TEORIA DEI CAMPI

Titolo nota 04/09/2007

K campo se sono definite due operazioni interne $+, \cdot \; K \times K \to K$ in modo che
$(K, +, 0)$ è un gruppo abeliano (cioè commutativo)
$(K \setminus \{0\}, \cdot, 1)$ è un gruppo abeliano
e vale la proprietà distributiva.
K è finito se $|K| < +\infty$
p polinomio a coefficienti in K è una scrittura del tipo $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_i \in K$.
$p : K \to K$ è una funzione polinomiale se

$p(a) = a_n a^n + \dots + a_0$ con $a_i \in K$ e non dipendono da a.

$K = \mathbb{F}_p$ $\quad p(x) = x \quad p(x) = x^p$

(commutativo con unità).

A Anello se sono definite due operazioni interne $+, \cdot$

$(A, +, 0)$ è gr. abeliano

$\cdot \; A \times A \to A$ associativa (con l'elemento neutro 1)

commutativa

e vale la proprietà distributiva. Esempio: $\mathbb{Z}$

$1 \in A \quad 1+1 \in A \quad 1+1+1 \in A, \dots,$

Se sono tutti distinti, $\mathbb{Z} \hookrightarrow A$ e si dice che

la <u>caratteristica di A è 0</u>.

Se invece si ripetono, $\exists$ numero naturale n t.c. $n \cdot 1 = 0$

n si dice caratteristica di A se è il minimo per cui vale questa proprietà.

La caratteristica di un campo è 0 oppure un numero primo. Se $6 \cdot 1 = 0$ $(2\cdot 1)\cdot(3\cdot 1) = 0$ $\mathbb{Z}/_{6\mathbb{Z}}$

$a \cdot b = 0$ $a^{-1} \cdot a \cdot b = 0 \Rightarrow b = 0$ oppure a era già 0.

$p(x)$ polinomio a coefficienti in K la funzione polinomiale associata a $p: K \to K$ sia p. Allora un elemento $a \in K$ tale che $p(a) = 0$ si dice <u>radice</u> <u>di p</u> <u>in K</u>.

I polinomi a coefficienti in K formano un anello $K[x]$.
Le unità di un anello sono gli elementi che hanno un inverso moltiplicativo.

Un polinomio è irriducibile se si può solo fattorizzare con elementi che siano tutte unità tranne uno.

$$x + 1 = (x+1) \cdot \frac{1}{2} \cdot \sqrt{2} \cdot \sqrt{2} \quad \text{in } \mathbb{R}[x]$$

Un elemento primo di un anello è un elemento che, se divide il prodotto di due fattori, allora divide anche almeno uno dei fattori.

In $K[x]$ primo e irriducibile coincidono.

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ $\qquad \alpha^2+\alpha+1=0 \qquad 1+1=0 \qquad \frac{1}{\alpha}? \quad \frac{1}{\alpha} = \alpha+1$

$(\alpha+1)^2 = \alpha^2 + \cancel{2\alpha} + 1 = \alpha$

$p(x) = x^2+x+1 \in \mathbb{F}_2[x] \qquad \mathbb{F}_2 \hookrightarrow \mathbb{F}_4 \qquad p(x) \hookrightarrow \mathbb{F}_4[x]$

in $\mathbb{F}_4$ p ha due radici: α e $\alpha+1$.

$$\frac{-1 \pm \sqrt{1-4}}{2}$$

In caratteristica p, $(a+b)^p = a^p + b^p$.

Tutti i campi finiti K hanno cardinalità $= p^k$ per qualche primo p, $k \geq 1$.

<u>Dim</u> K è finito $\Rightarrow$ ha caratteristica positiva p.

Ma allora $\mathbb{F}_p \hookrightarrow K$ $\quad \mathbb{F}_p \subset K \quad a \notin \mathbb{F}_p \quad a \in K$

$a \cdot \mathbb{F}_p \subset K$ e $|a \cdot \mathbb{F}_p| = p$ $\quad |a + \mathbb{F}_p| = p$ e $a + \mathbb{F}_p \cap \mathbb{F}_p = \emptyset$

$|\mathbb{F}_p \cdot (a + \mathbb{F}_p)| = p^2$ $\quad$ Se $x \in a + \mathbb{F}_p \cap \mathbb{F}_p$, $\quad x = k \quad k \in \mathbb{F}_p$

$x = h + a \quad h \in \mathbb{F}_p$

$x_1 \cdot (a + y_1) = x_2 \cdot a + y_2 \Rightarrow \begin{matrix} x_1 = x_2 \\ y_1 = y_2 \end{matrix}$ $\quad a = k - h \in \mathbb{F}_p$ assurdo.

Se $\mathbb{F}_p \cdot (a + \mathbb{F}_p) \neq K$, scelg $b \in K \setminus (\mathbb{F}_p \cdot (a + \mathbb{F}_p))$ $\quad b + \mathbb{F}_p$

$A, B \subset K$

$A \cdot B = \{ c \in K \mid \exists a, b \; a \in A \; b \in B \; c = a \cdot b \}$

Induttivamente, alla fine avremo

$K = \mathbb{F}_p \cdot (a_1 + \mathbb{F}_p) \cdot (a_2 + \mathbb{F}_p) \cdot \quad \dots \quad \cdot (a_k + \mathbb{F}_p)$

$\Rightarrow |K| = p^k$. $\quad K = \{ (x_1, \dots, x_n) \mid x_i \in \mathbb{F}_p \}$

$(0,0) = (0,1) \cdot (1,0)$ in $\mathbb{F}_2 \times \mathbb{F}_2$

$1 \quad \alpha$

$1, \quad \alpha+1$

$$(0,0) \longrightarrow 0$$
$$(1,0) \longrightarrow 1$$
$$(0,1) \longrightarrow \alpha$$
$$(1,1) \longrightarrow \alpha+1$$

Un corpo è un campo in cui la moltiplicazione può non essere commutativa.

Esempio: $\left\{ a+bi+cj+dk \mid a,b,c,d \in \mathbb{R},\ i^2=j^2=k^2=-1,\ ij=k \quad ji=-k \right\}$

$$(a+bi+cj+dk)(a-bi-cj-dk) \in \mathbb{R}$$

Teorema di Wedderburn: Ogni corpo finito è un campo.

Teorema di Jacobson: A anello in cui $\forall a \in A \ \exists\, n(a) \in \mathbb{N}$ tale che $a^{n(a)} = a \Rightarrow A$ è un campo.

Esercizio: $t>1$ $t \in \mathbb{N}$. $t^m-1 \mid t^n-1 \iff m \mid n$.

$K[x]$ è un anello euclideo.

Cioè il grado è una funzione che cala facendo la divisione con il resto.

Perciò $K[x]$ ha la fattorizzazione unica in irriducibili.

Se $p(x) = \prod_{i=1}^{n} q_i(x) = \prod_{i=1}^{m} r_i(x)$ con r_i e q_i irriducibili,

allora $n=m$ e esiste una corrispondenza $\sigma : \{1,..,n\} \to \{1,\dots,n\}$

tale che $q_i(x) = r_{\sigma(i)}(x) \cdot u_i(x)$ $u_i(x)$ unità, $(u_i(x) = u_i \in K)$

$\mathbb{Z}/6\mathbb{Z}$ $\quad 2 = 2 \cdot 4$ $\quad \mathbb{Z}[\sqrt{-5}] = \{ n + m\sqrt{-5} \mid n, m \in \mathbb{Z} \}$

$3^2 = (2+\sqrt{-5})(2-\sqrt{-5})$ $\quad |n+m\sqrt{-5}| = n^2+5m^2$

$p(x) \in K[x]$ $\deg p = n \Rightarrow p$ ha al più n radici in K.

Ruffini: Se $\alpha \in K$ è radice di p $x-\alpha \mid p(x)$. in $K[x]$.

Corollario: $\mathbb{F}_{p^k} \setminus \{0\}$ come gruppo moltiplicativo è ciclico.

<u>Dim</u> $\mathbb{F}^*_{p^k} = \mathbb{F}_{p^k} \setminus \{0\}$ $\left| \mathbb{F}^*_{p^k} \right| = p^k - 1$ elementi.

$p^k - 1 = \prod_{i=1}^{h} q_i^{\alpha_i}$ q_i primi $\alpha_i \geq 1$ q_i distinti

$a \in \mathbb{F}^*_{p^k}$, $a^{p^k - 1} = 1$ Sia a un elemento con ordine la massima potenza possibile di q_1. Sia q_1^β $\beta < \alpha_1$

$a^{q_1^\beta} = 1$ $(a^n)^{q_1^\beta} = 1$ ho q_1^β elementi tali che $x^{q_1^\beta} = 1$.

$x^{q_1^\beta} - 1 \in \mathbb{F}_{p^k}[x]$ Non può avere più di q_1^β radici.

$\Rightarrow$ Tutti gli elementi di ordine una potenza di q_1 sono potenze di a.

Così procedendo, ottengo h elementi $a_1 \cdots a_h$ di ordine $q_1^{\beta_1} \ldots q_h^{\beta_h}$ massimale.

$\overline{a} = a_1 \cdot a_2 \cdot \ldots \cdot a_h$ ha ordine $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_h^{\beta_h}$.

$\mathbb{F}_4$ $\quad \alpha \quad \alpha^2 = \alpha+1 \quad \alpha^3 = 1$

$\mathbb{F}_8$ $\quad 0, 1, \beta, \beta+1, \beta^2, \beta^2+1, \beta^2+\beta+1, \beta^2+\beta \qquad \beta^3+\beta+\cancel{1}=0.$

$\mathbb{F}_9$ $\quad 0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2 \qquad 1+1+1=0 \qquad \alpha^2-\alpha-1=0$

$\alpha^2 = \alpha+1$

$1, \beta, \beta^2, \beta+1, \beta^2+\beta, \beta^2+\beta+1, \beta^2+1, 1$

$1, \alpha, \alpha+1, 2\alpha+1, 2, 2\alpha, 2\alpha+2, \alpha+2, 1.$

Criterio della radice razionale.

$p(x) \in \mathbb{Z}[x] \qquad q \in \mathbb{Q}$ radice di $p \qquad q = \frac{m}{n}$ ai minimi termini. $\qquad p(x) = a_n x^n + \dots + a_0$

$\Rightarrow \quad n \mid a_n \quad m \mid a_0. \qquad$ (Se p è monico, $q \in \mathbb{Z}$)

Eisenstein: $\quad p(x) \in \mathbb{Z}[x] \quad$ se $\quad p(x) = a_n x^n + \dots + a_0$ e

$\exists p$ t.c. $\quad p \nmid a_n, \; p \mid a_{n-1}, p \mid a_{n-2}, \dots, p \mid a_1, p \mid a_0$ ma $p^2 \nmid a_0$

$\Rightarrow p$ è irriducibile in $\mathbb{Z}[x]$

Se $\overset{\text{monico}}{p(x)} \in \mathbb{Z}[x]$ e $\overline{p}(x) \in \mathbb{F}_p[x]$ ottenuto da $p(x)$ riducendo i coefficienti modulo p, e $\overline{p}(x)$ è irriducibile in $\mathbb{F}_p[x]$

Allora $p(x)$ è irriducibile in $\mathbb{Z}[x]$.

$p(x) \in K[x]$ $\quad a \in K$. Se a è radice di $p(x)$,

$p(x) = (x-a)\, q(x)$. Si può supporre che $p(x) = (x-a)^m \cdot \overline{q}(x)$

$\overline{q}(a) \neq 0$. Chiamiamo m <u>la molteplicità di a come radice</u> di p in K. Se $m>1$ a è una radice multipla.

$p(x)$ ha radici multiple in qualche estensione di K $\iff$ $p(x)$ e $p'(x)$ hanno fattori comuni.

Se p è irriducibile? In caratteristica 0 non ha mai radici multiple. In caratteristica p:

$x^p - 1$ in $\mathbb{F}_p$ $\qquad\qquad$ $p(x) = a_n x^n + \dots + a_0$, $p'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1$

$x^p - 1 = (x-1)^p$

In $\mathbb{F}_{p^k}$, se $p'(x)=0 \Rightarrow p(x)= q(x^p)$

Se $q'(x)=0$ $q(x)=h(x^p)$ $p(x)=h(x^{p^2})$

$x^{p^m}-a$ $x^{p^k}-a=x^{p^k}-a^{p^k}=$
$=(x-a)^{p^k}$

$p(x)=H(x^{p^m})$ H irriduc. e $H'\neq 0$.

Le radici di p sono radici di $x^{p^m}=\lambda_i$ con λ_i radici distinte di H.

Se $\alpha^{p^m}=\lambda_i$, $x^{p^m}=\alpha^{p^m}$ $x^{p^m}-\lambda_i=(x-\alpha)^{p^m}$.

$p(x)\in\mathbb{F}_p[x]$ $x^p-a=x^p-a^p=(x-a)^p$.

$p(x)$ $x^{p^k}-x$ su $\mathbb{F}_p$. $a\in\mathbb{F}_{p^k}$ $a^{p^k}-a=0$

$p'(x)=-1$. $\Rightarrow p(x)$ ha radici distinte. Anzi, esse sono tutti e soli gli elementi di $\mathbb{F}_{p^k}$. Questo vuol dire che $\mathbb{F}_{p^k}$ è il campo di spezzamento di $p(x)$ su $\mathbb{F}_p$, cioè il più piccolo campo che contiene $\mathbb{F}_p$ in cui $p(x)$ si fattorizza in fattori lineari.

$p(x)\in K[x]$ $F\supset K$ $E\supset K$ in cui p si spezza in fattori Lineari, ma p non lo fa in nessun campo H, $K\subset H\subset F$ o $K\subset H\subset E$.

Allora F e E sono K-isomorfi, cioè

$\exists\ \varphi : F \to E$ e $\psi : E \to F$ iniettive e surgettive

tali che $\varphi(k) = k$ $\psi(k) = k$ $\forall k \in K$ e

$\varphi(a+b) = \varphi(a) + \varphi(b)$ $\varphi(ab) = \varphi(a)\varphi(b)$ $\varphi(1) = 1$ $a, b \in F$

$\psi(a+b) = \psi(a) + \psi(b)$ $\psi(ab) = \psi(a)\psi(b)$ $\psi(1) = 1$ $a, b \in E$.

$\varphi \circ \psi = Id_E$ $\psi \circ \varphi = Id_F$.

Corollario: Tutti i campi finiti con lo stesso numero di elementi sono isomorfi.

$p(x) \in \mathbb{F}_p[x]$ $\deg p = n$ irriducibile su $\mathbb{F}_p$

Come faccio a trovare un campo dove lui abbia una radice?

α $\mathbb{F}_p[\alpha]$, $p(\alpha) = 0$ $\beta \in \mathbb{F}_p[\alpha]$ $\beta = a_{n-1}\alpha^{n-1} + \cdots + a_0$ $a_i \in \mathbb{F}_p$.

$\frac{1}{\alpha}$? $p(\alpha) = 0 = b_n\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0$. $b_n\alpha^{n-1} + b_{n-1}\alpha^{n-2} + \cdots + b_1 + \frac{b_0}{\alpha} = 0$.

$-\frac{1}{b_0}(b_n\alpha^{n-1} + \cdots + b_1) \sim \frac{1}{\alpha}$

$$\alpha \cdot \left(-\frac{1}{b_0}\left(b_n\alpha^{n-1}+\dots+b_1\right)\right) = -\frac{1}{b_0}\left(p(\alpha)-b_0\right)=1.$$

$\cancel{\forall}\ \beta \in \mathbb{F}_p[\alpha]$ $\quad \mathbb{F}_p[\alpha] \longrightarrow \mathbb{F}_p[\alpha]$ $\quad |\mathbb{F}_p[\alpha]| = p^n.$

$\gamma \longmapsto \beta\cdot\gamma$

In $\mathbb{F}_{p^n}$ c'è una radice di $p(x)$.

Quindi ogni polinomio irriducibile di grado n ha una radice in $\mathbb{F}_{p^n}$

$\mathbb{F}_p \subset K \subset \mathbb{F}_{p^n}$ $\quad K\setminus\{0\} \subset \mathbb{F}_{p^n}\setminus\{0\}$ sottogruppo moltiplicativo

$\quad p^k-1 \qquad p^n-1 \qquad \Rightarrow p^k-1 \mid p^n-1 \Rightarrow k \mid n.$

$$x^{p^n}-x = \prod_{\substack{p \text{ irriduc.} \\ \deg p \mid n}} p(x) \qquad a \in \mathbb{F}_{p^n} \quad a^{p^n-1}=1$$

$\lambda \in K$ $\quad \lambda^k=1$ e $\lambda^h \neq 1$ $0<h<k$ $\quad \lambda$ si dice radice primitiva k-esima dell'1.

$k=p$ $\quad x^p-1=(x-1)(x^{p-1}+\dots+x+1)$

$K \subset E$ in E ci sono tutte le radici k-esime dell'unità, λ.

$p(x) = \prod_{\substack{\lambda\ k\text{-esima} \\ \text{primitiva}}} (x-\lambda) = \Phi_k(x)$ k-esimo polinomio ciclotomico su K.

$\Phi_k(x)$ ha coefficienti in K. $\qquad x^3-1 = (x-1)(x^2+x+1)$

$x^n - 1 = \prod_{d|n} \Phi_d(x)$

$n=4 \quad x^2+1$
$n=2 \quad x+1$
$n=1 \quad x-1$

$\Phi_{105}(x)$ su $\mathbb{Q}$ $\qquad \deg \Phi_n(x) = \varphi(n) \qquad \varphi(105)=48$

$-2x^{41} \qquad -2x^7 \qquad$ max coeff. $\sim \dfrac{j^{1/2}}{(\lg j)^4}$.

su $\mathbb{Q}$

$\Phi_{p^r}(x) = \Phi_p(x^{p^{r-1}}) \qquad n = \prod p_i^{\alpha_i} \quad \Phi_n(x) = \Phi_{p_1 p_2 \cdots p_k}\left(x^{p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1}}\right)$

$\Phi_{2n}(x) = \Phi_n(-x) \qquad p \nmid n \quad \Phi_{pn}(x) = \dfrac{\Phi_n(x^p)}{\Phi_n(x)} \qquad p \mid n \quad \Phi_{pn}(x) = \Phi_n(x^p)$

$\Phi_n(x) = \prod_{d|n} \left(x^{n/d} - 1\right)^{\mu(d)}$

$\mu(1) = 1$
$\mu(p_1 \cdots p_r) = (-1)^r$
$\mu(p^2 \cdot h) = 0$

$f(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} \mu(n/d) f(d) \qquad \sum_{d|n} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & n \neq 1 \end{cases}$ $\Big\}$ $\mathbb{1}$

$f = g * \mathbb{1} \qquad g = \mu * f \qquad \mu * \mathbb{1} = u$

su $\mathbb{Q}$

$\Phi_n(x)$ ha coeff. interi

$\Phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ è isomorfismo di Frobenius

$x \to x^p$

$\Phi(x) = x \iff x \in \mathbb{F}_p$ $\Phi^{(k)}(x) = x \iff x \in \mathbb{F}_{p^k}$

$Aut(\mathbb{F}_{p^n}) = \{ Id, \Phi, \Phi^{(2)}, \dots \Phi^{(n-1)} \}$.

I punti costruibili con riga e compasso sono quelli le cui coordinate si ottengono da $\mathbb{Q}$ con un numero finito di estensioni quadratiche. (aggiungo soluzione di x^2+ax+b)

x^3-2 non si può costruire

$4\cos^3\alpha - 3\cos\alpha = \underline{\cos 3\alpha}$

$x^p - x - a$ su $\mathbb{F}_p$ ha il ruolo di $x^p - a$ in car. 0.

$\alpha^p - \alpha - a = 0$ $(\alpha+1)^p - (\alpha+1) - a = \alpha^p + \cancel{1} - \alpha - \cancel{1} - a = 0$

$\alpha, \alpha+1, \alpha+2, \dots \alpha+p-1$