
ATTI ACCADEMIA NAZIONALE DEI LINCEI
CLASSE SCIENZE FISICHE MATEMATICHE NATURALI

RENDICONTI

DANIEL R. HUGHES

Sottopiani non-Desarguesiani di piani finiti

*Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche,
Matematiche e Naturali. Rendiconti, Serie 8, Vol. 36 (1964), n.3, p. 315–318.*
Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1964_8_36_3_315_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

NOTE PRESENTATE DA SOCI

Matematica. — *Sottopiani non-Desarguesiani di piani finiti.*
Nota di DANIEL R. HUGHES (*), presentata (**) dal Socio B. SEGRE.

1. INTRODUZIONE. — In una conferenza del 1963, R. H. Bruck ha posto la seguente domanda: Ci sono piani finiti con sottopiani propri non-Desarguesiani? È sorprendente che tale domanda possa tuttora essere aperta; e qui mostreremo che ci sono molti piani finiti con sottopiani propri non-Desarguesiani. Più particolarmente, studieremo una classe di piani sopra quasikorpi distributivi; in questo caso, basterà studiare i sottoquasikorpi distributivi.

Adotteremo la terminologia di [3], per esempio, eccetto che usiamo il termine *sottopiano di Baer* per indicare un sottopiano π_0 di un piano π , tale che l'ordine di π_0 sia la radice quadrata dell'ordine di π . Inoltre, diremo che una collineazione di π che fissi tutti i punti, e tutte le rette, di un sottopiano π_0 di Baer è una *collineazione di Baer*; una *involutione di Baer* è una collineazione di Baer che sia ciclica d'ordine due. Un ben noto teorema di Baer ([3]) dice che una collineazione d'ordine due o è centrale o è un'involutione di Baer.

Un *quasicorpo* è notoriamente un insieme Q con due operazioni binarie, addizione e moltiplicazione, tali che:

- (1) $(Q, +)$ è un gruppo, il cui elemento neutro denotiamo con 0 ;
- (2) $(Q^*, \cdot)$, dove Q^* è l'insieme degli elementi $\neq 0$, è un capio (in inglese: «loop»); ciò vuol dire che, in Q^* , l'equazione $xy = z$ è tale che due qualunque elementi determinano unicamente il terzo, e v'è un elemento 1 tale che $1x = x1 = x$, per ogni x ;
- (3) $x(y + z) = xy + xz$, per ogni scelta di x, y, z in Q ;
- (4) $0x = 0$, per ogni x in Q .

Un *quasicorpo distributivo*, è un quasicorpo Q che soddisfi anche alla

- (5) $(x + y)z = xz + yz$, per ogni scelta di x, y, z in Q .

Ammetteremo sempre che tutti i quasicorpi considerati siano finiti. È ovvio che cosa debba intendersi per *sottoquasicorpo* (distributivo o no) di un dato quasicorpo. Il teorema di Baer, citato sopra, implica che un automorfismo d'ordine due di un quasicorpo (distributivo) Q debba fissare tutti gli elementi di un sottoquasicorpo (distributivo) Q_0 di Q , dove gli ordini $|Q|$, $|Q_0|$ di Q , Q_0 soddisfano alla $|Q| = |Q_0|^2$. (Il fatto che Q_0 sia chiuso rispetto alla moltiplicazione non è del tutto banale; desidero ringraziare M. V. D. Burmester per avermelo mostrato, sebbene ciò non sia importante per il

(*) Supported in part by the National Science Foundation under grant NSF G-18912.
L'Autore desidera ringraziare V. Corbas per alcune utili conversazioni su questo lavoro.

(**) Nella seduta del 14 marzo 1964.

seguito, perché è ovvio che un sottoquasicorpo definisce un sottopiano, e questo basterà per i nostri esempi). Ricordiamo infine che il piano sopra un quasicorpo distributivo Q è Desarguesiano se, e soltanto se, Q è associativo.

2. QUASICORPI DISTRIBUTIVI. - Scriviamo, brevemente, QD per quasicorpo distributivo. Anzitutto, definiamo una classe particolare di QD (Cfr. [2]). Sia R uno spazio vettoriale di dimensione due sopra un campo F con elementi base $1, \lambda$, sicché possiamo scrivere $R = \{x + \lambda y\}$, per x, y variabili in F . Siano d_0 e d_1 elementi di F , e σ automorfismo di F , tali che

$$(1) \quad w^{1+\sigma} = d_0 + d_1 w \quad \text{non abbia soluzioni } w \text{ in } F.$$

Se F non è d'ordine primo, e se $\sigma \neq 1$, è sempre possibile scegliere d_0 e d_1 in modo tale che la (1) risulti soddisfatta.

Definiamo una moltiplicazione in R , nel modo seguente:

$$(2) \quad (x + \lambda y)(u + \lambda v) = (xu + d_0 y^\sigma v) + \lambda(yu + x^\sigma v + d_1 y^\sigma v).$$

Allora R risulta un QD, che non è mai associativo se $\sigma \neq 1$. R ha ovviamente il sottoQD: $F = \{x + \lambda 0\}$, ma F è associativo (tutte le dimostrazioni trovansi in [2]); determineremo tuttavia dei sottoQD non-associativi.

Sia K un sottocampo di F , e sia R_K il sottoinsieme di R formato dagli elementi $a + \lambda b$, dove a, b variano in K . Chiaramente R_K sarà un sottoQD se, e soltanto se, d_0 e d_1 sono in K ; σ è un automorfismo di K (naturalmente solo nel caso finito), e, inoltre, R_K risulta non-associativo se, e soltanto se, σ subordina l'identità in K . Indichiamo con F_α il sottocampo di F formato dagli elementi che restano fissi per un dato automorfismo α .

LEMMA 1. - R_K è un sottoQD se, e soltanto se, d_0 e d_1 sono in K . Se R_K è un sottoQD, allora R_K è associativo se, e soltanto se, K è contenuto in F_σ .

Dimostrazione. - La prima parte è già stata dianzi stabilita. Per la seconda, vediamo che σ induce l'identità su K se, e soltanto se, K è contenuto nell'insieme degli elementi fissi per σ , cioè in F_σ .

Ora è ovvio che $|R| = |R_K|^n$, dove n denoti la dimensione di F sopra K . È possibile dimostrare il viceversa? Cioè, dato n , si tratta di trovare F e K , in modo che la dimensione di F sopra K sia n , e R_K sia un sottoQD, non-associativo.

A tal uopo, dato un numero primo $p \neq 2$, e l'intero $n > 0$, scegliamo un numero primo $q \neq 2$, e gl'interi $r > 0$ e $m > 0$, tali che:

$$(3) \quad n \not\equiv 0 \pmod{q},$$

$$(4) \quad p^r \equiv -1 \pmod{q},$$

$$(5) \quad p^m \equiv 1 \pmod{q}, \text{ e } m > r.$$

Incominciamo con lo stabilire il

LEMMA 2. - Se p, q, r, m, n soddisfano alle (3), (4), (5), allora esiste un elemento d_0 di $GF(p^m)$ che non si può scrivere sotto la forma $d_0 = x^{1+p^r}$ per nessun x di $GF(p^{mn})$.

Dimostrazione. — Si tratta di far vedere che non tutti gli elementi di $\text{GF}(p^m)$ sono potenze $(1 + p^r)$ -esime in $\text{GF}(p^{mn})$. Ora $\text{GF}(p^m)$ consiste esattamente delle potenze $(p^{mn} - 1)/(p^m - 1)$ -esime in $\text{GF}(p^{mn})$; sarà quindi sufficiente mostrare che esiste un numero primo che divide $p^{mn} - 1$ e $p^r + 1$, ma non divide $(p^{mn} - 1)/(p^m - 1)$. Ma:

$$p^m \equiv 1 \pmod{q} \text{ implica } p^{mn} \equiv 1 \pmod{q}, \text{ ossia } q \text{ divide } p^{mn} - 1;$$

$$p^r \equiv -1 \pmod{q} \text{ implica che } q \text{ divide } p^r + 1;$$

$$(p^{mn} - 1)/(p^m - 1) = p^{m(n-1)} + p^{m(n-2)} + \dots + p^m + 1$$

$$\equiv 1 + 1 + \dots + 1 \equiv n \pmod{q}, \text{ sicché } q \text{ non divide } n.$$

Pertanto q è un tale primo, onde l'asserto.

Teorema 1. — Dato un numero primo $p \neq 2$, e un intero $n > 0$, esistono un campo $F = \text{GF}(p^{mn})$, elementi d_0, d_1 di F , ed un automorfismo σ di F , tali che, se $K = \text{GF}(p^m)$, il QD R possiede un sottoQD R_K , non-associativo.

Dimostrazione. — Scegliamo q, m, r in modo che le (3), (4), (5), siano soddisfatte; sia $d_1 = 0$, ed d_0 un elemento di $\text{GF}(p^m)$ che (lemma 2) non sia della forma $d_0 = x^{1+p^r}$, con x in $\text{GF}(p^{mn})$. Si definisca σ assumendo $y^\sigma = y^{p^r}$, per ogni y in $\text{GF}(p^{mn})$. Poiché $r < m$, ne consegue che σ non induce l'identità su $K = \text{GF}(p^m)$; e ciò completa la dimostrazione.

Se n è pari, allora R contiene anche il sottoQD $\text{GF}(p^{2m})$, e quindi R contiene due sottoQD dello stesso ordine, non-isomorfi.

Più generalmente, se d_0 è in F_α , la corrispondenza $x + \lambda y \rightarrow x^\alpha + \lambda y^\alpha$ è un automorfismo di R che fissa R_{F_α} , onde quest'ultimo insieme è un sottoQD, perché contiene d_0 .

TEOREMA 2. — Usando la costruzione del Teorema 1, nell'ipotesi che sia $n = 2$, il piano sopra R viene a contenere due sottopiani di Baer non-isomorfi, di cui uno Desarguesiano, ciascuno formato dall'insieme degli elementi fissi per un'involuzione di Baer. Inoltre, le due involuzioni di Baer risultano fra loro permutabili.

DIMOSTRAZIONE. Poiché $n = 2$, abbiamo un sottoQD, R_K ; esiste inoltre un automorfismo σ di F , d'ordine due, i cui elementi fissi sono esattamente gli elementi di K . Otteniamo così uno dei sottopiani di Baer, con la relativa involuzione di Baer; e questo sottopiano è non-Desarguesiano. Per l'altro, usiamo il sottoQD F ; l'automorfismo ad esso relativo sarà la corrispondenza $x + \lambda y \rightarrow x - \lambda y$.

Per esempio, esiste un piano d'ordine 3^{16} , con due sottopiani di ordine 3^8 , non-isomorfi. Qui abbiamo usato il teor. 2 con $p = 3, q = 5, r = 2, m = 4$.

3. OSSERVAZIONI. — Senza dimostrazione o spiegazione, affermiamo che *tutti* i piani d'André ([3]) sono sottopiani propri di altri piani d'André. Il sottoinsieme dei piani d'André che ammettono coordinate in un quasicorpo associativo, si trovano come sottopiani propri di altri piani dello stesso tipo. Ma posseggono forse tutti i piani finiti questa proprietà? O meglio: dato un piano π , anche infinito, esiste un piano π_1 che possegga π come sottopiano di Baer? (Naturalmente, la definizione di sottopiano di Baer nel caso infinito va data altrimenti). In particolare, esiste un'involuzione di Baer di π_1 ,

i cui elementi fissi siano i punti e le rette di π ? già per una classe semplice come i piani di Hall ([1]), questo problema sembra difficile.

BIBLIOGRAFIA.

- [1] M. HALL, JR., *The Theory of Groups*, New York 1958.
- [2] D. R. HUGHES e E. KLEINFELD, *Seminuclear extensions of Galois Fields*, « Amer. J. Math. », 82, 389–392 (1960).
- [3] G. PICKERT, *Projektive Ebenen*, Berlin 1955.