*** V ***

RICHIAMI

Definizione 1. L'anello dei polinomi $K[x]$ (con coefficienti nel campo K).

- i) $K[x] = \left\{ f(x) = \sum_{r \geq 0} a_r x^r \mid a_r \in K \ \forall r \in \mathbb{N} \text{ e } \#\{r \in \mathbb{N} \mid a_r \neq 0\} < \infty \right\}$;
- ii) $\sum_{r \geq 0} a_r x^r + \sum_{r \geq 0} b_r x^r = \sum_{r \geq 0} (a_r + b_r) x^r$;
- iii) $\left(\sum_{r \geq 0} a_r x^r \right) \left(\sum_{r \geq 0} b_r x^r \right) = \sum_{r \geq 0} \sum_{s+t=r} (a_s b_t) x^r$.

Definizione 2. Il grado.

Il grado è la funzione $deg : K[x] \setminus \{0\} \rightarrow \mathbb{N}$ definita nel modo seguente:

$$deg\left(\sum_{r \geq 0} a_r x^r\right) = \max\{r \in \mathbb{N} \mid a_r \neq 0\}.$$

Osservazione

$K[x]$ è un dominio di integrità.

Più precisamente $f, g \neq 0 \Rightarrow fg \neq 0$ e $deg(fg) = deg(f) + deg(g)$.

$K \subsetneq K[x]$.

$K[x]^* = K^*$.

K non è un campo.

$f, g, f + g \neq 0 \Rightarrow deg(f + g) \leq \max\{deg(f), deg(g)\}$.

$\forall f, g \in K[x]$ con $g \neq 0 \exists q, r \in K[x]$ tali che $f = gq + r$ e $r = 0$ oppure $deg(r) < deg(g)$.

Definizione 3

$I \subseteq K[x]$ si dice *ideale* se:

- i) $I \neq \emptyset$;
- ii) $f, g \in I \Rightarrow f + g \in I$;
- iii) $f \in I, g \in K[x] \Rightarrow fg \in I$.

Osservazione

$I \subseteq K[x]$ ideale $\Rightarrow 0 \in I$.

$\{0\}$ e $K[x]$ sono ideali di $K[x]$.

Sia $I \subseteq K[x]$ un ideale; allora $I = K[x] \Leftrightarrow 1 \in I$.

Sia $f \in K[x]$; l'insieme $\{fg \mid g \in K[x]\}$ dei multipli di f è un ideale di $K[x]$, e si indica (f) .

La nozione di ideale generalizza quella di divisibilità:

$$f \mid g \Leftrightarrow (g) \subseteq (f); \quad (f) = (g) \Leftrightarrow \exists a \in K^* \text{ tale che } g = af.$$

Per ogni ideale $I \subseteq K[x]$ esiste $f \in I$ tale che $I = (f)$.

Esempio

Dati $f, g \in K[x]$, l'insieme $\{fp + gq | p, q \in K[x]\}$ è un ideale di $K[x]$ e si indica (f, g) .

$(f, g) = (d) \Leftrightarrow d$ è $MCD(f, g)$.

Osservazione

$(f, g) = 1, f|gh \Rightarrow f|h$.

Definizione 4

Sia $f \in K[x]$ non nullo e non invertibile. f si dice:

- i) irriducibile se $f = gh \Rightarrow g$ invertibile oppure h invertibile.
- ii) primo se $f|gh \Rightarrow f|g$ oppure $f|h$.

Osservazione

$f \in K[x]$ è irriducibile se e solo se è primo.

Teorema

$K[x]$ è un dominio a fattorizzazione unica, cioè:

- i) $\forall f \in K[x] \setminus \{0\} \exists r \in \mathbb{N}$ e $a \in K^*$ (se $r = 0$), $p_1, \dots, p_r \in K[x]$ irriducibili tali che

$$f = p_1 \cdot \dots \cdot p_r.$$

- ii) Se $p_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_s$ con p_i, q_j irriducibili per ogni i e j allora

$$r = s \text{ e a meno di cambio di ordine } p_i = q_i \forall i.$$

ESERCIZI sui POLINOMI a COEFFICIENTI in un CAMPO

- 1) Dire quali dei seguenti polinomi siano divisibili per $x + 3$ e quali siano divisibili per $x - i$:

$$x^5 + 3x^4, \quad x^5 + 3x^4 + x^3 + 3x^2, \quad x^3 + 2x + 9, \quad x^3 + 2x^2 + 9, \quad x - 3 + i.$$

- 2) Siano $f(x), g(x)$ i due polinomi definiti sotto.
Determinare $q(x), r(x)$ tali che

$$f(x) = g(x)q(x) + r(x)$$

con $\deg(r(x)) < \deg(g(x))$ oppure $r(x) = 0$.

Dire se $f(x)$ sia divisibile per $g(x)$.

Calcolare il MCD tra $f(x)$ e $g(x)$.

Trovare un polinomio $h(x)$ tale che

$$\left\{ a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in K[x] \right\} = (h(x)).$$

Scrivere $h(x)$ nella forma $h(x) = a(x)f(x) + b(x)g(x)$.

- i) $f(x) = x^5 - 3x^4 + 2x^2 - 4$ e $g(x) = x - 3$
- ii) $f(x) = x^5 - 2x^4 + 3x^2 - 4$ e $g(x) = x^2 + x - 2$;
- iii) $f(x) = x^3 + 2x^2 + 4x + 8$ e $g(x) = x^3 - 3x^2 + 4x - 12$;
- iv) $f(x) = x^3 + 2x^2 + 4x + 8$ e $g(x) = x^2 - 5x - 14$;
- v) $f(x) = x^3 + 2x^2 - x - 2$ e $g(x) = x^2 + x - 2$;
- vi) $f(x) = x^4 + 2x^2 + 4x + 2$ e $g(x) = x^3 - 3x + 1$;
- vii) $f(x) = x^4 + x^3 - x^2 + 2x + 3$ e $g(x) = x^3 + 3x^2 - 2$;
- viii) $f(x) = x^7 - 9x^6 + 14x^5 - 10x^4 + 2x^3 + 2$ e $g(x) = x^5 + x^4 + 4x^3 - 2$.

3) Siano $p(x), q(x), a(x), b(x)$ polinomi. Dimostrare che:

- i) $MCD(p(x), q(x)) \mid MCD(a(x)p(x) + b(x)q(x), q(x))$;
- ii) nel punto i) in genere non vale l'uguale;
- iii) $MCD(p(x), q(x)) = MCD(p(x) + a(x)q(x), q(x))$.

4) Sia $n > 0$; fattorizzare il polinomio $x^n - 1$ in $\mathbb{C}[x]$.

5) Fattorizzare i seguenti polinomi e trovarne tutti i divisori in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$:

$$x^3 + 2x, \quad x^3 + 2, \quad x^4 + x^3 - x^2 + x - 2, \quad x^4 + x^3 + x^2 + 3x - 6.$$

6) Fattorizzare i polinomi $x^4 + 4$, $x^4 + 2$, $x^4 + 1$ in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$.

7) Sia $p(x) \in \mathbb{R}[x]$ tale che $p(x) \mid x^4 + x^2 + 1$ e $0 < \deg(p(x)) < 4$.

Dire perché un tale $p(x)$ esiste.

Dimostrare che $x^4 + x^2 + 1 = p(x)p(-x)$ e determinare $p(x)$.

Dire se $p(x) \in \mathbb{Q}[x]$.

Fattorizzare $x^4 + x^2 + 1$ in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$.

8) Sia $p(x) \in \mathbb{R}[x]$ un fattore irriducibile di $x^4 - 2x^2 + 1$.

Determinare $p(x)p(-x)$; è vero che $x^4 - 2x^2 + 1 = p(x)p(-x)$?

È vero che esiste $q(x) \in \mathbb{Q}[x]$ tale che $x^4 - 2x^2 + 1 = q(x)q(-x)$?

Fattorizzare $x^4 - 2x^2 + 1$.

9) Sia $p(x) = x^5 - 4x^3 + ix^2 - x + 6 \in \mathbb{C}[x]$ e siano $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \in \mathbb{C}$ le radici di $p(x)$. Calcolare $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5$ e $\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5$.

10) Siano n un intero positivo e $\alpha > 0$. Dimostrare che l'insieme

$$\left\{ x \in \mathbb{R} \mid \sum_{k=1}^n \frac{k}{x-k} \geq \alpha \right\}$$

è l'unione di un numero finito di intervalli disgiunti, e calcolare la somma delle lunghezze di tali intervalli.

***** Il teorema di Fermat per polinomi *****

Il teorema di Fermat afferma che non esiste l'analogo delle terne pitagoriche per $n > 2$. Più precisamente se $n > 2$ l'equazione

$$x^n + y^n = z^n$$

non ha soluzioni intere non banali, dove le soluzioni banali sono le seguenti:

- i) $x = 0, y = z$;
- ii) $y = 0, x = z$;
- iii) $x = 0, y = -z$ (solo nel caso n pari);
- iv) $y = 0, x = -z$ (solo nel caso n pari);
- v) $z = 0, x = -y$ (solo nel caso n dispari).

Il teorema di Fermat è stato dimostrato nel 1994 da Wiles, più di 3 secoli dopo la morte di Fermat, ed è un teorema molto difficile.

Gli esercizi che seguono conducono a dimostrare l'analogo del teorema di Fermat per i polinomi a coefficienti in $\mathbb{C}$.

11) Siano $n \geq 2, a, b \in \mathbb{C}$; dimostrare che esiste $c \in \mathbb{C}$ tale che $a^n + b^n = c^n$.

12) Siano $n \geq 2$ e $f, g, h \in \mathbb{C}[x]$ tali che $f^n + g^n = h^n$. Dimostrare che

$$MCD(f, g) = MCD(f, h) = MCD(g, h) = MCD(f, g, h).$$

13) Ripercorrere lo studio delle terne pitagoriche per costruire tutte le terne di polinomi $f, g, h \in \mathbb{C}[x]$ primi tra loro tali che $f^2 + g^2 = h^2$.

14) Sia $\omega \in \mathbb{C}$ tale che $\omega^n = -1$. Osservare che la funzione

$$(f, g, h) \mapsto (f, g, \omega h)$$

determina una corrispondenza biunivoca tra le terne di polinomi $f, g, h \in \mathbb{C}[x]$ tali che $f^n + g^n + h^n = 0$ e le terne di polinomi $f, g, h \in \mathbb{C}[x]$ tali che $f^n + g^n = h^n$.

Più in generale osservare che una combinazione lineare nulla con coefficienti non nulli $af^n + bg^n + ch^n = 0$ determina una terna di polinomi αf , βg , γh tali che $(\alpha f)^n + (\beta g)^n = (\gamma h)^n$.

15) Siano $n \geq 2$, $h, g \in \mathbb{C}[x]$ primi tra loro con $\deg(h) = \deg(g) = d$. Fattorizzare il polinomio $h^n - g^n \in \mathbb{C}[x, y]$ come prodotto di n polinomi primi tra loro di cui almeno $n - 1$ di grado d ; qual è il grado dell' n -esimo fattore?

16) (Teorema di Fermat per polinomi) Siano $n > 2$, $f, g, h \in \mathbb{C}[x]$ primi tra loro tali che $f^n + g^n = h^n$.

Osservare che si può supporre $\deg(h) = \deg(g) \geq \deg(f)$: perché?

Dimostrare che f , g e h sono costanti.

[Suggerimento: procedere per induzione su $\deg(f) + \deg(g) + \deg(h)$].