H-ESTENSIONI, ELEVAZIONI DI QUASI-CORPI ED S-QUASI-ANELLI (*)

di GIORDANO GALLINA (a Parma) (**)

SOMMARIO.- *Si trattano problemi di esistenza e di numerazione nella classe degli S-quasi-anelli aventi un'unità sinistra. Si fa poi vedere che per ogni quasi-corpo di Dickson D esiste un S-quasi-anello locale R, intero e completamente primario, tale che* $R/J_2(R) \cong D$.

SUMMARY.- *We treat existence and numeration problems in the class of S-near-rings having a left identity. We show that, for every Dickson near-field D, there is a local integral completely primary S-near-ring R, such that* $R/J_2(R) \cong D$.

1. Introduzione.

Nel paragrafo 6 di [10], Maxson ha provato che, per ogni campo F, esistono almeno due quasi-anelli locali completamente primari non isomorfi, tali che il quoziente di ognuno di essi rispetto all'ideale massimale sia isomorfo ad F.

Si può porre più in generale il problema di costruire quasi-anelli con ideali notevoli, in modo che i quozienti siano strutture relativamente classiche, eventualmente con l'idea di poter proseguire studiando questi quasi-anelli come strutture analoghe a quelle già note. Per motivazioni più esplicite si veda ad esempio [9].

Ci occuperemo esplicitamente di S-quasi-anelli dotati di unità sinistra, ove, come in [4], un quasi-anello zero simmetrico R è un S-quasi-anello se, $\forall\, a \in R$, la relazione S_a, definita ponendo $xS_ay \Longleftrightarrow xa = ya$, è una congruenza.

Per p primo ed $m \in Z$, chiamiamo p_m-gruppo un p-gruppo abeliano di tipo $u = (m_1, \dots, m_k)$, dove $\forall\, r \in N$, il numero degli i, tali che $m_i = r$, è divisibile per m.

Si pongono naturalmente i seguenti problemi.

(*) Pervenuto in Redazione il 1° ottobre 1988.
Lavoro eseguito con il contributo del M.P.I.

(**) Indirizzo dell'Autore: Via Palermo, 2 - 43100 Parma (Italy).

Dato $v \geq 2$ ed assegnato un quasi-corpo di Dickson D, 1) vedere se esistano S-quasi-anelli non isomorfi con unità sinistra Q (e quanti ne esistano), tali che $J(Q)^v = \{0\}$, $J(Q)^{v-1} \neq \{0\}$, $Q/J(Q) \cong D$, [1] 2) vedere se esista un S-quasi-anello intero locale completamente primario, il cui quoziente rispetto all'ideale massimale sia isomorfo a D, 3) se $|D| = p^m$, dire se un p_m-gruppo sia il gruppo additivo di un S-quasi-anello locale, il cui quoziente rispetto al radicale nil sia isomorfo a D.

Con l'occasione, sfruttando il concetto di H-estensione qui introdotto, si completa la numerazione degli S-quasi-anelli direttamente irriducibili con unità sinistra, due a due non isomorfi, a gruppo additivo ciclico. Circa il problema 2), dimostriamo che, per ogni quasi-corpo di Dickson D, esiste un S-quasi-anello intero R, con un unico ideale proprio I, tale che $R/I \cong D$. Riguardo al problema 3), proviamo che se $|D| = p^m$, per ogni $n \in N$, un p_m-gruppo di tipo $(n, ..., n)$ oppure di tipo $(n + 1, ..., n + 1, n, ..., n)$ è sostegno di un S-quasi-anello locale R tale che $R/J(R) \cong D$.

2. Premesse.

Una funzione ϕ, da un anello al suo endomorfo, viene detta funzione di accoppiamento per R, se:

(i) $\phi(0) = 0_R$,
(ii) $\forall a,b \in R, \phi(a) \circ \phi(b) = \phi(a.b^{\phi(a)})$.

Se ϕ è una funzione di accoppiamento per R, allora $[R; +, \circ]$ è un quasi-anello, che diciamo di Dickson, accoppiato ad $[R; +, .]$ mediante ϕ.

Si noti che ϕ è un omomorfismo di semigruppi $[R, \circ] \to \mathrm{End}\, R$. Per a appartenente ad un quasi-anello R:

1) indichiamo con φ_a la funzione da R a R definita da φ_a:

$$x \to ax;$$

2) poniamo $A_s(a) = \{x \in R \mid xa = 0\}$.

Un R-gruppo Γ, sarà detto regolare se, per ogni unità sinistra ε di R e per ogni $\gamma \in \Gamma$, $\varepsilon\gamma = \gamma$.

(1) Con $J(Q)$ indichiamo il radicale nil di Q.

Sia N un quasi-anello fortemente monogeno, costruito, mediante il Teorema 10 di [2], a partire da un gruppo additivo, da un suo gruppo di automorfismi, e da un insieme X (di unità sinistre). Diremo che A è il gruppo di automorfismi corrispondente ad N.

OSSERVAZIONE 1. *Un quasi-anello zero-simmetrico intero R è un S-quasi- anello se e solo se ogni suo elemento non nullo è cancellabile a destra.*

Sia R un S-quasi-anello intero. Se in R $x_1b = x_2b$, allora $(x_1 - x_2)b = 0$, perché R è un S-quasi-anello. Per $b \neq 0$, essendo R intero, è $x_1 - x_2 = 0$, da cui $x_1 = x_2$.

Viceversa, se ogni elemento non nullo è cancellabile a destra, per $b \in R$, $A_s(b)$ è un ideale (banale) di R, e le classi della S_b sono i suoi laterali. Allora, per il Teorema 1 di [3], R è un S-quasi-anello. ◇

Il seguente asserto è di dimostrazione immediata.

LEMMA 2. *Siano G_1, G_2 due gruppi (additivi), A un gruppo di automorfismi di G_1, h un omomorfismo di A in Aut (G_2). Allora $C = \{<r, h(r)> \mid r \in A\}$ è un gruppo di automorfismi di $G = G_1 \oplus G_2$, e, se T è una traiettoria principale di A, allora $T \times G_2$ è un'unione di traiettorie principali di C.*

Fissato una volta per tutte un m $\in N$, poniamo, per brevità, $Z_n = (Z_{p^n}^+)^m$, e poniamo $H_i = p^{n-i}Z_n (i = 0, ..., n)$.

LEMMA 3. *Se A è un gruppo di automorfismi di H_1, di ordine primo con p, H_n ha un gruppo di automorfismi A', il quale:*
1) *coincide con A sopra H_1,*
2) *è simile ad A sopra ogni quoziente H_i/H_{i-1} $(i = 1, ..., n)$.*

La dimostrazione è del tutto analoga a quella dell'Oss. 6 di [4](2). ◇

3. H-estensioni.

Siano N un quasi-anello, Γ un N-gruppo, G un prodotto semidiretto di Γ^+ mediante N^+, rispetto ad un omomorfismo Θ: $N^+ \to$ Aut Γ^+. Sia $\cdot$ l'operazione sopra G definita da:

---

(2) Per una formulazione più generale del problema a cui è connesso l'asserto, si veda [1].

$$<a,b> \cdot <a',b'> = <ba',bb'>.$$

TEOREMA 4. *La struttura* $[G; +, .]$ *è un quasi-anello se e solo se, per ogni* $a \in \Gamma$ *e per ogni* $b, b' \in N$, *risulta*

$$b\Theta_{b'}(a) = \Theta_{bb'}(ba). \tag{1}$$

Il prodotto è banalmente associativo.

Assegnati tre generici elementi $<a,b>$, $<a',b'>$, $<a'',b''>$ di G, calcoliamo $<a, b> \cdot (<a',b'> + <a'',b''>) =$
$= <a,b> \cdot <a' + \Theta_{b'}(a''), b' + b''> =$
$= <b(a' + \Theta_{b'}(a'')), b(b' + b'')>.$

Poichè Γ è un N-gruppo, l'ultima espressione è uguale a

$$<ba' + b\Theta_{b'}(a''), bb' + bb''>. \tag{2}$$

D'altra parte:

$$<a,b> \cdot <a',b'> + <a,b> \cdot <a'',b''> =$$

$$= <ba',bb'> + <ba'',bb''> = <ba' + \Theta_{bb'}(ba''), bb' + bb''>.$$

Tale coppia ordinata è uguale alla (2) se e solo se $b\Theta_{b'}(a'') = \Theta_{bb'}(ba'')$. ◇

Allorquando la (2) è soddisfatta, il quasi-anello G sarà chiamato prodotto semidiretto dell'N-gruppo Γ e del quasi-anello N, rispetto all'omomorfismo Θ.

OSSERVAZIONE 5. *Un quasi-anello G è prodotto semidiretto di un N-gruppo* Γ *e di un quasi-anello N se e solo se:*
1) *N è un sotto quasi-anello,*
2) N^+ *è un sottogruppo normale di* G^+,
3) $\Gamma^+ \cap N^+ = \{0\}$,
4) $\forall\, a \in \Gamma, \forall\, b \in N \;\; \varphi_{a+b} = \varphi_b$.

OSSERVAZIONE 6. *Sia* G^+ *un prodotto semidiretto di* Γ^+ *e di* N^+, *rispetto a* Θ. *Se* $Im\,\Theta \subseteq \mathrm{Aut}_N(\Gamma)$, *e se,* $\forall b \in N \backslash A_s(\Gamma)$ $\forall b' \in N$, $\Theta_{bb'} = \Theta_{b'}$, *allora (1) è verificata.*

Siano b, $b' \in N$, $a \in \Gamma$. Se $b \in A_s(\Gamma)$, allora $ba = 0$, da cui $\Theta_{bb'}(ba) = 0$. D'altra parte, ovviamente, $b\Theta_{b'}(a) = 0$.
In tale caso, la (1) dunque sussiste.

Sia $b \notin A_s(\Gamma)$. Siccome $\Theta_b \in \mathrm{Aut}_N(\Gamma)$, risulta $b\Theta_{b'}(a) = \Theta_{b'}(ba)$.

Poichè $\Theta_{bb'} = \Theta_{b'}$, deve essere $\Theta_{bb'}(ba) = \Theta_{b'}(ba)$. In ogni caso vale quindi la (1). ◇

Consideriamo il caso particolare in cui: 1) G^+ sia prodotto diretto di Γ^+ e di N^+; 2) N sia fortemente monogeno generalizzato nel senso di [5]; 3) Γ sia un N- gruppo regolare tale che $b\Gamma = 0$, per ogni b nilpotente di N.

In tale caso, il quasi-anello G sarà detto un'H-estensione di N.

Sia N fortemente monogeno generalizzato. Se poniamo $bN = 0$, per ogni nilpotente b di N, otteniamo un quasi-anello fortemente monogeno, che chiamiamo associato ad N.

Risulta subito che, per determinare le H-estensioni di N, è sufficiente trovare tutti gli N'-gruppi regolari, essendo N' il quasi-anello fortemente monogeno associato ad N.

OSSERVAZIONE 7. *Se N è fortemente monogeno, tutti e soli gli N-gruppi regolari sono i gruppi additivi Γ per i quali: 1) esiste un omomorfismo $h: A \to \mathrm{Aut}\Gamma$, dove A è il gruppo di automorfismi corrispondente ad N, 2) per $n \in N \backslash A_s(N)$, $\gamma \in \Gamma$, si ha $n\gamma = h(a)(\gamma)$, dove a è l'unico elemento di A che manda un'unità sinistra di N in n, mentre $n\gamma = 0$, se $n \in A_s(N)$.*

Se N è fortemente monogeno, e Γ è un N-gruppo regolare, allora una H-estensione G di Γ mediante N è un quasi-anello fortemente monogeno. Infatti, se A è il gruppo di automorfismi corrispondente ad N, h l'omomorfismo $A \to \mathrm{Aut}\,\Gamma$ di cui all'Oss. 7, la data H- estensione di Γ mediante N è il quasi-anello fortemente monogeno in cui il gruppo additivo è $\Gamma^+ \oplus N^+$, il gruppo di automorfismi corrispondente è $C = \{<r, h(r)> \mid r \in A\}$, e l'insieme delle unità sinistre è $\Gamma \times X$, essendo X l'insieme delle unità sinistre di N.

Così, un'H-estensione G di un quasi-anello N, fatta mediante un suo N-gruppo Γ, è a sua volta un quasi-anello fortemente monogeno generalizzato nel senso di [5].

Al fine di mostrare questo, riprendiamo brevemente la costruzione introdotta nel paragrafo 2 di [5].

Supponiamo che un gruppo additivo N^+ *abbia un endomorfismo nilpotente f, permutabile con tutti gli elementi di un gruppo di automorfismi*

A di N^+. Sia n il minimo intero, tale che $f^n = 0$. Poniamo $f^0 = id_{N^+}$. Chiamiamo A_i la restrizione di A ad $f^i(N^+)$.

Supponiamo che:

1) A_i abbia un insieme non vuoto T_i di traiettorie principali contenute in $f^i(N^+)\backslash f^{i+1}(N^+)$ $(i = 0, ..., n-1)$.

2) f mandi traiettorie di T_i in traiettorie di T_{i+1}, ed inoltre, posto $\mathcal{T}_i = \bigcup_{t_i \in T_i} t_i$, sia $f^{-1}(\mathcal{T}_{i+1}) = \mathcal{T}_i$.

Sia X un *insieme di rappresentanti* delle traiettorie di T_0, tale che, per $i = 0, 1, ..., n-1$, ogni traiettoria di T_i contenga uno ed un solo elemento di $f^i(X)$ (per le nostre ipotesi, un tale X esiste). Il Teorema 1 di [5] indica come, a partire da A, da f, e dall'insieme X, è possibile trarre un particolare quasi-anello fortemente monogeno generalizzato N (sopra N^+).

Sia ora Γ un N-gruppo, e sia G un'H- estensione di N mediante Γ. Sappiamo che Γ è un N'-gruppo regolare, dove N' è il quasi-anello fortemente monogeno associato ad N. Il gruppo di automorfismi (di N'^+) corrispondente ad N' è il gruppo A. Indichiamo con h l'omomorfismo $A \to \mathrm{Aut}\,\Gamma^+$ corrispondente alla struttura di N'-gruppo Γ (Oss. 7).

Siano ora: 1) C il gruppo di automorfismi di $\Gamma^+ \oplus N^+$ uguale a $\{<r, h(r)> \mid r \in A\}$; 2) g l'endomorfismo di $\Gamma^+ \oplus N^+$ definito da $g: <x, y> \to <0, f(y)>$.

In base al Lemma 2, possiamo utilizzare la costruzione del paragrafo 2 di [5], partendo da C, da g, e dall'insieme $\Gamma \times X$, determinando in questo modo un quasi-anello sopra G^+, che si vede subito coincidere con l'H-estensione G preliminarmente considerata.

Per tale motivo, chiameremo G la H-estensione di N, fatta mediante Γ, rispetto all'omomorfismo $h: A \to \mathrm{Aut}\Gamma^+$, e la indicheremo con $\Gamma H_h N$.

4. Esempi.

Sia G_1 un gruppo (additivo) ciclico di ordine p^3 (p primo dispari), A il gruppo di automorfismi di ordine p di G_1. E' noto che ogni traiettoria principale di A è contenuta in uno ed un solo laterale di pG_1.

Sia X un insieme di rappresentanti delle traiettorie principali di A, e sia G_1^0 il quasi-anello fortemente monogeno sopra G_1, costruito partendo da A e da X. Consideriamo G_1, come un G_1^0-gruppo (nel modo naturale), e consideriamo il gruppo V, somma semidiretta di G_1 e di se stesso, rispetto ad un omomorfismo Θ, la cui immagine abbia ordine p.

Se $b \notin A_s(G_1)$, si vede subito che, $\forall b' \in G_1$, bb' e b' appartengono ad uno stesso laterale di Ker Θ. Quindi, $\Theta_{bb'} = \Theta_{b'}$. Inoltre, essendo End$G_1$ un anello commutativo, ImΘ è contenuta nell'automorfo del G_1^o-gruppo G_1. Le condizioni dell'Oss. 6 sono quindi soddisfatte.

Dunque, considerato il prodotto sopra V definito da: $<a,b> \cdot <a',b'> = <ba',bb'>$, la struttura $[V; +, .]$ è un quasi-anello.(3)

Per p primo dispari, l'anello $N = Z_{p^3}$ può essere ovviamente considerato come un quasi-anello fortemente monogeno generalizzato, nel quale il quasi-anello fortemente monogeno N' associato ha l'annullatore sinistro coincidente con pN, mentre il gruppo di automorfismi A, corrispondente ad N', è di ordine $(p-1)p^2$.

Sia h un omomorfismo $A \to$ Aut G_1, la cui immagine abbia ordine $p-1$.

Gli elementi N, G_1 ed h determinano un'H- estensione NH_hG_1.

5. S-quasi-anelli infiniti.

Indichiamo con $[K, +, .]$ un campo, con $D = [K; +, \circ]$ un quasi-corpo di Dickson, accoppiato a K, e con ϕ la relativa funzione di accoppiamento. Sia D^* il semigruppo $[D \backslash \{0\}; \circ]$. Poniamo $M^+ = \bigoplus_{i=1}^{m} K^+$.

Sia s l'endomorfismo (di scorrimento) di M^+ definito da: $s : <x_1, \dots, x_m> \to <0, x_1, \dots, x_{m-1}>$.

Per ogni $a \in K$ e per ogni $b = <x_1, \dots, x_m> \in M^+$, poniamo $a \circ b = <a \circ x_1, \dots, a \circ x_m>$, $a \cdot b = <a \cdot x_1, \dots, a \cdot x_m>$.

Sia $P(s)$ l'insieme delle funzioni $M^+ \to M^+$ del tipo $h' : b \to \sum_{i=0}^{m-1} a_i \cdot s^i(b)$ $(a_i \in K, a_0 = 1)$. Ogni elemento di $P(s)$ è un endomorfismo di M^+.

Dimostriamo che $P(s)$ è chiuso rispetto alla composizione. Sia $h'' \in P(s)$, $h'' : b \to \sum_{j=0}^{m-1} a''_j \cdot s^j(b)$.

Risulta $(h' \circ h'')(b) = h' \left(\sum_{j=0}^{m-1} a''_j \cdot s^j(b) \right) =$

$$= \sum_{k=0}^{m-1} \Big(\sum_{\substack{i,j \geq 0 \\ i+j=k}} a'_i a''_j \Big) s^k(b) .$$

Si riconosce subito dunque che $h' \circ h'' = h'' \circ h' \in P(s)$.

---

(3) Il quale risulta quindi prodotto semidiretto del G_1^o-gruppo G_1 e di G_1^o.

Dai calcoli precedenti, risulta che condizione necessaria e sufficiente affinché $h' \circ h'' = \mathrm{id}$ è che $\sum_{i+j=k} a'_i a''_j = 0$, $k = 1, \ldots, m-1$.

Fissate le a', si possono considerare le formule precedenti come un sistema nelle a''. Siccome $a'_1 + a''_1 = 0$, a''_1 deve essere uguale a $-a'_1$. Supponiamo che i valori di a''_1, a''_2, ..., a''_{m-2} esistano e siano unici. Dalla relazione $a'_{m-1} + a'_{m-2} a''_1 + \ldots + a'_1 a''_{m-2} + a''_{m-1} = 0$, si trae che a''_{m-1} esiste ed è unico. Il predetto sistema ammette dunque una ed una sola soluzione. Quindi, h' è invertibile, ed $h'^{-1} \in P(s)$. Dunque, $P(s)$ è un gruppo di automorfismi di M^+.

Indichiamo con L l'insieme delle corrispondenze $M^+ \to M^+$ del tipo $l_a : b \to a \circ b$, per $a \in D^*$. E' immediato, dall'associatività dei quasi-corpi di Dickson, che L forma un gruppo di automorfismi rispetto alla composizione.

Sia E il gruppo generato da L e da $P(s)$. Sia $\bar{x}_1 \in D^*$, e si ponga $u = <\bar{x}_1, 0, \ldots, 0>$. Utilizziamo la costruzione di [5] già ricordata, partendo da E, da s, e da u, come ovviamente lecito. Come risulta in [7] (Teor. 28), otteniamo così, per ogni m, un S-quasi-anello locale sottodirettamente irriducibile Q_m, sopra M^+, tale che, per $m \geq 3$, $Q_m/J(Q_m) \cong D$, $J(Q_m)^{m-1} = 0$, $J(Q_m)^{m-2} \neq 0$.

Possiamo ora enunciare il

TEOREMA 8. *Per ogni $v \geq 2$ e per ogni quasi-corpo di Dickson D, esistono infiniti S-quasi-anelli Q^0, aventi unità sinistra, direttamente irriducibili, soddisfacenti ad entrambe le condizioni catenarie sugli annullatori, sia sinistri che destri, e tali che: 1) $Q^0/J(Q^0) \cong D$, 2) $J(Q^0)^{v-1} \neq \{0\}$, 3) $J(Q^0)^v = \{0\}$.*

Consideriamo il gruppo L di automorfismi di M (per $m \geq 3$). Sia I un insieme non vuoto, e consideriamo il gruppo additivo $B_I^+ = \prod_{i \in I} D^+$. Per ogni $a \in D^*$, sia Ψ_a l'automorfismo di B_I^+ definito da: $\Psi_a (<y_i>_{i \in I}) = <a \circ y_i>_{i \in I}$.

Sia h il monomorfismo di A [4] in Aut (B_I^+), definito da $h(l_a) = \Psi_a$.

Si ponga $Q^0 = Q_m H_h B_I^+$. Tale Q^0 è un S-quasi-anello con unità sinistra, in cui $J(Q^0)$, che coincide con $B_I \times J(Q_m)$, è tale che $J(Q^0)^{m-1} = 0$, $J(Q^0)^{m-2} \neq 0$, $Q^0/J(Q^0) \cong D$.

Se facciamo variare la cardinalità di I, otteniamo subito l'asserto. ◊

(4) Ricordiamo che A è il gruppo delle traslazioni sinistre non nulle del quasi-corpo D.

Indichiamo con $F[x]$ l'anello di polinomi sopra F. Sia a il coefficiente del termine non nullo di grado più basso di $f \in F[x]$.

Poniamo $\phi'(f) : b_0 + \ldots + b_m x^m \to b_0^{\phi(a)} + \ldots + b_m^{\phi(a)} x^m$.

Si verifica facilmente che la corrispondenza $\phi' : F[x] \to \mathrm{End}\, F[x]$, $\phi' : f \to \phi'(f)$ è una funzione di accoppiamento per $F[x]$. Sia $R = [F[x]; +, \circ]$ il quasi-anello di Dickson accoppiato a $F[x]$ mediante ϕ'.

TEOREMA 9. *Esiste un S-quasi-anello locale, sottodirettamente irriducibile, intero e completamente primario, il cui quoziente rispetto all'(unico) ideale massimale è isomorfo a D, qualunque sia il quasi-corpo di Dickson D.*

Riprendiamo la costruzione precedente l'enunciato, e proviamo che ogni elemento non nullo g di R è cancellabile a destra. Per $f_1, f_2 \in R$, sia $f_1 \circ g = f_2 \circ g$. Siano a_1, a_2, b i coefficienti dei termini non nulli di grado più basso, rispettivamente di f_1, di f_2 e di g. Si ha allora, in D, $a_1 \circ b = a_2 \circ b$. Poiché D è un quasi-corpo, è $a_1 = a_2$. Immediatamente si vede che $\phi'(f_1) = \phi'(f_2)$. Di qui, $f_1 g^{\phi'(f_1)} = f_2 g^{\phi'(f_1)}$; quindi $f_1 = f_2$. Per l'Oss. 1, R è un S-quasi-anello.

L'insieme U degli elementi di R a termine noto non nullo, costituisce un sistema moltiplicativo, e R verifica la condizione sinistra di Ore rispetto ad U (cfr. [12], pag. 26). Esiste allora il quasi-anello R_U, dei quozienti sinistri di R rispetto ad U, che è un S-quasi-anello intero, locale, sottodirettamente irriducibile, il cui ideale massimale è l'ideale I generato da $\{x\}$. E' inoltre $R_U/I \cong D$. Ne segue l'asserto. ◇

Si noti che se $\alpha \notin \{0, 1\}$ appartiene al centro di D, e se $\alpha^{\phi(a)} = \alpha$, per ogni $a \in D^*$ (5), allora la funzione $T : R \to R$, $T : b_0 + b_1 x + \ldots + b_m x^m \to b_0 + b_1 \alpha x + \ldots + b_m \alpha^m x^m$ è un automorfismo di R.

Per ogni $g(x) \in F[x]$, indichiamo con $\delta(g(x))$ il grado di $g(x)$; poniamo inoltre $T^{-\infty} = 0_R$.

Si consideri la corrispondenza $\phi'' : F[x] \to \mathrm{End}\, F[x]$, definita dalla $\phi'' : g \to \phi'(g) \circ T^{\delta(g)}$.

Si verifica facilmente che ϕ'' è una funzione di accoppiamento per $F[x]$. Si consideri il quasi-anello $R' = [F[x]; +, \circ']$ accoppiato a $F[x]$ mediante ϕ''.

(5) Se D è uno qualunque dei quasi-corpi di Dickson ritenuti noti in [12], un tale α esiste. La cosa è evidente nei seguenti casi: 1) D è finito, 2) D è di caratteristica zero, 3) D è di caratteristica dispari. Rimane da considerare il quasi-corpo dell'esempio 8.29 di pag. 255 di [12], nel quale si ponga $|F| = 2$. In questo caso, un tale α è per esempio $\dfrac{x^4+x^2+1}{x^4+x^2}$.

OSSERVAZIONE 10. *Il quasi-anello R' è un S-quasi-anello intero, ha un solo ideale proprio I', ed R'/I' è isomorfo a D.*

Si verifica facilmente che R' è un S-quasi-anello intero. La dimostrazione del fatto che R' ha un solo ideale proprio I', tale che R'/I' è isomorfo a D, è del tutto analoga a quella del Teorema 8.6 di [1]. ◇

6. S-quasi-anelli finiti.

6-1. *S-quasi-anelli locali finiti di esponente non primo.*

Per il Teorema 7.4 di [10], un quasi-anello locale finito deve avere un p-gruppo come gruppo additivo.

Per il Teorema 4 di [4], se R è un S-quasi-anello finito direttamente irriducibile e con unità sinistra, tale che $|R/J(R)| = p^m$, allora: 1) se p è dispari, R^+ è abeliano, ed il suo p-sottogruppo di Sylow è un p_m-gruppo, 2) se R^+ è un 2-gruppo abeliano, allora R^+ è un 2_m- gruppo.

In questo sottoparagrafo, ci poniamo il problema di vedere quali p_m-gruppi siano gruppi additivi di S-quasi-anelli locali.

Ricordiamo che si è posto $H_i = p^{n-i}Z_n$ ($i = 0, \dots, n$, $Z_n = (Z_{p^n}^+)^m$).

Siano ora: 1) F un campo di gruppo additivo H_1 e di unità b_1, 2) D un quasi-corpo di Dickson, sopra H_1, accoppiato a F mediante una funzione di accoppiamento ϕ, 3) $V = \phi(F\backslash\{0\})$, 4) $<q = p^l, \alpha>$ la coppia di numeri di Dickson (6) relativa a D, 5) F' il sottocampo di ordine q di F, 6) f l'endomorfismo di Z_n $y \to py$.

Al fine di poter trattare i casi più generali possibili, è opportuno enunciare la

OSSERVAZIONE 11. *Z_n è sostegno di un anello commutativo locale $\overline{H}_n$, tale che $\overline{H}_n/J(\overline{H}_n) \cong F$.*

Sia A_1 il gruppo di automorfismi di H_1 costituito dalle φ_x non nulle di F.

Per il Lemma 3, esiste un gruppo di automorfismi A_n di Z_n, privo di coincidenze, il quale: 1) coincide con A_1 sopra H_1, 2) è simile ad A_1 sui quozienti H_i/H_{i-1}. Denotiamo con A_i la restrizione di A_n ad H_i.

---

(6) Una coppia ordinata $<q, n> \in N^2$ è detta coppia di numeri di Dickson se: a) q è una potenza di un numero primo, b) ogni fattore primo di n divide $q-1$, c) se $q \equiv 3 \pmod{n}$, allora 4 non divide n.

L'insieme U, costituito da b_1 e dalle sue controimmagini negli omomorfismi $f^i(i = 1, \ldots, n-1)$, è costituito da elementi appartenenti a traiettorie principali due a due distinte di A_n.

Le funzioni $H_2 \to H_2$ del tipo $z \to z + a \cdot (pz)$ $(a \in F)$, formano un gruppo di automorfismi B_2 di H_2. Il gruppo C_2, generato da B_2 e da A_2, è commutativo, ed ha come unica traiettoria principale $H_2 \backslash H_1$. E' dunque possibile utilizzare la costruzione del paragrafo 2 di [5], partendo da C_2, da f_2, e da un elemento $b_2 \in U \cap (H_2 \backslash H_1)$. Si determina un quasi-anello locale $\overline{H}_2$, tale che $\overline{H}_2/p\overline{H}_2 \cong F$. Siccome C_2 è abeliano, $\overline{H}_2$ è un anello commutativo.

Sia $b_3 \in U \cap (H_3 \backslash H_2)$, tale che $f(b_3) = b_2$. Al variare di a in $\overline{H}_2$, le funzioni $H_3 \to H_3$, del tipo $z \to z + a. (pz)$(7) formano un gruppo di automorfismi B_3 di H_3. Il gruppo C_3, generato da B_3 e da A_3, è commutativo, ed ha come unica traiettoria principale $H_3 \backslash H_2$. Sia $\overline{H}_3$ il quasi-anello fortemente monogeno generalizzato, definito, con riferimento al paragrafo 2 di [5], a partire da f_3, da C_3 e da b_3. Ora, $\overline{H}_3$ è un anello commutativo locale, tale che $\overline{H}_3/p\overline{H}_3 \cong F$. Se si prosegue in tale modo, si determina un anello commutativo locale $\overline{H}_n$, sopra Z_n, tale che $\overline{H}_n/p\overline{H}_n \cong F$. ◇

TEOREMA 12. *Il gruppo Z_n è un gruppo additivo di un S-quasi- anello locale R_n, tale che $R_n/J(R_n) \cong D$.*

Per il Lemma 3, esiste un gruppo di automorfismi V_n di Z_n, il quale: 1) coincide con V sopra H_1, 2) è simile a V sopra ogni quoziente H_i/H_{i-1}. Sia r il generatore di V_n, il quale manda $z \in F$ in z^q.

Per induzione sopra j, dimostriamo che esiste un elemento di $U \cap (H_j \backslash H_{j-1})$, tenuto fermo da V_n (per $j = 1, \ldots, n$). L'asserto è ovvio se $j = 1$. Supponiamo che esso sussista per $n-1$. Per l'ipotesi induttiva, esiste un $b \in U \cap (H_n \backslash H_{n-1})$, tale che $r([b]) = b + a$, essendo a un opportuno elemento di F. Poiché $r^\alpha(b) = b$, deve essere $Tr_{F/F'}(a) = 0$. Per il Teorema 2.25 di [8], esiste $d \in F$, tale che $a = d - d^q$. Di qui, $r(b + d) = b + a + d^q = b + d$. Quindi, $b + d \in U$ è tenuto fermo da V_n.

Nel seguito del paragrafo, indichiamo con c_n un elemento di $U \cap (H_n \backslash H_{n-1})$ tenuto fermo da V_n, e poniamo c_n uguale all'unità di $\overline{H}_n$.

Poniamo $L_n = [Z_n; +, .']$, il quasi-anello fortemente monogeno, dedotto dal gruppo di automorfismi A_n e dall'insieme U, mediante il Teorema 10 di [2].

Proviamo che r è un automorfismo di L_n.

---

(7) Dove $a \cdot (pz)$ è calcolato in $\overline{H}_2$

Siano $t_1, t_2 \in L_n \backslash \{0\}$, $t_2 \in H_i \backslash H_{i-1}$. Gli elementi $r(t_1 .' t_2)$ e $r(t_1) .' r(t_2)$ appartengono alla stessa traiettoria di $r(t_2)$, e sono mandati nello stesso elemento di H_i/H_{i-1} (dall'opportuna suriezione canonica). Questo basta per poter dire che coincidono. Se v è un elemento della traiettoria T_n (di A_n) rappresentata da c_n, e se $z \in \overline{H}_n$, è $v.z = v.'z$.

Per induzione sopra j, dimostriamo ora che r è un automorfismo di ogni $\overline{H}_j$. L'asserto è ovvio per $j = 1$. Si supponga che sussista per $j = n - 1$.

Siano $y, y' \in H_n \backslash \overline{H}_{n-1}$. Esistono $u_1, u_2 \in T_n$, $a_1, a_2 \in \overline{H}_{n-1}$, tali che $y = u_1 + (pu_1) .a_1$, $y' = u_2 + (pu_2) .a_2$, essendo $(pu_1) .a_1$ e $(pu_2) .a_2$ calcolati in $\overline{H}_{n-1}$.

Siccome $r(c_n) = c_n$, $r(u_1)$ e $r(u_2)$ appartengono a T_n. Quindi:

$$r(y) \cdot r(y') = (r(u_1) + r(pu_1) \cdot r(a_1)) \cdot (r(u_2) + r(pu_2) \cdot r(a_2)) =$$
$$= r(u_1) .'r(u_2) + r(pu_1) \cdot r(pu_2) \cdot r(a_2) + r(pu_1) \cdot r(pu_2) \cdot r(a_1) +$$
$$+ r(pu_1) \cdot r(p^2u_2) \cdot r(a_2) \cdot r(a_1);$$
$$r(y \cdot y') = r(u_1 .' u_2 + (pu_1) \cdot (pu_2) \cdot a_2 + (pu_1) \cdot (pu_2) \cdot a_1 +$$
$$+ (pu_1) \cdot (p^2u_2) \cdot a_2 \cdot a_1) = r(u_1) .' r(u_2) + (pr(u_1)) \cdot (pr(u_2)) \cdot$$
$$\cdot r(a_2) + (pr(u_1)) \cdot (pr(u_2)) \cdot r(a_1) + (pr(u_1)) \cdot (p^2r(u_2)) \cdot r(a_2) \cdot r(a_1).$$

Questo è sufficiente per provare che r è un automorfismo di $\overline{H}_n$.

Sia $\psi^n : H_n \to \mathrm{End}\, \overline{H}_n$, definita nel modo seguente:

1) $\psi^n(0) = 0_{\overline{H}_n}$;

2) per $x \neq 0$, $x \in H_i \backslash H_{i-1}$, $\psi^n(x)$ è l'elemento di V_n tale che $\forall z \in F$, $z^{\psi^n(x)} = z^{\phi(p^{i-1}x)}$.

E' ormai ovvio che, per $x, x' \in \overline{H}_n$, se $x \cdot x'^{\psi^n(x)} \neq 0$, allora $\psi^n(x \cdot x'^{\psi^n(x)}) = \psi^n(x) \circ \psi^n(x')$. Quindi, l'operazione $\circ$ definita sopra H_n da: $z \circ z' = z \cdot z'^{\psi^n(z)}$ è associativa. La struttura $R_n = [H_n; +, \circ]$ è allora un quasi-anello che verifica l'asserto. ◇

TEOREMA 13. *Un p_m-gruppo di tipo (n, n, ... , n), oppure di tipo (n + 1, n + 1, ... , n + 1, n, ... , n), è gruppo additivo di un S-quasi-anello locale, il cui quoziente rispetto all'ideale massimale è isomorfo a D.*

Per $n \in N$ arbitrario, poniamo $M = \bigoplus_{i \in I_t} H_n$. Indichiamo con g l'endomorfismo di M definito da:

$$g: \langle x_1, \dots, x_t \rangle \to \langle x_t, x_1, \dots, x_{t-2}, px_{t-1} \rangle.$$

Sia $g^0 = \mathrm{id}$, e si noti che g è nilpotente di indice $k = nt$. Si ponga $c = \langle 0, 0, \dots, c_n \rangle$. Siano: 1) D l'estensione naturale del gruppo A_n ad M; 2)

E l'estensione naturale di V_n ad M; 3) r' un generatore di E; 4) D_{k-i} ed E_{k-i} le restrizioni di D e di E a $g^{k-i}(M)$ $(i = 1, \ldots, k)$.

Il sottogruppo $g^{k-1}(M)$ è sostegno di un campo F' (isomorfo ad F) di unità $g^{k-1}(c)$, nel quale, $\forall x \in g^{k-1}(M)$, $x \neq 0$, si abbia φ_x uguale alla restrizione di quell'elemento di D che manda $g^{k-1}(c)$ in x.

Ricorsivamente rispetto ad i, costruiamo, sopra ogni $g^{k-i}(M)$, un anello commutativo locale N_{k-i}, di unità $g^{k-i}(c)$, con radicale nil uguale a $g^{k-i+1}(M)$, campo residuo isomorfo ad F, e nel quale E_{k-i} è gruppo di automorfismi.

Per $i = 1$, poniamo $N_{k-1} = F'$.

Per $1 \leq i < k$, supponiamo che sia stato costruito, sopra $g^{k-i}(M)$, un anello commutativo locale del tipo da noi richiesto.

Ora, le funzioni $g^{k-i-1}(M) \to g^{k-i-1}(M)$ del tipo $z \to z + a \cdot g(z)$ (8) $(a \in g^{k-i}(M))$ formano un gruppo di automorfismi B_{k-i-1} (di $g^{k-i-1}(M)$). Il gruppo C_{k-i-1}, generato da B_{k-i-1} e da D_{k-i-1}, è commutativo, ed ha come unica traiettoria principale $g^{k-i-1}(M) \setminus g^{k-i}(M)$. E' dunque possibile utilizzare la costruzione del paragrafo 2 di [5], partendo da C_{k-i-1}, da g, e da $g^{k-i-1}(c)$. Si determina un anello commutativo locale N_{k-i-1}, sopra $g^{k-i-1}(M)$, di unità $g^{k-i-1}(c)$.

Per induzione rispetto ad i, si può provare che r' è un automorfismo di N_{k-i}. La cosa è ovvia per $i = 1$. Si supponga che sussista per $i = k - 1$.

Indichiamo con T la traiettoria di D rappresentata da c.

Esistono $u_1, u_2 \in T$, $a_1, a_2 \in N_1$, tali che $y = u_1 + g(u_1) \cdot a_1$, $y' = u_2 + g(u_2) \cdot a_2$, essendo $g(u_1) \cdot a_1$ e $g(u_2) \cdot a_2$ calcolati in N_1. Risulta:

$$r'(y) \cdot r'(y') = (r'(u_1) + r'(g(u_1)) \cdot r'(a_1)) \cdot (r'(u_2) + r'(g(u_2)) \cdot r'(a_2)).$$

Considerazioni analoghe a quelle della dimostrazione del Teorema 8 mostrano che l'ultima espressione è uguale a $r'(y \cdot y')$. Si ha in definitiva che r' è un automorfismo di N_0.

Sia $\psi : N_0 \to \mathrm{End}\,(N_0)$ definito nel modo seguente:

1) $$\psi(0) = 0_{N_0};$$

2) per $x \neq 0, x \in N_{k-i-1} \setminus N_{k-i}$, $\psi(x)$ è l'elemento di E tale che, $\forall z \in F'$,

$$z^{\psi(x)} = z^{\phi(g^i(x))}.$$

(8) Dove $a \cdot g(z)$ è calcolato nell'anello N_{k-i}.

E' ormai evidente che, per $x, x' \in M$, se $x \cdot x'^{\psi(x)} \neq 0$, allora $\psi(x \cdot x'^{\psi(x)}) = \psi(x) \circ \psi(x')$. Quindi, l'operazione $\circ$ definita sopra M da: $z \circ z' = z \cdot z'^{\psi(z)}$ è associativa. La struttura $N'_0 = [M; +, \circ]$ è allora un quasi-anello che verifica l'asserto.

Sia ora $M' = \left(\bigoplus_{i \in I_t} H_{n+1}\right) \oplus \left(\bigoplus_{i \in I_s} H_n\right)$ $(H_n = pH_{n+1})$.

In tale caso, l'endomorfismo nilpotente che si deve considerare è il seguente:

$$g' : \langle x_1, \ldots, x_t, x_{t+1}, \ldots, x_{t+s} \rangle \to$$
$$\to \langle x_{t+s}, x_1, \ldots, x_{t-1}, px_t, x_{t+1}, \ldots, x_{t+s-1} \rangle.$$

Si noti che l'indice di nilpotenza di g' è $t(n+1) + sn$. ◇

Esistono d'altra parte S-quasi-anelli locali sopra p_m– gruppi di tipo diverso da quello descritto nel Teorema 13, come mostra il

TEOREMA 14. *Sia H un p_m-gruppo di esponente p. Per ogni $n \in N$, $M = H_n \oplus H$ è il gruppo additivo di un S-quasi-anello locale M', tale che $M'/J(M') \cong D$.*

Consideriamo il quasi-anello $R_n = [H_n; +, \circ]$, ed un quasi-anello $R' = [(H_n/H_{n-1}) \oplus H; +, \circ']$, costruito come nel paragrafo 3 di [7], contenente $(R_n/pR_n) \times \{0\}$ come sotto-quasi-anello. Definiamo l'operazione $*$ sopra M nel modo seguente:

$$\langle x, y \rangle * \langle x_1, y_1 \rangle = \langle x_2, y_2 \rangle, \text{ dove } x_2 = x \circ x_1,$$

mentre y_2 è tale che, in R', $\langle [x], y \rangle \circ \langle [x_1], y_1 \rangle = \langle [x_2], y_2 \rangle$. Allora $M' = [M; +, *]$ verifica l'asserto. ◇

6-2. *S-quasi-anelli a gruppo additivo ciclico.*

Usando tecniche precedenti, si riesce a completare l'enumerazione degli S-quasi-anelli con unità sinistra a gruppo additivo ciclico, iniziata in [6]. In particolare si ha che un S-quasi-anello direttamente irriducibile non fortemente monogeno, dotato di unità sinistra e a gruppo additivo ciclico, è sempre un'H-estensione di un anello isomorfo a $\mathbf{Z}_{p^n}$.

Osserviamo che *un gruppo ciclico di ordine pari, è sostegno di uno ed un solo S-quasi-anello fortemente monogeno*. Infatti, un S-quasi-anello fortemente monogeno G, di ordine pari, con gruppo additivo ciclico, è planare (Teorema 8 di [3]). Il suo elemento di caratteristica 2 è tenuto fermo da ogni automorfismo additivo, per cui, il gruppo delle φ_a non nulle deve avere ordine 1. Poiché, inoltre, $G/A_s(G)$ deve essere un campo (cfr. Teorema 7 di [3]), necessariamente $A_s(G) = 2G$, mentre l'insieme delle unità sinistre è $G \backslash 2G$.

LEMMA 15. *Un quasi-anello G^0, non fortemente monogeno, con unità sinistra, sopra $\mathbf{Z}_{p^n}^+$, è isomorfo a $\mathbf{Z}_{p^n}$.*

Sia u un'unità sinistra di G^0.

Per il Teorema 4 di [4], pG^0 è un ideale, G^0/pG^0 è un campo di ordine p e φ_h, per ogni $h \in G^0 \backslash pG^0$, è un automorfismo di $\mathbf{Z}_{p^n}^+$.

Vogliamo dimostrare che $A_s(u) = p^r G^0$, per un opportuno $r > 1$. Altrimenti, risulta $(pG^0)u = 0$, e dunque, per ogni $y \in G$, $(pG^0)y = (pG^0)uy = 0$. Dunque, G^0 non è uno zero-quasi-anello, e, per ogni a che divide lo zero a sinistra, è $aG^0 = 0$ (9). Pertanto, G^0 è fortemente monogeno, contro il supposto.

Sia $1 \leq k < r$. Proviamo che, qualunque sia $k' > k$, $(p^k u)u \notin p^{k'} G^0$. Altrimenti, $(p^k u)u = p^{k'} au$, in cui $a \in \mathbf{Z}$, $k' > k$. Moltiplichiamo a destra per u ambo i membri di questa uguaglianza, e teniamo conto che u è unità sinistra. Risulta $(p^k u)u = (p^{k'} au)u$. Poiché G^0 è un S-quasi-anello, è $(p^k u - p^{k'} au)u = 0$, ossia $(p^k(1 - p^{k'-k} a)u)u = 0$.

Ancora per il fatto che G^0 è un S-quasi-anello, si ha che, per ogni $b \in \mathbf{Z}$, $(p_k(1 - ap^{k'-k})bu)u = 0$. In quanto $1 - p^{k'-k} a$ *è primo con* p, gli elementi $p^k(1 - ap^{k'-k})bu$, al variare di b in $\mathbf{Z}$, descrivono l'intero $p^k G^0$. Quindi, $p^k G^0 \subseteq A_s(u)$, contro il supposto.

In modo analogo si dimostra che $(p^k u)u$ non può appartenere a nessun $p^{k''} G^0$, per $k'' < k$.

Dunque, per ogni $1 \leq k < r$, $(p^k u)u \in p^k G^0$.

Per quanto visto più sopra, esistono elementi $a', b' \in \mathbf{Z}$, primi con p, tali che $(p^{r-1}u)u = p^{r-1}a'u$, $(pu)u = pb'u$.

Intendiamo provare che $r = n$. Infatti, se così non fosse, si avrebbe: $(p^{r-1}u)((pu)u) = (p^{r-1}u)(pb'u) = pb'((p^{r-1}u)u) = p^r a'b' \neq 0$, mentre $[(p^{r-1}u)(pu)]u = [p((p^{r-1}u)u)]u = [p(p^{r-1}a'u)]u = (p^r a'u)u = 0$, essendo $p^r a'u \in A_s(u)$.

Pertanto, $A_s(u) = \{0\}$.

Sia $0 \leq k < n$ e sia h primo con p. Per quanto detto nella prima parte della dimostrazione, esiste un intero h', primo con p, tale che $(p^k hu)u =$

(9) Si noti che un elemento che divida lo zero a sinistra è necessariamente contenuto in pG^0.

$p^k h'u$. Poiché u è unità sinistra, risulta $(p^k hu)u = (p^k h'u)u$, da cui $((p^k h - p^k h')u)u = \{0\}$, essendo G^0 un S-quasi-anello. Quindi, $(p^k h - p^k h')u \in A_s(u) = \{0\}$. Allora $p^k hu = p^k h'u$.

L'elemento u è dunque l'unità di G^0. Il prodotto in G^0 è commutativo, in quanto $(k_1 u)(k_2 u) = k_2((k_1 u)u) = k_2(k_1 u) = (k_2 k_1)u = k_1(k_2 u) = k_1((k_2 u)u) = (k_2 u)(k_1 u)$.

Pertanto, G^0 è un anello commutativo unitario, necessariamente isomorfo a $\mathbf{Z}_{p^n}$. ◊

Se G è un gruppo additivo, indichiamo con $S(G)$ il numero degli S-quasi-anelli con unità sinistra, direttamente irriducibili, due a due non isomorfi, che hanno G come gruppo additivo.

TEOREMA 16. *Sia G un gruppo ciclico di ordine* $n = \prod_{i=1}^{m} p_i^{n_i}$, *con* $p_i < p_j$ *per* $i < j$. *Se* $S(G) \neq 0$, *allora* $p_1 - 1$ *divide ogni* $p_j - 1$, *ed inoltre* $S(G) = \varphi(p_1 - 1)^{m-1}$ *se* $n_1 = 1$, *mentre* $S(G) = 2\varphi(p_1 - 1)^{m-1}$ *se* $n_1 > 1$. *Se* $p_1 - 1$ *non divide ogni* $P_j - 1$, *allora* $S(G) = 0$.

Sia G^0 un quasi-anello sopra G, direttamente irriducibile e con unità sinistra; sia J il radicale nil di G^0. Per quanto visto nel paragrafo 2 di [4], G^0/J è un campo primo (di ordine p).

Se l'ordine di G è dispari, allora G^0 ha un gruppo di automorfismi privi di coincidenze non nulle di ordine $p - 1$. Per la struttura del gruppo degli automorfismi di G, deve essere $p = p_1$.

Se l'ordine di G^0 è pari, allora G^0 ha un solo elemento c di caratteristica 2. Necessariamente $G^0 c = \{0, c\}$. Di qui e dal Teorema 1 di [3], $|G^0/A_s(g)| = 2$, per cui si ha subito $p = p_1 = 2$. In ogni caso, dunque, G^0/J è un campo di ordine p_1. Pertanto, $J = p_1 G^0$.

Sia G_i il p_i-sottogruppo di Sylow di $G (i \in I_m)$.

Indichiamo con $\bar{u}$ un arbitrario elemento di $G_1 \backslash p_1 G_1$. E' immediato che $\bar{u} \in G \backslash p_1 G$. Per il Teorema 4 di [4], punto 1, un'opportuna potenza u, di $\bar{u}$, è un'unità sinistra di G^0.

Siccome G_1 è pienamente invariante in G^+, è $u \in G_1 \backslash p G_1$. Ancora per il fatto che G_1 è pienamente invariante, G_1 è sostegno di un sotto-S-quasi-anello G_1^0 di G^0. Per il Teorema 15, o G_1^0 è un S-quasi-anello fortemente monogeno, o è isomorfo all'anello $\mathbf{Z}_{p_1^{n_1}}$.

Supponiamo che G_1^0 sia fortemente monogeno. Per quanto visto in [3], $A_s(u) \cap G_1^0 = p_1 G_1^0$. Dunque, per ogni $g \in G^0$, e per ogni $t \in Z$, è $(p_1 tu)g = (p_1 tu)(ug) = ((p_1 tu)u)g = 0g = 0$. Pertanto, $p_1 G_1 \subseteq A_s(g)$.

Sia $\bar{g} \in p_1 G^0$. Siccome $\bar{g} \in J$, è $\bar{g}\, u \in J \cap G_1 = p_1 G_1$. Per quanto sopra, dunque, $(\bar{g}\, u) G^0 = \{0\}$. Per ogni x di G^0 si ha allora $\bar{g}\, x = \bar{g}\, (ux) = (\bar{g}\, u)x = 0x = 0$.

Dunque, ogni φ_y o è un automorfismo, o è l'endomorfismo nullo. Quindi, G^0 è fortemente monogeno.

Supponiamo ora che G_1^0 sia isomorfo all'anello $\mathbf{Z}_{p_1^{n_1}}$.

Se per assurdo è $A_s(u) \cap p_1^{n_1} G^0 \subset p_1^{n_1} G^0$, allora è $|G^0 u| > p_1^{n_1}$, per il Teorema 1 di [3]. Questo non può sussistere, in quanto G_1 è pienamente invariante in G. Conseguentemente, $(p_1^{n_1} G^0)u = 0$.

Dobbiamo ora dimostrare che, per ogni $j > 1$, $(p_1 u) G_j = \{0\}$.

Si supponga per assurdo che $(p_1 u) G_j \neq 0$. Poiché $p_1 G^0$ è il radicale nil di G^0, esiste un $s \in G_j$, tale che $(p_1 u)s \neq 0$, e $(p_1 u)^2 s = (p_1^2 u)s = 0$.

Tenuto conto di quanto sopra esposto, è allora

$$A_s(s) = p_1^2 G^0, \tag{3}$$

$$A_s((p_1 u)s) = p_1 G^0. \tag{4}$$

Osserviamo che i laterali di $p_1^2 G$, rappresentati da elementi di $G \backslash p_1 G$, sono $p_1(p_1 - 1)$. Per il Teorema 4 di [4], punto 1, l'insieme $\{\varphi_a \mid a \in G^0 \backslash J\}$ costituisce un gruppo di automorfismi Φ di G. Tenuto conto di (1) e del Teorema 1 di [3], la traiettoria di Φ rappresentata da s ha dunque ordine $p_1(p_1 - 1)$. Siccome $p_1 < p_2$, deve allora esistere un sottogruppo dell'automorfo di G_j, di ordine $p_1(p_1 - 1)$, e questo è necessariamente privo di coincidenze non nulle. Si ha allora, qualunque sia $s' \in G_j \backslash \{0\}$, $|\Phi(s')| = p_1(p_1 - 1)$.

In particolare,

$$|\Phi((p_1 u)s)| = p_1(p_1 - 1). \tag{5}$$

Da (3) e (5) si trae che $|G^0((p_1 u)s)| = p_1(p_1 - 1) + 1$.

D'altra parte, da (4) e dal Teorema 1 di [3], è $|G^0((p_1 u)s)| = p_1$, da cui l'assurdo. Pertanto, $(p_1 u) G_j = 0$. Allora, $A_s(G_j) = A_s(p_1^{n_1} G^0) = p_1 G^0$. Ancora per il Teorema 4 di [4], e per il Teorema 1 di [3], le restrizioni a $p_1^{n_1} G^0$ di tutte le φ_x, per x appartenente ad un fissato laterale non nullo di $p_1 G$ in G, coincidono con un unico automorfismo privo di coincidenze non nulle di $p_1^{n_1} G^0$.

Ne segue che G^0 è una h-estensione di G_1^0 $\left(\cong Z_{p_1^{n_1}}\right)$ mediante $p_1^{n_1}G$. Proviamo che $p_1G_1^0$ è un ideale di G^0.

Siano $i \in p_1G_1^0, n, n' \in G^0, n = n_{11} + n_{12}, n' = n_{21} + n_{22}$, dove n_{21}, $n_{11} \in G_1^0, n_{12}, n_{22} \in p_1^{n_1}G^0$. Calcoliamo $(n + i)n' - nn' =$

$$= (((n_{11} + i) + n_{12})n_{21} - (n_{11} + n_{12})n_{21}) + \\ + (((n_{11} + i) + n_{12})n_{22} - (n_{11} + n_{12})n_{22}). \tag{6}$$

Ma $p_1G + n_{11} + i + n_{12} = p_1G + n_{11} + n_{12}$. Si trae allora che il secondo termine di (6) è nullo.

Siccome $n_{12}n_{21} = 0$ e siccome G^0 è un S-quasi- anello, è $((n_{11} + i) + n_{12})n_{21} = (n_{11} + i)n_{21}$, e $(n_{11} + n_{12})n_{21} = n_{11}n_{21}$.

L'espressione (6) è dunque uguale a $in_{21} \in p_1G_1^0$. Pertanto, $p_1G_1^0$ è un ideale di G^0. Il quoziente di $G^0/p_1G_1^0$ ha ordine $p_1p_2^{n_2} \dots p_m^{n_m}$, e per la prima parte della dimostrazione, è un S-quasi-anello fortemente monogeno.

Per quanto visto in [6], è $S(p_1^{n_1-1}G) = \varphi(p_1 - 1)^{m-1}$. Ne segue subito l'asserto. ◇

COROLLARIO 17. *Un S-quasi-anello non fortemente monogeno G^0 è univocamente determinato, a meno di isomorfismi, dall'S-quasi-anello $G^0/p_1G_1^0$.*

COROLLARIO 18. *Un S-quasi-anello non fortemente monogeno, con unità sinistra, direttamente irriducibile, a gruppo additivo ciclico, è H-estensione di un anello Z_{p^n}, per p numero primo.*

BIBLIOGRAFIA

[1] R.M. BRYANT and G. KOVACS, *"Lie rapresentations and groups of prime power order"*, J. London Math. Soc. (2), *17* (1978), 415-421.

[2] G. FERRERO, *"Classificazione e costruzione degli stems p-singolari"*, Ist. Lombardo Accad. Sci. Lett. Rend. (A), *102* (1968), 597-613.

[3] G. GALLINA, *"Su certe relazioni di equivalenza nei quasi-anelli"*, Riv. Mat. Univ. Parma (4), *10* (1984), 1-5.

[4] G. GALLINA, *"Sui radicali di un S-quasi-anello"*, Boll. Un. Mat. Italiana (6), *4* (1985), 415-424.

[5] G. GALLINA, *"Generalizzazioni di quasi-anelli fortemente monogeni"*, Riv. Mat. Univ. Parma (4), *12* (1986), 31-34.

[6] G. GALLINA, *"Determinazione di certi quasi-anelli fortemente monogeni"*, Boll. Un. Mat. Italiana - Algebra e Geometria, Serie VI, Vol. IV - D.N. 1 - (1985), 123-130.

[7] G. GALLINA, *"On the structure of some near-rings"*, Ist. Lombardo Accad. Sci. Lett., A 121 (1987), 73-90.

[8] R. LIDL and H. NIEDERREITER, *"Finite fields", Addison-Wesley Publishing Company, Cambridge, 1983.*

[9] J.M. LORIMER, *"Affine Hjelmslev rings and planes"*, Annals of Discrete Mathematics, *37* (1958), 265-276.

[10] C.J. MAXSON, *"On local near-rings"*, Math. Zeitschr, *106* (1968), 197-205.

[11] C.J. MAXSON, *"Dickson near-rings"*, Journal of Algebra, *14* (1970), 152-169.

[12] G. PILZ, *"Near-rings"*, North-Holland, Amsterdam, 1977.