Capitolo 2

Seconda lezione

2.1 Prodotto cartesiano

Per descrivere le operazioni in modo piu' formale, ci servira' il concetto di prodotto cartesiano, che risulterà utile in molti altri contesti.

Definizione 2.1. [BBB02] *Siano A, B insiemi. Allora l'insieme delle coppie ordinate composte da un elemento di A ed uno di B si dice* prodotto cartesiano *di A e B e si scrive $A \times B$. Più formalmente*

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

Due elementi di $A \times B$ sono uguali se sono uguali elemento per elemento, ovvero

$$(a, b) = (c, d) \Leftrightarrow a = c \text{ e } b = d$$

Esempio 2.2. [BBB03] *Alcuni esempi:*

1. $\{2, 4, 6\} \times \{0, 1\} = \{(2, 0), (2, 1), (4, 0), (4, 1), (6, 0), (6, 1)\}$
2. $\mathbb{Q} \times \mathbb{R} = \{(q, r) \mid q \in \mathbb{Q},\ r \in \mathbb{R}\}$.
3. $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\} = \mathbb{R}^2$. *Il piano reale.*
4. $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\} = \mathbb{R}^3$. *Lo spazio reale.*
5. $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \mathbb{R}\}$. *Possimo generalizzare il prodotto cartesiano a più di due fattori.*

Definizione 2.3. [BBF07] *Dato A insieme, un operazione $\oplus$ su A è una funzione*

$$\begin{array}{rccc} \oplus\colon & A \times A & \to & A \\ & (a, b) & \mapsto & a \oplus b \end{array}$$

Osservazione 2.4. [BBB04] *Notiamo che se $(A, +_A, \cdot_A), (B, +_B, \cdot_B)$ sono anelli, allora possiamo considerare $A \times B$ anello con le operazioni ovvie. Ovvero $(A \times B, \oplus, \odot)$ è un anello con le operazioni*

$$\begin{array}{rccc} \oplus\colon & (A \times B) \times (A \times B) & \to & (A \times B) \\ & (a, b), (x, y) & \mapsto & (a +_A x, b +_B y) \end{array}$$

e

$$\begin{array}{rccc} \odot\colon & (A \times B) \times (A \times B) & \to & (A \times B) \\ & (a, b), (x, y) & \mapsto & (a \cdot_A x, b \cdot_B y) \end{array}$$

Dimostrazione. Il neutro additivo è $(0_A, 0_B)$, il neutro moltiplicativo è $(1_A, 1_B)$. Tutte le proprietà che richiediamo alle operazioni $\oplus, \odot$ discendono immediatamente dalle proprietà delle operazioni di anello $+_A, \cdot_A, +_B, \cdot_B$. □

Esempio 2.5. [BBB05] *In* $\mathbb{R}^2$ *abbiamo*

$$(1,-3)+(1,1)=(2,-2), \quad (1,-3)\cdot(1,1)=(1,-3) \quad (2,3)\cdot(0,2)=(0,6)$$

In $\mathbb{R}\times\mathbb{Q}[x]$ *abbiamo*

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

In $\mathbb{R}^2$ *abbiamo delle patologie:*

$$(2,0)\cdot(0,3)=(0,0)$$

Quindi esistono due elementi non nulli il cui prodotto è nullo.

Definizione 2.6. [BBB06] *Dato un anello* A*, un suo elemento* $a\neq 0$ *è detto* zero divisore *se esiste* $b\in A,\ b\neq 0$ *tale che* $a\cdot b=0$*.*

Esempio 2.7. [BBB07] $(\mathbb{R}^2+,\cdot)$ *non è un campo. Basta far vedere che l'elemento* $(0,1)$*, non nullo, non è invertibile, dato che in un campo tutti gli elementi non nulli devono avere inverso. Se fosse invertibile, esisterebbe il suo inverso, un elemento* $(x,y)\in\mathbb{R}^2$ *tale che*

$$(x,y)\cdot(0,1)=(1,1)\Leftrightarrow(0,y)=(1,1)\Leftrightarrow\begin{cases}0=1\\ y=1\end{cases}$$

che è assurdo perchè $1\neq 0$*. Analogamente,* $\mathbb{R}^n$ *non è un campo con le operazioni ovvie.*

2.2 Irriducibili e fattorizzazioni, Fattorizzazione unica

Generalizziamo alcune proprietà di $\mathbb{Z}$ a $\mathbb{K}[x]$.

Definizione 2.8. [AAA26] *Siano* $f(x), g(x)\in\mathbb{K}[x]$*, con* $deg(f(x))\geq\deg(g(x))>0$*. Allora Diciamo che* $g(x)$ *divide* $f(x)$ *se dividendo* $f(x)$ *per* $q(x)$ *abbiamo un resto nullo.*

Discende immediatamente dalla definizione precedente che

Osservazione 2.9. [AAB26] *Siano* $f(x), g(x)\in\mathbb{K}[x]$*, con* $deg(f(x))\geq\deg(g(x))>0$*. Allora Diciamo che* $g(x)$ *divide* $f(x)$ *se esiste* $q(x)\in\mathbb{K}[x], \deg q(x)>0$ *tale che* $f(x)=q(x)g(x)$*.*

Definizione 2.10. [AAA27] *Un polinomio* $f(x)\in\mathbb{K}[x]$ *di grado* ≥ 1 *che non abbia divisori propri (di grado maggiore di* 0*) si dice* irriducibile*. Un polinomio che non sia irriducibile si dice* riducibile*. Gli elementi di* $\mathbb{K}$ *si indicano spesso come* scalari*.*

Osservazione 2.11. [AAW27] *Se un polinomio* $f(x)\in\mathbb{K}[x]$ *di grado* ≥ 1 *è riducibile, dalla definizione di divisione esistono due polinomi* $g(x), h(x)\in\mathbb{K}[x]$ *di grado* ≥ 0 *tali che* $f(x)=g(x)\cdot h(x)$

Esempio 2.12. [AAA30]

- *Tutti i polinomi di grado* 1 *sono irriducibili, su qualunque rpo.*
- *Un polinomio* $p(x)=ax^2+bx+c$ *in* $\mathbb{R}[x]$
  1. *Se ha discriminante* $\Delta=b^2-4ac$ *negativo, è irriducibile.*

2. *Se ha discriminante Δ positivo, è riducibile n due fattori di grado 1(lineari) di molteplicità 1, e precisamente*

$$p(x) = \left(x - \frac{-b - \sqrt{\Delta}}{2}\right)\left(x - \frac{-b + \sqrt{\Delta}}{2}\right)$$

3. *Se ha discriminante Δ nullo, è riducibile con un fattore di grado 1 (lineare) (si dice che questo fattore ha molteplicità 2), e precisamente*

$$p(x) = \left(x + \frac{b}{2}\right)^2$$

- *$x^4 - 4$ è riducibile sia in $\mathbb{Q}[x]$ che in $\mathbb{R}[x]$, dato che $x^4 - 1 = (x^2 - 2)(x^2 + 2)$. Questa è una fattorizzazione in irriducibili su $\mathbb{Q}[x]$ ma non su $\mathbb{R}[x]$, mentre lo è la seguente*

$$x^4 - 4 = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)$$

dove i primi due fattori sono irriducibili in quanto di grado 1, mentre per il terzo lo è perchè ha Δ negativo.

Osservazione 2.13. *Nella divisibilià e per l'irriducibilià possiamo trascurare fattori invertibili (scalari).*

- *Il polinomio $2x - 2$ divide il polinomio $x^2 - 1 = (x + 1)(x - 1)$, dato che $x - 1 = \frac{1}{2} \cdot (2x - 2)$*
- *Il polinomio $2x - 2$ è irriducibile, dato che il polinomio $x - 1$ è irriducibile.*

Teorema 2.14 (Teorema Fattorizzazione Unica)**.** `[AAA28]` *Sia $f(x) \in \mathbb{K}[x]$. Allora esistono unici polinomi $f_1(x), \ldots, f_n(x) \in \mathbb{K}[x]$ irriducibili distinti e $\alpha_1, \ldots, \alpha_n \in \mathbb{N}^+$ (interi positivi) tali che*

$$f(x) = \prod_{i=1}^{n} f_i(x)^{\alpha_i} = f_1(x)^{\alpha_1} \cdots f_n(x)^{\alpha_n}$$

I polinomi $f_i(x)$ si dicono fattori irriducibili *di $f(x)$ e i naturali α_i sono le loro* molteplicità*.*

Esempio 2.15. `[AAA29]` *Dato $f(x) = x^4 - 1$, una sua fattorizzazione in irriducibli in $\mathbb{R}[x]$ è*

$$f(x) = (x - 1)(x + 1)(x^2 + 1)$$

Esempio 2.16. `[AAH29]` *Ricordando l'esercizio 1.13*

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

per la fattorizzazione unica, $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$.

Osservazione 2.17. `[AAA34]` *Per risolvere un equazione polinomiale in una variabile, fattrizzare il polinomio è un aiuto, spesso sostanziale.*

Problema 2.18. `[AAA35]` *Fattorizzare un polinomio. Se non è possibile, posso dire se il polinomio è irriducibile? Posso dire se due polinomi sono coprimi se non riesco a fattorizzarli?*

2.3 Radici e Ruffini

Definizione 2.19. `[AAA41]` *Sia* $f(x) = \sum_{i=0}^{n} a_i x^i$ *e* $c \in \mathbb{K}$. *Allora il numero reale*

$$f(c) = \sum_{i=0}^{n} a_i c^i$$

è detto valutazione *di* $f(x)$ *in* c.

Definizione 2.20. `[AAA42]` *Sia* $f(x) \in \mathbb{K}[x]$ *e* $a \in \mathbb{K}$. *Se* $f(a) = 0$ *allora* a *è detta* radice *del polinomio* $f(x)$.

Dalle sue radici possiamo trovare tutti e soli i fattori lineari di un polinomio sui razionali.

Teorema 2.21 (Teorema di Ruffini)**.** `[AAA45]` *Sia* $f(x)$ *un polinomio in* $\mathbb{K}[x]$ *e* $a \in \mathbb{K}$. *Allora*

$$f(a) = 0 \Leftrightarrow (x - a) \mid f(x)$$

Ovvero a *è una radice di* $f(x)$ *se e solo se* $x - a$ *è un fattore di* $f(x)$,

Osservazione 2.22. *Dato che ci sono infinite possibilità per le radici, abbiamo bisogno di un criterio che ci dica quali dobbiamo provare. Questo criterio esiste su* $\mathbb{Q}$ *ma non su* $\mathbb{R}$.

Teorema 2.23 (Teorema delle Radici)**.** `[AAA43]` *Sia*

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$$

un polinomio di grado n *(e quindi con* $a_n \neq 0$*) con coefficenti in* $\mathbb{Z}$. *Allora abbiamo che tutte le radici razionali sono date da un divisore del termine noto diviso un divisore del termine di testa. Ovvero, se* $b_1, \ldots, b_k$ *sono i divisori del termine di testa* $a_n \in \mathbb{Z}$ *e* $c_1, \ldots, c_p$ *i divisori del termine noto* a_0 *abbiamo che, per* $a \in \mathbb{Q}$

$$f(a) = 0 \Rightarrow a = \pm \frac{c_i}{b_j} \quad \text{per opportuni } i : 1 \ldots k, \quad j : 1 \ldots p$$

Esempio 2.24. `[AAA44]` *Cerchiamo le radici razionali del polinomio* $2x^3 - x^2 - 6x + 3$. *I divisori del termine di testa sono* $1, 2$. *I divisori del termine noto sono* $1, 3$. *Le possibili radici razionali sono quindi*

$$\pm\frac{1}{1} = \pm 1, \pm\frac{1}{2}, \pm\frac{3}{1} = \pm 3, \pm\frac{3}{2}$$

Vediamo quali delle possibili radici razionali è effettivamente radice, usando il Teorema di Ruffini

$$\begin{array}{ll} f(1) = 2 & f(-1) = 6 \\ f\left(\frac{1}{2}\right) = 0 & f\left(-\frac{1}{2}\right) = \frac{11}{2} \\ f(3) = 30 & f(-3) = -42 \\ f\left(\frac{3}{2}\right) = -\frac{3}{2} & f\left(-\frac{3}{2}\right) = 3 \end{array}$$

Quindi l'unica radice razionale è $\frac{1}{2}$ ed il nostro polnomio è diviso da $x - \frac{1}{2}$. Infatti

$$\begin{aligned} 2x^3 - x^2 - 6x + 3 &= \left(x - \frac{1}{2}\right)(2x^2 - 6) \\ &= \left(x - \frac{1}{2}\right)2(x^2 - 3) \\ &= (2x - 1)(x^2 - 3) \end{aligned}$$

Vediamo quindi che ci sono anche le due radici reali non razionali $\pm\sqrt{3}$, che non abbiamo potuto trovare col Teorema delle Radici 2.23.

2.4 Criterio di Eisenstein

Sui razionali, abbiamo un criterio parziale di di irriducibilità:

Teorema 2.25 (Criterio di Eisenstein)**.** `[AAA52]` *Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ di grado n. Allora se esiste $p \in \mathbb{N}$, primo tale che*

$$p \nmid a_n \quad p \mid a_{n-1}, \ldots, p \mid a_0 \quad e \quad p^2 \nmid a_0$$

il polinomio $f(x)$ è irriducibile su $\mathbb{Q}[x]$. Si dice che $f(x)$ è irriducibile per Eisenstein, con primo p.

Esempio 2.26. `[AAA53]` *Esaminiamo il polinomio $f(x) = 3x^5 - 6x^3 + 30 \in \mathbb{Q}[x]$. Vogliamo provare a verificarne l'irriducibilità col Criterio di Eisenstein. Esaminando il coefficenti $6, 30$, gli unici primi che li dividono entrambi sono $2, 3$. Dato che 3 divide il termine di testa, non fa al caso nostro. Dato che 2 non divide il termine di testa e 2^2 non divide il termine noto, $f(x)$ è irriducibile per Eisenstein, $p = 2$.*

Esempio 2.27. `[AAA54]`

1. *Il polinomio $f(x) = 3x^3 - 4x + 2$ è irriducibile su $\mathbb{Q}[x]$, dato che 2 è primo e che*

$$2 \nmid 3, \quad 2 \mid 4, \quad 2 \mid 2 \text{ e } 2^2 \nmid 2$$

2. *Il polinomio $f(x) = 3x^3 - 4x + 4$ è irriducibile su $\mathbb{Q}[x]$, ma non per Eisenstein dato non esiste un primo p che soddisfi le condisioni del Criterio. È irriducibile perchè per essere riducibile dovrebbe avere una radice razionale, ma le possibile radici sono*

$$\pm 1, \pm 2, \pm 4, \pm\frac{2}{3}, \pm\frac{1}{3}, \pm\frac{4}{3}$$

   nessuna delle quali è effetivamente una radice (verificare per esercizio).

3. *Il polinomio $x^2 - 5$ è irriducibile su $\mathbb{Q}[x]$, dato che 5 è primo e che*

$$5 \nmid 1, \quad 5 \mid 5 \quad e \quad 5^2 \nmid 5$$

4. *I polinomi della forma $x^n - p$, con p intero primo, sono irriducibili su $\mathbb{Q}$.*

5. *Quindi $\forall\ n \in \mathbb{N},\ n > 2 \quad \sqrt[n]{p} \notin \mathbb{Q}$.*

6. *La fattorizzazione $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ è in irriducibili su $\mathbb{Q}[x]$ per Eisenstein.*

Osservazione 2.28. `[AAA47]` *Notiamo che se $f(x) \in \mathbb{K}[x]$ e $f(a/b) = 0$, allora $(bx - a) \mid f(x)$.*

Osservazione 2.29. [AAA48] *Discende dal Teorema di Ruffini e dalla proposizione sulla divisione con resto per polinomi che un polinomio $p(x) \in \mathbb{K}[x]$ non nullo ha al più tante radici quanto è il suo grado.*

Osservazione 2.30. [AAA49] *Due polinomi $p(x), q(x) \in \mathbb{K}[x]$ di grado n con n radici uguali sono uguali a meno di un fattore invertibile.*

Esempio 2.31. [AAB55] *Il polinomio*

$$f(x) = \frac{5}{8}x^5 + \frac{1}{12} = \frac{1}{24}\left(15x^5 + 2\right)$$

è irriducibile su $\mathbb{Q}[x]$ dato che è il prodotto di un elemento invertibile e del polinomio $15x^5+2$ che è irriducibile per Eisenstein, $p = 2$.

Osservazione 2.32. [AAA56] *Un polinomio è irriducibile o meno a seconda del campo che consideriamo. Per esempio,*

$$(x^4 - 4) = (x^2 + 2)(x^2 - 2) = (x^2 + 2)(x - \sqrt{2})(x + \sqrt{2})$$

la prima è una fattorizzazione in irriducibili su $\mathbb{Q}[x]$, la seconda in $\mathbb{R}[x]$.

Esercizio 2.33. [AAA95] *[Proposto] Dimostrare che se $\mathbb{K}_1 \subset \mathbb{K}_2$ e $f(x)$ è irriducibile su $\mathbb{K}_2$ allora è irriducibile su $\mathbb{K}_1$. Il viceversa è falso.*

Definizione 2.34. [AAA88] *Sia $f(x) \in \mathbb{K}[x]$ con $LC(f(x)) = 1$ (il coefficente del termine di testa è 1). Allora il polinomio $f(x)$ si dice* monico.

Esempio 2.35. [AAA89] *Il polinomio $x^5 + 3x - 1$ è monico. Il polinomio $2x + 3$ non lo è.*

2.5 Massimo comun divisore, minimo comune multiplo

Definizione-Proposizione 2.36 (Massimo Comun Divisore, Minimo Comune Multiplo)**.** [AAA57] *Dati $f(x), g(x) \in \mathbb{K}$*

- *Il* massimo comun divisore *di $f(x), g(x)$ e' il polinomio monico di grado massimo tra quelli che dividono sia $f(x)$ che $g(x)$. Tale polinomio esiste a meno che entrambi $f(x)$ e $g(x)$ siano nulli. Si scrive* $\gcd(f(x), g(x))$.
- *Il* minimo comune multiplo *di $f(x), g(x)$ e' il polinomio monico di grado minimo tra quelli che sono divisi sia da $f(x)$ che da $g(x)$. Tale polinomio esiste sempre. Si scrive* $\operatorname{lcm}(f(x), g(x))$.
- *Notiamo che $\forall\ f(x) \in \mathbb{K}[x,]\ f(x) \neq 0$ $\gcd(f(x), 0) = f(x)$. (Tutti gli elementi di un anello dividono 0)*

Esempio 2.37. [AAZ58]

- $\gcd(3x - 3, 2x - 2) = x - 1$.
- $\gcd(x^2 - 4, x - 2) = x - 2$.
- $\gcd(x^2 + 1, x - 1) = 1$.
- $\gcd((x - 1)^2(x - 2), (x - 1)^3(x - 3)) = (x - 1)^2$.

Problema 2.38. [AAA58] *Come calcolare il massimo comun divisore di due polinomi?*

Come per il gcd in $\mathbb{Z}$, notiamo alcuni fatti utili.

Proposizione 2.39. [AAA59] *Siano*

$$f(x) = \prod_{i=1}^{n} f_i(x)^{\alpha_i} \quad e \quad g(x) = \prod_{i=1}^{m} g_i(x)^{\beta_i}$$

due polinomi in $\mathbb{K}[x]$*. Allora*

1. *Il massimo comun divisore di* $f(x), g(x)$ *è dato dal prodotto di tutti i fattori comuni ai due polinomi presi una sola volta con minimo esponente.*
2. *Il minimo comune multiplo di* $f(x), g(x)$ *è dato dal prodotto di tutti i fattori comuni e non comuni ai due polinomi presi una sola volta con massimo esponente.*

Esempio 2.40. [AAA60] *Dati i due polinomi*

$$h(x) = (x+1)^4(x-1)(x^2+1)^3 \qquad p(x) = (x+1)^2(x-1)^2(x^2+2)^3$$

abbiamo che

$$\begin{aligned}\gcd(h(x), p(x)) &= (x+1)^{\min(4,2)}(x-1)^{\min(1,2)} = (x+1)^2(x-1)\\ \operatorname{lcm}(h(x), p(x)) &= (x^2+1)^3(x^2+2)^3(x+1)^{\max(4,2)}(x-1)^{\max(1,2)}\\ &= (x^2+1)^3(x^2+2)^3(x+1)^4(x-1)^2\end{aligned}$$

Proposizione 2.41. [AAA82] *Conservando la notazione della proposizione precedente, notiamo alcuni fatti utili:*

1. *Notiamo che per ogni* $f(x), g(x) \in \mathbb{K}[x]$ *monici abbiamo che*

$$\gcd(f(x), g(x)) \cdot \operatorname{lcm}(f(x), g(x)) = f(x) \cdot g(x)$$

   Se $f(x), g(x)$ *non sono monici, l'uguaglianza vale a meno di un fattore invertibile.*

2. $\gcd(f(x), g(x)) = \gcd(g(x), f(x))$
3. *Dati* $f(x), g(x), h(x) \in \mathbb{K}[x]$ *possiamo definire*

$$\gcd(f(x), g(x), h(x)) = \gcd(\gcd(f(x), g(x)), h(x))$$

   Abbiamo altresì

$$\gcd(\gcd(f(x), g(x)), h(x)) = \gcd(f(x), \gcd(g(x), h(x)))$$

4. *Se* $f(x) = q(x)g(x) + r(x)$ *per opportuni* $q(x), r(x)$*, allora*

$$\gcd(f(x), g(x)) = \gcd(q(x)g(x) + r(x), g(x)) = \gcd(g(x), r(x))$$

Dimostrazione. Tutte queste proprietà discendono immediatamente dall'equivalenza delle tre definizioni del gcd. □

Problema 2.42. [AAA61] *Calcolare il* gcd *fattorizzando il polinomi è semplice, ma fattorizzare polinomi è difficile. Il problema è rilevante.*

Problema 2.43. [AAA62] *Risolvere in* $\mathbb{K}[x]$ *il sistema*

$$\begin{cases} 3x^4 + 3x^3 + x^2 - 2x - 2 = 0 \\ 3x^5 + x^3 + 3x^2 - 2x - 2 = 0 \end{cases}$$

Notiamo che e soluzioni del sistema sono tutte e sole le soluzioni comuni ai due polinomi. Per il teorema di Ruffini, i fattori lineari associati alle soluzioni sono tutti e soli i fattori lineari associati alle soluzioni che dividono entrambi i polinomi. Per definizione di gcd*, il prodotto di questi fattori divide il* gcd *dei due polinomi. Quindi*

$$\begin{cases} 3x^4 + 3x^3 + x^2 - 2x - 2 = 0 \\ 3x^5 + x^3 + 3x^2 - 2x - 2 = 0 \end{cases} \Leftrightarrow \gcd(3x^4 + 3x^3 + x^2 - 2x - 2, 3x^5 + x^3 + 3x^2 - 2x - 2) = 0$$

Il problema è calcolare questo gcd*.....*

2.6 Algoritmo Euclideo

Proposizione 2.44 (Algoritmo Euclideo)**.** [AAA63] *Dati* $f_0(x), f_1(x) \in \mathbb{K}[x]$*, con* $\deg f_0(x) \geq \deg f_1(x) > 0$*. Sia*

$$f_i(x) = q_i(x) f_{i+1}(x) + f_{i+2}(x)$$

la divisione con resto di $f_i(x)$ *rispetto a* $f_{i+1}(x)$*, per opportuni* $q_i(x)$*. La sequenza di coppie*

$$(f_i(x), f_{i+1}) \longrightarrow (f_{i+1}, f_{i+2}(x))$$

termina con una coppia $(g(x), 0)$*, e il* gcd *di ogni coppia è lo stesso, per cui* $\gcd(f_0(x), f_1(x)) = g(x)$*.*

Osservazione 2.45. [AAA83] *La definizione 2.36 e le proposizioni 2.39, 2.44 ci danno tre definizioni equivalenti di* gcd*. Possiamo usare caso per caso quella che ci viene più comoda.*

Un esempio di esecuzione dell'algoritmo euclideo sugli interi. È lo stesso meccanismo dei polinomi, ma la semplicità dei conti lo rende piu' comprensibile.

Esempio 2.46. [AAA93] *Calcoliamo* $\gcd(256, 211)$

$(256, 211)$	$256 = 211 + 45$
$(211, 45)$	$211 = 4 \cdot 45 + 31$
$(45, 31)$	$45 = 31 + 14$
$(31, 14)$	$31 = 2 \cdot 14 + 3$
$(14, 3)$	$31 = 4 \cdot 3 + 2$
$(3, 2)$	$3 = 2 + 1$
$(2, 1)$	$2 = 2 \cdot \boxed{1} + 0$
$(\boxed{1}, 0)$	$\Rightarrow \gcd(256, 211) = \boxed{1}$

Notiamo che appena è comparso $(45, 31)$ *avremmo poturo dire che* $\gcd(45, 31) = 1$*, dato che* 31 *è primo e* 45 *non è una potenza di* 31*. Avremmo anche potuto vededere immediatamente che* $\gcd(256, 211) = 1$ *dato che* $256 = 2^8$ *è una potenza di* 2*, e* 211 *è dispari.*

Esempio 2.47. [AAA64] *Sospettiamo gia' che il* $\gcd(x^6-1, x^5-1)$ *sia* $x-1$*. Verifichiamolo con l'Algoritmo Euclideo*

```
GCDPolyVerbose(x^6-1,x^5-1);

(x^6-1,x^5-1)
(x^6 - 1)=(x)*(x^5 - 1)+(x - 1)


(x^5-1,x - 1)
(x^5 - 1)=(x^4 + x^3 + x^2 + x + 1)*(x - 1)+(0)

(x - 1,0)
```

Quindi $\gcd(x^6-1, x^5-1) = x-1$

Esempio 2.48. [AAA65] *Calcoliamo* $\gcd(x^6-2, x^5-1)$.

```
GCDPolyVerbose(x^6-2,x^5-1);

(x^6-2,x^5-1)
(x^6 - 2)=(x)*(x^5 - 1)+(x - 2)

(x^5-1,x - 2)
(x^5 - 1)=(x^4 + 2x^3 + 4x^2 + 8x + 16)*(x - 2)+(31)

(x - 2,31)

(31,0)
```

Quindi $\gcd(x^6-2, x^5-1) = 31$ *o meglio* $\gcd(x^6-2, x^5-1) = 1$*. Ricordiamo che il* gcd *è monico, e in* $\mathbb{K}[x]$ *il numero* 31 *è invertibile, con inverso* $1/31$*.*

Proposizione 2.49. [AAA70] *Dati* $f(x), g(x), h(x) \in \mathbb{K}[x]$*,* $a \in \mathbb{K}$*,* $a \neq 0$*.*

1. $\gcd(f(x), ag(x)) = a \cdot \gcd(f(x), g(x)) = \gcd(f(x), g(x))$*. Ovvero possiamo, durante il calcolo del* gcd*, raccogliere e portare fuori scalari.*
2. $h(x) \mid \gcd(g(x)\cdot h(x), g(x)\cdot h(x))$*. Ovvero possiamo, durante il calcolo del* gcd*, raccogliere e portare fuori fattori comuni.*
3. *Se* $h(x) \in \mathbb{K}[x]$ *è coprimo con* $f(x)$*,* $g(x)$ *ho che*
$$\gcd(f(x), h(x)g(x)) = \gcd(f(x), g(x))$$
Posso quindi eliminare un fattore che sia coprimo con entrambi i polinomi.
4. *In* $\mathbb{K}[x]$ *un polinomio irriducibile non è coprimo solo con le sue potenze proprie. Quindi, un polinomio irriducibile è coprimo con ogni polinomio di grado minore del suo.*

Definizione 2.50. [AAA72] *Un polinomio* $f(x) \in \mathbb{K}[x]$ *che abbia fattorizzazione su* $\mathbb{K}[x]$ *in irriducibili distinti di molteplicità* 1*, ovvero*
$$\prod_{i=1}^{n} f_i(x)_i^{\alpha} \qquad \text{con } \alpha_1 = \cdots = \alpha_n = 1$$
si dice squarefree*.*

Definizione 2.51. [AAA73] *Dato* $f(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$ *definiamo come la* derivata FORMALE *di* $f(x)$ *il polinomio in* $\mathbb{K}[x]$

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1} = n a_n x^{n-1} + n - 1 a_{n-1} x^{n-2} + \cdots + a_1$$

Esempio 2.52. [AAA74]

$$(3x^5 + x^4 - 2x^3 + x^2 - x + 3)' = 15x^4 + 4x^3 - 6x^2 + 2x - 1$$

Proposizione 2.53. [AAA75] *Dati* $f(x), g(x) \in \mathbb{K}[x]$ *abbiamo che*

1. $(f(x) + g(x))' = f'(x) + g'(x)$.
2. $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.
3. $\deg f'(x) = \deg f(x) - 1$.
4. *La derivata di una costante è* 0.

Dimostrazione. In ogni caso, basta applicare la definizione di derivata formale e fare i conti □

2.7 Criterio della derivata

Teorema 2.54. [AAA76] *[Criterio della molteplicità o del* gcd*] Sia* $f(x) \in \mathbb{K}[x]$ *e una sua fattorizzazione in irriducibili su* $\mathbb{K}[x]$

$$f(x) = \prod_{i=1}^{n} f_i(x)^{\alpha_i}$$

Allora

1. $\gcd(f(x), f'(x)) = \prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$.
2. $f(x)$ *è squarefree se e solo se* $\gcd(f(x), f'(x)) = 1$.
3. *Il polinomio* $\frac{f(x)}{\gcd(f(x), f'(x))}$ *è squarefree, e ovviamente è un fattore di* $f(x)$*, come lo è* $\gcd(f(x), f'(x))$.

Dimostrazione non vista in classe.

1. Per le regole di derivazione del prodotto e della somma,

$$\begin{aligned} f'(x) &= (f_1(x)^{\alpha_1} \cdots f_n(x)^{\alpha_n})' \\ &= \alpha_1 f_1(x)^{\alpha_1 - 1} f_2(x)^{\alpha_2} \cdots f_n(x)^{\alpha_n} + \cdots \\ &\qquad + f_1(x)^{\alpha_1} \alpha_2 f_2(x)^{\alpha_2 - 1} f_3(x)^{\alpha_3} \cdots f_n(x)^{\alpha_n} + \cdots \\ &\qquad + f_1(x)^{\alpha_1} \cdots f_{n-1}(x)^{\alpha_{n-1}} \alpha_n f_n(x)^{\alpha_n - 1} \\ &= \prod_{i=1}^{n} f_i(x)^{\alpha_i - 1} \cdot \sum_{i=1}^{n} \left(\prod_{j \neq i} f_j^{\alpha_j} \right) \end{aligned} \tag{2.1}$$

raccogliendo il fattore $\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$ comune a tutti gli addendi. Vediamo che

- il polinomio $\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$ divide sia $f(x)$, per costruzione, che $f'(x)$.
- Si può dimostrare [Lasciato per esercizio] che un polinomio che divida sia $f(x)$ che $f'(x)$ deve necessariamente essere diviso da $\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$ e che quindi $\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$ è il divisore comune di grado maggiore possibile ed abbiamo

$$\gcd(f(x), f'(x)) = \prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$$

2. Abbiamo che

$$\begin{aligned} \frac{f(x)}{\gcd(f(x), f'(x))} &= \frac{\prod_{i=1}^{n} f_i(x)^{\alpha_i}}{\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}} \\ &= f_1(x) \cdots f_n(x) \end{aligned}$$

   e quindi $f(x)$ è squarefree se e solo se $\gcd(f(x), f'(x)) = 1$.

3. Segue immediatamente da quanto sopra.

□

Definizione-Proposizione 2.55. `[AAA31]` *Se due polinomi in $\mathbb{K}[x]$ non hanno fattori irriducibili comuni, allora $f(x), g(x)$ sono detti* coprimi. *Notiamo che $f(x), g(x)$ sono coprimi se e solo se* $\gcd(f(x), g(x)) = 1$.

Definizione 2.56. `[AAA50]` *Sia $f(x) \in \mathbb{K}[x]$ e $a \in \mathbb{K}$ una sua radice. Allora a è detta* radice di molteplicità *k del polinomio $f(x)$ se e solo se il fattore irriducibile $x - a$ ha molteplicità k nella fattorizzazione in irridubibili di $f(x)$. Alternativamente, se e solo se*

$$(x-a)^k \mid f(x) \text{ e } (x-a)^{k+1} \nmid f(x)$$

.

Esempio 2.57. `[AAA51]` *Dato $f(x) = x^2(x-1)(x+2)^3$, abbiamo che $f(x)$ ha tre radici, $0, 1, -2$, di molteplicità rispettiva $2, 1, 3$.*

Esempio 2.58. `[AAA33]` *I polinomi*

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

sono coprimi. I polinomi

$$x^4 - 1, 7x^3 - 7$$

non lo sono, visto che hanno a fattore comune $x - 1$.

Esempio 2.59. `[AAY33]` $\gcd(x^5 - 1, 7x^3 - 7) = \gcd(x^5 - 1, x^3 - 1)$ *dato che possiamo rimuovere il fattore invertibile 7 nel secondo polinomio*

$$\gcd(x^5 - 1, x^3 - 1) = (x - 1)$$

```
GCDPolyVerbose(x^5-1,x^3-1);
(x^5 - 1)=(x^2)*(x^3 - 1)+(x^2 - 1)
(x^3 - 1)=(x)*(x^2 - 1)+(x - 1)
(x^2 - 1)=(x + 1)*(x - 1)+(0)
```

```
Quindi

(x^5 - 1,x^3 - 1)
(x^3 - 1,x^2 - 1)
(x^2 - 1,x-1)
(x-1,0)
```

Esempio 2.60. `[AAG33]` $\gcd((x^4+x^3+x^2+x+1, x^2+x+1) = 1$ *dato che*

```
GCDPolyVerbose(x^4 + x^3 + x^2 + x + 1,x^2+x+1);
(x^4 + x^3 + x^2 + x + 1)=(x^2)*(x^2 + x + 1)+(x + 1)
(x^2 + x + 1)=(x)*(x + 1)+(1)
(x + 1)=(x + 1)*(1)+(0)

Quindi

(x^4 + x^3 + x^2 + x + 1,x^2+x+1)
(x^2 + x + 1,x + 1)
(x + 1,1)
(1,0)
```

e $\gcd(x^4+x^3+x^2+x+1, x^2+x+1) = 1$. *Abbiamo che*

$$\gcd(x^5-1, x^3-1) = (x-1)\gcd(x^4+x^3+x^2+x+1, x^2+x+1) = (x-1)$$