Note di Matematica Vol.VI, 139-154(1986)

SUL NUMERO DELLE SOLUZIONI DI CERTI SISTEMI ALGEBRICI DI CONGRUENZE IN UN CAMPO DI GALOIS(*)

Emanuela UGHI

Summary. *In this paper one proves a generalized version to the case of any number of variables of a result by U. Bartocci* [1] *concerning the existence of solutions of certain algebraic systems of congruences in a given Galois field.*

INTRODUZIONE. Fissati due qualsiasi interi $r > 1$ ed $n \geq 1$, considereremo nel presente lavoro la totalità $K(r)$ dei campi di Galois $GF(q)$ tali che r sia un divisore di $(q-1)$, e quindi la totalità $\Sigma(K(r))$ dei sistemi σ di equazioni algebriche della forma

$$\sigma : y_1^r = f_1(X), \ldots, y_m^r = f_m(X),$$

dove $X = (x_1, \ldots, x_n)$ rappresenti il complesso di n indeterminate x_j, $j=1,\ldots,n$, $m \geq 1$ sia un numero intero arbitrario, e gli elementi $f_i(X)$, $i=1,\ldots,m$, siano polinomi di grado positivo d_i a coefficienti in qualche campo di Galois $GF(q) \in K(r)$. Fissata adesso una coppia $(\sigma, GF(q))$ in modo tale che σ sia definito sopra $GF(q)$, quella che ci si propone di indagare è l'esistenza di n-ple ordinate $\bar{X} = (\bar{x}_1, \ldots, \bar{x}_n)$ $\in GF(q)^n$ tali che il sistema σ sia risolubile

---

(*) Lavoro eseguito nell'ambito dell'attività del Gruppo di ricerca nazionale in "Geometria Algebrica".

in $GF(q)^{n+m}$ mediante (n+m)-ple del tipo $(\bar{x}_1,\ldots,\bar{x}_n,\bar{y}_1,\ldots,\bar{y}_m)$ soddisfacenti alla condizione che tutte le $\bar{y}_i$, i=1,...,m, siano diverse da zero.

In altre parole, detto H(q,r) il sottogruppo moltiplicativo di $GF(q)^* = GF(q) - \{0\}$ di indice r, tale richiesta per l'n-pla $\bar{X}$ è equivalente alle condizioni $f_i(\bar{X}) \in H(q,r)$ per ogni i=1,...,m, condizioni che riassumeremo quindi dicendo che $\bar{X}$ è una soluzione definita sopra GF(q) del *sistema algebrico di congruenze*

$$f_i(X) \in H(q,r) , \qquad i=1,\ldots,m.$$

Detto tipo τ di un siffatto sistema l'(m+1)-pla ordinata $\tau = (m,d_1,\ldots,d_m)$, in un recente lavoro [1] viene stabilita la seguente

PROPOSIZIONE A. *Nell'ipotesi* n=1 *comunque assegnato un tipo* τ *di sistemi, esiste una costante* $C(\tau)$ *dipendente soltanto da* τ, *tale che un qualsiasi sistema algebrico di congruenze di tipo* τ *definito sopra un campo di Galois* GF(q) e K(r) *è risolubile in* GF(q) *non appena sia* $q \geq C(\tau)$ *e siano inoltre verificate le due seguenti condizioni:*

(a) *i polinomi* $f_i(x)$, i=1,...,m, *definenti il sistema siano privi di radici multiple;*

(b) *i polinomi* $f_i(x)$, i=1,...,m *siano a due a due primi fra di loro.*

In altre parole, considerata la totalità dei sistemi algebrici di congruenze di dato tipo e soddisfacenti alle due condizioni (a) e (b), si prova che essi sono sempre risolubili in un qualsiasi campo GF(q)eK(r) in cui si possano pensare definiti con l'ecce-

zione al più di un *numero finito* di campi GF(q) in K(r). Si noti esplicitamente che la totalità K(r) è così grande da contenere campi di Galois per infiniti valori della caratteristica p (a norma del Teorema di Dirichlet sui numeri primi), e che essa è *chiusa* rispetto alle estensioni di campo, nel senso che se $GF(q') \supseteq GF(q)$ e $GF(q) \in K(r)$, allora anche $GF(q') \in K(r)$. Ad esempio, nel caso r=2, K(2) coincide con l'intera totalità dei campi di Galois di ordine dispari, ovvero, di caratteristica diversa da 2.

La Proposizione A, che si riferisce sostanzialmente alla possibilità di risolvere simultaneamente infiniti sistemi algebrici di congruenze in un campo finito senza fare ricorso a successive estensioni del campo base, è stata utilizzata sia nel lavoro dianzi richiamato, che, in forme più semplificate, in altri recenti scritti [2], [3], nella costruzione di particolari esempi di strutture combinatorie, e sembra feconda di applicazioni nella ricerca di risposte di tipo asintotico ai problemi concernenti l'esistenza di siffatte configurazioni. Nel presente lavoro si dimostra come la Proposizione A continui a sussistere, con qualche leggera modificazione, anche quando si passi a considerare il caso di polinomi in un qualsivoglia numero n di variabili, e questa circostanza riveste qualche interesse in ordine a possibili generalizzazioni delle costruzioni cui si faceva cenno poc'anzi dal caso di un piano proiettivo a quello di un generico spazio proiettivo in un qualunque numero di dimensioni ([8], [9]).

Dimostreremo qui la seguente

PROPOSIZIONE B. *Con le stesse notazioni dianzi fissate e nella ipotesi* $n \geq 2$, *comunque assegnato un tipo* τ *di sistemi ed un numero intero* $\bar{N}>0$, *esiste una costante* $C(\tau,\bar{N})$ *dipendente soltanto da* τ *e da* $\bar{N}$, *tale che un qualsiasi sistema algebrico di congruenze di tipo* τ *definito sopra un campo di Galois* $GF(q) \in K(r)$ *ammette almeno* $\bar{N}$ *soluzioni distinte in* $GF(q)^n$ *non appena sia* $q \geq C(\tau,\bar{N})$, *e siano inoltre verificate le due seguenti condizioni:*

(a) *i polinomi* $f_i(X)$, $i=1,\ldots,m$ *siano semplici ed a due a due primi fra di loro (nell'anello* $GF(q)[X]$ *o nell'anello* $\overline{GF(q)}[X]$ *fa lo stesso, indicando con* $\overline{GF(q)}$ *la chiusura algebrica del campo* $GF(q)$);

(b) *i fattori irriducibili di ogni polinomio* $f_i(X)$ *in* $GF(q)[X]$ *continuino ad essere tali anche in* $\overline{GF(q)}[X]$, *ovvero, come si dice, siano assolutamente irriducibili.*

La Proposizione B consiste sostanzialmente nell'affermare che, comunque assegnato un carattere moltiplicativo χ di un campo di Galois $GF(q)$, allora si può sempre trovare in $GF(q)^n$ qualche soluzione di quello che chiameremo ancora un sistema algebrico di congruenze della forma $\chi(f_i(X)) = \varepsilon_i$, $i=1,\ldots,m$, ove gli ε_i siano possibili valori del carattere χ arbitrariamente assegnati, non appena q sia "abbastanza grande", ovvero, superiore ad una certa costante C dipendente soltanto dal numero dei polinomi $f_i(X)$ e dai loro gradi, oltreché naturalmente dalla specie del carattere χ (e non si dimentichino le due condizioni ulteriori (a) e (b)). Proveremo anzi che tale numero di soluzioni diverge al crescere di q, naturalmente una volta che restino fissati

tali invarianti, per il che si rimanda all'inizio del §2.

Notiamo anche come la dimostrazione della Proposizione B presenti, rispetto a quella della Proposizione A, l'ulteriore difficoltà costituita dalla comparsa di varietà singolari di dimensione superiore, per le quali non è pertanto possibile l'applicazione delle ben note stime di Deligne generalizzanti a qualsiasi numero di dimensioni quella famosa cosiddetta di Hasse-Weil concernente il caso delle curve e che viene usata in [1], e ciò a causa della perdurante mancanza di un conveniente teorema di desingolarizzazione delle varietà di dimensione superiore in caratteristica positiva. In vista di tale difficoltà, verranno nel seguito usate alcune stime sul numero dei punti di una varietà irriducibile qualsiasi meno forti di quelle, ma comunque sufficienti ai fini desiderati.

Nel §1 daremo una dimostrazione "diretta" della Proposizione B, la quale presenta però lo svantaggio di dover stabilire con opportune considerazioni di natura assai tecnica l'irriducibilità di una certa varietà di dimensione n. Nel §2 daremo quindi per questo motivo una dimostrazione meno diretta, la quale, attraverso l'utilizzazione di un metodo di Davenport già usato in [1] (cfr. [2]), riconduce tutta la questione al caso di sole ipersuperficie, per le quali le cose sono assai più facili.

§1. La dimostrazione "diretta" della Proposizione B discende dai due seguenti fatti:

PROPOSIZIONE 1. *La varietà algebrica* V *definita nello spazio affine* $(n+m)$*-dimensionale sopra al campo* $\overline{GF(q)}$ *dal sistema di equazioni* $y_i^r - f_i(x_1,\ldots,x_n) = 0$, $i=1,\ldots,m$, *è irriducibile (e di*

dimensione n *e codimensione* m) .

PROPOSIZIONE 2 (cfr. [7],p.263). *Se* V *è una varietà irriducibile* d-*dimensionale dello spazio affine* $\overline{GF(q)}^k$ *definita sopra il campo di Galois* GF(q) *da un sistema di equazioni* $F_1(x_1,\ldots,x_k)= \ldots = F_s(x_1,\ldots,x_k) = 0$, *il numero dei punti* $|V|_q$ *di* V *definiti sopra al campo* GF(q) *soddisfa alla disuguaglianza*

$$||V|_q - q^d| \leq c\, q^{d-1/2} ,$$

essendo c *una costante che dipende soltanto dal numero* k *delle variabili, da* s , *e dai gradi dei polinomi* $F_j(x_1,\ldots,x_k)$, j=1,..,s.

Rimandando per un attimo la dimostrazione della Proposizione 1, facciamo vedere subito come dalle due precedenti proposizioni consegua il risultato.

Un punto della varietà algebrica V definita nella Proposizione 1, diciamolo $(\bar{x}_1,\ldots,\bar{x}_n,\bar{y}_1,\ldots,\bar{y}_m)$, corrisponde ad una soluzione $(\bar{x}_1,\ldots,\bar{x}_n)$ del sistema di congruenze assegnato non appena esso sia definito sopra GF(q), e ciascuna delle coordinate $\bar{y}_i$, i=1,...,m, sia diversa dallo zero. Basta tenere conto del fatto che il sottogruppo H coincide esattamente con il sottogruppo di GF(q)* costituito dalle sue potenze r-me. Così, il numero N di siffatte soluzioni $(\bar{X})$ del sistema di congruenze assegnato risulta legato a quello $|V|_q$ dei punti della varietà V razionali sopra GF(q), per il tramite della relazione

$$N = \frac{1}{r^m} (|V|_q - |Z|_q), \tag{1}$$

nella quale $|Z|_q$ sta ad indicare il numero dei punti di V razionali sopra a GF(q) contenuti in qualcuno degli iperpiani coordinati

di equazione $y_i = 0$, $i=1,\ldots,m$. Basta allo scopo osservare che se $(\bar{X},\bar{Y})$ è un punto di V definito sopra GF(q) con tutte le $\bar{y}_i$ diverse da zero, allora è tale anche ogni punto del tipo $(\bar{X},\eta_1\bar{y}_1,\ldots,\eta_m\bar{y}_m)$, al variare arbitrario dei valori $\eta_1,\ldots,\eta_m$ nel gruppo delle radici r-me dell'unità in $\overline{GF(q)}$ (si ricordi che, nelle ipotesi attuali, tale gruppo è contenuto in GF(q), e che l'intero r è primo con p, la caratteristica del campo di Galois in questione). Ora, dalla Proposizione 2, tenuto conto dell'asserita irriducibilità di V, consegue che

$$|V|_q \geq q^n - c\, q^{n-1/2} , \tag{2}$$

per una qualche costante c dipendente soltanto da m,n,r e dai gradi dei polinomi $f_i(X)$ assegnati, mentre per l'intero $|Z|_q$ può provarsi invece che

$$|Z|_q \leq c_1\, r^{m-1}(q^{n-1} + c_2 q^{n-3/2}) , \tag{3}$$

per analoghe costanti c_1 e c_2.

Infatti, i punti che dobbiamo valutare sono quelli che stanno nel luogo algebrico $Z = \bigcup_{i=1}^{m}[V \cap (y_i=0)]$, sicché $|Z|_q$ sarà non superiore al numero dei punti definiti sopra GF(q) contenuti in ciascuna di quelle sezioni iperpiane di V. La i-ma di queste sezioni iperpiane ha a sua volta un numero di punti sopra GF(q) non superiore al numero dei punti sopra GF(q) dell'ipersuperficie di $\overline{GF(q)}^n$ avente equazione $f_i(X)=0$, questo moltiplicato per r^{m-1}, potendosi naturalmente, una volta fissato uno di questi punti, moltiplicare ciascuna delle altre coordinate y_j, $j=1,\ldots,m$, $j\neq i$, per arbitrari valori di radici r-me dell'unità contenute in GF(q)

analogamente a quanto visto prima. Si tratta in sostanza di stimare allora il numero dei punti razionali sopra a GF(q) di una siffatta ipersuperficie, e, tenuto conto che dall'ipotesi (b) consegue che ciascuna di queste ha tutte le sue componenti irriducibili definite sopra GF(q), il numero delle quali allora non supera evidentemente il grado di f_i, ed il cui ordine sarà pure pertanto non superiore a detto grado, si trova in definitiva, usando la Proposizione 2, che tale numero sarà non superiore a una quantità $c'_i(q^{n-1}+c''_i q^{n-3/2})$, per opportune costanti c'_i, c''_i del solito tipo. Da queste m disuguaglianze si deduce infine la (3) moltiplicando per r^{m-1} come già detto, e sommando rispetto ad i, i=1,...,m, dopo di aver sostituito ai valori c'_i e c''_i i loro valori massimi per ogni possibile tipo di spezzamento.

Combinando adesso le due stime (2) e (3), si ottiene dalla (1)

$$N = \frac{1}{r^m}(|V|_q - |Z|_q) \geq \frac{1}{r^m}[q^n - cq^{n-1/2} - c_1 r^{m-1}(q^{n-1}+c_2 q^{n-3/2})]$$

dalla quale discende immediatamente la conclusione desiderata al divergere di q.

Terminiamo il presente paragrafo con l'annunciata dimostrazione della Proposizione 1. Questa si può precisare nella

PROPOSIZIONE 3. *Se* K *è un campo algebricamente chiuso di caratteristica* p *qualsiasi, ed i polinomi* $f_1(X),...,f_m(X) \in K[X]$ (*al solito* $(X) = (x_1,...,x_n)$) *sono semplici ed a due a due primi fra di loro, allora i polinomi* $y_1^r - f_1(X),...,y_m^r - f_m(X)$ *generano un ideale primo* P_m *nell'anello* $R_m = K[X, y_1,...,y_m]$ *per qualunque valore*

dell'esponente r *naturale positivo purché non divisibile per* p.

La dimostrazione della Proposizione 3 richiede qualche dettaglio tecnico. Innanzi tutto, essa è vera nel caso m=1, risultando allora una conseguenza del

LEMMA 4. *Se* F *è un campo qualsiasi contenente le radici* r-me *dell'unità, ed* r *è primo con la caratteristica di* F, *allora il polinomio* y^r-a, *per ogni elemento* a ∈ F, *genera un ideale primo in* F[y] *se, e soltanto se, l'elemento* a *non è potenza* s-ma *in* F *per ogni intero* s>1 *divisore di* r,

(oltre che naturalmente del fatto che il polinomio $y_1^r-f_1(X)$ è attualmente primo in R_1 se e soltanto se lo è in $K(X)[y_1]$).

Il Lemma 4 è a sua volta una conseguenza di un ben noto teorema sulle estensioni cicliche di un campo (cfr. [6], p.214).

Ciò premesso, si procede poi per induzione rispetto ad m, considerando nel caso $m\geq 2$ la successione esatta $0\to P_m/P_{m-1}\to R_m/P_{m-1}\to R_m/P_m\to 0$, e provando che se P_{m-1} è primo in R_{m-1} allora il polinomio $y_m^r-f_m(X)$ genera un ideale primo nell'anello $P_m/P_{m-1} = R_{m-1}/P_{m-1}[y_m]$.

L'anello R_{m-1}/P_{m-1} risulterà un dominio di integrità, diciamolo A, e potremo usare ai nostri fini il Lemma 4 una volta che avremo osservato che il polinomio $y_m^r-f_m(X)$ genera un ideale primo in $A[y_m]$ se e soltanto se esso genera un ideale primo in $F[y_m]$, avendo indicato adesso con F il campo dei quozienti di A. Si tratta pertanto di provare che $f_m(X)$ non è potenza s-ma in F per ogni intero $s > 1$ divisore di r, ovvero di provare che $f_m(X)$ non è potenza s-ma in A per tali valori di s, e ciò in conseguenza del fatto che un elemento di A risulta nelle nostre ipotesi poten

za s-ma in F se e soltanto se lo è già in A, in quanto A risulta attualmente integralmente chiuso. Rimandiamo per un attimo la dimostrazione di questo fatto, e facciamo vedere subito come si possa ora ottenere la conclusione. Invero, ove fosse $f_m(X) \equiv g(X,y_1,\ldots,y_{m-1})^s \bmod P_{m-1}$ in R_{m-1}, allora il ciclo algebrico determinato in $GF(q)^{n+m-1}$ dalle equazioni $y_1^r - f_1(X) = \ldots = \ldots = y_{m-1}^r - f_{m-1}(X) = f_m(X) = 0$ risulterebbe singolare in ogni suo punto. D'altro canto, poiché i polinomi $f_1(X),\ldots,f_{m-1}(X),f_m(X)$ sono supposti semplici ed a due a due primi tra di loro, ecco che esisterà certamente in $\overline{GF(q)}^n$ un punto $(\bar{X})$ appartenente alla ipersuperficie di equazione $f_m(X) = 0$ che non sta su nessuna delle ipersuperficie di equazione $f_1(X) = 0,\ldots,f_{m-1}(X) = 0$, e che non è singolare per detta ipersuperficie. Se ne deduce allora l'esistenza di un punto $(\bar{X},\bar{y}_1,\ldots,\bar{y}_{m-1})$ in $\overline{GF(q)}^{n+m-1}$ il quale appartiene al ciclo in questione ma non è singolare per esso, in quanto il rango della matrice jacobiana

$$\begin{pmatrix} -\frac{\partial f_1}{\partial x_1} & \ldots\ldots & -\frac{\partial f_1}{\partial x_n} & r\,y_1^{r-1} & 0 & \ldots\ldots & 0 \\ \ldots\ldots\ldots & & & \ldots\ldots\ldots & & & \\ -\frac{\partial f_{m-1}}{\partial x_1} & \ldots & -\frac{\partial f_{m-1}}{\partial x_n} & 0 & 0 & \ldots & r\,y_{m-1}^{r-1} \\ \frac{\partial f_m}{\partial x_1} & \ldots\ldots & \frac{\partial f_m}{\partial x_n} & 0 & 0 & \ldots & 0 \end{pmatrix}$$

è manifestamente uguale a m in questo punto.

Resta soltanto da dimostrare che A è invero integralmente chiuso. Ciò discende sostanzialmente dal criterio di normalità

di Serre ([5], p.185), tenuto conto dei seguenti due fatti:

(I) A è un dominio di Cohen-Macaulay, in quanto quoziente di un anello di polinomi in n+m-1 variabili modulo un ideale primo n-dimensionale generato esattamente da (n+m-1)-n=m-1 elementi;

(II) per ogni ideale primo minimale $P \subset A$ la localizzazione A_P risulta un dominio regolare, in quanto la varietà di $\overline{GF(q)}^{n+m-1}$ individuata da P_{m-1} è palesemente non singolare in codimensione 1.

§2. Veniamo adesso alla seconda dimostrazione della Proposizione B che utilizza l'idea di Davenport precedentemente citata, evitando così la dimostrazione di irriducibilità di cui alla Proposizione 1.

Si consideri il carattere χ del gruppo $GF(q)^*$ ottenuto componendo la proiezione canonica $GF(q)^* \to GF(q)^*/H$ con un qualsiasi monomorfismo che immerga questo gruppo quoziente in $\mathbb{C}^*$. L'immagine di χ consiste allora dell'insieme delle radici r-me dell'unità complesse, che indicheremo con $\varepsilon_0 = 1, \ldots, \varepsilon_{r-1}$ e naturalmente la condizione $f_i(\bar{X}) \in H$ corrisponde alla $\chi(f_i(\bar{X}))=1$, fermo restando il significato dei simboli fin qui impiegati. Converremo poi di estendere χ a tutto $GF(q)$ ponendo $\chi(0) = 0$. Ciò premesso, associamo ad ogni elemento $(\bar{X}) \in GF(q)^n$ il numero intero

$$\varphi(\bar{X}) = \prod_{j=1}^{r-1} \prod_{i=1}^{m} (-\varepsilon_j + \chi(f_i(\bar{X}))) = \prod_{i=1}^{m} (\chi(f_i(\bar{X})^{r-1} + \ldots + 1).$$

Si vede subito infatti che $\varphi(\bar{X})$ assume esclusivamente i valori r^t, per qualche intero t compreso tra 1 ed m, oppure 0, la prima

circostanza verificandosi quando sia $\chi(f_i(\bar{X}))=1$ per esattamente t valori dell'indice i, mentre $f_i(\bar{X}) = 0$ per tutti i valori rimanenti, e la seconda verificandosi nel caso contrario, vale a dire quando esiste almeno un indice i tale che $\chi(f_i(\bar{X}))$ è diverso da 0 o da 1. In particolare, risulterà $\varphi(\bar{X}) = r^m$ se, e soltanto se, $(\bar{X})$ è una delle soluzioni in $GF(q)^n$ del sistema di congruenze assegnato.

Indicato adesso con N il numero di queste soluzioni, è immediato verificare che

$$(4) \qquad N = \frac{1}{r^m} \sum_{(\bar{X})\in GF(q)^n} \varphi(\bar{X}) \frac{1}{r^m} \sum_{(\bar{X})\in Z} \varphi(\bar{X}) \quad ,$$

ove con Z si indichi ora il luogo dei punti di $GF(q)^n$ che annullano qualcuno dei polinomi $f_i(X)$, $i=1,\ldots,m$, ovvero, il luogo dei punti razionali sopra GF(q) dell'ipersuperficie di $\overline{GF(q)}^n$ di equazione $f = f_1 \ldots f_m = 0$.

Studiamo separatamente i due addendi che compaiono nella (4). Il termine di destra si può maggiorare intanto, per quanto detto, con $\frac{1}{r^m} r^{m-1}|Z|$, e $|Z|$ a sua volta, ripetendo sostanzialmente l'argomentazione già riportata nel paragrafo precedente a proposito della dimostrazione della (3), con una quantità del tipo $c_1(q^{n-1}-c_2q^{n-3/2})$ ove le costanti c_1, c_2 che qui appaiono hanno il significato ormai consueto, sicché si può dire in definitiva che risulti

$$(5) \qquad \frac{1}{r^m} \sum_{(\bar{X})\in Z} \varphi(\bar{X}) \leq \frac{1}{r} c_1(q^{n-1}-c_2q^{n-3/2}).$$

Per quanto riguarda invece il primo termine, notiamo che $\varphi(\bar{X})$ può anche scriversi come $\varphi(\bar{X}) = 1 + \sum_F \chi(F(\bar{X}))$, ove F vari nell'insieme di tutti i polinomi di grado positivo ottenuti componendo fra di loro i fattori $f_i(X)$ ciascuno elevato ad una potenza h_i compresa fra 0 ed (r-1). Tali polinomi F sono pertanto in numero di r^m-1, e si ha allora che

$$(6)\quad \frac{1}{r^m}(\bar{X})\sum_{\epsilon GF(q)^n}\varphi(\bar{X}) = \frac{q^n}{r^m}+\frac{1}{r^m}\,(\bar{X})\sum_{\epsilon GF(q)^n}(\sum_F \chi(F(\bar{X})) =$$

$$= \frac{q^n}{r^m} + \frac{1}{r^m}\sum_F\Big((\bar{X})\sum_{\epsilon GF(q)^n}\chi(F(\bar{X}))\Big)\ .$$

Proviamo adesso che ciascuno dei termini $(\bar{X})\sum_{\epsilon GF(q)^n}\chi(F(\bar{X}))$ per ogni fissato polinomio F può essere maggiorato in modulo con

$$(7)\qquad \Big|(\bar{X})\sum_{\epsilon GF(q)^n}\chi(F(\bar{X}))\Big| \leq c\ q^{n-3/2}\ ,$$

essendo qui c una costante del solito tipo.

Infatti, senza perdere in generalità, possiamo supporre che sia $F(X)=f_1(X)^{h_1}\ldots f_m(X)^{h_m}$ con $0 < h_i \leq r-1$, $i=1,\ldots,m$, e che inoltre risulti $d = MCD(h_1,\ldots,h_m) = 1$ (nel caso $d > 1$ risulterebbe $(\bar{X})\sum_{\epsilon GF(q)^n}\chi(F(\bar{X})) = (\bar{X})\sum_{\epsilon GF(q)^n}\chi^d(f_1(\bar{X})^{h_1/d}\ldots f_m(\bar{X})^{h_m/d})$ e χ^d, essendo $d \leq r-1$, risulterebbe ancora un carattere non banale di $GF(q)^*$ per il quale potrebbe ripetersi il ragionamento, tenuto conto naturalmente del suo cambiamento di specie). Si ha allora $(\bar{X})\sum_{\epsilon GF(q)^n}\chi(F(\bar{X})) = \sum_{i=0}^{r-1}\epsilon_i N_i$, ove N_i designi il numero dei punti

$(\bar{X}) \in GF(q)^n$ tali che $\chi(F(\bar{X})) = \varepsilon_i$. Questo numero N_i risulta legato a quello ν_i dei punti razionali sopra GF(q) dell'ipersuperficie di $\overline{GF(q)}^{n+1}$ di equazione $u_i y^r = F(X)$ - avendo fissato in GF(q)* un qualunque elemento u_i tale che $\chi(u_i) = \varepsilon_i$ - per il tramite dell'identità

$$\nu_i = r\, N_i + \delta \quad , \tag{8}$$

avendo indicato con δ il numero dei punti $(\bar{X})$ in $GF(q)^n$ tali che $F(\bar{X}) = 0$.

Se ne deduce allora che

$$\left|\sum_{(\bar{X})\in GF(q)^n} \chi(F(\bar{X}))\right| = \frac{1}{r}\left|\sum_{i=0}^{r-1} r\, N_i \varepsilon_i\right| = \frac{1}{r}\left|\sum_{i=0}^{r-1} \varepsilon_i (r\, N_i - q^n + \delta)\right| =$$

$$= \frac{1}{r}\left|\sum_{i=0}^{r-1} \varepsilon_i (\nu_i - q^n)\right| \leq \frac{1}{r} \sum_{i=0}^{r-1} |\nu_i - q^n| \leq \frac{1}{r}\, r\, c\, q^{(n-1)-1/2},$$

avendo tenuto conto della Proposizione 2 e del fatto che nelle ipotesi attuali ciascuna delle ipersuperficie $u_i y^r = F(X)$ definite sopra GF(q) è assolutamente irriducibile (si tratta del caso m=1 della Proposizione 3), oltre che naturalmente del fatto che $\sum_{i=0}^{r-1} \varepsilon_i = 0$.

Combinando infine la (5) con le (7) si ottiene che

$$N = \frac{q^n}{r^m} + \frac{1}{r^m} \sum_{F} \Big(\sum_{(\bar{X})\in GF(q)^n} \chi(F(\bar{X})) \Big) - \frac{1}{r^m} \sum_{(\bar{X})\in Z} \varphi(\bar{X}) \geq$$

$$\geq \frac{q^n}{r^m} - \frac{1}{r^m} \sum_{F} \left| \sum_{(\bar{X})\in GF(q)^n} \chi(F(\bar{X})) \right| - \frac{1}{r^m} \sum_{(\bar{X})\in Z} \varphi(\bar{X}) \geq$$

$$\geq \frac{q^n}{r^m} - \frac{1}{r^m}(r^m - 1)c\, q^{n-3/2} - \frac{c_1}{r}(q^{n-1} - c_2 q^{n-3/2})$$

dalla quale discende immediatamente la conclusione desiderata al divergere di q.

ACKNOWLEDGMENT

L'autrice ringrazia vivamente il **Dott. Lucio Guerra** per gli utili suggerimenti ricevuti durante la compilazione del presente lavoro.

BIBLIOGRAFIA

[1] U.BARTOCCI: k-insiemi densi in piani di Galois, *Boll.U.M.I., Algebra e Geometria,* (6), 2(1983), 71-77.

[2] H.DAVENPORT: On the distribution of quadratic residues mod p, *J.London Math. Soc.* 6(1931), 49-54.

[3] L.GUERRA-E.UGHI: On the distribution of Legendre symbols in Galois fields, *Discrete Mathematics* 42(1982), 197-208.

[4] L.GUERRA-E.UGHI: On a conjecture of S. Ilkka, *Ann. of Discrete Math.* 18(1983), 419-426.

[5] R.HARTSHORNE, *Algebraic Geometry,* Springer-Verlag, 1977.

[6] S.LANG: *Algebra,* Addison-Wesley, 1965.

[7] W.M.SCHMIDT: Equations over Finite Fields, *Lecture Notes in Math.* 536 Springer-Verlag, 1976.

[8] E.UGHI: Saturated configurations in Galois spaces(in corso di pubblicazione).

[9] E.UGHI, (k,n)-blocking sets with relatively small n in projective Galois spaces(in corso di pubblicazione).

Ricevuto il 5/9/1985

Dipartimento di Matematica
Università degli Studi
P E R U G I A