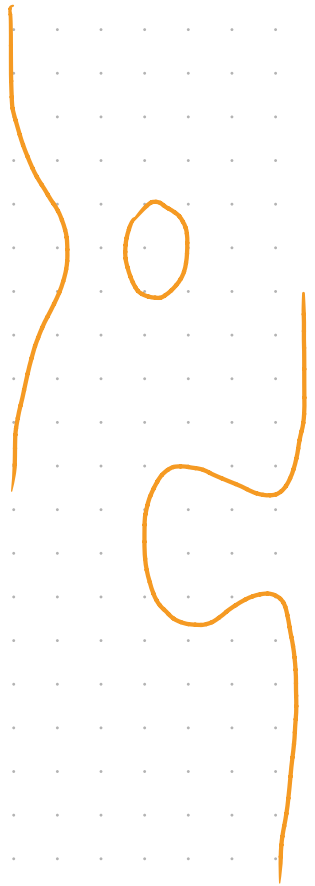
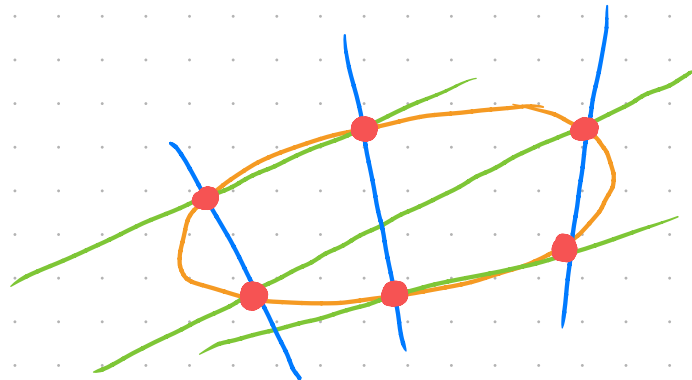
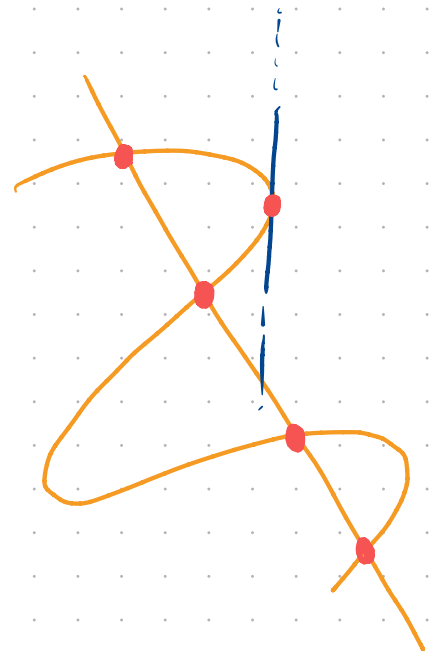




Benvenuti al corso di:

Istituzioni di algebra & geometria



§2: Preliminari di Algebra & Geometria

$n \in \mathbb{N}$
dimensione $A_K^n :=$ SPAZIO AFFINE CANONICO o STANDARD
 n -DIMENSIONALE sul campo K

con sistema di riferimento affine standard o canonico:

$$O := (0, \dots, 0)$$

$$B := \{e_1, e_2, \dots, e_n\}$$

$\mathbb{P}_K^n := \frac{K^{n+1} \setminus \{0\}}{\sim} =$ SPAZIO PROIETTIVO CANONICO
o STANDARD n -DIMENSIONALE
sul campo K

$v \sim w \iff w = \exists \lambda \in K^\times \cdot v$

con sistema di riferimento proiettivo standard o canonico:

$$(P_0, \dots, P_{n+1}) = ([e_0], [e_1], \dots, [e_n], [\sum_{i=0}^n e_i])$$

con $\{e_i\}_{i=0}^n$ base canonica di K^{n+1}

$(1:0:0:\dots:0)$ $(0:0:\dots:1)$ $(1:1:\dots:1)$

§ 2.3. Anello di Polinomi

anello, in questo corso campo

DEF $0 \neq f \in R[x_1, \dots, x_n]$ **IRRIDUCIBILE** $\Leftrightarrow \nexists f^{-1} \wedge (f = g \cdot h \Rightarrow \exists g^{-1} \vee \exists h^{-1})$

Esempi:

- 1) $f = 5 \in K[x_1, x_2, x_3]$ **RIDUCIBILE** (i.e. NON IRRIDUCIBILE), $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- 2) $f = x_1 + 1 \in K[x_1, x_2]$ **IRRIDUCIBILE** per $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- 3) $f = x_1^2 + 1 \in K[x_1]$ **IRRID** per $K = \mathbb{Q}, \mathbb{R}$ **MA RIDUCIBILE**
per $K = \mathbb{C}$ perché $f(x_1) = (x_1 - i)(x_1 + i) \in \mathbb{C}[x_1]$
 $\begin{matrix} g'' & & h \\ \uparrow & & \uparrow \\ \text{nessuno dei quali} \\ & & \text{è invertibile in } \mathbb{C}[x_1]! \end{matrix}$

Concetto chiave: la **RIDUCIBILITÀ / IRRIDUCIBILITÀ** di un polinomio **DIPENDE DAL CAMPO DEI COEFFICIENTI**
(• eventualmente anello)

(DEF) $R[x_1, \dots, x_n]$ è U.F.D. $\Leftrightarrow f \in R[x_1, \dots, x_n] \Rightarrow$

anello *ie. DOMINIO a FATTORIZZAZIONE UNICA*

f si DECOMPONE UNIVOCAMENTE come

$\exists \mu_i$ è detto MOLTEPLICITÀ ALGEBRICA del fattore $f_i \in R[x_1, \dots, x_n]$

$f = f_1^{\mu_1} \cdot \dots \cdot f_r^{\mu_r}$

a meno di permutazione dei fattori e moltiplicazione per elementi invertibili

dette COMPONENTI IRRIDUCIBILI di f

usuale moltiplicazione di polinomi

dove $f_i = f_i(x_1, \dots, x_n)$ sono IRRIDUCIBILI in $R[x_1, \dots, x_n]$,
sono a due a due COPRIMI (i.e. $\text{GCD} \equiv 1 \in R[x_1, \dots, x_n]$)

Inoltre:

f RIDOTTO $\Leftrightarrow \mu_i = 1 \quad \forall i = 1, \dots, r$

f HA UN' UNICA COMPONENTE IRRIDUCIBILE $\Leftrightarrow r = 1$

f IRRIDUCIBILE $\Leftrightarrow r = 1 \wedge \mu_1 = 1$

compatibile con le DEF precedenti in caso di UFD

DOMANDA: QUANDO $R[x_1, \dots, x_n]$ è UFD?

(LEMMA di GAUSS): $R \text{ UFD} \Rightarrow R[x_1] \text{ UFD}$ ← QUINDI IMPLICA ANCHE $R[x_1, \dots, x_n]$ UFD

Quindi la risposta è: almeno ogni qualvolta R stesso è UFD.
In particolare **OGNI CAMPO K è UFD $\Rightarrow K[x_1, \dots, x_n]$ UFD.**

Controesempio: $\mathbb{Z}/12\mathbb{Z} \ni [0] = [2] \cdot [6] = [3] \cdot [4]$ ← TUTTI ZERO DIVISORI QUINDI NON INVERTIBILI

↑ ANELLO MA NON UFD (E NON CAMPO, 12 NON PRIMO)

↑ DUE DECOMPOSIZIONI DISTINTE IN IRRIDUCIBILI

Un esempio notevole: $f(x) := x^4 + 1 \in K[x]$

(PROP) f IRRIDUCIBILE sul campo $K = \mathbb{Q}$ e RIDUCIBILE sui campi $K = \mathbb{R}, \mathbb{C}$ e su ogni campo finito $K = \mathbb{F}_p^n$ con p primo

Dim: *anche se non lo troviamo deve esistere per il TEOREMA FONDAM. DELL'ALGEBRA!*

- $K = \mathbb{C} \Rightarrow f(x) = \prod_{k=1}^4 (x - e^{i(2k-1)\pi/4}) \in \mathbb{C}[x]$

- $K = \mathbb{R} \Rightarrow f(x) = (x^2 + \sqrt{2} \cdot x + 1) \cdot (x^2 - \sqrt{2} \cdot x + 1) \in \mathbb{R}[x]$

- $K = \mathbb{F}_p^n$ VEDI NOTE

*entrambi non invertibili perché non costanti, non nulli, e irriducibili.
Non è scontato che esistano per $\mathbb{R}[x]$!
(perché non abbiamo il THM FOND. ALG. per $\mathbb{R}$).*

- $K = \mathbb{Q} \Rightarrow f(x) = g(x) \cdot h(x)$ per assurdo g, h entrambi irriducibili $\Rightarrow \deg(g) = \deg(h) = 2$ (se $\deg(g) = 1 \Rightarrow$ esisterebbe radice razionale di $f(x) \Rightarrow g \cdot h$ è fattorizzabile in IRRIDUCIBILI, ma $\mathbb{R}[x]$ è UFD $\Rightarrow g(x), h(x) = x^2 \pm \sqrt{2} \cdot x + 1$ per unicità $\Rightarrow g, h \notin \mathbb{Q}[x]$

OSS $K = \overline{K} \Rightarrow |K| = +\infty$ (ogni campo algebricamente chiuso ha infinito elementi)

Dim.: se per assurdo $K = \{\alpha_1, \dots, \alpha_m\}$, $m \geq 1$, allora

$$f(x) := \prod_{k=1}^m (x - \alpha_k) + 1_K \in K[x]$$

Allora $f(t) = 1_K \quad \forall t \in K \Rightarrow f$ ha grado positivo e non ha radici in $K \Rightarrow K \neq \overline{K}$ contraddizione $\square$

§ 2.3.1. Polinomi omogenei

(DEF) $K[x_0, x_1, \dots, x_n]_d :=$ INSIEME POLI di GRADO d nelle x_i

Esempio:

$$F(x_0, x_1, x_2) := \underbrace{x_0^4}_{\substack{\uparrow n \geq 0 \\ \uparrow d \geq 0}} - 2x_0x_1x_2 + \underbrace{x_1^2x_2}_{\substack{\uparrow \\ \uparrow}} - x_2^3 + \underbrace{x_0x_1 + 8x_2^2}_{\substack{\uparrow \\ \uparrow}} - 3x_0 + 5x_1 + 7x_2 - 1$$

$\uparrow$ perdiamo la struttura di anello! cosa rimane?

$\uparrow$ $\uparrow$ $\uparrow$ $\uparrow$ $\uparrow$ $\uparrow$

$\mathbb{K}[x_0, x_1, x_2]_4$ $\mathbb{K}[x_0, x_1, x_2]_4$ $\mathbb{K}[x_0, x_1, x_2]_4$ $\mathbb{K}[x_0, x_1, x_2]_4$ $\mathbb{K}[x_0, x_1, x_2]_4$ $\mathbb{K}[x_0, x_1, x_2]_4$

$$F = F_4 + F_3 + F_2 + F_1 + F_0$$

$\uparrow$ $\uparrow$ $\uparrow$ $\uparrow$ $\uparrow$

"la parte omogenea di grado quattro" "grado 3" "...grado 2" ...

Ogni polinomio si può sempre decomporre nella somma delle sue **COMPONENTI OMOGENEE** raccogliendo i termini grado per grado.

(DEF) $F \in K[x_0, \dots, x_n]_d$ è **OMOGENEO** $\Leftrightarrow$ la sua decomposizione in componenti omogenee ha un unico termine: $F = F_i$ $\exists i \in \mathbb{N}$ (e immediatamente abbiamo $i = d$).

(LEMMA) Let $d \geq 1$. cosa succede per $d=0$? Che grado ha il polinomio nullo?

$$\underbrace{F \in K[x_0, \dots, x_n]_d}_{\text{OMOGENEO}} \iff \underbrace{F(tx_0, \dots, tx_n) = t^d F(x_0, \dots, x_n)}_{\substack{\cap \\ K[x_0, \dots, x_n, t]}}$$

Dim.: È sufficiente testare la condizione su un singolo monomio (ogni monomio è omogeneo)

$$t^d F(x_0, \dots, x_n) = \alpha \cdot x_0^{d_0} \cdots x_n^{d_n} t^d = \alpha \cdot (tx_0)^{d_0} \cdots (tx_n)^{d_n} = F(x_0, \dots, x_n)$$

$\uparrow$ let $F := \alpha \cdot x_0^{d_0} \cdots x_n^{d_n}$
 $\uparrow$ $d = d_0 + \dots + d_n$

ed è chiaro che vale per più monomi $\iff$ hanno lo stesso grado
 $\iff$ appartengono allo stesso termine omogeneo nella decomposz.
 $\iff$ la decomposz. ha un unico termine omogeneo $\iff F$ omogeneo

□

OSS

$$\dim_{\mathbb{K}} (\mathbb{K}[x_0, x_1, \dots, x_n]_d) = \binom{n+d}{d}$$

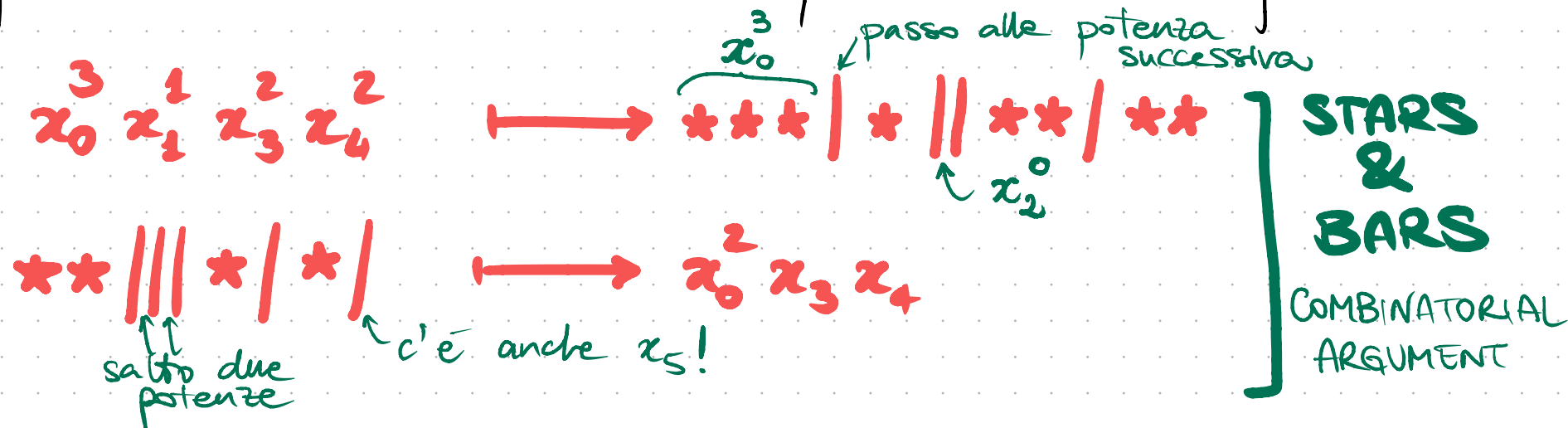
quindi bisogna mostrare che questi monomi sono in numero $\binom{n+d}{d}$!

Come spazio vettoriale!

$$\left\{ \sum_{\substack{\vec{d} \\ \sum d_i = d}} \alpha_{\vec{d}} \prod_{i=0}^n x_i^{d_i} \mid \alpha_{\vec{d}} \in \mathbb{K} \right\} \Rightarrow \mathcal{B} := \left\{ \prod_{i=0}^n x_i^{d_i} \mid \sum d_i = d \right\}$$

base

Dim.: Basta stabilire una biezione tra i monomi monici di grado $= d$ in $n+1$ variabili e qualcosa che sia facile contare:



Allora esiste una **BIEZIONE** tra monomi monici $\deg=d$ in $x_0, \dots, x_n$ e **STRINGHE** di d **STELLE** ed $n+1-1=n$ **BARRE**. Ogni stringa è identificata dalla scelta di d stelle su $d+n$ oggetti, quindi sono in totale binomiale $\binom{n+d}{d}$ $\square$

§ 2.3.2. Teorema di Vieta

$$e_0(x_1, \dots, x_n) := 1$$

$$e_1(x_1, \dots, x_n) := x_1 + \dots + x_n$$

$$e_2(x_1, \dots, x_n) := x_1 x_2 + x_1 x_3 + \dots + x_1 x_n + x_2 x_3 + \dots + x_2 x_n + \dots + x_{n-1} x_n$$

$$e_3(x_1, \dots, x_n) := x_1 x_2 x_3 + x_1 x_2 x_4 + \dots + x_1 x_2 x_n + \dots + x_{n-2} x_{n-1} x_n$$

⋮

$$e_{n-1}(x_1, \dots, x_n) := x_1 x_2 \cdots x_{n-1} + x_1 x_2 \cdots x_{n-2} x_n + \dots + x_2 x_3 \cdots x_n$$

$$e_n(x_1, \dots, x_n) := x_1 x_2 \cdots x_n$$

$$e_{n+1}(x_1, \dots, x_n) := 0$$

$$e_{n+2}(x_1, \dots, x_n) := 0$$

nelle variabili
 $x_1, \dots, x_n$ e a
coefficienti nel
campo K

DEF L' i -ESIMO POLINOMIO SIMMETRICO ELEMENTARE e_i

$$e_i(x_1, \dots, x_n) := \sum_{1 \leq j_1 < \dots < j_i \leq n} x_{j_1} x_{j_2} \cdots x_{j_i} \in K[x_1, x_2, \dots, x_n]_i$$

$i \geq 1$, poi $e_0 := 1$

grado = i

(THM) [VIETA, 1579] $\mathbb{K} = \overline{\mathbb{K}}$. $f(x) := \underbrace{\sum_{j=0}^d a_j x^j}_{\text{forma standard polinomiale}} = a_d \cdot \underbrace{\prod_{j=1}^d (x - \alpha_j)}_{\text{forma fattorizzata}} \in \mathbb{K}[x]$

Consideriamo i coefficienti a_j
come FUNZIONI DELLE RADICI α_j

$$a_j = a_j(\alpha_i) = a_d \cdot (-1)^{d-j} \cdot e_{d-j}(\alpha_1, \dots, \alpha_d)$$

Dim.: per espansione del prodotto della fattorizzazione $\square$

Esempio: $d=3$.

$$\begin{aligned} f(x) &= 5(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \\ &\downarrow \\ &= 5x^3 + (-5) \underbrace{(\alpha_1 + \alpha_2 + \alpha_3)}_{= e_1(\alpha_1, \alpha_2, \alpha_3)} x^2 + 5 \underbrace{(\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3)}_{= e_2(\alpha_1, \alpha_2, \alpha_3)} x + (-5) \underbrace{\alpha_1 \alpha_2 \alpha_3}_{= e_3(\alpha_1, \alpha_2, \alpha_3)} \end{aligned}$$

$\uparrow$
 $1 = e_0(\alpha_1, \alpha_2, \alpha_3)$

Domande:

- Come funziona per $f(x)$ di grado 2?
- Quanti termini ha $e_i(x_1, \dots, x_n)$?
- Esiste un polinomio simmetrico che ha $\binom{n+i}{i}$ termini?
Quante basi di polinomi simmetrici esistono?