Stage Senior 2011 – Livello Advanced

Stampato integrale delle lezioni

Autori vari

Indice

SENIOR 2011 – ALGEBRA (Advanced)

Titolo nota 09/09/2011

$f(x+f(y)) = y + f(x)$

$x=0 \Rightarrow$ iniett. e surg. ; $\exists\, x_0 \in \mathbb{R}$ t.c. $f(x_0)=0 \rightsquigarrow x_0=0$

$y = f(z) \to$ Cauchy $\to f(x) = \pm x$ su $\mathbb{Q}$

$\{q_i\}_{i\in I}$ base $\qquad f(q_1) = -q_1 \qquad f(q_i) = q_i$

$f: \mathbb{R}\to\mathbb{R} \qquad g:\mathbb{R}\to\mathbb{R}$ periodiche $\qquad f(x)+g(x) = x \ \ \forall x\in\mathbb{R}$

Base di Hamel $= \{q_1\} \cup \{q_i\}_{i\in I}$

Ogni $x\in\mathbb{R}$ si scrive $c_1 q_1 + \sum_{i\in I} c_i q_i$ (↑ solo # finito $\neq 0$)

$f(x) = c_1 q_1 \qquad g(x) = x - c_1 q_1$

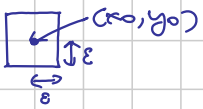
f: periodica di periodo uno qualunque dei $q_i \neq q_1$

g: periodica di periodo q_1

$f(x+q_i) = f(c_1 q_1 + \text{roba}) = c_1 q_1$

Se $f:\mathbb{R}\to\mathbb{R}$ è sol. della Cauchy e $\exists$ quadrato del piano in cui il grafico non entra, allora $f(x) = f(1)\,x \quad \forall x\in\mathbb{R}$.

Dim. Posso supporre WLOG che $f(x)\neq 0$ per ogni $x\in\mathbb{Q}$.
Suppongo $\exists\, y\in\mathbb{R}$ t.c. $f(y)\neq 0$ WLOG >0 (sia y, sia $f(y)$)
Allora il grafico entra in ogni $\square$.



Voglio entrare in $(x_0-\varepsilon, x_0+\varepsilon)\times(y_0-\varepsilon, y_0+\varepsilon)$
Considero
$f(q_1+q_2 y)$ con $q_1, q_2 \in \mathbb{Q}$
$= f(q_1) + q_2 f(y)$
$= q_2 f(y) \to q_2 f(y)$ può essere vicino a piacere a y_0
$\to q_1 + q_2 y$ " " " " " x_0

Frazioni egizie Dato $X \subseteq \mathbb{N}$ e $r \in \mathbb{Q}$ t.c.

$$\sum_{x \in X} \frac{1}{x} < r$$

Allora $\exists\ X \subseteq Y \subseteq \mathbb{N}$ t.c. $\sum_{y \in Y} \frac{1}{y} = r$.

Idea euristica: fare scendere il numeratore del resto. Sia $\frac{p}{q}$ il resto. Se uso $\frac{1}{n}$, il nuovo resto è

$$\frac{p}{q} - \frac{1}{n} = \frac{np-q}{nq} \qquad \text{Voglio } \begin{matrix} np-q \geq 0 \\ np-q < p \end{matrix} \quad \begin{matrix} n \geq \frac{q}{p} \\ (n-1)p < q \end{matrix} \quad n < \frac{q}{p} + 1$$

Quindi $n = \left\lceil \frac{q}{p} \right\rceil$. Due pbm: — già usato?
— succ. diverso?

Il successivo sarebbe $\left\lceil \frac{nq}{np-q} \right\rceil > \left\lceil \frac{q}{p} \right\rceil$. Basta che sia

$$\frac{nq}{np-q} \geq \frac{q}{p} + 1 = \frac{q+p}{p} \iff \cancel{npq} \geq \cancel{npq} + np^2 - q^2 - qp$$
$$\iff q^2 + qp \geq np^2 \iff \boxed{q(q+p) \geq np^2}$$

$\frac{1}{x_1} + \dots + \frac{1}{x_n} + \frac{1}{x_{n+1}} + \frac{1}{x_{n+2}} + \dots$ L'ultimo usato $\frac{1}{k}$ e $\frac{p}{q} < \frac{1}{k+1}$

$$\frac{p}{q} < \frac{1}{k+1} \implies \frac{q}{p} > k+1 \implies \left\lceil \frac{q}{p} \right\rceil \geq k+2 \quad \text{e quindi OK.}$$

Serve $q(q+p) \geq \left\lceil \frac{q}{p} \right\rceil p^2$; $p^2 \left\lceil \frac{q}{p} \right\rceil < p^2 \left(\frac{q}{p} + 1 \right) = pq + p^2 \leq pq + q^2$

Dim. Step 1 Partendo dal max di X aggiungo frazioni fino a quando posso
Step 2 Resto con $\lceil\ \rceil$.

— o — o —

RMM 2009-4 $\sum_{x \in X} \arctan\left(\frac{1}{x}\right) < \frac{\pi}{2}$ $\implies$ posso arrivare a $\frac{\pi}{2}$

Devo aggiungere $\sum_{z \in Z} \arctan\left(\frac{1}{z}\right) = \frac{\pi}{2} - \text{prec.}$

$$\tan\left(\quad \right) = \tan\left(\tfrac{\pi}{2} - \text{prec}\right) = \frac{1}{\tan(\text{prec})} \in \mathbb{Q}$$

$\tan\left(\sum_{z \in Z} \arctan\frac{1}{z}\right) = \frac{p}{q}$ dato el. di Z abbast. grandi

Step 1 Aggiungo finché posso a partire da $\frac{1}{\max X + 1}$

Step 2 Mi fermo su $\arctan\frac{1}{k}$ quando $\frac{1}{k+1} > \frac{p}{q}$ ← tan (resto)

Ora uso $\frac{1}{n}$ e vedo che serve

$$\frac{1}{n} < \frac{p}{q} \quad \text{e} \quad \tan\left(\arctan\frac{p}{q} - \arctan\frac{1}{n}\right) = \frac{\frac{p}{q} - \frac{1}{n}}{1 + \frac{p}{qn}} = \frac{np - q}{nq + p}$$

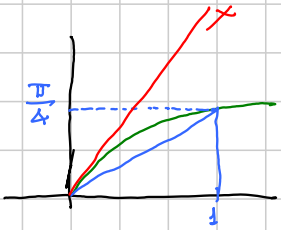
$$np - q < p \qquad n < \frac{q}{p} + 1 \qquad n = \left\lceil \frac{q}{p} \right\rceil.$$

$$\frac{1}{k+1} > \frac{p}{q} \Rightarrow n = \left\lceil \frac{q}{p} \right\rceil \text{ è nuovo}$$

Il successivo $\left\lceil \frac{nq+p}{np-q} \right\rceil > \left\lceil \frac{q}{p} \right\rceil$ e questo viene...

— o — o —

$\sum a_n$ Confronto: se $\sum b_n = +\infty$ e $a_n \geq b_n \ \forall n \geq 1$, allora $\sum a_n = +\infty$



$\arctan x \leq x \quad \forall x \geq 0$

$\arctan x \geq \frac{\pi}{4} x \quad \forall x \in [0,1]$ } seguono dalla concavità

$\arctan\frac{1}{n} \geq \frac{\pi}{4}\cdot\frac{1}{n} \quad \forall n \in \mathbb{N}$

$f'(x) = \frac{1}{1+x^2}$ è decrescente per $x \geq 0$ Alternativa studio $f(x) = x - \arctan x$ e vedo che è strett. crescente.

— o — o —

$$\underbrace{\left[\overbrace{g(f(x))}^{x}\right]'}_{1} = g'(f(x)) \cdot f'(x)$$

Conosco $f(x)$, $f'(x)$
$g(x)$ inversa

$$g'(\underbrace{f(x)}_{g(x)}) = \frac{1}{f'(x)} \Rightarrow g'(x) = \frac{1}{f'(g(x))}$$

$f(x) = \tan x \quad f'(x) = 1 + \tan^2 x \Rightarrow g'(x) = \frac{1}{1+\tan^2(g(x))} = \frac{1}{1+x^2}$

— o — o —

Confronto asintotico: se $a_n > 0$, $b_n > 0$, e $\lim_{n\to+\infty} \frac{a_n}{b_n} = \ell \neq 0 \neq +\infty$

Allora $\sum a_n$ converge $\Leftrightarrow$ $\sum b_n$ converge
diverge $\Leftrightarrow$ diverge

Dim. per n grande $\quad \frac{\ell}{2} < \frac{a_n}{b_n} < \ell+1 \quad \frac{\ell}{2} b_n < a_n < (\ell+1) b_n$

Nell'esempio $\lim_{n\to+\infty} \frac{\arctan \frac{1}{n}}{\frac{1}{n}} = \lim_{x\to 0} \frac{\arctan x}{x} = 1.$

— o — c —

INF–SUP | IMO 1982-3 $\{x_n\}$ succ. di reali t.c.
$1 = x_0 \geq x_1 \geq x_2 \geq \dots$

$\frac{x_0^2}{x_1} + \frac{x_1^2}{x_2} + \dots + \frac{x_{n-1}^2}{x_n}$ $\quad \exists n \geq 1$ t.c. espressione $\geq 3{,}999$

Se $x_n = \frac{1}{2^n}$ diventa $2 + 1 + \frac{1}{2} + \frac{1}{4} + \dots < 4 \quad \forall n \in \mathbb{N}.$

Partiamo con x_0 qualunque e poniamo

$F(x_0, n) = \inf \{$ Espressione al variare delle succ. con x_0 fissato $\}$

$F(x_0, n+1) = \inf \left\{ \frac{x_0^2}{x_1} + F(x_1, n) : x_1 \in [0, x_0] \right\}$

$F(x_0, n) = ? \; F(1, n)$

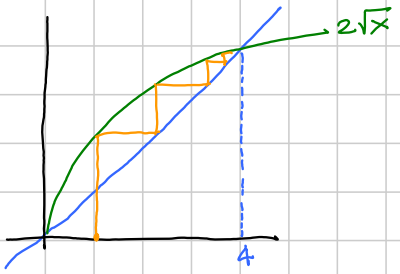
$$\frac{x_0^2}{x_1} + \frac{x_1^2}{x_2} + \frac{x_2^2}{x_3} + \dots = x_0 \left(\frac{1}{\frac{x_1}{x_0}} + \frac{\left(\frac{x_1}{x_0}\right)^2}{\frac{x_2}{x_0}} + \frac{\left(\frac{x_3}{x_0}\right)^3}{\frac{x_2}{x_0}} + \dots \right)$$

$$\geq x_0 F(1, n)$$

Quindi $F(x_0, n) \geq x_0 F(1, n)$ in realtà anche $= \dots$

$$F(1, n+1) = \inf \left\{ \frac{1}{x_1} + F(x_1, n) \right\}$$
$$\geq \inf \left\{ \frac{1}{x_1} + x_1 F(1, n) \right\}$$
$$\geq \inf \left\{ 2\sqrt{F(1,n)} \right\} = 2\sqrt{F(1,n)}$$

Quindi $F(1,n+1) \geq 2\sqrt{F(1,n)}$



Se $F_{n+1} \geq 2\sqrt{F_n} \Rightarrow F_n$ supera $4-\varepsilon$ per ogni $\varepsilon > 0$.

Dim. per induzione che $F_n \geq 4 - \frac{4}{n}$

Spero $2\sqrt{F_n} = 4\sqrt{1-\frac{1}{n}} \overset{?}{\geq} 4 - \frac{4}{n+1}$

— o — o —

IMO SL 2001 $\quad \frac{x_1}{1+x_1^2} + \frac{x_2}{1+x_1^2+x_2^2} + \dots + \frac{x_n}{1+x_1^2+x_2^2+\dots+x_n^2} < \sqrt{n}$

$x_i \geq 0$

$F(a,n) = \sup\{\text{Espr. con } a \text{ al denom. invece di } 1\}$

① Ricorrenza $\quad F(1,n+1) = \sup\left\{\frac{x}{1+x^2} + F(1+x^2,n) : x \geq 0\right\}$

② Dip. da a: $\quad F(a,n) = \frac{1}{\sqrt{a}} F(1,n)$

$$\frac{x_1}{a+x_1^2} + \frac{x_2}{a+x_1^2+x_2^2} + \dots = \frac{1}{a}\left\{\frac{x_1}{1+\frac{x_1^2}{a}} + \frac{x_2}{1+\frac{x_1^2}{a}+\frac{x_2^2}{a}} + \dots\right\}$$

$$= \frac{1}{\sqrt{a}}\left\{\frac{\frac{x_1}{\sqrt{a}}}{1+\left(\frac{x_1}{\sqrt{a}}\right)^2} + \dots\right\}$$

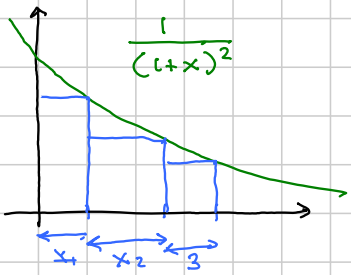
$$F(1,n+1) = \sup \frac{x}{1+x^2} + \frac{1}{\sqrt{1+x^2}} F(1,n)$$

$$< \sup\left\{\frac{x}{1+x^2} + \frac{\sqrt{n}}{\sqrt{1+x^2}}\right\} < \sqrt{n+1}$$

Svolgo tutto e viene **WC 2007**

Esercizio $\frac{1}{1+x_1} + \frac{1}{1+x_1+x_2} + \dots + \frac{1}{1+x_1+\dots+x_n} < \sqrt{\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n}}$

$$\frac{1}{\sqrt{x_1}} \frac{\sqrt{x_1}}{1+x_1} + \frac{1}{\sqrt{x_2}} \frac{\sqrt{x_2}}{1+x_1+x_2} + \dots \leq \text{C.S.} \sqrt{\frac{1}{x_1} + \dots + \frac{1}{x_n}} \sqrt{\frac{x_1}{(1+x_1)^2} + \frac{x_2}{(1+x_1+x_2)^2} + \dots}$$



$$\int_0^N \frac{1}{(1+x)^2}\,dx = \left[-\frac{1}{1+x}\right]_0^N = 1 - \frac{1}{1+N} < 1$$

$$\frac{x_1}{(1+x_1)^2} + \frac{x_2}{(1+x_1+x_2)^2} + \dots \leq 1 - \frac{1}{1+x_1+\dots+x_n}$$

$$\leq \frac{x_1}{1\cdot(1+x_1)} + \frac{x_2}{(1+x_1)(1+x_1+x_2)}$$

$$\left(1 - \frac{1}{1+x_1}\right) + \left(\frac{1}{1+x_1} - \frac{1}{1+x_1+x_2}\right)$$

IMO 1985 – 6 $\quad x_{n+1} = x_n\left(x_n + \frac{1}{n}\right)$ $\quad x_1$ dato

$\exists! x_1$ t.c. $\quad 0 < x_n < x_{n+1} < 1$ per ogni $n \in \mathbb{N}$

Come si comporta al variare di x_1.

Fatto 1 $\exists\, x_1$ per cui $x_n \to +\infty$ ($x_{n+1} \geq x_n^2$ e se parto alto...)

Fatto 2 L'insieme degli x_1 per cui $x_n \to +\infty$ è una semiretta (se x_1 va bene, tutti i successivi vanno bene). Non sappiamo se con o senza p.to iniziale.

Fatto 3 Se per un certo x_1 esiste n t.c. $x_n > 1$, allora $x_n \to +\infty$.

Borderline: supponiamo che $x_n \to \ell \in \mathbb{R}$. Allora

$$x_{n+1} = x_n\left(x_n + \frac{1}{n}\right)$$
$$\downarrow \quad \downarrow \quad \downarrow$$
$$\ell \quad \ell \cdot \ell$$

$\ell = \ell^2 \Rightarrow \ell = 0, 1.$

Fatto 4 Per $x_1 = 0$ abbiamo che $x_n \to 0$

Se x_1 è abbastanza piccolo, allora $x_n \to 0$
(per induzione si dim. che $x_n \le \left(\frac{3}{4}\right)^n$ $x_n \le \frac{1}{2^n}$)

Fatto 5 L'insieme degli x_1 per cui $x_n \to 0$ è un segmento, con 0 senza estremo destro.

Fatto 6 Se $\exists\, n$ t.c. $x_{n+1} < x_n$, allora x_n è decrescente da lì in poi e $x_n \to 0$.
(La decrescenza è una banale induzione (occhio: per la crescenza non vale)).
Teo. mist. (succ. monotone) Una successione monotona e limitata dalla parte giusta ha limite reale.
Quindi $x_n \to l$ e $l \neq 1$ perché quando ha iniziato a decrescere stava sotto 1.

Fatto 7 Partendo dalla terra di nessuno deve stare sempre ≤ 1 (vedi fatto 3) e essere crescente (vedi fatto 6), quindi in particolare $x_n \to 1$. Resta da dim. che è $\neq \emptyset$.

Fatto 8 Continuità. Fisso $n \ge 1$. Allora il valore di x_n è una funzione continua di x. È addirittura polinomiale.

Fatto 9 La zona rossa è aperta. Prendo x_1 in zona rossa. $\exists\, n$ t.c. $x_n \ge 2$, ma allora per x_1 vicini $x_n \ge \frac{3}{2}$ (stesso n), ma allora sono pure in zona rossa.

Fatto 10 La zona verde è aperta. Se ho $x_{n+1} < x_n$ per un certo n ed un certo x_1, allora ce l'ho per gli x_1 vicini.

Fatto 11 La terra di nessuno è fatta da un solo elemento.
Supponiamo che esistano 2 valori iniziali $\alpha < \beta$ per cui $x_n \not\to 1$. $x_n(\alpha)$ $x_n(\beta)$

$$x_{n+1}(\beta) - x_{n+1}(\alpha) = x_n^2(\beta) + \frac{1}{n} x_n(\beta) - x_n^2(\alpha) - \frac{1}{n} x_n(\alpha)$$

$= (x_n(\beta) - x_n(\alpha))\underbrace{(x_n(\beta) + x_n(\alpha))}_{\to 2} + \underbrace{\frac{1}{n}(x_n(\beta) - x_n(\alpha))}_{\geq 0}$

$\geq x_n(\beta) - x_n(\alpha)$ per n grande abbastanza

Dunque $x_n(\beta) - x_n(\alpha)$ non può tendere a 0.

Quindi tesi di massimo = inf rosso = sup verde.

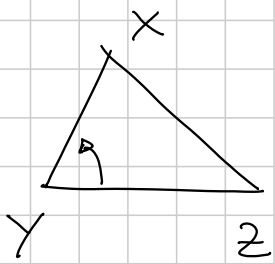
COORDINATE BARICENTRICHE E TRILINEARI

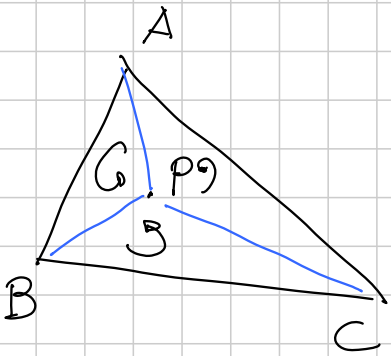
Titolo nota 05/09/2011

$[XYZ] = (\text{area di } \hat{XYZ}) \cdot \begin{cases} 1 & \text{antiorario} \\ -1 & \text{orario} \end{cases}$

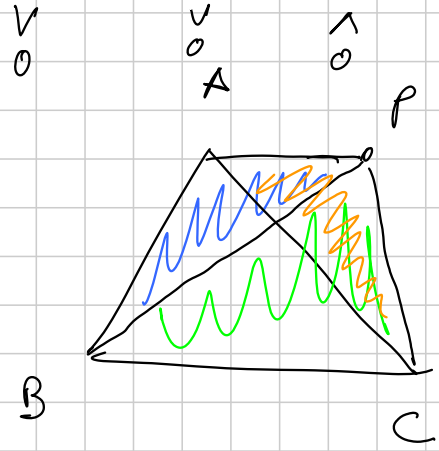
$= \frac{1}{2}(Z-Y) \times (X-Y)$ (\$ \times \$)

$= \frac{1}{2} ZY \cdot XY \cdot \operatorname{sen} Z\hat{Y}X$





$[ABP] + [BCP] + [CAP] = [ABC]$



Oss: $[ABC] = [BCA] = [CAB] = -[ACB] = -[CBA] = -[BAC]$

$[BPA] + [APC] + [CPB] = \frac{1}{2}\{(A-P)\times(B-P) + (C-P)\times(A-P) +$

$+ (B-P)\times(C-P)\} = \frac{1}{2}\{A\times B - P\times B - A\times P + C\times A - P\times A - C\times P +$

$+ B\times C - P\times C - B\times P\} = \frac{1}{2}\{A\times B + B\times C + C\times A\} =$

$= \frac{1}{2}\{(C-B)\times(A-B)\} = [ABC]$

$P \longrightarrow \left[\frac{[CPB]}{[ABC]}, \frac{[APC]}{[ABC]}, \frac{[BPA]}{[ABC]} \right]$ coord. baric. ogette di P

$[\lambda, \mu, \nu]$ $\quad \lambda + \mu + \nu = 1$

$\vec{P'} = \lambda \vec{A} + \mu \vec{B} + \nu \vec{C}$

$2[CP'B] = (B - P') \times (C - P') = [-\lambda A + (1-\mu)B - \nu C] \times [-\lambda A - \mu B + (1-\nu)C]$

$= +\lambda\mu\, A \times B - \lambda(1-\nu)\, A \times C - \lambda(1-\mu)\, B \times A + (1-\mu)(1-\nu)\, B \times C$

$+ \lambda\nu\, C \times A + \mu\nu\, C \times B = \lambda A \times B (\mu + 1 - \mu) + \lambda C \times A (\nu + 1 - \nu) +$

$+ B \times C \left(\underbrace{1 - \mu - \nu}_{\lambda} + \mu\nu - \mu\nu \right) = \lambda \cdot 2[ABC]$

$\Rightarrow P' = P.$

Coord. baricentriche di $P = (l : m : n)$ t.c. $\underset{[CPB] : [APC] : [BPA]}{l : m : n}$

$P = [p_1, p_2, p_3]$ $\quad Q = [q_1, q_2, q_3]$

pt. medio di $PQ = \dfrac{p_1 A + p_2 B + p_3 C + q_1 A + q_2 B + q_3 C}{2} =$

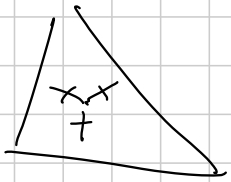
$= \frac{p_1 + q_1}{2} A + \dots \Rightarrow \left[\frac{p_1+q_1}{2}, \frac{p_2+q_2}{2}, \frac{p_3+q_3}{2} \right]$

K t.c. $\dfrac{PK}{KQ} = \dfrac{\lambda_1}{\lambda_2}$ $\quad \dfrac{\lambda_2 P + \lambda_1 Q}{\lambda_2 + \lambda_2} = K$

$\left[\frac{\lambda_2 p_1 + \lambda_1 q_1}{2}, \dots \right]$

Es: $G = (1:1:1)$

$I = (a:b:c)$



$A = (1:0:0) \quad B = (0:1:0) \quad C = (0:0:1)$

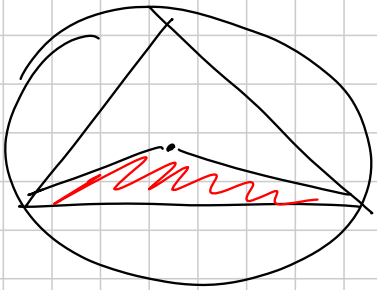
$E_{xcentri} = (-a:b:c), (a:-b:c), (a:b:-c)$

$O = (\sin 2\alpha : \sin 2\beta : \sin 2\gamma) =$

$= (\sin\alpha\cos\alpha : \_\_) =$

$= \left(a\frac{b^2+c^2-a^2}{2bc} : \_\_\right) =$

$= (a^2(b^2+c^2-a^2) : \_\_)$



$\frac{1}{2}R^2 \sin 2A$

Ex: cerchio di simil. inverso fra (O), (I)

S_i

$s = \frac{a+b+c}{2}$

$\frac{R}{r} = \frac{abc}{4S}\cdot\left(\frac{2S}{a+b+c}\right)^{-1} = \frac{(a+b+c)abc}{8S^2} = \frac{abc}{4S^2}$

$\frac{OS_i}{S_iI} = \frac{R}{r} = \frac{abc}{4S^2}$

$I = (a:b:c)\frac{1}{2S}$

$O = (a^2(b^2+c^2-a^2) : \_\_)\frac{1}{16S^2}$

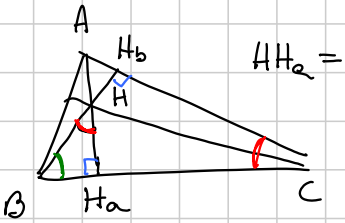
$2(a^2b^2+b^2c^2+c^2a^2) - a^4 - b^4 - c^4$

$\sqrt{s(s-a)(s-b)(s-c)}$

$S_i = [a^2(b+c-a), \_\_]$

$H \rightarrow$ area

$\rightarrow \frac{HG}{GO} = 2$



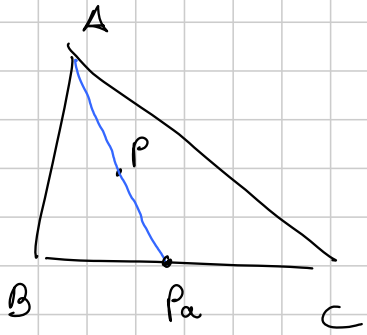
$HH_a = CH_b \cdot \frac{BH_a}{H_bB} =$

$= \frac{a\cos\gamma \cdot c\cos\beta}{a\cdot\sin\gamma}$

$(a\cos\gamma\cos\beta : \_\_) =$

$= \left(\frac{a}{\cos\alpha} : \text{——}\right) = \left(\tan\alpha : \text{——}\right) = \left(\frac{1}{b^2+c^2-a^2} : \text{——}\right)$

M = centro della cp. di F. $= [a\cos(\beta-\gamma) : \text{——}]$



$P = (p_1 : p_2 : p_3)$

$P_a = (0 : p_2 : p_3)$

P_b ——

P_c ——

$(x, y, z) \in \mathbb{R}^3 \qquad x+y+z \neq 0.$

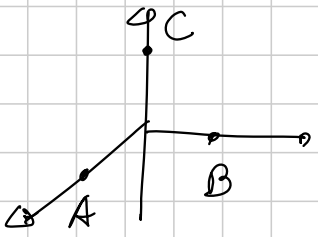
$\downarrow$

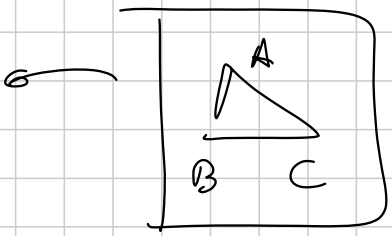
$\left(\frac{x}{x+y+z}, \frac{y}{x+y+z}, \frac{z}{x+y+z}\right) \in \{x+y+z = 1\}$

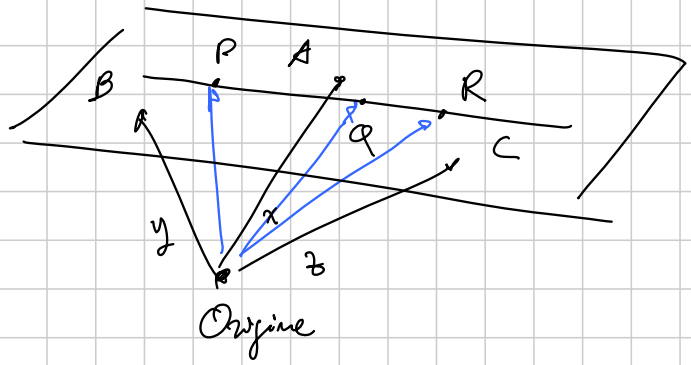
$f(P) = (\lambda, \mu, \nu)$ coord. bar. esatte

$f(\lambda P + (1-\lambda)Q) = \lambda f(P) + (1-\lambda) f(Q)$

$f(P), f(Q), f(R)$ allineati $\Longleftrightarrow$ P, Q, R allineati





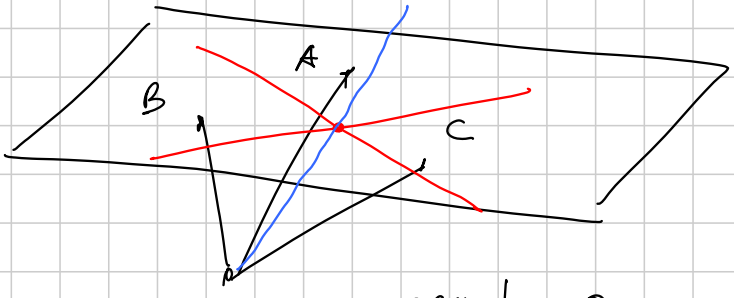


$F(e_1) = OP$
$F(e_2) = OQ$
$F(e_3) = OR$

P, Q, R all. $\Leftrightarrow$ F non sing. $\Leftrightarrow$ $\det M = 0$ $\quad M = \left(OP \mid OQ \mid OR\right)$

3 punti P, Q, R di coord bar. $(p_i), (q_i), (r_i)$

sono all. $\Leftrightarrow$ $\det \begin{pmatrix} p_1 & q_1 & r_1 \\ p_2 & q_2 & r_2 \\ p_3 & q_3 & r_3 \end{pmatrix} = 0$



$\begin{cases} cy - bz = 0 \\ x - y = 0 \end{cases}$ $\quad \begin{cases} y = \frac{b}{c} z \\ x = y \end{cases}$

$\left(\frac{b}{c} : \frac{b}{c} : 1\right)$

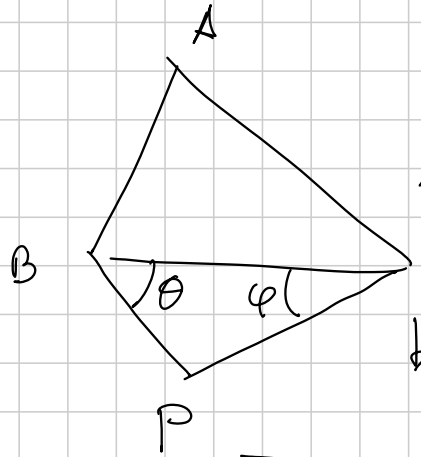
Piano: $\ell_1 x + m_1 y + n_1 z = 0$

$(\ell_1, m_1, n_1) \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$

$\ell_2 \ldots$
$\ell_3 \ldots$

$\exists \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ t.c. $\begin{pmatrix} \ell_1 & m_1 & n_1 \\ \ell_2 & m_2 & n_2 \\ \ell_3 & m_3 & n_3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

Conclusione: le rette $\ell_1 x + m_1 y + n_1 z = 0$, $\ell_2 x + m_2 y + n_2 z = 0$, $\ell_3 x + m_3 y + n_3 z = 0$ concorrono se $\det \begin{pmatrix} \ell_1 & m_1 & n_1 \\ \ell_2 & m_2 & n_2 \\ \ell_3 & m_3 & n_3 \end{pmatrix} = 0$.



$2[PCB] = -T$

$\frac{T}{\sin\theta} = BP \cdot BC$ $\quad BP = \frac{T}{a\sin\theta}$

$\frac{T}{\sin\varphi} = CP \cdot BC$ $\quad CP = \frac{T}{a\sin\varphi}$

$$2[PAB] = c \cdot \frac{T}{a\sin\theta} \cdot \sin(\beta+\theta) = \frac{cT}{a}\left(\frac{\sin\beta\cos\theta}{\sin\theta} + \frac{\cos\beta\sin\theta}{\sin\theta}\right) =$$

$$= \frac{cT}{a}\sin\beta\left(\cot\theta + \cot\beta\right)$$

$$2[PCA] = \frac{bT}{a}\sin\gamma(\cot\varphi + \cot\gamma)$$

Formula di CONWAY

$$P = \left(-a^2 : 2[ABC](\cot\theta + \cot\beta) : 2[ABC](\cot\varphi + \cot\gamma)\right)$$

$S_\theta = 2[ABC]\cdot\cot\theta$ Notazione di CONWAY

$S_{\theta\varphi} = S_\theta \cdot S_\varphi$

$$P = (-a^2 : S_\theta + S_B : S_\varphi + S_C)$$

i) $S_B + S_C = a^2$

$S_A = bc\cdot\sin\alpha\cdot\frac{\cos\alpha}{\sin\alpha} = \frac{b^2+c^2-a^2}{2bc}\cdot bc =$

ii) $S_{AB} + S_{BC} + S_{CA} = S^2 = 4[ABC]^2$ $\quad = \frac{b^2+c^2-a^2}{2}$

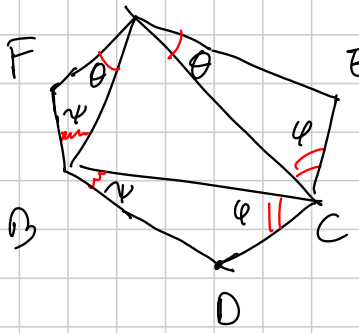
$\cot\alpha\cot\beta + \cot\beta\cot\gamma + \cot\gamma\cot\alpha = 1$

$H = \left(\frac{1}{S_A} : \frac{1}{S_B} : \frac{1}{S_C}\right)$

$O = \left(a^2 S_A : b^2 S_B : c^2 S_C\right) = \left(S_A(S_B+S_C) : \_\_\_\_\right)$

$N = \left(S^2 + S_{BC} : \_\_\_\_\right)$

Teo di Nagel



$\Rightarrow AD, BE, CF$ concorrono

$D = (-a^2 ; S_B + S_\psi : S_C + S_\varphi)$

$AD \cap BC = (0 : S_B + S_\psi : S_C + S_\varphi)$

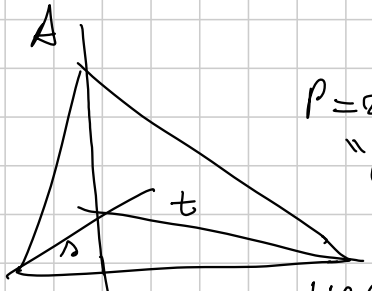
$BE \cap AC = (S_A + S_\theta : 0 : S_C + S_\varphi)$

$CF \cap AB = (S_A + S_\theta : S_B + S_\psi : 0)$

———— ∘ ————

Passaggio alle Trilineari: $Tri(P) = \left(d(P,BC) : d(P,AC) : d(P,AB)\right)$

$bari(P) = (\lambda, \mu, \nu) \longmapsto \left(\frac{\lambda}{a}, \frac{\mu}{b}, \frac{\nu}{c}\right) = Tri(P)$



$P = r \cap s \cap t$ $\quad\rightsquigarrow [p:q:i]$

$P' = r' \cap s' \cap t'$ $\quad\rightsquigarrow \left(\frac{1}{p} : \frac{1}{q} : \frac{1}{r}\right)$

$r = \left\{P : \frac{d(P,AB)}{d(P,AC)} = k\right\}$ $\qquad r' = \left\{\ldots = \frac{1}{k}\right\}$

in Baricentriche: $(\lambda:\mu:\nu) \to \left(\frac{\lambda}{a} : \frac{\mu}{b} ; \frac{\nu}{c}\right) \to \left(\frac{a}{\lambda} : \frac{b}{\mu} ; \frac{c}{\nu}\right)$

$\left(\frac{a^2}{\lambda} : \frac{b^2}{\mu} : \frac{c^2}{\nu}\right)$ ⟵

Es: $H = \left(\frac{1}{S_A}, --\right) \qquad O = (a^2 S_A, --)$

$K = (a^2 : b^2 : c^2)$ punto di Lemoine

Fatto: Coniug. isog. della cf. circoscritta non esiste

$P = (\lambda : \mu : \nu)$ t.c. $\frac{a^2}{\lambda} + \frac{b^2}{\mu} + \frac{c^2}{\nu} = 0$

$a^2 \mu\nu + b^2 \lambda\nu + c^2 \lambda\mu = 0$

$\left\{ a^2 yz + b^2 xz + c^2 xy = 0 \right\} = \Gamma$

cf. di F = immagine di Γ tramite l'omot. di centro G e fattore $-\frac{1}{2}$.

$P \in$ cf di F $\quad P = [\lambda ; \mu ; \nu] \quad \lambda + \mu + \nu = 1$

$\downarrow$ omot.

$$-2(P - G) + G = -2\left[\left(\lambda - \tfrac{1}{3}\right) + \mu - \tfrac{1}{3}, \nu - \tfrac{1}{3}\right] + \left[\tfrac{1}{3}, \tfrac{1}{3}, \tfrac{1}{3}\right] =$$

$$= \left[-2\lambda + 1, -2\mu + 1, -2\nu + 1\right]$$

$$a^2 (-2\mu + 1)(-2\nu + 1) + b^2 (-2\lambda + 1)(-2\nu + 1) + c^2 (-2\lambda + 1)(-2\mu + 1) = 0$$

$$4\mu\nu a^2 + 4\lambda\nu b^2 + 4\lambda\mu c^2 - 2a^2\mu - 2a^2\nu - 2b^2\lambda - 2b^2\nu - 2c^2(\lambda + \mu)$$

$$+ a^2 + b^2 + c^2 = 0$$

$$4\left(a^2 yz + b^2 xz + c^2 xy\right) + (x + y + z)\left[(a^2 b^2 + a^2 c^2)(x + y + z) - 2a^2(y + z) - 2b^2(x + z) - 2c^2(x + y) \right]$$

$$K\left(a^2 yz + \cdots\right) + (x + y + z)\left[\quad \right]$$

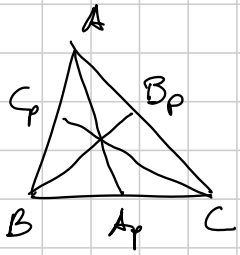
COORDINATE BARICENTRICHE - 2

Titolo nota 07/09/2011

$S_\theta = 2[ABC]\cot\theta$ $\quad S_{\theta\varphi} = S_\theta \cdot S_\varphi$

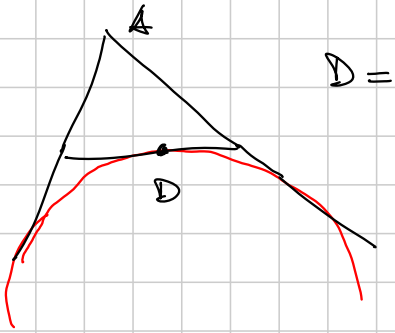
G, O, H, I, N

Oss: $P=(u:v:w) \iff$



$A_P=(0:v:w)$
$B_P=(u:0:w)$
$C_P=(u:v:0)$

Es: Punto di NAGEL (forse) $\quad s=\frac{a+b+c}{2}$



$D=(0:s-b:s-c)$

$N_a=(s-a:s-b:s-c)$

$G_e=\left(\frac{1}{s-a}:\frac{1}{s-b}:\frac{1}{s-c}\right)$

- $P=(u:v:w)$ $\quad P'=\left(\frac{a^2}{u}:\frac{b^2}{v}:\frac{c^2}{w}\right)$ coniug. isogonale

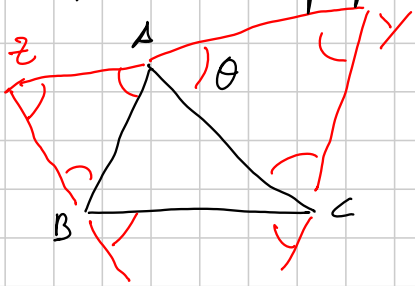
$P^*=\left(\frac{1}{u}:\frac{1}{v}:\frac{1}{w}\right)$ coniug. isotomico

Oss(+): $X=(*:q:r)$ $\quad Y=(p:*:r)$ $\quad Z=(p:q:*)$

AX, BY, CZ concorrono in $(p:q:r)=P$

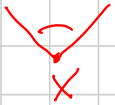
$\triangle ABC$, $\triangle XYZ$ sono prospettici in P

Es:



$\theta=\frac{\pi}{3}$ $\quad \cot\theta=\frac{1}{\sqrt{3}}$

$X=\left(-a^2:\frac{S}{\sqrt{3}}+S_C:\frac{S}{\sqrt{3}}+S_B\right)$



$$Y = \left(S_C + \frac{S}{\sqrt{3}} : -b^2 : S_A + \frac{S}{\sqrt{3}}\right)$$

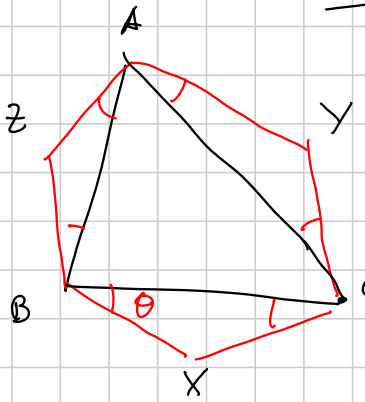
$$Z = \left(S_B + \frac{S}{\sqrt{3}} : S_A + \frac{S}{\sqrt{3}} : -c^2\right)$$

$$X = \left(\frac{-a^2}{\left(S_C + \frac{S}{\sqrt{3}}\right)\left(S_B + \frac{S}{\sqrt{3}}\right)} : \frac{1}{S_B + \frac{S}{\sqrt{3}}} : \frac{1}{S_C + \frac{S}{\sqrt{3}}}\right)$$ idem per gli altri due

$$AX \cap BY \cap CZ = \left(\frac{1}{S_A + \frac{S}{\sqrt{3}}} : \frac{1}{S_B + \frac{S}{\sqrt{3}}} : \frac{1}{S_C + \frac{S}{\sqrt{3}}}\right)$$

$$= \left(\frac{1}{\sqrt{3}S_A + S} : \text{—}\right)$$

— $\circ$ —



$$X = \left(-a^2 : S_C + S_\theta : S_B + S_\theta\right)$$

$$X = \left(\ast : \frac{1}{S_B + S_\theta} : \frac{1}{S_C + S_\theta}\right)$$

$\Downarrow$

AX, BY, CZ concorrono in

punto di KIEPERT di angolo θ (di XYZ) $\rightarrow$

$$K(\theta) = \left(\frac{1}{S_A + S_\theta} : \frac{1}{S_B + S_\theta} : \frac{1}{S_C + S_\theta}\right)$$

— $\circ$ —

$$P_t = (u + t : v + t : w + t) \qquad t \in \mathbb{R}$$

$$x - y + \frac{v - u}{v - w}(y - z) = 0$$

$$P_t' = \left(\frac{a^2}{u + t} : \frac{b^2}{v + t} : \frac{c^2}{w + t}\right) \Downarrow$$

$$\frac{a^2}{x} - \frac{b^2}{y} + \frac{v - u}{v - w}\left(\frac{b^2}{y} - \frac{c^2}{z}\right) = 0$$

$$\begin{cases} a^2yz - b^2xz + \frac{v-u}{v-w}\left(b^2xz - c^2xy\right) = 0 \\ x+y+z=0 \end{cases}$$

$$\begin{cases} x-y+\frac{v-u}{v-w}(y-z)=0 \\ a^2yz + b^2xz + c^2xy = 0 \end{cases}$$

$$a^2(v+t)(w+t) + b^2(u+t)(w+t) + c^2(u+t)(v+t) =$$

$$= t^2(a^2+b^2+c^2) + t\left(u(b^2+c^2) + v(a^2+c^2) + w(a^2+b^2)\right) +$$

$$+ a^2vw + b^2uw + c^2uv$$

$$\left[\begin{array}{l} u^2b^4 + u^2c^2 + 2u^2b^2c^2 \\ + v^2a^4 + v^2c^4 + 2v^2a^2c^2 \\ + w^2a^4 + w^2b^4 + 2w^2a^2b^2 + \\ 2uvw^2 + 2uvc^2b^2 \\ + 2uva^2c^2 + 2uvc^4 + \\ + 2uwa^2b^2 + 2uwb^4 + \\ + 2uwc^2a^2 + 2uwc^2b^2 + \\ + 2vwa^4 + 2vwa^2b^2 \\ + 2vwc^2a^2 + 2vwc^2b^2 \end{array}\right] - 4\left(a^4vw + a^2b^2uw + a^2c^2uv + a^2b^2vw + b^4uw + b^2c^2uv + c^2a^2vw + c^2b^2uw + c^4uv\right)$$

Eq: Retta di Eulero

$(1:1:1) \quad (S_{BC}:S_{CA}:S_{AB})$

$$0 = \det\begin{pmatrix} x & y & z \\ 1 & 1 & 1 \\ S_{BC} & S_{CA} & S_{AB} \end{pmatrix} = x(S_{AB}-S_{CA}) - y(S_{AB}-S_{BC}) + z(S_{CA}-S_{BC}) =$$

$$= x(S_{AB}-S_{CA}) + y(S_{BC}-S_{AB}) + z(S_{CA}-S_{BC}) =$$

$$= \sum_{cyc} S_A(S_B-S_C)x$$

Retta IO: $(a:b:c) \quad (a^2S_A : b^2S_B : c^2S_C)$

$$0 = \sum_{cyc}\left(b^2S_Bc - c^2S_Cb\right)x = \sum_{cyc} bc(bS_B - cS_C)x = 0$$

$$bS_B - cS_C = b\,ac\sin\beta\,\frac{\cos\beta}{\sin\beta} - c\,\frac{a^2+b^2-c^2}{2} =$$

$$\left(\cos\beta = \frac{a^2+c^2-b^2}{2ac}\right)$$

$$= \frac{ba^2+bc^2-b^3-ca^2-cb^2+c^3}{2} = (b-c)\,\frac{a^2-bc-c^2-bc-b^2}{2} =$$

$$= (b-c)\,\frac{a^2-(b+c)^2}{2} = -2(b-c)\,S(S-a)$$

$$\sum_{cyc} bc(b-c)(S-a)x = 0 \qquad \sum_{cyc} \frac{(b-c)(S-a)}{a}x = 0$$

$$F_{\pm} = \left(\frac{1}{\sqrt{3}S_A \pm S} : \frac{1}{\sqrt{3}S_B \pm S} : \frac{1}{\sqrt{3}S_C \pm S}\right)$$

$$\begin{cases} \sum_{cyc} (S_B - S_C)(3S_{AA} - S^2)x = 0 \\ \sum_{cyc} S_A(S_B - S_C)x = 0 \end{cases}$$

$$\begin{cases} p_1x + q_1y + r_1z = 0 \\ p_2x + q_2y + r_2z = 0 \end{cases} \qquad (q_1r_2 - q_2r_1 : r_1p_2 - p_1r_2 : p_1q_2 - q_1p_2)$$

$$S_B(S_C-S_A)(S_A-S_B)(3S_{CC}-S^2) - S_C(S_A-S_B)(S_C-S_A)(3S_{BB}-S^2) =$$

$$= (S_C-S_A)(S_A-S_B)\left[S_B(3S_{CC}-S^2) - S_C(3S_{BB}-S^2)\right] =$$

$$= (S_C-S_A)(S_A-S_B)\left[3S_{BCC} - S_BS^2 - 3S_{BBC} + S_CS^2\right] =$$

$$= (S_C-S_A)(S_A-S_B)\left[3S_{BC}(S_C-S_B) + S^2(S_C-S_B)\right] =$$

$$= (\ )(\ )(\ )\left[3S_{BC}+S^2\right]$$

$$\left(3S_{BC}+S^2 : \_\_\_\_\right)$$

$H = \left(\frac{S_{BC}}{S^2} : \frac{S_{CA}}{S^2} : \frac{S_{AB}}{S^2}\right)$ $\quad S_{BC}+S_{CA}+S_{AB}=S^2$

$G = \left(\frac{1}{3} : \frac{1}{3} : \frac{1}{3}\right)$ $\quad \frac{S_{BC}}{S^2} + \frac{1}{3} = \frac{3S_{BC}+S^2}{3S^2}$

$\frac{1}{\sqrt{3}S_A \pm S}$ $\quad S^2 \pm \sqrt{3}S(S_B+S_C) + 3S_{BC}$ $\quad (S_B+S_C = a^2)$

$6S^2 \pm \sqrt{3}S(a^2+b^2+c^2)$

$$\frac{S^2+\sqrt{3}Sa^2+3S_{BC}}{6S^2+\sqrt{3}S(a^2+b^2+c^2)} + \frac{S^2-\sqrt{3}Sa^2+3S_{BC}}{6S^2-\sqrt{3}S(a^2+b^2+c^2)} =$$

$$= 6S^4 + \cancel{6\sqrt{3}S^3a^2} + 18S^2S_{BC} - \cancel{\sqrt{3}S^3(a^2+b^2+c^2)} - \cancel{3S^2a^2(a^2+b^2+c^2)} -$$

$$- \cancel{3\sqrt{3}SS_{BC}(a^2+b^2+c^2)} + 6S^4 - \cancel{6\sqrt{3}S^3a^2} + 18S^2S_{BC} + \cancel{\sqrt{3}S^3(a^2+b^2+c^2)}$$

$$- 3S^2a^2(a^2+b^2+c^2) + \cancel{3\sqrt{3}SS_{BC}(a^2+b^2+c^2)} =$$

$$= 12S^4 + 36S^2S_{BC} - 6S^2a^2(a^2+b^2+c^2) =$$

$$= 2S^2 + 6S_{BC} - a^2(a^2+b^2+c^2) \simeq (b^2-c^2)^2$$

$$\left((b^2-c^2)^2 : (a^2-c^2)^2 : (a^2-b^2)^2\right)$$

<u>Es</u>: $K(\pm\theta)$ le rette Tra loro è $\sum_{cyc}(S_B-S_C)(S_{AA}-S_{\cot^2\theta})_{x=0}$

Al variare di θ queste rette passano per un punto fisso che è il punto di Lemoine.

— o —

$x+y+z=0$ $\quad \mathbb{P}^2(\mathbb{R}) = \{[x:y:z] \mid x,y,z \in \mathbb{R} \text{ non tutti nulli}\}$

$v, w \in \mathbb{R}^3 - \{0\}$ $\quad v \vee w$ se $\exists \lambda \in \mathbb{R}$ t.c. $\lambda v = w$

$$\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^3 \setminus \{0\} / \sim$$

$\mathbb{P}^2(\mathbb{R}) \setminus$ retta $\cong \mathbb{R}^2$

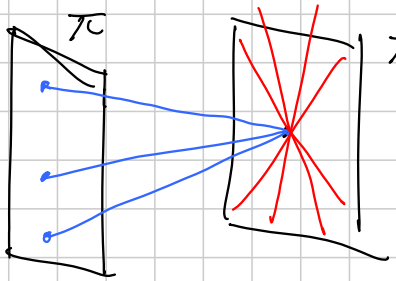
retta $= \{ p(x,y,z) = 0 \}$? p omogeneo di 1° grado.

$$(\mathbb{R}^3 \setminus \{0\}) \setminus \{ p(x,y,z) = 0 \}$$

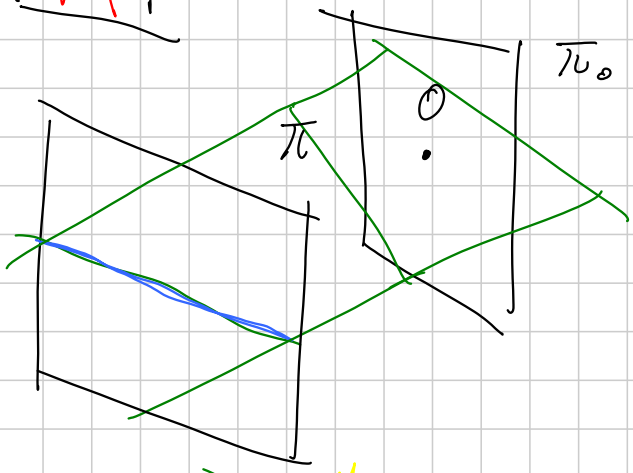
$$\pi_0 = \{ \alpha x + \beta y + \gamma z = 0 \}$$

$$\pi = \{ \alpha x + \beta y + \gamma z = 1 \}$$

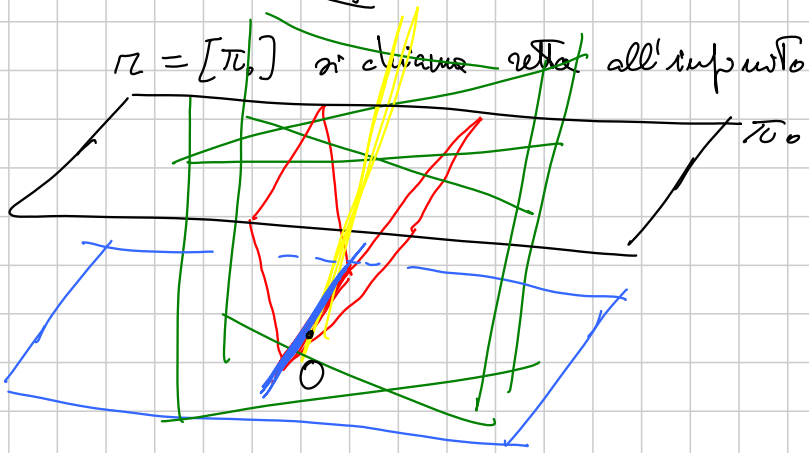
$\pi \subseteq \mathbb{R}^3 \setminus \pi_0$ $\quad \forall [x:y:z] \in \mathbb{P}^2(\mathbb{R})$ $\exists$ al più un punto $P \in \pi$ t.c. $[P] = [x:y:z]$



$\Rightarrow \forall [x:y:z] \in \mathbb{RP}^2 \setminus r \quad \exists!\ P \in \pi$ t.c. $[P] = [x:y:z]$

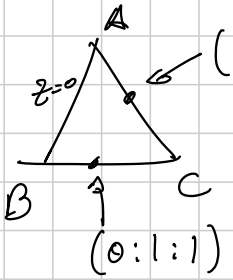


$r = [\pi_0]$ si chiama retta all'infinito di π.



in baricentriche

$z=0$



$x+y-z=0$

$\begin{cases} z=0 \\ x+y-z=0 \end{cases}$ $\begin{cases} z=0 \\ x+y=0 \end{cases}$ $(1;-1:0)$

$\begin{cases} px+qy+rz=0 \\ x+y+z=0 \end{cases}$ $(q-r;\ r-p;\ p-q) \in \mathcal{L}^\infty$

$[u,v,w]$ $\det \begin{vmatrix} x & y & z \\ u & v & w \\ q-r & r-p & p-q \end{vmatrix} =$

$= x\big(v(p-q)-w(r-p)\big)+y\big(w(q-r)-u(p-q)\big)+$

$+z\big(u(r-p)-v(q-r)\big)=0.$

Oss: $A_H=\left(0:\frac{1}{S_B}:\frac{1}{S_C}\right)=(0:S_C:S_B)$

$A=(1:0:0)=(S_B+S_C:0:0)=(a^2:0:0)$

$A_H-A=(-a^2:S_C:S_B)$

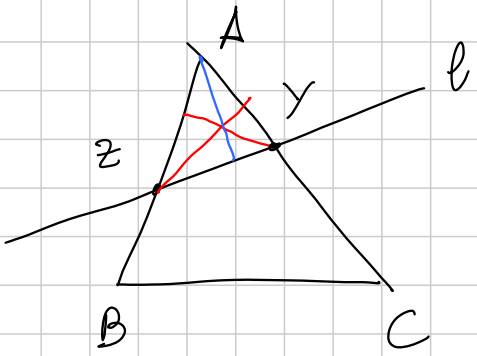
$\begin{vmatrix} x & y & z \\ -a^2 & S_C & S_B \\ u & v & w \end{vmatrix}=0$

$\|$

$-(S_B v-S_C w)x+(S_B u+a^2 w)y-(S_C u+a^2 v)z=0$

Se interseco con BC $\{x=0\}$ $A_{(P)}=(0:S_C u+a^2 v:S_B u+a^2 w)$

$\Rightarrow$ Tri pedale di $P=\begin{pmatrix} 0 & S_C u+a^2 v & S_B u+a^2 w \\ S_C v+b^2 u & 0 & S_A v+b^2 w \\ S_B w+c^2 u & S_C w+c^2 v & 0 \end{pmatrix}=A$



Fatto: se ℓ ha pt. all'∞ $(f:g:h)$ allora le pp hanno pt. all'∞

$$(f':g':h') = (S_B g - S_C h : S_C h - S_A f : S_A f - S_B g)$$

$$(f:g:h) \perp (f':g':h') \iff S_A ff' + S_B gg' + S_C hh' = 0$$

Es: Il Tri circumcevviano è simile al Tri pedale

$P = (u:v:w)$ $\quad AP = \{vz - wy = 0\}$

$$\begin{cases} vz - wy = 0 \\ a^2 yz + b^2 xz + c^2 xy = 0 \end{cases}$$

Risolviamo il problema ausiliario omogeneo

$$\begin{cases} vc^2 y - wb^2 z = 0 \\ x + y + z = 0 \end{cases}$$

$$x + z\left(1 + \frac{wb^2}{vc^2}\right) = 0 \qquad y = \frac{wb^2}{vc^2} z$$

$$x + z\left(\frac{vc^2 + wb^2}{vc^2}\right) = 0 \qquad x = -(vc^2 + wb^2) \quad y = wb^2 \quad z = vc^2$$

$$\left(-(vc^2 + wb^2) : wb^2 : vc^2\right)$$

$$\left(\frac{-a^2 vw}{c^2 v + b^2 w} : v : w\right)$$ A-vertice del Tri circumcevviano

Tornando al Tri pedale $\quad \det A = (u+v+w)(S^2)(a^2 vw + b^2 wu + \dots)$

se P è circoscritta $\Rightarrow P = \left(\frac{a^2}{f} : \frac{b^2}{g} : \frac{c^2}{h}\right)$ $\quad (f:g:h) \in \mathcal{L}^\infty$

se $(f':g':h') \perp (f:g:h) \Rightarrow x\frac{f}{f'} + y\frac{g}{g'} + z\frac{h}{h'} = 0$ è la retta di Simson

$(f' : g' : h') =$ retta di Simson di $P \cap \mathcal{Z}^\infty$

$$f' = S_B g - S_C h$$

$$\frac{a^2}{f'} = a^2 (S_C h - S_A f)(S_A f - S_B g) =$$

$$= a^2 (S_{CA} hf - S_{CB} hg - S_A^2 f^2 + S_{AB} fg)$$

$$(a^2 g h : b^2 h f : c^2 fg)$$

— • —

$$\mathcal{C} = \{ a^2 yz + b^2 xz + c^2 xy - (x+y+z)(px+qy+rz) = 0 \}$$

asse radicale
Tre cp e qz uguali.

$$\begin{cases} \mathcal{C} \\ x = 0 \end{cases} \Rightarrow a^2 yz - (y+z)(qy+rz) = 0$$

$$(0 : 1-c : 1-b)$$

$$qy^2 + zy(q+r-a^2) + rz^2 = k((1-c)z - (1-b)y)^2$$

$$k = 1$$

$$q = (1-b)^2 \qquad p = (1-a)^2$$

$$r = (1-c)^2$$

Inc. $a^2 yz + b^2 xz + c^2 xy - (x+y+z)((1-a)^2 x + (1-b)^2 y + (1-c)^2 z) = 0$

A-ex $\qquad 1^2 \qquad (1-b)^2 \qquad (1-c)^2$

cp. di F: $a^2 yz + b^2 xz + c^2 xy - \frac{1}{2}(x+y+z)(S_A x + S_B y + S_C z) = 0$

$$\sum_{cyc}' \left((1-a)^2 - \frac{1}{2} S_A \right) x = 0$$

$$\left(\frac{b+c-a}{2}\right)^2 - \frac{1}{2}\left(\frac{b^2+c^2-a^2}{2}\right) =$$

$$= \frac{1}{4}\left[b^2 + c^2 + a^2 + 2bc - 2ac - 2ab - b^2 - c^2 + a^2\right] =$$

$= \frac{1}{2}(a^2 - a(b+c) + bc) = \frac{1}{2}(a-b)(a-c)$

$\sum (a-b)(a-c)x = 0 \qquad \sum \frac{x}{b-c} = 0$ Tg a ch. inscr. e Feuer.

tg. Γ nel ch. A-esc. e F. $\frac{x}{b-c} + \frac{y}{a+c} - \frac{z}{a+b} = 0$

— ∘ —

retta Eulero → Jerabek (iperbole)

OK ⟶ iperbole di Kiepert $\sum (b^2-c^2) yz = 0$

$\{ \alpha yz + \beta xz + \gamma xy = 0 \}$ passano per i vertici

Coniche inscritte: 1. devono passare o per 3 punti: all'incentro o nei piedi di 3 cevie concorrenti

$P = (p : q : 2)$

$\frac{x^2}{p^2} + \frac{y^2}{q^2} + \frac{z^2}{2^2} - \frac{2yz}{q2} - \frac{2zx}{2p} - \frac{2xy}{pq} = 0$

"TON" ADVANCED

Titolo nota 06/09/2011

ESERCIZIO: (IMO 6 / 2007)

SIA $S = \{(x,y,z) \in \mathbb{Z}^3 : 0 \le x \le \ell, 0 \le y \le m, 0 \le z \le n, (x,y,z) \neq (0,0,0)\}$

QUANTI PIANI SERVONO CHE NON PASSINO PER ORIGINE TALI CHE $S \subseteq$ UNIONE PIANI?

$\ell+m+n$ BASTANO $x=1,\dots,x=\ell$ $y=1,\dots,y=m$ $z=1,\dots,z=n$

K PIANI CHE VANNO BENE $(K < \ell+m+n)$

$S \subseteq$ UN, PIANI

$P_i = \{(x,y,z) : a_i x + b_i y + c_i z + d_i = 0\}$

$UP_i = \{\prod_{i=1}^{K} (a_i x + b_i y + c_i z + d_i) = 0\}$

MA PIÙ IN GEN, POL $f(x,y,z)$ CHE GRADO DEVE AVERE?

$g(x,y,z) = f(x+1,y,z) - f(x,y,z)$

$\deg g = \deg f - 1$

$g(0,0,0) = f(1,0,0) - f(0,0,0) = -f(0,0,0) \neq 0$

$0 \le x \le \ell-1$, $0 \le y \le m$, $0 \le z \le n$ $(x,y,z) \neq (0,0,0)$

$g(x,y,z) = f(x+1,y,z) - f(x,y,z) \neq 0$

PER INDUZ. SI CONCLUDE.

COMBINATORIAL NULLSTELLENSATZ

$f(x)$ POL. DI GRADO d HA AL PIÙ d RADICI.

$f(x_1,\dots,x_n)$ $\deg f$ IN $x_i = d_i$ $f \neq 0$

se posso scegliere x_i in d_i+1 modi
riesco a non farlo annullare.

$S_1,\dots,S_n$ $|S_i| = d_i+1$ $\exists\, x \in S_1 \times \dots \times S_n$:
$f(x) \neq 0$?

C. NSS :

$f(x_1,\dots,x_n)$ POLINOMIO DI GR. d.

$\sum c_{d_1,\dots,d_n} \cdot x_1^{d_1} \cdot \dots \cdot x_n^{d_n}$

SE ESISTE UN MONOMIO $x_1^{d_1} \cdot \dots \cdot x_n^{d_n}$ CON
$d_1 + d_2 + \dots + d_n = d$ DI COEFF. NON NULLO

ALLORA "SE POSSO SCEGLIERE x_i IN d_i+1 MODI
RIESCO A NON FARLO ANNULLARE"

E) $x^2y + y^3$ FUNZIONA MEGLIO IL TH NUOVO.

DEF $f(x_1,\dots,x_n)$ $P_1(x_1) = \prod_{s \in S_1} (x_1 - s)$ $P_2(x_2) = \dots$

P_1 SI ANN. SU $S_1 \times \dots \times S_n$

P_1 HA GRADO $d_1 + 1$

CAUCHY – DAVENPORT!

$A, B \subseteq \mathbb{Z}_p$ $\quad A+B := \{a+b \mid a \in A, b \in B\}$

$\boxed{A+B = \mathbb{Z}_p}$ OPPURE $|A+B| \geq |A| + |B| - 1$

$\prod_{c \in A+B} (x+y-c) =: f(x,y)$

$|A+B| \leq |A| + |B| - 2$

$x^{d_1} y^{d_2}$ $\quad d_1 \leq |A|-1$ $\quad d_2 \leq |B|-1$

$d_1 + d_2 = |A+B|$

$\boxed{\binom{|A+B|}{d_1}}$

ES $\quad A+A = \{a+b \mid a, b \in A, a \neq b\}$

$A \subseteq \mathbb{Z}_p$ $\quad$ Th $\quad A+A = \mathbb{Z}_p$ OPPURE $|A+A| \geq 2|A| - 3$

CHEVALLEY WARING

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_K(x_1, \dots, x_n) = 0 \end{cases} \qquad x_i \in \mathbb{Z}_p$$

SE $n > \deg(f_1) + \dots + \deg(f_K) \Rightarrow$

$\#$ SOL. AL SIST. IN $(\mathbb{Z}_p)^n$ È DIVISIBILE PER p.

OSS $1 - x^{p-1}$ È 0 SE E SOLO SE x NON LO È.

DEF $F(X) := \prod_{i=1}^{K} \left(1 - f_i(X_1, \dots, X_n)^{p-1}\right)$

$\#\,\text{SOL} \equiv \sum_{X \in \mathbb{Z}_p^n} F(X) \equiv 0$

$\sum_{\lambda=1}^{p} \lambda^K \equiv 0 \pmod p$ SE $p-1 \nmid K$

EF AGGIUSTA I DETTAGLI

COR SE CI È UNA SOL. CHE N'È UN'ALTRA.

NSS $\Rightarrow$ COR.

$X_1 = a_1, \dots, X_n = a_n$ SIA SOL.

$\left| \prod_{i=1}^{K} \left(1 - f_i(X_1, \dots, X_n)^{p-1}\right) - \prod_{i=1}^{n} \left(1 - (X_i - a_i)^{p-1}\right) \right|$

$\downarrow$

$n \geq \deg(f_1) + \dots + \deg(f_K)$

HA GRADO $n-(p-1)$

SE NON SI ANNULLA C'HO UN'ALTRA SOLUZIONE

$X_1^{p-1} \cdot \dots \cdot X_n^{p-1}$ HA COEFF. $\neq 0$ E È DI GR. MAX

PONENDO $S_i = \mathbb{Z}_p$ $\forall i$ E NSS. TROVO PT CON VAL $\neq 0 \Rightarrow$ NUOVA SOL.

$$X_1^{\alpha} + \dots + X_{\alpha}^{\alpha} \equiv K \pmod p$$

$x_1^d + \dots + x_d^d \equiv K x_{d+1}^d \pmod p$

$\left(\frac{x_1}{x_{d+1}}\right)^d + \dots + \left(\frac{x_d}{x_{d+1}}\right)^d \equiv K$

CON CHEVALLEY-WARING FACCIO $K \equiv -1$ (È VALIDO).

$\left|\left\{x_1^d \mid x_1 \in \mathbb{Z}_p\right\}\right| = \frac{p-1}{MCD(p-1,d)} + 1 \geq \frac{p-1}{d} + 1$

CAUCHY DAVENPORT A RAFFICA!

$|A_1 + \dots + A_d| \geq |A_1| + \dots + |A_d| - d + 1$

$\sum_{i=1}^{k} a_i x_i^{d_i} = m$ SI SCEGLIE $p \equiv 1 \bmod d_i$

ES SE $a_i \not\equiv 0 \bmod p \ \forall i$ E $\sum \frac{1}{d_i} \geq 1$

C'È SOL MOD p

$x^2 - 3y^2 = -1$

ES $A + A = \{a + b \mid a, b \in A, a \neq b\}$

$A \subseteq \mathbb{Z}_p$ TH $A + A = \mathbb{Z}_p$ OPPURE $|A + A| \geq 2|A| - 3$

ES IL PRIMO PROBL. ITA UNA SOL. CON NSS.

SAPRESTE TROVARLA?

LEMMA DEL PERMANENTE

A MATRICE $n \times n$ A COEFF. IN F

b VETT. lungo n

FISSATI $S_1, \dots, S_n$ con $|S_i| \geq 2$

$\exists x \in F^n$: Ax E b hanno n le coord. sim. ($Ax - b$ ha n coord. $\neq 0$).

A PATTO PERM $(A) \neq 0$.

$$\sum_{\sigma} a_{i,\sigma} x_{\sigma} - b_i \neq 0 \quad \forall i$$

$$\prod_{i} \left(\sum_{\sigma} a_{i,\sigma} x_{\sigma} - b_i \right) \quad \text{HA GR. } n.$$

$$\sum_{\sigma} \prod_{i=1}^{n} a_{i,\sigma(i)} \quad \text{DETTO PERM.}$$

APPL:

WL DI UN PO' DI METRO PA. CE FORSE MAI QUANTI EL DI $(\mathbb{Z}_p)^n$ POSSO PRENDERE A CASO CHE NESSUNA SOMMA PARZIALE FACCIA 0? (non per forza distinti)

$n(p-1)$ LI TROVI.

$p-1$ VOLTE $\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$ $p-1$ VOLTE $\begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}$

$n(p-1)+1$ NON SI PUÒ!

ES CON CAUCHY-DAVENPORT

MA SI PUÒ FARE DI PIÙ

PRENDIAMO $n(p-1)$ VETTORI $v_1, \dots, v_{n(p-1)}$

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_{n(p-1)} \\ v_1 & & & \\ \vdots & & & \\ v_1 & v_2 & \cdots & v_{n(p-1)} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_{n(p-1)} \end{pmatrix}$$

$\neq$ MODO, PER MODO. $\begin{pmatrix} v+1 \\ v+2 \\ \vdots \\ v+p-1 \end{pmatrix}$

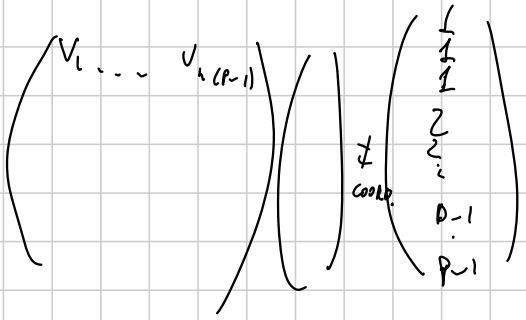
$$\begin{pmatrix} v \\ \vdots \\ v \end{pmatrix} \qquad \begin{pmatrix} v+1 \\ v+2 \\ \vdots \\ v+p-1 \end{pmatrix}$$

$$\begin{pmatrix} v+1 \\ \vdots \\ v+1 \end{pmatrix}$$

E SE PERM $(\Pi) = 0$?

$$\prod_i \left(\sum_j a_{ij} x_j - b_i \right) - \lambda \prod_j (1 - x_j)$$

$$\sum_\sigma \prod_i a_{i\sigma(i)} = 0$$



$V_{1,1}, \dots, V_{n(p-1)}$

C.N. $\Rightarrow$) se nessuna somma fin. è zero, le somme sono suriettive (1)

NSS $\Rightarrow$) se $\det(\Pi) \neq 0$ le somme sono surj

NSS $\Rightarrow$) se $\det(\Pi) = 0$ ALLORA c'è somma fin $= 0$.

GRAFI (Γ, Σ, ι)

G grafo finito V vertici E lati

$(p-1)|V| \leq |E|$

OGNI VERTICE HA AL PIÙ $2p-1$ VICINI (GRADO $\leq 2p-1$)

TH. ESISTE SOTTOGRAFO p-REGOLARE.

x_e $e \in E$ le variabili

$$\prod_{v \in V} \left[1 - \left(\sum_{e \text{ "PASSA PER } v\text{"}} x_e \right)^{p-1} \right] - \prod_{e \in E} (1 - x_e)$$

$$v \in V \left\{ \sum_{e \text{ "PASSA PER } v\text{"}} x_e^{p-1} = 0 \right.$$

TROVO S. GRAFO p-REG.

TH ERDÖSS-GINZBURG-ZIV

PRESI $2p-1$ INTERI (NON PER FORZA DISTINTI)

NE POSSO SCEGLIERE p LA CUI SOMMA

È MULTIPLA DI p. (E.W) (E.D.) $\Sigma x_{i_1} + \dots + x_{i_p}$

AND NOW FOR SOMETHING

COMPLETELY DIFFERENT!

$\Phi_n(X) = \prod_{\omega \text{ rad. prim. } n\text{-esima di unità}} (X-\omega)$ Φ_n È MONICO CON COEFF. INTERI

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

$X^n - 1 \qquad nX^{n-1} \qquad p|n \cdot nX^{n-1} \equiv 0$

$-(X^n-1) + \frac{X}{n} \cdot nX^{n-1} = 1 \qquad p \nmid n$ NON HA FATTORI DOPPI

RIDURSI MOD DA INF. SU COSA DEVE ESSERE FATTA UNA FATT. IN $\mathbb{Z}$.

CRIT. DI EISENSTEIN

$X^n + a_{n-1}X^{n-1} + \dots + a_0 = f(X)$ $p|a_i \ \forall i$ IL POL. $p^2 \nmid a_0 \Rightarrow$ È IRR.

$f(X) = g^{\alpha}(X) \cdot h^{\beta}(X)$

$f(X) = g(X) \cdot h(X)$ $\quad$ (mod p)

$g(X) = X^{\alpha} + p(\dots)$ $\qquad h(X) = X^{\beta} + p(\dots)$

$\Phi_p(X) = \dfrac{X^p - 1}{X - 1} = X^{p-1} + \dots + 1$

$X = Y + 1$ $\qquad \dfrac{(Y+1)^p - 1}{Y} = Y^{p-1} + \sum_{i=1}^{p-1} Y^{i-1} \binom{p}{i}$

$\Phi_p(X)$ È IRRIDUCIBILE.

$\Phi_n(X) = f(X) g(X)$ $\qquad p \nmid n$

ω RAD. DI f

$\boxed{\Phi_n(X) = f(X) g(X)}$ VALE IN $\mathbb{F}_p$

$\omega = f(\alpha)^p = f(\alpha^p)$ $\qquad (\alpha+\beta)^p = \alpha^p + \beta^p$

α RAD. DI $f(X) \Rightarrow \alpha^p$ RAD. DI $f(X)$ IN $\mathbb{C}$. $\forall p \nmid n$

α $\qquad \alpha^K = \alpha^{p_1 \cdot p_2 \cdots p_2}$

α rad. $f \Rightarrow \alpha^{p_1}$ rad. $f \Rightarrow (\alpha^{p_1})^{p_2}$ rad $f \dots \Rightarrow \alpha^K$ rad f.

$\Rightarrow \Phi_n(X)$ IRR.

$\boxed{(X-\omega)\cdot(X-\omega^p)\cdot\dots\cdot(X-\omega^{p^K})}$ $\qquad K = \operatorname{ord}_n(p) - 1$

come si comp. modulo p.

a INTERO $\Phi_n(a)$ $p \mid \Phi_n(a)$

$p \nmid n$ $x^n - 1$ NON HA RADICI DOPPIE

a è UNA RADICE DI $x^n - 1$.

$\mathrm{ord}_p(a) \mid n$ $a^d = 1$ $d < n$

$\Rightarrow$ $x - a \mid x^d - 1$ $x - a \mid \Phi_n(x)$

$(x^d - 1)$ $\Phi_n(x) \mid x^n - 1 \Rightarrow \mathrm{ord}_p(a) = n$

$\mathrm{ord}_p(a) = n \Rightarrow \Phi_n(a) \equiv 0 \pmod p$

$p \mid n$ $n = p \cdot d$ $a^d \equiv 1 \pmod p$

$\Phi_n(x) \mid \dfrac{x^{dp} - 1}{x^d - 1}$ $p \mid \dfrac{a^{dp} - 1}{a^d - 1}$

$n = p^k \cdot s$ $(n, s) = 1$

$\mathrm{ord}_p(a) < s$ $s = \mathrm{ord}_p(a) \cdot r$ $r \geq 1$

$\Phi_n(x) \mid \dfrac{x^{p^k \cdot \mathrm{ord}_p(a) \cdot r} - 1}{x^{p^k \cdot \mathrm{ord}_p(a)} - 1}$

$n = p^k \cdot \mathrm{ord}_p(a)$ $p \parallel \Phi_n(a)$.

a n INT. POS. p T.C. a HA ORD $n \bmod p$,

$\Phi_n(a) = \pm p$ $p \leq n$

$\Phi_n(a) \mid \leq n$

$a \geq 3$

$\left| \prod_{\substack{\omega \text{ rad.} \\ \text{prim}}} (a-\omega) \right| = \prod |a-\omega| \geq 2^{\phi(n)} \geq n$

ASSURDO.

COR $\exists$ inf. primi $\equiv 1 \pmod n$

SUPP. CHE CI SIANO FIN. $P = \prod_{p \equiv 1 (n)} p$

$\exists\, p$ PRIMO, T.C. $\text{Ord}_p(P) = n \Rightarrow p \equiv 1 (n)$

$\Rightarrow p \mid P$

$X^{p-1} - 1$ HA TT. LE RAD MOD p (SI CP. IN FATT. LIN.)

$\Phi_{p-1}(X)$ HA TT. RAD MOD p $\quad \Phi_{p-1}(X) \mid X^{p-1} - 1$

α rad. di $\Phi_{p-1}(X)$ IN $\mathbb{F}_p$

$p \nmid p-1 \;\; \text{ord}_p(\alpha) = p-1 \qquad X^{p-1} - 1 = \prod_{d \mid p-1} \Phi_d(X)$

ES p PRIMO $\exists q$ T.C. p NON È UN RESIDUO p-ESIMO IN $\mathbb{Z}_q$

$p \equiv n^p \pmod q$ NON HA SOL

ITO 6 ANNI IGNOTO

Campi finiti

Titolo nota 08/09/2011

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

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

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

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

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

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

$a+b\sqrt{d}$

$\mathbb{F}_{16}$ $\quad x^4+x+1$ 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. $\overbrace{1+1+1+\dots+1}^{k \text{ volte}}=0$

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 $\operatorname{char} K>0$.

$0\ 1\ \alpha\ \alpha+1$

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

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

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

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

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

$=0$

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

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

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

$V_1=\mathbb{F}_p$

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

$n_1b_2+a_1=n_2b_2+a_2$ $\qquad b_2=\frac{a_2-a_1}{n_1-n_2}\in\mathbb{F}_p$ 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. $\operatorname{ord}(g)=p$.

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

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

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

$|K| = p^k$

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

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

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

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

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

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

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

$\mathbb{F}_p$ $p(x)$ irriducibile 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 $\mathrm{ord}(\alpha) = p^k - 1$

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

$$X_a \equiv X_{a \cdot p^k} \pmod{p}$$

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

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

$$X_{n \cdot p} = \left(C_1 \alpha_1^{np} + C_2 \alpha_2^{np} + \dots \right) = \left(d_1 \alpha_1^n + d_2 \alpha_2^n + \dots \right)^p \qquad d_i^p = C_i$$

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

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

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

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

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 $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^h} \iff k \mid h$ $\qquad \left(p^k\right)^m$ 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 : $a_0 = \cosh(b_0)$

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

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

$A = 2 + \sqrt{3}$

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

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

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

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

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

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

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

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

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

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

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

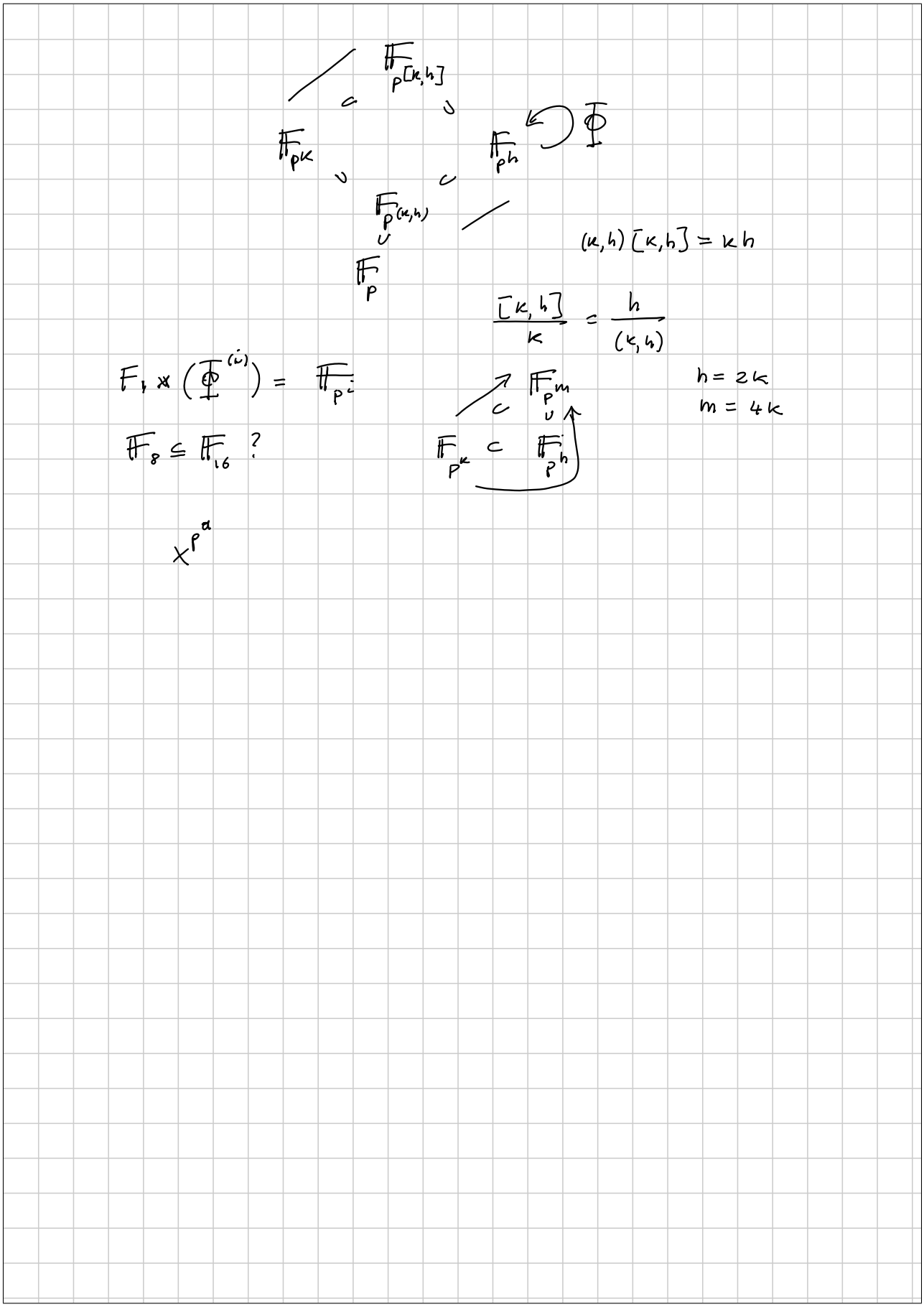
q_i irr, monici
$\deg q_i \mid k$

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


$\mathbb{F}_{p^{[k,h]}}$
$\mathbb{F}_{p^k}$
$\mathbb{F}_{p^h}$
$\mathbb{F}_{p^{(k,h)}}$
$\mathbb{F}_p$
$(k,h)[k,h] = kh$
$\frac{[k,h]}{k} = \frac{h}{(k,h)}$
$F_4 \hookrightarrow \left(\overline{\mathbb{F}}_p^{(i)}\right) = \mathbb{F}_{p^i}$
$\mathbb{F}_8 \subseteq \mathbb{F}_{16}$?
$\mathbb{F}_{p^m}$
$\mathbb{F}_{p^k} \subset \mathbb{F}_{p^h}$
$h = 2k$
$m = 4k$
X^{p^a}