato:

Proposizione 29. *Sia $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$, con $a_n \neq 0$. Allora ogni radice di f in $\mathbb{Q}$ si scrive come frazione u/v, dove u e v sono interi coprimi, u divide a_0 e v divide a_n.*

Dimostrazione. Ogni numero razionale si può scrivere come frazione ridotta, quindi nella forma u/v, dove u e v sono interi coprimi (e $v \neq 0$). Se una tale frazione u/v è radice di f allora $0 = f(u/v) = \sum_{i=0}^{n} a_i(u/v)^i$. Moltiplicando per v^n otteniamo:

$$a_0v^n + a_1uv^{n-1} + a_2u^2v^{n-2} + \cdots + a_{n-2}u^{n-2}v^2 + a_{n-1}u^{n-1}v + a_nu^n = 0.$$

Ora, escluso (per il momento) il primo, tutti gli addendi a primo membro sono multipli di u. Ma, poiché la loro somma vale 0, il primo addendo a_0v^n è l'opposto della somma dei rimanenti: $a_0v^n = -\sum_{i=1}^{n} a_iu^iv^{n-i}$, quindi anch'esso è multiplo di u. Dunque u divide a_0v^n. Ma u è coprimo con v, quindi con v^n, dunque u divide a_0, come richiesto dall'enunciato. In modo analogo si dimostra che v divide a_n: nella somma considerata sopra, escluso l'ultimo addendo a_nu^n tutti gli altri sono multipli di v, ma a_nu^n è l'opposto della somma degli addendi rimanenti, quindi v divide a_nu^n e, dal momento che v e u^n sono coprimi, v divide a_n. □

Ricordiamo che ogni polinomio in $\mathbb{Q}[x]$ è associato (in $\mathbb{Q}[x]$) ad un polinomio in $\mathbb{Z}[x]$, che avrà le sue stesse radici (in $\mathbb{Q}$). Dunque, volendo ricercare le radici razionali (cioè in $\mathbb{Q}$) di un polinomio $f \in \mathbb{Q}[x]$ possiamo procedere in questo modo: sostituiamo innanzitutto il polinomio con un suo associato a coefficienti in $\mathbb{Z}$, di questo consideriamo il coefficiente direttore a_n ed il termine noto a_0; le radici di f andranno cercate tra le frazioni ridotte con numeratore divisore di a_0 e denominatore divisore di a_n. È chiaro che (escluso il caso, banalmente semplificabile, in cui $a_0 = 0$) esiste solo un numero finito di tali frazioni, possiamo allora verificare per ciascuna di esse se è o meno radice del nostro polinomio.

Esempio 30. Consideriamo il polinomio $f = x^4 - 4x^2 + (3/2)x + 3 \in \mathbb{Q}[x]$. Un suo associato a coefficienti interi è $2f = 2x^4 - 8x^2 + 3x + 6$, con coefficiente direttore 2 e termine noto 6. Le frazioni della forma u/v con u e v interi coprimi tali che u divida 6 e v divida 2 sono: $1 = 1/1$, $1/2$, 2, 3, $3/2$, 6 ed i loro opposti -1, $-1/2$, -2, -3, $-3/2$, -6. Per cercare tutte le radici razionali di f non dobbiamo fare altro che controllare quali di questi dodici numeri sono radici di f. Nel nostro caso la verifica diretta mostra che solo -2, tra questi dodici, è radice. Concludiamo che -2 è l'unica radice di f in $\mathbb{Q}[x]$. Possiamo proseguire lo studio di questo polinomio cercando di fattorizzarlo in prodotto di irriducibili. Usiamo il teorema di Ruffini; dividendo f per $x + 2$ (cioè $x - (-2)$) otteniamo $f = (x+2)(x^3 - 2x^2 + 3/2)$. Il secondo fattore f_1 di questo prodotto è associato a $2f_1 = 2x^3 - 4x^2 + 3$. Ora, applicando direttamente la Proposizione 29 concluderemmo che le radici di f_1 sono da cercare tra le frazioni ridotte della forma u/v dove $u, v \in \mathbb{Z}$, u divide 3 e v divide 2. In realtà non è necessario esaminare tutte queste frazioni (sono in tutto otto: 1, $1/2$, 3, $3/2$ ed i loro opposti), perché ogni radice di f_1 è anche radice di f e di tutte queste frazioni, tranne -2, sappiamo che non sono radici di f, quindi nemmeno di f_1. Dobbiamo allora esaminare solo -2; si ha $f_1(-2) = (-2)^3 - 2(-2)^2 + 3/2 \neq 0$, quindi -2 non è radice di f_1. Pertanto f_1 non ha radici in $\mathbb{Q}$; poiché $\nu f_1 = 3$ concludiamo, per la Proposizione 23, che f_1 è irriducibile in $\mathbb{Q}[x]$. Dunque una fattorizzazione (l'unica a meno dell'ordine) di f in prodotto di irriducibili monici in $\mathbb{Q}[x]$ è $f = (x + 2)(x^3 - 2x^2 + 3/2)$.

Una situazione in cui la Proposizione 29 è particolarmente utile è quella in cui il polinomio f che appare nell'enunciato è monico. In questo caso, infatti, il denominatore v di una radice u/v di f in $\mathbb{Q}$ deve dividere 1, quindi $v = 1$ o $v = -1$; ciò comporta che la radice u/v è un numero intero. Abbiamo allora:

Corollario 31. *Sia f un polinomio monico in $\mathbb{Z}[x]$. Allora ogni radice razionale di f è intera.*

Esempio 32. Poco fa abbiamo detto, ma non giustificato, che il polinomio $f = x^3 + 2x + 1$ è irriducibile in $\mathbb{Q}[x]$. Sappiamo che questa affermazione equivale al fatto che f (che ha grado 3) è privo di radici in $\mathbb{Q}$, per la Proposizione 23. In effetti, ogni (eventuale) radice razionale di f deve essere intera, per il Corollario 31, inoltre, ancora per la Proposizione 29, essa deve dividere il termine noto di f, che è 1. Dunque gli unici due numeri razionali che potrebbero essere radici di f sono i divisori interi di 1, cioè 1 e -1. Ma $f(1) = 4$ e $f(-1) = -2$, quindi nessuno di questi due numeri è radice di f e così f è privo di radici. Per questo motivo f è irriducibile in $\mathbb{Q}[x]$.

Un'altra applicazione del Corollario 31 ha a che fare con le radici dei numeri interi. Se $a \in \mathbb{N}$ e $n \in \mathbb{N}^*$, la radice n-esima di a, $\sqrt[n]{a}$, è un numero reale la cui n-esima potenza sia a (precisamente, l'unico tale numero, se n è dispari, quello non negativo se n è pari). Quindi $\sqrt[n]{a}$ è una radice del polinomio monico $x^n - a \in \mathbb{Z}[x]$. Le radici razionali di questo polinomio sono intere, quindi $\sqrt[n]{a}$ è o intera (ad esempio, se $n = 2$ e $a = 4$) oppure irrazionale. Questo è un modo per dimostrare che numeri come $\sqrt{2}$, $\sqrt{3}$ o $\sqrt[11]{37}$, che certamente non sono interi, sono irrazionali.

Esempio 33. Fattorizziamo in prodotti di invertibili e irriducibili in $\mathbb{Q}[x]$ i polinomi $f = 2x^5 - x^3 + 2x^2 - 1$ e $g = x^5 + x^4 + x^3 + x^2 + x + 1$ dell'Esempio 9. Sappiamo che un loro massimo comun divisore è $(7/4)(x^3 + 1)$, quindi $d = x^3 + 1$ è il loro massimo comun divisore monico. Per fattorizzare f, conviene iniziare con lo sfruttare questa informazione, che fornisce un divisore non banale, per l'appunto d, di f. Dividendo f per d abbiamo $f = df_1$, dove $f_1 = 2x^2 - 1$. Per fattorizzare in irriducibili f basta dunque fattorizzare separatamente d e f_1. Iniziamo con $d = x^3 + 1$; poiché ha grado 3 esso è irriducibile se e solo se non ha radici in $\mathbb{Q}$, per la Proposizione 23. La Proposizione 29 (ed il Corollario 31) ci dicono che le radici razionali di d sono intere e dividono 1, quindi le sole possibili radici razionali di d sono 1 e -1. Ora, $d(1) = 2$ e $d(-1) = 0$, quindi 1 non è radice di d, ma -1 lo è. Allora, per il teorema di Ruffini, d è divisibile per $x - (-1) = x + 1$. Si ha $d = (x+1)(x^2 - x + 1)$. Le radici razionali di $h = x^2 - x + 1$ sono radici di d, la cui unica radice razionale è -1; quindi -1 è l'unica possibile radice razionale di h in $\mathbb{Q}$. Ma -1 non è radice di h, infatti $h(-1) = 3$, quindi h non ha radici in $\mathbb{Q}$ ed è così irriducibile per la Proposizione 23. Ovviamente avremmo anche potuto osservare, in alternativa, che h non ha radici reali, quindi non ha radici razionali, perché il suo discriminante è $-3 < 0$. Abbiamo così la fattorizzazione di d in irriducibili monici: $d = (x + 1)(x^2 - x + 1)$. Passiamo ora a $f_1 = 2x^2 - 1 = 2(x^2 - 1/2)$. Le radici di f_1 in $\mathbb{R}$ sono $1/\sqrt{2}$ e $-1/\sqrt{2}$, che sono irrazionali (se $1/\sqrt{2}$ fosse razionale sarebbe razionale anche il suo reciproco $\sqrt{2}$, ma sappiamo che $\sqrt{2} \notin \mathbb{Q}$). Quindi f_1 non ha radici razionali e, essendo di secondo grado, è quindi irriducibile. Mettendo insieme le fattorizzazioni di d e di f_1 otteniamo così la fattorizzazione di f come prodotto di un invertibile (il suo coefficiente direttore 2) ed irriducibili monici: $f = 2(x + 1)(x^2 - x + 1)(x^2 - 1/2)$. Questa fattorizzazione è unica a meno dell'ordine dei fattori (vedi Proposizione 19).

Fattorizziamo ora g. Come per f, iniziamo col dividere g per il suo divisore non banale d, ottenendo $g = dg_1$, dove $g_1 = x^2 + x + 1$. Abbiamo già la fattorizzazione completa di d; non è difficile verificare che g_1 è irriducibile, perché ha secondo grado ed è privo di radici. Quest'ultimo fatto si può verificare o osservando che il discriminante di g è negativo (quindi g non ha radici in $\mathbb{R}$), oppure che, per la Proposizione 29, le radici razionali di g sono da cercare tra 1 e -1, ma queste non sono radici di g. La fattorizzazione di g in prodotto di polinomi irriducibili monici in $\mathbb{Q}[x]$ è quindi $g = (x + 1)(x^2 - x + 1)(x^2 + x + 1)$.

Possiamo anche fattorizzare f e g in $\mathbb{R}[x]$. Conviene partire dalle fattorizzazioni in invertibili e irriducibili ottenute in $\mathbb{Q}[x]$. Nella fattorizzazione $f = 2(x + 1)(x^2 - x + 1)(x^2 - 1/2)$ il fattore di primo grado $x + 1$ è ovviamente irriducibile in $\mathbb{R}[x]$, i due fattori di secondo grado sono irriducibili in $\mathbb{R}[x]$ se e solo se sono privi di radici reali. Come già detto, $h = x^2 - x + 1$ non ha radici reali, quindi h è irriducibile in $\mathbb{R}$, mentre $x^2 - 1/2$ ha due radici reali, $1/\sqrt{2} = 2/\sqrt{2}$ e $-1/\sqrt{2}$, quindi $x^2 - 1/2 = (x - 1/\sqrt{2})(x + 1/\sqrt{2})$ per il teorema di Ruffini generalizzato. I due fattori appena trovati hanno grado uno e quindi sono irriducibili in $\mathbb{R}[x]$. La fattorizzazione in un invertibile e irriducibili monici di f in $\mathbb{R}[x]$ è dunque $f = 2(x+1)(x^2 - x + 1)(x - 1/\sqrt{2})(x + 1/\sqrt{2})$. Invece, entrambi i fattori di secondo grado nella fattorizzazione $g = (x + 1)(x^2 - x + 1)(x^2 + x + 1)$ di g sono privi di radici reali, quindi irriducibili anche in $\mathbb{R}[x]$, pertanto la stessa fattorizzazione è la fattorizzazione di g in prodotto di irriducibili monici in $\mathbb{R}[x]$.

A proposito del'uso del teorema di Ruffini per ottenere fattorizzazioni in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ o $\mathbb{C}[x]$, menzionamo per completezza il fatto che, così come esiste una formula che fornisce la radici di un polinomio di secondo grado (in cui appare l'estrazione di una radice quadrata), esistono formule simili, ma un pò più complicate, che forniscono le radici dei polinomi di terzo e quarto grado (in cui appaiono estrazioni di radici terze o quarte, rispettivamente) ma non esistono (meglio: non possono esistere) formule dello stesso tipo che forniscano le radici di polinomi di grado superiore al quarto.

I due esempi conclusivi riguardano polinomi su campi finiti. Soprattutto quando la cardinalità del campo finito F è piccola il metodo più efficace per la ricerca delle radici di un polinomio $f \in F[x]$ è spesso la verifica diretta eseguita per ogni elemento, vale a dire il calcolo di $f(c)$ per ogni elemento c del campo.

Esempio 34. Per alcuni valori del primo p fattorizziamo f_p, il polinomio $f = 2x^5 - x^3 + 2x^2 - 1$ dell'esempio precedente riguardato come polinomio a coefficienti in $\mathbb{Z}_p$. Tra le applicazioni della proprietà universale viste

nella Sezione 2 ricordiamo l'omomorfismo suriettivo $\bar{\varepsilon}_p$ che ad ogni polinomio in $\mathbb{Z}[x]$ associa il polinomio stesso riguardato come polinomio a coefficienti in $\mathbb{Z}_p[x]$. Il fatto che $\bar{\varepsilon}_p$ sia un omomorfismo permette di 'tradurre' fattorizzazioni di un polinomio in $\mathbb{Z}[x]$ in fattorizzazioni della sua immagine in $\mathbb{Z}_p[x]$: per il nostro f, se $g, h \in \mathbb{Z}[x]$ sono tali che $f = gh$, allora $f^{\bar{\varepsilon}_p} = g^{\bar{\varepsilon}_p} h^{\bar{\varepsilon}_p}$.

Scriviamo allora f come prodotto di polinomi a coefficienti interi e irriducibili in $\mathbb{Z}[x]$, utilizzando quanto ottenuto nell'esempio precedente: $f = (x+1)(x^2-x+1)(2x^2-1)$. Per ogni primo p abbiamo $f_p = (x+1)^{\bar{\varepsilon}_p}(x^2-x+1)^{\bar{\varepsilon}_p}(2x^2-1)^{\bar{\varepsilon}_p}$. Per ottenere una fattorizzazione in prodotto di polinomi irriducibili in $\mathbb{Z}_p[x]$ si devono allora ulteriormente fattorizzare in prodotto di irriducibili (in $\mathbb{Z}_p[x]$) i tre fattori $h_{p,1} = (x+1)^{\bar{\varepsilon}_p}$, $h_{p,2} = (x^2-x+1)^{\bar{\varepsilon}_p}$ e $h_{p,3} = (2x^2-1)^{\bar{\varepsilon}_p}$. Non c'è nessun problema per il primo fattore, che è di primo grado e quindi irriducibile qualsiasi sia il primo p, vanno invece considerati con maggiore attenzione gli altri due fattori, che vanno studiati considerando separatamente i valori di p a cui siamo interessati. Qui consideriamo i primi minori o uguali a 7:

$p = 2$: $f_2 = x^3 + \bar{1} \in \mathbb{Z}_2[x]$ ha grado 3. Il terzo dei fattori appena presi in esame, infatti, in questo caso si riduce a $[1]_2$: $h_{2,3} = (\bar{2}x^2 - \bar{1})^{\bar{\varepsilon}_p} = \bar{1}$. Il secondo fattore $h_{2,2} = x^2 + x + \bar{1}$ è privo di radici in $\mathbb{Z}_2[x]$, infatti $h_{2,2}([0]_2) = h_{2,2}([1]_2) = [1]_2 \neq [0]_2$. Quindi, per la Proposizione 23, $h_{2,2}$ è irriducibile in $\mathbb{Z}_2[x]$ (vedi anche l'esempio successivo). La fattorizzazione di f_2 in prodotto di irriducibili in $\mathbb{Z}_2[x]$ è dunque $f_2 = (x + \bar{1})(x^2 + x + \bar{1})$.

$p = 3$: Se $p > 2$, quindi anche nel caso $p = 3$ che consideriamo ora, $\nu f_p = 5$. Sia $h_{3,2}$ che $h_{3,3}$ hanno grado 2, ricerchiamone le (eventuali) radici in $\mathbb{Z}_3$. Gli elementi di $\mathbb{Z}_3$ sono $[0]_3$, $[1]_3$, e $[-1]_3$, abbiamo $h_{3,2}([0]_3) = h_{3,2}([1]_3) = [1]_3 \neq [0]_3 = h_{3,2}([-1]_3)$, quindi $[-1]_3$ è l'unica radice di $h_{3,2}$ in $\mathbb{Z}_3$. Dal momento che $\nu h_{3,2} = 2$, allora $h_{3,2}$ è riducibile (è divisibile per $x + \bar{1}$, per il teorema di Ruffini) ed è il prodotto di due polinomi di primo grado, che possiamo anche scegliere monici perché $h_{3,2}$ è monico, dunque $h_{3,2} = (x + \bar{1})(x - c)$ dove c è una radice di $h_{3,2}$. Ma $[-1]_3$ è l'unica radice di $h_{3,2}$ in $\mathbb{Z}_3$ quindi $c = [-1]_3$ ed allora $h_{3,2} = (x + \bar{1})^2 \in \mathbb{Z}_3[x]$ (cosa che, ovviamente si può anche verificare direttamente: in $\mathbb{Z}_3[x]$ si ha $(x+\bar{1})^2 = x^2 + \bar{2}x + \bar{1} = x^2 - x + \bar{1} = h_{3,2}$). Consideriamo ora $h_{3,3} = -(x^2 + \bar{1})$; questo non ha radici in $\mathbb{Z}_3$, infatti $h_{3,3}([0]_3) = [-1]_3$ e $h_{3,3}([1]_3) = h_{3,3}([-1]_3) = [1]_3$. Dunque $h_{3,3}$ è irriducibile e la fattorizzazione di f_3 nel prodotto di un invertibile ed irriducibili monici è $f_3 = (-\bar{1})(x + \bar{1})^3(x^2 + \bar{1})$.

$p = 5$: Calcolando $h_{5,2}(c) = c^2 - c + [1]_5$ per ogni $c \in \mathbb{Z}_5$ verifichiamo rapidamente che $h_{5,2}([0]_5) = h_{2,5}([1]_5) = [1]_5$, $h_{5,2}([-1]_5) = [3]_5 = [-2]_5 = h_{5,2}([2]_5)$ e $h_{5,2}([-2]_5) = [2]_5$. Quindi $h_{5,2}$ non ha radici in $\mathbb{Z}_5$ e la Proposizione 23 ne garantisce l'irriducibilità. Per quanto riguarda $h_{5,3}$ abbiamo poi $h_{5,3} = \bar{2}x^2 - \bar{1} = \bar{2}x^2 + \bar{4} = \bar{2}(x^2 + \bar{2}) = \bar{2}(x^2 - \bar{3})$. Come si verifica subito, $[3]_5$ non è un quadrato in $\mathbb{Z}_5$ (infatti $[0]_5^2 = [0]_5$, $[1]_5^2 = [-1]_5^2 = [1]_5$ e $[2]_5^2 = [-2]_5^2 = [4]_5$), quindi anche $h_{5,3}$ è privo di radici in $\mathbb{Z}_5$ ed è così irriducibile in $\mathbb{Z}_5[x]$. Dunque, la fattorizzazione di f_5 nel prodotto di un invertibile ed irriducibili monici è $f_5 = \bar{2}(x + \bar{1})(x^2 - x + \bar{1})(x^2 + \bar{2})$.

$p = 7$: Ragionando come nei casi precedenti, cerchiamo le radici di $h_{7,2}$. Scopriamo che $[-2]_7$ e $[3]_7$ sono radici di $h_{7,2}$. Abbiamo poi $h_{7,3} = \bar{2}x^2 - \bar{1} = \bar{2}x^2 + \bar{6} = \bar{2}(x^2 + \bar{3}) = \bar{2}(x^2 - \bar{4}) = \bar{2}(x + \bar{2})(x - \bar{2})$ (quindi $h_{7,3}$ ha radici $[2]_7$ e $[-2]_7$). Allora tutti i fattori irriducibili di f_7 hanno primo grado; la fattorizzazione nel prodotto di un invertibile ed irriducibili monici è $f_7 = \bar{2}(x + \bar{1})(x - \bar{3})(x + \bar{2})^2(x - \bar{2})$.

Esempio 35. Possiamo usare i risultati di queste due ultime sezioni per elencare, uno per uno, tutti i polinomi irriducibili di assegnato grado in $\mathbb{Z}_2[x]$. Per qualsiasi campo K e per ogni $n \in \mathbb{N}$ i polinomi di grado n in $K[x]$ sono tutti quelli della forma $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ dove $a_0, a_1, \ldots, a_{n-1} \in K$ e $a_n \in K \smallsetminus \{0_K\}$. Nel nostro caso, in cui $K = \mathbb{Z}_2$, richiedere $a_n \in \mathbb{Z}_2 \smallsetminus \{0_{\mathbb{Z}_2}\}$ significa richiedere $a_n = [1]_2$, dunque tutti i polinomi non nulli in $\mathbb{Z}_2[x]$ sono monici. Abbiamo allora:

- esattamente due polinomi di grado uno: $x = x + \bar{0}$ e $x + \bar{1}$. Essendo di grado uno, questi sono irriducibili.
- I polinomi di grado due sono quelli della forma $x^2 + a_1 x + a_0$, dove a_1 e a_0 possono essere $\bar{0}$ o $\bar{1}$. Abbiamo dunque quattro polinomi di grado due: x^2, $x^2 + x$, $x^2 + \bar{1}$, $x^2 + x + \bar{1}$. Tra questi sono irriducibili tutti e soli quelli privi di radici. I primi due hanno $\bar{0}$ come radice, il terzo ha $\bar{1}$ come radice, il quarto non ha né $\bar{0}$ né $\bar{1}$ come radice, quindi è privo di radici ed è così irriducibile in $\mathbb{Z}_2[x]$, l'unico irriducibile di grado 2.
- Passiamo ai polinomi di grado tre: questi hanno la forma $x^3 + a_2x^2 + a_1x + a_0$, dove a_2, a_1 e a_0 possono essere scelti tra $\bar{0}$ e $\bar{1}$. Abbiamo così otto polinomi di grado tre; tra questi quelli privi di radici in $\mathbb{Z}_2$, cioè irriducibili in $\mathbb{Z}_2[x]$, sono: $x^3 + x^2 + \bar{1}$, $x^3 + x + \bar{1}$ e nessun altro.
- Per i polinomi di grado due o tre abbiamo usato la Proposizione 23; questa non può essere più utilizzata nel caso dei polinomi di quarto grado. Dei sedici polinomi di quarto grado esattamente quattro sono privi di radici in $\mathbb{Z}_2$, essi sono: $x^4+x^3+x^2+x+\bar{1}$, $x^4+x^3+\bar{1}$, $x^4+x^2+\bar{1}$ e $x^4+x+\bar{1}$. Un polinomio f di quarto grado (su un campo qualsiasi) che sia riducibile ma non abbia radici deve avere una fattorizzazione non banale del tipo $f = gh$ in cui $4 = \nu g + \nu h$ ma $\nu g \neq 1 \neq \nu h$, perché se f avesse un fattore di grado 1 allora avrebbe una radice (Proposizione 21), quindi deve aversi $\nu g = \nu h = 2$ Inoltre, poiché f è privo di radici anche g ed h sono privi di radici, quindi irriducibili. Dunque, un polinomio di quarto grado a coefficienti in un campo è irriducibile se e solo se è privo di radici e non è il prodotto di due polinomi irriducibili di grado due. Nel caso del campo $\mathbb{Z}_2$, che stiamo considerando, abbiamo visto che esiste solo un polinomio irriducibile di grado due: $x^2+x+\bar{1}$. Allora i polinomi irriducibili di grado quattro in $\mathbb{Z}_2[x]$ sono tutti e soli quelli privi radici ad eccezione di $(x^2+x+\bar{1})^2$. Poiché, come si vede rapidamente, $(x^2+x+\bar{1})^2 = x^4+x^2+\bar{1}$,

concludiamo che i polinomi irriducibili di grado quattro in $\mathbb{Z}_2[x]$ sono: $x^4+x^3+x^2+x+\bar{1}$, $x^4+x^3+\bar{1}$ e $x^4+x+\bar{1}$.

Abbiamo così stabilito che in $\mathbb{Z}_2[x]$ esistono esattamente due polinomi irriducibili di grado 1, uno di grado 2, due di grado 3, tre di grado 4. Si potrebbe continuare, con lo stesso metodo, ad elencare i polinomi irriducibili in $\mathbb{Z}_2[x]$ di gradi maggiori. Ad esempio, osservando che i polinomi irriducibili di grado cinque a coefficienti in un campo sono quelli privi di radici che non siano prodotto di un polinomio di grado due ed uno di grado tre si può arrivare a concludere che i polinomi irriducibili di grado cinque in $\mathbb{Z}_2[x]$ sono esattamente sei.

Si può anche ripetere l'esercizio per altri campi finiti. In questo caso non è più vero che i polinomi non nulli sono tutti monici, ma per trovare tutti quelli irriducibili basta comunque trovare gli irriducibili monici ed aggiungere poi alla lista i loro associati. Ad esempio, i polinomi irriducibili di secondo grado in $\mathbb{Z}_3[x]$ sono $x^2+\bar{1}$, $x^2+x-\bar{1}$, $x^2-x-\bar{1}$ (che sono i polinomi monici di grado due privi di radici) ed i loro opposti, che sono i loro altri associati.