Capitolo 6: Campi di spezzamento:

Idea:
Studiare i polinomi a coefficienti in un campo.

Definizione (Algebrico e trascendente):

Dati $K \subseteq L$ campi, un elemento $\alpha \in L$ si dice **algebrico** su K se $\exists\, f(x) \in K[x] \mid f(\alpha) = 0$
Dati $K \subseteq L$ campi, un elemento $\alpha \in L$ si dice **trascendente** su K se non è algebrico.

Funzione di valutazione:

Dati $K \subseteq L$ campi, $\alpha \in L$
$\varphi_\alpha : K[x] \to L \mid \varphi_\alpha\big(f(x)\big) = f(\alpha)$

Osservazione:
È un omomorfismo la cui immagine si indica con $K[\alpha]$

Osservazione:
α trascendente $\to$ φ_α iniettiva
α algebrico $\to$ φ_α non iniettiva

Osservazione:
Se φ_α è iniettivo allora $K[x] \cong K[\alpha]$

Se φ_α è non iniettivo allora consideriamo:

$$\begin{array}{ccc} K[x] & \to_{\varphi_\alpha} & K[\alpha] \\ \downarrow^{\pi} & \nearrow_{\lambda} & \\ \frac{K[x]}{\ker(\varphi_\alpha)} & & \end{array}$$

Dove $\ker(\varphi_\alpha) = \big(h(x)\big)$ in quanto è ideale di un Dominio ad I.P.

Notazione:

Dati $K \subseteq L$ campi allora:
$K[\alpha]$ è il minimo sottoanello di L contenente K e α.
$K(\alpha)$ è il minimo sottocampo di L contenente K e α.

Osservazione:
Se α algebrico allora: $K[\alpha] \cong K(\alpha)$
Se α trascendente allora $K[\alpha] \cong K[x]$ e $K(\alpha) \cong K(x) = \left\{\frac{f(x)}{g(x)} \mid f, g \in K[x], g \neq 0\right\}$

Definizione (Polinomio minimo di α su K):

Siano $K \subseteq L$ campi e $\alpha \in L$ un elemento algebrico su K.
Si dice polinomio minimo di α su K il generatore monico dell'ideale $\big(h(x)\big) = \ker \varphi_a$

Spazi vettoriali:

Siano $K \subseteq L$ campi, allora L e $K[\alpha]$ sono K-spazi vettoriali.

Proposizione:

Sia $\alpha \in L$ allora:

Se α è trascendente allora la dimensione su K di $K[\alpha]$ è ∞.
Se α è algebrico allora $\dim_{\mathrm{K}} K[\alpha]$ =grado del polinomio minimo di α.

Osservazione:

Una base di $K[\alpha]$ può essere $\{\alpha^i \mid 0 \leq i \leq (n-1)\}$

Definizione (Estensione):

Di un'estensione di campi $K \subseteq F$ è $[F\colon K] = \dim_{\mathrm{K}} F$
È la dimensione di F come K-spazio vettoriale

Osservazione:

Un'estensione si dice finita se $[F\colon K] < \infty$

Proposizione (Dimensione di una composizione di estensioni):

Siano $K \subseteq E \subseteq F$ campi (E estensione finita di K ed F estensione finita di E).

Allora F è estensione finita di K e vale:

$$[F\colon K] = [F\colon E] \cdot [E\colon K]$$

Definizione (Estensione algebrica):

Un'estensione di campi $K \subseteq F$ si dice algebrica se ogni $\alpha \in F$ è algebrico su K.

Proposizione:

Ogni estensione finita è algebrica, il viceversa è falso.

Proposizione:

Siano K, E, F campi, se E/K , F/E sono estensioni algebriche allora anche F/K è un'estensione algebrica.

Proposizione (Costruzione campo):

Siano $K \subseteq F$ campi, l'insieme $A = \{\alpha \in F \mid \alpha \text{ algebrico su } K\}$ è un campo.

Idea:

Dato un campo K individuare un'estensione E di K | ogni polinomio di grado > 0 in $K[x]$ abbia una radice in E.

Lemma:

Siano K campo e $f(x) \in K[x]$ | $\deg(f) \geq 1$ allora ∃ un campo $E \supseteq K$ | $f(x)$ ha una radice in E.

Lemma:

Siano K campo e $f_0(x), \dots, f_n(x) \in K[x]$ | $\deg(f_i(x)) \geq 1$ allora ∃ un campo $L \supseteq K$ | $f_i(x)$ ha una radice in L.

Definizione (Algebricamente chiuso):

Un campo L si dice algebricamente chiuso se ogni polinomio di $L(x)$ di grado maggiore di 0 ha una radice in L.

Teorema (Campo algebricamente chiuso):

Sia K campo, allora ∃ un campo $E \supseteq K$ | $\forall f(x) \in K[x]$ di grado > 0, abbia una radice in E.

Corollario:

Dato un campo K ∃ $\overline{K}$ algebricamente chiuso contenente K e algebrico su K.

Teorema fondamentale dell'algebra:

Il campo $\mathbb{C}$ è algebricamente chiuso.

Teorema (Chiusura algebrica):

Sia K di caratteristica 0 o $K = {}^{Z}/_{pZ}$.

Un polinomio irriducibile di $K[x]$ ha radici distinte in un campo algebricamente chiuso L contenente K (La **chiusura algebrica di K**).

Idea importante (Campi di spezzamento di un polinomio):

Cercare il campo nel quale il polinomio dato è completamente fattorizzabile (In pratica aggiungere le radici)

Sfruttiamo il teorema di omomorfismo:
Sia K un campo, L la sua chiusura algebrica ed $f(x)$ un polinomio irriducibile di $K[x]$

Proiettiamo $K[x] \to_\pi {K[x]}/{f(x)}$ che sappiamo essere un campo (Questo ci assicura l'esistenza di

λ) che mi porti in un'estensione di K che fattorizzi almeno in parte $f(x)$.

Vogliamo costruire un omomorfismo $\lambda: K[x] \to L \mid \lambda_{|K} = \mathrm{Id}$ e che assegni ad x i valore di una delle radici distinte di $f(x)$.

Se $f(x)$ ha *n* radici distinte allora ho *n* modi di costruire l'omomorfismo λ.

Esempio 1:
Siano $K = \mathbb{Q}$, $f(x) = x^3 - 2$, $L = \mathbb{C}$ allora:
$\mathbb{Q}[x] \to_\pi {\mathbb{Q}[x]}/{(x^3 - 2)} \to_\varphi \mathbb{C}$ e $\mathbb{Q}[x] \to_\lambda \mathbb{C}$

Come condizioni abbiamo che $\lambda_{|\mathbb{Q}} = \mathrm{Id}$ quindi possiamo assegnare ad x le radici di $x^3 - 2$ in $\mathbb{C}$ ed otteniamo:
$\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2\xi})$, $\mathbb{Q}\left(\sqrt[3]{2\xi^2}\right)$ dove ξ è la radice terza dell'unità.

Osservazioni:
Queste estensioni possono coincidere oppure no, in questo caso sono tutte distinte.

Esempio 2:
Siano $K = \mathbb{Q}$, $f(x) = x^2 - 5$, $L = \mathbb{C}$ allora come estensioni otteniamo:
$\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(-\sqrt{5})$ che coincidono come estensioni.

Proposizione:

Siano K un campo di caratteristica 0 e L una chiusura algebrica di K. Sia $E \supseteq K$ un'estensione finita di $K \mid [E:K] = n$, allora $\exists\, n$ omomorfismi $\varphi: E \to L \mid \varphi_{|K} = \mathrm{Id}$.

Definizione (Campo di spezzamento):

Sia $f(x) \in K[x]$, il campo di spezzamento del polinomio $f(x)$, il campo di spezzamento di $f(x)$ è un'estensione algebrica di K generata da tutte le radici del polinomio.

Osservazione:

Siano $a_0, \dots, a_k \in L$ radici distinte di $f(x)$ allora il campo di spezzamento è $K(a_0, \dots, a_k)$.

Osservazione:

I campi di spezzamento E di un polinomio $f(x) \in K[x]$ hanno la proprietà che ogni omomorfismo $\sigma: E \to L \mid \sigma_{|K} = \mathrm{Id}$ lascia fisso E ($\sigma(E) = E$, σ automorfismo di E).

Osservazione:

$K(\alpha) \cong {K[x]}/{(f(x))} \mid f(x)$ polinomio minimo di α.

Quindi la dimensione come spazio vettoriali di $K(\alpha)$ è uguale al grado del polinomio minimo.

Proprietà pratiche per calcolare il grado di un campo di Spezzamento:

Proprietà 1:

Il grado del campo di spezzamento è minore di $n!$ con n grado del polinomio.

Motivo:

Ogni volta devo moltiplicare il valore precedente per il grado del minimo polinomio che si annulli nella nuova radice, quindi nel peggiore dei casi è di grado *n* al primo passo, $n-1$ al secondo, etc.

Proprietà 2 (Estensione per torri):

Si estende dal campo di partenza di una sola radice per volta individuando ogni volta il grado del polinomio minimo. Il grado del campo di spezzamento sarà divisore del prodotto di quelle estensioni.

Motivo:

Abbiamo già individuato dei polinomi in K che mi si annullino in quelle radici, aumentando il numero di coefficienti il grado del polinomio potrà solo ridursi.

Proprietà 3:

Se abbiamo già individuato una catena di estensioni il grado del campo di spezzamento sarà multiplo di quella catena.

Proprietà 4:

Per verificare se due estensioni coincidono abbiamo svariati sistemi:

1- Se gli elementi sono ottenibili come combinazione dell'altro con i coefficienti del campo le due estensioni coincidono. (Tipicamente inverso, opposto). Attenzione a non verificare solo un'inclusione.

2- Nel caso in cui $K \subseteq_2 K(\alpha) \subseteq_{\leq 2} K(\alpha,\beta)$ quando vale $K(\alpha) = K(\beta)$.

Possiamo porre $\alpha = \sqrt{k_1}$; $\beta = \sqrt{k_2}$ con $k_1, k_2 \in K$. Ci chiediamo quando $K\left(\sqrt{k_1}\right) = K\left(\sqrt{k_2}\right)$.

Questo accade se $\frac{k_1}{k_2} = k$ è un quadrato in K.

Equivalente $\sqrt{k_1} \cdot \sqrt{k_2} \in K$

Proprietà 5 (fattorizzare):

1- Un polinomio è fattorizzabile come fattori di primo grado su $\mathbb{Q}$ ↔ lo è su $\mathbb{Z}$.

2- Su $\mathbb{Z}$ le radici devono dividere il termine noto.

3- Per verificare l'irriducibilità di un polinomio si può proiettarlo su $\mathbb{Z}/_{p\mathbb{Z}}$

Ricordando inoltre che su $\mathbb{Z}/_{2\mathbb{Z}}$ l'unico polinomio irriducibile di grado 2 è $x^2 + x + 1$

4- Applicare il criterio di irriducibilità di Eisenstein.

5- Metodo della forza bruta, per verificare se sia possibile spezzare un polinomio in due di grado dato si inseriscono i due polinomi con coefficienti non assegnati e si risolve il sistema.

Campi finiti:

Sono i campi $\mathbb{F}$ con caratteristica *p*;

Osservazione:

$\exists\, n \mid |\mathbb{F}| = p^n$

Osservazione:

$\mathbb{F}_{p^n}$ è il campo di spezzamento del polinomio $x^{p^n} - x$ su $\mathbb{Z}/p\mathbb{Z}$

Osservazione:

Tutti i campi finiti sono isomorfi ad un dato $\mathbb{F}_{p^n}$

Osservazione:

$\left[\mathbb{F}_{p^n}: \mathbb{F}_p\right] = n$; $\left[\mathbb{F}_{p^n}: \mathbb{F}_{p^m}\right] = \frac{n}{m}$

Teorema:

$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \leftrightarrow m|n$

Osservazione:

$\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ è normale.

Proposizione:

K campo, allora $G < K^*$ finito $\rightarrow$ G ciclico.

Corollario:

$\left(\mathbb{F}_{p^n}\right)^*$ è ciclico.

Osservazione:

Vale $\mathbb{F}_{p^n} = \mathbb{F}(\alpha) \cong \mathbb{F}_p[x]/(f(x))$ con $\deg(f(x)) = n = \left[\mathbb{F}_{p^n}: \mathbb{F}_p\right] \rightarrow \forall\, n\ \exists$ un polinomio irriducibile di grado n in $\mathbb{F}_p[x]$.

Osservazione pratica:

Su $\mathbb{F}_p$ la formula di risoluzione delle equazioni di secondo grado rimane valida.

Esempi ed esercizi:

Esempio 1 (C.d.s. standard):
Sia $f(x) = x^4 - 4x^2 + 2$.
Determinarne il grado del campo di spezzamento su $\mathbb{Q}$; $\mathbb{Q}(i)$; $\mathbb{F}_7$

$\mathbb{Q}$:
Individuiamo le radici di $f(x)$ e ricaviamone il campo di spazzamento di $f(x)$.
$\mathbb{Q}\left(\pm\sqrt{2+\sqrt{2}}\,;\ \pm\sqrt{2-\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\,;\ \sqrt{2-\sqrt{2}}\right)$
La torre delle estensioni è:
$\mathbb{Q} \to^4 \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) \to^1 \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\,;\ \sqrt{2-\sqrt{2}}\right)$

4:
In quanto $f(x)$ non ha radici in $\mathbb{Q}$ e dunque non è spezzabile nel prodotto di un monomio per qualcosa e siccome i prodotti fra radici non sono comunque appartenenti a $\mathbb{Q}$ non scomponibile nemmeno come prodotto di due funzioni di secondo grado, in altre parole $f(x)$ è irriducibile e monico, dunque è il polinomio minimo di $\sqrt{2+\sqrt{2}}$

1:
Basta osservare che $\sqrt{2+\sqrt{2}}\ \cdot\sqrt{2-\sqrt{2}} = \sqrt{2} \in \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$
Volendo esibire il polinomio di primo grado che annulla $\sqrt{2-\sqrt{2}}$ in $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$:
$p(x) = \sqrt{2+\sqrt{2}}\cdot x - \left(\left(\sqrt{2+\sqrt{2}}\right)^2 - 2\right)$

Dunque $\left[\mathbb{Q}\left(\sqrt{4+\sqrt{2}}\,;\ \sqrt{4-\sqrt{2}}\right) : \mathbb{Q}\right] = 4$

$\mathbb{Q}(i)$:
Con procedimento identico (Le radici sono tutte reali) si ottiene:
$\left[\mathbb{Q}\left(\sqrt{4+\sqrt{2}}\,;\ \sqrt{4-\sqrt{2}}\,;i\right) : \mathbb{Q}(i)\right] = 4$

$\mathbb{F}_7$:
In $\mathbb{F}_7$ esiste un valore che l quadrato faccia 2, dunque possiamo fattorizzare $f(x)$ come:
$x^4 - 4x^2 + 2 = (x^2 - 5)(x^2 + 1)$ che sono entrambi irriducibili per verifica diretta (I quadrati in $\mathbb{F}_7$ sono rispettivamente $\{1,4,2,2,4,1\}$ e $5, -1$ non appartengono a questo insieme.
Dunque il campo di spezzamento di $f(x)$ è $\mathbb{F}_{7^2}$ di grado 2 in quanto è il minimo comune multiplo fra i gradi delle due estensioni.

Esempio 2 (Radici n-esime dell'unità):

Siano $f(x) = x^{24} - 1$; $g(x) = x^8 - 1$ e $h(x) = x^3 - 1$ K, E, F i loro rispettivi campi di spezzamento su $\mathbb{Q}$.

a. Dimostrare che $K = EF$

b. Sia $L = K \cap \mathbb{R}$. Determinare una base di L come $\mathbb{Q}$ spazio vettoriale.

a.

Dimostriamo la doppia inclusione. I generatori di EF sono la radice ottava e la radice terza dell'unità. Ma entrambe queste radici elevate alla 24 fanno 1, dunque appartengono a K.

Al contrario vogliamo mostrare che il generatore di K, ossia la rdice ventiquattresima dell'unità, è ottenibile partire da $\mathbb{Q}$; ξ_3 ; ξ_8.

Ma $\xi_8^3 \xi_3^{-1}$ è una radice 24-esima dell'unità. Scelgo questi valori sfruttando la forma esponenziale: $e^{k\frac{2i\pi}{8}} e^{h\frac{2i\pi}{3}} = e^{(3k+8h)\frac{2i\pi}{24}} = e^{\frac{2i\pi}{24}} = \xi_{24}$ scegliendo $k = 3$; $h = -1$

b.

L'idea è di capire come sono fatte le due singole estensioni e poi provare d accostarle.

Il campo di spezzamento di $x^3 - 1$ su $\mathbb{Q}$ è $\mathbb{Q}(i\sqrt{3})$ mentre il campo di spezzamento di $x^8 - 1$ su $\mathbb{Q}$ è $\mathbb{Q}(\sqrt{2}, i)$. Per il risultato precedente $K = \mathbb{Q}(i\sqrt{3}, \sqrt{2}, i) = \mathbb{Q}(i, \sqrt{3}, \sqrt{2})$ e $K \cap \mathbb{R} = \mathbb{Q}(\sqrt{3}, \sqrt{2})$ che ha grado 4 e h come base: $\{1, \sqrt{3}, \sqrt{2}, \sqrt{6}\}$

Idea (Radici n-esime):

È utile ricordare che una radice n-esima dell'unità è calcolabile mediante la formula: $\cos\left(\frac{2\pi}{n}\right) + i \cdot \sin\left(\frac{2\pi}{n}\right)$

Inoltre le radici di un polinomio della forma $x^n - 1$ sono tutte generate dalla radice n-esima dell'unità.

Nel caso n cui si stia lavorando con un polinomio del tipo $x^n - k$ allora tutte le radici saranno generate da $\sqrt[n]{k}$ ·radice n-esima dell'unità.

Può essere utile scriverli in forma esponenziale $\xi_n = e^{\frac{2i\pi}{n}}$; vale $\xi_n^{n-1} + \xi_n^{n-2} + \cdots + \xi_n + 1 = 0$

Si dicono primitive le radici n-esime che generano il gruppo, sono quelle di esponente coprimo con n dunque sono $\phi(n)$

Osservazione: Per ogni radice n-esima ξ_n vale $(\xi_n + \xi_n^{-1}) \in \mathbb{R}$

Ricordare:

$\sqrt{3} \in \mathrm{cds}(x^3 - 1)$; $\sqrt{5} \in \mathrm{cds}(x^5 - 1)$

Esempio 3 (C.d.s. Teorico):
Sia $f(x) = x^4 - x^3 + x^2 - x + 1 \in \mathbb{Q}[x]$ e α una sua radice complessa. Determinare in funzione di c il valore di $[\mathbb{Q}(\alpha + c\alpha^{-1}) : \mathbb{Q}]$

Se riuscissimo a determinare $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ avremmo che $[\mathbb{Q}(\alpha + c\alpha^{-1}) : \mathbb{Q}]$ lo divide.
$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1,2,4$ perché deve dividere il grado del polinomio.
Non può essere 1 in quanto i valori appartenenti a $\mathbb{Q}$ che possono annullare questo polinomi devono essere della forma $\frac{a}{b}$ con a trmine noto e b coefficiente di grado massimo, in questo caso dunque solo ± 1 e $f(1) = 1$; $f(-1) = 5$
Proviamo costruire una fattorizzazione in prodotto di polinomi di secondo grado (Metodo della forza bruta):
$(x^2 + Ax + B)(x^2 + Cx + D) = x^4 + (D + B)x^3 + (E + BD + C)x^2 + (BE + CD)x + (CE)$
Da cui:
$$\begin{cases} D + B = -1 \\ E + BD + C = 1 \\ BE + CD = -1 \\ CE = 1 \end{cases}$$
Osserviamo che dall'ultima equazione $C = E = \pm 1$ ma inserendola nella terza se fosse -1 otterremmo un assurdo con la prima. Dunque $C = E = 1$ e il sistema si riduce a:
$\begin{cases} D + B = -1 \\ BD = -1 \end{cases} \rightarrow B(-1 - B) = -1 \rightarrow B^2 + B - 1 = 0 \rightarrow B \notin \mathbb{Q}$ Assurdo.
Dunque $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$

Dobbiamo capire se $[\mathbb{Q}(\alpha + c\alpha^{-1}) : \mathbb{Q}]$ è 1,2 o 4.
Se fosse 1 avremmo che $\alpha + c\alpha^{-1} \in \mathbb{Q} \rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ Assurdo.
Se fosse 2 significa che gli elementi $\{(\alpha + c\alpha^{-1}), \alpha + c\alpha^{-1}, 1\}$ sono linearmente dipendenti come $\mathbb{Q}$-spazio vettoriale.
Ricordiamo che per ipotesi $\{\alpha^3, \alpha^2, \alpha, 1\}$ sono indipendenti e che $\alpha^4 = \alpha^3 - \alpha^2 + \alpha - 1$ dunque:
$\{(\alpha + c\alpha^{-1}), \alpha + c\alpha^{-1}, 1\} = \{\alpha^2 + 2c + c^2\alpha^{-2}, \alpha + c\alpha^{-1}, 1\} =$
$=^{\cdot \alpha^2} \{\alpha^4 + 2c\alpha^2 + c^2, \alpha^3 + c\alpha, \alpha^2\} = \{\alpha^3 + (2c - 1)\alpha^2 + \alpha + (c^2 - 1), \alpha^3 + c\alpha, \alpha^2\}$ in vettori:
$\begin{pmatrix} 1 \\ 2c - 1 \\ 1 \\ c^2 - 1 \end{pmatrix}$; $\begin{pmatrix} 1 \\ 0 \\ c \\ 0 \end{pmatrix}$; $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ che sono dipendenti $\leftrightarrow c = 1$
Dunque se $c = 1$ $[\mathbb{Q}(\alpha + c\alpha^{-1}) : \mathbb{Q}] = 2$ altrimenti $[\mathbb{Q}(\alpha + c\alpha^{-1}) : \mathbb{Q}] = 4$