Funzioni simmetriche e polinomi di Newton

Maurizio Monge

Università di Pisa

Tesi di Laurea in Matematica

26 Settembre 2008

Campi simmetrici (1/2)

- Sia k un campo (di caratteristica zero o p), e $x_1, \ldots, x_n$ algebricamente indipendenti su k.

Campi simmetrici (1/2)

- Sia k un campo (di caratteristica zero o p), e $x_1, \ldots, x_n$ algebricamente indipendenti su k.
- Sia
$$F = F^k = k(x_1, \ldots, x_n)$$
il campo delle *funzioni razionali* in $x_1, \ldots, x_n$ sul campo k,

Campi simmetrici (1/2)

- Sia k un campo (di caratteristica zero o p), e $x_1, \ldots, x_n$ algebricamente indipendenti su k.
- Sia
$$F = F^k = k(x_1, \ldots, x_n) = \operatorname{Frac} k[x_1, \ldots, x_n]$$
il campo delle *funzioni razionali* in $x_1, \ldots, x_n$ sul campo k, costituito dalle *frazioni di polinomi*.

Campi simmetrici (1/2)

- Sia k un campo (di caratteristica zero o p), e $x_1, \ldots, x_n$ algebricamente indipendenti su k.
- Sia
$$F = F^k = k(x_1, \ldots, x_n) = \operatorname{Frac} k[x_1, \ldots, x_n]$$
il campo delle *funzioni razionali* in $x_1, \ldots, x_n$ sul campo k, costituito dalle *frazioni di polinomi*.
- Sia
$$S = S^k = F^{S_n}$$
il sottocampo delle *funzioni simmetriche*, invarianti per permutazione di $x_1, \ldots, x_n$.

Campi simmetrici (2/2)

- F è estensione finita di Galois su S, e

$$\mathrm{Gal}(F/S) \;=\; S_n.$$

Campi simmetrici (2/2)

- F è estensione finita di Galois su S, e

$$\mathrm{Gal}(F/S) \;=\; S_n.$$

- S è generato dalle *funzioni simmetriche elementari*

$$e_r = \sum_{1 \le i_1 < i_2 < \cdots < i_r \le n} x_{i_1} x_{i_2} \ldots x_{i_n}, \qquad \text{per } r = 1, \ldots, n.$$

Campi simmetrici (2/2)

- F è estensione finita di Galois su S, e

$$\mathrm{Gal}(F/S) \;=\; S_n.$$

- S è generato dalle *funzioni simmetriche elementari*

$$e_r = \sum_{1 \le i_1 < i_2 < \cdots < i_r \le n} x_{i_1} x_{i_2} \ldots x_{i_n}, \qquad \text{per } r = 1, \ldots, n.$$

- F è il campo di spezzamento del polinomio

$$X^n - e_1 X^{n-1} + e_2 X^{n-2} - \cdots + (-1)^n e_n \;\in\; S[X].$$

Polinomi di Newton

- Definiamo i polinomi di Newton come

$$N_r = x_1^r + x_2^r + \cdots + x_n^r, \qquad \text{per } r \geq 1.$$

Polinomi di Newton

- Definiamo i polinomi di Newton come

$$N_r = x_1^r + x_2^r + \cdots + x_n^r, \qquad \text{per } r \geq 1.$$

- Possiamo considerare il campo generato da m tali polinomi

$$\mathcal{N}_a = \mathcal{N}_{a_1,\ldots,a_m} = \mathcal{N}_a^k = k(N_{a_1}, \ldots, N_{a_m}),$$

per $a_1 > a_2 > \cdots > a_m$.

Polinomi di Newton

- Definiamo i polinomi di Newton come

$$N_r = x_1^r + x_2^r + \cdots + x_n^r, \qquad \text{per } r \geq 1.$$

- Possiamo considerare il campo generato da m tali polinomi

$$\mathcal{N}_a = \mathcal{N}_{a_1,\ldots,a_m} = \mathcal{N}_a^k = k(N_{a_1}, \ldots, N_{a_m}),$$

per $a_1 > a_2 > \cdots > a_m$.

- **Problema:** sotto quali ipotesi su $a = (a_1, \ldots, a_m)$ abbiamo

$$S = \mathcal{N}_a,$$

cioè $N_{a_1}, \ldots, N_{a_m}$ generano tutto S?

Polinomi di Newton (preliminari, 1/2)

- È necessario che $m \geq n$ altrimenti $\mathcal{N}_a$ ha grado di trascendenza $< n$, e quindi non può essere S.

Polinomi di Newton (preliminari, 1/2)

- È necessario che $m \geq n$ altrimenti $\mathcal{N}_a$ ha grado di trascendenza $< n$, e quindi non può essere S.
- È necessario che

$$\gcd(a_1, a_2, \ldots, a_m) = 1,$$

Polinomi di Newton (preliminari, 1/2)

- È necessario che $m \geq n$ altrimenti $\mathcal{N}_a$ ha grado di trascendenza $< n$, e quindi non può essere S.
- È necessario che

$$\gcd(a_1, a_2, \ldots, a_m) = 1,$$

altrimenti se $g = \gcd(a_1, a_2, \ldots, a_m)$ allora

$$\mathcal{N}_a \subseteq S^{(g)},$$

il campo simmetrico in $x_1^g, \ldots, x_n^g$,

Polinomi di Newton (preliminari, 1/2)

- È necessario che $m \geq n$ altrimenti $\mathcal{N}_a$ ha grado di trascendenza $< n$, e quindi non può essere S.
- È necessario che

$$\gcd(a_1, a_2, \ldots, a_m) = 1,$$

altrimenti se $g = \gcd(a_1, a_2, \ldots, a_m)$ allora

$$\mathcal{N}_a \subseteq S^{(g)},$$

il campo simmetrico in $x_1^g, \ldots, x_n^g$, e

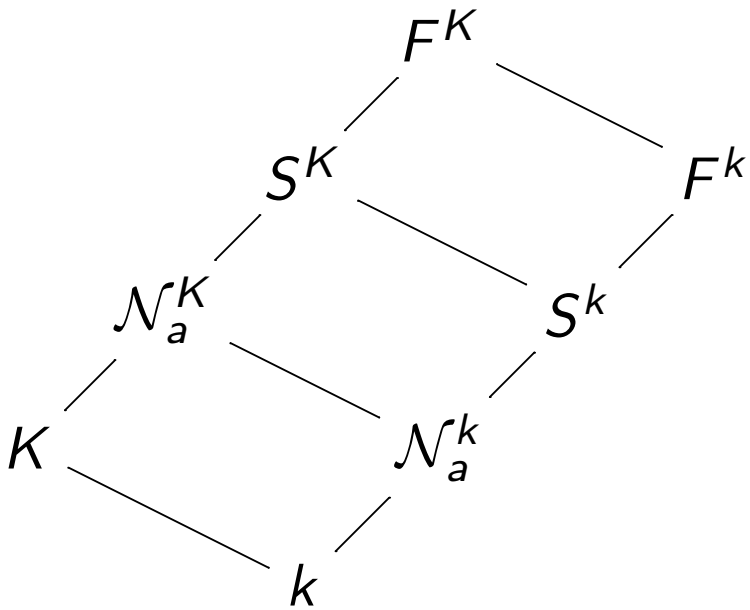
$$[S : \mathcal{N}_a] = g^n \cdot [S : \mathcal{N}_{a/g}].$$

Polinomi di Newton (preliminari, 2/2)

- Il problema dipende solo dalla caratteristica del campo base:

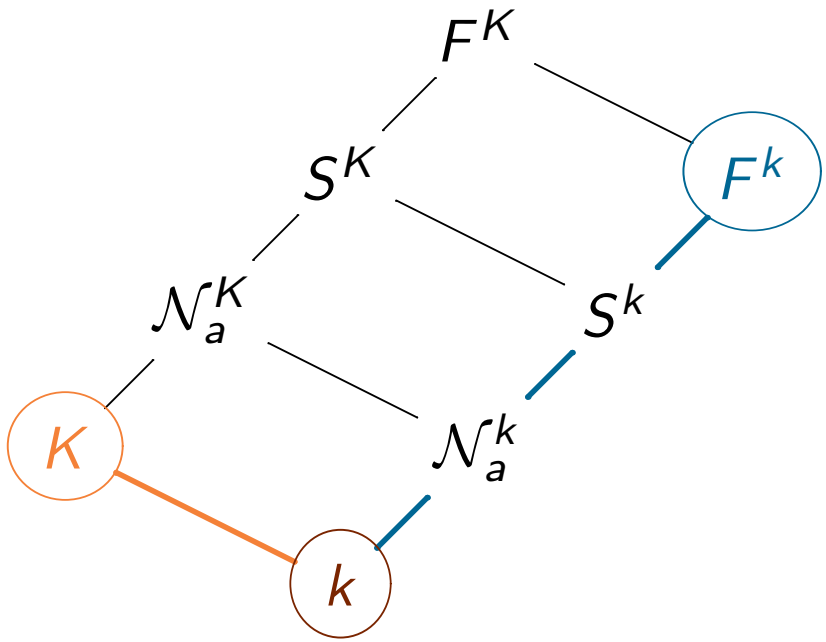
Polinomi di Newton (preliminari, 2/2)

- Il problema dipende solo dalla caratteristica del campo base: se K/k e $x_1, \ldots, x_n$ sono algebricamente indipendenti su K



Polinomi di Newton (preliminari, 2/2)

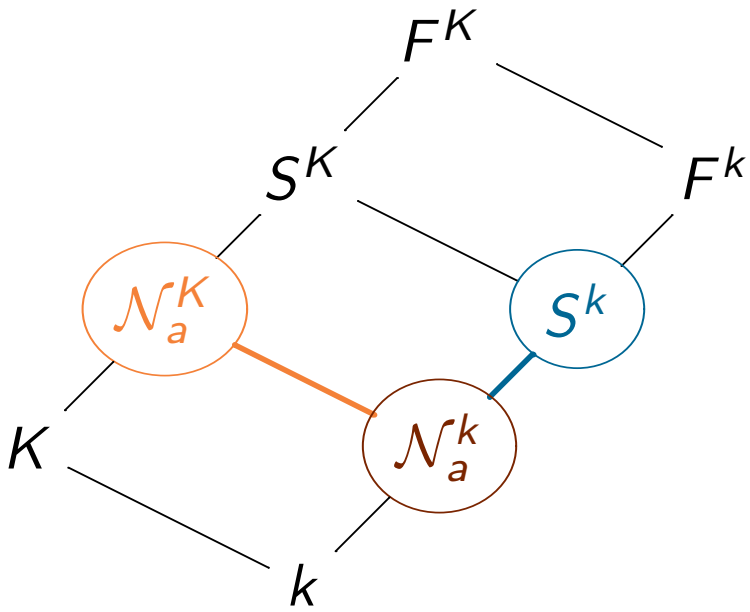
- Il problema dipende solo dalla caratteristica del campo base: se K/k e $x_1, \ldots, x_n$ sono algebricamente indipendenti su K



- K e F^k sono linearmente disgunti su k,

Polinomi di Newton (preliminari, 2/2)

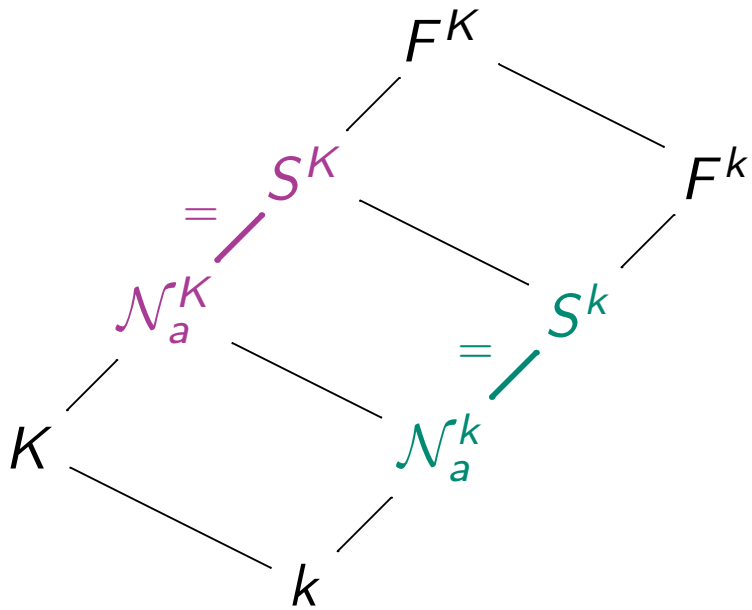
- Il problema dipende solo dalla caratteristica del campo base: se K/k e $x_1, \ldots, x_n$ sono algebricamente indipendenti su K



- K e F^k sono linearmente disgunti su k,
- e quindi anche $\mathcal{N}_a^K$ e S^k sono linearmente disgunti su $\mathcal{N}_a^k$,

Polinomi di Newton (preliminari, 2/2)

- Il problema dipende solo dalla caratteristica del campo base: se K/k e $x_1, \ldots, x_n$ sono algebricamente indipendenti su K



- K e F^k sono linearmente disgunti su k,
- e quindi anche $\mathcal{N}_a^K$ e S^k sono linearmente disgunti su $\mathcal{N}_a^k$,
- i gradi coincidono.

Derivazioni

- Una derivazione sul campo k è una funzione che soddisfa

$$D(x+y) = Dx + Dy, \qquad D(xy) = xDy + yDx.$$

Derivazioni

- Una derivazione sul campo k è una funzione che soddisfa

$$D(x+y) = Dx + Dy, \qquad D(xy) = xDy + yDx.$$

- Un'estensione a K/k esiste ed è unica se e solo se K/k è algebrica separabile.

Derivazioni

- Una derivazione sul campo k è una funzione che soddisfa

$$D(x+y) = Dx + Dy, \qquad D(xy) = xDy + yDx.$$

- Un'estensione a K/k esiste ed è unica se e solo se K/k è algebrica separabile.

Teorema (Criterio dello jacobiano)

Sia $L = k(\alpha_1, \ldots, \alpha_n)$, *e* $f_1, \ldots, f_n \in k[X_1, \ldots, X_n]$ *relazioni fra gli* α_i. *Se*

$$\det(\partial f_i/\partial X_j)_{1\leq i,j\leq n}\Big|_{(\alpha_1,\ldots,\alpha_n)} \neq 0$$

allora L/k *è algebrica e separabile.*

Derivazioni

- Una derivazione sul campo k è una funzione che soddisfa

$$D(x+y) = Dx + Dy, \qquad D(xy) = xDy + yDx.$$

- Un'estensione a K/k esiste ed è unica se e solo se K/k è algebrica separabile.

Teorema (Criterio dello jacobiano)

Sia $L = k(\alpha_1, \ldots, \alpha_n)$, e $f_1, \ldots, f_n \in k[X_1, \ldots, X_n]$ relazioni fra gli α_i. Se

$$\det(\partial f_i/\partial X_j)_{1\leq i,j\leq n}\Big|_{(\alpha_1,\ldots,\alpha_n)} \neq 0$$

allora L/k è algebrica e separabile.

- In n variabili dati $a = (a_1, \ldots, a_n)$ distinti e primi con p, $S/\mathcal{N}_a$ è *algebrica finita separabile*, e $N_{a_1}, \ldots, N_{a_n}$ algebricamente indipendenti.

Polinomi di Newton in due variabili

- In due variabili e con due polinomi, conosciamo il grado

$$[S : \mathcal{N}_{a,b}] = \begin{cases} \frac{ab}{2} & \text{se } ab \text{ è pari,} \\ \frac{(a-1)b}{2} & \text{se } ab \text{ è dispari.} \end{cases}$$

per $a > b \geq 1$ coprimi, e primi con la caratteristica p (dimostrato da Mead e Stein, 1998).

Polinomi di Newton in due variabili

- In due variabili e con due polinomi, conosciamo il grado

$$[S : \mathcal{N}_{a,b}] = \begin{cases} \frac{ab}{2} & \text{se } ab \text{ è pari,} \\ \frac{(a-1)b}{2} & \text{se } ab \text{ è dispari.} \end{cases}$$

  per $a > b \geq 1$ coprimi, e primi con la caratteristica p (dimostrato da Mead e Stein, 1998).
- Due polinomi di Newton generano S solo nei casi

$$\mathcal{N}_{1,2} \qquad \mathcal{N}_{1,3} \qquad (p \neq 2, 3).$$

Polinomi di Newton in due variabili

- In due variabili e con due polinomi, conosciamo il grado

$$[S : \mathcal{N}_{a,b}] = \begin{cases} \frac{ab}{2} & \text{se } ab \text{ è pari,} \\ \frac{(a-1)b}{2} & \text{se } ab \text{ è dispari.} \end{cases}$$

  per $a > b \geq 1$ coprimi, e primi con la caratteristica p (dimostrato da Mead e Stein, 1998).
- Due polinomi di Newton generano S solo nei casi

$$\mathcal{N}_{1,2} \qquad \mathcal{N}_{1,3} \qquad (p \neq 2, 3).$$

- Mead e Stein congetturarono anche che su $\mathbb{Q}$ valesse

$$S = \mathcal{N}_{a,b,c},$$

  per tutti gli $a > b > c \geq 1$ coprimi.

Polinomi di Newton, risultati in due variabili

Teorema (Dvornicich-Zannier, 2003)

Siano $a > b > c \geq 1$ *coprimi. Allora*

$$N_a = x^a + y^a, \qquad N_b = x^b + y^b, \qquad N_c = x^c + y^c$$

generano l'intero campo simmetrico S *in* x, y *su* $\mathbb{Q}$.

Polinomi di Newton, risultati in due variabili

Teorema (Dvornicich-Zannier, 2003)

Siano $a > b > c \geq 1$ *coprimi. Allora*

$$N_a = x^a + y^a, \qquad N_b = x^b + y^b, \qquad N_c = x^c + y^c$$

generano l'intero campo simmetrico S *in* x, y *su* $\mathbb{Q}$.

- È ancora vero in caratteristica positiva p?

Polinomi di Newton, risultati in due variabili

Teorema (Dvornicich-Zannier, 2003)

Siano $a > b > c \geq 1$ *coprimi. Allora*

$$N_a = x^a + y^a, \qquad N_b = x^b + y^b, \qquad N_c = x^c + y^c$$

generano l'intero campo simmetrico S *in* x, y *su* $\mathbb{Q}$.

- È ancora vero in caratteristica positiva p?
- La risposta è **no**, almeno con le stesse ipotesi.

Polinomi di Newton, risultati in due variabili

Teorema (Dvornicich-Zannier, 2003)

Siano $a > b > c \geq 1$ *coprimi. Allora*

$$N_a = x^a + y^a, \qquad N_b = x^b + y^b, \qquad N_c = x^c + y^c$$

generano l'intero campo simmetrico S *in* x, y *su* $\mathbb{Q}$.

- È ancora vero in caratteristica positiva p?
- La risposta è **no**, almeno con le stesse ipotesi.
- Ma se richiediamo addizionalmente che

$$a, b, c, a - b, a - c, b - c$$

siano primi con p, allora la riposta è **sì**!

Polinomi di Newton, risultati in due variabili

Teorema (Dvornicich-Zannier, 2003)

Siano $a > b > c \geq 1$ *coprimi. Allora*

$$N_a = x^a + y^a, \qquad N_b = x^b + y^b, \qquad N_c = x^c + y^c$$

generano l'intero campo simmetrico S *in* x, y *su* $\mathbb{Q}$.

- È ancora vero in caratteristica positiva p?
- La risposta è **no**, almeno con le stesse ipotesi.
- Ma se richiediamo addizionalmente che

$$a, b, c, a-b, a-c, b-c$$

  siano primi con p, allora la riposta è **sì**!
- Procediamo supponendo p la caratteristica, la strada che seguiamo può essere adattata anche al caso di caratteristica zero.

Non possono esserci due fra a, b, c divisibili per p

- Se due fra a, b, c sono divisibili per p, allora

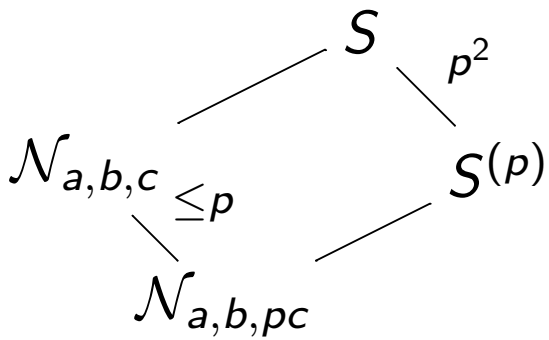
$$S \supsetneq \mathcal{N}_{a,b,c}.$$

Non possono esserci due fra a, b, c divisibili per p

- Se due fra a, b, c sono divisibili per p, allora

$$S \supsetneq \mathcal{N}_{a,b,c}.$$

- Infatti poniamo $p|a$ e $p|b$. Allora $\mathcal{N}_{a,b,pc} \subseteq S^{(p)}$, e

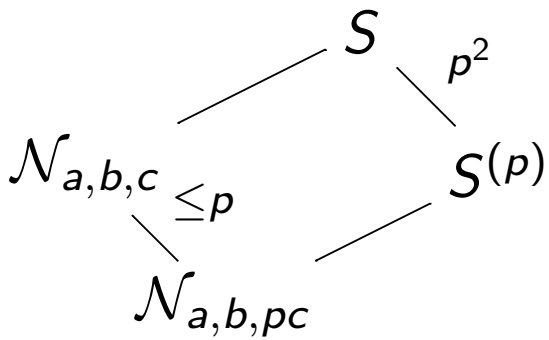


Non possono esserci due fra a, b, c divisibili per p

- Se due fra a, b, c sono divisibili per p, allora

$$S \supsetneq \mathcal{N}_{a,b,c}.$$

- Infatti poniamo $p|a$ e $p|b$. Allora $\mathcal{N}_{a,b,pc} \subseteq S^{(p)}$, e



dato che N_c soddisfa

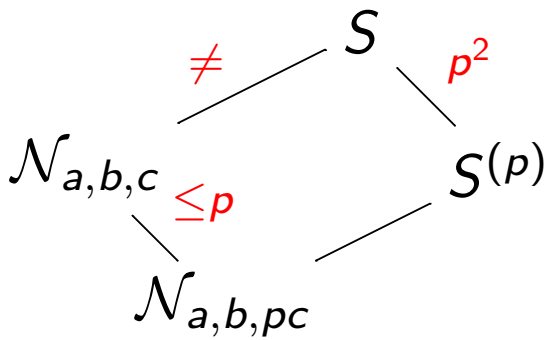
$$N_c^p - N_{pc} = 0.$$

Non possono esserci due fra a, b, c divisibili per p

- Se due fra a, b, c sono divisibili per p, allora

$$S \supsetneq \mathcal{N}_{a,b,c}.$$

- Infatti poniamo $p|a$ e $p|b$. Allora $\mathcal{N}_{a,b,pc} \subseteq S^{(p)}$, e



dato che N_c soddisfa

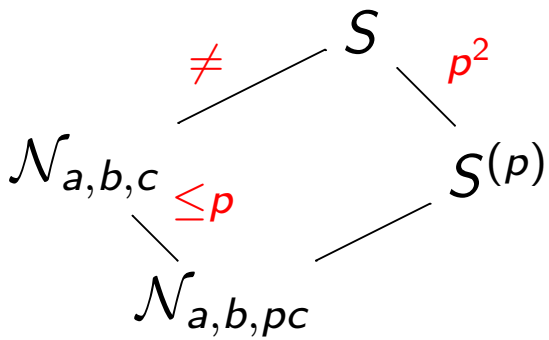
$$N_c^p - N_{pc} = 0.$$

Non possono esserci due fra a, b, c divisibili per p

- Se due fra a, b, c sono divisibili per p, allora

$$S \supsetneq \mathcal{N}_{a,b,c}.$$

- Infatti poniamo $p|a$ e $p|b$. Allora $\mathcal{N}_{a,b,pc} \subseteq S^{(p)}$, e



dato che N_c soddisfa

$$N_c^p - N_{pc} = 0.$$

- Infatti in caratteristica p vale l'uguaglianza delle elementari

$$(u+v)^p = u^p + v^p, \qquad \forall u, v.$$

Uno fra a, b, c divisibile per p non dà fastidio (1/2)

Proposizione

Se a, b, c sono primi con p e $S = \mathcal{N}_{a,b,c}$ allora

$$S = \mathcal{N}_{a,b,p^r c} \qquad \text{per ogni } r \geq 1.$$

Uno fra a, b, c divisibile per p non dà fastidio (1/2)

Proposizione

Se a, b, c sono primi con p e $S = \mathcal{N}_{a,b,c}$ allora

$$S = \mathcal{N}_{a,b,p^r c} \qquad \text{per ogni } r \geq 1.$$

- Infatti $S = \mathcal{N}_{a,b,c} = \mathcal{N}_{a,b,p^r c}(N_c)$, e

$$N_c^{p^r} - N_{p^r c} = 0,$$

Uno fra a, b, c divisibile per p non dà fastidio (1/2)

Proposizione

Se a, b, c sono primi con p e $S = \mathcal{N}_{a,b,c}$ allora

$$S = \mathcal{N}_{a,b,p^r c} \qquad \text{per ogni } r \geq 1.$$

- Infatti $S = \mathcal{N}_{a,b,c} = \mathcal{N}_{a,b,p^r c}(N_c)$, e

$$N_c^{p^r} - N_{p^r c} = 0,$$

e quindi $S/\mathcal{N}_{a,b,p^r c}$ è *puramente inseparabile*.

Uno fra a, b, c divisibile per p non dà fastidio (1/2)

Proposizione

Se a, b, c sono primi con p e $S = \mathcal{N}_{a,b,c}$ allora

$$S = \mathcal{N}_{a,b,p^r c} \qquad \text{per ogni } r \geq 1.$$

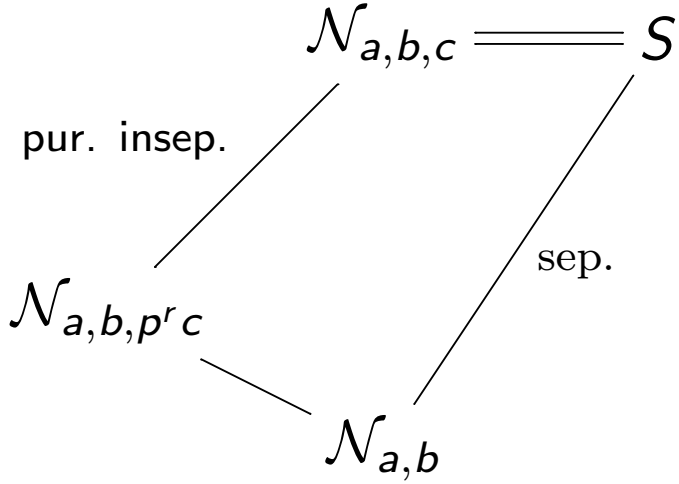
- Infatti $S = \mathcal{N}_{a,b,c} = \mathcal{N}_{a,b,p^r c}(N_c)$, e

$$N_c^{p^r} - N_{p^r c} = 0,$$

  e quindi $S/\mathcal{N}_{a,b,p^r c}$ è *puramente inseparabile*.
- Ma $S/\mathcal{N}_{a,b}$ è *separabile* (per il criterio dello jacobiano).

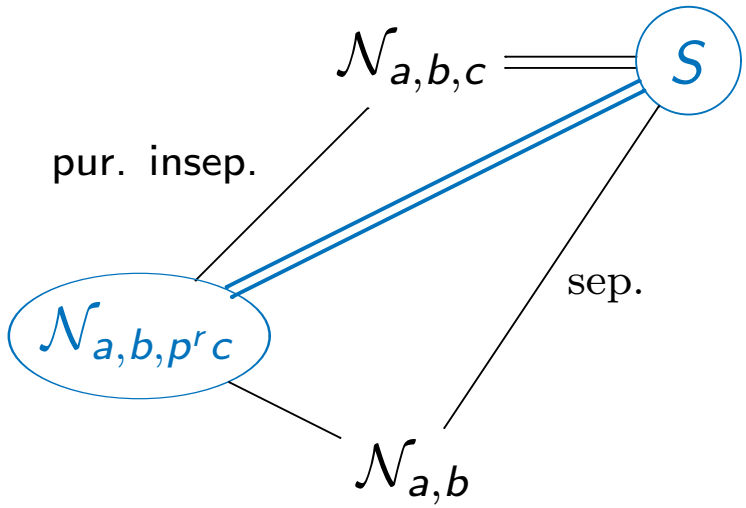
Uno fra a, b, c divisibile per p non dà fastidio (1/2)

- Riassumendo:



Uno fra a, b, c divisibile per p non dà fastidio (1/2)

- Riassumendo:



- Essendo $S/\mathcal{N}_{a,b,p^r c}$ sia separabile che puramente inseparabile, deve essere *banale*.

Dimostrazione (1/5)

Proposizione

Siano $a > b > c \geq 1$ *coprimi, e tali che* p *non divide* $a, b, c, a - b, a - c, b - c$. *Allora*

$$S = \mathcal{N}_{a,b,c}.$$

Dimostrazione (1/5)

Proposizione

Siano $a > b > c \geq 1$ *coprimi, e tali che* p *non divide* $a, b, c, a - b, a - c, b - c$. *Allora*

$$S = \mathcal{N}_{a,b,c}.$$

- Basta dimostrare che il grado $[F : \mathcal{N}_{a,b,c}]$ è 2.

Dimostrazione (1/5)

Proposizione

Siano $a > b > c \geq 1$ *coprimi, e tali che* p *non divide* $a, b, c, a - b, a - c, b - c$. *Allora*

$$S = \mathcal{N}_{a,b,c}.$$

- Basta dimostrare che il grado $[F : \mathcal{N}_{a,b,c}]$ è 2.
- Inoltre $F = \mathcal{N}_{a,b,c}(x)$, quindi basta dimostrare che x ha grado 2 su $\mathcal{N}_{a,b,c}$.

Dimostrazione (1/5)

Proposizione

Siano $a > b > c \geq 1$ *coprimi, e tali che* p *non divide* $a, b, c, a - b, a - c, b - c$. *Allora*

$$S = \mathcal{N}_{a,b,c}.$$

- Basta dimostrare che il grado $[F : \mathcal{N}_{a,b,c}]$ è 2.
- Inoltre $F = \mathcal{N}_{a,b,c}(x)$, quindi basta dimostrare che x ha grado 2 su $\mathcal{N}_{a,b,c}$.
- Supponiamo x abbia coniugati diversi da x, y in una chiusura algebrica di $\mathcal{N}_{a,b,c}$.

Dimostrazione (1/5)

Proposizione

Siano $a > b > c \geq 1$ *coprimi, e tali che* p *non divide* $a, b, c, a-b, a-c, b-c$. *Allora*

$$S = \mathcal{N}_{a,b,c}.$$

- Basta dimostrare che il grado $[F : \mathcal{N}_{a,b,c}]$ è 2.
- Inoltre $F = \mathcal{N}_{a,b,c}(x)$, quindi basta dimostrare che x ha grado 2 su $\mathcal{N}_{a,b,c}$.
- Supponiamo x abbia coniugati diversi da x, y in una chiusura algebrica di $\mathcal{N}_{a,b,c}$.
- Se z è un tale coniugato, allora per qualche w

$$x^m + y^m = N_m = z^m + w^m \qquad \text{per } m = a, b, c.$$

Dimostrazione (2/5)

$$x^m + y^m = z^m + w^m \qquad \text{per } m = a, b, c.$$

- Supponiamo quindi $\{x, y\} \neq \{z, w\}$.

Dimostrazione (2/5)

$$x^m + y^m = z^m + w^m \qquad \text{per } m = a, b, c.$$

- Supponiamo quindi $\{x, y\} \neq \{z, w\}$.
- Non ci sono due fra x, y, z, w che hanno rapporto costante.

Dimostrazione (2/5)

$$x^m + y^m = z^m + w^m \qquad \text{per } m = a, b, c.$$

- Supponiamo quindi $\{x, y\} \neq \{z, w\}$.
- Non ci sono due fra x, y, z, w che hanno rapporto costante.
- Infatti se $z = \mu x$ avremmo

$$\begin{aligned}\left((1-\mu^a)x^a + y^a\right)^b &= \left((1-\mu^b)x^b + y^b\right)^a,\\ \left((1-\mu^a)x^a + y^a\right)^c &= \left((1-\mu^c)x^c + y^c\right)^a.\end{aligned}$$

Dimostrazione (2/5)

$$x^m + y^m = z^m + w^m \qquad \text{per } m = a, b, c.$$

- Supponiamo quindi $\{x, y\} \neq \{z, w\}$.
- Non ci sono due fra x, y, z, w che hanno rapporto costante.
- Infatti se $z = \mu x$ avremmo

$$\begin{aligned}\left((1-\mu^a)x^a + y^a\right)^b &= \left((1-\mu^b)x^b + y^b\right)^a,\\ \left((1-\mu^a)x^a + y^a\right)^c &= \left((1-\mu^c)x^c + y^c\right)^a.\end{aligned}$$

- Dobbiamo avere $\mu^a = \mu^b = \mu^c = 1$,

Dimostrazione (2/5)

$$x^m + y^m = z^m + w^m \qquad \text{per } m = a, b, c.$$

- Supponiamo quindi $\{x, y\} \neq \{z, w\}$.
- Non ci sono due fra x, y, z, w che hanno rapporto costante.
- Infatti se $z = \mu x$ avremmo

$$\begin{aligned}\left((1-\mu^a)x^a + y^a\right)^b &= \left((1-\mu^b)x^b + y^b\right)^a,\\ \left((1-\mu^a)x^a + y^a\right)^c &= \left((1-\mu^c)x^c + y^c\right)^a.\end{aligned}$$

- Dobbiamo avere $\mu^a = \mu^b = \mu^c = 1$, e quindi $\mu = 1$

$$x = z, \qquad y = w.$$

Dimostrazione (3/5)

$$x^m + y^m = z^m + w^m \qquad \text{per } m = a, b, c.$$

- Estendiamo a una chiusura algebrica separabile di $k(z, w) \supset \mathcal{N}_{a,b,c}$ la derivazione ordinaria $\frac{\partial}{\partial z}$, che indichiamo con un apice.

Dimostrazione (3/5)

$$x^m + y^m = z^m + w^m \qquad \text{per } m = a, b, c.$$

- Estendiamo a una chiusura algebrica separabile di $k(z, w) \supset \mathcal{N}_{a,b,c}$ la derivazione ordinaria $\frac{\partial}{\partial z}$, che indichiamo con un apice. Derivando abbiamo

$$mx^{m-1}x' + my^{m-1}y' = mz^{m-1} \qquad \text{per } m = a, b, c,$$

Dimostrazione (3/5)

$$x^m + y^m = z^m + w^m \qquad \text{per } m = a, b, c.$$

- Estendiamo a una chiusura algebrica separabile di $k(z, w) \supset \mathcal{N}_{a,b,c}$ la derivazione ordinaria $\frac{\partial}{\partial z}$, che indichiamo con un apice. Derivando abbiamo

$$mx^{m-1}x' + my^{m-1}y' = mz^{m-1} \qquad \text{per } m = a, b, c,$$

- e quindi

$$x^{m-1}x' + y^{m-1}y' - z^{m-1} = 0 \qquad \text{per } m = a, b, c,$$

dato che a, b, c sono primi con p.

Dimostrazione (4/5)

$$x^{m-1}x' + y^{m-1}y' - z^{m-1} = 0 \qquad \text{per } m = a, b, c,$$

Dimostrazione (4/5)

$$x^{m-1}x' + y^{m-1}y' - z^{m-1} = 0 \qquad \text{per } m = a, b, c,$$

- queste equazioni equivalgono al sistema

$$\begin{pmatrix} x^a & y^a & z^a \\ x^b & y^b & z^b \\ x^c & y^c & z^c \end{pmatrix} \cdot \begin{pmatrix} x'/x \\ y'/y \\ -1/z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

Dimostrazione (4/5)

$$x^{m-1}x' + y^{m-1}y' - z^{m-1} = 0 \qquad \text{per } m = a, b, c,$$

- queste equazioni equivalgono al sistema

$$\begin{pmatrix} x^a & y^a & z^a \\ x^b & y^b & z^b \\ x^c & y^c & z^c \end{pmatrix} \cdot \begin{pmatrix} x'/x \\ y'/y \\ -1/z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

- e in particolare ci dicono che

$$\det \begin{pmatrix} x^a & y^a & z^a \\ x^b & y^b & z^b \\ x^c & y^c & z^c \end{pmatrix} = 0,$$

Dimostrazione (4/5)

$$x^{m-1}x' + y^{m-1}y' - z^{m-1} = 0 \qquad \text{per } m = a, b, c,$$

- queste equazioni equivalgono al sistema

$$\begin{pmatrix} x^a & y^a & z^a \\ x^b & y^b & z^b \\ x^c & y^c & z^c \end{pmatrix} \cdot \begin{pmatrix} x'/x \\ y'/y \\ -1/z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

- e in particolare ci dicono che

$$\det \begin{pmatrix} x^a & y^a & z^a \\ x^b & y^b & z^b \\ x^c & y^c & z^c \end{pmatrix} = 0, \qquad \det \begin{pmatrix} x^A & y^A & z^A \\ x^B & y^B & z^B \\ 1 & 1 & 1 \end{pmatrix} = 0$$

- dividendo le colonne, ponendo $A = a - c, B = b - c$.

Dimostrazione (5/5)

Il polinomio annullato da x, y, z è

$$R(X, Y, Z) = \det \begin{pmatrix} X^A & Y^A & Z^A \\ X^B & Y^B & Z^B \\ 1 & 1 & 1 \end{pmatrix},$$

Dimostrazione (5/5)

Il polinomio annullato da x, y, z è

$$R(X,Y,Z) = \det \begin{pmatrix} X^A & Y^A & Z^A \\ X^B & Y^B & Z^B \\ 1 & 1 & 1 \end{pmatrix},$$

$$V(X,Y,Z) = \det \begin{pmatrix} X^2 & Y^2 & Z^2 \\ X & Y & Z \\ 1 & 1 & 1 \end{pmatrix}.$$

Dimostrazione (5/5)

Il polinomio annullato da x, y, z è

$$R(X,Y,Z) = \det \begin{pmatrix} X^A & Y^A & Z^A \\ X^B & Y^B & Z^B \\ 1 & 1 & 1 \end{pmatrix},$$

$$V(X,Y,Z) = \det \begin{pmatrix} X^2 & Y^2 & Z^2 \\ X & Y & Z \\ 1 & 1 & 1 \end{pmatrix}.$$

Sia $d = \gcd(A,B)$, e

$$T(X,Y,Z) = T_{A,B}(X,Y,Z) = \frac{R(X,Y,Z)}{V(X^d, Y^d, Z^d)}$$

Dimostrazione (5/5)

Il polinomio annullato da x, y, z è

$$R(X,Y,Z) = \det \begin{pmatrix} X^A & Y^A & Z^A \\ X^B & Y^B & Z^B \\ 1 & 1 & 1 \end{pmatrix},$$

$$V(X,Y,Z) = \det \begin{pmatrix} X^2 & Y^2 & Z^2 \\ X & Y & Z \\ 1 & 1 & 1 \end{pmatrix}.$$

Sia $d = \gcd(A,B)$, e

$$T(X,Y,Z) = T_{A,B}(X,Y,Z) = \frac{R(X,Y,Z)}{V(X^d, Y^d, Z^d)}$$

- Siccome nessuno fra x, y, z differisce per una costante, allora $T(x,y,z) = 0$, perché $V(x^d, y^d, z^d) \neq 0$.

Dimostrazione (5/5)

Il polinomio annullato da x, y, z è

$$R(X,Y,Z) = \det \begin{pmatrix} X^A & Y^A & Z^A \\ X^B & Y^B & Z^B \\ 1 & 1 & 1 \end{pmatrix},$$

$$V(X,Y,Z) = \det \begin{pmatrix} X^2 & Y^2 & Z^2 \\ X & Y & Z \\ 1 & 1 & 1 \end{pmatrix}.$$

Sia $d = \gcd(A,B)$, e

$$T(X,Y,Z) = T_{A,B}(X,Y,Z) = \frac{R(X,Y,Z)}{V(X^d, Y^d, Z^d)}$$

- Siccome nessuno fra x, y, z differisce per una costante, allora $T(x,y,z) = 0$, perché $V(x^d, y^d, z^d) \neq 0$.
- Il risultato in caratteristica zero è stato ottenuto calcolando il gruppo di Galois di un polinomio collegato a $T(X,Y,Z)$, grazie al teorema di esistenza di Riemann.

Irriducibilità di $T_{A,B}(X, Y, Z)$ (1/2)

Per $s \geq r > 1$, sia

$$f(U) = f_s U^s + \cdots + f_r U^r + f_{r-1} U^{r-1} + \cdots + f_1 U + f_0 \in A[U].$$

Irriducibilità di $T_{A,B}(X, Y, Z)$ (1/2)

Per $s \geq r > 1$, sia

$$f(U) = f_s U^s + \cdots + \underset{\not\in P}{f_r} U^r + \underset{\in P}{f_{r-1}} U^{r-1} + \cdots + \underset{\in P}{f_1} U + \underset{\in P \setminus P^2}{f_0} \in A[U].$$

- per un certo ideale primo $P \subset A$.

Irriducibilità di $T_{A,B}(X, Y, Z)$ (1/2)

Per $s \geq r > 1$, sia

$$f(U) = f_s U^s + \cdots + \underset{\not\in P}{f_r} U^r + \underset{\in P}{f_{r-1}} U^{r-1} + \cdots + \underset{\in P}{f_1} U + \underset{\in P \setminus P^2}{f_0} \in A[U].$$

- per un certo ideale primo $P \subset A$.
- Chiameremo questa proprietà di $f(U)$ *segnatura bassa di lunghezza r relativa a P.*

Irriducibilità di $T_{A,B}(X, Y, Z)$ (1/2)

Per $s \geq r > 1$, sia

$$f(U) = f_s U^s + \cdots + \underset{\not\in P}{f_r} U^r + \underset{\in P}{f_{r-1}} U^{r-1} + \cdots + \underset{\in P}{f_1} U + \underset{\in P\setminus P^2}{f_0} \in A[U].$$

- per un certo ideale primo $P \subset A$.
- Chiameremo questa proprietà di $f(U)$ *segnatura bassa di lunghezza r relativa a P.*
- Questa è una *segnatura alta*:

$$f(U) = \underset{\in P\setminus P^2}{f_s} U^s + \underset{\in P}{f_{s-1}} U^{s-1} + \cdots + \underset{\in P}{f_{s-r+1}} U^{s-r+1} + \underset{\not\in P}{f_{s-r}} U^{s-r} + \cdots + f_0.$$

Irriducibilità di $T_{A,B}(X, Y, Z)$ (2/2)

$$f(U) = f_s U^s + \cdots + \underset{\not\in P}{f_r U^r} + \underset{\in P}{f_{r-1} U^{r-1}} + \cdots + \underset{\in P}{f_1 U} + \underset{\in P \setminus P^2}{f_0} .$$

Irriducibilità di $T_{A,B}(X, Y, Z)$ (2/2)

$$f(U) = f_s U^s + \cdots + \underset{\not\in P}{f_r U^r} + \underset{\in P}{f_{r-1} U^{r-1}} + \cdots + \underset{\in P}{f_1 U} + \underset{\in P \setminus P^2}{f_0} .$$

- se $f(U) = g(U)h(U)$ è una fattorizzazione,

Irriducibilità di $T_{A,B}(X, Y, Z)$ (2/2)

$$f(U) = f_s U^s + \cdots + \underset{\not\in P}{f_r U^r} + \underset{\in P}{f_{r-1} U^{r-1}} + \cdots + \underset{\in P}{f_1 U} + \underset{\in P\setminus P^2}{f_0} .$$

- se $f(U) = g(U)h(U)$ è una fattorizzazione, uno dei fattori, $g(U)$ poniamo, deve *ereditare* la segnatura

$$g(U) = g_t U^t + \cdots + \underset{\not\in P}{g_r U^r} + \underset{\in P}{g_{r-1} U^{r-1}} + \cdots + \underset{\in P}{g_1 U} + \underset{\in P\setminus P^2}{g_0} .$$

Irriducibilità di $T_{A,B}(X, Y, Z)$ (2/2)

$$f(U) = f_s U^s + \cdots + \underset{\not\in P}{f_r U^r} + \underset{\in P}{f_{r-1} U^{r-1}} + \cdots + \underset{\in P}{f_1 U} + \underset{\in P\setminus P^2}{f_0} .$$

- se $f(U) = g(U)h(U)$ è una fattorizzazione, uno dei fattori, $g(U)$ poniamo, deve *ereditare* la segnatura

$$g(U) = g_t U^t + \cdots + \underset{\not\in P}{g_r U^r} + \underset{\in P}{g_{r-1} U^{r-1}} + \cdots + \underset{\in P}{g_1 U} + \underset{\in P\setminus P^2}{g_0} .$$

- In particolare deve avere grado almeno r.

Irriducibilità di $T_{A,B}(X, Y, Z)$ (2/2)

$$f(U) = f_s U^s + \cdots + \underset{\not\in P}{f_r U^r} + \underset{\in P}{f_{r-1} U^{r-1}} + \cdots + \underset{\in P}{f_1 U} + \underset{\in P\setminus P^2}{f_0} .$$

- se $f(U) = g(U)h(U)$ è una fattorizzazione, uno dei fattori, $g(U)$ poniamo, deve *ereditare* la segnatura

$$g(U) = g_t U^t + \cdots + \underset{\not\in P}{g_r U^r} + \underset{\in P}{g_{r-1} U^{r-1}} + \cdots + \underset{\in P}{g_1 U} + \underset{\in P\setminus P^2}{g_0} .$$

- In particolare deve avere grado almeno r.
- Se $r = s$, allora $h(U)$ è costretto ad avere grado 0. E questo è il critero di irriducibilità di Eisenstein.

Caso con $d \neq B$ e $d \neq A - B$ (1/3)

$$I(X,Y,Z) = \frac{R(X,Y,Z)}{(X^d - Y^d)} = T(X,Y,Z) \cdot (Z^d - X^d)(Z^d - Y^d) =$$

$$= Z^A \prod_{\substack{\zeta^B=1 \\ \zeta^d \neq 1}} (X - \zeta Y) - Z^B \prod_{\substack{\xi^A=1 \\ \xi^d \neq 1}} (X - \xi Y) + X^B Y^B \prod_{\substack{\vartheta^{A-B}=1 \\ \vartheta^d \neq 1}} (X - \vartheta Y).$$

Caso con $d \neq B$ e $d \neq A - B$ (1/3)

$$I(X,Y,Z) = \frac{R(X,Y,Z)}{(X^d - Y^d)} = T(X,Y,Z) \cdot (Z^d - X^d)(Z^d - Y^d) =$$

$$= Z^A \prod_{\substack{\zeta^B=1 \\ \zeta^d \neq 1}} (X - \zeta Y) - Z^B \prod_{\substack{\xi^A=1 \\ \xi^d \neq 1}} (X - \xi Y) + X^B Y^B \prod_{\substack{\vartheta^{A-B}=1 \\ \vartheta^d \neq 1}} (X - \vartheta Y).$$

- Gli ζ, ξ, ϑ sono tutti distinti.

Caso con $d \neq B$ e $d \neq A - B$ (1/3)

$$I(X,Y,Z) = \frac{R(X,Y,Z)}{(X^d - Y^d)} = T(X,Y,Z) \cdot (Z^d - X^d)(Z^d - Y^d) =$$

$$= Z^A \prod_{\substack{\zeta^B=1 \\ \zeta^d \neq 1}} (X - \zeta Y) - Z^B \prod_{\substack{\xi^A=1 \\ \xi^d \neq 1}} (X - \xi Y) + X^B Y^B \prod_{\substack{\vartheta^{A-B}=1 \\ \vartheta^d \neq 1}} (X - \vartheta Y).$$

- Gli ζ, ξ, ϑ sono tutti distinti.
- Ha una segnatura bassa lunga B relativa ai $P_\vartheta = \langle X - \vartheta Y \rangle$ per ogni $\vartheta^{A-B} = 1, \vartheta^d \neq 1$,

Caso con $d \neq B$ e $d \neq A - B$ (1/3)

$$I(X,Y,Z) = \frac{R(X,Y,Z)}{(X^d - Y^d)} = T(X,Y,Z) \cdot (Z^d - X^d)(Z^d - Y^d) =$$

$$= Z^A \prod_{\substack{\zeta^B=1 \\ \zeta^d \neq 1}} (X - \zeta Y) - Z^B \prod_{\substack{\xi^A=1 \\ \xi^d \neq 1}} (X - \xi Y) + X^B Y^B \prod_{\substack{\vartheta^{A-B}=1 \\ \vartheta^d \neq 1}} (X - \vartheta Y).$$

- Gli ζ, ξ, ϑ sono tutti distinti.
- Ha una segnatura bassa lunga B relativa ai $P_\vartheta = \langle X - \vartheta Y \rangle$ per ogni $\vartheta^{A-B} = 1, \vartheta^d \neq 1$,
- e una segnatura alta lunga $A - B$ relativa ai $Q_\zeta = \langle X - \zeta Y \rangle$ per ogni $\zeta^B = 1, \zeta^d \neq 1$.

Caso con $d \neq B$ e $d \neq A - B$ (1/3)

$$I(X,Y,Z) = \frac{R(X,Y,Z)}{(X^d - Y^d)} = T(X,Y,Z) \cdot (Z^d - X^d)(Z^d - Y^d) =$$

$$= Z^A \prod_{\substack{\zeta^B=1 \\ \zeta^d \neq 1}} (X - \zeta Y) - Z^B \prod_{\substack{\xi^A=1 \\ \xi^d \neq 1}} (X - \xi Y) + X^B Y^B \prod_{\substack{\vartheta^{A-B}=1 \\ \vartheta^d \neq 1}} (X - \vartheta Y).$$

- Gli ζ, ξ, ϑ sono tutti distinti.
- Ha una segnatura bassa lunga B relativa ai $P_\vartheta = \langle X - \vartheta Y \rangle$ per ogni $\vartheta^{A-B} = 1, \vartheta^d \neq 1$,
- e una segnatura alta lunga $A - B$ relativa ai $Q_\zeta = \langle X - \zeta Y \rangle$ per ogni $\zeta^B = 1, \zeta^d \neq 1$.
- Le segnature vengono tutte ereditate da $T(X, Y, Z)$.

Caso con $d \neq B$ e $d \neq A - B$ (2/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

Caso con $d \neq B$ e $d \neq A - B$ (2/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- $T(X, Y, Z)$ ha grado $A - 2d$ in Z,

Caso con $d \neq B$ e $d \neq A - B$ (2/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- $T(X, Y, Z)$ ha grado $A - 2d$ in Z,
- un unico fattore, $G_1(X, Y, Z)$, poniamo eredita *tutte* le segnature, e ha grado $\geq \max(A - B, B)$.

Caso con $d \neq B$ e $d \neq A - B$ (2/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- $T(X, Y, Z)$ ha grado $A - 2d$ in Z,
- un unico fattore, $G_1(X, Y, Z)$, poniamo eredita *tutte* le segnature, e ha grado $\geq \max(A - B, B)$.
- Se $I \subseteq \{2, 3, \ldots, k\}$, $I \neq \emptyset$,

$$\prod_{i \in I} G_i(X, Y, Z) = Z^t + \cdots + X^r Y^s,$$

Caso con $d \neq B$ e $d \neq A - B$ (2/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- $T(X, Y, Z)$ ha grado $A - 2d$ in Z,
- un unico fattore, $G_1(X, Y, Z)$, poniamo eredita *tutte* le segnature, e ha grado $\geq \max(A - B, B)$.
- Se $I \subseteq \{2, 3, \ldots, k\}$, $I \neq \emptyset$,

$$\prod_{i \in I} G_i(X, Y, Z) = Z^t + \cdots + X^r Y^s,$$

- e non può essere simmetrico.

Caso con $d \neq B$ e $d \neq A - B$ (3/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- Quindi S_3 come gruppo che permuta X, Y, Z agisce *transitivamente* sui $G_i(X, Y, Z)$.

Caso con $d \neq B$ e $d \neq A - B$ (3/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- Quindi S_3 come gruppo che permuta X, Y, Z agisce *transitivamente* sui $G_i(X, Y, Z)$.
- L'azione conserva il grado omogeneo.

Caso con $d \neq B$ e $d \neq A - B$ (3/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- Quindi S_3 come gruppo che permuta X, Y, Z agisce *transitivamente* sui $G_i(X, Y, Z)$.
- L'azione conserva il grado omogeneo.
- $G_1(X, Y, Z)$ ha grado $\geq A - B$ in Z, ed eredita $B - d$ segnature alte,

Caso con $d \neq B$ e $d \neq A - B$ (3/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- Quindi S_3 come gruppo che permuta X, Y, Z agisce *transitivamente* sui $G_i(X, Y, Z)$.
- L'azione conserva il grado omogeneo.
- $G_1(X, Y, Z)$ ha grado $\geq A - B$ in Z, ed eredita $B - d$ segnature alte, quindi ha grado omogeneo $\geq A - d$

Caso con $d \neq B$ e $d \neq A - B$ (3/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- Quindi S_3 come gruppo che permuta X, Y, Z agisce *transitivamente* sui $G_i(X, Y, Z)$.
- L'azione conserva il grado omogeneo.
- $G_1(X, Y, Z)$ ha grado $\geq A - B$ in Z, ed eredita $B - d$ segnature alte, quindi ha grado omogeneo $\geq A - d$
- $T(X, Y, Z)$ ha grado omogeneo $A + B - 3d \nleq 2(A - d)$,

Caso con $d \neq B$ e $d \neq A - B$ (3/3)

$$T(X, Y, Z) = \prod_{i=1}^{k} G_i(X, Y, Z)$$

- Quindi S_3 come gruppo che permuta X, Y, Z agisce *transitivamente* sui $G_i(X, Y, Z)$.
- L'azione conserva il grado omogeneo.
- $G_1(X, Y, Z)$ ha grado $\geq A - B$ in Z, ed eredita $B - d$ segnature alte, quindi ha grado omogeneo $\geq A - d$
- $T(X, Y, Z)$ ha grado omogeneo $A + B - 3d \nleq 2(A - d)$,
- quindi $G_1(X, Y, Z)$ è l'unico fattore.

Caso con $d = B$ o $d = A - B$

- Questo discorso non funziona se $d = B$ o $d = A - B$.

Caso con $d = B$ o $d = A - B$

- Questo discorso non funziona se $d = B$ o $d = A - B$.
- Se $d = A - B$, rimpiazzando X, Y, Z con X^{-1}, Y^{-1}, Z^{-1} possiamo ricondurci al caso con $B = d$.

Caso con $d = B$ o $d = A - B$

- Questo discorso non funziona se $d = B$ o $d = A - B$.
- Se $d = A - B$, rimpiazzando X, Y, Z con X^{-1}, Y^{-1}, Z^{-1} possiamo ricondurci al caso con $B = d$.
- Se $A = r$ e $d = 1$,

$$T_{r,1}(X, Y, Z)$$

è la somma dei monomi di grado $r - 2$, e definisce una varietà non singolare in $\mathbb{P}^2$.

Caso con $d = B$ o $d = A - B$

- Questo discorso non funziona se $d = B$ o $d = A - B$.
- Se $d = A - B$, rimpiazzando X, Y, Z con X^{-1}, Y^{-1}, Z^{-1} possiamo ricondurci al caso con $B = d$.
- Se $A = r$ e $d = 1$,

$$T_{r,1}(X, Y, Z)$$

è la somma dei monomi di grado $r - 2$, e definisce una varietà non singolare in $\mathbb{P}^2$.

- Successivamente si può mostrare che

$$T_{dr,d}(X, Y, Z) = T_{r,1}(X^d, Y^d, Z^d)$$

definisce una varietà non singolare anche per $d \neq 1$.

Caso con $d = B$ o $d = A - B$

- Questo discorso non funziona se $d = B$ o $d = A - B$.
- Se $d = A - B$, rimpiazzando X, Y, Z con X^{-1}, Y^{-1}, Z^{-1} possiamo ricondurci al caso con $B = d$.
- Se $A = r$ e $d = 1$,

$$T_{r,1}(X, Y, Z)$$

è la somma dei monomi di grado $r - 2$, e definisce una varietà non singolare in $\mathbb{P}^2$.

- Successivamente si può mostrare che

$$T_{dr,d}(X, Y, Z) = T_{r,1}(X^d, Y^d, Z^d)$$

definisce una varietà non singolare anche per $d \neq 1$.

- Essi devono quindi essere irriducibili.

Conclusione della dimostrazione (1/3)

- Supponiamo quindi che

$$x^m + y^m - z^m = w^m, \qquad \text{per } m = a, b, c.$$

Conclusione della dimostrazione (1/3)

- Supponiamo quindi che

$$x^m + y^m - z^m = w^m, \qquad \text{per } m = a, b, c.$$

- Dato che $T(x, y, z) = 0$ e non esistono due che differiscano per una costante, si ricava che due qualunque fra x, y, z devono essere *algebricamente indipendenti*.

Conclusione della dimostrazione (1/3)

- Supponiamo quindi che

$$x^m + y^m - z^m = w^m, \qquad \text{per } m = a, b, c.$$

- Dato che $T(x, y, z) = 0$ e non esistono due che differiscano per una costante, si ricava che due qualunque fra x, y, z devono essere *algebricamente indipendenti*.
- Possiamo quindi definire

$$\hat{\varepsilon} : k(x, y) \to k(x, z)$$
$$x \mapsto x,$$
$$y \mapsto z,$$

Conclusione della dimostrazione (1/3)

- Supponiamo quindi che

$$x^m + y^m - z^m = w^m, \qquad \text{per } m = a, b, c.$$

- Dato che $T(x, y, z) = 0$ e non esistono due che differiscano per una costante, si ricava che due qualunque fra x, y, z devono essere *algebricamente indipendenti*.
- Possiamo quindi definire

$$\hat{\varepsilon} : k(x, y) \to k(x, z)$$
$$x \mapsto x,$$
$$y \mapsto z,$$
$$\varepsilon : k(x, y, z) \to k(x, y, z)$$
$$z \mapsto y,$$

- visto che $T(X, Y, Z)$ è simmetrico e irriducibile, e z soddisfa su x, y la stessa relazione di y su x, z.

Conclusione della dimostrazione (2/3)

- Avevamo quindi che

$$x^m + y^m - z^m = w^m, \qquad \text{per } m = a, b, c,$$

Conclusione della dimostrazione (2/3)

- Avevamo quindi che

$$x^m + y^m - z^m = w^m, \qquad \text{per } m = a, b, c,$$

- Estendendo ε a una chiusura algebrica di $k(x, y, z)$,

Conclusione della dimostrazione (2/3)

- Avevamo quindi che

$$x^m + y^m - z^m = w^m, \qquad \text{per } m = a, b, c,$$

- Estendendo ε a una chiusura algebrica di $k(x, y, z)$,
- applicato all'equazione abbiamo

$$x^m + z^m - y^m = u^m, \qquad \text{per } m = a, b, c,$$

Conclusione della dimostrazione (2/3)

- Avevamo quindi che

$$x^m + y^m - z^m = w^m, \qquad \text{per } m = a, b, c,$$

- Estendendo ε a una chiusura algebrica di $k(x, y, z)$,
- applicato all'equazione abbiamo

$$x^m + z^m - y^m = u^m, \qquad \text{per } m = a, b, c,$$

e sommando

$$2x^m = w^m + u^m, \qquad \text{per } m = a, b, c.$$

Conclusione della dimostrazione (3/3)

$$2x^m = w^m + u^m, \qquad \text{per } m = a, b, c.$$

Conclusione della dimostrazione (3/3)

$$2x^m = w^m + u^m, \qquad \text{per } m = a, b, c.$$

- Analogamente a quanto fatto prima con x, y, z avremmo potuto dimostrare che ogni due fra x, y, w sono algebricamente indipendenti.

Conclusione della dimostrazione (3/3)

$$2x^m = w^m + u^m, \qquad \text{per } m = a, b, c.$$

- Analogamente a quanto fatto prima con x, y, z avremmo potuto dimostrare che ogni due fra x, y, w sono algebricamente indipendenti.
- Ma eliminando u abbiamo

$$(2x^a - w^a)^b - (2x^b - w^b)^a = 0,$$

Conclusione della dimostrazione (3/3)

$$2x^m = w^m + u^m, \qquad \text{per } m = a, b, c.$$

- Analogamente a quanto fatto prima con x, y, z avremmo potuto dimostrare che ogni due fra x, y, w sono algebricamente indipendenti.
- Ma eliminando u abbiamo

$$(2x^a - w^a)^b - (2x^b - w^b)^a = 0,$$

- che ci dice che w e x sono algebricamente dipendenti.

Conclusione della dimostrazione (3/3)

$$2x^m = w^m + u^m, \qquad \text{per } m = a, b, c.$$

- Analogamente a quanto fatto prima con x, y, z avremmo potuto dimostrare che ogni due fra x, y, w sono algebricamente indipendenti.
- Ma eliminando u abbiamo

$$(2x^a - w^a)^b - (2x^b - w^b)^a = 0,$$

- che ci dice che w e x sono algebricamente dipendenti.
- Assurdo.

Riflessioni sulle ipotesi

- Abbiamo visto che se due fra a, b, c sono divisibili per p allora $\mathcal{N}_{a,b,c}$ non è mai uguale a S.

Riflessioni sulle ipotesi

- Abbiamo visto che se due fra a, b, c sono divisibili per p allora $\mathcal{N}_{a,b,c}$ non è mai uguale a S.
- Anche se uno solo è divisibile per p ci può andare male,

Riflessioni sulle ipotesi

- Abbiamo visto che se due fra a, b, c sono divisibili per p allora $\mathcal{N}_{a,b,c}$ non è mai uguale a S.
- Anche se uno solo è divisibile per p ci può andare male, ad esempio se gli indici sono a, b, pb e a, b coprimi e diversi da $1, 2$ o $1, 3$.

Riflessioni sulle ipotesi

- Abbiamo visto che se due fra a, b, c sono divisibili per p allora $\mathcal{N}_{a,b,c}$ non è mai uguale a S.
- Anche se uno solo è divisibile per p ci può andare male, ad esempio se gli indici sono a, b, pb e a, b coprimi e diversi da $1, 2$ o $1, 3$.
- Viene però da chiedersi se l'ipotesi sulle differenze sia realmente necessaria.

Riflessioni sulle ipotesi

- Abbiamo visto che se due fra a, b, c sono divisibili per p allora $\mathcal{N}_{a,b,c}$ non è mai uguale a S.
- Anche se uno solo è divisibile per p ci può andare male, ad esempio se gli indici sono a, b, pb e a, b coprimi e diversi da $1, 2$ o $1, 3$.
- Viene però da chiedersi se l'ipotesi sulle differenze sia realmente necessaria.
- Dalla dimostrazione ricaviamo che dobbiamo cercare dei casi in cui $T(X, Y, Z)$ si fattorizzi. E anzi che la fattorizzazione deve avere fattori non simmetrici.

Fattorizzazioni

Abbiamo che

$$T_{p^r,1}(X,Y,Z) = \prod_{\substack{\alpha\in\mathbb{F}_{p^r}\\ \alpha\neq 0,1}} (Z-\alpha X+(\alpha-1)Y),$$

Fattorizzazioni

Abbiamo che

$$T_{p^r,1}(X,Y,Z) = \prod_{\substack{\alpha\in\mathbb{F}_{p^r}\\ \alpha\neq 0,1}} (Z - \alpha X + (\alpha - 1)Y),$$

e che

$$T_{p^{2r}-1,p^r-1}(X,Y,Z) = \prod_{\substack{\alpha,\beta\in\mathbb{F}_{p^r}\\ \alpha,\beta\neq 0}} (Z - \alpha X - \beta Y).$$

Fattorizzazioni

Abbiamo che

$$T_{p^r,1}(X,Y,Z) = \prod_{\substack{\alpha\in\mathbb{F}_{p^r}\\ \alpha\neq 0,1}} (Z-\alpha X+(\alpha-1)Y),$$

e che

$$T_{p^{2r}-1,p^r-1}(X,Y,Z) = \prod_{\substack{\alpha,\beta\in\mathbb{F}_{p^r}\\ \alpha,\beta\neq 0}} (Z-\alpha X-\beta Y).$$

- Un po' in analogia con la fattorizzazione

$$X^{p^r-1}-Y^{p^r-1} = \prod_{\substack{\alpha\in\mathbb{F}_{p^r}\\ \alpha\neq 0}} (X-\alpha Y)$$

Controesempio (1/5)

- Supponiamo $p \neq 2$.

Controesempio (1/5)

- Supponiamo $p \neq 2$.
- Consideriamo il polinomio

$$P_\eta(X) \;=\; X^2 - 2\eta X + \eta, \qquad \text{per } \eta \in \mathbb{F}_p.$$

Controesempio (1/5)

- Supponiamo $p \neq 2$.
- Consideriamo il polinomio

$$P_\eta(X) \;=\; X^2 - 2\eta X + \eta, \qquad \text{per } \eta \in \mathbb{F}_p.$$

- Una radice α identifica univocamente η ($\alpha = 1/2$ non è mai radice per nessun η).

Controesempio (1/5)

- Supponiamo $p \neq 2$.
- Consideriamo il polinomio

$$P_\eta(X) \;=\; X^2 - 2\eta X + \eta, \qquad \text{per } \eta \in \mathbb{F}_p.$$

- Una radice α identifica univocamente η ($\alpha = 1/2$ non è mai radice per nessun η).
- $P_\eta(X)$ e $P_\kappa(X)$ non hanno radici in comune per $\eta \neq \kappa$,

Controesempio (1/5)

- Supponiamo $p \neq 2$.
- Consideriamo il polinomio

$$P_\eta(X) \;=\; X^2 - 2\eta X + \eta, \qquad \text{per } \eta \in \mathbb{F}_p.$$

- Una radice α identifica univocamente η ($\alpha = 1/2$ non è mai radice per nessun η).
- $P_\eta(X)$ e $P_\kappa(X)$ non hanno radici in comune per $\eta \neq \kappa$,
- e ciascuno ha due radici distinte a meno che

$$\Delta P_\eta(X) = 4(\eta^2 - \eta) = 0,$$

Controesempio (1/5)

- Supponiamo $p \neq 2$.
- Consideriamo il polinomio

$$P_\eta(X) \;=\; X^2 - 2\eta X + \eta, \qquad \text{per } \eta \in \mathbb{F}_p.$$

- Una radice α identifica univocamente η ($\alpha = 1/2$ non è mai radice per nessun η).
- $P_\eta(X)$ e $P_\kappa(X)$ non hanno radici in comune per $\eta \neq \kappa$,
- e ciascuno ha due radici distinte a meno che

$$\Delta P_\eta(X) = 4(\eta^2 - \eta) = 0,$$

- che succede solo per $\eta = 0, 1$.

Controesempio (1/5)

- Supponiamo $p \neq 2$.
- Consideriamo il polinomio

$$P_\eta(X) \;=\; X^2 - 2\eta X + \eta, \qquad \text{per } \eta \in \mathbb{F}_p.$$

- Una radice α identifica univocamente η ($\alpha = 1/2$ non è mai radice per nessun η).
- $P_\eta(X)$ e $P_\kappa(X)$ non hanno radici in comune per $\eta \neq \kappa$,
- e ciascuno ha due radici distinte a meno che

$$\Delta P_\eta(X) = 4(\eta^2 - \eta) = 0,$$

- che succede solo per $\eta = 0, 1$.
- In totale abbiamo quindi $2p - 2 \gneqq p$ radici.

Controesempio (2/5)

- Quindi per qualche $\eta \in \mathbb{F}_p$ il polinomio

$$P_\eta(X) = X^2 - 2\eta X + \eta$$

è *irriducibile*,

Controesempio (2/5)

- Quindi per qualche $\eta \in \mathbb{F}_p$ il polinomio

$$P_\eta(X) = X^2 - 2\eta X + \eta$$

  è *irriducibile*,
- e le radici α, β vengono scambiate dall'automorfismo di Frobenius.

Controesempio (2/5)

- Quindi per qualche $\eta \in \mathbb{F}_p$ il polinomio

$$P_\eta(X) = X^2 - 2\eta X + \eta$$

è *irriducibile*,

- e le radici α, β vengono scambiate dall'automorfismo di Frobenius.
- Vengono scambiate applicando il Frobenius un numero qualunque *dispari* di volte

$$\alpha^{p^{2k+1}} = \beta, \qquad \beta^{p^{2k+1}} = \alpha$$

per ogni k.

Controesempio (3/5)

$$p_\eta(X) = X^2 - \underset{\alpha+\beta}{2\eta}\, X + \underset{\alpha\beta}{\eta}$$

- Per costruzione abbiamo che

$$2\alpha\beta = 2\eta = \alpha + \beta.$$

Controesempio (3/5)

$$p_\eta(X) \;=\; X^2 - \underset{\substack{\| \\ \alpha+\beta}}{2\eta}\, X + \underset{\substack{\| \\ \alpha\beta}}{\eta}$$

- Per costruzione abbiamo che

$$2\alpha\beta = 2\eta = \alpha + \beta.$$

- Quindi prendiamo

$$z = \alpha x + (1-\alpha)y, \qquad w \;=\; (1-\alpha)x + \alpha y,$$

Controesempio (3/5)

$$p_\eta(X) = X^2 - \underset{\alpha+\beta}{2\eta}\, X + \underset{\alpha\beta}{\eta}$$

- Per costruzione abbiamo che

$$2\alpha\beta = 2\eta = \alpha + \beta.$$

- Quindi prendiamo

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y,$$

- in modo da avere

$$x + y = z + w.$$

Controesempio (4/5)

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y$$

Inoltre per ogni k intero

$$z^{p^{2k+1}+1} + w^{p^{2k+1}+1}$$

Controesempio (4/5)

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y$$

Inoltre per ogni k intero

$$z^{p^{2k+1}+1} + w^{p^{2k+1}+1} = z^{p^{2k+1}} \cdot z + w^{p^{2k+1}} \cdot w$$

Controesempio (4/5)

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y$$

Inoltre per ogni k intero

$$\begin{aligned} z^{p^{2k+1}+1} + w^{p^{2k+1}+1} &= z^{p^{2k+1}} \cdot z + w^{p^{2k+1}} \cdot w \\ &= \big(\alpha x + (1-\alpha)y\big)^{p^{2k+1}} \big(\alpha x + (1-\alpha)y\big) \\ &\quad + \big((1-\alpha)x + \alpha y\big)^{p^{2k+1}} \big((1-\alpha)x + \alpha y\big) \end{aligned}$$

Controesempio (4/5)

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y$$

Inoltre per ogni k intero

$$\begin{aligned} z^{p^{2k+1}+1} + w^{p^{2k+1}+1} &= z^{p^{2k+1}} \cdot z + w^{p^{2k+1}} \cdot w \\ &= \big(\alpha x + (1-\alpha)y\big)^{p^{2k+1}} \big(\alpha x + (1-\alpha)y\big) \\ &\quad + \big((1-\alpha)x + \alpha y\big)^{p^{2k+1}} \big((1-\alpha)x + \alpha y\big) \\ &= \big(\beta x^{p^{2k+1}} + (1-\beta)y^{p^{2k+1}}\big)\big(\alpha x + (1-\alpha)y\big) \\ &\quad + \big((1-\beta)x^{p^{2k+1}} + \beta y^{p^{2k+1}}\big)\big((1-\alpha)x + \alpha y\big) \end{aligned}$$

Controesempio (4/5)

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y$$

Inoltre per ogni k intero

$$\begin{aligned}
z^{p^{2k+1}+1} + w^{p^{2k+1}+1} &= z^{p^{2k+1}} \cdot z + w^{p^{2k+1}} \cdot w \\
&= \big(\alpha x + (1-\alpha)y\big)^{p^{2k+1}} \big(\alpha x + (1-\alpha)y\big) \\
&\quad + \big((1-\alpha)x + \alpha y\big)^{p^{2k+1}} \big((1-\alpha)x + \alpha y\big) \\
&= \big(\beta x^{p^{2k+1}} + (1-\beta)y^{p^{2k+1}}\big)\big(\alpha x + (1-\alpha)y\big) \\
&\quad + \big((1-\beta)x^{p^{2k+1}} + \beta y^{p^{2k+1}}\big)\big((1-\alpha)x + \alpha y\big) \\
&= \big(2\alpha\beta - \alpha - \beta + 1\big)\big(x^{p^{2k+1}+1} + y^{p^{2k+1}+1}\big) \\
&\quad + \big(\beta + \alpha - 2\beta\alpha\big)\big(x^{p^{2k+1}} y + x y^{p^{2k+1}}\big)
\end{aligned}$$

Controesempio (4/5)

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y$$

Inoltre per ogni k intero

$$\begin{aligned}
z^{p^{2k+1}+1} + w^{p^{2k+1}+1} &= z^{p^{2k+1}} \cdot z + w^{p^{2k+1}} \cdot w \\
&= \big(\alpha x + (1-\alpha)y\big)^{p^{2k+1}} \big(\alpha x + (1-\alpha)y\big) \\
&\quad + \big((1-\alpha)x + \alpha y\big)^{p^{2k+1}} \big((1-\alpha)x + \alpha y\big) \\
&= \big(\beta x^{p^{2k+1}} + (1-\beta)y^{p^{2k+1}}\big)\big(\alpha x + (1-\alpha)y\big) \\
&\quad + \big((1-\beta)x^{p^{2k+1}} + \beta y^{p^{2k+1}}\big)\big((1-\alpha)x + \alpha y\big) \\
&= \big(2\alpha\beta - \alpha - \beta + 1\big)\big(x^{p^{2k+1}+1} + y^{p^{2k+1}+1}\big) \\
&\quad + \big(\beta + \alpha - 2\beta\alpha\big)\big(x^{p^{2k+1}} y + x y^{p^{2k+1}}\big)
\end{aligned}$$

Controesempio (4/5)

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y$$

Inoltre per ogni k intero

$$\begin{aligned}
z^{p^{2k+1}+1} + w^{p^{2k+1}+1} &= z^{p^{2k+1}} \cdot z + w^{p^{2k+1}} \cdot w \\
&= \big(\alpha x + (1-\alpha)y\big)^{p^{2k+1}} \big(\alpha x + (1-\alpha)y\big) \\
&\quad + \big((1-\alpha)x + \alpha y\big)^{p^{2k+1}} \big((1-\alpha)x + \alpha y\big) \\
&= \big(\beta x^{p^{2k+1}} + (1-\beta)y^{p^{2k+1}}\big)\big(\alpha x + (1-\alpha)y\big) \\
&\quad + \big((1-\beta)x^{p^{2k+1}} + \beta y^{p^{2k+1}}\big)\big((1-\alpha)x + \alpha y\big) \\
&= \big(2\alpha\beta - \alpha - \beta + 1\big)\big(x^{p^{2k+1}+1} + y^{p^{2k+1}+1}\big) \\
&\quad + \big(\beta + \alpha - 2\beta\alpha\big)\big(x^{p^{2k+1}} y + x y^{p^{2k+1}}\big) \\
&= x^{p^{2k+1}+1} + y^{p^{2k+1}+1}
\end{aligned}$$

dato che $\alpha + \beta = 2\alpha\beta$.

Controesempio (5/5)

- Quindi prendiamo a, b, c uguali a $1, p^{2k+1}+1, p^{2\ell+1}+1$ per $k > \ell \geq 0$

Controesempio (5/5)

- Quindi prendiamo a, b, c uguali a $1, p^{2k+1}+1, p^{2\ell+1}+1$ per $k > \ell \geq 0$
- e abbiamo la coppia 'alternativa'

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y,$$

Controesempio (5/5)

- Quindi prendiamo a, b, c uguali a $1, p^{2k+1}+1, p^{2\ell+1}+1$ per $k > \ell \geq 0$
- e abbiamo la coppia 'alternativa'

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y,$$

- e quindi in questo caso $\mathcal{N}_{a,b,c} \subsetneq S$.

Controesempio (5/5)

- Quindi prendiamo a, b, c uguali a $1, p^{2k+1}+1, p^{2\ell+1}+1$ per $k > \ell \geq 0$
- e abbiamo la coppia 'alternativa'

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y,$$

- e quindi in questo caso $\mathcal{N}_{a,b,c} \subsetneq S$.
- È anzi possibile mostrare che dati $r > s \geq 0$, e $m = \gcd(r,s)$

$$[S : \mathcal{N}_{p^r+1,p^s+1,1}] = \begin{cases} 1 & \text{se } 2m \nmid (r-s) \\ \frac{p^m+1}{2} & \text{se } 2m \mid (r-s) \end{cases}$$

Controesempio (5/5)

- Quindi prendiamo a, b, c uguali a $1, p^{2k+1}+1, p^{2\ell+1}+1$ per $k > \ell \geq 0$
- e abbiamo la coppia 'alternativa'

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y,$$

- e quindi in questo caso $\mathcal{N}_{a,b,c} \subsetneq S$.
- È anzi possibile mostrare che dati $r > s \geq 0$, e $m = \gcd(r,s)$

$$[S : \mathcal{N}_{p^r+1,p^s+1,1}] = \begin{cases} 1 & \text{se } 2m \nmid (r-s) \\ \frac{p^m+1}{2} & \text{se } 2m \mid (r-s) \end{cases}$$

- Si costruisce un controesempio simile anche in caratteristica 2, e in questo caso il grado è

$$[S : \mathcal{N}_{2^r+1,2^s+1,1}] = 2^{m-1}.$$

Teorema di Kakeya

Teorema (Kakeya)

Sia $\alpha = (\alpha_1, \ldots, \alpha_n)$ *una tupla di interi positivi distinti tali che il complementare nei naturali positivi*

$$C_\alpha \;=\; \mathbb{N}^+ \setminus \{\alpha_1, \ldots, \alpha_n\}$$

è chiuso rispetto all'addizione. Allora $p_{\alpha_1}, \ldots, p_{\alpha_n}$ *generano l'intero campo delle funzioni simmetriche in n variabili* $x_1, \ldots, x_n$.

Teorema di Kakeya

Teorema (Kakeya)

Sia $\alpha = (\alpha_1, \ldots, \alpha_n)$ *una tupla di interi positivi distinti tali che il complementare nei naturali positivi*

$$C_\alpha \;=\; \mathbb{N}^+ \setminus \{\alpha_1, \ldots, \alpha_n\}$$

è chiuso rispetto all'addizione. Allora $p_{\alpha_1}, \ldots, p_{\alpha_n}$ *generano l'intero campo delle funzioni simmetriche in n variabili* $x_1, \ldots, x_n$.

- Include i casi con N_1, N_2 e N_1, N_3 in due variabili.

Teorema di Kakeya

Teorema (Kakeya)

Sia $\alpha = (\alpha_1, \ldots, \alpha_n)$ *una tupla di interi positivi distinti tali che il complementare nei naturali positivi*

$$C_\alpha \;=\; \mathbb{N}^+ \setminus \{\alpha_1, \ldots, \alpha_n\}$$

è chiuso rispetto all'addizione. Allora $p_{\alpha_1}, \ldots, p_{\alpha_n}$ *generano l'intero campo delle funzioni simmetriche in n variabili* $x_1, \ldots, x_n$.

- Include i casi con N_1, N_2 e N_1, N_3 in due variabili.
- Si congettura che valga il se e solo se.

Teorema di Kakeya

Teorema (Kakeya)

Sia $\alpha = (\alpha_1, \ldots, \alpha_n)$ *una tupla di interi positivi distinti tali che il complementare nei naturali positivi*

$$C_\alpha \;=\; \mathbb{N}^+ \setminus \{\alpha_1, \ldots, \alpha_n\}$$

è chiuso rispetto all'addizione. Allora $p_{\alpha_1}, \ldots, p_{\alpha_n}$ *generano l'intero campo delle funzioni simmetriche in* n *variabili* $x_1, \ldots, x_n$.

- Include i casi con N_1, N_2 e N_1, N_3 in due variabili.
- Si congettura che valga il se e solo se.
- In generale il grado di S sul campo generato da n polinomi di Newton è difficile da calcolare (mentre per $n = 2$ c'è la formula semplice di Mead e Stein).

Soluzione in più variabili

Teorema (Dvornicich-Zannier, 2008)

Sia $a = (a_1, \ldots, a_{n+1})$ *una tupla di interi positivi distinti e coprimi. Allora in* n *variabili* $x_1, \ldots, x_n$ *il campo* $\mathcal{N}_a$ *generato dai polinomi di Newton* $N_{a_1}, \ldots, N_{a_{n+1}}$ *è l'intero campo simmetrico in* n *variabili.*

Soluzione in più variabili

Teorema (Dvornicich-Zannier, 2008)

Sia $a = (a_1, \ldots, a_{n+1})$ *una tupla di interi positivi distinti e coprimi. Allora in* n *variabili* $x_1, \ldots, x_n$ *il campo* $\mathcal{N}_a$ *generato dai polinomi di Newton* $N_{a_1}, \ldots, N_{a_{n+1}}$ *è l'intero campo simmetrico in* n *variabili.*

- È un risultato difficile!

Soluzione in più variabili

Teorema (Dvornicich-Zannier, 2008)

Sia $a = (a_1, \ldots, a_{n+1})$ *una tupla di interi positivi distinti e coprimi. Allora in* n *variabili* $x_1, \ldots, x_n$ *il campo* $\mathcal{N}_a$ *generato dai polinomi di Newton* $N_{a_1}, \ldots, N_{a_{n+1}}$ *è l'intero campo simmetrico in* n *variabili.*

- È un risultato difficile!
- Se $T(X_1, \ldots, X_n)$ è l'analogo in n variabili di $T(X, Y, Z)$, è possibile giungere alla conclusione usando soltanto l'irriducibilità, come quanto fatto in caratteristica p.

Fine

Domande?

Grazie per l'ascolto!