Lezioni del 15,18,20,22 aprile, I. Registro dettagliato

1 Numeri complessi

1.1 Numeri complessi.

Per questa parte, si rimanda a EAV14, Cap. 3, Par. 3.6 "I numeri complessi", parti "Costruzione formale", "La costruzione geometrica", "La costruzione universitaria", "Il campo complesso non e' ordinato", "La chiusura algebrica", "Nota". Di seguito riportiamo alcune sottolineature e un approfondimento sulla "Costruzione universitaria".

1.2 Sottolineature.

- Il Teorema fondamentale dell'algebra si puo' esprimere nelle seguenti forme equivalenti

(1) Ogni polinomio non costante a coefficienti in $\mathbb{C}$ ha almeno una radice in $\mathbb{C}$;

(2) in $\mathbb{C}[x]$ ogni polinomio non costante ha almeno un fattore lineare;

(3) in $\mathbb{C}[x]$ ogni polinomio di grado $n > 0$ si fattorizza come prodotto di n fattori lineari;

(4) ogni polinomio di grado $n > 0$ a coefficienti in $\mathbb{C}$ ha esattamente n radici in $\mathbb{C}$, contate con la loro molteplicita'.

Le dimostrazioni piu' dirette del Teorema fondamentale dell'algebra sono date dal punto di vista dell'analisi. Per qualsiasi campo $\mathbb{K}$, le proprieta' (1), ..., (4) sono equivalenti; se una di esse e' soddisfatta e dunque tutte sono soddisfatte, allora si dice che il campo $\mathbb{K}$ e' algebricamente chiuso.

- Per ciascun intero positivo n, le n radici $n-$me dell'unita' sono a due a due distinte, formano un sottogruppo del gruppo moltiplicativo di $\mathbb{C}$, e questo sottogruppo e' ciclico. Per ciascun intero positivo n e ciascun $c \neq 0$ in $\mathbb{C}$, le n radici $n-$me di c sono a due a due distinte; comunque scelta una radice $n-$ma di c, i prodotti di questa radice per le n radici $n-$me dell'unita' danno tutte le n radici $n-$me di c.

- Il modulo e l'argomento di ciascuna delle n radici $n-$me di un $c \neq 0$ in $\mathbb{C}$ si possono esprimere direttamente in funzione del modulo e dell'argomento di c (per avere unicita', qui consideriamo argomenti nell'intervallo $[0, 2\pi[$). Altro problema e' esprimere in modo efficiente le parti reale e immaginaria di ciascuna delle n radici $n-$me di c in funzione della parte reale e immaginaria di c.

- Per ogni $a, b, c \in \mathbb{C}$ con $a \neq 0$, le due radici dell'equazione di II grado

$$ax^2 + bx + c = 0$$

sono distinte o coincidenti secondo che $\Delta = b^2 - 4ac$ sia uguale o diverso da zero, e sono date rispettivamente da $\frac{-b}{2a}$ o

$$\frac{-b \pm \delta}{2a}$$

dove δ e' una delle due radici quadrate di Δ.

1.3 Approfondimento. Aggiunzione simbolica.

Teorema 1. *Sia $\mathbb{K}$ un campo e sia $p(x) \in \mathbb{K}[x]$ un polimomio irriducibile. Esiste uno e, a meno di isomorfismi, un solo campo $\mathbb{F}$ che continene un sottocampo $\tilde{\mathbb{K}}$ copia isomorfa di $\mathbb{K}$ ed un elemento α tali che α sia una radice del polinomio $\tilde{p}(x) \in \tilde{\mathbb{K}}[x]$ associato al polinomio $p(x) \in \mathbb{K}[x]$, ed $\mathbb{F}$ sia generato come campo da $\tilde{\mathbb{K}}$ ed α. Un modello e' dato dall'anello quoziente $\mathbb{K}[x]/(p(x))$, con il sottocampo $\pi(\mathbb{K})$ e l'elemento $\pi(x)$ immagini del campo $\mathbb{K}$ e dell'indeterminata x tramite la proiezione canonica $\pi : \mathbb{K}[x] \to \mathbb{K}[x]/(p(x))$.*

Dim.

Unicita'. Supponiamo che esista un campo $\mathbb{F}$ con un sottocampo $\tilde{\mathbb{K}} \subset \mathbb{F}$ e con un elemento $\alpha \in \mathbb{F}$ tale che $\tilde{p}(\alpha) = 0$ ed $\mathbb{F}$ sia generato come campo da $\tilde{\mathbb{K}}$ ed α.

Si ha allora uno ed un solo omomorfismo di anelli $E : \mathbb{K}[x] \to \mathbb{F}$, che manda ogni elemento di $\mathbb{K}$ nel corrispondente elemento di $\tilde{\mathbb{K}}$ e l'indeterminata x in α. Questo omomorfismo induce un isomorfismo di anelli $\mathbb{K}[x]/\mathrm{Ker}(E) \to \mathrm{Im}(E)$.

Si ha

- $\mathrm{Ker}(E) = (p(x))$ (in quanto $\mathbb{K}[x] \supset \mathrm{Ker}(E) \supseteq (p(x))$ e $p(x)$ e' irriducibile);

- $\mathbb{K}[x]/(p(x))$ e' un campo (in quanto $p(x)$ e' irriducibile);

- $\mathrm{Im}(E) = \mathbb{F}$ (poiche' $\mathrm{Im}(E)$ e' un sottocampo di $\mathbb{F}$ che contiene $\tilde{\mathbb{K}}$ ed α).

Dunque

$$\mathbb{F} \simeq \mathbb{K}[x]/(p(x)).$$

Esistenza. Consideriamo l'anello $\mathbb{K}[x]/(p(x))$, che in realta' e' un campo (in quanto $p(x)$ e' irrriducibile). Si ha l'omomorfismo di proiezione $\pi : \mathbb{K}[x] \to \mathbb{K}[x]/(p(x))$, dato da $\pi : f(x) \mapsto [f(x)] = f(x) + (p(x))$. La restrizione di π al sottoanello $\mathbb{K}$ delle costanti in $\mathbb{K}[x]$ fornisce un isomorfismo da $\mathbb{K}$ al sottoanello $\tilde{\mathbb{K}}$ delle classi delle costanti in $\mathbb{K}[x]/(p(x))$.

Al polinomio $p(x) = a_n x^n + \cdots + a_1 x + a_0$ in $\mathbb{K}[x]$ corrisponde il polinomio $\tilde{p}(x) = [a_n]x^n + \cdots + [a_1]x + [a_0]$ in $\tilde{\mathbb{K}}[x]$. L'elemento $\pi(x) = [x] \in \mathbb{K}[x]/(p(x))$ e' una radice di $\tilde{p}(x)$ in quanto

$$\tilde{p}([x]) = [a_n][x]^n + \cdots + [a_1][x] + [a_0] = [a_n x^n + \cdots + a_1 x + a_0] = [p(x)] = 0$$

in $\mathbb{K}[x]/(p(x))$. Infine, $\mathbb{K}[x]/(p(x))$ e' generato da $\tilde{\mathbb{K}}$ ed $[x]$ (poiche' $\mathbb{K}[x]$ e' generato da $\mathbb{K}$ ed x, che dalla proiezione canonica π vengono mandati in $\tilde{\mathbb{K}}$ e $[x]$).

Con lievi variazioni, questi stessi argomenti possono essere usati per provare il Teorema nella seguente forma

Teorema 2. *Sia $\mathbb{K}$ un campo con un polinomio $p(x)$ irriducibile in $\mathbb{K}[x]$, e sia $\pi : \mathbb{K}[x] \to \mathbb{K}[x]/(p(x))$ la proiezione canonica. Il campo $\mathbb{K}[x]/(p(x))$ con il monomorfismo ristretto $\pi : \mathbb{K} \to \mathbb{K}[x]/(p(x))$ e l'elemento $\pi(x) = [x]$ radice di $\pi(p)(x)$ possiede la seguente proprieta' universale: per ogni campo $\mathbb{F}$ con un monomorfismo $\rho : \mathbb{K} \to \mathbb{F}$ e un elemento $\alpha \in \mathbb{F}$ radice di $\rho(p)(x)$, esiste uno ed un solo monomorfismo $\sigma : \mathbb{K}[x]/(p(x)) \to \mathbb{F}$ tale che $\rho = \sigma \circ \pi$ e $\sigma([x]) = \alpha$.*

Il campo descritto nell'enunciato di questi teoremi si dice "campo ottenuto aggiungendo a $\mathbb{K}$ una radice del polinomio irriducibile $p(x)$" (in francese "corps de rupture", da non confondersi con il "corps de decomposition"). Dalla proprieta' universale segue che se $\mathbb{F}_1$ con $\rho_1 : \mathbb{K} \to \mathbb{F}_1$ e $\alpha_1 \in \mathbb{F}_1$ radice di $\rho_1(p)(x)$ e $\mathbb{F}_2$ con $\rho_2 : \mathbb{K} \to \mathbb{F}_2$ e $\alpha_2 \in \mathbb{F}_2$ radice di $\rho_2(p)$ sono "corps de rupture" di $p(x)$ su $\mathbb{K}$, allora esiste uno ed un solo isomorfismo $\sigma_{21} : \mathbb{F}_1 \to \mathbb{F}_2$ tale che $\rho_2 = \sigma_{21} \circ \rho_1$ e $\sigma_{21}(\alpha_1) = \alpha_2$.

Un "campo complesso" e' un campo che contiene un sottocampo isomorfo al campo reale $\mathbb{R}$, contiene un elemento con quadrato uguale a -1, e non contiene alcun sottocampo proprio con queste proprieta'. Dagli argomenti sviluppati, si ha che esiste un campo complesso, unico a meno di isomorfismi, ed e' il "corps de rupture" del polinomio $x^2 + 1$ sul campo $\mathbb{R}$. Un modello del campo complesso e' dato dal quoziente $\mathbb{R}[x]/(x^2 + 1)$, con l'immersione canonica di $\mathbb{R}$ in esso e l'elemento $[x]$ che e' una radice di $x^2 + 1$ in esso. L'unicita' del campo complesso vale nel senso forte seguente: se C_1 e C_2 sono due campi complessi, con monomorfismi $\rho_1 : \mathbb{R} \to C_1$ e $\rho_2 : \mathbb{R} \to C_2$, e con elementi $i_1 \in C_1$ e $i_2 \in C_2$ tali che $i_1^2 = -1$ e $i_2^2 = -1$, allora esiste uno ed un solo isomorfismo $\sigma : C_1 \to C_2$ tale che $\rho_2 = \sigma \circ \rho_1$ e $\sigma(i_1) = i_2$.