Riv. Mat. Univ. Parma (2) **2** (1961), 183-190

GIUSEPPE RUSSO (*)

Una classe di decomposizioni tattiche di un piano di Galois. (**)

1. – Diremo con DEMBOWSKI [1] (1) che:

Una partizione delle rette e dei punti di un piano grafico finito π in classi disgiunte di rette e di punti si chiama decomposizione tattica di π quando, scelta comunque una classe r di rette e una classe $\mathfrak{S}$ di punti, esse costituiscono una configurazione tattica, cioè quando, comunque si scelgano $\mathfrak{S}$ ed r, si abbia:

a) ogni retta della classe r appartiene ad un medesimo numero di punti della classe $\mathfrak{S}$.

b) ogni punto di $\mathfrak{S}$ appartiene ad uno stesso numero di rette di r.

Tra i numerosi teoremi contenuti nella memoria di DEMBOWSKI, ci sarà utile nel seguito il seguente:

In una decomposizione tattica di un piano grafico finito il numero delle classi di punti uguaglia quello delle classi di rette.

Scopo del presente lavoro è quello di dare esempi di decomposizione tattica di un piano di GALOIS, costruiti mediante un procedimento puramente algebrico-aritmetico.

(*) Indirizzo, Istituto di Matematica, Università Palermo (Italia).
(**) Ricevuto il 12 luglio 1961.
(1) I numeri in neretto e tra [ ] rinviano alla Bibliografia in fine.

Chiameremo con B. SEGRE [3] « piano di GALOIS » un piano lineare sopra un campo finito.

L'idea generale del DEMBOWSKI sopra riassunta, e molti dei risultati della sua Memoria [1], valgono invece anche nel caso di un piano grafico non desarguesiano e pertanto diverso dal piano linerare sopra un corpo.

2. Sia π un piano lineare sopra un campo di GALOIS con q elementi ($q = p^t$; p, numero primo, caratteristica del campo).

È noto che un piano siffatto possiede $q^2 + q + 1$ punti e altrettante rette. L'equazione di una retta non parallela all'asse y si può porre nella forma: $y = mx + n$.

Assumeremo m ed n come coordinate non omogenee della retta $y = mx + n$ (in simboli: $[m, n]$). Alla retta $x = a$ associeremo le coordinate $[\infty, a]$; alla retta impropria $[0, \infty]$.

Suddividiamo, in un primo momento, i punti e le rette di π in classi nel modo seguente:

Poniamo in una medesima classe quei punti (rette) tali che il prodotto $x' y' = k$ ($m' n' = h$ nel caso delle retta) delle loro coordinate $x' \neq 0$, $y' \neq 0$ ($m' \neq 0$, $n' \neq 0$) risulti un dato quadrato in $GF(q)$, come prodotto di due quadrati; in un'altra classe quei punti (rette) tali che il prodotto $x' y' = k$ ($m' n'$ per le rette) risulti un dato quadrato, prodotto di due non quadrati; in un'altra classe quei punti (rette) tali che il prodotto $x' y'$ ($m' n'$), risulti un dato non quadrato, prodotto di un quadrato per un non quadrato; in un'altra classe ancora quei punti (rette) tali che il prodotto $x' y'$ ($m' n'$) risulti un non quadrato, prodotto di un non quadrato per un quadrato.

In simboli:

$$(k)_{qq}; \quad (k)_{nn}; \quad (h)_{qn}; \quad (h)_{nq}, \quad \text{per i punti;}$$

$$[k]_{qq}; \quad [k]_{nn}; \quad [h]_{qn}; \quad [h]_{nq}, \quad \text{per le rette.}$$

(Adottiamo i simboli usati da L. LOMBARDO-RADICE in un lavoro in corso di pubblicazione [2]).

Una tale decomposizione, in generale, non è una decomposizione tattica, come faremo vedere più avanti su di un esempio.

Siano (x', y') e $[m, n]$ le coordinate rispettivamente di un punto e di una retta appartenenti ciascuno ad una delle classi precedenti. È evidente che il punto $(t^z x', t^x y')$ e la retta $[mt^y, nt^x]$ con t quadrato in $GF(q)$, appartengono rispettivamente alla classe cui appartiene il punto (x', y') e la retta $[m, n]$ quando e soltanto quando x, y, z, soddisfano le relazioni:

$$x + z \equiv 0 \quad \text{mod.} \quad \left(\frac{q-1}{2}\right)$$

$$x + y \equiv 0 \quad \text{mod} \quad \left(\frac{q-1}{2}\right).$$

Infatti:

$$t^z x' \cdot t^x y' = t^{x+z} x' y' = t^{x+z} k$$

$$mt^y \cdot nt^x = t^{x+y} mn = t^{x+y} k,$$

e $t^r = 1$ in $GF(q)$ (t è un quadrato) quando e solo quando $r \equiv 0$ mod. $\left(\frac{q-1}{2}\right)$. (Per le proprietà valide nei campi di GALOIS, vedi B. SEGRE [3]).

Supponiamo poi, che il punto (x', y') appartenga alla retta $[m, n]$, sempre nella ipotesi che nessuna delle coordinate sia 0 o ∞. La condizione, necessaria e sufficiente, affinchè il punto $(t^z x', t^x y')$ appartenga alla retta $[mt^y, nt^x]$ è che:

$$t^x y' = mt^y t^z + nt^x = t^{y+z} \cdot mx' + t^x n,$$

cioè che:

$$y + z \equiv x \quad \text{mod.} \quad \left(\frac{q-1}{2}\right).$$

Suddividiamo allora i punti e le rette del piano π in classi del tipo:

(1) $(t^z x', \quad t^x y')$ classi di punti

(2) $[nt^y, \; nt^x]$ classi di rette

fissando tre interi x, y, z in modo tale che siano soddisfatte le condizioni:

$$(3) \qquad \begin{cases} y + z \equiv x \\ x + z \equiv 0 \quad \text{mod.} \quad \left(\frac{q-1}{2}\right) \\ x + y \equiv 0 \end{cases}$$

Si nota subito che ogni classe del tipo (1) è definita a partire da un suo punto qualunque, non dipende cioè dalla scelta del punto iniziale (x', y'). Ed infatti sia $x'' = t^z x'$; $y'' = t^x y'$ un punto di una delle classi di tipo (1), definita a partire da (x', y'). Si ha:

$$x' = t^{-z} x'' = (t^{-1})^z x''$$

$$y' = t^{-x} y'' = (t^{-1})^x y''$$

Moltiplicando membro a membro, ricordando la seconda delle (3) e il fatto che t^{-1} è un quadrato se lo è t, avremo:

$$x' y' = x'' y''$$

il che prova che il punto (x', y') appartiene alla classe (1) definitiva da (x'', y'').

Osserviamo poi che una classe (1) non coincide in genere con la classe $(i)_{rs}$ cui apparteneva il punto (x', y') anzi ne è una sottoclasse. Ciò è dovuto al fatto che le potenze x-me dei quadrati t, sono, in generale, in numero minore dei quadrati stessi.

Ne discende che ognuna delle classi (1), (2) conterrà un numero m di punti (rette) che sarà in generale un divisore di $\left(\frac{q-1}{2}\right)$. Il numero m indica il numero delle potenze x-me dei quadrati t (dalla 2ª e 3ª delle (3) si deduce subito che m è anche il numero delle potenze y-me e z-me dei quadrati). Facilmente si deduce allora che il numero delle classi (1) è:

$$\frac{(q-1)^2}{m} \tag{4}$$

Infatti una classe $(i)_{rs}$ contenente $\frac{q-1}{2}$ punti darà luogo a $\frac{q-1}{2m}$ classi (1). E poichè le classi $(i)_{rs}$ sono $\frac{q-1}{2}$, avremo in definitiva:

α) $\frac{q-1}{2m} \cdot \frac{q-1}{2} = \frac{(q-1)^2}{4m}$ classi per cui il prodotto $x' y'$ è $q \cdot q$

β) $\frac{q-1}{2m} \cdot \frac{q-1}{2} = \frac{(q-1)^2}{4m}$ classi per cui il prodotto $x' y'$ è $n \cdot n$

γ) $\frac{q-1}{2m} \cdot \frac{q-1}{2} = \frac{(q-1)^2}{4m}$ classi per cui il prodotto $x' y'$ è $n \cdot q$

δ) $\frac{q-1}{2m} \cdot \frac{q-1}{2} = \frac{(q-1)^2}{4m}$ classi per cui il prodotto $x' y'$ è $q \cdot n$

Sommando si ha la (4).

Quanto è stato detto per le classi (1) di punti vale ovviamente per le classi (2) di rette.

Il numero totale dei punti (rette) contenuti nelle classi (1) e (2) è quindi:

$$\frac{(q-1)^2}{m}\cdot m = (q-1)^2$$

I rimanenti $3q$ punti (rette) li suddividiamo nelle seguenti classi:

a) Una classe d'un sol punto (retta):

$$(0,0), \qquad [0,\ 0];$$

b) Una classe d'un sol punto (retta):

$$(\infty,\ 0), \qquad [\infty,\ 0];$$

c) Una classe d'un sol punto (retta):

$$(0,\ \infty), \qquad [0,\ \infty];$$

d) $\dfrac{q-1}{m}$ classi contenenti ciascuna m elementi:

$$(t^z x',\ 0), \qquad [mt^y,\ 0];$$

e) $\dfrac{q-1}{m}$ classi ciacuna contenente m elementi:

$$(\infty,\ t^x y'), \qquad [\infty,\ t^x n];$$

f) $\dfrac{q-1}{m}$ classi ciacuna contenente m elementi:

$$(0,\ t^x y'), \qquad [0,\ t^x n].$$

Abbiamo così decomposto il piano π in:

$$\frac{(q-1)^2}{m} + 3\,\frac{q-1}{m} + 3 = \frac{(q+2)\,(q-1)}{m} + 3$$

classi di punti e altrettante di rette.

3. - La precedente decomposizione del piano nelle classi (1), (2), a), b), c), d), e), f), è una decomposizione tattica.

Per dimostrare ciò basta far vedere che se una retta di una classe ha un dato numero, i, di incidenze con i punti di una data classe, ogni retta di quella classe ha lo stesso numero di incidenze con i punti della data classe, e viceversa.

Sia infatti (x', y') un punto di una delle classi (1) e $y = mx + n$ una retta di una delle classi (2). Se il punto dato e la retta data si appartengono, se cioè si ha: $y' = mx' + n$, si ha anche in virtù delle (3):

$$t^x y' = mt^y \cdot t^z x' + nt^x$$

Ciò esprime il fatto che il punto $(t^z x', t^x y')$ della classe (x', y') e la retta $[mt^y, nt^x]$ della classe $[m, n]$ si appartengono; e con ciò le condizioni a) e b) del n. **1** sono soddisfatte per le classi in discorso. Fino ad ora abbiamo escluso la presenza del simbolo ∞, ma non quella dello 0 (cioè: x', y', m, n possono assumere il valore 0).

Si verifica poi facilmente che le condizioni *a*) e *b*) del n. **1** valgono in generale.

4. Concludiamo il lavoro con un esempio.

Sia $q = 13$. I punti di un piano π sopra un GF (13) sono 183; altrettante sono le rette.

I quadrati di GF (13) sono: 1, 3, 4, 9, 10, 12.

I non quadrati: 2, 5, 6, 7, 8, 11.

Scegliamo $x = 2$, $y = 4$, $z = 4$; le (3) sono soddisfatte. Al variare di t tra i quadrati si ha: $t^2 = 1, 9, 3$, e quindi $m = 3$.

Le $\dfrac{(q-1)^2}{m} = 48$ classi di punti (rette) con coordinate entrambe non nulle sono:

(1,1),	(3,9),	(9,3);	(4,10),	(10,4),	(12,12).	$(1)_{qq}$
(3,1),	(9,9),	(1,3);	(4,4),	(12,10),	(10,12).	$(3)_{qq}$
(4,1),	(12,9),	(10,3);	(1,4),	(3,10),	(9,12).	$(4)_{qq}$
(9,1),	(1,9),	(3,3);	(12,4),	(10,10),	(4,12).	$(9)_{qq}$
(10,1),	(4,9),	(12,3);	(9,4),	(1,10),	(3,12).	$(10)_{qq}$
(12,1),	(10,9),	(4,3);	(3,4),	(9,10),	(1,12).	$(12)_{qq}$

(7,2),	(8,5),	(11,6);	(2,7),	(6,11),	(5,8).	$(1)_{nn}$
(8,2),	(11,5),	(7,6);	(6,7),	(5,11),	(2,8).	$(3)_{nn}$
(2,2),	(6,5),	(5,6);	(8,7),	(11,11),	(7,8).	$(4)_{nn}$
(11,2),	(7,5),	(8,6);	(5,7),	(2,11),	(6,8).	$(9)_{nn}$
(5.2),	(2,5),	(6,6);	(7,7),	(8,11),	(11,8).	$(10)_{nn}$
(6,2),	(5,5),	(2,6);	(11,7),	(7,11),	(8,8).	$(12)_{nn}$
(1,2),	(3,5),	(9,6);	(4,7),	(12,11),	(10,8).	$(2)_{qn}$
(1,5),	(3,6),	(9,2);	(10,7),	(4,11),	(12,8).	$(5)_{qn}$
(1,6),	(3,2),	(9,5);	(12,7),	(10,11),	(4,8).	$(6)_{qn}$
(1,7),	(3,11),	(9,8);	(10,2),	(4,5),	(12,6).	$(7)_{qn}$
(1,8),	(3,7),	(9,11);	(4,2),	(12,5),	(10,6).	$(8)_{qn}$
(1,11),	(3,8),	(9,7);	(12,2),	(10,5),	(4,6).	$(11)_{qn}$
(2,1),	(6,9),	(5,3);	(7,4),	(11,12),	(8,10).	$(2)_{nq}$
(5,1),	(2,9),	(6,3);	(11,4),	(7,10),	(8,12).	$(5)_{nq}$
(6,1),	(5,9),	(2,3);	(8,4),	(11,10),	(7,12).	$(6)_{nq}$
(7,1),	(8,9),	(11,3);	(5,4),	(2,10),	(6,12).	$(7)_{nq}$
(8,1),	(11,9),	(7,3);	(2,4),	(6,10),	(5,12).	$(8)_{nq}$
(11,1),	(7,9),	(8,3);	(6,4),	(5,10),	(2,12).	$(11)_{nq}$

La classe a) d'un sol punto (retta) è:

$$(0,\ 0), \qquad [0,\ 0].$$

La classe b) d'un sol punto (retta) è

$$(\infty, 0), \qquad [\infty, 0].$$

La classe c) d'un sol punto (retta) è

$$(0, \infty), \qquad [0, \infty].$$

Le quattro classi d) sono:

(1,0), (3,0), (9,0), ove 1, 3, 9, sono le quarte potenze dei quadrati; (4,0), (10,0), (12,0); (2,0), (5,0), (6,0); (7,0), (8,0), (11,0).

(Anche queste ultime tre classi sono ottenute a partire da un qualunque elemento).

Le quattro classi e) ciascuna contenente tre punti (rette) sono:

$$(\infty, 1), \ (\infty, 9), \ (\infty, 3); \qquad (\infty, 4), \ (\infty, 10), \ (\infty, 12).$$

$$(\infty, 2), \ (\infty, 5), \ (\infty, 6); \qquad (\infty, 7), \ (\infty, 8), \ (\infty, 11).$$

Le quattro classi f) ciascuna contenente tre punti (rette) sono:

$$(0,1), \ (0, 9), \ (0, 3); \qquad (0, 4), \ (0, 10), \ (0,12).$$

$$(0, 2), \ (0, 5), \ (0,6); \qquad (0, 7), \ (0,8), \ (0,11).$$

Si ha così una decomposizione tattica del piano lineare finito sopra GF (13) in 63 classi di punti e in altrettante di rette.

Bibliografia.

[1] P. Dembowski, *Verallgemeinerungen von Transitivitätklassen endlicher projektiver Ebenen*, Math. Z. **69** (1958), 59-89.

[2] L. Lombardo-Radice, *Le decomposizioni tattiche di un piano finito associate a un k-arco*, Ann. Mat. Pura Appl. (in corso di pubblicazione).

[3] B. Segre, *Lectures on modern geometry*, Monografie del C.N.R., Cremonese, Roma (1960).