**Lezioni del 15,18,20,22 aprile, II. Registro dettagliato**

# 1 Estensioni in $\mathbb{C}$, automorfismi, polinomi.

## 1.1 Estensioni di sottocampi di $\mathbb{C}$.

Una coppia di campi, uno contenuto nell'altro, si dice "estensione di campi"; indicati con $\mathbb{F}$ e $\mathbb{K}$ il campo maggiore e il campo minore dei due, si indica l'estensione con $\mathbb{F}/\mathbb{K}$. Nel seguito ci limiteremo a considerare sottocampi del campo complesso.

Sia data un'estensione di campi $\mathbb{F}/\mathbb{K}$. Il campo $\mathbb{F}$ e' in modo naturale uno spazio vettoriale su $\mathbb{K}$; l'estensione $\mathbb{F}/\mathbb{K}$ si dice "finita" se e solo se $\mathbb{F}$ e' finitamente generato come spazio vettoriale su $\mathbb{K}$; la dimensione di $\mathbb{F}$ su $\mathbb{K}$ si dice "grado" di $\mathbb{F}$ su $\mathbb{K}$ e si indica con $[\mathbb{F} : \mathbb{K}]$.

Per ogni $\alpha \in \mathbb{F}$ si hanno

- un anello $\mathbb{K}[\alpha]$, dato dal sottoanello di $\mathbb{F}$ generato da $\mathbb{K}$ ed $\alpha$, cioe' dall'insieme delle "espressioni polinomiali" a coefficienti in $\mathbb{K}$ nell'elemento $\alpha$, cioe' dall'immagine dell'omomorfismo $\mathbb{K}[x] \to \mathbb{F}$ di sostituzione di $x$ in $\alpha$;

- un campo $\mathbb{K}(\alpha)$, dato dal sottocampo di $\mathbb{F}$ generato da $\mathbb{K}$ ed $\alpha$, cioe' dall'insieme delle "espressioni razionali" a coefficienti in $\mathbb{K}$ nell'elemento $\alpha$.

**Definizione 1.** *Sia $\mathbb{F}/\mathbb{K}$ un'estensione di campi. Un elemento di $\mathbb{F}$ si dice algebrico su $\mathbb{K}$ se e' una radice di un polinomio non nullo a coefficienti in $\mathbb{K}$; un elemento di $\mathbb{F}$ che non e' radice di alcun polinomio non nullo a coefficienti in $\mathbb{K}$ si dice trascendente su $\mathbb{K}$. Al posto di dire "numero algebrico su $\mathbb{Q}$" o "numero trascendente su $\mathbb{Q}$" si dice in breve "numero algebrico" o "numero trascendente".*

Si sono gia' visti in precedenza esempi di numeri reali algebrici e trascendenti. Ogni numero complesso $\alpha \in \mathbb{C}$ e' algebrico su $\mathbb{R}$, in quanto e' radice del polinomio $(x-\alpha)(x-\bar{\alpha}) = x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$, che ha coefficienti in $\mathbb{R}$. Numeri algebrici di particolare interesse sono le radici complesse di numeri razionali, piu' in particolare le radici dell'unita'.

In prima battuta l'anello e il campo associati ad un elemento di un'estensione sono descritti nel caso algebrico e nel caso trascendente dalla seguente

**Proposizione 1.** *Siano $\mathbb{F}/\mathbb{K}$ un'estensione di campi, $\alpha$ un elemento di $\mathbb{F}$, e $E_\alpha : \mathbb{K}[x] \to \mathbb{F}$ l'omomorfismo di sostituzione di $x$ in $\alpha$.*

*(1) Se $\alpha$ e' algebrico su $\mathbb{K}$ allora*

- $\mathbb{K}[x]/\mathrm{Ker}(E_\alpha) \simeq \mathbb{K}[\alpha]$ *e' un $\mathbb{K}-$dominio di integrita' di dimensione finita;*

- $\mathbb{K}[\alpha]$ *e' un campo, e $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.*

*(2) Se $\alpha$ e' trascendente su $\mathbb{K}$, allora*

- $\mathbb{K}[x] \simeq \mathbb{K}[\alpha] \subset \mathbb{K}(\alpha)$.

La dimostrazione segue direttamente da quanto visto in precedenza sugli anelli di polinomi a coefficienti in un campo. In particolare, da questa proposizione si ha la seguente caratterizzazione degli elementi algebrici

**Corollario 1.** *Sia $\mathbb{F}/\mathbb{K}$ un'estensione di campi. Un elemento $\alpha \in \mathbb{F}$ e' algebrico su $\mathbb{K}$ se e solo se l'estensione $\mathbb{K}(\alpha)/\mathbb{K}$ e' finita.*

Sia $\mathbb{F}/\mathbb{K}$ un'estensione di campi, $\alpha \in \mathbb{F}$ ed $E_\alpha : \mathbb{K}[x] \to \mathbb{F}$ l'omomorfismo di sostituzione di $x$ in $\alpha$. Se $\alpha$ e' algebrico su $\mathbb{K}$, allora $\mathrm{Ker}(E_\alpha)$ non e' ridotto al solo polinomio nullo ed e' generato come ideale dal suo unico polinomio monico di grado minimo, che coincide col suo unico polinomio monico irriducibile in quanto $\mathbb{K}[x]/\mathrm{Ker}(E_\alpha)$ e' un campo. Questo polinomio si dice "polinomio minimo di $\alpha$ su $\mathbb{K}$", ed il suo grado si dice "grado di $\alpha$ su $\mathbb{K}$".

In una qualsiasi estensione, un elemento $\alpha$ e' algebrico di grado 1 sul campo minore se e solo se $\alpha$ ha polinimo minimo $x-\alpha$ sul campo minore se e solo se $\alpha$ appartiene al campo minore. Ogni elemento $\alpha \in \mathbb{C}$ con $\alpha \notin \mathbb{R}$ ha polinomio minimo $x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$ su $\mathbb{R}$ e dunque ha grado 2 su $\mathbb{R}$.

Le due radici primitive terze dell'unita' hanno entrambe polinomio minimo $x^2 + x + 1$ su $\mathbb{Q}$ e dunque hanno grado 2 su $\mathbb{Q}$. Le tre radici terze di 2 hanno tutte polinoimio minimo $x^3 - 2$ su $\mathbb{Q}$ e dunque hanno grado 3 su $\mathbb{Q}$. Le due radici terze non reali di 2 hanno entrambe polinoimio minimo $x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$ su $\mathbb{R}$ e dunque hanno grado 2 su $\mathbb{R}$.

Un criterio operativo per verificare se un elemento e' algebrico e in tal caso determinarne il polinomio minimo e' dato dalla seguente

**Proposizione 2.** *Sia $\mathbb{F}/\mathbb{K}$ un'estensione di campi. Un elemento $\alpha \in \mathbb{F}$ e' algebrico su $\mathbb{K}$ se e solo se la sequenza $1, \alpha, \alpha^2, \ldots$ e' linearmente dipendente su $\mathbb{K}$; in tal caso, indicato con $n$ il minimo intero positivo tale che $\alpha^n$ e' combinazione lineare di $1, \alpha, \ldots, \alpha^{n-1}$ e posto*

$$\alpha^n = a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n, \qquad (a_i \in \mathbb{K}),$$

*si ha che $n$ e' il grado di $\alpha$ su $\mathbb{K}$ e che il polinomio minimo di $\alpha$ su $\mathbb{K}$ e' dato da*

$$p(x) = x^n - a_1x^{n-1} - \cdots - a_{n-1}x - a_n.$$

La dimostrazione segue direttamente dalle definizioni.

Una descrizione piu' fine del campo associato ad un elemento algebrico e' data dal

**Teorema 1.** *Siano $\mathbb{F}/\mathbb{K}$ un'estensione di campi, $\alpha$ un elemento di $\mathbb{F}$ algebrico su $\mathbb{K}$, $p(x) = x^n + a_1x + \cdots + a_n$ il polinomio minimo $\alpha$ su $\mathbb{K}$, e $r_{ij}(x)$ il resto della divisione di $x^{i+j}$ su $p(x)$ $(0 \le i, j < n)$. Allora il campo $\mathbb{K}[\alpha]$ e' la $\mathbb{K}-$algebra con base $1, \alpha, \ldots, \alpha^{n-1}$, e prodotto indotto da $\alpha^i\alpha^j = r_{ij}(\alpha)$ $(0 \le i, j < n)$.*

## 1.2 Composizione di estensioni.

**Teorema 2.** *Siano $F/L$ ed $L/K$ estensioni di campi. $F/K$ e' finita se e solo se sia $F/L$ che $L/K$ sono finite; inoltre in tal caso si ha $[F : K] = [F : L][L : K]$.*

**Idea della dim.**

Se $F/L$ e $L/K$ sono finite e $\{u_i;\ i=1,\dots,m\}$ e' una base di $F$ su $L$ e $\{v_j;\ j=1,\dots,n\}$ e' una base di $L$ su $K$, allora $\{u_iv_j;\ i=1,\dots,m,\ j=1,\dots,n\}$ e' una base di $F$ su $K$.

Se $F/K$ e' finita di grado $\ell$, allora ogni sottinsieme di $L$ linearmente indipendente su $K$ ha cardinalita' al piu' $\ell$ ed ogni sottinsieme di $F$ linearmente indipendente su $L$, essendo in particolare linearmente indipendente su $K$, ha cardinalita' al piu' $\ell$.

Osserviamo che dalla dimostrazione si ha anche una costruzione di una base di $F$ su $K$ a partire da una base di $F$ su $L$ ed una base di $L$ su $K$.

Da questo teorema, per la caratterizzazione degli elementi algebrici mediante la finitezza delle associate estensioni, segue la

**Proposizione 3.** *Se $F/K$ e' un'estensione finita, allora ogni elemento di $F$ e' algebrico su $K$, ed il suo grado divide il grado di $F$ su $K$. In particolare, se $F/K$ ha grado primo $p$, allora ogni $\alpha \in F$ con $\alpha \notin K$ e' algebrico di grado $p$ su $K$, ed $F = K[\alpha]$.*

Sempre dallo stesso Teorema segue la

**Proposizione 4.** *Sia $F/K$ un'estensione di campi. (1) Se $\alpha, \beta \in F$ sono algebrici su $K$, allora anche $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, $\alpha/\beta$ ($\beta \neq 0$) sono algebrici su $K$; (2) Se $\alpha \in F$ e' algebrico su $K$ e $\beta \in F$ e' algebrico su $K(\alpha)$, allora $\beta$ e' algebrico su $K$.*

Da questa proposizione segue direttamente la

**Proposizione 5.** *Sia $F/K$ un'estensione di campi, con $F$ algebricamente chiuso. Allora l'insieme degli elementi di $F$ algebrici su $K$ e' un sottocampo algebricamente chiuso di $F$. In particolare, l'insieme dei numeri algebrici e' un sottocampo algebricamente chiuso di $\mathbb{C}$.*

**Esempio** Nell'estensione $\mathbb{R}/\mathbb{Q}$ consideriamo gli elementi $\alpha = \sqrt{2}$ e $\beta = \sqrt{3}$, algebrici su $\mathbb{Q}$ con polinomi minimi rispettivi $x^2-2$ e $x^2-3$. Osserviamo che

- essendo $\alpha$ algebrico di grado 2 su $\mathbb{Q}$, il campo $\mathbb{Q}(\alpha)$ ha come $\mathbb{Q}-$base $1, \alpha$;

- $\beta$ e' algebrico su $\mathbb{Q}(\alpha)$, con polinomio minimo $x^2-3$;

- essendo $\beta$ algebrico di grado 2 su $\mathbb{Q}(\alpha)$ il campo $\mathbb{Q}(\alpha)(\beta)$ ha come $\mathbb{Q}(\alpha)-$base $1, \beta$;

- per il teorema sulla composizione di estensioni, si ha che il campo $\mathbb{Q}(\alpha)(\beta)$ ha come $\mathbb{Q}-$base $1, \alpha, \beta, \alpha\beta$.

Per la Proposizione di sopra, sappiamo che $\alpha+\beta$ e' algebrico su $\mathbb{Q}$. Ne cerchiamo il polinomio minimo.

Posto $\gamma = \alpha+\beta$, consideriamo le potenze di $\gamma$ :

$\gamma^0 = 1$

$\gamma = \alpha+\beta$

$\gamma^2 = 5+2\alpha\beta$

$\gamma^3 = 11\alpha+9\beta$

$\gamma^4 = 49+20\alpha\beta$

Osserviamo che la prima potenza di $\gamma$ che e' combinazione lineare su $\mathbb{Q}$ delle precedenti potenze di $\gamma$ e' la quarta; inoltre, eliminando $\alpha\beta$ dalla seconda e dalla quarta uguaglianza, si ha $\gamma^4 - 10\gamma^2 = -1$. Dunque $\gamma = \alpha + \beta$ e' radice del polinomio a coefficienti in $\mathbb{Q}$

$$x^4 - 10x^2 + 1.$$

Questo e' il polinomio minimo di $\gamma$ su $\mathbb{Q}$.

Osserviamo che $1, \gamma, \gamma^2, \gamma^3$ sono 4 elementi linearmente indipendenti su $\mathbb{Q}$ nello spazio vettoriale $\mathbb{Q}(\alpha, \beta)$ che e' 4-dimensionale du $\mathbb{Q}$, dunque $1, \gamma, \gamma^2, \gamma^3$ sono una base di $\mathbb{Q}(\alpha, \beta)$, e $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$.

## 1.3 Accenno ai numeri costruibili con riga e compasso.

In termini leggermente informali, i numeri reali costruibili con riga e compasso sono, a meno del segno, le lunghezze rispetto ad un segmento fissato dei segmenti ottenibili a partire dal segmento fissato usando soltanto riga e compasso. Con strumenti di geometria sintetica, si puo' provare che i numeri costruibili con riga e compasso formano un sottocampo di $\mathbb{R}$. Identificando il piano euclideo col prodotto cartesiano $\mathbb{R} \times \mathbb{R}$ mediante un sistema di riferimento cartesiano ortogonale monometrico, ed usando i primi fatti della geometria analitica delle rette e delle circonferenze, si puo' tradurre la costruibilita' con riga e compasso nei termini algebrici dati dal seguente

**Teorema 3.** *Un numero reale $\alpha$ e' costruibile con riga e compasso se e solo se esistono un numero finito di numeri reali $\lambda_1, \lambda_2, \lambda_3, \ldots$ tali che $\lambda_1^2 \in \mathbb{Q}$, $\lambda_2^2 \in \mathbb{Q}(\lambda_1)$, $\lambda_3^2 \in \mathbb{Q}(\lambda_1, \lambda_2)$, ... e $\alpha \in \mathbb{Q}(\lambda_1, \lambda_2, \lambda_3, \ldots)$.*

Dal Teorema sulla composizione di estensioni e dalla Proposizione sua prima conseguenza segue allora la

**Proposizione 6.** *Ogni numero costruibile con riga e compasso e' algebrico di grado potenza di due su $\mathbb{Q}$.*

Questa Proposizione a sua volta permette di dare risposta negativa ai problemi classici di costruzioni come la quadratura del cerchio, la duplicazione del cubo e la trisezione dell'angolo.

## 1.4 Automorfismi di un'estensione.

**Definizione 2.** *Sia $F/K$ un'estensione di campi. Un $K-$automorfismo di $F$ e' un automorfismo di campo di $F$ che ristretto a $K$ e' l'identita' su $K$. Esplicitamente, un $K-$automorfismo di $F$ e' una funzione $\sigma : F \to F$ tale che $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ e $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ per ogni $\alpha, \beta \in F$ e $\sigma(\gamma) = \gamma$ per ogni $\gamma \in K$.*

**Esempio.** L'estensione $\mathbb{C}/\mathbb{R}$ ha esattamente due $\mathbb{R}-$automorfismi: l'identita' e il coniugio. Infatti, se $\sigma : \mathbb{C} \to \mathbb{C}$ e' un $\mathbb{R}-$automorfismo, allora da $i^2 = -1$ si ottiene $\sigma(i^2) = \sigma(-1)$ cioe' $\sigma(i)^2 = -1$ e dunque che $\sigma(i) = i$ oppure $\sigma(i) = -i$. A queste

due condizioni corrispondono due soli possibili $\mathbb{R}-$automorfismi di $\mathbb{C}$, l'identita' e il coniugio, che a loro volta sono effettivamente $\mathbb{R}-$automoorfismi di $\mathbb{C}$.

**Esempio.** Sia $u = \sqrt[3]{2}$ l'unica radice cubuca reale di 2. L'estensione $\mathbb{Q}(u)/\mathbb{Q}$ ha un solo $\mathbb{Q}-$automorfismo: l'identita'. Infatti, se $\sigma : \mathbb{Q}(u) \to \mathbb{Q}(u)$ e' un $\mathbb{Q}-$automorfismo, allora da $u^3 = 2$ si ottiene $\sigma(u^3) = \sigma(2)$ cioe' $\sigma(u)^3 = 2$ e dunque che $\sigma(u) = u$, in quanto deve anche essere $\sigma(u) \in \mathbb{Q}(u) \subset \mathbb{R}$. A questa condizione corrisponde il solo $\mathbb{Q}-$automorfismo identita' di $\mathbb{Q}(u)$.

## 1.5 Polinomi, coefficienti, radici, estensione associata.

Siano $f(x)$ un polinomio monico di grado $n > 0$ in $\mathbb{C}[x]$, $a_1, \ldots, a_n$ i suoi coefficienti e $\alpha_1, \ldots, \alpha_n$ le sue radici:

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

I coefficienti sono dati in funzione delle radici da [1]

$$\begin{aligned} a_1 &= -\sum_{1 \le i \le n} \alpha_i \\ a_2 &= \sum_{1 \le i < j \le n} \alpha_i \alpha_j \\ &\vdots \\ a_n &= (-1)^n \alpha_1 \cdots \alpha_n. \end{aligned}$$

Al polinomio $f(x)$ associamo

- il campo dei coefficienti di $f$, cioe' il campo $K_0 = \mathbb{Q}(a_1, \ldots, a_n)$ generato dei coefficienti di $f$;

- il campo di spezzamento di $f$, cioe' il campo $F = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$; generato dalle radici di $f$.

Essendo ogni coefficiente di $f$ dato da un polinomio nelle radici di $f$, si ha che $K_0$ e' contenuto in $F$. UNa prima informazione sull'estensione $F/K_0$ e' data dalla

**Proposizione 7.** *Siano $f(x)$ un polinomio monico di grado $n > 0$ in $\mathbb{C}[x]$ e $K_0$ ed $F$ i campi dei coefficienti e di spezzamento di $f(x)$. Allora*

$$[F : K_0] \le n!.$$

**Idea della Dim.** Per induzione su $n$, usando il teorema sulla composizione di estensioni ed il fatto che se un polinomio $g \in K[x]$ di grado $\nu$ e' irriducibile su $K$ e $\alpha \in \mathbb{C}$ e' una sua radice, allora $[K[\alpha] : K] = \nu$.

[1] Un polinomio in piu' indeterminate si dice "simmetrico" se e solo se e' invariante rispetto alle permutazioni delle indeterminate. I polinomi

$$e_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k}, \qquad (1 \le k \le n)$$

sono simmetrici, si dicono "polinomi simmetrici elementari" in $x_1, \ldots, x_n$.

**Esempio** Consideriamo il polinomio

$$f(x) = x^3 - 1 = (x-1)(x-\xi)(x-\xi^2),$$

dove $\xi$ e' una radice primitiva terza dell'unita', ad esempio $\xi = \frac{-1+\sqrt{-3}}{2}$. Si ha che

- il campo dei coefficienti di $f$ e' $K_0 = \mathbb{Q}$;

- il campo di spezzamento di $f$ e' $F = \mathbb{Q}(1, \xi, \xi^2) = \mathbb{Q}(\xi)$.

Dunque $[F : K_0] = [\mathbb{Q}(\xi) : \mathbb{Q}] = 2$.

**Esempio** Consideriamo il polinomio

$$f(x) = x^3 - 2 = (x-u)(x-\xi u)(x-\xi^2 u),$$

dove $u = \sqrt[3]{2}$ e $\xi$ e' una radice primitiva terza dell'unita'. Si ha che

- il campo dei coefficienti di $f$ e' $K_0 = \mathbb{Q}$;

- il campo di spezzamento di $f$ e' $F = \mathbb{Q}(u, \xi u, \xi^2 u) = \mathbb{Q}(u, \xi)$.

Dunque $[F : K_0] = [\mathbb{Q}(u, \xi) : \mathbb{Q}] = [\mathbb{Q}(u)(\xi) : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = 3 \cdot 2 = 6$.

## 1.6 Estensioni quadratiche.

Di seguito si descrive, nei vari aspetti secondo i termini introdotti in precedenza, la classe di estensioni piu' semplice non banale: quelle delle estensioni quadratiche.

Sia $F/K$ un'estensione di campi con $[F : K] = 2$, e sia $v \in F \setminus K$ arbitrariamente fissato.

(1) L'insieme $\{1, v\}$ e' una base di $F$ come spazio vettoriale su $K$; l'elemento $v$ e' algebrico su $K$ con un polinomio minimo di secondo grado $p(x) = x^2 + bx + c$ $(b, c \in K)$. Indicate con $v_1 = v$ e $v_2$ le radici di $p(x)$ in $\mathbb{C}$, si ha che non solo $v_1 \in F$ ma anche e $v_2 \in F$, inoltre $v_1 \neq v_2$ (essendo $b = -(v_1 + v_2)$, $v_1 \in F \setminus K$ e $b \in K$). Il campo $F$ e' il campo di spezzamento di $p(x)$ su $K$.

(2) Il discriminante $\Delta = b^2 - 4c$ del polinimio $p(x)$ e' non nullo; indicata con $\delta$ una delle sue due radici quadrate in $\mathbb{C}$ si ha che $\delta \in F \setminus K$, l'insieme $\{1, \delta\}$ e' una base di $F$ come spazio vettoriale su $K$, e $\delta$ e' algebrico su $K$ con polinomio minimo $x^2 - \Delta$. Il campo $F$ e' il campo di spezzamento di $x^2 - \Delta$ su $K$.

(3) Sia $\sigma : F \to F$ un $K-$automorfismo di $F$. Si ha $\sigma(\delta) = \delta$ oppure $\sigma(\delta) = -\delta$ (essendo $\delta^2 = \Delta$, $\Delta \in K$, e dunque $\sigma(\delta)^2 = \Delta$.) Ciascuna di queste due condizioni individua uno ed un solo $K-$automorfismo di $F$ : la prima individua l'identita' $\mathrm{id}_F$ su $F$, e la seconda un $K-$automorfismo che indichiamo con $\bar{\sigma}$. Questo $K-$automorfismo di $F$ fissa solo gli elementi di $K$.