BENEDITO CASTRUCCI

F U N D A M E N T O S

D A

G E O M E T R I A   P R O J E T I V A

F I N I T A

N - D I M E N S I O N A L

Tese apresentada no concurso para provimento da CADEIRA IX - GEOMETRIA ANALÍTICA, PROJETIVA E DESCRITIVA - da Faculdade de Filosofia, Ciências e Letras da Universidade de São Paulo.

1951

À

M E M Ó R I A

D E

M E U S   P A I S

INTRODUÇÃO

As questões relativas à Geometria Finita surgiram, segundo nos parece, com os trabalhos de G. Fano [1] em 1892 e B. Levi [2] em 1904, de que temos notícia apenas pelos comentadores.

A seguir, vêm as publicações de Veblen e Bussey [3 e 4], em 1906 e 1907, de B. Levi [5] em 1907 e as referências sôbre o assunto contidas no excelente tratado de Geometria Projetiva de Veblen and Young [6], em 1910.

Depois de um interregno de aproximadamente vinte anos, recomeçaram as investigações nesse sector, a partir de 1930, com um trabalho de R. D. Carmichael [7], seguido por grande número de publicações, entre as quais podemos enumerar: R. Moufang [8, 9, 10, 11, 12, 13, 14], em 1931, 1932, 1933 e 1934; R. Brauer [15], em 1936; J. Singer [16], em 1938; R. Baer [17, 18], em 1942; F. W. Levi [19], em 1942; M. Hall [20], em 1943; R. Baer [21, 22, 23, 24], em 1945, 1946 e 1947; C. T. Yang [25], em 1947.

As aplicações à estatística, nos delineamentos de experimentos, apareceram nos estudos de Fisher [26] e Yates [27], em 1937; R. C. Bose [28], em 1938; W. L. Stevens [29], em 1939; R. C. Bose e K. R. Nair [30], em 1941; W. L. Stevens [30'], em 1949.

Esta intensificação de estudos nesse domínio da Geometria é que nos animou a apresentar uma exposição pessoal dos fundamentos da Geometria Projetiva N-dimensional, onde tivemos oportunidade de obter alguns resultados.

No capítulo I, aproveitamos o método empregado, no corpo real, por O. Schreier und E. Sperner [31], da associação de um espaço vectorial ao espaço projetivo. No cálculo de algumas fórmulas, seguimos R. D. Carmichael [32].

No cap. II, obtivemos generalizações de alguns resultados do trabalho de Chung Tao Yang [25], que generaliza um resultado de M. Steck [33]. Inserimos, também, algumas propriedades relativas às homografias sem pontos unidos.

No final do cap. II, incluimos estudos de B. Segre [34], sôbre as homografias involutórias.

Devido à limitação de tempo, não nos foi possível tratar das reciprocidades, principalmente no caso involutório, campo onde se nos afigura haver possibilidade de obtenção de resultados interessantes.

Para facilitar a leitura dêstre trabalho, colocamos entre colchetes os números que indicam a ordem da colocação na bibliografia, que se acha no fim.

CAPÍTULO I

§ 1º - CONCEITOS PRELIMINARES

1. Seja K um corpo finito de característica p e de ordem $q = p^n$. Indiquemos por K* ao conjunto K com exclusão de zero. Consideremos as aplicações [35, pag.7] do conjunto finito I dos inteiros 0, 1, 2, 3,...,N em K.

DEFINIÇÃO 1. Chamam-se (N+1)-uplas ordenadas [36,pag.6] às famílias [35,pag.13] $(x_i)_{i \in I}$ de elementos de K.

Daqui em diante, referir-nos-emos às (N+1)-uplas ordenadas simplesmente como (N+1)-uplas.

DEFINIÇÃO 2. A (N+1)-upla $(x_i)_{i \in I}$ é equivalente à (N+1)-upla $(y_i)_{i \in I}$, se e sòmente se

$$x_i = ky_i \tag{1}$$

qualquer que seja i, onde $k \in K^*$.

É claro que com a definição 2, temos uma <u>relação</u> R <u>de equivalência</u> [35,pag.28,29] no conjunto P de tôdas as (N+1)-uplas.

Os elementos do <u>conjunto quociente</u> de P pela relação R, isto é, P/R, são as <u>classes de equivalencia</u> segundo R.

DEFINIÇÃO 3. Chama-se ponto ou P_0 a qualquer classe de equivalência pertencente a P/R, com exclusão da constituida pela (N+1)-upla (0,0,...,0).

Indicaremos um ponto por uma (N+1)-upla representante da classe de equivalência, i.e., por $(x_0,\dots,x_N)$, ou (x_i), ou ainda simplesmente por (x).

Dois pontos são <u>coincidentes</u>, quando estão indicados por representantes da mesma classe de equivalência; <u>distintos</u>, se tal não acontece.

DEFINIÇÃO 4. Chama-se <u>espaço</u> P_N ao conjunto de todos os pontos.

DEFINIÇÃO 5. Chama-se <u>reta</u> ou P_1 de P_N ao conjunto de todos os pontos (x_i) obtidos das equações

$$x_i = \sigma y_i + \rho z_i \qquad (i=0,1,2,\dots,N) \tag{2}$$

onde (y_i) e (z_i) são dois pontos dados e distintos; σ e ρ variam em K, excluindo-se $\sigma = \rho = 0$ simultâneamente.

Um ponto (w_i) pertence a uma reta r $(x_i = \sigma y_i + \rho z_i)$, se existem valores σ_1 e ρ_1 de σ e ρ, tais que

$$w_i = \sigma_1 y_i + \rho_1 z_i;$$

se tal não é possível, $(w_i) \notin r$.

Duas retas coincidem, se e sòmente se, todo ponto de cada uma delas pertence à outra.

É evidente que por dois pontos distintos <u>passa uma e uma só reta</u>. Daí concluimos que a reta determinada por dois pontos A e B de uma reta r coincide com r.

DEFINIÇÃO 6. Consideradas uma reta r ou P_1

$$x_i = \sigma y_i + \rho z_i \quad (i=0,\ldots,N)$$

e um ponto $P \equiv (w_i) \notin r$ (*), chama-se <u>plano</u> ou P_2 de P_N ao conjunto de todos os pontos das retas determinadas por P e pelos pontos de P_1.

Os pontos (v_i) do plano são dados por

$$(3) \qquad v_i = \tau w_i + \nu x_i = \tau w_i + \nu(\sigma y_i + \rho z_i)$$

ou

$$v_i = \tau w_i + \lambda y_i + \mu z_i \quad (i=0,\ldots,N)$$

Anàlogamente, temos que um ponto $P \equiv (m_i) \in P_2$ se e sòmente se, existem valores τ_1, λ_1, μ_1 de τ, λ, μ, tais que

$$m_i = \tau_1 w_i + \lambda_1 y_i + \mu_1 z_i ;$$

se assim não for, $P \notin P_2$.

Sucessivamente, definimos sub-espaços P_3, P_4, ..., de P_N, com a definição recorrente.

DEFINIÇÃO 7. Considerados um P_{M-1} $(2 \leq M \leq N)$ e um ponto $P \equiv (w_i)$ que não pertença ao P_{M-1} (*), chama-se <u>sub-espaço</u> P_M de P_N ao conjunto de todos os pontos das retas determinadas por P e pelos pontos de P_{M-1}.

(*) A existência aparece no cálculo do nº 2.

Os pontos (x_i) de P_{M-1} são dados por

$$x_i = \sum_{j=0}^{M} \lambda_j y_i^{\,j} \qquad (i=0,\dots,N) \tag{4}$$

e os (v_i) de P_M são:

$$v_i = \sigma w_i + \nu x_i = \sigma w_i + \nu\Big(\sum_{j=0}^{M} \lambda_j y_i^{\,j}\Big) = \sum_{j=0}^{M+1} \tau_j y_i^{\,j} \tag{5}$$

$$(i=0,\dots,N)$$

O conceito acima não vale se $M-1 = N$, pois, nesse caso, não existe ponto que não pertença a P_N.

Ao sub-espaço P_{N-1} de P_N, chama-se de <u>hiperplano</u>.

O número M de P_M se denomina <u>dimensão</u> de P_M.

Aqui, também, é fácil ver que que, escolhidos $M+1$ pontos de P_M nas condições acima, êles determinam o mesmo P_M.

2. É de bastante interêsse o cálculo que faremos a seguir, dos números de elementos do P_N.

a) <u>Número de pontos do</u> P_N.

O número das $(N+1)$-uplas é q^{N+1} e, excluindo-se a $(0,\dots,0)$, ficam $q^{N+1} - 1$; o número das classes de equivalência é, então:

$$\frac{q^{N+1}-1}{q-1} = q^N + q^{N-1} + \dots + 1 = \sum_{i=0}^{N} q^{N-i} \tag{6}$$

b) <u>Número de pontos de cada reta do</u> P_N.

O número de pontos de uma reta é igual ao de escolhas de (σ, ρ) em K, excluindo-se $(0,0)$, a menos de fator de K^*, portanto, temos:

$$\frac{q^2 - 1}{q-1} = q + 1 \,. \tag{7}$$

c) <u>Número de pontos de cada plano do</u> P_N.

Com cálculo análogo ao caso b), vem:

$$\frac{q^3 - 1}{q-1} = q^2 + q + 1 \tag{8}$$

d) <u>Número de pontos de um</u> P_M <u>do</u> P_N.

Um cálculo baseado na expressão (5) nos dá:

$$(9) \quad \frac{q^M-1}{q-1} = \sum_{i=1}^{M} q^{M-i} \quad .$$

e) <u>Número de retas de cada plano do</u> P_N.

Baseados na observação da definição 5, temos que cada par de pontos determina uma reta, donde

$$(10) \quad \frac{A_{q^2+q+1,2}}{A_{q+1,2}} = \frac{(q^2+q+1)(q^2+q)}{(q+1)q} = q^2+q+1.$$

f) <u>Número de retas do</u> P_N.

Anàlogamente ao caso e), vem

$$(11) \quad \frac{A_{\sum_{i=0}^{N} q^{N-i},2}}{A_{q+1,2}} = \frac{\left(\sum_{i=0}^{N} q^{N-i}\right)\left(\sum_{i=0}^{N-1} q^{N-i}\right)}{q(q+1)} = \frac{\frac{q^{N+1}-1}{q-1} \cdot \frac{q^N-1}{q-1}}{q+1} =$$

$$= \frac{(q^{N+1}-1)(q^N-1)}{(q^2-1)(q-1)} \quad .$$

g) <u>Número de</u> P_M <u>do</u> P_N. [32,pag.327]

O P_M é determinado por um P_{M-1} e um ponto $P \notin P_{M-1}$; anàlogamente, P_{M-i} é determinado por um P_{M-i-1} e um ponto $Q \notin P_{M-i-1}$. Começando-se por $i = M-1$, temos a escolha de um ponto P_o, feita de $\sum_{i=0}^{N} q^{N-i}$ maneiras; a seguir, um ponto $Q \neq P$ para determinar P_1 e que é de $\sum_{i=0}^{N-1} q^{N-i}$ modos; finalmente, um (M+1)º ponto não pertencente a P_{M-1}, de $\sum_{i=0}^{N-M} q^{N-i}$ modos. Daí inferimos:

$$\prod_{h=0}^{M}\left(\sum_{i=0}^{N-h} q^{N-i}\right)$$ modos de escolher os M+1 pontos do P_M.

Como quaisquer M+1 pontos do P_M, nas condições da definição determinam o mesmo P_M, concluimos que devemos dividir o número obtido por $\prod_{h=0}^{M}\left(\sum_{i=0}^{h} q^{M-i}\right)$, donde

(12)
$$\prod_{h=0}^{M}\left(\frac{\sum_{i=0}^{N-h} q^{N-i}}{\sum_{i=0}^{N-h} q^{M-i}}\right) = \frac{(q^{N+1}-1)(q^{N}-1)\ \dots\ (q^{N-M+1}-1)}{(q^{M+1}-1)(q^{M}-1)\ \dots\ (q-1)}$$

Observação: Por g) vê-se que o número de hiperplanos P_{N-1} de P_N é dado por

$$(13)\qquad \frac{(q^{N+1}-1)(q^{N}-1)\ \dots\ (q^{N-N+1+1}-1)}{(q^{N}-1)(q^{N-1}-1)\ \dots (q^{2}-1)(q-1)} = \frac{q^{N+1}-1}{q-1}$$

que é igual ao número de pontos do P_N.

De um modo mais geral, o número de P_K de P_N é igual ao número de P_{N-1-k} de P_N. Com efeito, temos:

$$(14)\qquad \text{Nº de } P_K = \frac{(q^{N+1}-1)(q^{N}-1)\ \dots\ (q^{N-k+1}-1)}{(q^{k+1}-1)(q^{k}-1)\ \dots\ (q-1)}$$

$$(15)\qquad \text{Nº de } P_{N-1-k} = \frac{(q^{N+1}-1)(q^{N}-1)\ \dots\ (q^{N-N+1+k+1}-1)}{(q^{N-1-k+1}-1)(q^{N-1-k}-1)\dots(q-1)} =$$

$$= \frac{(q^{N+1}-1)(q^{N}-1)\ \dots\ (q^{N-k+1}-1)}{(q^{k+1}-1)\dots\ (q-1)}\ .$$

3. TEOREMA 1. Todos os pontos (x_i) de um P_{N-1} satisfazem a uma equação

$$(16)\qquad \sum_{i=0}^{N} A_i x_i = 0\ ,$$

onde os $A_i \in K$ e não são todos nulos; reciprocamente, o conjunto de todos os pontos do P_N que satisfazem a uma equação (16) é um P_{N-1}.

Seja o hiperplano

(17) $$x_i = \lambda_o y_i^o + \dots + \lambda_{N-1} y_i^{N-1}$$

e provemos que os x_i satisfazem a uma equação do tipo (16).

Com efeito, o determinante

(18) $$\begin{vmatrix} x_i \\ y_i^o \\ \vdots \\ y_i^{N-1} \end{vmatrix}$$

é nulo, por (17), donde, desenvolvido segundo os elementos da primeira linha, nos dá:

(19) $$\sum_{i=0}^{N} A_i x_i = 0 \quad .$$

Os A_i não são todos nulos, pois se tal acontecesse, a matriz

(20) $$\begin{pmatrix} y_i^o \\ y_i^1 \\ \vdots \\ y_i^{N-1} \end{pmatrix}$$

teria característica $< N$, e, então, seria, por exemplo,

(21) $$y_i^o = \sum_{s=1}^{N-1} k_s y_i^s$$

e os N pontos estariam num espaço de dimensão $< N-1$, contra a hipótese inicial.

<u>Reciprocamente</u>, seja a equação

(22) $$\sum_{i=0}^{N} A_i x_i = 0$$

com os $A_i \in K$ e não todos nulos.

Suposto $A_o \neq 0$, tomemos N pontos, que satisfaçam (22), a saber:

$$(23) \qquad \begin{array}{l} \left(-\frac{A_1}{A_o}, 1, 0, 0, \ldots, 0\right) \\ \left(-\frac{A_2}{A_o}, 0, 1, 0, \ldots, 0\right) \\ \quad\vdots \\ \left(-\frac{A_N}{A_o}, 0, 0, 0, \ldots, 1\right) . \end{array}$$

Seja a reta definida pelos dois primeiros pontos:

$$(24) \qquad \begin{cases} x_o = -\sigma\frac{A_1}{A_o} - \rho\frac{A_2}{A_o} \\ x_1 = \sigma \\ x_2 = \rho \\ x_i = 0 \quad (i \geqq 3) . \end{cases}$$

O terceiro ponto não pertence a essa reta (24) e define com ela um plano:

$$(25) \qquad \begin{cases} x_o = -\sigma\frac{A_1}{A_o} - \rho\frac{A_2}{A_o} - \tau\frac{A_3}{A_o} \\ x_1 = \sigma \\ x_2 = \rho \\ x_3 = \tau \\ x_i = 0 \quad (i \geqq 4) . \end{cases}$$

O quarto ponto não estando nesse plano (25) define com êle um P_3 e assim sucessivamente, chegaremos a um hiperplano:

$$(26)\quad \begin{cases} x_0 = -\sigma_1 \dfrac{A_1}{A_0} - \ \dots\ - \sigma_N \dfrac{A_N}{A_0} \\ x_1 = \sigma_1 \\ x_2 = \qquad \sigma_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ x_N = \qquad\qquad\qquad \sigma_N \end{cases}$$

Resta provar que qualquer ponto de (26) satisfaz à equação (22) e, reciprocamente.

Com efeito, substituindo-se as (26) em (22), teremos:

$$(27)\quad A_0\left(-\sigma_1\frac{A_1}{A_0} - \dots - \sigma_N\frac{A_N}{A_0}\right) + A_1\sigma_1 + \dots + A_N\sigma_N ,$$

que é evidentemente igual a zero.

Tomemos agora um ponto (z_i) de (22), isto é:

$$(28)\qquad A_0 z_0 + A_1 z_1 + \dots + A_N z_N = 0$$

e provemos que existem valores dos σ_i para os quais obtemos (z_i) em (26).

Temos as equações:

$$\begin{cases} -\sigma_1\dfrac{A_1}{A_0} - \ \dots\ - \sigma_N\dfrac{A_N}{A_0} = z_0 \\ \sigma_1 \qquad\qquad\qquad = z_1 \\ \qquad \sigma_2 \qquad\qquad = z_2 \\ \dots\dots\dots\dots\dots\dots\dots \\ \qquad\qquad\qquad \sigma_N = z_N \end{cases}$$

Tomando-se para σ_i os z_i, vemos que, pela hipótese, a primeira das (29) é satisfeita.

Passemos a uma proposição mais geral.

TEOREMA 2. A intersecção de um conjunto finito de hiperplanos de P_N dados por

$$(30)\quad \begin{cases} a_{oo}x_o + \dots + a_{oN}x_N = 0 \\ a_{1o}x_o + \dots + a_{1N}x_N = 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{mo}x_o + \dots + a_{mN}x_N = 0 \end{cases}$$

é um sub-espaço P_r de P_N, se a característica da matriz

$$(31)\quad \begin{pmatrix} a_{oo} & \dots & a_{oN} \\ \dots & \dots & \dots \\ a_{mo} & & a_{mN} \end{pmatrix}$$

fôr N-r.

Com efeito, se a característica fôr N-r, teremos em (31) um menor de ordem N-r, $\neq 0$, que, para facilidade de notação, suponhamos seja

$$(32)\quad \begin{vmatrix} a_{oo} & a_{o1} & \dots & a_{o,N-r-1} \\ a_{1o} & a_{11} & \dots & a_{1,N-r-1} \\ \dots & \dots & \dots & \dots \\ a_{N-r-1,o} & \dots & & a_{N-r-1,N-r-1} \end{vmatrix} \neq 0$$

No sistema de equações

$$(33)\quad \begin{cases} a_{oo}x_o + \dots + a_{o,N-r-1}x_{N-r-1} = -a_{o,N-r}x_{N-r} - \dots - a_{oN}x_N \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{N-r-1,o}x_o + \dots + a_{N-r-1,N-r-1}x_{N-r-1} = \\ \qquad = -a_{N-r-1,N-r}x_{N-r} - \dots - a_{N-r-1,N}x_N \end{cases}$$

escolhemos arbitràriamente os valores de x_i $(i=N-r,\dots,N)$ e determinamos os $x_o,\dots,x_{N-r-1}$. Tomando-se para x_i $(i=N-r,\dots,N)$, os valores:

$$(34)\quad \begin{matrix} (1,0,\dots,0) \\ (0,1,\dots,0) \\ \dots\dots\dots \\ (0,0,\dots,1) \end{matrix}$$

teremos os vectores-soluções do sistema (30):

$$(35)\qquad \begin{cases} x_0^0 & x_1^0 & \dots & x_{N-r-1}^0 & 1 & 0 & \dots & 0 \\ x_0^1 & x_1^1 & \dots & x_{N-r-1}^1 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ x_0^r & x_1^r & & x_{N-r-1}^r & 0 & 0 & \dots & 1 \end{cases}$$

que são <u>linearmente</u> <u>independentes</u>, pois a matriz $(r+1)\times(N+1)$ formada com (35) tem característica r+1, como é fácil ver.

Devemos mostrar que qualquer combinação linear dos r+1 pontos

$$(36)\qquad (x_0^h \quad x_1^h \dots x_{N-r-1}^h \; 0 \dots \overset{h}{1} \dots 0)$$

é solução do sistema (30), e, reciprocamente, qualquer solução do sistema (30) é combinação linear dos r+1 pontos (36).

Sejam as combinações lineares

$$(37)\qquad \begin{cases} X_0 = \lambda_0 x_0^0 + \lambda_1 x_0^1 + \dots \lambda_r x_0^r \\ X_1 = \lambda_0 x_1^0 + \lambda_1 x_1^1 + \dots \lambda x_1^r \\ \dots\dots\dots\dots\dots\dots \\ X_{N-r-1} = \lambda_0 x_{N-r-1}^0 + \lambda_1 x_{N-r-1}^1 + \dots \\ \qquad\qquad \dots + \lambda_r x_{N-r-1}^r \\ X_{N-r} = \lambda_0 \\ X_{N-r-1} = \qquad \lambda_1 \\ \dots\dots\dots\dots\dots\dots \\ X_N = \qquad\qquad \lambda_r \end{cases}$$

Verifiquemos que é solução de uma equação de (30), i.e.:

$$a_{00}X_0 + a_{01}X_1 + \dots + a_{0,N-r-1}X_{N-r-1} + a_{0,N-r}X_{N-r} + \dots$$
$$\dots + a_{0N}X_N =$$

$$= \lambda_o(a_{oo}x_o^o + a_{o1}x_1^o + \dots + a_{o,N-r-1}x_{N-r-1}^o + a_{o,N-r}) +$$

$$+ \lambda_1(a_{oo}x_o^1 + \dots + a_{o,N-r-1}x_{N-r-1}^1 + a_{o,N-r}) + \dots$$

$$\dots + \lambda_r(a_{oo}x_o^r + \dots + a_{o,N-r-1}x_{N-r-1}^r + a_{o,N-r})$$

é igual a zero, pois as expressões entre parênteses são nulas, por hipótese.

Anàlogamente, pode ser feito com as demais equações.

Recìprocamente, seja a solução do sistema (30)

(38) $$(y_o \quad y_1 \quad \dots \quad y_N)$$

e vamos mostrar que existem valores de λ_i em (37), que permitem encontrar (38).

Como se sabe da teoria das equações [31 - vol.I], o vector solução $\vec{Y}$ é combinação linear dos (35), donde o teorema está provado.

---o---

§ 2º - ESPAÇO PROJETIVO

1. Vamos verificar que o nosso espaço P_N é projetivo, i.e., os seus elementos satisfazem aos postulados de Veblen [3-pags.241,242]:

I_V) Dados os pontos A e B ($A \neq B$), há uma e uma só reta que contém ambos A e B.

II_V) Se os pontos A, B, C não pertencem a u'a mesma reta, e se uma reta r contém um ponto de AB e um ponto de AC, então, r e BC se cortam.

III_V) Se $M < N$, há pontos em P_N que não estão em P_M.

IV_V) Cada reta contém, pelo menos, três pontos.

V_V) Não há ponto que não pertença ao P_N.

Diante das definições, considerações e cálculos do § 1º, os postulados I_V, III_V, IV_V e V_V são imediatos. Examinemos, então, o postulado II_V.

Sejam os pontos $A \equiv (v_i)$, $B \equiv (y_i)$ e $C \equiv (z_i)$.

Consideremos a reta AB:

(1) $$x_i = \lambda_o v_i + \lambda_1 y_i \qquad (i=0,\dots,N)$$

e o ponto $D \in AB$, dado por

(2) $$a_i = \rho_o v_i + \rho_1 y_i \ .$$

Na reta BC

(3) $$x_i = \nu_o y_i + \nu_1 z_i ,$$

seja o ponto E dado por

(4) $$b_i = \sigma_o y_i + \sigma_1 z_i \ .$$

Suponhamos que a reta DE não passe por A e C, senão a propriedade está provada.

A reta DE é dada por:

(5) $$x_i = \tau_o a_i + \tau_1 b_i \ .$$

Substituindo-se (2) e (4) em (5), vem:

(6) $$x_i = \tau_o(\rho_o v_i + \rho_1 y_i) + \tau_1(\sigma_o y_i + \sigma_1 z_i) =$$

$$= \tau_o \rho_o v_i + (\tau_o \rho_1 + \tau_1 \sigma_o) y_i + \tau_1 \sigma_1 z_i \ .$$

Tomando-se em (5) τ_o e τ_1 não todos nulos, tais que

$$\tau_o \rho_1 + \tau_1 \sigma_o = 0 ,$$

ou seja

$$\tau_o = \sigma_o \qquad \text{e} \qquad \tau_1 = -\rho_1 ,$$

temos

(8) $$x_i = \sigma_o \rho_o v_i - \sigma_1 \rho_1 z_i ,$$

que é um ponto de AC.

---o---

§ 3º - ESPAÇO VECTORIAL ASSOCIADO AO P_N

1. Consideremos tôdas as (N+1)-uplas e demos as seguintes definições:

a) Dadas duas (N+1)-uplas $(x_0,x_1,\ldots,x_N)$ e $(y_0,y_1,\ldots,y_N)$, soma das duas é a (N+1)-upla

$$(x_0+y_0,\ x_1+\ y_1,\ \ldots,\ x_N+y_N)\ .$$

b) Produto escalar de um elemento $\alpha\in K$ pela (N+1)-upla $(x_0,x_1,\ldots,x_N)$ é a (N+1)-upla

$$(\alpha x_0,\alpha x_1,\ \ldots,\alpha x_N)\ .$$

Com estas definições, é fácil ver que o conjunto de tôdas as (N+1)-uplas é um espaço vectorial V_{N+1} sôbre o corpo K [37-pags.7,8; 38-pags.167,168].

Associemos a cada vector $(x_0,x_1,\ldots,x_N)$ não nulo de V_{N+1}, o ponto do P_N, definido pela classe de equivalência da qual um representante é a (N+1)-upla dada pelo vector. É claro que a cada vector não nulo do V_{N+1} corresponde um e um só ponto do P_N.

Por outro lado, cada ponto $(x_0,x_1,\ldots,x_N)$ do P_N provém do conjunto V_1^* dos vectores $\lambda(x_0,x_1,\ldots,x_N)$, com $\lambda\in K^*$.

Há, então, correspondência biunívoca entre os pontos de P_N e os conjuntos V_1^* de V_{N+1}.

DEFINIÇÃO 1. Chamamos V_{N+1} de espaço vectorial associado ao espaço projetivo P_N. [34-vol.II,pags.142,143]

DEFINIÇÃO 2. Se $Q\equiv(x_0,x_1,\ldots,x_N)$ é um ponto do P_N, cada um dos vectores

$$\lambda\vec{X}=(\lambda x_0,\lambda x_1,\ldots,\lambda x_N)\qquad(\lambda\in K^*)$$

do V_{N+1} é denominado vector-coordenada de Q [31-vol.II, pag.143].

TEOREMA 1. O conjunto de todos os vectores-coordenadas dos pontos de um $P_r\subset P_N$ mais o vector nulo é um

$V_{r+1} \subset V_{N+1}$.

Reciprocamente, o conjunto de todos os pontos cujos vectores-coordenadas pertencem a um mesmo $V_{r+1} \subsetneq V_{N+1}$, constitue um $P_r \subset P_N$ [31-vol.II,pag.144].

Seja um $P_r \subsetneq P_N$ dado por

$$(1) \qquad x_i = \sum_{s=0}^{r} \lambda_s y_i^s \qquad (i=o,\dots,N) .$$

É fácil ver que: a) os r+1 vectores-coordenadas $\vec{a} \equiv (y_i^s)$ para $s=0,\dots,r$ são linearmente independentes; b) quaisquer r+2 vectores-coordenadas dos pontos de P_r são linearmente dependentes.

a) Com efeito se os $\vec{a}_s$ fôssem linearmente dependentes, então, haveria a relação

$$(2) \qquad \sum_{s=0}^{r} \alpha_s \vec{a}_s = 0 ,$$

com os α_s não todos nulos; então, suposto $\alpha_o \neq 0$, teríamos:

$$(3) \qquad \vec{a}_o = \sum_{i=1}^{r} \beta_i \vec{a}_i ,$$

com $\beta_i = -\dfrac{\alpha_i}{\alpha_o}$ $(i=1,\dots,r)$.

De (3), decorreria para as componentes:

$$(4) \qquad y_j^o = \sum_{i=1}^{r} \beta_i y_j^i ,$$

e o ponto (y_j^o) pertenceria ao espaço P_{r-1} dos demais, contrariando a definição de P_r.

b) Se houvesse r+2 vectores-coordenadas $\vec{b}_s$ $(s=0,\dots,r+2)$ linearmente independentes, então, pela (1), teríamos:

(5) $$\vec{b}_s = \sum_{i=0}^{r} \lambda_i^s \vec{a}_i \qquad (s=0,\ldots,r+1)$$

Os r+2 vectores, então, pertencem ao mesmo espaço V_{r+1}, gerado pelos $\vec{a}_s$, logo não podem ser linearmente independentes.

Disto inferimos que qualquer vector-coordenada de pontos de P_r pertence ao V_{r+1} gerado pelos $\vec{a}_s$ e qualquer vector de V_{r+1}, exceto o vector nulo, é vector-coordenada de um ponto de P_r.

Recíprocamente, escolhamos entre os vectores de V_{r+1}, r+1 linearmente independentes $\vec{a}_s \equiv (y_i^s)$ para s = o,...,r, formando uma base de V_{r+1}.

Todos os vectores de V_{r+1} são da forma:

(6) $$(x_i) = \left(\sum_{s=0}^{r} \lambda_s y_i^s\right).$$

Os r+1 pontos (y_i^s) não pertencem a um mesmo P_{r-1}, senão, teríamos, por exemplo,

(7) $$y_i^o = \sum_{s=1}^{r} \mu_s y_i^s$$

e os vectores $\vec{a}_s$ seriam linearmente dependentes.

Concluimos que todos os pontos (x_i) constituem um mesmo $P_r \subset P_N$.

DEFINIÇÃO 3. Dados o P_r e o V_{r+1} correspondente, cada um é associado do outro.

TEOREMA 2. Se a V_{r+1} corresponde um P_r, a V_{s+1} um P_s, e se $P_r \subset P_s$, então, $V_{r+1} \subset V_{s+1}$. Recíprocamente, de $V_{r+1} \subset V_{s+1}$ segue-se $P_r \subset P_s$.

Seja $P_r \subset P_s$. Como $r < s$, podemos indicar os pontos de P_r e P_s, respectivamente por:

$$(8) \qquad x_i = \sum_{m=0}^{r} \lambda_m y_i^m \qquad (i=0,\ldots,N)$$

e

$$(9) \qquad x_i = \sum_{m=0}^{s} \lambda_m y_i^m \qquad (i=0,\ldots,N) .$$

Os vectores-coordenadas dos pontos de P_r são, então, combinações lineares dos vectores $\vec{a}_m \equiv (y_i^m)$, $m = 0,\ldots,r$, que pertencem ao V_{s+1}, donde, todo vector de V_{r+1} pertence ao V_{s+1}, i.e., $V_{r+1} \subset V_{s+1}$.

Recìprocamente, se $V_{r+1} \subset V_{s+1}$, então, tomadas as bases de V_{r+1} e V_{s+1} respectivamente:

$$\vec{a}_m \equiv (y_i^m) \quad (m=0,\ldots,r) \qquad \text{e} \qquad \vec{a}_m \equiv (y_i^m) \quad (m=0,\ldots,s),$$

temos que os pontos de P_r e P_s são dados por:

$$(10) \qquad x_i = \sum_{m=0}^{r} \lambda_m y_i^m$$

e $\qquad (i=0,\ldots,N)$

$$(11) \qquad x_i = \sum_{m=0}^{s} \lambda_m y_i^m .$$

Os pontos de P_r são obtidos dos de P_s, para $\lambda_m = 0$ $(m = r+1,\ldots,s)$, logo $P_r \subset P_s$.

Dêste teorema, segue-se a unicidade do espaço vectorial associado ao projetivo, e recìprocamente; justificando-se, também, a definição 3.

---o---

§4º - DEPENDÊNCIA LINEAR E CONSEQUÊNCIAS.

1\. DEFINIÇÃO 1. Sejam os pontos $A_j \equiv (x_i^j)$ para $j = 0,1,\ldots k$ do P_N. Dizemos que os A_j são linearmente independentes (ou dependentes), quando e sòmente quando os vectores-coordenadas de A_j $(j = 0,\ldots,k)$ são linearmente independentes (ou dependentes) [31 - vol. II, pag. 144].

É essencial mostrar que a definição não depende do conjunto particular de vectores-coordenadas dos pontos.

Sejam os k+1 pontos $Q_0 \equiv (y_i)$, $Q_1 \equiv (z_i),\ldots,Q_k \equiv (v_i)$. Os vectores coordenadas são $\vec{a}_0 \equiv (y_i)$, $\vec{a}_1 \equiv (z_i),\ldots,$ $\vec{a}_k \equiv (v_i)$, ou $\vec{b}_0 \equiv (h_0 y_i)$, $\vec{b}_1 \equiv (h_1 z_i),\ldots,$ $\vec{b}_k \equiv (h_k v_i)$, com $h_i \in K^*$.

TEOREMA 1. Se os $\vec{a}_i$ são linearmente dependentes (ou independentes), o mesmo acontece com os $\vec{b}_i$ e reciprocamente.

Suponhamos que

$$\sum_{i=0}^{k} \alpha_i \vec{a}_i = 0 \tag{1}$$

com os α_i não todos nulos.

De

$$\sum_{i=0}^{k} \alpha_i \vec{a}_i = \sum_{i=0}^{k} \alpha_i \frac{1}{h_i} \vec{b}_i \quad , \tag{2}$$

segue-se que, para $\beta_i = \dfrac{\alpha_i}{h_i}$, $(i=0,\ldots,k)$,

$$\sum_{i=0}^{k} \beta_i \vec{b}_i = 0 \quad , \tag{3}$$

onde nem todos os β_i são nulos.

Reciprocamente, de (3) e do fato de ser

$$\sum_{i=0}^{k} \beta_i \vec{b}_i = \sum_{i=0}^{k} \beta_i h_i \vec{a}_i \quad , \tag{4}$$

segue-se (1), o que prova a afirmação.

É fácil ver, por absurdo, o que acontece no caso da independência.

DEFINIÇÃO 2. Um ponto (x_i) é combinação linear dos pontos (y_i^s) $(s=0,\dots,k)$, se tal acontece com os vectores-coordenadas $\vec{X}\equiv(x_i)$ e $\vec{a}_s\equiv(y_i^s)$.

DEFINIÇÃO 3. Chama-se <u>espaço-união</u> de um conjunto de pontos Q_i a um espaço P_q tal que:

a) Se P_r contém todos os Q_i, $P_q \subset P_r$;

b) nenhum espaço P_{q-1} $(i \geq 1)$ contém todos os Q_i.

É fácil ver que o espaço-união contém tôdas as combinações lineares dos Q_i e, portanto, os sub-espaços por êles determinados.

DEFINIÇÃO 4. O espaço-união de dois espaços P_r e P_s é o é o espaço-união da reunião $P_r \cup P_s$ [35 - pag.5].

<u>Observação</u>. a) Dois pontos coincidentes são linearmente dependentes e vice-versa; b) dois pontos distintos são linearmente independentes e vice-versa; c) r+1 pontos linearmente dependentes pertencem a um mesmo sub-espaço P_{r-i} $(i \geq 1)$ e vice-versa; d) r+1 pontos linearmente independentes pertencem a um mesmo P_r e não a um P_{r-i} $(i \geq 1)$ e vice-versa.

TEOREMA 2. A intersecção [35-pag.5] dos conjuntos dos pontos de dois sub-espaços P_r e P_q, não sendo vazia, é um sub-espaço.

Consideremos os espaços vectoriais associados V_{r+1} e V_{q+1}, com

$$V_{r+1} \cap V_{q+1} = V_{h+1} .$$

Então, V_{h+1} é um espaço vectorial associado de um P_h, que vamos provar ser $P_r \cap P_q$.

Primeiramente, vemos que, como $V_{h+1} \subset V_{r+1}$ e $V_{h+1} \subset V_{q+1}$, então, pelo teorema 2 do §3º, segue-se que $P_h \subset P_r$ e $P_h \subset P_q$, donde $P_h \subset P_r \cap P_q$.

Por outro lado, considerado um ponto $P \in P_r \cap P_q$, temos que $P \in P_r$ e $P \in P_q$, donde o vector-associado de P pertence a V_{r+1} e a V_{q+1} e, portanto, a $V_{r+1} \cap V_{q+1} = V_{h+1}$. Pelo teorema 2, do § 3º, temos que $P \in P_h$, logo $P_r \cap P_q \subset P_h$.

Concluimos, assim, que $P_h = P_r \cap P_q$.

No caso em que $P_r \cap P_q = \emptyset$, então, $V_{r+1} \cap V_{q+1}$ se reduz ao vector nulo.

TEOREMA 3. Se P_i é a intersecção $P_{r_1} \cap P_{r_2}$ de dois sub-espaços, P_u o espaço-união de $P_{r_1} \cup P_{r_2}$, então vale a relação

$$r_1 + r_2 = i + u ,$$

entendendo-se, para $i = -1$, o caso de $P_{r_1} \cap P_{r_2} = \emptyset$ [31-vol.II, pags.145,146 e 147].

Sejam V_{r_1+1} e V_{r_2+1} os espaços vectoriais associados. Chamemos $I = V_{r_1+1} \cap V_{r_2+1}$ e U a <u>soma</u> [31-vol.I;38,pag.170], $V_{r_1+1} + V_{r_2+1}$.

Suponhamos que as dimensões de I e U sejam i' e u'.

Se I não fôr o V_o, então, é associado de um espaço $P_{i'-1}$. Por outro lado, U é associado de um espaço $P_{u'-1}$.

Pelo teorema anterior, $P_{i'-1} = P_{r_1} \cap P_{r_2}$ e, portanto, $i = i' - 1$.

Provemos que o espaço-união P_u de P_{r_1} e P_{r_2} é o associado de U.

Chamando P ao espaço associado de U, e levando em conta que todo vector de U é da forma $\vec{a}_1 + \vec{a}_2$, onde $\vec{a}_1 \in V_{r_1+1}$ e $\vec{a}_2 \in V_{r_2+1}$, temos que $V_{r_1+1} \subset U$ e $V_{r_2+1} \subset U$, donde $P_{r_1} \subset P$ e $P_{r_2} \subset P$ (teorema 2, do § 3º).

Seja P' um espaço que contenha P_{r_1} e P_{r_2}; então, o espaço vectorial V, associado de P' contém V_{r_1+1} e V_{r_2+1} (teorema 2, § 3º), logo, contém o vector $\vec{a}_1 + \vec{a}_2$, donde $V \supset U$ e, daí, $P' \supset P$.

Por outro lado, nenhum espaço P" de dimensão menor que a de P' contém $P_{r_1} \cup P_{r_2}$, pois se tal acontecer, então, o espaço vectorial V" associado de P" estará contido em U, o que é absurdo.

Concluimos assim, que P é o espaço-união de P_{r_1} e P_{r_2} e, então, é $P \equiv P_u$. Como U é associado de P_u, então, $u = u'-1$.

Pelo teorema da dimensão de espaço vectorial [38-pags.179, 180], temos:

(5) $$r_1 + 1 + r_2 + 1 = i' + u' \ ,$$

ou

(6) $$r_1 + 1 + r_2 + 1 = i + 1 + u + 1 \ ,$$

ou ainda

(7) $$r_1 + r_2 = i + u \ ,$$

o que prova o teorema.

No caso em que $I = V_0$, então, vem na (5):

(8) $$r_1 + 1 + r_2 + 1 = 0 + u' = u'$$

ou

$$r_1 + 1 + r_2 + 1 = u + 1 \ ,$$

ou seja,

(9) $$r_1 + r_2 = u - 1 \ .$$

Vemos assim que a (7) é verdadeira nesse caso, para $i = -1$.

2. DEFINIÇÃO 5. O conjunto de r+1 pontos linearmente independentes e dos espaços P_i $(i < r)$ determinados por êles chama-se <u>simplexo</u> <u>r-dimensional</u>.

Vamos calcular o <u>número de simplexos r-dimensionais de um sub-espaço P_r do P_N</u>.

O simplexo da reta é dado por dois pontos distintos; então, no P_1 temos

$$(10) \qquad C_{q+1,2} = \frac{q(q+1)}{2} \qquad \frac{(q^2-1)(q^2-q)}{2!(q-1)^2}$$

simplexos distintos uni-dimensionais S_1.

No P_N, temos o produto de

$$\frac{(q^{N+1}-1)(q^N-1)}{(q^2-1)(q-1)} \quad (\text{nº de retas do } P_N) \quad \text{por}$$

$$\frac{q(q+1)}{2} \quad \text{simplexos do } P_1,$$

isto é,

$$(11) \qquad \frac{(q^{N+1}-1)(q^N-1)q\cancel{(q+1)}}{2\cancel{(q+1)}(q-1)(q-1)} = \frac{1}{2}\cdot\frac{(q^{N+1}-1)(q^{N+1}-q)}{(q-1)^2}$$

simplexos S_1.

No P_2, o simplexo é um triângulo e a escolha é dada pelo produto de

$$\frac{q^3-1}{q-1} \quad (\text{nº de pontos do } P_2) \quad \text{por}$$

$$\frac{q^3-q}{q-1} \quad (\text{nº de pontos do } P_2 \text{ distintos de um dado ponto}) \quad \text{por}$$

$$\frac{q^3-1}{q-1} - \frac{q^2-1}{q-1} \quad (\text{nº de pontos do } P_2 \text{ fora de uma reta dada})$$

dividido pelo número de permutações dos três vértices, isto é:

$$(12) \qquad \frac{(q^3-1)(q^3-q)(q^3-q^2)}{3!\ (q-1)^3} \qquad \text{simplexos } S_2.$$

No P_N, temos o produto de

$$\frac{(q^{N+1}-1)(q^N-1)(q^{N-1}-1)}{(q^3-1)(q^2-1)(q-1)} \quad (\text{nº de } P_2 \text{ do } P_N) \quad \text{por}$$

$$\frac{(q^3-1)(q^3-q)(q^3-q^2)}{3!\ (q-1)^3} \qquad \text{simplexos do } P_2,$$

isto é:

$$(13) \qquad \frac{(q^{N+1}-1)(q^N-1)(q^{N-1}-1)(q^3-1)(q^3-q)(q^3-q^2)}{3!\ (q-1)^3(q^3-1)(q^2-1)(q-1)} =$$

$$= \frac{(q^{N+1}-1)(q^{N+1}-q)(q^{N+1}-q\ \ )(q^3-1)(q^2-1)(q-1)}{3!\ (q-1)^3(q^3-1)(q^2-1)(q-1)} =$$

$$= \frac{(q^{N+1}-1)(q^{N+1}-q)(q^{N+1}-q^2)}{3!\ (q-1)^3}$$

No P_r, o número de simplexos S_r é dado pelo produto de

$\dfrac{q^{r+1}-1}{q-1}$ (nº de pontos do P_r) por

$\dfrac{q^{r+1}-q}{r-1}$ (nº de pontos distintos de um dado ponto do P_r), por

$\dfrac{q^{r+1}-q^2}{r-1}$ (nº de pontos fora de um $P_1 \subset P_r$) por

$\dfrac{q^{r+1}-q^r}{r-1}$ (nº de pontos fora de um $P_{r-1} \subset P_r$)

dividido pelo nº $(r+1)!$ de permutações dos r+1 pontos, i.e.,

$$(14) \qquad \prod_{i=0}^{r} \frac{q^{r+1}-q^i}{(r+1)!(q-1)^{r+1}} .$$

Finalmente, no P_N, o número de simplexos S_r é dado pelo produto de

$$\frac{(q^{N+1}-1)(q^N-1)\ \ldots\ (q^{N-r+1}-1)}{(q^{r+1}-1)(q^r-1)\ \ldots\ (q-1)} \qquad (\text{nº de } P_r \text{ do } P_N), \text{ por}$$

$$\frac{(q^{r+1}-1)(q^{r+1}-q)\ \ldots\ (q^{r+1}-q^r)}{(r+1)!(q-1)^{r+1}} \quad , \text{ isto é,}$$

$$\frac{(q^{N+1}-1)(q^N-1)\ \ldots\ (q^{N-r+1}-1)(q^{r+1}-1)(q^{r+1}-q)\ \ldots\ (q^{r+1}-q^r)}{(r+1)!(q-1)^{r+1}(q^{r+1}-1)(q^r-1)\ \ldots\ (q-1)} =$$

$$= \frac{(q^{N+1}-1)(q^{N+1}-q)\ \ldots\ (q^{N+1}-q^r)(q^{r+1}-1)(q^r-1)\ \ldots\ (q-1)}{(r+1)!(q-1)^{r+1}(q^{r+1}-1)(q^r-1)\ \ldots\ (q-1)} =$$

$$= \frac{(q^{N+1}-1)(q^{N+1}-q)\ \ldots\ (q^{N+1}-q^r)}{(r+1)!(q-1)^{r+1}} \quad ,$$

ou seja:

$$(15) \qquad \frac{1}{(r+1)!(q-1)^{r+1}} \prod_{i=0}^{r} (q^{N+1}-q^i) \quad \text{simplexos } S_r \text{ no } P_N.$$

3. Vamos agora calcular o número de pares de sub-espaços do P_N, cuja intersecção é um sub-espaço dado [34-pags.176,177].

A escolha, no P_N, de um sub-espaço P_r pode ser feita de

$$(16) \qquad \frac{(q^{N+1}-1)(q^N-1)\ \ldots\ (q^{N-r+1}-1)}{(q^{r+1}-1)(q^r-1)\ \ldots\ (q-1)}$$

modos diferentes, conforme § 1º, 2, g).

Anàlogamente, a escolha de um P_d num P_r $(d \leqq r)$ pode ser de

$$(17) \qquad \frac{(q^{r+1}-1)(q^{r+1}-1)\ \ldots\ (q^{r-d+1}-1)}{(q^{d+1}-1)(q^d-1)\ \ldots\ (q-1)}$$

maneiras diferentes.

Procuremos um P_s em P_N tal que $P_r \cap P_s = P_d$.

Comecemos por tomar um ponto $Q_1 \in P_N$ tal que $Q_1 \notin P_r$, o que se pode fazer de

$$(18) \quad \frac{q^{N+1}-1}{q-1} - \frac{q^{r+1}-1}{q-1} = \frac{q^{N+1}-q^{r+1}}{q-1} = \frac{q^{r+1}(q^{N-r}-1)}{q-1}$$

maneiras.

A seguir, tomemos $Q_2 \in P_N$, com $Q_2 \notin P_{r+1}$, onde P_{r+1} é o espaço-união de Q_1 e P_r. Isto pode ser de

$$(19)\qquad \frac{q^{N+1}-1}{q-1} - \frac{q^{r+2}-1}{q-1} = \frac{q^{r+2}(q^{N-r-1}-1)}{q-1} = \frac{q^{N+1}-q^{r+2}}{q-1}$$

modos.

Assim, sucessivamente, até chegarmos à escolha de um ponto $Q_{s-d} \in P_N$, com $Q_{s-d} \notin P_{r+s-d-1}$, onde $P_{r+s-d-1}$ é o espaço-união de $Q_1, Q_2, \ldots, Q_{s-d-1}$ e P_r, o que pode ser de

$$(20)\qquad \frac{q^{N+1}-1}{q-1} - \frac{q^{r+s-d}-1}{q-1} = \frac{q^{r+s-d}(q^{N-r-s+d+1}-1)}{q-1} = \frac{q^{N+1}-q^{r+s-d}}{q-1}$$

maneiras diversas.

Por outro lado, dados os sub-espaços P_r e P_s que se cortam em P_d, o ponto Q_1 pode ser escolhido em P_s e fora de P_d, de

$$(21)\qquad \frac{q^{s+1}-1}{q-1} - \frac{q^{d+1}-1}{q-1} = \frac{q^{s+1}-q^{d+1}}{q-1} = \frac{q^{d+1}(q^{s-d}-1)}{q-1}$$

modos diferentes.

O ponto Q_2 no P_s e fora de P_{d+1}, união de P_d e Q_1, pode ser escolhido de

$$(22)\qquad \frac{q^{s+1}-1}{q-1} - \frac{q^{d+2}-1}{q-1} = \frac{q^{s+1}-q^{d+2}}{q-1} = \frac{q^{d+2}(q^{s-d-1}-1)}{q-1}$$

processos diversos.

Sucessivamente, o $Q_{s-d} \in P_s$ e $Q_{s-d} \notin P_{d+s-d-1} = P_{s-1}$, união de $P_d, Q_1, Q_2, \ldots, Q_{s-d-1}$ pode ser escolhido de

$$(23)\qquad \frac{q^{s+1}-1}{q-1} - \frac{q^{s}-1}{q-1} = \frac{q^{s+1}-q^{s}}{q-1} = \frac{q^{s}(q-1)}{q-1} = q^{s}$$

maneiras diferentes.

O número de possibilidades da escolha de P_r e P_s, tal que $P_r \cap P_s = P_d$, é dado pelo produto das expressões (16), (17), (18), (19), (20), dividido pelo produto das expressões (21), (22) e (23), isto é:

$$\frac{\dfrac{(q^{N+1}-1)\cdots(q^{N-r+1}-1)}{(q^{r+1}-1)\cdots(q-1)}\cdot\dfrac{(q^{r+1}-1)\cdots(q^{r-d+1}-1)}{(q^{d+1}-1)\cdots(q-1)}\cdot\dfrac{(q^{N+1}-q^{r+1})}{q-1}\cdot\dfrac{q^{N+1}-q^{r+2}}{q-1}\cdots\dfrac{q^{N+1}-q^{r+s-d}}{q-1}}{\dfrac{q^{s+1}-q^{d+1}}{q-1}\cdot\dfrac{q^{d+1}-q^{d+2}}{q-1}\cdot\ \cdots\ \cdot\dfrac{q^{s+1}-q^{s}}{q-1}} =$$

$$= \frac{\dfrac{(q^{N+1}-1)\cdots(q^{N-r+1}-1)(q^{r+1}-1)\cdots(q^{r-d+1}-1)q^{r+1}(q^{N-r}-1)q^{r+2}(q^{N-r-1}-1)q^{r+s-d}(q^{N-r-s+d+1}-1)}{(q^{r+1}-1)\cdots(q-1)(q^{d+1}-1)\cdots(q-1)(q-1)^{s-d}}}{\dfrac{q^{d+1}(q^{s-d}-1)q^{d+2}(q^{s-d-1}-1)\cdots q^{s}(q-1)}{(q-1)^{s-d}}} =$$

$$= \frac{\dfrac{q^{(r+1)+(r+2)+\cdots+(r+s-d)}\prod_{i=0}^{r}(q^{N+1-i}-1)\prod_{i=0}^{s-d-1}(q^{N-r-i}-1)}{\prod_{i=0}^{r}(q^{r+1-i}-1)\prod_{i=0}^{d}(q^{d+1-i}-1)}}{q^{(d+1)+(d+2)+\cdots+(d+s-d)}\prod_{i=0}^{s-d-1}(q^{s-d-i}-1)} =$$

$$= \frac{q^{(s-d)(r-d)}\prod_{i=0}^{r}(q^{N+1-i}-1)\prod_{i=0}^{s-d-1}(q^{N-r-i}-1)}{\prod_{i=0}^{r}(q^{r+d-i}-1)\prod_{i=0}^{d}(q^{d+1-i}-1)\prod_{i=0}^{s-d-1}(q^{s-d-i}-1)} .$$

A expressão final é:

$$(24)\qquad \frac{q^{(s-d)(r-d)}\displaystyle\prod_{i=0}^{r}\frac{q^{N+1-i}-1}{q^{r+d-i}-1}\prod_{i=0}^{s-d-1}\frac{q^{N-r-i}-1}{q^{s-d-i}-1}}{\displaystyle\prod_{i=0}^{d}(q^{d+1-i}-1)}$$

---o---

§ 5º - COORDENADAS PROJETIVAS

1. Tomemos r+1 pontos independentes $Q_0, Q_1, \ldots, Q_r$ em $P_r \subset P_N$ e sejam $\lambda\vec{X}_i$ os vectores-coordenadas dos Q_i.

Um vector-coordenada de um ponto $Q \in P_r$ é dado por

$$(1)\qquad \vec{X} = \sum_{i=0}^{r} \mu_i \vec{X}_i$$

onde os μ_i não são todos nulos.

Consideremos um outro vector-coordenada $\vec{Y}$ de Q. Então, vale

$$(2)\qquad \vec{Y} = \lambda\vec{X} \qquad (\lambda \in K^*)$$

e, também,

$$(3)\qquad \vec{Y} = \sum_{i=0}^{r} \mu_i' \vec{X}_i \ .$$

De (1), (2) e (3), decorre

$$\sum \mu_i' \vec{X}_i = \lambda \sum \mu_i \vec{X}_i$$

ou

$$(4)\qquad \sum (\mu_i' - \lambda\mu_i)\vec{X}_i = 0.$$

Como os vectores $\vec{X}_i$ são linearmente independentes, então, de (4), vem:

(5) $$\mu_i' = \lambda\mu_i \quad (i=0,\ldots,r)$$

Dêste modo, a cada ponto $Q \in P_r$ correspondem $(r+1)$-uplas $(\mu_0,\mu_1,\ldots,\mu_r)$ que diferem entre si por um fator $\lambda \in K^*$, onde os μ_i não são todos nulos [31-vol.II,pag.148].

Recìprocamente, tomemos uma classe de $(r+1)$-uplas $(\mu_0,\mu_1,\ldots,\mu_r)$ que difiram por $\lambda \in K^*$, onde os μ_i não sejam todos nulos. A uma $(r+1)$-upla, corresponde o vector

(6) $$\vec{X} = \sum_{i=0}^{r} \mu_i \vec{X}_i$$

e a uma outra $(\lambda\mu_0,\lambda\mu_1,\ldots,\lambda\mu_r)$ da mesma classe corresponde o vector

(7) $$\vec{Y} = \lambda\sum_{i=0}^{r} \mu_i \vec{X}_i = \lambda\vec{X}$$

Aos vectores $\lambda\vec{X}$ corresponde um só ponto $Q \in P_r$.

Naturalmente, a correspondência biunívoca entre os pontos Q e as classes das $(r+1)$-uplas depende dos pontos Q_i e dos vectores-coordenadas $\vec{X}_i$.

TEOREMA 1. Se $\vec{X}_i$ e $\vec{Y}_i$ são dois sistemas de vectores-coordenadas dos pontos Q_i, de tal modo que as $(r+1)$-uplas de um ponto Q sejam de mesma classe, então, $\vec{Y}_i = \lambda\vec{X}_i$, onde $\lambda \in K^*$ e <u>recìprocamente</u> [31-vol.II,pag.148].

Com efeito, se $\vec{X}_i$ e $\vec{Y}_i$ são dois sistemas de vectores-coordenadas dos pontos Q_i, então,

(8) $$\vec{Y}_i = \lambda_i\vec{X}_i \qquad (\lambda_i \in K^*)$$

Dado Q, vem para os seus vectores-coordenadas, de acôrdo com a hipótese

(9) $$\vec{X} = \sum_{i=0}^{r} \mu_i \vec{X}_i$$

$$\vec{Y} = \sum_{i=0}^{r} \rho\mu_i \vec{Y}_i \qquad (\rho \in K^*)\ .$$

É claro que $\vec{Y} = \lambda\vec{X}$, donde

(10) $$\sum \rho\mu_i\vec{Y}_i = \lambda\sum \mu_i\vec{X}_i \,.$$

Mas, por hipótese,

$$\vec{Y}_i = \lambda_i\vec{X}_i \,,$$

donde vem em (10):

(11) $$\sum \rho\mu_i\lambda_i\vec{X}_i = \sum \mu_i\lambda\vec{X}_i \,, \quad \text{ou}$$

(12) $$\sum \mu_i(\rho\lambda_i - \lambda)\vec{X}_i = 0$$

e como os μ_i não são todos nulos, concluimos que:

$$\rho\lambda_i = \lambda,$$

donde os λ_i são todos iguais e $\vec{Y}_i = \lambda\vec{X}_i$.

<u>Recìprocamente</u>, se $\vec{Y}_i = \lambda\vec{X}_i$ ($\lambda \in K^*$), as (r+1)-uplas de um mesmo ponto Q pertencem à mesma classe, tanto no caso dos vectores-coordenadas $\vec{X}_i$ como $\vec{Y}_i$.

Como

$$\vec{Y} = \lambda\vec{X},$$

e

$$\vec{Y} = \sum \mu_i\vec{Y}_i \quad \text{e} \quad \vec{X} = \sum \rho_i\vec{X}_i, \text{ temos:}$$

(13) $$\sum \mu_i\vec{Y}_i = \sigma\sum \rho_i\vec{X}_i = \sum \sigma\rho_i\vec{X}_i \qquad (\sigma \in K^*).$$

Mas, $\vec{Y}_i = \lambda\vec{X}_i$, por hipótese, donde se infere:

(14) $$\sum \mu_i\lambda\vec{X}_i = \sum \sigma\rho_i\vec{X}_i$$

ou

$$\sum (\mu_i\lambda - \sigma\rho_i)\vec{X}_i = 0 \,.$$

Como os vectores $\vec{X}_i$ são independentes, temos:

(15) $$\mu_i\lambda - \sigma\rho_i = 0 \,,$$

isto é, $\mu_i = \frac{\sigma}{\lambda}\rho_i$ $\left(\frac{\sigma}{\lambda} \in K^*\right)$, e as $(r+1)$-uplas pertencem à mesma classe.

DEFINIÇÃO. No caso examinado, diz-se que em P_r foi estabelecido um sistema de <u>coordenadas projetivas homogêneas</u> relativo ao simplexo fundamental dado pelos Q_i e o ponto unidade U, isto é, o ponto que corresponde à $(r+1)$-upla $(1,1,\ldots,1)$ [31-vol.II, pag.149].

Indica-se o sistema por $(Q_0,Q_1,\ldots,Q_r|U)$ e as coordenadas de um ponto Q por $[\mu_0,\mu_1,\ldots,\mu_r]$.

2. Escolhidos, arbitràriamente, r+1 pontos linearmente independentes em P_r, vamos vêr se há alguma restrição na escolha de U. A resposta é dada pelo

TEOREMA 2. Quaisquer r+1 vectores dos r+2 vectores-coordenadas de Q_i e de U são linearmente independentes [31-vol. II,pag.150].

Como $U \equiv [1,1,\ldots,1]$, então, o vector-coordenada V e os vectores-coordenadas $\vec{X}_i$ de Q_i estão ligados pela relação

$$\vec{V} = \vec{X}_0 + \vec{X}_1 + \ldots + \vec{X}_r \tag{16}$$

Vamos provar que $\vec{V}, \vec{X}_0, \vec{X}_1, \ldots, \vec{X}_{r-1}$ são linearmente independentes. Com efeito, se assim não fosse,

$$\vec{V} = \sum_{i=0}^{r-1} \lambda_i \vec{X}_i \, . \tag{17}$$

De (17) e (16), vem:

$$(1-\lambda_0)\vec{X}_0 + (1-\lambda_1)\vec{X}_1 + \ldots + (1-\lambda_{r-1})\vec{X}_{r-1} + \vec{X}_r = 0 \tag{18}$$

donde os $\vec{X}_i$ não seriam linearmente independentes, contra a hipótese.

TEOREMA 3. Escolhido $\vec{V}$, de modo que quaisquer r+1 dos r+2 vectores $\vec{X}_0, \vec{X}_1, \ldots, \vec{X}_r, \vec{V}$ sejam linearmente independentes, então o ponto U, cujo vector-coordenada é $\vec{V}$, tem coordenadas $[1,1,\ldots,1]$.

Com efeito, temos:

$$\vec{V} = \rho_0\vec{X}_0 + \ldots + \rho_r\vec{X}_r \tag{19}$$

com $\rho_i \in K^*$, por causa da hipótese.

Tomando-se para vectores-coordenadas dos pontos Q_i, $\rho_i \vec{X}_i = \vec{Y}_i$, teremos:

$$\vec{V} = \vec{Y}_0 + \vec{Y}_1 + \ldots + \vec{Y}_r \tag{20}$$

o que prova o teorema.

3. No espaço P_N, teremos, então, o sistema de coordenadas $(Q_0, Q_1, \ldots, Q_N | U)$.

TEOREMA 4. É sempre possível escolher um sistema conveniente de coordenadas, de modo que as coordenadas de um ponto $P \equiv (x_0, x_1, \ldots, x_N)$ sejam $[x_0, x_1, \ldots, x_N]$ [31-vol.II, pag. 151].

Escolhamos, para pontos Q_i, os pontos

$$(0, 0, \ldots, \underbrace{1}_{i}, \ldots, 0)$$

e para U, o ponto $(1, 1, \ldots, 1)$; o vector-coordenada $\vec{X}$ de um ponto $P \equiv (x_0, x_1, \ldots, x_N)$, cujas coordenadas no sistema são $[\mu_0, \mu_1, \ldots, \mu_N]$, será dado por:

$$\vec{X} = \sum_{i=0}^{N} \mu_i \vec{X}_i \tag{21}$$

ou, usando as componentes,

$$(x_0, x_1, \ldots, x_N) = \mu_0(1, 0, \ldots, 0) + \mu_1(0, 1, 0, \ldots, 0) + \ldots$$

$$\ldots + \mu_N(0, 0, \ldots, 0, 1) = (\mu_0, \mu_1, \ldots, \mu_N)$$

e daí,

$$x_i = \mu_i$$

e as coordenadas do ponto são $[x_0, x_1, \ldots, x_N]$.

4. Examinemos, por fim, o problema da <u>transformação de coordenadas</u> [31-vol.II, pag.153].

Consideremos o sistema $(Q_0, Q_1, \ldots, Q_N | U)$ e sejam $\vec{a}_i$, os vectores-coordenadas de Q_i, e

$$\sum_{i=0}^{N} \vec{a}_i \quad \text{o de U.}$$

Se $Q \equiv (x_o, x_1, \dots, x_N)$ tem as coordenadas $[y_o, y_1, \dots, y_N]$ no sistema dado, então, o vector-coordenada de Q é, por definição,

$$(22) \qquad \sum_{i=0}^{N} y_i \vec{a}_i \; .$$

Seja, agora, o sistema particular em que as coordenadas de Q são $[x_o, x_1, \dots, x_N]$. Teremos:

$$(23) \qquad \sum_{i=0}^{N} y_i \vec{a}_i = \lambda (x_o, x_1, \dots, x_N)$$

ou, designando as componentes de $\vec{a}_i$ por $(a_{oi}, a_{1i}, \dots, a_{Ni})$,

$$(24) \qquad \sum_{i=0}^{N} y_i (a_{oi}, a_{1i}, \dots, a_{Ni}) = \lambda (x_o, x_1, \dots, x_N).$$

De (24), vem:

$$(25) \qquad \begin{cases} x_o = a_{oo} y_o + a_{o1} y_1 + \dots + a_{oN} y_N \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ x_N = a_{No} y_o + a_{N1} y_1 + \dots + a_{NN} y_N \end{cases}$$

Indicando-se as coordenadas $[y_i]$ e $[x_i]$ pelas matrizes

$$(26) \qquad Y = \begin{pmatrix} y_o \\ y_1 \\ \vdots \\ y_N \end{pmatrix} \qquad X = \begin{pmatrix} x_o \\ x_1 \\ \vdots \\ x_N \end{pmatrix}$$

e designando por A a matriz não singular

$$(27) \qquad A = \begin{pmatrix} a_{oo} & a_{o1} & \dots & a_{oN} \\ a_{1o} & a_{11} & \dots & a_{1N} \\ \cdot & \cdot & \dots & \cdot \\ a_{No} & a_{N1} & \dots & a_{NN} \end{pmatrix}$$

podemos usar a notação matricial para a transformação dada pela (23):

$$(28) \qquad \lambda Y = A\, X \; .$$

Como A e não singular, teremos a transformação inversa:

(29 $$\lambda A^{-1}Y = A^{-1}AX$$
ou

$$\frac{1}{\lambda} X = A^{-1}Y .$$

É fácil ver que para cada matriz não singular A, existe um sistema de coordenadas $(Q_o, Q_1, \ldots, Q_N | U)$, cujas transformações para o sistema em que as coordenadas de $Q \equiv (x_o, x_1, \ldots, x_N)$ são $[x_o, x_1, \ldots, x_N]$, são dadas por (28) e (29).

5. O caso geral entre os sistemas $(Q_o, Q_1, \ldots, Q_N | U)$ e $(L_o, L_1, \ldots, L_N | V)$, fazemos por intermédio do anterior. Sejam as coordenadas de $Q \equiv (x_o, x_1, \ldots, x_N)$, respectivamente, nos dois sistemas: $[y_o, y_1, \ldots, y_N]$ e $[z_o, z_1, \ldots, z_N]$. Teremos:

(30) $$\lambda Y = AX$$
e
(31) $$\rho Z = BX .$$

De (31), vem:

(32) $$\frac{1}{\rho} X = B^{-1}Z .$$

De (30) e (32), temos: $\lambda Y = A\rho B^{-1}Z$, ou

(33) $$\frac{\lambda}{\rho} Y = AB^{-1}Z$$

que, juntamente com

(34) $$\frac{\rho}{\lambda} Z = BA^{-1}Y ,$$

nos dão as expressões da transformação.

6. TEOREMA 5. Um sub-espaço P_r não muda de dimensão por uma transformação de coordenadas.

É suficiente mostrar que os pontos (y_i^s), para $s = 0, \ldots, r$, linearmente independentes, continuam a ser linearmente independentes.

Com efeito, se os vectores $\vec{Y}_s \equiv (y_i^s)$ são linearmente independentes, então a matriz N×N:

$$Y_1 = \begin{pmatrix} y_o^o & \cdots & y_N^o \\ y_o^1 & \cdots & y_N^1 \\ \cdot & \cdots & \cdot \\ y_o^r & \cdots & y_N^r \\ 0 & \cdots & 0 \\ \cdot & \cdots & \cdot \\ 0 & \cdots & 0 \end{pmatrix} \qquad (35)$$

tem característica $r+1$, e aplicando-se a transformação

$$\rho X = A \;\; Y \qquad (36)$$

para cada vector (y_i^s), vem:

$$\begin{cases} \rho x_o^s = a_{oo} y_o^s + \ldots + a_{oN} y_N^s \\ \rho x_1^s = a_{1o} y_o^s + \ldots + a_{1N} y_N^s \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \rho x_N^s = a_{No} y_o^s + \ldots + a_{NN} y_N^s \end{cases} \qquad (37)$$

Mas podemos colocar, pela (37)

$$\rho \begin{pmatrix} x_o^o \ldots x_o^r \; 0 \ldots 0 \\ x^o \ldots x^r \; 0 \ldots 0 \\ \cdots\cdots\cdots\cdots \\ x^o \ldots x^r 0 \ldots 0 \end{pmatrix} = \begin{pmatrix} a_{oo} & a_{o1} & \cdots & a_{oN} \\ a_{1o} & a_{11} & \cdots & a_{1N} \\ \cdots & \cdots & \cdots & \cdots \\ a_{No} & a_{N1} & \cdots & a_{NN} \end{pmatrix} \cdot \begin{pmatrix} y_o^o \ldots y_o^r \; 0 \ldots 0 \\ y_1^o \ldots y_1^r \; 0 \ldots 0 \\ \cdots\cdots\cdots\cdots \\ y_N^o \ldots y_N^r \; 0 \ldots 0 \end{pmatrix} \qquad (38)$$

ou

$$\rho \begin{pmatrix} x_o^o \; x_o^1 \ldots x_o^r \; 0 \ldots 0 \\ x^o \; x^1 \ldots x^r \; 0 \ldots 0 \\ \cdots\cdots\cdots\cdots \\ x^o \; x^1 \ldots x^r \; 0 \ldots 0 \end{pmatrix} = \begin{pmatrix} \sum a_{oi} y_i^o & \sum a_{oi} y_i^1 & \cdots & \sum a_{oi} y_i^r 0 \ldots 0 \\ \sum a_{1i} y_i^o & \sum a_{1i} y_i^1 & \cdots & \sum a_{1i} y_i^r 0 \ldots 0 \\ \cdots & \cdots & \cdots & \cdots \\ \sum a_{Ni} y_i^o & \sum a_{Ni} y_i^1 & & \sum a_{Ni} y_i^r 0 \ldots 0 \end{pmatrix}$$

ou então, chamando de X_1 a matriz do primeiro membro,

$$\rho X_1 = A Y_1' .$$

Como A é não singular e Y_1' tem característica $r+1$, então, a característica de AY_1' é, também, $r+1$, o que demonstra o teorema.

§ 6º - COORDENADAS DE HIPERPLANO

1. Um hiperplano do P_N tem a equação:

$$\sum_{i=0}^{N} u_i x_i = 0 \ , \tag{1}$$

onde os u_i não todos nulos.

Se $\sum_{i=0}^{N} v_i x_i = 0$ representa o mesmo hiperplano (1), então a matriz

$$\begin{pmatrix} u_0 & u_1 & \cdots & u_N \\ v_0 & v_1 & \cdots & v_N \end{pmatrix} \tag{2}$$

tem característica 1 e, portanto,

$$u_i = \lambda v_i \qquad (\lambda \in K^*) \ . \tag{3}$$

Assim, as (n+1)-uplas u_i, a menos do fator $\lambda \in K^*$, determinam os hiperplanos e, por conseguinte, os u_i são denominados <u>coordenadas dos hiperplanos</u> [31-vol.II, pag.159].

Verifica-se que o número de hiperplanos também, por êste caminho, é dado por

$$\frac{q^{N+1}-1}{q-1} \ . \tag{4}$$

2. Calculemos o número de hiperplanos que passam por um P_{N-2}.

As equações de dois hiperplanos por um P_{N-2} são dadas por

$$\begin{matrix} \sum a_i x_i = 0 \\ \sum b_i x_i = 0 \end{matrix} \qquad \text{com} \qquad \begin{pmatrix} a_i \\ b_i \end{pmatrix}_2 \ . \tag{5}$$

Daí, concluimos que todo hiperplano por êsse P_{N-2} tem as coordenadas:

$$v_i = \lambda_0 a_i + \lambda_1 b_i \qquad (i=0,\ldots,N) \tag{6}$$

com λ_0 e λ_1 não nulos ao mesmo tempo.

Disto decorre que o número de hiperplanos pelo P_{N-2} é dado por

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

De um modo geral, o número de hiperplanos que passam por um P_{N-M-1} é dado por

$$\frac{q^{M+1}-1}{q-1}$$

---o---

§ 7º - DUALIDADE

1. Já tivemos oportunidade de ver que o número de $P_r \subset P_N$ é igual ao número de P_{N-r-1} de P_N. Vamos, agora, provar que os cinco postulados de Veblen são verdadeiros, quando se toma para ponto P_o, um P_{N-1}; para reta P_1, um P_{N-2} e para P_r, um P_{N-r-1}.

I_V) Para dois P_{N-1} distintos, existe um e um só P_{N-2} ao qual êles pertencem.

Sejam os P_{N-1} distintos dados por:

(1) $$\sum_{i=0}^{N} a_i x_i = 0$$

$$\sum^{N} b_i x_i = 0$$

com $\begin{pmatrix} a_o & a_1 & \dots & a_N \\ b_o & b_1 & \dots & b_N \end{pmatrix}$ de característica 2. O conjunto de pontos comuns a êles é um P_{N-2}, conforme vimos no § 1º,teor.2.

II_V) Dados os hiperplanos A_{N-1}, B_{N-1} e C_{N-1}, dois a dois distintos, não pertencentes ao mesmo P_{N-2}, escolhidos um hiperplano D_{N-1}, distinto de A_{N-1} e de B_{N-1} e pertencente a $A_{N-1} \cap B_{N-1} = R_{N-2}$ e um hiperplano E_{N-1} distinto de A_{N-1} e de C_{N-1} e pertencente a $A_{N-1} \cap C_{N-1} = L_{N-2}$, então, os hiperplanos D_{N-1} e E_{N-1} se cortam num P_{N-2}, que pertence aos hiperplanos B_{N-1} e C_{N-1}.

Sejam os hiperplanos A_{N-1}, B_{N-1} e C_{N-1} dados pelas equações:

$$(2) \qquad \sum_{i=0}^{N} a_i x_i = 0 \qquad \sum_{i=0}^{N} b_i x_i = 0 \qquad \sum_{i=0}^{N} c_i x_i = 0 .$$

Como os hiperplanos não pertencem ao mesmo P_{N-2}, a matriz

$$(3) \qquad \begin{pmatrix} a_o & a_1 & \dots & a_N \\ b_o & b_1 & \dots & b_N \\ c_o & c_1 & \dots & c_N \end{pmatrix}$$

tem característica 3 e a intersecção é um P_{N-3}.

Um hiperplano D_{N-1} pelo $R_{N-2} = A_{N-1} \cap B_{N-1}$ tem a equação

$$(4) \qquad \lambda_o(a_o x_o + \dots + a_N x_N) + \lambda_1(b_o x_o + \dots + b_N x_N) = 0$$

onde os λ_o, λ_1 pertencem a K*, por ser distinto de A_{N-1} e de B_{N-1}.

Analogamente, um hiperplano E_{N-1} pelo $L_{N-2} = A_{N-1} \cap C_{N-1}$ e distinto de A_{N-1} e de C_{N-1} tem a equação

$$(5) \qquad \mu_o(a_o x_o + \dots + a_N x_N) + \mu_1(c_o x_o + \dots + c_N x_N) = 0,$$

com μ_o, μ_1 pertencentes a K*.

Um hiperplano pelo P_{N-2}, intersecção de B_{N-1} e C_{N-1}, tem a equação:

$$(6) \qquad \alpha(b_o x_o + \dots + b_N x_N) + \beta(c_o x_o + \dots + c_N x_N) = 0,$$

com α, β não todos nulos.

Da mesma forma, os hiperplanos do P_{N-2}, intersecção de D_{N-1} e E_{N-1} têm a equação:

$$(7) \qquad \gamma[\lambda_o(a_o x_o + \dots + a_N x_N) + \lambda_1(b_o x_o + \dots + b_N x_N)] + \\ + \delta[\mu_o(a_o x_o + \dots + a_N x_N) + \mu_1(c_o x_o + \dots + c_N x_N)] = 0.$$

Devemos determinar α, β, γ, δ, de modo que (6) e (7) representem o mesmo hiperplano. Para isto, é suficiente

$$(8) \qquad \begin{aligned} \gamma\lambda_o + \delta\mu_o &= 0 \\ \gamma\lambda_1 &= k\alpha \\ \delta\mu_1 &= k\beta \end{aligned} \qquad \text{ou} \qquad \begin{aligned} k\alpha - \gamma\lambda_1 &= 0 \\ k\beta - \delta\mu_1 &= 0 \\ \gamma\lambda_o + \delta\mu_o &= 0 \end{aligned}$$

onde λ_o, λ_1, μ_o, μ_1 são elementos fixos de K*.

Temos em (8) um sistema homogêneo de três equações com 4 incógnitas, onde a matriz dos coeficientes

$$(9) \qquad \begin{pmatrix} k & 0 & -\lambda_1 & 0 \\ 0 & k & 0 & -\mu_1 \\ 0 & 0 & \lambda_o & \mu_o \end{pmatrix}$$

tem característica 3, como é fácil ver.

Resolvendo o sistema, temos:

$$(10) \qquad \begin{aligned} \beta &= -\frac{\alpha\lambda_o\mu_1}{\mu_o\lambda_1} \\ \gamma &= \frac{k\alpha}{\lambda_1} \\ \delta &= -\frac{k\alpha\lambda_o}{\mu_o\lambda_1} \end{aligned}$$

o que mostra a existência do P_{N-2} comum.

É imediato que o hiperplano de (6) que coincide com o (7) tem a equação

$$(11) \qquad \sum (b_i - \frac{\lambda_o\mu_1}{\mu_o\lambda_1} c_i)x_i = 0$$

III_V) Em cada P_{N-2} passam, pelo menos, três P_{N-1}.

Com efeito, um P_{N-2} contém

$$\frac{q^{N-1}-1}{q-1}$$

pontos e o espaço P_N,

$$\frac{q^{N+1}-1}{q-1} \quad ;$$

portanto, há

$$\frac{q^{N+1}-1}{q-1} - \frac{q^{N-1}-1}{q-1} = \frac{q^{N+1}-q^{N-1}}{q-1} = q^{N-1}(q+1)$$ pontos fora de um P_{N-2}.

Um ponto Q dêstes forma com o P_{N-2} um P_{N-1}.

Considerado em seguida um ponto $R \notin P_{N-1}$, o que se pode fazer de

$$(12) \qquad \frac{q^{N+1}-1}{q-1} - \frac{q^{N}-1}{q-1} = \frac{q^{N+1}-q^{N}}{q-1} = q^{N}$$

modos diferentes, vemos que R, com o P_{N-2}, forma um outro P_{N-1}.

A seguir, consideramos um ponto S fora dos dois P_{N-1}, o que se pode realizar em

$$(13) \qquad \frac{q^{N+1}-1}{q-1} - 2\cdot\frac{q^{N}-1}{q-1} = \frac{q^{N}(q-2)+1}{q-1}$$

maneiras diferentes, notando-se que (13) é sempre $\geqq 1$ para $q \geqq 2$

O ponto S com o P_{N-2} dá um terceiro P_{N-1}.

IV_V) Se $M < N$, os P_{N-1} não passam todos pelo mesmo P_{N-M-1}.

Como vimos no § 6º - 3, o número de P_{N-1} que passam por um P_{N-M-1} é dado por

$$(14) \qquad \frac{q^{M+1}-1}{q-1} \; .$$

Como o número de hiperplanos é $\dfrac{q^{N+1}-1}{q-1}$, então, temos

$$(15) \qquad \frac{q^{N+1}-q^{M+1}}{q-1}$$

hiperplanos, além dos que passam pelo P_{N-M-1}.

V_V) Não há P_{N-1} fora do P_N.

É claro, em face do V_V) do § 2º.

Com as proposições acima, concluimos o PRINCÍPIO GERAL DE DUALIDADE:

Se uma proposição de pertinência, baseada nos axiomas I_V) a V_V) do § 2º, é verdadeira, então, o é também a que se obtém pela troca dos P_k por P_{N-k-1}.

§ 8º - TEOREMAS DE DESARGUES E DE PAPPUS

1. A geometria que vimos construindo é desarguesiana, isto é, vale o célebre teorema de Desargues sôbre triângulos perspectivos de um plano:

> Se dois triângulos ABC e A'B'C' são tais que as retas AA', BB', CC' passam por um ponto O, então os pontos AB.A'B', BC.B'C' e AC.A'C' pertencem a u'a mesma reta [6-vol.I, pag. 41].

Vamos dar uma demonstração direta.

Sejam os pontos $O\equiv(o_i)$, $A\equiv(a_i)$, $A'\equiv(a_i')$ numa reta r; O, $B\equiv(b_i)$, $B'\equiv(b_i')$ noutra reta r'; O, $C\equiv(c_i)$, $C'\equiv(c_i')$ em r", onde r, r' e r" estão num mesmo plano ou não e ABC, A'B'C' são triângulos.

Teremos, pelas hipóteses:

$$(1)\qquad \begin{aligned} a_i' &= o_i + \lambda a_i \\ b_i' &= o_i + \mu b_i \\ c_i' &= o_i + \rho c_i \end{aligned} \qquad (i=0,\ldots,N)\ ,$$

com $\lambda, \mu, \rho \in K^*$.

Os pontos (b_i'), (c_i') e $b_i' - c_i'$ são colineares; mas, pela (1), $b_i' - c_i' = \mu b_i - \rho c_i$, logo, o ponto $P\equiv(b_i'-c_i')\equiv(\mu b_i-\rho c_i)$ é B'C'.BC.

Anàlogamente, o ponto $Q\equiv(a_i'-b_i')\equiv(\lambda a_i-\mu b_i)$ é AB.A'B'; $R\equiv$ $\equiv(c_i'-a_i')\equiv(\rho c_i-\lambda a_i)$ é AC.A'C'.

Os pontos P, Q e R são colineares, pois

$$b_i'-c_i'+c_i'-a_i'+a_i'-b_i' = 0.$$

2. Nesta geometria, vale, também, o teorema de Pappus:

> Se A,B,C são pontos distintos de uma reta e A',B',C', pontos distintos de uma outra reta complanar com a primeira, então os pontos AB'.A'B, AC'.A'C e BC'.B'C pertencem a u'a mesma reta [6-vol.I, pag.98].

Com efeito, todo <u>corpo finito é comutativo</u> pelo teorema de Weddeburn-Mac Lagan [19,pags.33,34,35].

Por outro lado, se o corpo é comutativo, vale o teorema de Staudt e reciprocamente [6-vol.I,pag.148;vol.II,pags.3,4]. Mas o teorema de Staudt é equivalente ao de Pappus [39,pags.32,33, 34,35,36].

Concluimos, então, que nesta geometria vale o teorema de Pappus.

Conforme o teorema de Hessenberg [40], o teorema de Desargues é consequência do de Pappus, donde temos uma nova confirmação do que dissemos no nº 1.

3. Podemos calcular o número de configurações de Desargues existentes num plano P_N.

A escolha do ponto O no P_2 é em

$$\frac{q^3-1}{q-1} \tag{2}$$

modos.

A escolha de $A \neq O$ é feita em

$$\frac{q^3-q}{q-1} \tag{3}$$

maneiras.

A de $A' \in OA$ e tal que $A' \neq O$ e $A' \neq A$, pode ser em

$$\frac{q^2-1}{q-1} - 2 = \frac{q\ \ -2q+1}{q-1} = q-1 \tag{4}$$

modos.

Um ponto $B \notin OA$ pode ser escolhido em

$$\frac{q^3-1}{q-1} - \frac{q^2-1}{q-1} = \frac{q^3-q^2}{q-1} \tag{5}$$

modos diferentes.

Um ponto $B' \in OB$ e tal que $B' \neq O$ e $B' \neq B$ é escolhido em

$$\frac{q^2-1}{q-1} - 2 = q-1 \tag{6}$$

maneiras.

Um ponto $C \notin OA$, $\notin OB$ e $\notin AB$ pode ser escolhido em

$$\frac{q^3-1}{q-1} - 3q = \frac{q^3-1-3q^2+3q}{q-1} = \frac{q^3-3q^2+3q-1}{q-1} = \frac{(q-1)^3}{q-1} = (q-1)^2 \tag{7}$$

modos.

Finalmente, um ponto $C' \in OC$, $\notin A'B'$ e tal que $C' \neq O$ e $C' \neq C$, pode ser tomado em

$$\frac{q^2-1}{q-1} - 3 = \frac{q^2-1-3q+3}{q-1} = \frac{q^2-3q+2}{q-1} = q-2 \tag{8}$$

O número de configurações é, então, dado pelo produto das expressões (2),(3),(4),(5),(6),(7),(8), isto é:

$$(q^3-q^2)(q^3-q)(q^3-1)(q-1)(q-2) \ . \tag{9}$$

Vemos que, no caso do corpo primo de característica 2, não há essa configuração geral.

4. Calculemos, agora, o número de configurações de Pappus, num plano do P_N.

Primeiramente, a escolha de uma reta do plano pode ser em

$$\frac{q^3-1}{q-1} \tag{10}$$

modos diversos.

A escolha de um ponto na reta pode ser em

$$\frac{q^2-1}{q-1} \tag{11}$$

maneiras.

A seguir, a de um segundo ponto da reta, distinto do primeiro, se faz em

$$\frac{q^2-q}{q-1} \tag{12}$$

processos.

A escolha de um terceiro ponto da reta, distinto dos dois primeiros é feita em

$$\frac{q^2-1}{q-1} - 2 = \frac{(q-1)^2}{q-1} = q-2 \tag{13}$$

modos diferentes.

Uma reta, distinta da primeira, pode ser tomada em

$$\frac{q^3-1}{q-1} - 1 = \frac{q^3-q}{q-1} \tag{14}$$

caminhos diversos.

A escolha de um ponto nesta reta, distinto da intersecção das duas retas, pode ser feita em

$$\frac{q^2-1}{q-1} - 1 = \frac{q^2-q}{q-1} \tag{15}$$

modos diferentes.

Um segundo ponto, distinto do primeiro e de O, pode ser tomado em

$$\frac{q^2-1}{q-1} - 2 = \frac{q^2-1-2q+2}{q-1} = \frac{q^2-2q+1}{q-1} = q-1 \tag{16}$$

modos diversos.

A escolha de um terceiro ponto, distinto dos dois primeiros e de O, pode ser feita em

$$\frac{q^2-1}{q-1} - 3 = \frac{q^2-1-3q+3}{q-1} = \frac{q^2-3q+2}{q-1} = q-2 \tag{17}$$

processos diferentes.

O número de configurações é dado pelo produto das expressões (10) a (17), isto é:

$$(18)\qquad \frac{q^3-1}{q-1}\cdot\frac{q^2-1}{q-1}\cdot\frac{q^2-q}{q-1}\cdot(q-1)\cdot\frac{q^3-q}{q-1}\cdot\frac{q^2-q}{q-1}\cdot(q-1)(q-2)$$

ou

$$q^2(q^3-1)(q^3-q)(q+1)(q-2) .$$

Vemos que não há esse tipo geral de configuração, no caso do corpo primo de característica 2.

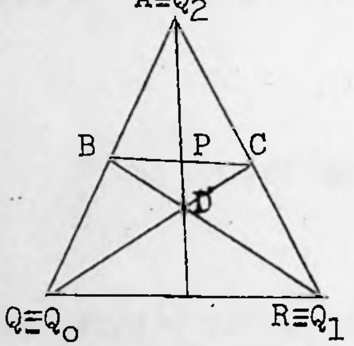
---o---

§ 9º - TEOREMA DO QUADRÂNGULO

1. Vamos demonstrar o importante

TEOREMA. Uma condição necessária e suficiente para que os três pontos diagonais de um quadrângulo plano completo sejam colineares é que o corpo seja de característica 2 [6-vol.I, pag.45].

Seja o quadrângulo ABCD e os pontos diagonais P, Q, R. Tomemos três dos vértices Q_o, Q_1, Q_2 do simplexo fundamental nos pontos Q,R,A.



As coordenadas de Q_o,Q_1,Q_2, são (1,0,...,0), (0,1,0,...,0), e (0,0,1,0,...,0).

Os pontos $B \in AQ \equiv Q_oQ_2$ e $C \in AR \equiv Q_1Q_2$ têm, respectivamente, as coordenadas (a,0,b,0,...,0) e (0,c,d,0,...,0), com a, b, c, d $\in K^*$.

As equações da reta Q_oC são:

$$(1)\qquad \begin{aligned} x_o &= \lambda_o \\ x_1 &= \lambda_1 c \\ x_2 &= \lambda_1 d \\ x_i &= 0 \qquad (i=3,\dots,N) \end{aligned}$$

As da reta Q_1B são:

$$(2)\qquad \begin{aligned} x_o &= \rho_1 a \\ x_1 &= \rho_o \\ x_2 &= \rho_1 b \\ x_i &= 0 \qquad (i=3,\dots,N) \end{aligned}$$

As coordenadas do ponto $D \equiv BR.QC$ são:

$$(a,\frac{bc}{d},b,0,\dots,0) \ .$$

As retas BC e AD têm, respectivamente, as equações:

$$(3) \qquad \begin{aligned} x_0 &= \lambda_0 a \\ x_1 &= \lambda_1 c \\ x_2 &= \lambda_0 b+\lambda_1 d \\ x_i &= 0 \quad (i=3,\dots,N) \end{aligned} \qquad \text{e} \qquad \begin{aligned} x_0 &= \rho_1 a \\ x_1 &= \rho_1 \cdot \frac{bc}{d} \\ x_2 &= \rho_0+\rho_1 b \\ x_i &= 0 \quad (i=3,\dots,N) \end{aligned}$$

O ponto $P \equiv AD.BC$ tem coordenadas:

$$(a,\frac{bc}{d},2b,0,\dots,0)$$

Se P, Q, R são alinhados, então, os vectores $(1,0,\dots,0)$, $(0,1,0,\dots,0)$ e $(a,\frac{bc}{d},2b,0,\dots,0)$ são linearmente dependentes, donde a matriz

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ a & \frac{bc}{d} & 2b & \dots & 0 \end{pmatrix}$$

tem característica 2, logo o determinante

$$(4) \qquad \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & \frac{bc}{d} & 2b \end{vmatrix} = 2b$$

é igual a zero, donde $2b = 0$, e como $b \in K^*$, se segue que o corpo tem característica 2.

Reciprocamente, se o corpo tem característica 2, o determinante (4) é nulo, e os vectores são linearmente dependentes e, portanto, os pontos diagonais são colineares.

---0---

§ 10º - RAZÃO ANARMÔNICA

1. Seja r uma reta definida pelas equações

(1) $$x_i = \lambda_o y_i^o + \lambda_1 y_i^1 \qquad (i=0,\dots,N) .$$

Consideremos os pontos Q_o, Q_1 e E da reta para os valores do par (λ_o,λ_1), respectivamente (0,1), (1,0) e (1,1).

DEFINIÇÃO 1. Dado um ponto $P=(\lambda_o,\lambda_1)$, chama-se <u>razão anarmônica</u> dos pontos Q_o,Q_1,E,P e se indica por $(Q_o\ Q_1\ E\ P)$, ao número $\frac{\lambda_o}{\lambda_1}$, se $P \not\equiv Q_o$; ao símbolo ∞, se $P \equiv Q_o$ [31-vol.II,pag. 167].

É claro que, se $P \equiv Q_1$, $(Q_oQ_1E\ Q_1) = 0$; se $P \equiv Q_2$, $(Q_oQ_1E\ E) = 1$.

Vejamos como se estende o conceito a $(Q_oQ_1Q\ P)$, onde o vector coordenada de Q é $\mu_o y_i^o + \mu_1 y_i^1$ $(\mu_o\mu_1 \in K^*)$.

Tomemos $\mu_o y_i^o = z_i^o$ e $\mu_1 y_i^1 = z_i^1$ e consideremos a (1) na forma

(2) $$x_i = \frac{\lambda_o}{\mu_o}(\mu_o y_i^o) + \frac{\lambda_1}{\mu_1}(\mu_1 y_i^1) = \frac{\lambda_o}{\mu_o} z^o + \frac{\lambda_1}{\mu_1} z_i^1 .$$

A razão é, então, pela definição 1:

(3) $$(Q_o\ Q_1\ Q\ P) = \frac{\lambda_o}{\mu_o} : \frac{\lambda_1}{\mu_1} .$$

Supostos os pontos A_1, A_2, A_3, dois a dois distintos, vejamos como se calcula a razão anarmônica

$$(A_1\ \ A_2\ \ A_3\ \ A_4) ,$$

conhecendo-se as razões

(4) $$a_i = (Q_o\ Q_1\ E\ \ A_i) \quad \text{para } i=1,2,3,4 \text{ e } a_i \in K.$$

Para isto, é suficiente calcular as coordenadas de A_3 e A_4 no sistema em que A_1 e A_2 são pontos fundamentais.

Denominados os vectores-coordenadas de Q_o e Q_1, $\vec{X}$ e $\vec{Y}$, temos que, de (4) decorre que os vectores de A_i são:

(5) $$\vec{Z}_i = a_i\vec{X} + \vec{Y} \qquad (i=1,2,3,4).$$

Das duas primeiras (5), vêm:

(6) $$\vec{Z}_1 - \vec{Z}_2 = (a_1 - a_2)\,\vec{X}.$$

Pela substituição de (6) na terceira de (5), temos:

(7) $$\vec{Z}_3 = a_3.\frac{\vec{Z}_1-\vec{Z}_2}{a_1-a_2} + \vec{Y}\ .$$

Substituindo-se $\vec{Y}$ da quarta de (5) em (7), vem:

(8) $$\vec{Z}_3 = a_3.\frac{\vec{Z}_1-\vec{Z}_2}{a_1-a_2} + \vec{Z}_1 - a_1.\frac{\vec{Z}_1-\vec{Z}_2}{a_1-a_2}$$

ou

$$\vec{Z}_3 = \vec{Z}_1.\frac{a_3-a_2}{a_1-a_2} + \vec{Z}_2.\frac{a_1-a_3}{a_1-a_2}$$

De modo anàlogo, obtemos:

(9) $$\vec{Z}_4 = \vec{Z}_1.\frac{a_4-a_2}{a_1-a_2} + \vec{Z}_2.\ \frac{a_1-a_4}{a_1-a_2}$$

De (2), (8) e (9), vem:

(10) $$(A_1\ A_2\ A_3\ A_4) = \frac{(a_2-a_4)(a_1-a_3)}{(a_2-a_3)(a_1-a_4)}$$

Se $A_1 \equiv A_4$, pela definição 1, $(A_1A_2A_3A_4) = \infty$.

No caso em que $A_1 \equiv Q_o$, isto é,

$$(Q_o\ Q_1\ E\ \ A_1) = (Q_o\ Q_1\ E\ \ Q_o) = \infty\ ,$$

temos os vectores coordenadas dos A_i:

(11) $$\vec{Z}_1 = \vec{X}$$
$$\vec{Z}_i = a_i\vec{X} + \vec{Y} \quad (i=2,3,4).$$

Com raciocínio idêntico ao anterior, vem

(12) $$(A_1\ A_2\ A_3\ A_4) = (Q_o\ A_2\ A_3\ A_4) = \frac{a_2-a_4}{a_2-a_3}\ .$$

O mesmo se faz nos casos de $A_2 \equiv Q_o$, $A_3 \equiv Q_o$ e $A_4 \equiv Q_o$.

Note-se pelas expressões (10) e (12) a unicidade de um elemento, fixados os outros três.

2. Pelo princípio de dualidade, obtemos os mesmos resultados do nº 1 para os hiperplanos de u'a mesma reta.

3. Cortando-se um feixe de hiperplanos com uma reta que não corte o eixo, temos o

TEOREMA 1. Se os pontos A_1, A_2 e A_3 da reta pertencem aos hiperplanos $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, então, uma condição necessária e suficiente para que $A_4 \in \alpha_4$ é que $(A_1\ A_2\ A_3\ A_4) = (\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4)$ [31-vol.II,pag.173].

Sejam os vectores-coordenadas de $A_1, A_2, A_3, \alpha_1, \alpha_2, \alpha_3$, : $\vec{X}_1$, $\vec{X}_2, \vec{X}_3, \vec{U}_1, \vec{U}_2$ e $\vec{U}_3$, com $\vec{X}_3 = \vec{X}_1 + \vec{X}_2$ e $\vec{U}_3 = \vec{U}_1 + \vec{U}_2$.

Se $(A_1 A_2 A_3 A_4) = \lambda$ e $(\alpha_1 \alpha_2 \alpha_3 \alpha_4) = \rho$, então, os vectores-coordenadas de A_4 e α_4 são:

$$\lambda \vec{X}_1 + \vec{X}_2 \qquad \text{e} \qquad \rho \vec{U}_1 + \vec{U}_2. \tag{13}$$

Como $A_i \in \alpha_i$ $(i=1,2,3)$, então:

$$\sum_{i=0}^{N} u_i^1 x_i^1 = 0\ ,\ \sum_{i=0}^{N} u_i^2 x_i^2 = 0 \quad \text{e} \quad \sum_{i=0}^{N} (u_i^1 + u_i^2)(x_i^1 + x_i^2) = 0. \tag{14}$$

Da última das (14), temos:

$$\sum_{i=0}^{N} u_i^1 x_i^1 + \sum_{i=0}^{N} u_i^1 x_i^2 + \sum_{i=0}^{N} u_i^2 x_i^1 + \sum_{i=0}^{N} u_i^2 x_i^2 = \sum_{i=0}^{N} u_i^2 x_i^1 + \sum_{i=0}^{N} u_i^1 x_i^2 = 0\ . \tag{15}$$

Tomando-se a relação

$$\sum_{i=0}^{N} (\lambda x_i^1 + x_i^2)(\sum_{i=0}^{N} \rho u_i^1 + u_i^2) = \lambda\rho \sum_{i=0}^{N} u_i^1 x_i^1 + \lambda \sum_{i=0}^{N} u_i^2 x_i^1 + \rho \sum_{i=0}^{N} u_i^1 x_i^2 + \sum_{i=0}^{N} u_i^2 x_i^2 = \lambda \sum_{i=0}^{N} u_i^2 x_i^1 + \rho \sum_{i=0}^{N} u_i^1 x_i^2$$

e substituindo-se nela a (15), vem:

$$\lambda(-\sum_{i=0}^{N} u_i^1 x_i^2) + \rho \sum_{i=0}^{N} u_i^1 x_i^2 = (\lambda - \rho) \sum_{i=0}^{N} u_i^1 x_i^2. \tag{16}$$

Daí, temos que (16) fôr nula, então $\lambda = \rho$, pois $\sum u_i^1 x_i^2 \neq 0$ i.e., se $A_4 \in \alpha_4$, as razões serão iguais; se $\lambda = \rho$, então,

$A_4 \in \alpha_4$.

No caso do plano, isto é, N=2, o teorema 1 é verdadeiro para feixe de retas.

4. DEFINIÇÃO 2. Se $(A_1\ A_2\ A_3\ A_4) = -1$, dizemos que A_1, A_2, A_3, A_4 constituem um <u>conjunto harmônico</u>.

No caso do corpo K de característica 2, $(A_1A_2A_3A_4) = 1$ e, portanto, $A_3 \equiv A_4$.

Vamos provar o

TEOREMA 2. Uma condição necessária e suficiente para que A_1, A_2, A_3 e A_4 constituam um conjunto harmônico é que exista um quadrângulo plano completo com dois lados opostos contendo A_1, dois contendo A_3, um que passe por A_2 e o último por A_4.

a) <u>A condição é necessária</u>. Seja o quadrângulo PQRS, com os lados QP e RS por A_1, QR e PS por A_3, PR por A_2 e QS por A_4. Provemos que $(A_1A_2A_3A_4) = -1$.

Se a característica de K fôr 2, então, $A_2 \equiv A_4$, como vimos no § 9º do cap. I e $(A_1A_2A_3A_4) = 1 = -1$.

Seja $p \neq 2$. Tomemos o sistema de coordenadas $(A_1A_3P|R)$ no P_2. Sejam os vectores-coordenadas de A_1, A_3, P: $\vec{X}, \vec{Y}, \vec{Z}$; o de R é $\vec{X} + \vec{Y} + \vec{Z}$.

Como $\vec{X}+\vec{Y}$, por um lado, é combinação linear de $\vec{X}$ e $\vec{Y}$ e, por outro lado é de $\vec{X}+\vec{Y}+\vec{Z}$ e $\vec{Z}$, então, o ponto associado de $\vec{X}+\vec{Y}$ está nas retas A_1A_3 e PR, isto é, é A_2.

Anàlogamente, os vectores-coordenadas de Q e S são $\vec{X}+\vec{Z}$ e $\vec{Y}+\vec{Z}$. o $\vec{W}$ de A_4 é combinação linear tanto de $\vec{X}$ e $\vec{Y}$, como de $\vec{X}+\vec{Z}$ e $\vec{Y}+\vec{Z}$, isto é:

$$\vec{W} = \lambda\vec{X} + \rho\vec{Y} \tag{17}$$
$$\vec{W} = \tau(\vec{X}+\vec{Z}) + \sigma(\vec{Y}+\vec{Z}) .$$

De (17), decorre claramente

$$(\lambda - \tau)\vec{X} + (\rho - \sigma)\vec{Y} + (-\tau - \sigma)\vec{Z} = \vec{0} . \tag{18}$$

De (18), devido à independência linear dos vectores X, Y e Z, vem:

$$\lambda = \tau, \qquad \rho = \sigma, \qquad \tau = -\sigma \tag{19}$$

Obtemos, devido a (19):

(20) $$\vec{W} = \lambda\vec{X} - \lambda\vec{Y}\ .$$

Os vectores-coordenadas de A_1, A_2, A_3, A_4 são $\vec{X}, \vec{Y}, \vec{X}+\vec{Y}$ e $\lambda\vec{X} - \lambda\vec{Y}$ e, portanto, pelo nº 1, $(A_1A_2A_3A_4) = -1$.

b) <u>A condição é suficiente</u>. Seja $(A_1A_2A_3A_4) = -1$. Se $p=2$, então, $(A_1A_2A_3A_4) = 1$ e $A_2 \equiv A_4$; existe, portanto, um quadrângulo com dois lados opostos por A_1, dois por A_3, um por A_2 e o último por A_4.

Se $p \neq 2$, construido o quadrângulo nas condições acima, se o último lado passar por um ponto A_4', teremos:

$$(A_1\ A_2\ A_3\ A_4) = (A_1\ A_2\ A_3\ A_4') = -1\ ,$$

e, pela unicidade do quarto elemento, fixados os três primeiros, $A_4 \equiv A_4'$, o que prova a afirmação.

C A P Í T U L O I I

§ 1º - COLINEAÇÕES E PROPRIEDADES FUNDAMENTAIS

1. DEFINIÇÃO 1. Fixado um automorfismo σ do corpo K, chama-se COLINEAÇÃO entre os pontos de duas retas ou da mesma reta, à correspondência biunívoca pontual tal que se a A,B,C,D correspondem A',B',C',D', então:

$$\sigma(A\ B\ C\ D) = (A'B'C'D'), \quad \text{se } (A\ B\ C\ D) \in K;$$
$$\text{se } (A\ B\ C\ D) = \infty, \text{ então, } (A'B'C'D') = \infty.$$

Quando σ é o automorfismo idêntico, então, a colineação é denominada HOMOGRAFIA.

É claro que:

a) Se o corpo K é primo, tôda colineação é homografia;

b) Se K é de ordem $q = p^n$, então, há n escolhas do automorfismo; c) Tôda colineação entre retas conserva o conjunto harmônico, pois, $\sigma(-1) = -1$.

Demonstraremos agora o

TEOREMA DE DARBOUX. Tôda correspondência biunívoca entre retas ou na mesma reta sôbre um corpo de característica $p \neq 2$, que conserva o conjunto harmônico, é uma colineação [41].

a) Escolhamos os sistemas de coordenadas nas duas retas em pontos correspondentes, de modo que a correspondência ω seja tal que

$$\omega(\infty) = \infty, \qquad \omega(0) = 0, \qquad \omega(1) = 1.$$

Provemos que

(1) $\omega(2x) = 2\omega(x)$.

Como $(0,2x,x,\infty) = -\dfrac{x}{x} = -1$, então,

$$(0,\omega(2x),\omega(x),\infty) = -1,$$

ou

$$\frac{-\omega(x)}{\omega(2x)-\omega(x)} = -1$$

e

$$\omega(2x) = 2\omega(x).$$

Vamos agora provar que

(2) $$\omega(x+y) = \omega(x) + \omega(y).$$

Temos que $(2x, 2y, x+y, \infty) = \dfrac{x-y}{-x+y} = -1$. Daí, vem

$$(3) \qquad (\omega(2x),\omega(2y),\omega(x+y),\infty) = \frac{\omega(2x) - \omega(x+y)}{\omega(2y) - \omega(x+y)} = -1.$$

Levando (1) em (3), temos:

$$2\omega(x) - \omega(x+y) + 2\omega(y) - \omega(x+y) = 0$$

ou

$$\omega(x+y) = \omega(x) + \omega(y).$$

De (2) decorre imediatamente que

$$(4) \qquad \omega(-x) = -\omega(x).$$

Demonstremos que

$$(5) \qquad \omega(x^2) = [\omega(x)]^2.$$

Temos que $(x, -x, 1, x^2) = -1$, donde,

$$(\omega(x),\omega(-x), 1,\omega(x^2)) = -1,$$

ou

$$(6) \qquad \frac{(\omega(x) - 1)(\omega(-x) - \omega(x^2))}{(\omega(-x) - 1)(\omega(x) - \omega(x^2))} = -1.$$

Aplicando-se (4) em (6), vem:

$$(\omega(x) - 1)(-\omega(x) - \omega(x^2)) + (-\omega(x) - 1)(\omega(x) - \omega(x^2)) =$$

ou

$$-[\omega(x)]^2 - \omega(x)\omega(x^2) + \omega(x) + \omega(x^2) - [\omega(x)]^2 + \omega(x)\omega(x^2) -$$
$$-\omega(x) + \omega(x^2) = 0,$$

donde temos:

$$(7) \qquad \omega(x^2) = [\omega(x)]^2.$$

Provemos, agora, que

$$(8) \qquad \omega(xy) = \omega(x)\omega(y).$$

Temos, pela (7), que

$$[\omega(x+y)]^2 = \omega(x+y)^2.$$

Daí vem, pela (1), (2) e pela (7):

$$[\omega(x)+\omega(y)]^2 = \omega(x^2 + 2xy + y^2)$$

ou

$$[\omega(x)]^2 + [\omega(y)]^2 + 2\omega(x)\omega(y) = [\omega(x)]^2 + 2\omega(xy) + [\omega(y)]^2$$

ou ainda

$$\omega(xy) = \omega(x)\omega(y).$$

Pelas propriedades demonstradas (1) e (8), concluimos que ω é um automorfismo do corpo K, donde, se A_1', A_2', A_3', A_4' são correspondentes, respectivamente, de A_1, A_2, A_3, A_4, para as coordenadas a_i' e a_i valem as relações:

(9) $$a_i' = \omega(a_i).$$

De (9), vem que

$$(a_1' \ a_2' \ a_3' \ a_4') = (\omega(a_1), \omega(a_2), \omega(a_3), \omega(a_4)) = \omega(a_1 \ a_2 \ a_3 \ a_4)$$

o que prova o teorema.

b) Se na correspondência ω entre r e r', a ∞, 0 e 1 de r correspondem a', b' e c' de r', então, com uma transformação T de coordenadas em r', da forma

(10) $$\begin{cases} \rho y_1' = (c'-a')x_1' + b'(a'-c')x_2' \\ \rho y_2' = (c'-b')x_1' + a'(b'-c')x_2' \end{cases}$$

mudamos as coordenadas a', b', c' em ∞, 0, 1.

A correspondência $T\omega$ é análoga à do caso a) e, portanto, é um automorfismo σ do corpo K. Temos, então:

$$\omega = T^{-1}\sigma$$

dada por

(11) $$x' = \frac{a'(c'-b')\,\sigma(x) + b'(a'-c')}{(c'-b')\,\sigma(x) + a' - c'}$$

e que, como fàcilmente se vê, leva (A B C D) em ω(A B C D).

No caso da correspondência ω na mesma reta r, em que aos pontos de coordenadas ∞, 0, 1 correspondem os de coordenadas a,b,c, consideramos uma outra reta r' distinta da primeira. Entre r e r', tomamos um automorfismo σ de K que leva ∞,0,1, de r, em ∞,0,1, de r'. Considerada a correspondência entre r' e r que leva ∞,0,1, de r', em a,b,c, de r, vemos que, pela b), é ela da forma

$$T^{-1}\tau,$$

onde τ é um automorfismo de K.

Finalmente, temos que

$$\omega = T^{-1}\tau\sigma,$$

e, como $\tau\sigma$ é um automorfismo ρ de K, recaímos na equação (11), o que demonstra o teorema.

DEFINIÇÃO 2. Chama-se <u>colineação</u> entre pontos de dois P_r ($r \geq 2$), ou do mesmo P_r a uma correspondência pontual biunívoca que conserva o alinhamento, isto é, tal que a um $P_1 \subset P_r$ faz corresponder um P_1 do mesmo ou de outro P_r.

TEOREMA 1. Em tôda colineação entre dois P_r $(r \geqq 2)$ ou do mesmo P_r, a um conjunto harmônico de pontos de uma reta corresponde um da mesma ou de outra reta.

É suficiente aplicar o teorema 2, do § 10º, do cap. I.

TEOREMA 2. A colineação entre dois P_r $(r \geqq 2)$ ou do mesmo P_r induz uma colineação entre as retas correspondentes, associada sempre a um mesmo automorfismo.

Pelo teorema 1 dêste §, é claro que entre as retas correspondentes há uma correspondência que conserva o conjunto harmônico.

Se o corpo fôr de característica $p \neq 2$, então, pelo teorema de Darboux, concluimos que entre as duas retas correspondentes, há uma colineação associada a um automorfismo σ.

No caso de ser $p = 2$, vamos provar que, escolhido um sistema conveniente de coordenadas, a correspondência é um automorfismo.

Suponhamos que aos pontos ∞, 0 e 1 de uma reta correspondam pontos de coordenadas ∞, 0 e 1 da outra, o que sempre é possível, com sistemas convenientes.

Consideremos dois pontos de coordenadas x e y de uma das retas e os seus correspondentes x' e y' da outra reta.

Tomado um quadrângulo RXSL, em que os lados opostos LR e SX passam por x e y, os lados opostos RX e LS por T, o lado RS por 0 e o lado LX por z, vamos provar que $z = x + y$.

Com efeito, chamando T a intersecção de LX e RS, temos, por projeções e secções convenientes:

$$(0\ x\ z\ \infty) = (0\ R\ T\ S) = (0\ \infty\ z\ y)\ .$$

Daí, vem:

$$\frac{-z}{x-z} = \frac{-z}{-y}$$

ou

$$z = x + y\ .$$

Devido à conservação do alinhamento, teremos um quadrângulo R'X'S'L' na mesma situação na reta r', onde teremos que z' é correspondente de z e é igual a $x' + y'$.

Fazendo o mesmo com um quadrângulo TSRL, com dois lados opostos por x e y, outros dois por z e ∞, um por 1 e o oposto por 0, teremos, por projeções e secções convenientes, chamando de L a intersecção de LS e RT:

$$(1\ x\ z\ \infty) = (1\ T\ V\ R) = (1\ 0\ z\ y),$$

donde vem:

$$\frac{1-z}{x-z} = \frac{-(1-z)y}{-z(1-y)}$$

ou seja

$$z = xy.$$

Na reta r', tomado o quadrângulo T'S'R'L' correspondente, vemos que o ponto z', correspondente de z, é igual a x'y'. A correspondência é, então, um automorfismo.

Devemos, agora, provar que se, entre duas retas correspondentes r e r', há um automorfismo σ, entre duas outras correspondentes s e s' intervém o mesmo σ.

É suficiente provar no caso em que r e s sejam co-planares, o que também acontece com r' e s'.

Sejam os pontos B_1, B_2, B_3, B_4 de s e os correspondentes B_1', B_2', B_3', B_4' de s'.

De um ponto $O \notin r$ e $\notin s$, projetemos os B_i em A_i de r; o mesmo do ponto O' correspondente de O, para obter os A_i' de r'. Temos, então:

$$(12) \quad \begin{array}{c} (B_1\ B_2\ B_3\ B_4) = (A_1\ A_2\ A_3\ A_4) \\ \text{e} \\ (B_1'\ B_2'\ B_3'\ B_4') = (A_1'\ A_2'\ A_3'\ A_4') \end{array}$$

pelo teorema 1, do § 10º, do cap. I.

Como entre r e r' temos

$$\sigma(A_1\ A_2\ A_3\ A_4) = (A_1'\ A_2'\ A_3'\ A_4'),$$

vem, com (12):

$$\sigma(B_1\ B_2\ B_3\ B_4) = (B_1'\ B_2'\ B_3'\ B_4'),$$

o que prova o teorema.

TEOREMA 3. Numa colineação entre dois P_r $(r \geq 2)$ ou do mesmo P_r:

a) a um P_q $(q < r)$ corresponde um P_q;

b) entre os P_q correspondentes há uma colineação definida pelo mesmo automorfismo σ.

Como a correspondência conserva a independência linear, é imediata a prova de a).

Para demonstrar b) é suficiente aplicar a definição entre os P_q.

TEOREMA 4. Tôda correspondência do tipo

$$\rho x_i' = \sum_{k=0}^{N} a_{ik}\sigma(x_k) \qquad (i=0,\dots,N)$$

onde o determinante $|a_{ik}| \neq 0$ e σ é um automorfismo do corpo K, é uma colineação.

Por ser linear e $|a_{ik}| \neq 0$, a correspondência é biunívoca.

É fácil ver que conserva o alinhamento. Com efeito, dada a reta de equações

$$(13) \qquad x_i = \lambda_o y_i^o + \lambda_1 y_i^1 \qquad (i=0,\dots,N) ,$$

temos que a (13) corresponde

$$(14) \quad \rho x_i' = \sum^{N} a_{ik}\sigma(\lambda_o y_i^o + \lambda_1 y_i^1) =$$

$$= \sigma(\lambda_o)\sum_{k=0}^{N} a_{ik}\sigma(y_i^o) + \sigma(\lambda_1)\sum_{k=0}^{N} a_{ik}\sigma(y_i^1)$$

ou

$$(15) \qquad \rho x' = \rho\,\sigma(\lambda_o)y_i'^{\,o} + \rho\,\sigma(\lambda_1)y_i'^{\,1}$$

ou ainda

$$x_i' = \sigma(\lambda_o)y_i'^{\,o} + \sigma(\lambda_1)y_i'^{\,1} ,$$

que são as equações de uma reta.

2. TEOREMA DE STAUDT. Se numa homografia do P_N, sôbre K, com $q \neq 2$, houver N+2 pontos linearmente independentes unidos ou auto-correspondentes, todos os demais serão unidos. Se $q = 2$, o teorema é verdadeiro para N+1 pontos.

Para N=1 e $q \neq 2$, o teorema é verdadeiro; basta aplicar a definição de homografia e a proposição relativa à unicidade do quarto elemento da razão anarmônica.

Suponhamos verdadeiro para N-1 e vamos demonstrar que o é para N.

Consideremos N+1 pontos dos N+2. Como são unidos, tomado qualquer P_{N-1} definido por N pontos dos N+1, é unido. A reta determinada pelos dois pontos restantes é unida e como não pertence ao P_{N-1} considerado, a intersecção é um ponto P_o, como é fácil de ver. P_o é unido, como se vê do fato de serem unidos P_{N-1} e P_1.

O ponto P_o não coincide com nenhum dos N pontos unidos do P_{N-1}, senão haverá três pontos unidos dos N+2 numa mesma reta, o que é contra a hipótese da independência dos N+1 pontos. Dêste modo, todos os pontos do P_{N-1} são unidos pela hipótese de indução.

Assim, os $\binom{N+2}{N+1} = N+2$ espaços P_{N-1} obtidos dos N+2 pontos unidos são de pontos unidos.

Dado um ponto P, consideremos por êle uma reta que não passe por nenhum dos vértices do simplexo dos N+1 pontos; certamente, ela encontrará três ou mais P_{N-1} em pontos que são unidos, donde, pelo caso N=1, P é unido.

No caso em que q = 2, o teorema é verdadeiro para N = 1, pois, se dois pontos da reta são unidos, o ponto restante, também, o é, devido à correspondência biunívoca.

Suponhamos verdadeiro para N-1 e demonstremos para N.

Com efeito, dados os N+1 pontos unidos, pela hipótese de indução, cada P_{N-1} tendo N pontos unidos é de pontos unidos, donde temos N+1 espaços P_{N-1} de pontos unidos.

Dado P, e considerada por êle uma reta P_1 que passe por um dos vértices do simplexo, esta encontra o P_{N-1} determinado pelos N pontos restantes num ponto unido, como é fácil de ver.

A reta P_1 tendo dois pontos unidos é unida, conforme o caso N = 1. Fica assim provado o teorema.

TEOREMA FUNDAMENTAL. Dados N+2 pares de pontos N+1 a N+1 linearmente independentes de um P_N e fixado um automorfismo σ de K, no caso de $q \neq 2$, existe uma e uma só colineação que faz se corresponderem os N+2 pares de pontos numa ordem determinada. Se q = 2, o teorema é verdadeiro para N+1 pares de pontos linearmente independentes.

a) Para demonstrar a existência, é suficiente tomarmos N+2 pontos como sistema fundamental de coordenadas $(Q_o, Q_1, \ldots$ $\ldots, Q_N | Q_{N+1})$, e os correspondentes terão coordenadas $Q' \equiv (a_i^k)$

$(k=0,\ldots,N+1;i=0,\ldots,N)$.

Devemos determinar os coeficientes das equações

(16) $$\rho x_i' = \sum_{k=0}^{N} a_{ik}\sigma(x_k) \qquad \text{com } |a_{ik}| \neq 0.$$

Impondo-se a correspondência, vem o sistema de (N+1)(N+2) equações:

(17)
$$\begin{aligned}
\rho_0 a_i^0 &= a_{i0} \qquad (i=0,\ldots,N)\\
\rho_1 a_i^1 &= a_{i1}\\
&\ldots\ldots\ldots\\
\rho_N a_i^N &= a_{iN}\\
\rho_{N+1} a_i^{N+1} &= \sum_{k=0}^{N} a_{ik}
\end{aligned}$$

nas (N+1)(N+2) incógnitas ρ_i e a_{ik}, onde os ρ_i são a menos de fator de K*.

Assim, com a hipótese da independência linear, determinamos os coeficientes com $|a_{ik}| \neq 0$, o que prova o teorema.

Se q = 2, o teorema é verdadeiro para N+1 pares de pontos. De fato, nas equações (17), os fatores $\rho_i (i=0,\ldots,N)$ são todos iguais a 1, e, portanto, os coeficientes a_{ik} são iguais a a_i^k e as equações da colineação ficam determinadas.

b) Para a unicidade, basta ver que se houvesse duas colineações ω e τ para o mesmo σ, de equações:

(18) $$\rho x_i' = \sum_{k=0}^{N} a_{ik}\sigma(x_k) \qquad \text{e} \qquad \rho x_i' = \sum_{k=0}^{N} b_{ik}\sigma(x_k)\ ,$$

então, a inversa de τ é:

$$\sigma(x_k) = \sum_{i=0}^{N} B_{ki}x_i'$$

ou seja

$$\mu x_k = \sum \sigma^{-1}(B_{ik})\,\sigma^{-1}(x_i')\ .$$

Concluimos disto que $\tau^{-1}\omega$ é uma colineação correspondendo ao automorfismo idêntico, donde é uma homografia, e, pelo teorema de Staudt, é a identidade, como é fácil ver. Com isto temos $\tau^{-1}\omega = I$ e, por conseguinte, $\omega = \tau$.

Pelo que vimos anteriormente, podemos dizer que a tôda colineação corresponde um sistema de equações do tipo (18), e reciprocamente.

3. Vamos calcular o número de homografias e de colineações [42]. Calculemos primeiramente o número total de pontos existentes nos espaços P_{N-i} $(i=1,\ldots,N)$ de um simplexo N-dimensional do P_N.

No P_1, o número é $S_1 = 2$. No P_2, o número S_2 é dado por

$$\frac{q^3 - (q-1)^3 - 1}{q-1} \quad . \tag{19}$$

Por indução, obtemos para o P_N:

$$S_N = \frac{q^{N+1} - (q-1)^{N+1} - 1}{q-1} \quad . \tag{20}$$

Pelo teorema fundamental, o número de homografias depende da escolha de N+2 pontos, N+1 a N+1 linearmente independentes. A escolha do primeiro é dada por

$$\frac{q^{N+1} - 1}{q-1} \tag{21}$$

possibilidades.

A escolha do segundo, distinto do primeiro, é em

$$\frac{q^{N+1} - q}{q-1} \tag{22}$$

modos.

A escolha do terceiro, fora da reta dos dois primeiros, pode ser em

$$\frac{q^{N+1} - q^2}{q-1} \tag{23}$$

maneiras.

Finalmente, a escolha do (N+1)º, fora do P_{N-1} dos outros, pode ser em

$$\frac{q^{N+1} - q^N}{q-1} = q^N \tag{24}$$

modos diferentes.

A escolha do (N+2)º ponto, fora do simplexo dos N+1 pontos escolhidos, pode ser feita em

$$\frac{q^{N+1} - 1}{q-1} - S_N = (q-1)^N \tag{25}$$

processos diferentes.

O número total de escolhas é, portanto, efetuado em

(26) $$H = \frac{1}{q-1} \prod_{i=0}^{N} (q^{N+1} - q^i)$$

modos diferentes, o que nos dá o número procurado.

O número de colineações depende ainda da escolha de um automorfismo do corpo, automorfismos êsses que são em número de n, logo temos:

(27) $$C = \frac{n}{q-1} \prod_{i=0}^{N} (q^{N+1} - q^i)$$

---o---

§ 3º - HOMOGRAFIA ENTRE PONTOS DO P_N

1. No caso de homografia entre pontos do mesmo P_N, temos o problema dos pontos unidos, o que conduz ao dos sub-espaços unidos.

As equações da homografia, como já vimos, são:

(1) $$\rho x'_i = \sum_{k=0}^{N} a_{ik} x_k \qquad (i=0,\dots,N) .$$

Para um ponto ser unido é necessário e suficiente que $kx'_i = x_i$ $(i=0,\dots,N)$, com $k \in K^*$, donde, pela (1), virá que os pontos têm coordenadas que satisfazem às

(2) $$\sigma x_i = \sum_{k=0}^{N} a_{ik} x_k \qquad \text{ou} \qquad \sum_{k=0}^{N} a_{ik} x_k - \sigma x_i = 0$$
$$(i=0,\dots,N).$$

Como o sistema (2) é linear e homogêneo em x_i e êstes não podem ser todos nulos, então , o determinante dos coeficientes será nulo. Reciprocamente, se o determinante fôr nulo, então, os x_i não serão todos nulos.

Indicando-se a matriz (a_{ik}) por A, a unidade por I, temos a equação:

(3) $$|A - \sigma I| = 0 ,$$

que é a equação característica da matriz A.

Assim, para cada σ, solução da equação algébrica (3) de grau N+1, teremos um espaço de pontos unidos, constituido por tôdas as soluções (x_i) do sistema (2).

Se a uma raiz σ_1 de (3), que é sempre $\neq 0$, corresponde uma característica N+1-r da matriz

$$(A - \sigma I),$$

então, no sistema (2), há N+1-r equações independentes; donde, o conjunto de pontos unidos, cujas coordenadas são soluções do sistema, é um espaço de dimensão N+1-(N+1-r)=r, isto é, um P_r.

Por outro lado, podemos ver que existe um espaço de hiperplanos associado ao espaço P_r de pontos unidos.

Consideremos o hiperplano de coordenadas u'_i, cuja equação é

$$\sum_{i=0}^{N} u'_i x'_i = 0. \tag{4}$$

Usando (1) em (4), temos o hiperplano de equação

$$\sum_{i=0}^{N} u'_i \sum_{k=0}^{N} a_{ik} x_k = 0 \tag{5}$$

ou, agrupando os termos:

$$\sum_{i,k=0}^{N} a_{ik} u'_i x_k = 0. \tag{6}$$

O hiperplano correspondente de (4) pela homografia tem equação

$$\sum_{i=0}^{N} u_i x_i = 0 . \tag{7}$$

Pelo fato de (6) e (7) representarem o mesmo hiperplano, temos:

$$\rho u_i = \sum_{k=0}^{N} a_{ki} u'_i \qquad (i=0,\ldots,N). \tag{8}$$

Os hiperplanos unidos estão associados às raizes da equação característica da matriz $A'=(a_{ki})$, isto é, de

$$|A' - \rho I| = 0 ,$$

que é equivalente, evidentemente, à (3).

Assim, se a σ_1 corresponde um P_r de pontos unidos, então, no sistema (8), há N+1-r equações independentes, donde o conjunto de hiperplanos unidos forma, dualmente, um espaço P_r de hiperplanos unidos. A intersecção dêsses hiperplanos é um P_{N+1-r} unido.

Um fato importante é dado pelo

TEOREMA 1. As raizes da equação (3) são invariantes para mudança de coordenadas.

Com efeito, temos, denominando a matriz da transformação de coordenadas de B,

$$|B^{-1}AB-\sigma I|=|B^{-1}AB-\sigma B^{-1}IB|=|B^{-1}(A-\sigma I)B|=$$
$$=|B^{-1}||A-\sigma I||B|=|A-\sigma I|.$$

TEOREMA 2. A intersecção dos espaços P_r e P_s de pontos unidos correspondentes a duas raizes σ_1 e σ_2 ($\sigma_1 \neq \sigma_2$) de (3) é **vazia**.

Com efeito, seja (y_i) um ponto de $P_r \cap P_s$. Teremos, então,

$$\sum_{k=0}^{N} a_{ik}y_k - \sigma_1 y_k = 0 \quad \text{e} \quad \sum_{k=0}^{N} a_{ik}y_k - \sigma_2 y_k = 0 .$$

Fazendo-se a diferença, temos:

$$(9) \qquad (\sigma_2 - \sigma_1)y_i = 0.$$

Como, pelo menos um dos y_i é diferente de zero, temos um absurdo na expressão (9).

2. O problema do estudo direto da equação (3) num corpo de característica $p \neq 0$ não é simples como no caso de $p = 0$.

Entretanto, examinaremos a existência das homografias de certos tipos, como aparecem no conhecido caso do corpo real.

Comecemos pelo exame das homografias, que com transformações convenientes de coordenadas, podem ter a matriz na forma diagonal.

A existência é imediata, pois basta tomar N+1 elementos a_i de K*, distintos ou não, e, em seguida, construida a matriz

$$\begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_1 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 0 & a_N \end{pmatrix}$$

escrever as equações da homografia:

$$\rho x_i' = a_i x_i \qquad (i=0,\ldots,N)$$

No caso de $q = 2$, os $a_i = 1$ e a única homografia dêsse tipo é a que tem todos os pontos unidos, isto é, a <u>identidade</u>.

Calculemos o número de homografias dêsse tipo.

Seja a matriz diagonal da forma

$$(10) \qquad \begin{pmatrix} \underbrace{1 \;\; 1 \;\; \cdots \;\; 1}_{k_1} & & & & 0 \\ & \underbrace{\alpha_2 \;\; \alpha_2 \;\; \cdots \;\; \alpha_2}_{k_2} & & & \\ & & \ddots & & \\ & & & \underbrace{\alpha_m \;\; \alpha_m \;\; \cdots \;\; \alpha_m}_{k_m} & \\ 0 & & & & \end{pmatrix}$$

A escolha de $\alpha_2 \in K^*$, distinto de 1, é feita em $q-2$ modos diferentes; a de $\alpha_3 \in K^*$, distinto de 1 e α_2, é em $q-3$ maneiras; a de $\alpha_m \in K^*$, diferente de $1, \alpha_2, \alpha_3, \ldots, \alpha_{m-1}$, é em $q-m$ modos. Concluimos, então, que o número de possibilidades é dado por

$$(11) \qquad \prod_{i=2}^{m} (q-i) \, .$$

A escolha de um P_{k_1-1} no P_N, se faz em

$$(12) \qquad \prod_{i=0}^{k_1-1} \frac{q^{N+1-i}-1}{q^{k_1-1}-1} \qquad (\S\ 1^{\text{o}}, 2, \text{cap. I}) \, .$$

A escolha de um ponto fora do P_{k_1-1} se faz em

$$(13)\qquad \frac{q^{N+1}-1}{q-1}-\frac{q^{k_1}-1}{q-1}=\frac{q^{N+1}-q^{k_1}}{q-1}$$

modos.

Acrescentando-se um dêsses pontos ao P_{k_1-1}, temos um P_{k_1}.

O número de pontos do P_N fora do P_{k_1} é dado por

$$(14)\qquad \frac{q^{N+1}-1}{q-1}-\frac{q^{k_1+1}-1}{q-1}=\frac{q^{N+1}-q^{k_1+1}}{q-1} .$$

A seguir, formando-se um P_{k_1+1} com o P_{k_1} mais um dos pontos de P_N, temos que o número de pontos do P_N fora do P_{k_1+1} é

$$(15)\qquad \frac{q^{N+1}-q^{k_1+2}}{q-1} .$$

Sucessivamente, chegaremos à conclusão de que o número de pontos do P_N fora do $P_{k_1+k_2+\ldots+k_m-2}$ é dado por

$$(16)\qquad \frac{q^{N+1}-q^{k_1+k_2+\ldots+k_m-1}}{q-1} .$$

O número total de possibilidades é, então, dado pelo produto de (11), (12), (13), (14), (15) e (16), dividido pelo número de permutações de N+1, tomadas $k_1, k_2, \ldots, k_m$ iguais entre si.

Temos, então:

$$(17)\qquad \frac{\dfrac{q^{N+1}-q^{k_1}}{q-1}\cdot\dfrac{q^{N+1}-q^{k_1+1}}{q-1}\cdots\dfrac{q^{N+1}-q^{k_1+k_2+\ldots+k_m-1}}{q-1}\cdot\displaystyle\prod_{i=0}^{k_1-1}\frac{q^{N+1-i}-1}{q^{k_1-i}-1}\cdot\prod_{i=2}^{m}(q-i)}{\dfrac{(N+1)!}{k_1!\ldots k_m!}}$$

ou

$$(18)\qquad \frac{k_1!k_2!\ldots k_m!}{(N+1)!}\;\frac{\displaystyle\prod_{i=0}^{k_1-1}\frac{q^{N+1-i}-1}{q^{k_1-i}-1}}{(q-1)^{k_2+\ldots+k_m-1}}\cdot\prod_{i=2}^{m}(q-i)\cdot\prod_{i=k_1}^{k_1+\ldots+k_m-1}(q^{N+1}-q^{i})$$

Como casos particulares, temos:

a) Número de homografias com N+1 pontos distintos unidos e independentes. Obtém-se de (18) com $k_1=k_2=\ldots=k_m=1$ e $m=N+1$.

Vem:

$$(19)\qquad \frac{1}{(N+1)!}\;\frac{\dfrac{q^{N+1}-1}{q-1}}{(q-1)^{N}}\;\prod_{i=2}^{N+1}(q-i)\;\prod_{i=1}^{N}(q^{N+1}-q^{i})$$

ou

$$\frac{1}{(N+1)!}\;\frac{q^{N+1}-1}{(q-1)^{N+1}}\;\prod_{i=2}^{N+1}(q-i).\prod_{i=1}^{N}(q^{N+1}-q^{i})$$

ou ainda

$$(20)\qquad \frac{1}{(N+1)!(q-1)^{N+1}}\cdot\prod_{i=2}^{N+1}(q-i).\prod_{i=0}^{N}(q^{N+1}-q^{i})\quad .$$

Como vemos pela (20), para $q = 2$, não existe homografia dêsse tipo.

Também, não há homografias dêsse tipo no caso em que $q \leq N+1$.

Para o caso de $N = 2$, obtém-se a fórmula de Chung Tao Yang:

$$\frac{1}{6}\, q^{3}(q-2)(q-3)(q+1)(q^{2}+q+1) \qquad [25,\text{pag.}163].$$

b) Para $k_1 = N$, $k_2 = 1$ e $m = 2$, em (18), temos o número de homologias gerais. Obtemos então

$$\frac{N!}{(N+1)!}\cdot\frac{q^{N+1}-q^{N}}{q-1}\cdot(q-2).\prod_{i=0}^{N-1}\frac{q^{N+1-i}-1}{q^{N-i}-1}$$

ou

$$\frac{1}{N+1}\cdot\frac{q^{N+1}-q^{N}}{q-1}\cdot(q-2)\cdot\frac{q^{N+1}-1}{q-1}$$

ou ainda

$$(21)\qquad \frac{1}{N+1}\cdot\frac{q^{N}(q^{N+1}-1)(q-2)}{q-2} = \frac{1}{N+1}.q^{N}(q^{N}+q^{N-1}+\ldots+1)(q-2)\quad .$$

3. Uma outra classe de homografias é a das que não possuem <u>pontos unidos</u>.

Preliminarmente, vamos provar a existência de tais homografias.

Com efeito, pela teoria dos corpos de Galois ou dos corpos finitos [43,pag.205], sabemos que em K, há polinômios irredutíveis de grau N+1.

Seja, então, o polinômio irredutível

(22) $\sigma^{N+1} + a_1\sigma^N + \dots + a_{N+1} = 0$, com $a_i \in K$ e $a_{N+1} \in K^*$..

Pela teoria das matrizes, podemos construir a matriz, cujo polinômio característico seja o primeiro membro de (22) [44, pags.81,82].

Teremos, então, a matriz A:

$$(23) \qquad A = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_{N+1} \\ 1 & 0 & \dots & 0 & -a_N \\ 0 & 1 & \dots & 0 & -a_{N-1} \\ \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & \dots & 0 & -a_1 \end{pmatrix}$$

A homografia de equações

$$(24) \qquad \begin{cases} \rho x'_0 = & & -a_{N+1}x_N \\ \rho x'_1 = x_0 & & -a_N x_N \\ \rho x'_2 = & x_1 & -a_{N-1}x_N \\ \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \\ \rho x'_N = & & x_{N-1} - a_1 x_N \end{cases}$$

não tem pontos unidos.

O número de polinômios irredutíveis de grau N+1, num corpo K é dado por

$$(25) \qquad \frac{1}{N+1}\sum_{d\,|\,N+1} \mu(d)\, q^{(N+1)/d} \qquad (*)$$

onde $\mu(d)$ é a função de Möbius [45,pags. 269,270] ou por uma expressão que se encontra em G. Scorza [45,pags.126 a 129].

4. Vejamos algumas propriedades interessantes das homografias sem pontos unidos.

Para isto, tomemos o polinômio característico irredutível de grau N+1 da matriz A:

$$\sigma^{N+1} + a_1\sigma^N + \dots + a_{N+1} .$$

(*) Resultado inédito do prof. J. Delsarte.

Consideremos a extensão K' de grau N+1 do corpo K, que é de ordem q^{N+1}, onde o polinômio é redutível, pois a extensão é galoisiana, como se sabe da Álgebra.

As raizes $\sigma_0, \sigma_1, \ldots, \sigma_N$, de (22) são distintas e pertencem tôdas a K', sem que pertençam a qualquer extensão de K,de grau $d < N+1$ e divisor de N+1.

Aplicando-se, então, um automorfismo τ não idêntico do corpo K' ao conjunto das raizes $\sigma_0, \sigma_1, \ldots, \sigma_N$, o mesmo se reproduz, isto é, os $\tau(\sigma_i)$ são os σ_i numa outra ordem.

Por outro lado, nenhuma das raizes σ_i é invariante pelos automorfismos τ, salvo o caso de que o mesmo seja o idêntico.

DEFINIÇÃO 1. Consideradas as (N+1)-uplas de elementos de K', assim como as classes de equivalência, conforme § 1º, 1, do cap. I, obtemos um espaço projetivo $\mathcal{P}_N$ sôbre K', a que chamaremos espaço extensão.

Para ccada raiz σ_1 de (22) em K', obtemos um ponto (ξ_i^s), tal que

$$(26) \qquad \sum_{k=0}^{N} a_{ik}\xi_k^s - \sigma_s\xi_i^s = 0 \quad (i=0,\ldots,N)$$

ou, vectorialmente,

$$(27) \qquad A\vec{\xi}_s = \sigma_s\vec{\xi}_s .$$

Êsses pontos são unidos em $\mathcal{P}_N$ e são linearmente independentes, o que não é difícil de ver.

Com efeito, pela teoria das matrizes, sabemos que é sempre possível determinar uma transformação de coordenadas tal que a nova matriz

$$(28) \qquad A' = B^{-1}AB$$

seja diagonal.

Neste caso, as raizes são $\sigma_i = a_{ii}$ e é claro que os N+1 pontos unidos são (1,0,...,0),...,(0,0,...,0,1) que são linearmente independentes.

O espaço $\mathcal{P}_N$ contém um sub-espaço $\bar{P}_N$, cujos pontos são de elementos exclusivos de K.

O espaço $\bar{P}_N$ é isomorfo ao P_N.

TEOREMA 3. Uma condição necessária e suficiente para que uma homografia do $\mathcal{P}_N$ tenha os elementos α_{ij} da matriz $\mathfrak{a}$ correspondente no corpo K é que transforme todo ponto de $\bar{P}_N$ em ponto do próprio $\bar{P}_N$, isto é, invarie $\bar{P}_N$.

A condição é necessária, pois de $\alpha_{ij} \in K$, então, é claro que a todo ponto de $\bar{P}_N$ de coordenadas (x_i) com $x_i \in K$ corresponde um ponto (x_i') de coordenadas em K.

Vejamos que é suficiente. Suponhamos uma homografia de matriz $\mathfrak{a}$ que invaria $\bar{P}_N$; então, para qualquer (x_i) de $\bar{P}_N (x_i \in K)$ corresponde um ponto (x_i') de $\bar{P}_N$, isto é, $x_i' \in K$.

Em particular, o ponto $(1,0,\dots,0)$ é de $\bar{P}_N$ e substituindo-se em

(29) $$\rho x_i' = \sum \alpha_{ij} x_j \qquad \rho \in K'^*$$

vem

(30) $$\rho x_i' = \alpha_{io}$$

de K, donde os $\alpha_{io} \in K$. De um modo geral, considerando-se os pontos $(0,\dots,\underset{j}{1},\dots,0)$ com $i = 0,\dots,N$, temos que todos os $\alpha_{ij} \in K$.

TEOREMA 4. Uma condição necessária e suficiente para que uma homografia de $\mathcal{P}_N$ invarie $\bar{P}_N$ é que a matriz $\mathfrak{a}$ correspondente comute com todos os automorfismos τ_i de K'.

A condição é necessária. Lembremos, para isso, que os automorfismos τ_i invariam os elementos de K.

Tomemos, agora, um ponto (ξ_i) de $\mathcal{P}_N$ com $\xi_i \in K'$. Pela homografia dada, teremos que o ponto correspondente (ξ_i'), onde $\xi_i' \in K'$, é obtido pelas equações

(31) $$\rho \xi_i' = \sum \alpha_{ij} \xi_j' \qquad (\rho \in K'^*).$$

Aplicando-se τ_i às (31), vem:

(32) $$\tau_i(\rho)\tau_i(\xi_i') = \tau_i(\sum \alpha_{ij}\xi_j') = \sum \tau_i(\alpha_{ij})\tau_i(\xi_j') \; .$$

Como, por hipótese, $\tau_i(\alpha_{ij}) = \alpha_{ij}$, então

(33) $$\tau_i(\rho)\cdot\tau_i(\xi_i') = \sum \alpha_{ij}\cdot\tau_i(\xi_j') \; .$$

De (32) e (33), concluimos que

$$(34) \qquad \tau_i \mathfrak{A} = \mathfrak{A} \tau_i$$

para qualquer ponto de $\mathfrak{P}_N$, onde $\mathfrak{A} = (\alpha_{ij})$.

Vejamos a suficiência da condição para invariar P_N.

Suponhamos que valha a (34) e sejam, então, (x_i) um ponto do P_N com $x_i \in K$ e o seu correspondente (x_i').

Teremos

$$(35) \qquad \tau_i \mathfrak{A}(x_i) = \mathfrak{A} \tau_i(x_i)$$

e

$$(36) \qquad \tau_i(\rho x_i') = \tau_i \mathfrak{A}(x_i) = \mathfrak{A} \tau_i(x_i).$$

Mas $\tau_i(\rho x_i') = \mathfrak{A}(x_i)$, pois $x_i \in K$. Então, de (36), vem:

$$(37) \qquad \tau_i(\rho x_i') = \mathfrak{A}(x_i)$$

qualquer que seja τ_i.

Como $\rho x_i' = \mathfrak{A} x_i$, então, de (37), vem:

$$(38) \qquad \rho x_i' = \tau_i(\rho x_i')$$

e, por conseguinte, $\rho x_i' \in K$ e a homografia $\mathfrak{A}$ invaria P_N.

TEOREMA 5. Uma condição necessária e suficiente para que uma homografia de matriz $\mathfrak{A}$ com N+1 pontos unidos distintos em $\mathfrak{P}_N$, invarie $\bar{P}_N$ é que os automorfismos τ_i sejam tais que

$$\tau_i(\xi_i^k) = \rho_m \xi_i^m$$

isto é, os τ_i permutem os pontos unidos.

Com efeito, se a homografia de matriz $\mathfrak{A}$ invaria $\bar{P}_N$, então, pelo teorema 4, ela comuta com os τ_i; logo temos

$$\tau_i \mathfrak{A} = \mathfrak{A} \tau_i$$

donde

$$(39) \qquad \mathfrak{A}[\tau_i(\xi_i^k)] = \tau_i \mathfrak{A}(\xi_i^k) = \tau_i(\rho_k \xi_i^k) = \tau_i(\rho_k) \tau_i(\xi_i^k) =$$

$$= \sigma_m \tau_i(\xi_i^m)$$

e, então, necessàriamente $\tau_i(\xi_i^m) = \rho_m \xi_i^m$.

Recìprocamente, seja $\tau_i(\xi_i^m) = \rho_m \xi_i^m$; então, vem:

(40) $\alpha[\tau_i(\xi_i^k)] = \alpha(\rho_m \xi_i^m) = \rho_m \alpha(\xi_i^m) = \rho_m \sigma_m \xi_i^m = \rho_m \tau_i(\sigma_m) \xi_i^m =$

$$= \tau_i(\sigma_m)\tau_i(\xi_i^k) = \tau_i(\sigma_k \xi_i^k) = \tau_i \alpha(\xi_i^k) .$$

De (40) vem que τ_i e α comutam, logo, pelo teorema 4, a homografia invaria $\bar{P}_N$.

Dos teoremas precedentes, concluimos a caracterização das homografias em $\mathcal{P}_N$, que invariam um $\bar{P}_N$, sem pontos unidos em $\bar{P}_N$.

Resumindo, podemos caracterizar tais homografias do seguinte modo:

a) dar um elemento $\sigma_o \in K'$, tal que os $\tau_i(\sigma_o)$ sejam todos diferentes, quando τ_i percorre o conjunto dos automorfismos de K';

b) escolher uma (N+1)-upla (ξ_i) em $\mathcal{P}_N$, tal que os $\tau_i(\xi_i)$ sejam (N+1)-uplas distintas, quando τ_i descreve os automorfismos de K', constituindo um conjunto de pontos linearmente independentes.

A escolha de σ_o com a propriedade a) deve obedecer ao fato de que $\sigma_o, \sigma_o^q, \sigma_o^{q^2}, \ldots, \sigma_o^{q^N}$, são elementos distintos e, ainda mais, raizes de uma equação de grau N+1 sôbre K e irredutível sobre.

Os elementos de K' são em número de q^{N+1}.

Se $\alpha \in K'$ não é raiz de uma equação de grau N+1 irredutível sôbre K, então, o é de uma equação de grau d, também irredutível sôbre K. Como $\alpha \in K'$, conclui-se que $K' \supset K_d$, extensão de grau d de K, logo d é divisor de N+1.

Chamando de A_d o número de elementos de K' que são raizes de uma equação de grau d irredutível sôbre K, onde d é divisor de N+1, temos

(41)
$$q^{N+1} = \sum_{d|N+1} A_d .$$

Pela inversão de Möbius, vem:

(42) $$A_{N+1} = \sum \mu(d) q^{\frac{N+1}{d}} \quad .$$

Como, para cada raiz σ_o, temos que os $\tau_i(\sigma_o)$ são também raizes, concluimos que as escolhas de σ_o são em número de

(43) $$\frac{1}{N+1} A_{N+1} \quad .$$

Por outro lado, para que a escolha de uma (N+1)-upla (ξ_i) $(\xi_i \in K')$ seja tal que os pontos $\tau_i(\xi_i)$ sejam linearmente independentes, é necessário e suficiente que o determinante

(44) $$\Delta(\xi) = \begin{vmatrix} \xi_o & \xi_1 & \ldots & \xi_N \\ \xi_o^q & \xi_1^q & \ldots & \xi_N^q \\ . & . & \ldots & . \\ \xi^{q^N} & \xi^{q^N} & \ldots & \xi^{q^N} \end{vmatrix}$$

seja $\neq 0$.

A determinação do número V de(N+1)-uplas que satisfazem (44) é um problema do qual não conhecemos solução.

Êsse número V, dividido por $q^{N+1}-1$, nos dá as possibilidades de escolhas dos pontos nas condições anteriores.

5. Outro caso é o em que a homografia possui elementos unidos no P_N e, também, num $\mathcal{P}_N$ extensão.

Com efeito, suponhamos que o polinômio característico

(45) $$|A - \sigma I|$$

contenha um fator irredutível de grau r $(r > 1)$.

Fazendo-se uma extensão de grau r do corpo K a um corpo K', obtemos um espaço $\mathcal{P}_N$ sôbre K' e, nele, podemos raciocinar como no nº 4, verificando-se que há, então, r pontos unidos. No espaço P_N, teremos elementos unidos correspondentes à natureza das raizes doutro fator de (45), que é de grau N-r+1.

A existência de uma tal homografia é imediata, pois sabemos que existem polinômios irredutíveis de grau r no corpo K.

Seja

(46) $$\sigma^r + a_1\sigma^{r-1} + \ldots + a_r$$

um polinômio nessas condições.

Consideremos um outro polinômio de grau N-r+1, redutível sôbre K, por exemplo:

(47) $$\prod_{i=1}^{N-r+1} (\sigma - b_i) \,, \qquad \text{com } b_i \in K \,.$$

Tomemos o polinômio de grau N+1, produto de (46) e (47):

(48) $$\prod_{i=1}^{N-r+1} (\sigma - b\ )(\sigma^r + a_1\sigma^{r-1} + \ldots + a_r)$$

e suponhamos que, efetuado o cálculo, tenhamos obtido:

(49) $$\sigma^{N+1} + c_1\sigma^N + \ldots + c_{N+1} \,.$$

A homografia correspondente à matriz

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & -c_{N+1} \\ 1 & 0 & 0 & \ldots & -c_N \\ 0 & 1 & 0 & \ldots & -c_{N-1} \\ \cdot & \cdot & \cdot & \ldots & \cdot \\ 0 & 0 & 0 & \ldots\ 1 & -c_1 \end{pmatrix}$$

resolve a questão.

6. Finalmente, teremos ainda o caso das chamadas <u>homografias especiais</u>, em que, nenhuma transformação de coordenadas leva a matriz à forma diagonal, quer no corpo K, quer em extensões do corpo.

Para verificar a existência, tomemos a matriz

(51) $$A = \begin{pmatrix} 1 & 0 & \ldots & a_{oN} \\ 0 & 1 & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ 0 & 0 & \ldots & 1 \end{pmatrix}.$$

A equação característica é dada por

(52) $$\begin{vmatrix} 1-\sigma & 0 & \ldots & a_{oN} \\ 0 & 1-\sigma & \ldots & \\ \cdot & \cdot & \ldots & \cdot \\ 0 & 0 & \ldots & 1-\sigma \end{vmatrix} = 0 \,,$$

ou

(53) $$(1-\sigma)^{N+1} = 0 \,,$$

donde $\sigma = 1$ é raiz múltipla de ordem N+1. Por outro lado, a característica da matriz

$$(54) \qquad (A - \sigma I)$$

para $\sigma = 1$ é 1, donde temos um hiperplano P_{N-1} de pontos unidos.

A esta homografia não pode corresponder uma transformação que leve a matriz à forma diagonal, pois se tal acontecesse, a característica viria a ser 0, e todos os pontos seriam unidos; a homografia seria a identidade, contra a hipótese.

Por outro lado, não é nenhum dos tipos de homografia descritos nos números 3, 4 e 5.

---o---

§ 3º - HOMOGRAFIAS INVOLUTÓRIAS

1. Consideremos a homografia de equações

$$(1) \qquad \sigma x'_i = \sum_{k=0}^{N} a_{ik} x_k \qquad (i = 0, \ldots, N)$$

A inversa é dada por

$$(2) \qquad \mu x_i = \frac{1}{|A|} \sum_{k=0}^{N} A_{ki} x_i \qquad (i=0,\ldots,N)$$

onde $|A| = |a_{ik}| \neq 0$.

Se as (2), a (x_i) fazem corresponder (x'_i), isto é,

$$(3) \qquad \rho x' = \frac{1}{|A|} \sum_{k=0}^{N} A_{ki} x_i \quad (i=0,\ldots,N)$$

então,

$$(4) \qquad \lambda \cdot \frac{1}{|A|} \cdot A_{ki} = a_{ik}$$

com $\lambda \in K^*$.

Finalmente, temos

$$|A| = |a_{ik}| = |\lambda \frac{1}{|A|} A_{ki}| = \frac{\lambda^{N+1}}{|A|^{N+1}} |A_{ki}| = \frac{\lambda^{N+1}}{|A|^{N+1}} |A|^N = \frac{\lambda^{N+1}}{|A|},$$

ou

$$(5) \qquad |A|^2 = \lambda^{N+1} .$$

Seja agora, um ponto $P \equiv (x_i)$ e o correspondente $P' \equiv (x'_i)$.

A reta PP' é unida e, nela existe uma involução subordinada pela homografia.

Os pontos de PP' são, com exclusão de (x_i), dados por

(6) $$y_i = x_i' + kx_i \qquad (i=0,\ldots,N)$$

A (y_i) corresponde (y_i'), dado por

(7) $$y_i' = x_i' + k'x_i \qquad (i=0,\ldots,N)$$

Devido a (4), a (x_i') corresponde (λx_i); daí, a (y_i) corresponde

(8) $$\sigma y_i' = \lambda x_i + kx_i' \quad (i=0,\ldots,N)$$

Mas, pela (7),

(9) $$\sigma y_i' = \sigma x_i' + \sigma k'x_i \qquad (i=0,\ldots,N) .$$

De (8) e (9), concluimos que

(10) $$(\sigma - k)x_i' + (\sigma k' - \lambda)x_i = 0 .$$

Pelo fato de (x_i) não ser unido, de (10), vem

$$\sigma - k = 0 \qquad \text{e} \qquad \sigma k' - \lambda = 0, \text{ ou seja,}$$

(11) $$kk' = \lambda.$$

Os pontos unidos de PP' correspondem aos valores de k, que satisfazem à equação

(12) $$k^2 = \lambda.$$

TEOREMA 1. As raizes de (12), se existirem, são, também, os zeros da função característica da matriz A, e reciprocamente [34,pag.153].

Suponhamos que k_1 seja uma raiz de (12); o ponto

$$z_i = x_i' + k_1x_i \qquad (i=0,\ldots,N)$$

é unido, logo existe uma raiz σ_1 de

(13) $$|A - \sigma I| = 0 ,$$

tal que

(14) $$\sum_{k=0}^{N} a_{ik}z_k = \sigma_1 z_i \qquad (i=0,\ldots,N) .$$

De (12), temos

$$(15)\quad \begin{cases} (a_{oo}-\sigma_1)(x_o'+k_1x_o)+a_{o1}(x_1'+k_1x_1)+\ \dots\ +a_{oN}(x_N'+k_1x_N)=0\\ a_{1o}(x_o'+k_1x_o)+(a_{11}-\sigma_1)(x_1'+k_1x_1)+\ \dots\dots \qquad =0\\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\ a\quad (x'+k\ x\ )+\ \dots \qquad\qquad \dots\ +(a_{NN}-\sigma_1)(x_N'+k_1x_N)=0 \end{cases}$$

Aplicando-se em (15)

$$\sum_{k=0}^{N} a_{ik}x_k = x_i' \qquad \text{e} \qquad \sum_{k=0}^{N} a_{ik}x_k' = \lambda x_i \ ,$$

temos

$$\lambda x_i + k_1x_i' - \sigma_1x_i' - \sigma_1k_1x_i = 0 \quad (i=0,\dots,N)$$

ou

$$(16)\qquad (\lambda - \sigma_1k_1)x_i + (k_1 - \sigma_1)\ x_i' = 0.$$

De (16), vem:

$$(17)\qquad x_i = \frac{k_1 - \sigma_1}{\lambda-\sigma_1k_1}\ x_i' \ .$$

Mas, os pontos (x_i) e (x_i') são distintos, logo

$$\frac{k_1 - \sigma_1}{\lambda-\sigma_1k_1} = 0 \qquad \text{ou} \qquad k_1 = \sigma_1 \ ,$$

o que prova a afirmação.

Devemos provar que tôda raiz σ_1 de (13) é, também, de (12).

Suponhamos que σ_1 não satisfaça à equação (12) e consideremos uma raiz k_1 de (12) em K (ou numa extensão de K). Então, k_1 é também uma raiz de (13) em K ou na extensão, conforme o teorema direto.

Os espaços de pontos unidos P_r e P_s relativos às raizes k_1 e σ têm intersecção vazia, conforme o teorema 2, do § 3º, dêste capítulo.

Observemos que nenhum dos espaços P_r e P_s é contido num espaço de pontos unidos de dimensão maior.

Consideremos as retas que unem cada ponto de P_r a um de P_s. Tais retas são unidas e nelas a involução é a identidade, senão, no caso de $p\neq 2$, haverá dois pontos unidos provenientes das raizes de (12), mais um que provém de uma raiz de (13), e que não é de (12). No caso em que p=2, a equação (12) terá uma só raiz e haverá um ponto unido por êsse caminho, mas haverá um outro ponto unido que provém da raiz de (13), que não é de (12), e, neste caso, temos a identidade, pois numa reta, com $2^n + 1$ pontos, a involução é a identidade, se tiver dois pontos unidos.

Daí, concluimos que o espaço união de P_r e P_s é de pontos unidos, em desacordo com a observação feita anteriormente; portanto, toda raiz de (13) é de (12).

2. Suponhamos que N seja par. Estudemos o caso em que $p \neq 2$ e em que a equação (12) tem solução em K.

Teremos duas raizes k_1 e k_2, às quais correspondem dois espaços de pontos unidos P_r e P_s.

TEOREMA 2. O espaço união de P_r e P_s é P_N [34, pag.154].

Com efeito, por qualquer ponto do P_N, fora de P_r e de P_s, passa uma reta onde está subordinada uma involução, e que tem um ponto unido em P_r e outro em P_s. Esta reta pertence ao espaço união de P_r e P_s e, portanto, o mesmo acontece com todos os seus pontos. Desta forma, vemos que todos os pontos de P_N estão no espaço união e como não há ponto fora do P_N, o espaço união de P_r e P_s é P_N.

Conforme vimos no teorema 2 do § 3º dêste capítulo, $P_r \cap P_s = \emptyset$, donde temos a relação

(18) $$N - 1 = r + s.$$

Para a raiz k_1, à qual corresponde P_r, a matriz A terá característica N+1-r.

Pela (18), temos:

(19) $$N+1-r = N+1-(N-1-s) = 2+s .$$

De (19), vem:

(20) $$N+1-s = 2+r .$$

O número de homografias involutórias com espaços P_r e P_s neste caso é dado pela fórmula do nº 3, do § 4º, do cap. I, em que s=N-r-1 e d=-1, ou seja:

$$(21)\quad q^{(r+1)(N-r)} \frac{\prod_{i=0}^{r} (q^{N+1-i}-1)}{\prod_{i=0}^{r} (q^{r+1-i}-1)} = q^{(r+1)(N-r)} \prod_{i=0}^{r} \frac{q^{N+1-i}-1}{q^{r+1-i}-1} .$$

O número total de homografias involutórias é, então, dado por

$$(22)\quad \frac{1}{2} \sum_{r=1}^{N} q^{(r+1)(N-r)} \prod_{i=0}^{r} \frac{q^{N+1-i}-1}{q^{r+1-i}-1} \quad [34, pag.178].$$

Em particular, o número de homologias harmônicas é fornecido por (21), onde $r=1$, isto é:

$$(23)\quad q^{2(N-1)} \prod_{i=0}^{1} \frac{q^{N+1-i}-1}{q^{2-i}-1} = q^{2(N-1)} . \frac{q^{N+1}-1}{q^{2}-1} . \frac{q^{N}-1}{q-1} .$$

3. Discutamos, agora, o caso em que (12) não tem solução em K. Nesta hipótese, devemos procurar as soluções em K' e, como se sabe da Álgebra, $r=s$.

Consluimos, então, de (20), que $N+1 = 2(1+r)$, isto é, $N+1$ é par, o que é absurdo, pois N é par. Disto se infere o

TEOREMA 3. Não há homografias involutórias sem pontos unidos, se N fôr par e $p\neq 2$.

Suponhamos, agora, N par e $p=2$.

Vamos admitir que a (12) tenha solução em K. Neste caso, pela Álgebra, vemos que sòmente há uma solução k_1, à qual corresponde um espaço de pontos unidos P_r.

Como vimos, no § 3º, nº 1, teremos um $\overline{P}_r$ de hiperplanos unidos, os quais terão em comum um P_{N-r+1} unido.

TEOREMA 4. O espaço unido P_{N+1-r} está contido no espaço de pontos unidos P_r, isto é, $N+1-r \leq r$ ou $r \geq \frac{N+1}{2}$ [34, pag.156]

Consideremos os espaços $P_i = P_{N+1-r} \cap P_r$ e P_u, o espaço união de P_{N+1-r} e P_r.

Vemos que $P_i \neq \emptyset$, pois, a involução subordinada pela homografia no P_{N+1-r} tem pontos unidos e êstes pertencem ao P_r.

Seja $Q \not\in P_u$ um pontode P_N. É claro que o ponto Q', correspondente de Q, é distinto de Q. Na reta QQ' existe uma involução e, portanto, há ponto unido. Por isto, se infere que QQ' encontra P_r e não é contida em P_u.

Considerado, agora, o espaço P_{N+2-r} determinado por P_{N+1-r} e pelo ponto Q, vemos que é unido, pois, todos os hiperplanos por P_{N+1-r} são unidos e, por conseguinte, o ponto $Q' \in P_{N+2-r}$.

A reta QQ', então encontra o P_{N+1-r} e como não pode estar contida em P_u, concluimos que os seus pontos de encontro com P_r e com P_{N+1-r} não são distintos, logo temos um ponto $L \in P_i$.

O espaço de P_u com Q é unido.

Como Q é arbitrário em P_N, então, é fácil ver que todo hiperplano que contém P_i é unido e $P_i \supset P_{N+1-r}$. Mas $P_i \subset P_{N+1-r}$, logo $P_i \equiv P_{N+1-r}$ e, portanto, $P_{N+1-r} \subset P_r$, isto é,

$$r \geqq \frac{N+1}{2} .$$

Como N é par, então P_{N+1-r} é sub-espaço próprio de P_r, isto é, $r > (N+1)/2$.

O número de homografias involutórias, neste caso, é dado pelo de espaços P_{N-r+1} e P_r com intersecção P_{N-r+1}, isto é, na fórmula do nº 3, do § 4º, do cap. I, devemos colocar $s=N+1-r$ e $d=N+1-r$, de onde vem:

$$(24) \qquad \frac{q^{[N+1-r-(N+1-r)][r-(N+1-r)]}}{\left[\prod_{i=0}^{N}(q^{N+1-i}-1)\right]^3} \, .$$

$$\cdot \prod_{i=o}^{r+N+1-r-(N+1-r)+2}(q^{N+1-i}-1) \prod_{i=o}^{N-r+N+1-r}(q^{N+1-i}-1) \prod_{i=o}^{N-(N+1-r)-1}(q^{N+1-i}-1) \, .$$

$$\cdot \prod_{i=o}^{N-(N+1-r)+N+1-r}(q^{N+1-i}-1) =$$

$$= \frac{\prod_{i=0}^{r+2}(q^{N+1-i}-1)\prod_{i=0}^{2(N-r)+1}(q^{N+1-i}-1)\prod_{i=0}^{r-2}(q^{N+1-i}-1)\prod_{i=0}^{N}(q^{N+1-i}-1)}{\left[\prod^{N}(q^{N+1-i}-1)\right]^3} .$$

O número total é dado para r variando até N, mas com $r > \frac{N+1}{2}$.

5. Suponhamos que a equação (12) não tenha solução em K. Neste caso, vale o

TEOREMA 5. Não há homografia involutória sem pontos unidos, se N é par e p = 2.

Com efeito, na hipótese do teorema, a equação (12) não tem solução em K, e, então, $P_r \equiv P_{N+1-r}$ isto é, $r = (N+1)/2$; pois se $2r > N+1$, $2r \geqq N+2$, e daí, $2(N+1)-2r \leqq 2(N+1)-(N+2)$, ou $2(N+1-r) \leqq N$.

O P_r pode ser representado por N+1-r equações independentes, da forma

$$(25)\quad \begin{cases} (a_{oo}-\sigma_1)x_o + \cdots\cdots\cdots\cdots\cdots + a_{oN}x_N = 0 \\ a_{1o}x_o \quad + (a_{11}-\sigma_1)x_1 + \cdots\cdots\cdots + a_{1N}x_N = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{N-r,o}x_o + \cdots\cdots + (a_{N-r,N-r}-\sigma_1)x_{N-r,N-r} + \cdots \\ \qquad \cdots + a_{N-r,N}x_N = 0 . \end{cases}$$

Porém, em K, o sistema de 2(N+1-r) equações:

$$\begin{cases} a_{oo}x_o + \cdots\cdots\cdots\cdots\cdots\cdots\cdots + a_{oN}x_N = 0 \\ \quad x_o \qquad\qquad\qquad\qquad\qquad = 0 \\ a_{1o}x_o + \cdots\cdots\cdots\cdots\cdots\cdots\cdots + a_{1N}x_N = 0 \\ \qquad\qquad x_1 \qquad\qquad\qquad = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{N-r,o}x_o + \cdots\cdots\cdots\cdots\cdots + a_{N-r,N}x_N = 0 \\ \qquad\qquad\qquad\qquad x_{N-r,N-r} = 0 \end{cases}$$

teria solução não trivial, pois $2(N+1-r) \leqq N$; logo, haveria ponto unido no P_r, contra a hipótese.

Disto inferimos que $P_r \equiv P_{N-r+1}$ e $2r = N+1$, o que é absurdo, visto que N é par.

6. Passemos a estudar o caso em que N é impar e $p \neq 2$.

Suposto que a (12) tenha solução em K, estamos na situação do nº 2, com os mesmos resultados, inclusive o cálculo.

7. Se a (12) não tem solução, então, com o raciocínio do nº3, vemos que $2r = N+1$, o que é possível, pois N é impar; assim temos uma homografia no P_N, sem pontos unidos.

Tomamos, então, um $P_{\frac{N+1}{2}-1} \subset P_N$ e o seu correspondente pela homografia, $P'_{\frac{N+1}{2}-1}$. É claro que $P_{\frac{N+1}{2}} \cap P'_{\frac{N+1}{2}} = \emptyset$.

As equações ficam, pois:

$$(27)\quad \begin{cases} \sigma x_0 = k_1 x_{r+1} \\ \sigma x_1 = k_1 x_{r+2} \\ \dots\dots\dots\dots\dots\dots \\ \sigma x_r = k_1 x_N \\ \sigma x_{r+1} = k_1 x_0 \\ \dots\dots\dots\dots\dots\dots \\ \sigma x_N = k_1 x_r \end{cases}$$

O determinante do sistema é nulo, e é dado por:

$$(28)\quad \begin{vmatrix} \sigma & 0 & \dots & 0 & -k_1 & 0 & \dots & 0 \\ 0 & \sigma & \dots & 0 & 0 & -k_1 & \dots & 0 \\ \dots & & & & & & & \dots \\ 0 & 0 & \dots & \sigma & 0 & 0 & \dots & -k_1 \\ -k_1 & 0 & & 0 & \sigma & 0 & \dots & 0 \\ \dots & & & & & & & \dots \\ 0 & 0 & \dots & -k_1 & 0 & 0 & \dots & \sigma \end{vmatrix}$$

No determinante (28), multiplicando-se os elementos da 1ª linha por k_1 e somando-se aos da (r+2)ª multiplicados por σ, vem:

$$(29)\qquad \left|\begin{array}{cccccccc} \sigma & 0 & \cdots & 0 & -k_1 & 0 & \cdots & 0 \\ 0 & \sigma & \cdots & 0 & 0 & -k_1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & \sigma & 0 & \cdots & -k_1 \\ 0 & 0 & \cdots & \sigma^2 & -k_1^2 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & -k_1 & 0 & 0 & \cdots & \sigma \end{array}\right| .$$

Efetuando esta operação r vezes, para as linhas 2ª e (r+3)ª, etc., vem que o determinante (28) é

$$(\sigma^2 - k_1^2)^r \sigma^r = 0, \text{ donde } \sigma^2 = k_1^2 = \lambda .$$

Assim, o número de tais homografias é o de pares de $P_{\frac{N+1}{2}-1}$ com intersecção vazia. Vale, então, a fórmula

$$(30)\qquad q^{(\frac{N+1}{2})^2} \cdot \frac{\prod_{i=0}^{N+2}(q^{N+1-i}-1)\left[\prod_{i=0}^{\frac{N-1}{2}}(q^{N+1-i}-1)\right]^2}{\left[\prod_{i=0}^{N}(q^{N+1-i}-1)\right]^2}$$

8. Seja o caso de p=2 e em que a (12) tem solução em K. Então, estamos na hipótese do nº4, inclusive o cálculo.

9. Se a (12) não tem solução em K, vale o mesmo que no nº 5 e 2r = N+1.

Aí, escolhidos como no nº 7, o espaço $P_{\frac{N+1}{2}-1}$ e o correspondente $P'_{\frac{N+1}{2}-1}$, temos $P_{\frac{N+1}{2}-1} \cap P'_{\frac{N+1}{2}-1} = \emptyset$, donde o número de homografias é o mesmo que em 7.

BIBLIOGRAFIA

1. G. FANO - Sui postulati fondamentali della G. Proiettiva in uno spazio lineare a um numero qualunque di dimensioni. Gionali di Matematica (30)-1892 (por citação).
2. B. LEVI - Fondamenti della metrica proiettiva. R. Acc. delle Scienze di Torino, ser.2,vol. 54-1904 (por citação).
3. O. VEBLEN and BUSSEY - Finite Projective Geometry. Trans. Amer. Math. Soc., vol. 7, nº 2-1906.
4. O. VEBLEN - Collineations in a Finite Projective Geometry. Trans. Amer. Math. Soc., vol. 8, n+ 3-1907.
5. B. LEVI - Geometrie Proiettive di Congruenza e Geometrie Proiettive e Finite. Idem, do nº 4.
6. O. VEBLEN and J. W. YOUNG - Projective Geometry - vol I (1910) e vol. II (1918) - Ginn & Co., Boston.
7. R. D. CARMICHAEL - Finite Geometries and the Theory of Groups. Amer. J. of Mathematics, vol. LII, 4, 1930.
8. R. MOUFANG - Zur Struktur der projectiven Geometrie der Ebene. Math. Ann., vol. 105-1931.
9. Idem. - Die Einführung der idealen Elemente in die ebene Geometrie mit Hilfe des Satzes von vollstandigen Vierseit. Math. Ann., vol. 105-1931.
10. Idem - Die Schnittpunktsatze des projektiven speziellen Fünfecksnetzes in ihrer Abhangigkeit voneinder. Math. Ann., vol. 106-1932.
11. Idem - Ein Satz uber die Schnittpunktsatze des allgemeinen Fünfecksnetzes. Math. Ann., vol. 107-1932.
12. Idem - Die Desarguesschen Satz von Rang 10. Math. Ann., vol. 108-1939.
13. Idem - Alternativkörper und der Satz von vollstandigen Vierseit. Abh. Math. Sem. Hamburgischen Univ., vol. 9-1939 (por citação).
14. Idem - Zur Struktur von Alternativkörpern. Math. Ann., vol. 110-1934.
15. R. BRAUER - A characterization of null systems in projective space. Bull. Amer. Math. Soc., vol. 42-1936.
16. J. SINGER - A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc., vol. 43, nº 3-1938.
17. R.BAER - A unified theory of projective spaces and finite abelian groups. Trans. Amer. Math. Soc., vol. 52, nº 2-1942.
18. Idem - Homogeneity of projective planes. Amer. J. of Mathem., vol. 64-1942.
19. F. W. LEVI - Finite Geometrical Systems. The University of Calcutta, 1942.
20. M. HALL - Projective planes. Trans.Amer.Math.Soc., vol. 54, nº 2-1943.

21. R. BAER - Nul systems in Projective Space. Bull. Amer. Math. Soc., vol. 51, nº 12-1945.
22. Idem - Polarities in Finite Projective Plane. Bull. Amer. Math. Soc., vol. 52, nº 2-1946.
23. Idem - Projectivities with fixed points on every line of the plane. Bull. Amer. Math. Soc., vol. 52, 1946.
24. Idem - Projectivities of Finite Projective Planes. Amer. J. of Math., vol. LXIX, nº 14-1947.
25. C. T. YANG - Projective collineations in a Finite Projective Plane. Mathematical Institute National University of Chekiang-Hongchow, China, 1947.
26. R. A. FISCHER - The Design of Experiments. Edimburgh, 1937 (por citação).
27. F. YATES - The Design and Analysis of Factorial Experiments. Imperial Bureau of Soil Science. Technical Communication nº 35-1937 (por citação).
28. R. C. BOSE - On the application of the properties of Galois Fields to the problem of construction of Hyper-Graeco-Latin squares. Sankhya, vol. 3, 4-1938.
29. W. L. STEVENS - The completely orthogonalized Latin square. Annals of Eugenics, vol. 9-1939 (por citação).
30. R. C. BOSE and K. R. NAIR - On complets sets of Latin squares. Sankhya, vol. 5, 4-1941.
30'. W. L. STEVENS - Desenvolvimentos modernos do delineamento de experimentos. Instituto Agronômico. Campinas, 1949.
31. O. SCHREIER und E. SPERNER - Einführung in die Analytische Geometrie und Algebra, vols. I e II, 1935, Teubner, Leipsig.
32. R. D. CARMICHAEL - Groups of Finite Order. Ginn & Co., Boston, 1937.
33. M. STECK - Crelles Journal . -179-1938 (por citação).
34. B. SEGRE - Lezioni di Geometria Moderna. Zanichelli, Bolonha, 1948.
35. N. BOURBAKI - Théorie des Ensembles. Hermann & Cie. Paris, 1939.
36. E. FARAH - Sôbre a medida de Lebesgue. Gráfica Omega. S.Paulo, 1950.
37. A. LICHNEROWICZ - Algèbre et Analyse Linéaires. Masson & Cie. Paris, 1947.
38. G. BIRKHOFF and S. MACLANE - A Survey of Modern Algebra. MacMillan Co., N.Y., 1944.
39. G. de B. ROBINSON - The Foundations of Geometry. The University of Toronto Press, Canadá, 1940.
40. G. HESSENBERG - Beweis des Desarguesschen Satzes aus dem Pascalschen. Math. Annalen, vol. 61-1905.
41. M. G. DARBOUX - Sur le Théorème Fondamental de la Géometrie Projective. Math. Annalen, vol. 17-1880.
42. B. CASTRUCCI - Cálculo da ordem do grupo de homografias do espaço N-dimensional sôbre um corpo de ordem $q=p^n$. Boletim da Soc. de Mat. de S. Paulo, 1949.

43. J. A. DIEUDONNÉ - Teoria dos Corpos Comutativos, vol. II. Soc. de Matemática de S. Paulo, 1947.
44. C. C. MAC-DUFFEE - Veetors and Matrices. The Mathematical Association of America, 1943.
45. L. E. DICKSON - Modern Elementary Theory of Numbers. The University of Chicago Press, Illinois, 1943.
46. G. SCORZA - Corpi Numerici e Algebre. Casa Principato. Messina, 1921.

ÍNDICE

Mimeografado por Geraldo dos Santos Lima Filho.
Departamento de Matemática da Faculdade de Filosofia, Ciências e Letras da Universidade de São Paulo.