Campi finiti

Titolo nota 08/09/2011

$\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ $\quad \mathbb{F}_p$

$\mathbb{F}_2$ $\quad x^2+x+1$ $\quad \alpha^2+\alpha+1=0$ $\quad$ 0 1 / α $\alpha+1$

$\alpha+\alpha+1=1$ $\quad \alpha+1+1=\alpha$ $\quad \alpha\cdot(\alpha+1)=\alpha^2+\alpha=\alpha+1+\alpha=$

$=1$ $\quad \alpha\cdot\alpha=\alpha+1$ $\quad \mathbb{F}_4$

$\mathbb{F}_p$ $\quad x^2-x+1$ $\quad \alpha^2-\alpha+1=0$

$\frac{1}{\alpha}=1-\alpha$ $\quad \mathbb{F}_{p^2}=\{\alpha x+y \mid x,y\in\mathbb{F}_p\}$

$a+b\sqrt{d}$

$\mathbb{F}_{16}$ $\quad x^4+x+1$ irriducibile su $\mathbb{F}_2$

Infatti x^2+x+1 è l'unico di grado 2, ma

$(x^2+x+1)^2=x^4+x^2+1$ $\quad (a+b)^p=a^p+b^p$

K campo. 1) Se $\exists k$ t.c. $\overbrace{1+1+1+1+\dots+1}^{k \text{ volte}}=0$

dico che $\operatorname{char} K=\min\{k>0 \mid \overbrace{1+1+\dots+1}^{k}=0\}$

2) Se non $\exists k$ come sopra, dico che $\operatorname{char} K=0$

Oss. Se $\operatorname{char} K>0$, è un numero primo. Un campo finito ha $\operatorname{char} K>0$.

0 1 α $\alpha+1$

α^2 α^2+1 $\alpha^2+\alpha$ $\alpha^2+\alpha+1$

α^3 α^3+1 $\alpha^3+\alpha$ $\alpha^3+\alpha+1$

$\alpha^3+\alpha^2$ $\alpha^3+\alpha^2+1$ $\alpha^3+\alpha^2+\alpha$ $\alpha^3+\alpha^2+\alpha+1$

$(\alpha^2+\alpha)^2+(\alpha^2+\alpha)+1=$

$=\alpha+\alpha+\alpha^2+\alpha^2+\alpha+\alpha+1=$

$=0$

$\frac{1}{\alpha}=\alpha^3+1$ $\quad (x^3+x+1,\ x^4+x+1)=1$

Esistono $P(x)$ $Q(x)$ tali che

$$P(x)\cdot(x^3+x+1)+Q(x)(x^4+x+1)=1$$

in $\mathbb{F}_2[x]$ $\quad P(\alpha)(\alpha^3+\alpha+1)+Q(\alpha)(\alpha^4+\alpha+1)=1$

quindi $P(\alpha)$ è l'inverso di $\alpha^3+\alpha+1$.

$\beta^3+\beta+1=0$

$\mathbb{F}_8$ $\quad 0\ 1\ \beta\ \beta+1$
$\beta^2\ \beta^2+1\ \beta^2+\beta\ \beta^2+\beta+1$

Teorema: K campo finito $|K|=p^k$

Dim. $\operatorname{char} K=p$. $\quad 0,1,1+1,1+1+1,\dots,p-1$

$\Rightarrow K\supseteq\mathbb{F}_p$ $\quad$ Se $K=\mathbb{F}_p$ ok. $\quad b_1=1$

Altrimenti $\exists\ b_2\in K\setminus\mathbb{F}_p$ $\quad \overbrace{b_2\cdot 0\ b_2\cdot 1\ b_2\cdot 2\ \dots\ b_2\cdot(p-1)}^{p}$

$n(b_2+a)$ $\qquad b_2\cdot\mathbb{F}_p$

$V_1=\mathbb{F}_p$

$$V_2=\mathbb{F}_p+(b_2\cdot\mathbb{F}_p)=\{n\cdot b_2+a \mid n,a\in\mathbb{F}_p\}$$

$n_1b_2+a_1=n_2b_2+a_2$ $\qquad b_2=\dfrac{a_2-a_1}{n_1-n_2}\in\mathbb{F}_p$ ass. se $n_1\neq n_2$

e se $n_1=n_2$ $\quad a_1=a_2$

$|V_2|=p^2$ $\qquad$ Induzione

Quando $V_k=K$ $\quad |K|=p^k$. $\square$

Se G è un gruppo e $p\mid|G|$ allora esiste

$g\in G$ t.c. $\operatorname{ord}(g)=p$.

$K \supseteq \mathbb{F}_p$ $\quad$ K è uno spazio vett. su $\mathbb{F}_p$

$v_1, \dots, v_k$ $\quad$ $a_1 v_1 + \dots + a_k v_k$

$a_1, \dots, a_k \in \mathbb{F}_p$

$|K| = p^k$

$\mathbb{F}_{p^k}$ $\quad$ $\mathbb{Z}_{p^k}$

$\wr$ $\quad$ $(\mathbb{F}_p)^k$ $\quad$ $= \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{F}_3\}$

Per i coraggiosi: $\mathbb{F}_{27}$ $\quad$ $27 = 3^3$

$(a, b, c) \cdot (d, e, f) = (?, ?, ?)$

Osservazioni: $\mathbb{F}_{p^k}^*$ è ciclico.

$\mathbb{F}_{p^k} \setminus \{0\}$

Teorema: tutti i campi con p^k elementi sono isomorfi

$\mathbb{F}_p$ $\quad$ $p(x)$ irriducibile $\quad$ posso costruire un campo che contiene $\mathbb{F}_p$ e una radice di $p(x)$.

$$Q(x) = x^{p^k} - x = \prod_{p_i \text{ irr.}} p_i(x)$$

Se α_1 è radice di $Q(x)$, trovo $K_1 \supseteq \mathbb{F}_p$ e $K_1 \ni \alpha_1$

Se $Q(x)$ non si spezza in fattori lineari su K_1, prendo α_2 radice di un fattore irriducibile di grado ≥ 2 e costruisco $K_2 \supseteq K_1$

Induzione: $\exists K_j$ in cui $Q(x)$ ha tutte le radici

$Q'(x) = -1$ quindi $Q(x)$ ha p^k radici distinte.

Sia $\mathbb{F}_{p^k} = \{\alpha \in K_j \text{ t.c. } Q(\alpha)=0\}$

$0, 1 \in \mathbb{F}_{p^k}$ $\quad \alpha_1, \alpha_2 \in \mathbb{F}_{p^k}$ $\quad (\alpha_1 \cdot \alpha_2)^{p^k} = \alpha_1^{p^k} \cdot \alpha_2^{p^k} = \alpha_1 \cdot \alpha_2$

$\Rightarrow \alpha_1 \cdot \alpha_2 \in \mathbb{F}_{p^k}$.

$(\alpha_1 + \alpha_2)^{p^k} = \alpha_1^{p^k} + \alpha_2^{p^k} = \alpha_1 + \alpha_2 \Rightarrow \alpha_1 + \alpha_2 \in \mathbb{F}_{p^k}$.

$\left(\frac{1}{\alpha_1}\right)^{p^k} = \frac{1}{\alpha_1^{p^k}} = \frac{1}{\alpha_1} \Rightarrow \frac{1}{\alpha_1} \in \mathbb{F}_{p^k}$.

$\mathbb{F}_{p^k}$ ha grado k su $\mathbb{F}_p$

Più in generale, se $F \subseteq K$ K è spazio vettoriale su F $\dim_F K$ è detta grado di K su F, $[K:F]$.

$[\mathbb{F}_{16} : \mathbb{F}_4]$? $\quad (a, b) \quad a, b \in \mathbb{F}_4$

$[\mathbb{F}_{16} : \mathbb{F}_4] = 2$

$[\mathbb{F}_{16} : \mathbb{F}_2] = 4 \quad [\mathbb{F}_4 : \mathbb{F}_2] = 2$

$[\mathbb{F}_{16} : \mathbb{F}_2] = [\mathbb{F}_{16} : \mathbb{F}_4] \cdot [\mathbb{F}_4 : \mathbb{F}_2]$

$\mathbb{F}_{16}$
| 2
$\mathbb{F}_4$
| 2
$\mathbb{F}_2$

4

Automorfismo di Frobenius:

$\Phi : \mathbb{F}_{p^k} \longrightarrow \mathbb{F}_{p^k}$
$x \longmapsto x^p$

$\Phi(x+y) = \Phi(x) + \Phi(y)$
$\Phi(xy) = \Phi(x)\Phi(y)$
$\Phi(0) = 0 \quad \Phi(1) = 1$

$\Phi(x) = x \quad x^p - x = 0 \Leftrightarrow x \in \mathbb{F}_p$

$p(x) \in \mathbb{F}_p[x] \quad \Phi(p(x)) = p(x)$

$p(\alpha) = 0 \quad \Phi(p(\alpha)) = p(\alpha^p) = 0$

$\Phi(\Phi(\alpha)) = \alpha^{p^2} \quad \Phi^{(i)}(\alpha) = \alpha^{p^i} \quad \alpha^{p^k} = \alpha$

1) $\Phi^{(k)}$ è l'identità su $\mathbb{F}_{p^k}$

2) così trovo k radici distinte se $ord(\alpha) = p^k - 1$

$$\begin{cases} X_0 = 4 \\ X_1 = X_2 = 0 \\ X_3 = 3 \\ X_{n+4} = X_n + X_{n+1} \end{cases}$$

$$X_\alpha \equiv X_{\alpha \cdot p^k} \pmod p$$

$$p(t) = t^4 - t - 1 \qquad \alpha_1, \alpha_2, \alpha_3, \alpha_4$$

$$X_n = C_1 \alpha_1^n + C_2 \alpha_2^n + \dots + C_4 \alpha_4^n$$

$$X_{n \cdot p} = \left(C_1 \alpha_1^{np} + C_2 \alpha_2^{np} + \dots\right) =$$

$$= \left(d_1 \alpha_1^n + d_2 \alpha_2^n + \dots\right)^p \qquad d_i^p = C_i$$

$$X^{p^k} = X \qquad Y = \left(X^{p^{k-1}}\right)^p$$

$$\boxed{C_1 = C_2 = \dots = 1}$$

$$= (X_n)^p \equiv X_n \pmod p$$

$$X_{n \cdot p^k} = \Phi^{(k)}\left(\alpha_1^n + \dots + \alpha_4^n\right) \equiv X_n \pmod p$$

X_{n+1} = espressione nei termini precedenti

$q(X)$ irriduc. mod p.

$\alpha \in \mathbb{F}_{p^k}$ $\quad k = \deg q \quad$ $\alpha^{p^k} = \alpha$

Periodicità $\mid p^k - 1$

$\Phi^{(i)}(\alpha)$ sono tutte le radici di $q(x)$

$$\alpha_1^n + \dots + \alpha_k^n$$

$\alpha^m \equiv 1 \qquad \Phi(\alpha)^m = \Phi(\alpha^m) = 1$

Ricorrenza a 3 termini che mod 3 abbia periodo 13

$\alpha^{26} = 1$ $(\mathbb{F}_{27})$

$\alpha^{13} = 1$

$\varphi(26) = 12$

$\varphi(13) = 12$

$\varphi(2) = 1$

$\varphi(1) = 1$

Se β va bene, $\Phi(\beta) = \beta^3$

e $\Phi^{(2)}(\beta) = \beta^9$ va bene

α genera $\mathbb{F}_{27}^*$ $\Rightarrow$ α^2 ha ordine 13

$\alpha^3 - \alpha - 1$

$\alpha^3 = \alpha + 1$

$\alpha^9 = (\alpha+1)^3 = \alpha^3 + 1$

$= \alpha + 2$

$\beta = \alpha^2$, $\beta^3 = \alpha^6 = (\alpha^3)^2 = (\alpha+1)^2 = \alpha^2 + 2\alpha + 1$

$\alpha^{18} = (\alpha^2 + 2\alpha + 1)^3 = \alpha^6 + 2\alpha^3 + 1$

$= \alpha^2 + 2\alpha + 1 + 2\alpha + 2 + 1 =$

$= \alpha^2 + \alpha + 1$

$(X - \alpha^2)(X - (\alpha^2 + 2\alpha + 1))(X - (\alpha^2 + \alpha + 1)) =$

$= X^3 - X^2 \cdot 2 - 2X - 1$

$-1 = \alpha^{26}$

$X_{n+1} = 2X_n + 2X_{n-1} + 1$

$$(X-\alpha)(X-\alpha^p)(X-\alpha^{p^2}) = X^3 - X - 1$$

$$a_1 \alpha^n + a_2 \alpha^{np} + a_3 \alpha^{n \cdot p^2}$$

$n \mapsto n+13$ $\quad X_{n+13} = a_1 \alpha^{n+13} + a_2 \alpha^{3(n+13)}$

$$+ a_3 \alpha^{9(n+13)}$$

$$= - X_n$$

K campo finito, $x^2 - 5$ irriducibile

char $K \neq 2$

$x^5 + a$ è riducibile su $K[x]$

$\left(\frac{5}{p}\right) = -1 \iff \left(\frac{p}{5}\right) = -1 \qquad (p \equiv 2, 3 \ (5))$

$x \longmapsto x^5$ è surgettivo $(-a = q^5)$

$(5, p^n - 1) \neq 1 \Longrightarrow n$ pari (perché $p \not\equiv \pm 1$)

Siamo in $\mathbb{F}_{p^{2a}} \supseteq \mathbb{F}_{p^2}$

Teo $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^h} \iff k \mid h$ $\qquad (p^k)^m$ elementi

$x^{p^k} = x$

$\mathbb{F}_{p^2} = \mathbb{F}_p + \mathbb{F}_p \sqrt{a}$

$\Rightarrow x^2 - 5$ è riducibile

$$\begin{cases} a_0 = 2 \\ a_{k+1} = 2a_k^2 - 1 \end{cases} \qquad p \mid a_n \Rightarrow 2^{n+3} \mid p^2 - 1$$

$2t^2 - 1 \qquad 2\cos^2\vartheta - 1 = \cos(2\vartheta)$

$2\cosh^2 x - 1 = \cosh(2x)$

$\cosh x = \dfrac{e^x + e^{-x}}{2} \qquad \cosh(ix) = \cos(x)$

$a_k = \cosh(b_k) \qquad a_{k+1} = \cosh(2b_k)$

Esiste b_0 : $a_0 = \cosh(b_0)$

$a_k = \cosh(2^k b_0)$

$$a_k = \frac{A^{2^k} + A^{-2^k}}{2}$$

$A = 2 + \sqrt{3}$

$$0 \equiv a_k \equiv \frac{(2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}}{2} \qquad \mathbb{F}_{p^2}$$

$$(2+\sqrt{3})^{2^k} = -(2-\sqrt{3})^{2^k}$$

$(2+\sqrt{3})(2-\sqrt{3}) = 1$

$(2+\sqrt{3})^{2^{k+1}} = -1 \qquad \mathbb{F}_{p^2}$

$\operatorname{ord}_{\mathbb{F}_{p^2}}(2+\sqrt{3}) = 2^{k+2} \qquad x^{p^2-1} = 1$

$2^{k+2} \mid p^2 - 1$

$(2+\sqrt{3}) = \dfrac{(1+\sqrt{3})^2}{2}$

$p \mid a_k = 2a_{k-1}^2 - 1 \qquad 2 \equiv (a_{k-1}^{-1})^2 \pmod{p}$

$(2+\sqrt{3}) = B^2 \qquad B \in \mathbb{F}_{p^2}$

$\operatorname{ord} B = 2^{k+3}$

$$X^{p^k} - X = \prod q_i(x)$$

q_i irr, monici

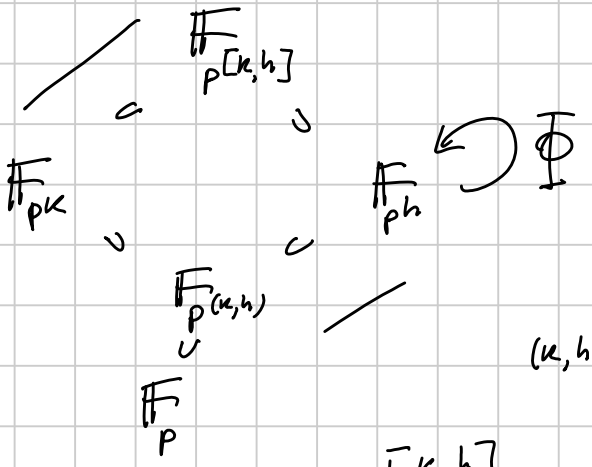
$\deg q_i \mid k$

α radice sx. $\quad \alpha \in \mathbb{F}_{p^h} \quad h \mid k$

$$1, \alpha, \alpha^2, \dots, \alpha^{h-1}, \alpha^h$$

$$\alpha^h = c_{h-1}\alpha^{h-1} + \dots + c_0$$

$q(x)$ un polin. grado min. risp. da α

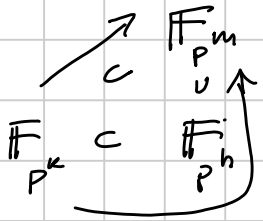


$(k,h)\,[k,h] = kh$

$$\frac{[k,h]}{k} = \frac{h}{(k,h)}$$

$F_1 \ast \left(\Phi^{(i)}\right) = \mathbb{F}_{p^i}$

$\mathbb{F}_8 \subseteq \mathbb{F}_{16}$?



$h = 2k$

$m = 4k$

X^{p^a}