

Istituzioni di Algebra e Geometria

1. Nozioni preliminari

1.1. Geometria affine

Def. uno spazio affine su uno spazio vettoriale V su un campo K è un insieme A , non-noto, assieme a un'applicazione

$$t: A \times A \rightarrow V$$

tale per cui:

1. $\forall P, Q, R \in A$, si ha $t(P, Q) + t(Q, R) = t(P, R)$

2. $\forall P \in A$, l'applicazione

$$t(P, \cdot): A \rightarrow V$$

$$Q \mapsto t(P, Q)$$

è biettiva

gli elementi di A sono detti punti; talvolta si utilizza la notazione $\overrightarrow{PQ}$ per indicare l'elemento $t(P, Q)$

Def. se A uno spazio affine su uno spazio vettoriale V ; allora poniamo $\dim A := \dim V$

In questo corso avremo sempre a che fare con spazi affini di

dimensione finita.

Def. sia K un campo, sia $n \in \mathbb{N}$ e $V := K^n$; consideriamo l'insieme $A := K^n$ e notiamo che possiamo dotarlo della struttura di uno spazio affine su V , definendo:

$$t: A \times A \longrightarrow V$$

$$(a_1, \dots, a_n), (b_1, \dots, b_n) \longmapsto \begin{pmatrix} b_1 - a_1 \\ \vdots \\ b_n - a_n \end{pmatrix}$$

(notiamo che indichiamo gli elementi di A come vettori riga, mentre gli elementi di V come vettori colonna)

questo spazio affine è detto spazio affine standard, ed è denotato con A_K^n .

Def. sia A uno spazio affine su V e sia $O \in A$ e $\{v_1, \dots, v_n\}$ una base di V ; lo coppia $(O, \{v_1, \dots, v_n\})$ è detto un referimento affine per A ; dato $P \in A$, le coordinate del vettore $\overrightarrow{OP}$ rispetto alla base $\{v_1, \dots, v_n\}$ sono dette le coordinate affini di P rispetto al sistema di referimento affine $(O, \{v_1, \dots, v_n\})$;

quando $A = K^n$ è lo spazio affine standard, e scegliamo $O = (0, \dots, 0)$ e $\{v_1, \dots, v_n\} = \{e_1, \dots, e_n\}$ la base

standard di $V = K^n$, allora otteniamo il riferimento affine standard; per esso, se $P \in A_K^n$ e $P = (p_1, \dots, p_n)$, allora $\overrightarrow{OP} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$ e dunque le coordinate affini di P rispetto al riferimento affine standard sono $(p_1, \dots, p_n)$, ovvero coincidono con le componenti di P come elemento di K^n .

1.2 Geometria proiettiva

Def. sia V uno spazio vettoriale su un campo K , allora definiamo il proiettivizzato di V come l'insieme

$$\mathbb{P}(V) := \frac{V \setminus \{0\}}{\sim}$$

dove se $v, w \in V$, allora $v \sim w$ se e solo se esiste $\lambda \in K \setminus \{0\}$ tale che $w = \lambda v$; nel caso in cui abbiamo uno $V = K^n$ con la sua struttura standard di spazio vettoriale, allora $\mathbb{P}(V)$ si denota $\mathbb{P}_K^n$.

Def. sia V uno spazio vettoriale su un campo K , sia B una base di V e sia $P \in \mathbb{P}(V)$, ovvero $P = [v]$ per qualche $v \in V \setminus \{0\}$; le coordinate di v rispetto a B sono dette le coordinate omogenee di P rispetto a B ; se

$B = \{v_1, \dots, v_n\}$ e le coordinate di $v \in V \setminus \{0\}$ rispetto a B sono $(p_1, \dots, p_n)$, allora le coordinate omogenee di $P = [v]$ rispetto a B si denotano con

$$(p_1 : \dots : p_n)$$

notiamo che le coordinate omogenee di un punto $P \in \mathbb{P}(V)$ sono definite soltanto a meno di un fattore di proporzionalità: infatti, se $P = [v] = [w]$, allora per definizione vale che $w = \lambda \cdot v$ per qualche $\lambda \in K \setminus \{0\}$, e quindi se le coordinate di v rispetto a B sono $(p_1, \dots, p_n)$, allora le coordinate di w rispetto a B sono $(\lambda p_1, \dots, \lambda p_n)$ e pertanto scriviamo

$$(p_1 : \dots : p_n) = (\lambda p_1 : \dots : \lambda p_n)$$

soltanto quando lavoriamo con lo spazio proiettivo $\mathbb{P}_K^n$, scegliamo la base standard $B = \{e_1, \dots, e_n\}$ di K^n per calcolare le coordinate omogenee dei punti di $\mathbb{P}_K^n$.

Sappiamo che $\mathbb{P}_K^n$ può essere "recoperto" da una serie di copie di A_K^n .

Def. sia K un campo, sia $n \in \mathbb{N}$, definiamo la funzione:

$$j_0: A_K^n \rightarrow \mathbb{P}_K^n$$

$$(a_1, \dots, a_n) \mapsto (1: a_1: \dots: a_n)$$

si dimostra che j_0 è iniettiva (ma non suriettiva),
e posto $U_0 := j_0(A_K^n)$, allora vale che

$$\mathbb{P}_K^n = U_0 \cup \left\{ (0: a_1: \dots: a_n) : (a_1: \dots: a_n) \in \mathbb{P}_K^{n-1} \right\}$$

analogamente ad j_0 possiamo definire $j_1, \dots, j_n$ cambiando
la posizione dell'entità a cui è associato il valore 1;
l'inverso di j_0 è dato da (su U_0)

$$p_0: U_0 \rightarrow A_K^n$$

$$(a_0: a_1: \dots: a_n) \mapsto (a_1/a_0, \dots, a_n/a_0)$$

Oss. se $K = \mathbb{R}$, allora A_K^n può essere dotato di una topologia, ovvero la topologia euclidea di $\mathbb{R}^n$; anche $\mathbb{P}_{\mathbb{R}}^n$ può essere dotato di una topologia, dal momento che possiamo pensare $\mathbb{P}_{\mathbb{R}}^n$ come il quoziente di S^n (la sfera unitaria n -dimensionale in $\mathbb{R}^{n+1}$) rispetto alla relazione di equivalenza che identifica punti antipodali; in questo modo, la

funzione j_0 è continua ed è un'immersione, ovvero

$j_0: A_{\mathbb{R}}^n \rightarrow U_0$ è un omeomorfismo;

notiamo che, con la topologia euclidea, $A_{\mathbb{R}}^n$ è uno spazio

non compatto, mentre $P_{\mathbb{R}}^n$ con la topologia indotta da S^n

è compatto, e visto che $U_0 \subseteq P_{\mathbb{R}}^n$ è omeomorfo ad $A_{\mathbb{R}}^n$

allora possiamo pensare a $P_{\mathbb{R}}^n$ come a una compattificazione

di $A_{\mathbb{R}}^n$.

1.3. Anelli di polinomi

Sia K un campo e sia $n \in \mathbb{N}$. Allora sappiamo costruire l'anello

dei polinomi $K[x_1, \dots, x_n]$, i cui elementi sono del tipo

$$\sum_{\alpha \in \mathbb{N}^n} c_{\alpha} x^{\alpha}$$

dove $\forall \alpha \in \mathbb{N}^n$, $c_{\alpha} \in K$ e se $\alpha = (\alpha_1, \dots, \alpha_n)$, allora

$$x^{\alpha} := x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$$

ed inoltre solo un numero finito di coefficienti c_{α} sono non

nulli. L'anello dei polinomi è uno spazio vettoriale di dimensione

infinita su K : una sua base è formata dall'insieme dei monomi,

$$\{x^{\alpha} : \alpha \in \mathbb{N}^n\}$$

Teorema: sia K un campo, sia $n \in \mathbb{N}$; l'anello dei polinomi

$K[x_1, \dots, x_n]$ è un UFD, ovvero un dominio a fattorizzazione
unica; ciò significa che se $f \in K[x_1, \dots, x_n]$, allora f si
 può scrivere come $f = f_1^{\mu_1} \cdot \dots \cdot f_r^{\mu_r}$ dove $f_1, \dots, f_r$ so-
 no elementi irriducibili di $K[x_1, \dots, x_n]$ (ovvero, sono ele-
 menti che non possono essere scritti come il prodotto di due
 elementi entrambi non invertibili), e tale scrittura è essenzia-
 mente unica, ovvero è unica a meno di permutazione dei fattori
 e a meno di elementi associati (ovvero, ad esempio le due
 fattorizzazioni $f = f_1 \cdot f_2$ ed $f = (a \cdot f_1) \cdot (a^{-1} \cdot f_2)$ sono considera-
 te la medesima fattorizzazione); dato $f \in K[x_1, \dots, x_n]$ e una
 scrittura $f = f_1^{\mu_1} \cdot \dots \cdot f_r^{\mu_r}$ con f_i irriducibili e non associati,
 allora il numero naturale μ_i è detto moltiplicità del fattore f_i
 in f . (le moltiplicità sono univocamente individuate da f)

Oss.: dal teorema fondamentale dell'algebra e dal teorema di Ruffini
 segue che gli unici elementi irriducibili di $\mathbb{C}[x]$ sono i poli-
 nomi della forma $ax + b$ con $a \neq 0$

Esercizio: • calcolare una fattorizzazione in fattori irriducibili di
 $x^2 + 5xy + 6y^2 \in \mathbb{C}[x, y]$

• dimostrare che $x^2 + y^2 - 1$ e $y - x^2$ sono irriducibili in $\mathbb{C}[x, y]$

Oss: sempre come conseguenza del teorema fondamentale dell'algebra e del teorema di Buffini, si dimostra che gli elementi irriducibili di $\mathbb{R}[x]$ sono tutti e soli i polinomi della forma $ax+b$ con $a \neq 0$ oppure della forma ax^2+bx+c con $a \neq 0$ e con discriminante negativo.

Se consideriamo i campi finiti, curiosi fenomeni accadono.

Lemma: sia K un campo finito e siano $a, b \in K$; se né a né b è il quadrato di un elemento di K , allora ab è il quadrato di un elemento di K .

Dim: se $\text{char } K = 2$, allora la mappa di Frobenius

$$\begin{aligned} \sigma: K &\rightarrow K \\ x &\mapsto x^2 \end{aligned}$$

è un automorfismo (infatti è un automorfismo di campi a causa della caratteristica di K , e si può dimostrare la sua invertibilità; a questo punto la finitezza di K implica la suriettività), dunque ogni elemento di K è un quadrato; possiamo quindi supporre che $\text{char } K$ sia un primo p dispari; consideriamo la mappa $\delta: K^* \rightarrow K^*$ che manda x in x^2 ; essa è un automorfismo di gruppi il cui nucleo è costituito

dal sottogruppo $\{1, -1\}$ che, vista l'ipotesi sulla caratteristica del campo, ha cardinalità 2: infatti, $x^2 = 1 \Leftrightarrow x^2 - 1 = 0 \Leftrightarrow (x+1)(x-1) = 0 \Leftrightarrow x = 1$ oppure $x = -1$; quindi vale che $|\delta(K^*)| = \frac{|K^*|}{2}$, ovvero $\delta(K^*)$ è un sottogruppo di indice 2 in K^* , ed è dunque normale in K^* (esercizio); questo significa che $K^*/\delta(K^*) \cong \mathbb{Z}_2$;

ora, notiamo che $\delta(K^*)$ non è altro che l'insieme dei quadrati non nulli di K ; se ne è a ne è b è un quadrato, allora $[a]_{\delta(K^*)}$ e $[b]_{\delta(K^*)}$ sono entrambi uguali all'elemento non banale di $K^*/\delta(K^*)$, il che implica che $[a]_{\delta(K^*)} \cdot [b]_{\delta(K^*)} = [1]_{\delta(K^*)}$ e quindi $ab \in \delta(K^*)$, ovvero ab è un quadrato.

Prop: il polinomio $x^4 + 1$ è irriducibile in $\mathbb{Q}[x]$, ma è riducibile in $K[x]$ per qualsiasi campo finito K

Dim: il fatto che $x^4 + 1$ sia irriducibile in $\mathbb{Q}[x]$ deriva dalla considerazione che esso non ammette nessuna radice razionale, e dalla verifica tramite computazione esplicita che non è possibile scomporlo come prodotto di due fattori.

tori, entrambi di secondo grado (esercizio); sia dunque K un campo finito; se $\text{char } K = 2$, allora

$$x^4 + 1 = (x^2 + 1)^2 = (x + 1)^4$$

e dunque esso è riducibile; in tutti gli altri casi, consideriamo gli elementi $-1, 2, -2 \in K$: per il lemma precedente almeno uno di questi tre elementi deve essere un quadrato in K ; distinguiamo i casi:

i. se $-1 = \alpha^2$ con $\alpha \in K$, allora

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

ii. se $2 = \alpha^2$ con $\alpha \in K$, allora

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

iii. se $-2 = \alpha^2$ con $\alpha \in K$, allora

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

in tutti e tre i casi, dunque, il polinomio è riducibile.

Consideriamo una classe di polinomi che si rivelerà fondamentale per lo studio delle curve nel piano proiettivo.

Prop.: sia K un campo e sia $F \in K[x_1, \dots, x_n]$; allora F si può scrivere in modo unico come

$$F = F_0 + F_1 + \dots + F_d$$

per un certo $d \in \mathbb{N}$, in modo che nel polinomio F_i compaiono tutti e soli i monomi di F di grado i (ovvero F_0 è un polinomio costante, F_1 è un polinomio formato solo da monomi di primo grado, e così via...)

Def. sia K un campo, sia $F \in K[x_1, \dots, x_n]$ e siano $F_0, \dots, F_d$ i polinomi che compaiono nella decomposizione data dalla proposizione precedente; i polinomi $F_0, \dots, F_d$ si dicono le componenti omogenee di F ; il polinomio F si dice omogeneo se $F_0 = \dots = F_{d-1} = 0$, ovvero se in F compaiono solamente monomi di grado d .

Esempio: sia $F \in \mathbb{Q}[x, y, z]$ dato da

$$F = 2 + x + yz + y^2 + xyz + yz^2$$

allora vale che

$$F = F_0 + F_1 + F_2 + F_3 \quad \text{con}$$

$$F_0 = 2 \quad F_1 = x \quad F_2 = yz + y^2 \quad F_3 = xyz + yz^2$$

Oss. le componenti omogenee di un polinomio sono esse stesse polinomi omogenei

Prop. (identità di Eulero)

sia K un campo e sia $F \in K[x_1, \dots, x_n]$; allora

F è omogeneo di grado d

$\Leftrightarrow$

$$F(tx_1, \dots, tx_n) = t^d F(x_1, \dots, x_n)$$

come polinomi in $K[x_1, \dots, x_n, t]$

Dim. " $\Rightarrow$ " supponiamo che F sia omogeneo; allora F può essere

scritto come $F = \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| = d}} c_\alpha x^\alpha$ per qualche $d \in \mathbb{N}$,

dove se $\alpha \in \mathbb{N}^n$, $\alpha = (\alpha_1, \dots, \alpha_n)$, allora $|\alpha| = \sum_{i=1}^n \alpha_i$

dunque

$$F(tx_1, \dots, tx_n) = \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| = d}} c_\alpha (tx_1)^{\alpha_1} \cdot \dots \cdot (tx_n)^{\alpha_n}$$

$$= \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| = d}} c_\alpha t^{\alpha_1 + \dots + \alpha_n} x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$$

$$= \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| = d}} c_\alpha t^{|\alpha|} x^\alpha = t^d F(x_1, \dots, x_n)$$

" $\Leftarrow$ " supponiamo che valga $F(tx_1, \dots, tx_n) = t^d F(x_1, \dots, x_n)$

come polinomi in $K[x_1, \dots, x_n, t]$; per l'implicazione precedente

degre, se decomponiamo F nelle sue componenti omogenee

wee $F = F_0 + \dots + F_s$ con F_i omogeneo di grado i ,

abbiamo che

$$F(tx_1, \dots, tx_n) = F_0(tx_1, \dots, tx_n) + F_1(tx_1, \dots, tx_n) + \dots + F_s(tx_1, \dots, tx_n)$$

$$= F_0(x_1, \dots, x_n) + t F_1(x_1, \dots, x_n) + \dots + t^s F_s(x_1, \dots, x_n)$$

affinche' quest' ultima espressione sia uguale a $t^d F(x_1, \dots, x_n)$

deve quindi accadere che $s=d$ e $F_0 = \dots = F_{d+1} = 0$,

ovvero che F e' omogeneo di grado d .