Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Hipercubos não-singulares e aplicações ao estudo de semicorpos finitos

por

Josimar da Silva Rocha

Brasília

2011

Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Hipercubos não-singulares e aplicações ao estudo de semicorpos finitos

por

Josimar da Silva Rocha *

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

Mestre em Matemática

27 de setembro de 2001

Comissão Examinadora:

Prof. Noraí Romeu Rocco - MAT/UnB (Orientador)

Prof. Said Najati Sidki - MAT/UnB (Membro)

Prof. Alexandre Grichkov - IME/USP (Membro)

*O autor foi bolsista da CAPES durante a elaboração deste trabalho.

Resumo

Neste trabalho estudamos semicorpos finitos e suas representações por 3-cubos não-singulares, bem como a presença de semicorpos como anéis ternários coordenatizando planos projetivos não-desarguesianos. O conceito de isotopia e o seu significado geométrico são explorados. Este contexto permite-nos caracterizar o subgrupo das translações e *shears* do grupo de colineações de um plano coordenatizado por um semicorpo. Concluímos com exemplos de semicorpos próprios de todas as ordens possíveis.

Palavras chaves: Semicorpos; Hipercubos não-singulares; Planos projetivos não-desarguesianos.

Resumo

In this work we study finite semifields and its representations by nonsingular 3-cubes, as well as the presence of semifields as ternary rings coordinatizing non-Desarguesian projective planes. The concept of isotopy and its geometric meaning are explored. This context allows us to characterize the subgroup of the translations and shears of the group of colineations of a plane coordinatized by a proper semifield. We conclude with examples of proper semifields of all possible orders.

Keywords: Semifields; Nonsingular hypercubes; Non-Desarguesian projective planes.

Agradecimentos

Agradeço a Deus, por mais esta conquista.

Agradeço a minha mãe, pelo incentivo, pela compreensão nos momentos difíceis e pela confiança que depositou em mim.

Agradeço ao Prof. Noraí Romeu Rocco, o orientador deste trabalho, pelas sugestões, ensinamentos, e pela ajuda na escolha do tema dessa dissertação.

Agradeço à Tânia Maria S. Sertão, da secretaria de pós-graduação, pela maneira simpática, carinhosa e eficiente com que resolve as burocracias de nossa vida acadêmica.

Agradeço a todos os meus amigos, pelo carinho, alegria, estímulo e companheirismo, fatores essenciais nesta fase de minha vida.

Agradeço aos demais professores e funcionários do Departamento de Matemática da Universidade de Brasília, que de alguma forma contribuíram para a realização deste trabalho.

Finalmente, agradeço à CAPES, pelo suporte financeiro.

Sumário

Introdução

O objetivo principal desta dissertação é o estudo dos semicorpos, isto é, sistemas algébricos munidos de duas operações fundamentais, adição e multiplicação, satisfazendo propriedades semelhantes às que definem um corpo, com exceção eventual da comutatividade e associatividade na multiplicação. Tais sistemas (semifields) são também chamados de anéis de divisão não-associativos (semicorpos próprios). Estes são de interesse especial porque os planos projetivos construídos a partir deles têm propriedades especiais. O artigo de D. Knuth [12] serviu como referência básica para a elaboração deste trabalho.

No Capítulo 1 abordamos as definições básicas e as propriedades fundamentais de semicorpos finitos e de anéis de divisão, onde também apresentamos dois exemplos de semicorpos próprios de ordem 16.

Um tratamento geométrico é considerado no Capítulo 2, onde abordamos conceitos fundamentais e alguns resultados da *Geometria Projetiva* necessários para o desenvolvimento subseqüente. Para tanto, introduzimos coordenadas homogêneas para representar pontos e retas de um plano projetivo arbitrário, em termos de seu anel ternário. O conceito de isotopia é generalizado quando aplicamos a anéis ternários arbitrários, e apresentamos um método de Knuth para construção de todos os anéis ternários isotópicos a um dado anel ternário. Alguns teoremas sobre colineações de planos, e de semicorpos em particular, são provados usando notação homogênea. Finalmente, analisando a estrutura e as propriedades do subgrupo gerado pelas translações e *shears* do grupo das colineações de um plano coordenatizado por um semicorpo, abordamos a seguinte questão:

> *Seja p um número primo. Descrever todos os grupos de ordem p^{3n}, de classe de nilpotência 2, contendo subgrupos X e Y tais que $|X| = |Y| = p^n$ e quaisquer*

elementos não-triviais $x \in X$ e $y \in Y$ não comutam (cf. [14], Problema 10.1; veja também [16]).

Os hipercubos de dimensão finita são o assunto do Capítulo 3. Primeiramente, discutimos operações de adição e multiplicação sobre estes hipercubos. Posteriormente, introduzimos a noção de hipercubos *não-singulares*. Mostramos que semicorpos são equivalentes a certos tipos de 3-cubos (hipercubos tridimensionais) e que planos projetivos coordenatizados por semicorpos estão em correspondência biunívoca com as classes de equivalência dos 3-cubos não-singulares.

No Capítulo 4 abordamos rapidamente os conceitos de dual e transposto de um plano projetivo. Utilizamos isto para verificar que a cota superior para o número de isótopos não-isomorfos de um dado anel ternário (Capítulo 2 - Teorema 5) é a melhor possível.

Finalizamos o trabalho com o Capítulo 5, onde discutimos a questão das possíveis ordens de um semicorpo próprio. Verificamos que tais semicorpos têm ordens da forma p^n, com p primo, $n \geq 3$ e $p^n \geq 16$. Uma série de exemplos subseqüentes mostram que essas condições são suficientes para a existência dos mesmos.

Capítulo 1

Semicorpos e Pré-semicorpos

1.1 Semicorpos e anéis de divisão

Definição 1. *Um* **semicorpo finito** S *é um sistema algébrico finito contendo ao menos dois elementos;* S *possui duas operações binárias, adição e multiplicação, que satisfazem os seguintes axiomas:*

A1. *Para a adição é um grupo, com elemento identidade* 0.

A2. *Se* $ab = 0$, *então* $a = 0$ *ou* $b = 0$.

A3. $a(b + c) = ab + ac$; $(a + b)c = ac + bc$, *para todos* $a, b, c \in S$.

A4. *Existe um elemento* 1 *em* S *tal que* $1a = a1 = a$, *para todo* $a \in S$.

Aqui o termo semicorpo será usado apenas para designar um semicorpo finito. A definição acima é insuficiente para semicorpos infinitos, pois o axioma $A2$ deve ser substituido pela condição de que as equações $ax = b$ e $ya = b$ são unicamente solúveis para x e y.

Semicorpo é muito semelhante a um corpo, exceto que a multiplicação por elementos não-nulos é meramente um *loop* em vez de um grupo abeliano.

Todo corpo é um semicorpo. O termo **semicorpo próprio** será utilizado para denotar um semicorpo finito que não é um corpo; i.e., existem elementos a, b, c tais que $(ab)c \neq a(bc)$ em um semicorpo próprio.

Definição 2. *Um* **anel de divisão** *(ou skewfield) K é um sistema algébrico contendo pelo menos dois elementos, 0 e 1; K possui duas operações binárias, adição e multiplicação, satisfazendo os seguintes axiomas:*

(1) Para a adição é um grupo abeliano, com elemento identidade 0;

(2) Para a multiplicação entre elementos não-nulos de K é um grupo (não necessariamente abeliano), com elemento identidade 1;

(3) $a(b+c) = ab + ac$ e $(a+b)c = ac + bc$ para todos $a, b, c \in K$.

Todo corpo é um anel de divisão e todo anel de divisão finito é um corpo (Teorema de Wedderburn).

No Capítulo 2 veremos que os anéis de divisão coordenatizam planos projetivos desarguesianos enquanto os semicorpos próprios coordenatizam planos projetivos não-desarguesianos.

Os semicorpos próprios são também chamados de anéis de divisão não-associativos.

1.2 Exemplos de semicorpos

O seguinte sistema V é um semicorpo próprio com 16 elementos: seja F o corpo $GF(4)$ com elementos 0, 1, ω e $\omega^2 = \omega + 1$. Os elementos de V são da forma $x + \lambda y$, onde $x,\ y \in F$. A adição é definida de maneira óbvia:

$$(u + \lambda v) + (x + \lambda y) = (u + x) + \lambda(v + y) \tag{1.1}$$

usando a adição de F. A multiplicação é também definida em termos da multiplicação e da adição de F, usando a seguinte regra:

$$(u + \lambda v)(x + \lambda y) = (ux + v^2 y) + \lambda(vx + u^2 y + v^2 y^2). \tag{1.2}$$

Claramente, $F \subset V$, e V, com estas operações, satisfaz **A1, A3** e **A4.** Para demonstrar **A2,** suponhamos que $(u + \lambda v)(x + \lambda y) = 0$. Assim,

$$\begin{cases} ux + v^2 y = 0 \\ vx + u^2 y + v^2 y^2 = 0 \end{cases}$$

Em particular, $ux + v^2y = 0$, e se nenhum dos fatores desta equação é nulo, então existe um elemento não-nulo $z \in F$ tal que $x = zv^2$ e $y = zu$. Então

$$vx + u^2y + v^2y^2 = zv^3 + zu^3 + z^2u^2v^2 = 0.$$

Mas isto é impossível em F, a menos que $u = v = 0$. No caso em que algum fator de $ux + v^2y = 0$ é nulo, temos

$$\begin{cases} ux = 0 \\ v^2y = 0 \\ vx + u^2y = 0 \end{cases} .$$

Assim:

- se $x = 0$ então ($u^2y = 0$ e $v^2y = 0$), donde segue que ($y = 0$ ou $u + \lambda v = 0$);
- se $u = 0$ então ($v^2y = 0$ e $vx = 0$), donde segue que ($v = 0$ ou $x + \lambda y = 0$).

Além disso, V é um semicorpo próprio, pois V não é comutativo ($\omega\lambda = \lambda\omega^2 \neq \lambda\omega$). Para analizarmos o grau de associatividade em V, sejam $u + \lambda v$, $x + \lambda y$ e $m + \lambda n$ elementos de V. Assim,

$$(u + \lambda v)\left((x + \lambda y)(m + \lambda n)\right) + \left((u + \lambda v)(x + \lambda y)\right)(m + \lambda n)$$

$$= \left[vyn + v^2y^2n^2\right] + \lambda\left[v^2y^2(m + m^2) + v^2n^2(x + x^2) + y^2n^2(u + u^2) + vy(n^2 + vn)\right]$$

o qual será nulo se quaisquer dois elementos do conjunto $\{u + \lambda v,\ x + \lambda y,\ m + \lambda n\}$ estiverem em F; ou, equivalentemente, $a(bc) = (ab)c$ sempre que quaisquer dois elementos do conjunto $\{a, b, c\}$ estão em F.

Agora, mostraremos que V possui 6 automorfismos, enquanto um corpo de 16 elementos possui apenas 4 automorfismos. Afirmamos que todos os automorfismos de V são do tipo σ_{ij}, dados por:

$$(u + \lambda v)\sigma_{ij} = u^j + \lambda\omega^i v^j \ \text{ para } \ i = 0,\ 1,\ 2;\ j = 1,\ 2. \tag{1.3}$$

De fato, como

$$\left((u + \lambda v)(x + \lambda y)\right)\sigma_{ij} = \left((ux + v^2y) + \lambda(vx + u^2y + v^2y^2)\right)\sigma_{ij}$$

$$= (ux + v^2y)^j + \lambda\omega^i(vx + u^2y + v^2y^2)^j$$

$$= [x^ju^j + \omega^{3i}v^{2j}y^j] + \lambda[\omega^iv^jx^j + u^{2j}\omega^iy^j + \omega^{4i}y^{2j}v^{2j}]$$

$$= (u^j + \lambda\omega^iv^j)(x^j + \lambda\omega^iy^j) = ((u + \lambda v)\sigma_{ij})\,((x + \lambda y)\sigma_{ij})\,,$$

então σ_{ij} é um automorfismo de V. Além disso, λ e ω satisfazem

$$\begin{cases} \omega(\lambda\omega) + (\omega\lambda)\omega = 0 \\ \lambda(\omega\lambda) + (\lambda\omega)\lambda \neq 0 \\ \lambda^2 = 1 + \lambda \\ \omega^2 = 1 + \omega \\ \omega\lambda = \lambda\omega^2 \end{cases} \tag{1.4}$$

Denotando por ω^σ e λ^σ as imagens de ω e λ por um automorfismo σ, temos

$$\begin{cases} \omega^\sigma(\lambda^\sigma\omega^\sigma) + (\omega^\sigma\lambda^\sigma)\omega^\sigma = 0 \\ \lambda^\sigma(\omega^\sigma\lambda^\sigma) + (\lambda^\sigma\omega^\sigma)\lambda^\sigma \neq 0 \\ (\lambda^\sigma)^2 = 1 + \lambda^\sigma \\ (\omega^\sigma)^2 = 1 + \omega^\sigma \\ \omega^\sigma\lambda^\sigma = \lambda^\sigma(\omega^\sigma)^2 \end{cases} \tag{1.5}$$

Portanto,

$$\omega^\sigma \in \{\omega,\, \omega^2\} \;\text{ e }\; \lambda^\sigma \in \{\lambda,\, \lambda\omega,\, \lambda\omega^2\},$$

e todos os automorfismos de V são como em (1.3).

Outro exemplo que tem propriedades em comum com V é o sistema W, obtido definindo-se a multiplicação pela regra

$$(u + \lambda v)(x + \lambda y) = (ux + \omega v^2y) + \lambda(vx + u^2y), \tag{1.6}$$

em vez da regra dada por (1.2). Este sistema é outro semicorpo próprio contendo F e tem a propriedade de $(ab)c = a(bc)$ sempre que qualquer elemento do conjunto $\{a, b, c\}$ pertencer a F. Os automorfismos de W são da forma σ_i, dados por $(a+\lambda b)\sigma_i = a+\lambda\omega^ib$ para $i = 0, 1, 2$.

No Capítulo 5 veremos que um semicorpo próprio precisa ter pelo menos 16 elementos.

1.3 Pré-semicorpo

Definição 3. *Dizemos que um sistema algébrico S é um pré-semicorpo se satisfaz os axiomas* **A1**, **A2** *e* **A3**, *mas que não precisa, necessariamente, satisfazer o axioma* **A4** *da definição de semicorpo.*

Um exemplo muito simples de pré-semicorpo pode ser construído a partir de um corpo F que possui mais de um automorfismo. Se $\sigma \neq I$ é um automorfismo, defina uma nova operação de multiplicação $\circ$ sobre os elementos de F por $x \circ y = (xy)^{\sigma}$. Então F com operação de adição $+$ e com operação de multiplicação $\circ$ é um pré-semicorpo; pois $1 \circ 1 = 1$ implica em 1 ser a identidade multiplicativa, se esta existir, já $1 \circ y = y^{\sigma} \neq y$ para algum y.

No Capítulo 4 veremos que um pré-semicorpo finito pode ser visto como um vetor com n^3 entradas em $\mathbb{Z}$ e que um semicorpo pode ser construído através de um pré-semicorpo.

1.4 O grupo aditivo

É fácil mostrar que o grupo aditivo de um pré-semicorpo S é comutativo. Pelas leis distributivas,

$$(ac + ad) + (bc + bd) = (a + b)(c + d) = (ac + bc) + (ad + bd).$$

Conseqüentemente, por **A1,** $ad + bc = bc + ad$, e qualquer elemento que puder ser escrito como produto comuta sobre a adição. Mas por **A2** e pela finitude, qualquer elemento de S pode ser escrito como produto; logo, o grupo aditivo é abeliano.

Outro argumento igualmente simples mostra que o grupo aditivo é **abeliano elementar.** De fato, sejam $a \neq 0$ e p a ordem aditiva de a. Então p é primo, já que $(na)(ma) = ((mn)a)a$ para $n, m \in \mathbb{Z}$. O fato de que todo elemento não-nulo tem ordem prima é suficiente para mostrar que o grupo é abeliano elementar; isto é, todos os elementos não-nulos têm a mesma ordem prima p. Este número p é chamado *característica* do pré-semicorpo.

1.5 Representação por espaço vetorial

Seja S um pré-semicorpo e F o corpo $GF(p)$, onde p é a característica de S. Então podemos considerar os elementos de F como "escalares", e S como um espaço vetorial sobre F. Em particular, S tem p^n elementos, onde n é a dimensão de S sobre F.

As observações do parágrafo anterior são bastante úteis pois muitos conceitos de semicorpos e pré-semicorpos são traduzidos em termos de espaços vetoriais. Isto será explorado no Capítulo 3. Podemos, por exemplo, parafrasear as leis distributivas como a seguir: Seja a um elemento não-nulo de S, e definamos funções L_a e R_a por

$$bL_a = ab \ \text{ e } \ bR_a = ba, \ \text{ para todo } \ b \in S. \tag{1.7}$$

Então as leis distributivas **A3** são equivalentes à afirmação de que L_a e R_a são transformações lineares do espaço vetorial em si mesmo. Além disso, o axioma **A2** estabelece que estas transformações são todas não-singulares se $a \neq 0$. Portanto, L_a e R_a podem ser representados como matrizes não-singulares com elementos em $GF(p)$.

1.6 Núcleos

Para um dado semicorpo S podemos também considerar os seguintes sistemas, os quais indicam certo grau de associatividade do semicorpo:

Núcleo à esquerda : $N_l := \{x \in S \mid (xa)b = x(ab), \forall a,\ b \in S\}$

Núcleo médio : $N_m := \{x \in S \mid (ax)b = a(xb), \forall a,\ b \in S\}$

Núcleo à direita : $N_r := \{x \in S \mid (ab)x = a(bx), \forall a,\ b \in S\}$

O **núcleo** N é a interseção dos núcleos à esquerda, médio e à direita. O corpo $GF(p)$, onde p é a característica de S, é sempre parte do núcleo.

Em muitos casos, o núcleo será trivial, igual a $GF(p)$, onde p é a característica do semicorpo. Este é o caso do sistema V na Seção 1.2. Mas o sistema W da mesma seção possui núcleo $F = GF(4)$.

Cada um dos núcleos é um corpo. Para verificar isto, consideremos, por exemplo, o núcleo à esquerda N_l. As seguintes propriedades são verificadas:

(A) 1 e 0 pertencem a N_l.

(B) Se x e y pertencem a N_l então $x+y$ e xy pertencem a N_l.

(C) Se $x \in N_l$ então $-x \in N_l$.

(D) Se $z \in N_l$ então existe $\overline{z} \in N_l$ tal que $z\overline{z} = \overline{z}z = 1$.

Demonstração. (A) $(0a)b = 0 = 0(ab)$ e $(1a)b = 1(ab)$.

(B) Se x e y pertencem a N_l, então,

$$((x+y)a)b = (xa+ya)b = (xa)b + (ya)b = x(ab) + y(ab) = (x+y)(ab)$$

e

$$((xy)a)b = (x(ya))b = x((ya)b) = x(y(ab)) = (xy)(ab).$$

(C) Se x pertence a N_l, então,

$$x(ab) + (-x)(ab) = 0 = (xa)b + ((-x)a)b = x(ab) + ((-x)a)b,$$

que implica em $(-x)(ab) = ((-x)a)b$.

(D) Sejam L_z e R_z as aplicações da seção anterior, onde z é um elemento não-nulo de N_l. Como N_l é fechado para a multiplicação, então L_z e R_z são bijeções de N_l em N_l. Conseqüentemente, existem z_1 e z_2 pertencentes a N_l tais que $z_1 L_z = z_2 R_z = 1$; i.e., $zz_1 = z_2 z = 1$. Assim, $z_2(zz_1) = (z_2 z)z_1$, donde segue que $z_2 = z_1 = \overline{z}$, como queríamos. □

As propriedades (A)-(D) mostram que N_l é um anel de divisão finito e, portanto, um corpo. As outras demonstrações para N_m e N_r são feitas de modo análogo. S é um espaço vetorial sobre qualquer um de seus núcleos; é um espaço vetorial à esquerda sobre N_l, N_m e N; é um espaço vetorial à direita sobre N_m, N_r e N. As operações L_a e R_a definidas pela equação (1.7) não são, necessariamente, transformações lineares sobre o núcleo; mas R_a é uma transformação linear sobre N_l, enquanto L_a é uma transformação linear sobre N_r, quando S é visto como um espaço vetorial à esquerda e à direita, respectivamente.

Capítulo 2

Plano Projetivo e Isotopia

2.1 Definições Básicas

Sejam K um anel de divisão e V um espaço vetorial de dimensão finita sobre K (à esquerda ou à direita). Neste capítulo estudaremos *o reticulado dos subspaços* de V. A coleção dos subespaços de V, junto com a relação natural de inclusão é o que chamaremos de **geometria projetiva** $\pi(V)$**,** e diremos que o subespaço W é **incidente com** o subspaço U se W contém U ou se U contém W. Sempre que for apropriado adotaremos a terminologia padrão, algébrica ou geométrica, como "U está sobre W"(ou "em W"), "W contém U", "W passa por U", etc.

Se V é um espaço vetorial de dimensão n sobre um anel de divisão K, então os subspaços unidimensionais de V serão chamados **pontos,** os subspaços bidimensionais de V serão chamados **retas,** os subspaços tridimensionais de V serão chamados **planos** e os subspaços $(n-1)$-dimensionais serão chamados **hiperplanos.** Se pensarmos em pontos como os elementos mais fundamentais de $\pi(V)$, então a interseção de dois pontos poderá ser o "natural"conjunto vazio: o subspaço de V cuja dimensão é zero será o **espaço nulo** em $\pi(V)$. Se W é um subspaço de V então $\pi(W)$ está contido naturalmente em $\pi(V)$ e todos os elementos de $\pi(W)$ são também elementos de $\pi(V)$, com a mesma dimensão.

Embora estejamos interessados em geometrias projetivas em que V é um espaço vetorial tridimensional sobre o anel de divisão K, neste caso chamadas *Planos Projetivos,* algumas idéias são mais facilmente entendidas quando estamos trabalhando

com espaços vetoriais de dimensão arbitrária.

Olhando para a estrutura de incidência, um plano projetivo pode ser definido também da seguinte forma:

Definição 4. *Um* **Plano Projetivo** *é um conjunto de pontos e retas, junto com uma relação de incidência entre pontos e retas, satisfazendo os seguintes axiomas:*

P1. Cada par de pontos distintos é incidente com uma única reta.

P2. Cada par de retas distintas é incidente com um único ponto.

P3. Existem quatro pontos tais que quaisquer três deles não são incidentes com uma mesma reta.

2.2 Espaço Dual e Coordenadas Homogêneas

Se V é um espaço vetorial à esquerda sobre um anel de divisão K, então um **funcional linear** de V é uma aplicação f' de V em K tal que

(i) para quaisquer v, w em V, $(v+w)f' = vf' + wf'$ e

(ii) para qualquer v em V e k em K, $(kv)f' = k(vf')$.

(Escreveremos os funcionais lineares como vetores colunas no lugar de aplicações). Se f' e g' são dois funcionais lineares, definimos $f'+g'$ por: $v(f'+g') = vf' + vg'$, enquanto se f' é um funcional linear e b é um elemento de K, definimos $f'b$ por: $v(f'b) = (vf')b$. Com estas operações o conjunto V', dos funcionais lineares, é um espaço vetorial à direita sobre K. Se $e_1, e_2, \cdots, e_n$ é uma base de V e se definirmos aplicações f'_i, para $i = 1, 2, \cdots, n$, por $(x_1e_1 + \cdots + x_ne_n)f'_i = x_i$, então não é difícil mostrar que os f'_i's são elementos de V', que são linearmente independentes e que geram V'.

Analisaremos agora o relacionamento existente entre as geometrias $\pi(V)$ e $\pi(V')$. Uma conexão entre estas geometrias projetivas pode ser expressa em termos da aplicação θ_V dos subspaços de V nos subspaços de V' dada por: se $W \subset V$ então $W^{\theta_V} = \{v' \in V' \mid wv' = 0, \text{ para todo } w \in W\}$. Já que os elementos de $\pi(V)$ são os subspaços de V, temos que θ_V é uma aplicação de $\pi(V)$ em $\pi(V')$. Além disso, se V é

um espaço vetorial à esquerda de dimensão n sobre K, então θ_V manda subspaços i-dimensionais de V em subspaços $(n-i)$-dimensionais de V' (*Princípio da Dualidade*). Em particular θ_V manda pontos de $\pi(V)$ em hiperplanos de $\pi(V')$.

Se U é qualquer hiperplano de $\pi(V)$, então o ponto U^{θ_V} em $\pi(V')$ define e é definido unicamente por U. Recordando a definição de θ_V, vimos que o ponto E de $\pi(V)$ está sobre o hiperplano U de $\pi(V)$ se, e somente se, $eu' = 0$ para todo e em E e todo u' em U^{θ_V}. Como E e U^{θ_V} têm dimensão um, E consiste de múltiplos ke, onde k varia sobre K, para algum e não-nulo em E; analogamente U^{θ_V} consiste dos múltiplos $u'k$, onde k varia sobre K para algum vetor não-nulo u' em U^{θ_V}. Assim, podemos representar E por um de seus vetores não-nulos e o hiperplano U por qualquer um dos vetores não-nulos u' em U^{θ_V}. Então a relação de incidência será dada pela regra:

se E é identificado por e, U por u', então E está em U se, e somente se, $eu' = 0$.

Esta importante regra habilita-nos a identificar completamente, por exemplo, todo elemento de um plano projetivo, e toda relação de incidência. Suponhamos que V seja um espaço tridimensional sobre K e V' o seu espaço dual. Então $\pi(V)$ pode ser pensado como o objeto cujos pontos são subspaços unidimensionais de V e cujas retas são subspaços unidimensiomais de V'; aqui a regra de incidência é dada por "anulamento", ou seja, o ponto $E = \langle e \rangle$ está sobre a reta $L' = \langle w' \rangle$ se, e somente se, $ew' = 0$. Se escolhermos um sistema de coordenadas, então $E = \langle (x, y, z) \rangle$ está sobre $L' = \langle (a, b, c)' \rangle$ se, e somente se, $xa + yb + zc = 0$. Isto é, o "produto interno"ordinário do vetor linha (x, y, z) e o vetor coluna (a, b, c) é zero.

Esta regra é eficaz para geometrias projetivas de dimensão maior, já que qualquer geometria projetiva é completamente definida pelos seus pontos e hiperplanos e as relações de incidência entre eles.

Este uso do espaço dual para dar "coordenadas"para hiperplanos conduz ao que chamam de **coordenadas homogêneas:** uma vez que uma base tenha sido escolhida, qualquer ponto pode ser representado por um vetor linha v, ou pelo subspaço $\langle v \rangle$, e qualquer hiperplano por um vetor coluna w', ou pelo subspaço $\langle w' \rangle$. No caso do plano, onde retas e hiperplanos são a mesma coisa, todo elemento é representado ou por um vetor linha ou por um vetor coluna (ou pelos subspaços gerados por eles).

Agora é evidente que se V é um espaço vetorial à direita, então tudo será revertido: os pontos de $\pi(V)$ serão representados por vetores-colunas e as retas de $\pi(V)$, que são os pontos de $\pi(V')$, serão vetores-linhas. O ponto $\langle(x, y, z)'\rangle$ está sobre a reta $\langle(a, b, c)\rangle$ se , e somente se, $ax + by + cz = 0$.

2.3 Introdução de Coordenadas

Seja π um plano projetivo qualquer e escolhamos quatro pontos X, Y, O e I, três a três não-colineares. Chamemos a reta XY *de reta do infinito,* L_∞. A reta OI é dada por $y = x$.

Na reta OI damos as coordenadas $(0, 0)$ para O, $(1, 1)$ para I e a coordenada simples (1) para o ponto C que é a interseção de OI e XY. Para outros pontos de OI assinalemos coordenadas (b, b) tomando diferentes símbolos b para pontos diferentes. Para um ponto P não pertencente à reta L_∞, sejam XP interceptando OI em (b, b) e YP interceptando OI em (a, a). Então assinalemos coordenadas (a, b) para P. Esta regra é compatível com a escolha prévia de coordenadas para os pontos de OI. Suponhamos que a reta que liga $(0, 0)$ e $(1, m)$ intercepte L_∞ no ponto M. Assinalemos para M a coordenada simples (m), que podemos pensar intuitivamente como representando a inclinação da reta unindo O a M. Agora assinalamos coordenadas para todo ponto exceto Y, e para este assinalamos arbitrariamente a coordenada simples (∞) (Veja Fig. 1).

Usaremos as retas de nosso plano para definir operações algébricas no sistema de coordenadas. Este sistema algébrico será um *anel ternário* T, e toda reta de π, exceto L_∞, terá uma equação expressável em termos das operações desse anel ternário. Se (x, y) é um ponto finito de OI, temos $y = x$ e, assim, tomamos $y = x$ como a equação de OI. Uma reta passando por Y diferente de L_∞ terá a propriedade que todos os pontos finitos (x, y) terão a mesma ordenada x, digamos $x = c$.

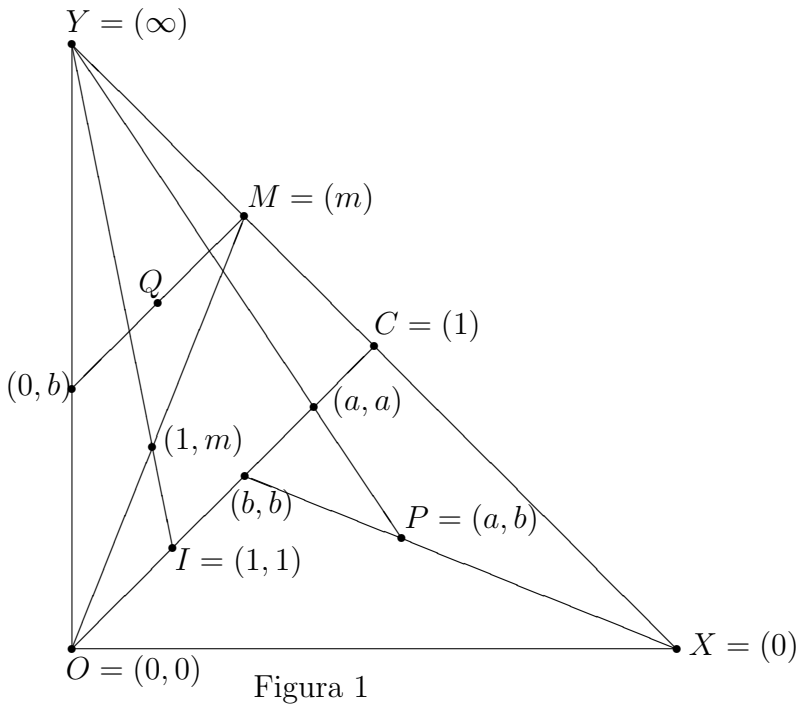


Figura 1

Se (x, y) é um ponto finito da reta unindo $C = (1)$ e $(0, b)$ definimos uma operação binária de adição,

$$y = x + b; \tag{2.1}$$

e tomamos esta como sendo a equação da respectiva reta. Se (x, y) é um ponto finito da reta unindo $O = (0, 0)$ e (m), definimos uma operação binária de multiplicação,

$$y = xm; \tag{2.2}$$

e tomamos esta como sendo a equação da respectiva reta. Em geral, qualquer reta não passando por Y interceptará L_∞ em algum ponto (m) e OY em algum ponto $(0, b)$. Se $Q = (x, y)$ é um ponto desta reta, definiremos uma operação ternária:

$$y = x \cdot m \circ b; \tag{2.3}$$

e tomamos esta como a equação da respectiva reta. Portanto ambos, a adição e a multiplicação, são casos especiais da operação ternária, e vemos que

$$\begin{aligned} x + b &= x \cdot 1 \circ b, \\ xm &= x \cdot m \circ 0. \end{aligned} \tag{2.4}$$

Os elementos 0 e 1 têm as propriedades familiares:

$$\begin{aligned} 0 + a = a + 0 = a, \\ 0m = m0 = 0, \\ 1m = m1 = m. \end{aligned} \tag{2.5}$$

O plano π pode ser representado por um anel ternário T cujas operações ternárias satisfazem as propriedades dadas pelas equações (2.1), (2.2), (2.3), (2.4) e (2.5); reciprocamente, um anel ternário com tais propriedades determina um plano projetivo univocamente. Isto estabelece o teorema principal sobre anéis ternários, cuja demonstração encontra-se em [7]:

Teorema 1. *Toda escolha de quatro pontos X, Y, O e I, três quaisquer deles não-incidentes com uma mesma reta, determina um anel ternário T. Os elementos de T incluem um zero, 0, um elemento unidade $1 \neq 0$. A operação ternária satisfaz as seguintes leis:*

(I) $0 \cdot m \circ c = a \cdot 0 \circ c = c$.

(II) $1 \cdot m \circ 0 = m \cdot 1 \circ 0 = m$.

(III) Dados a, m e c existe um único z tal que $a \cdot m \circ z = c$.

(IV) Se $m_1 \neq m_2$, b_1 e b_2 são dados, então existe um único x tal que

$$x \cdot m_1 \circ b_1 = x \cdot m_2 \circ b_2.$$

(V) Se $a_1 \neq a_2$, c_1 e c_2 são dados, então existe um unico par (m, b) tal que

$$a_1 \cdot m \circ b = c_1 \text{ e } a_2 \cdot m \circ b = c_2.$$

□

Naturalmente, semicorpos e anéis de divisão são anéis ternários, pois suas operações de adição e multiplicação quando simbolizadas por $\circ$ e $\cdot$, respectivamente, satisfazem as propriedades (I) - (V) do Teorema 1.

Exemplo 1. *Seja F o corpo $GF(9)$. Defina uma nova "multiplicação"$\circ$ em F por $x \circ y = xy$ se x é um quadrado e $x \circ y = xy^3$ se x não é um quadrado. É fácil mostrar que F com adição original e esta nova multiplicação $\circ$ é um anel ternário. Entretanto este não é um semicorpo porque não satisfaz uma das leis distributivas. De fato, sendo $\{1, \omega\}$ uma base de $GF(9)$ sobre $GF(3)$, com $\omega^2 = 2$, os elementos ω e $1+\omega$ não são quadrados. Assim $(1+\omega)\circ\omega = 2\omega+1$ enquanto $1\circ\omega+\omega\circ\omega = \omega+1$.* □

A partir de agora utilizaremos $(T, \circ, \cdot)$ para denotar um anel ternário T com operação ternária $a \cdot b \circ c$.

Definição 5. *Dizemos que um plano projetivo π é* **coordenatizado por** *T se, e somente se, π é representado por um anel ternário T cuja operação ternária satisfaz as propriedades (I) - (V) do Teorema 1.*

Agora faremos uma correspondência entre as coordenadas ora introduzidas e as coordenadas introduzidas via o espaço vetorial à direita V, sobre um anel ternário K, com K-base

$$\{e_1, e_2, e_3\} = \{(1,0,0), (0,1,0), (0,0,1)\}.$$

Associaremos o ponto arbitrário $P = (x, y)$ com o espaço vetorial unidimencional V_P,

$$(e_1 + e_2 \cdot x + e_3 \cdot y)z,$$

onde z é um elemento não-nulo arbitrário de K.

Assim, se (x_1, x_2, x_3) é um vetor não-nulo em V_P, então $x_1 = z,\ x_2 = xz$ e $x_3 = yz$ serão as coordenadas homogêneas de P, e V_P e P serão identificados pelo ponto $(1, x, y)$.

Em coordenadas homogêneas o ponto unitário $I = (1,1,1)$.

Todos os ponto sobre XY, exceto Y, serão obtidos de $(e_2 + e_3 \cdot u) \cdot z$, enquanto o próprio Y será dado por $e_3 \cdot z$. Conseqüentemente, as coordenadas homogêneas dos pontos sobre XY serão $(0, 1, u)$, mas a de Y será $(0, 0, 1)$. Assim teremos

$$O = (0,0,0),\ X = (0,1,0),\ Y = (0,0,1),\ I = (1,1,1).$$

Identificando pontos por $(x_1, x_2, x_3) \neq (0,0,0)$ ou pelo subspaço $\langle (x_1, x_2, x_3) \rangle$ e retas por $[y_1, y_2, y_3] \neq [0,0,0]$ ou pelo subspaço $\langle [y_1, y_2, y_3] \rangle$, com a relaçao de incidência

dada por

$$(x_1, x_2, x_3) \in [y_1, y_2, y_3] \longleftrightarrow x_3 \cdot y_1 = x_2 \cdot y_2 \circ x_1 \cdot y_3,$$

temos a seguinte representação de pontos e retas em notação homogênea:

	Notação Homogênea	Notação anterior
Pontos:	$(0, 0, 1)$	(∞)
	$(0, 1, a)$	(a)
	$(1, a, b)$	(a, b)
Retas:	$[0, 0, 1]$	L_∞
	$[0, 1, a]$	$x + a = 0$
	$[1, a, b]$	$y = x \cdot a \circ b,$

onde a e b são elementos arbitrários de um anel ternário T.

Evidentemente, podemos utilizar esta notação a todo plano projetivo π e anel ternário T que coordenatiza π. A principal vantagem desta notação é que o ponto (x_1, x_2, x_3) é incidente com a reta $[y_1, y_2, y_3]$ se, e somente se,

$$y_1 x_3 = x_2 \cdot y_2 \circ x_1 y_3. \tag{2.6}$$

Já que y_1 e x_1 devem ser iguais a 0 ou 1, o significado das "multiplicações" $y_1 x_3$ e $x_1 y_3$ está claro nesta relação. O fato da relação de incidência entre pontos e retas ser expressa em uma simples fórmula ajudará muito na demonstração dos próximos teoremas.

Denotaremos a reta unindo os pontos A e B por $A : B$ e o ponto comum as retas L e M por $L \cap M$. Além disso, definimos os elementos $a \sim$ e $\sim a$ pelas equações

$$(a \sim) + a = 0 \quad \text{e} \quad a + (\sim a) = 0.$$

As seguintes fórmulas podem ser facilmente verificadas:

$$\sim (a \sim) = (\sim a) \sim = a$$

$$[0,0,1] = (0,0,1) : (0,1,0) \quad (0,0,1) = [0,0,1] \cap [0,1,0]$$

$$[0,1,\sim a] = (0,0,1) : (1,a,b) \quad (0,1,a) = [0,0,1] \cap [1,a,b] \tag{2.7}$$

$$[1,a,b] = (0,1,a) : (1,0,b) \quad (1,a,b) = [0,1,\sim a] \cap [1,0,b]$$

2.4 Perspectividades e Planos Desarguesianos

Definição 6. *Um* **isomorfismo** α **entre planos projetivos** *é uma correspondência biunívoca entre pontos e retas que preserva a incidência; ou seja, o ponto P está na reta L se, e somente se, o ponto $P\alpha$ está na reta $L\alpha$. Um automorfismo de um plano é comumente chamado uma* **colineação**

Definição 7. *Se uma colineação fixa todos os pontos de uma reta em um plano projetivo π, então a colineação é chamada uma* **perspectividade.**

Definição 8. *Se α é uma colineação que fixa todos os pontos de uma reta ℓ e todas as retas que passam por um ponto V, então α é chamada uma* (V,ℓ)**-perspectividade**. *O ponto V é chamado o* **centro** *de α e ℓ chama-se* **eixo** *de α. Surgem daí duas possibilidades: se V é incidente com ℓ diz-se que α é uma* **elação;** *em caso contrário, diz-se que α é uma* **homologia.**

Configuração de Desargues

Sejam π um plano projetivo e $\alpha \neq 1$ uma (V,ℓ)-perspectividade.

Se P_1 é um ponto que não é fixo por α então a imagem de P_2, para algum outro ponto P_2 não-fixo por α e não-incidente com P_1V, pode ser construída como a seguir: Seja $P_1P_2 \cap \ell = X$. Portanto, já que $P_2 = VP_2 \cap XP_1$, segue que $P_2^\alpha = (VP_2)^\alpha \cap (XP_1)^\alpha = VP_2 \cap XP_1^\alpha$ (Note que $(VP_2)^\alpha = VP_2$ porque α fixa todas as retas passando por V).

Agora, seja P_3 um ponto qualquer não-incidente em qualquer das retas VP_1 ou VP_2. Então podemos construir P_3^α como anteriormente, mas poderemos escolher tanto P_1 quanto P_2 como o outro ponto na construção. Já que P_3^α é único, tomando

$P_2P_3 \cap \ell = Y$ e $P_3P_1 \cap \ell = Z$ temos $P_3^\alpha = VP_3 \cap ZP_1^\alpha = VP_3 \cap YP_2^\alpha$, pelo argumento anterior.

Qualquer subconjunto de pontos e retas de π é chamado uma **configuração,** e a configuração formada pelos dez pontos V, X, Y, Z, P_1, P_1^α, P_2, P_2^α, P_3, P_3^α e as dez retas ℓ, VPP_1^α, $VP_2P_2^\alpha$, $VP_3P_3^\alpha$, XP_1P_2, $XP_1^\alpha P_2^\alpha$, YP_2P_3, $YP_2^\alpha P_3^\alpha$, ZP_3P_1, $ZP_3^\alpha P_1^\alpha$ é chamada **configuração de Desargues.** Claramente qualquer plano que admite uma perspectividade tem muitas configurações de Desargues.

Seja $\triangle_i\,(i = 1, 2)$ um triângulo com vértices A_i, B_i, C_i e arestas opostas a_i, b_i, c_i. Se existe um ponto V tal que $VA_1 = VA_2$, $VB_1 = VB_2$ e $VC_1 = VC_2$ então dizemos que os triângulos $\triangle_1$ e $\triangle_2$ estão **em perspectiva de** V. A definição de $\triangle_1$ e $\triangle_2$ estarem em perspectiva de uma reta ℓ é estabelecida de maneira dual.

A discussão anterior sobre perspectividades pode ser resumida pelo seguinte teorema, cuja demonstração encontra-se em [10]:

Teorema 2. *Seja π um plano projetivo. Se α é uma (V, ℓ)-perspectividade e se $\triangle$ é um triângulo qualquer que não tem lados ou vértices fixos por α, então os triângulos $\triangle$ e $\triangle^\alpha$ estão em perspectiva de V e ℓ.*

Observação 1. *Aqui estamos utilizando a notação óbvia: se $\triangle$ é o triângulo determinado por A, B e C então $\triangle^\alpha$ é o triângulo $A^\alpha B^\alpha C^\alpha$.*

Agora estamos habilitados para dar uma definição formal de configuração de Desargues.

Sejam $\triangle_i$ $(i = 1, 2)$ dois triângulos quaisquer com vértices A_i, B_i, C_i e lados opostos a_i, b_i, c_i tais que estão em perspectiva de um ponto V e de uma reta ℓ. Então a configuração formada pelos dez pontos V, A_1, A_2, B_1, B_2, C_1, C_2, $\ell b_1 b_2$, $\ell c_1 c_2$ e as dez retas ℓ, a_1, a_2, b_1, b_2, c_1, c_2, VA_1A_2, VB_1B_2, VC_1C_2 é chamada **configuração de Desargues** (Veja Fig. 2). Na situação especial onde V está em ℓ a configuração é também chamada **pequena configuração de Desargues.**

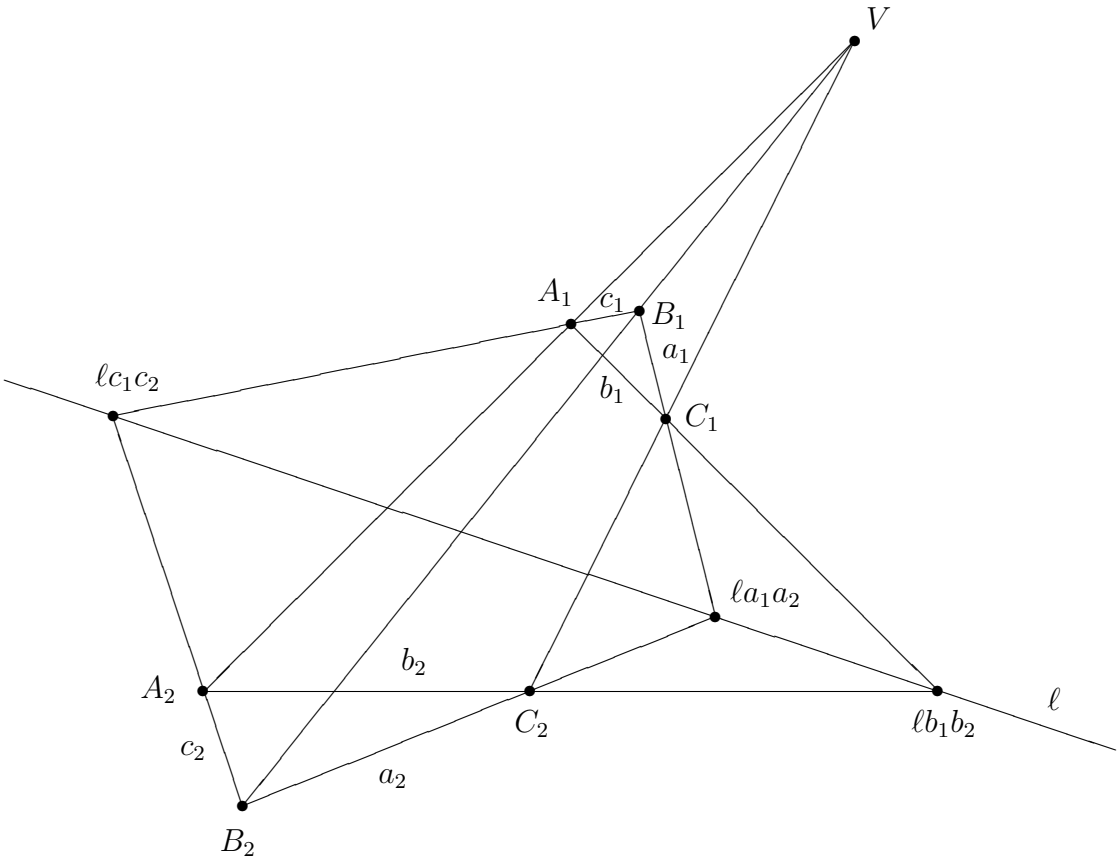


Figura 2

Definição 9. *Um plano projetivo π é dito ser* (V, ℓ)**-desarguesiano** *se, para cada par de triângulos não-degenerados $\triangle_i$ $(i = 1, 2)$ com vértices A_i, B_i, C_i e lados opostos a_i, b_i, c_i com*

(a) $\triangle_1$ e $\triangle_2$ em perspectiva de V e (b) a_1a_2, b_1b_2 incidentes com ℓ,

então c_1c_2 também é incidente com ℓ.

Definição 10. *Um plano projetivo π é chamado* **desarguesiano** *se é (V, ℓ)-desarguesiano para todas as escolhas de V e ℓ. Caso contrário π é dito ser* **não-desarguesiano.**

Semicorpos e anéis de divisão, como anéis ternários, coordenatizam planos projetivos. O seguinte teorema caracteriza os planos projetivos conforme o anel ternário que os coordenatiza:

Teorema 3. *Um plano projetivo é* **desarguesiano** *se, e somente se, for coordenatizado por um anel de divisão.*

Demonstração. Veja referência [10]. □

Como conseqüência do Teorema 3, concluímos que planos projetivos coordenatizados por semicorpos próprios são não-desarguesianos.

2.5 Isotopias

Definição 11. *Sejam T e T_1 anéis ternários. Um* **isotopismo** *de T_1 sobre T é um conjunto de três funções (F, G, H), correspondências biunívocas de T_1 a T, tais que*

$$\begin{aligned} &(0)H = 0, \\ &(a \cdot b \circ c)H = (aF) \cdot (bG) \circ (cH), \quad \text{para todos} \quad a, b, c \in T_1. \end{aligned} \tag{2.8}$$

Teorema 4. *Sejam T e T_1 anéis ternários e (F, G, H) um isotopismo de T_1 em T. Então*

$$H = F\psi = G\varphi, \tag{2.9}$$

onde $\varphi = L_{1F}$, $\psi = R_{1G}$, com L e R denotando multiplicações à esquerda e à direita em T.

Demonstração. Fazendo $c = 0$ na fórmula (2.8) obtemos

$$(ab)H = (aF)(bG).$$

Em particular,

$$aH = (aF)(1G) = aFR_{1G} = aF\psi,$$

$$bH = (1F)(bG) = bGL_{1F} = bG\varphi.$$

□

Definição 12. *Dizemos que os anéis ternários $(R_1, \circ, \cdot)$ e $(R_2, \diamond, \star)$ são* **isomorfos** *se existe uma bijeção α de R_1 em R_2, com*

$$(a \cdot b \circ c)\alpha = a\alpha \star b\alpha \diamond c\alpha, \quad \forall\ a, b, c \in R_1.$$

Neste caso α é dito ser um **isomorfismo** *de R_1 em R_2.*

Teorema 5. *Seja T um anel ternário com n elementos. O número de anéis ternários não-isomorfos isotópicos a T é de no máximo $(n-1)^2$.*

Demonstração. Sejam T_1 e T_2 anéis ternários isotópicos a T, com funções $(F_1, G_1, H_1) : T_1 \longrightarrow T$ e $(F_2, G_2, H_2) : T_2 \longrightarrow T$. Seja a operação ternária de T_1 denotada por (a, b, c) e seja a operação ternária de T_2 denotada por $[a, b, c]$. Mostraremos que se $1F_1 = 1F_2 = y$, e se $1G_1 = 1G_2 = z$, então T_1 e T_2 são isomorfos. Já que existem $(n-1)$ escolhas para $1F_1$ e $(n-1)$ escolhas independentes para $1G_1$, existem no máximo $(n-1)^2$ anéis ternários não-isomorfos, como queríamos.

Pelo Teorema 4 temos que

$$F_1\psi = G_1\varphi = H_1,$$

$$F_2\psi = G_2\varphi = H_2,$$

onde $\varphi = L_y,\ \psi = R_z$. Conseqüentemente,

$$F_1F_2^{-1} = G_1G_2^{-1} = H_1H_2^{-1} = \alpha.$$

Agora α é um isomorfismo, já que

$$[a\alpha, b\alpha, c\alpha] = (a\alpha F_2 \cdot b\alpha G_2 \circ c\alpha H_2)H_2^{-1}$$

$$= (aF_1 \cdot bG_1 \circ cH_1)H_1^{-1}\alpha = (a, b, c)\alpha.$$

□

O limite $(n-1)^2$ é o melhor possível porque existe um anel ternário com 32 elementos que tem 31^2 anéis ternários isotópicos distintos (Veja Capítulo 4). Mas se T é um corpo, temos o outro extremo onde todos os anéis isotópicos são isomorfos a T.

Teorema 6. *Sejam T um anel ternário, y e z elementos não-nulos de T, $\varphi = L_y,\ \psi = R_z,\ F = \psi^{-1},\ G = \varphi^{-1}$ e T_1 o sistema consistindo dos elementos de T com uma nova operação ternária definida por:*

$$a \star b \diamond c = aF \cdot bG \circ c. \tag{2.10}$$

Então T_1 é também um anel ternário, tendo elemento identidade yz. T_1 é isotópico a T e, além disso, todos os anéis ternários isotópicos a T podem ser construídos desta maneira (a menos de isomorfismo).

Demonstração. Note que F e G estão bem definidas já que y e z não-nulos. A parte posterior deste teorema segue do teorema anterior; devemos mostrar somente que $a \star b \diamond c$ satisfaz as condições para que seja um anel ternário.

(I) $0 \star b \diamond c = 0 \cdot bG \circ c = c = aF \cdot 0 \circ c = a \star 0 \diamond c$.

(II) $yz \star b \diamond 0 = y \cdot bG \circ 0 = y(bG) = bG\varphi = b$.

$a \star yz \diamond 0 = aF \cdot z \circ 0 = (aF)z = aF\psi = a$.

(III) Podemos resolver $a \star b \diamond x = c$ unicamente para x, já que $aF \cdot bG \circ x = c$ é unicamente solúvel para x.

(IV) Podemos resolver $x \star b_1 \diamond c_1 = x \star b_2 \diamond c_2$ unicamente para x, se $b_1 \neq b_2$, já que $xF \cdot b_1G \circ c_1 = xF \cdot b_2G \circ c_2$ é justamente solúvel para xF.

(V) Finalmente, podemos resolver $a_1 \star w \diamond x = c_1$, $a_2 \star w \diamond x = c_2$ unicamente para (w, x), se $a_1 \neq a_2$, já que podemos resolver $a_1F \cdot wG \circ x = c_1$, $a_2F \cdot wG \circ x = c_2$ unicamente para (wG, x).

□

O Teorema 6 é essencialmente a recíproca do Teorema 4, porque diz que as relações $(0)H = 0$ e $H = F\psi = G\varphi$ são suficientes para construirmos uma nova operação ternária. Além disso, este teorema provê uma maneira conveniente para calcularmos todos os anéis ternários isotópicos a um dado anel ternário. Um isotopismo onde H é a identidade é chamado um "isótopo principal".

2.6 O significado de isotopia na geometria.

Teorema 7. *Sejam π e π' planos projetivos e α um isomorfismo de π' em π tal que*

$$(0, 0, 1)\alpha = (0, 0, 1)$$

$$(0, 1, 0)\alpha = (0, 1, 0)$$

$$(1, 0, 0)\alpha = (1, 0, 0).$$

Então os anéis ternários de π e π' são isotópicos.

Demonstração. $[0,0,1]\alpha = (0,0,1)\alpha : (0,1,0)\alpha = (0,0,1) : (0,1,0) = [0,0,1]$. Conseqüentemente, $(0,1,a)\alpha$ está em $[0,0,1]$, e aí existe uma correspondência biunívoca G tal que

$$(0,1,a)\alpha = (0,1,aG) \tag{2.11}$$

Similarmente encontramos que $[0,1,0]\alpha = [0,1,0]$ e $[1,0,0]\alpha = [1,0,0]$; conseqüentemente existem correspondências biunívocas H e F tais que

$$\begin{gathered}(1,0,b)\alpha = (1,0,bH) \text{ e} \\ (1,a,0)\alpha = (1,aF,0).\end{gathered} \tag{2.12}$$

Podemos agora calcular as imagens de todas as retas:

$$\begin{gathered}[0,1,\sim a]\alpha = (0,0,1)\alpha : (1,a,0)\alpha = [0,1,\sim (aF)] \\ [1,a,b]\alpha = (0,1,a)\alpha : (1,0,b)\alpha = [1,aG,bH].\end{gathered} \tag{2.13}$$

Finalmente, encontramos a imagem de todo ponto:

$$(1,a,b)\alpha = [0,1,\sim a]\alpha \cap [1,0,b]\alpha = (1,aF,bH). \tag{2.14}$$

Agora podemos obter a regra desejada:

$$\begin{aligned}(1,x_2,x_3) \in [1,y_2,y_3] &\longleftrightarrow (1,x_2,x_3)\alpha \in [1,y_2,y_3]\alpha \\ &\longleftrightarrow (1,x_2F,x_3H) \in [1,x_2G,x_3H],\end{aligned} \tag{2.15}$$

ou seja,

$$x_3 = x_2 \cdot y_2 \circ y_3 \longleftrightarrow x_3H = x_2F \cdot y_2G \circ y_3H,$$

e esta é precisamente a relação usada para isotopia. □

Teorema 8 (Recíproca do Teorema 7)**.** *Seja (F,G,H) uma isotopia de um anel ternário T' em T, e sejam π' e π os planos correspondentes. Defina α pelas Eq. (2.11)-(2.14); então α é um isomorfismo entre π' e π.*

Demonstração. Já que as Eq. (2.11)-(2.14) mostram que α é uma bijeção, e (2.15) se verifica diretamente da lei da isotopia, existem poucos casos a considerar.

$$
\begin{array}{lllllll}
\text{I.} & (1,x_2,x_3) & \in [0,y_2,y_3] & \longleftrightarrow & y_2=1 & \text{e} & y_3 \sim\!= x_2, \\
 & (1,x_2,x_3)\alpha & \in [0,y_2,y_3]\alpha & \longleftrightarrow & y_2=1 & \text{e} & y_3 \sim F = x_2F. \\
\text{II.} & (0,x_2,x_3) & \in [1,y_2,y_3] & \longleftrightarrow & x_2=1 & \text{e} & x_3 = y_2, \\
 & (0,x_2,x_3)\alpha & \in [1,y_2,y_3]\alpha & \longleftrightarrow & x_2=1 & \text{e} & x_3G = y_2G. \\
\text{III.} & (0,x_2,x_3) & \in [0,y_2,y_3] & \longleftrightarrow & x_2=0 & \text{ou} & y_2 = 0, \\
 & (0,x_2,x_3)\alpha & \in [0,y_2,y_3]\alpha & \longleftrightarrow & x_2=0 & \text{ou} & y_2 = 0.
\end{array}
$$

□

Definimos *autotopismo* de maneira bastante intuitiva, como um isotopismo de um anel ternário em si mesmo. Se (F,G,H) e (F',G',H') são autotopismos,

$$(a\cdot b\circ c)HH' = (aF\cdot bG\circ cH)H' = aFF'\cdot bGG'\circ cHH',$$

também definimos o produto de dois autotopismos como

$$(F,G,H)(F',G',H') = (FF',GG',HH'). \tag{2.16}$$

Um *automorfismo* é o caso especial (F,F,F) de um autotopismo onde todas as três permutações são iguais.

Corolário 1. *Todos os anéis ternários isotópicos coordenatizam o mesmo plano projetivo. As colineações de um plano projetivo que fixam* $(0,0,1)$, $(0,1,0)$, *e* $(1,0,0)$ *formam um grupo isomorfo ao grupo dos autotopismos do anel ternário.*

Proposição 1. *Seja* $(T,\circ,\cdot)$ *isotópico ao* $(T',\diamond,\star)$. *Então o grupo dos autotopismos de* $(T,\circ,\cdot)$ *é conjugado do grupo dos autotopismos de* $(T',\diamond,\star)$.

Demonstração. Sejam $(F,G,H) : T \longrightarrow T'$ um isotopismo e (F',G',H') um autotopismo de T'. Assim,

$$(a\cdot b\circ c)HH'H^{-1} = (aF\star bG\diamond cH)H'H^{-1} = (aFF'\star bGG'\diamond cHH')H^{-1}$$

$$= aFF'F^{-1}\cdot bGG'G\circ cHH'H^{-1}.$$

Logo $(FF'F^{-1},GG'G^{-1},HH'H^{-1})$ pertencerá ao grupo dos autotopismos de $(T,\circ,\cdot)$ sempre que (F',G',H') pertencer ao grupo dos autotopismos de $(T',\diamond,\star)$ e $(F,G,H) : T \longrightarrow T'$ é um isotopismo. Para o restante da demonstração, toma-se um autotopismo de $(T,\circ,\cdot)$ e o isotopismo inverso $(F^{-1},G^{-1},H^{-1}) : T' \longrightarrow T$. □

Teorema 9. *Seja T um anel ternário com n elementos, e seja h a ordem do grupo de autotopismos de T. Então*

$$(n-1)^2 = \sum_{T'} \frac{h}{k(T')}, \tag{2.17}$$

onde T' varia sobre todos os anéis ternários não-isomorfos isotópicos a T e $k(T')$ é o número de automorfismos de T'.

Demonstração. Sejam y e z variando sobre os elementos não-nulos de T, e considere os $(n-1)^2$ anéis ternários construídos como no Teorema 6. Se T' é qualquer desses anéis ternários, mostraremos que existem exatamente $h/k(T')$ anéis ternários deste conjunto que são isomorfos a T', e isto prova a fórmula (2.17).

Necessitamos apenas mostrar que $h/k(T)$ dos anéis ternários são isomorfos a T, porque os grupos dos autotopismos de T' e T têm a mesma ordem, pela Proposição 1, e os $(n-1)^2$ anéis ternários formados de T' são isomorfos aos $(n-1)^2$ anéis ternários formados de T (usando o Teorema 5, já que os anéis são determinados por $1F$ e $1G$).

Seja α um isomorfismo de T no anel $T'(R_z^{-1}, L_y^{-1}, 1)$. Existem $k(T)$ tais isomorfismos. Então

$$(a \cdot b \circ c)\alpha = a\alpha \star b\alpha \diamond c\alpha = a\alpha R_z^{-1} \cdot b\alpha L_y^{-1} \circ c\alpha,$$

isto é, $(\alpha R_z^{-1}, \alpha L_y^{-1}, \alpha)$ é um autotopismo. Pelo Teorema 4, todo autotopismo é desta forma e define y e z. Conseqüentemente, se r dos pares (y, z) dão anéis isomorfos, existem $h = rk(T)$ autotopismos. □

2.7 Isotopia de Semicorpos

Um semicorpo é um tipo particular de anel ternário, onde $a \cdot b \circ c = ab + c$ e os axiomas **A1-A4** se verificam. Nesta seção utilizaremos o material das seções anteriores para nos especializarmos um pouco mais em semicorpos.

Teorema 10. *Seja S um semicorpo de característica p. Todos os anéis ternários isotópicos a S são semicorpos. (F, G, H) é um isotopismo de S' em S se, e somente se, F, G e H são transformações lineares não-singulares de S' em S sobre $GF(p)$, satisfazendo a condição*

$$(ab)H = (aF)(bG). \tag{2.18}$$

Demonstração. Suponhamos que S' seja isotópico a S e que $(a \cdot b \circ c)H = (aF)(bG) + cH$. Então $(a \cdot 1 \circ c)H = (aF)(1G) + cH = aH + cH$, de forma que H é um isomorfismo do grupo aditivo $(S', +)$ no grupo aditivo $(S, +)$, ou seja, H é uma transformação linear não-singular sobre $GF(p)$. Agora, $H = F\psi = G\varphi$, pelo Teorema 4, onde ψ e φ, sendo funções de multiplicação à esquerda e à direita, são transformações lineares não-singulares sobre $GF(p)$ de S em si mesmo. Conseqüentemente F e G são também transformações lineares não-singulares. A parte recíproca do teorema é trivial. Também está claro que S' é um semicorpo. □

Teorema 11. *Toda colineação de um plano coordenatizado por um semicorpo próprio fixa* $(0, 0, 1)$ *e* $[0, 0, 1]$.

Demonstração. Este teorema é bem conhecido, mas sua prova requer mais ferramentas geométricas do que dispomos. Sua demonstração pode ser encontrada em [2] e [3]. □

Se π é um plano coordenatizado por um semicorpo próprio então qualquer elação com centro $(0, 0, 1)$ e eixo afim é chamada um *shear* (ou *cisalhamento*).

As colineações padrões, válidas em qualquer plano coordenatizado por um semicorpo, são as translações $\tau(h, k)$ e os *shears* generalizados $\sigma(h, k)$, definidos para todos h, k no semicorpo como a seguir:

$$\begin{aligned}
(x_1, x_2, x_3)\,\tau(h,k) &= (x_1, x_2 + x_1h, x_3 + x_1k) \\
[y_1, y_2, y_3]\,\tau(h,k) &= [y_1, y_2, y_3 - hy_2 + y_1k] \\
(x_1, x_2, x_3)\,\sigma(h,k) &= (x_1, x_2, x_3 + x_2h + x_1k) \\
[y_1, y_2, y_3]\,\sigma(h,k) &= [y_1, y_2 + y_1h, y_3 + y_1k] \qquad (2.19)
\end{aligned}$$

A demonstração de que as translações e os *shears* generalizados são colineações é muito simples com coordenadas homogêneas:

$$\begin{aligned}
& y_1x_3 = x_2y_2 + x_1y_3 \\
\longleftrightarrow\ & y_1(x_3 + x_1k) = (x_2 + x_1h)y_2 + x_1(y_3 - hy_2 + y_1k) \\
\longleftrightarrow\ & y_1(x_3 + x_2h + x_1k) = x_2(y_2 + y_1h) + x_1(y_3 + y_1k),
\end{aligned}$$

onde $x_1, y_1 \in \{0, 1\}$.

Representando a colineação correspondendo a um autotopismo (F, G, H) por $\alpha(F, G, H)$, como na demonstração do Teorema 7, temos:

$$(0, 0, 1)\,\alpha(F, G, H) = (0, 0, 1)$$

$$(0, 1, x_3)\,\alpha(F, G, H) = (0, 1, x_3 G)$$

$$(1, x_2, x_3)\,\alpha(F, G, H) = (1, x_2 F, x_3 H)$$

$$[0, 0, 1]\,\alpha(F, G, H) = [0, 0, 1]$$

$$[0, 1, \sim x_3]\,\alpha(F, G, H) = [0, 1, \sim (x_3 F)]$$

$$[1, x_2, x_3]\,\alpha(F, G, H) = [1, x_2 G, x_3 H]. \tag{2.20}$$

As seguintes relações podem ser facilmentes calculadas, utilizando as fórmulas de (2.19) e (2.20):

$$\tau(0, k) = \sigma(0, k)$$

$$\tau(h, k)\,\tau(h', k') = \tau(h + h', k + k')$$

$$\sigma(h, k)\,\sigma(h', k') = \sigma(h + h', k + k')$$

$$\alpha(F, G, H)\,\alpha(F', G', H') = \alpha(FF', GG', HH')$$

$$\tau(h, k)^{-1}\,\sigma(l, m)\,\tau(h, k) = \sigma(l, m - hl)$$

$$\sigma(h, k)^{-1}\,\tau(l, m)\,\sigma(h, k) = \tau(l, m + lh)$$

$$\alpha(F, G, H)^{-1}\,\tau(h, k)\,\alpha(F, G, H) = \tau(hF, kH)$$

$$\alpha(F, G, H)^{-1}\,\sigma(h, k)\,\alpha(F, G, H) = \sigma(hG, kH). \tag{2.21}$$

Teorema 12 (Albert)**.** *Dois semicorpos coordenatizam o mesmo plano se, e somente se, são isotópicos.*

Demonstração. Se β é um isomorfismo entre dois planos coordenatizados por semicorpos, então $(0, 0, 1)\beta = (0, 0, 1)$ e $[0, 0, 1]\beta = [0, 0, 1]$ porque este ponto e esta reta são caracterizados pelo Teorema 11 e pelas colineações padrões. Conseqüentemente,

$$(0, 1, 0)\beta = (0, 1, a) \text{ e } (1, 0, 0)\beta = (1, b, c).$$

Seja

$$\alpha = \beta\, \sigma(-a, 0)\, \tau(-b, ba - c).$$

Então

$$(0, 0, 1)\alpha = (0, 0, 1); \quad (1, 0, 0)\alpha = (1, 0, 0);$$

$$(0, 1, 0)\alpha = (0, 1, 0);$$

e o Teorema 7 é aplicado. A recíproca é parte do Corolário 1. □

Teorema 13. *Seja G o grupo das colineações de um plano coordenatizado por um semicorpo; seja T o subgrupo das translações, S o subgrupo dos shears generalizados, H o subgrupo correspondendo aos autotopismos, e A o grupo abeliano elementar aditivo do semicorpo. Então temos a seguinte série normal de G :*

$$I \lhd T \cap S \lhd T \lhd \langle T, S\rangle \lhd \langle T, S, H\rangle = G. \tag{2.22}$$

Os grupos quocientes são isomorfos, respectivamente, a A, A, A e H.

Demonstração. Segue das fórmulas (2.21), e de $G = \langle T, S, H\rangle$, como provado no teorema anterior. □

Os Teoremas 12 e 13 são bem conhecidos e indicam que isotopia é muito importante quando trabalhamos com planos coordenatizados por semicorpos. O uso de coordenadas homogêneas simplificou bastante as demonstrações desses teoremas.

2.8 Relacionamento entre pré-semicorpos e certos p-grupos de classe 2

Analisaremos agora as possíveis soluções para o problema:
($\mathcal{P}$) *Seja p um número primo. Descrever todos os grupos de ordem p^{3n}, de classe de nilpotência 2, contendo subgrupos X e Y tais que $|X| = |Y| = p^n$ e quaisquer elementos não-triviais $x \in X$ e $y \in Y$ não comutam* (cf. [14], Problema 10.1).

Utilizando notação aditiva, dados elementos x, y e z num grupo arbitrário G, o **conjugado** de x por y é $x^y := (-y) + x + y$ e o **comutador** de x e y é o elemento

$[x,y] := (-x)+x^y(= (-x)+(-y)+x+y)$. Utilizaremos as seguintes identidades que são de uso freqüente no cálculo com comutadores:

$$\begin{aligned} [x+y,z] &= [x,z]^y + [y,z]; \\ [x,y+z] &= [x,z] + [x,y]^z. \end{aligned} \tag{2.23}$$

Se X e Y são dois subconjuntos de G, o **subgrupo gerado** por X e Y é denotado por $< X, Y >$ e o **subgrupo comutador** de X e Y é o subgrupo $[X,Y]$ de G, gerado por todos os comutadores $[x,y]$ com $x \in X$ e $y \in Y$. O **fêcho normal** de X em G é o subgrupo $< X >^G$ de G, gerado por todos os conjugados x^g com $x \in X$ e $g \in G$. A **série central inferior** de G, $\gamma_i(G)$, $i \geq 1$, é definida recursivamente por $\gamma_1(G) := G$ e, para $i \geq 1$, $\gamma_{i+1}(G) := [\gamma_i(G), G]$. Em particular, $\gamma_2(G) = G'$, o **grupo derivado** de G. Diz-se que G é **nilpotente** se $\gamma_{n+1}(G) = 1$ para algum $n \in \mathbb{N}$, e o menor tal n é a **classe de nilpotência** de G, que no que segue denominamos simplesmente classe. Particularmente, num grupo de classe 2 o grupo derivado está contido no **centro** $Z(G)$ de G, de modo que as identidades entre os comutadores acima são, neste caso, relações de *bilinearidade:*

$$[x+y,z] = [x,z] + [y,z] \;\text{ e }\; [x,y+z] = [x,y] + [x,z]. \tag{2.24}$$

Cabe observar que se um grupo arbitrário G é gerado por dois subgrupos X e Y, então o subgrupo comutador $[X,Y]$ é normal em H, porque o conjugado de um gerador qualquer $[x,y] \in [X,Y]$ por um elemento $x_1 \in X$ é, pelas relações (2.23),

$$[x,y]^{x_1} = [x+x_1,y] + (-[x_1,y]) \;\; (\in [X,Y]);$$

analogamente, $[x,y]^{y_1} \in [X,Y]$ para todo $y_1 \in Y$, e a afirmação segue então pelo fato de H ser gerado por X e Y.

Como o grupo gerado pelas translações e *shears* de plano coordenatizado por um semicorpo satisfazem ao problema $\mathcal{P}$, então, utilizando as relações (2.21), chegamos ao seguinte teorema que relaciona pré-semicorpos com p-grupos de classe 2 :

Teorema 14. *Sejam $(S, +, \cdot)$ um pré-semicorpo e G o conjunto das ternas (a, b, c), com $a, b, c \in S$ e operação $*$ dada por*

$$(a,\, b,\, c) * (d,\, e,\, f) = (a+d,\, b+e,\;\; c+f+b\cdot d) \tag{2.25}$$

Então $(G, *)$ é um grupo solução para o problema $\mathcal{P}$.

Demonstração. É fácil ver que $(G,\, *)$ é um grupo. O elemento $(0,\, 0,\, 0)$ é a identidade de G e, para quaisquer elementos $a, b \in S - \{0\}$, temos

$$[(a,\, 0,\, 0), (0,\, b,\, 0)] = (0,\, 0,\, -b \cdot a) \neq (0,\, 0,\, 0)$$

e

$$[(0,\, b,\, 0), (a,\, 0,\, 0)] = (0,\, 0,\, b \cdot a) \neq (0,\, 0,\, 0).$$

O centro de G é formado de todos os elementos na forma $(0,\, 0,\, c)$, pois

$$\begin{aligned}
& ((a,\, b,\, c) * (d,\, e,\, f) = (d,\, e,\, f) * (a,\, b,\, c),\ \forall\, a,\, b,\, c \in S) \\
\iff\ & ((a+d,\, b+e,\, c+f+b \cdot d) = (d+a,\, e+b,\, f+c+e \cdot a),\ \forall\, a,\, b,\, c \in S) \\
\iff\ & (b \cdot d = e \cdot a,\ \forall\, a,\, b \in S) \\
\iff\ & (d = 0 \ \text{ e } \ e = 0)\,.
\end{aligned}$$

Além disso, $(a,\, 0,\, 0) * (0,\, b,\, 0) * (0,\, 0,\, c) = (a,\, b,\, 0) * (0,\, 0,\, c) = (a,\, b,\, c)$.

Para mostrar que $(G,\, *)$ é solução para o problema $\mathcal{P}$, considere os seguintes subgrupos facilmente identificáveis em G :

$$X = \langle (a,\, 0,\, 0) : a \in S \rangle\,;$$

$$Y = \langle (0,\, b,\, 0) : b \in S \rangle\,.$$

Assim, pelos cálculos do parágrafo anterior, $G =< X, Y >,\ Z(G) = G' = [X, Y]$ e quaisquer elementos não-triviais $x \in X$ e $y \in Y$ não comutam. □

Teorema 15 (Recíproca do Teorema 14)**.** *Seja G um grupo solução para o problema $\mathcal{P}$, então podemos sempre escrevê-lo como o conjunto das ternas (a, b, c), onde a, b e c pertencem a algum pré-semicorpo, e com operação $*$ dada pela Eq. (2.25).*

Demonstração. Seja G um grupo de ordem p^{3n}, de classe de nilpotência 2, contendo subgrupos X e Y tais que $|X| = |Y| = p^n$ e quaisquer elementos não-triviais $x \in X$ e $y \in Y$ não comutam. Se $H =< X, Y >$, então, pela normalidade de $[X, Y]$ em H temos que

$$< X >^H = X[X, Y] \ \text{ e } \ < Y >^H = Y[X, Y].$$

Conseqüentemente,

$$H = XY[X, Y] = Y < X >^H\,. \tag{2.26}$$

Seja $\mathcal{NC}$ a condição de não-comutatividade:

$$\forall\, x \in X - \{0\},\ \forall\, y \in Y - \{0\},\ [x, y] \neq 0.$$

Portanto, por $\mathcal{NC}$, segue-se que

$$X \cap Y = \{0\}, \tag{2.27}$$

e como G tem classe 2, $[G, G] \leq Z(G)$, donde

$$[G, G] \cap X = \{0\} = [G, G] \cap Y.$$

Em particular,

$$[X, Y] \cap X = \{0\} = [X, Y] \cap Y \tag{2.28}$$

e $[X, X] = [X, X] \cap X = \{0\} = [Y, Y] \cap Y = [Y, Y]$. Conseqüentemente, X e Y são abelianos.

Mostraremos agora que

$$Y \cap < X >^H = \{0\}. \tag{2.29}$$

De fato, se $y \in Y \cap < X >^H$ $(= Y \cap X[X, Y])$ então $y = x + [x_1, y_1] + \cdots + [x_k, y_k]$ para algum $k \in \mathbb{N}$, onde, por (2.27) e (2.28), $x \neq 0$ e $\sum_{i=1}^{k} [x_i, y_i] \neq 0$. Logo,

$$\begin{aligned} 0 \;=\; [y, y] \;&=\; [x + [x_1, y_1] + \cdots + [x_k, y_k], y] \\ &=\; [x, y]^{[x_1, y_1] + \cdots + [x_k, y_k]} + [[x_1, y_1] + \cdots + [x_k, y_k], y] \\ &=\; [x, y] \qquad \text{(por classe 2)}, \end{aligned}$$

o que contradiz $\mathcal{NC}$.

Seja $\varphi : Y \longrightarrow [x, Y]$, $y \to [x, y]$, para algum $x \in X - \{0\}$. Então φ é injetiva. De fato, se $y_1,\ y_2 \in Y$, então

$$[x, y_1] = [x, y_2]$$

$\Rightarrow ([x, y_1 + (-y_2)] = 0$, porque G é nilpotente de classe 2)

$\Rightarrow (y_1 = y_2$, por $\mathcal{NC}$).

Assim, $|[X, Y]| \geq p^n$ e, por (2.26), (2.27), (2.28) e (2.29), segue que

$$p^{3n} \geq |H| = |Y| \cdot |X| \cdot |[X, Y]| \geq p^{3n}.$$

Conseqüentemente, $H = G$ e $|[X, Y]| = p^n$.

Agora $Z(G) = [X, Y]$ pois, para $x_2 \in X,\ y_2 \in Y$ e $z_2 \in [X, Y]$, temos que

$((y_1 + x_1 + z_1) + (y_2 + x_2 + z_2) = (y_2 + x_2 + z_2) + (y_1 + x_1 + z_1),\ \forall y_1 \in Y,\ \forall x_1 \in X,\ \forall z_1 \in [X, Y])$

$\Rightarrow ([y_1, y_2] + [x_1, y_2] + [y_1, x_2] + [x_1, x_2] = 0,\ \forall y_1 \in Y,\ \forall x_1 \in X$, por classe 2.)

$\Rightarrow ([x_1, y_2] + [y_1, x_2] = 0,\ \forall y_1 \in Y,\ \forall x_1 \in X$, por $\mathcal{NC}$.)

$\Rightarrow (x_2 = 0$ e $y_2 = 0)$.

Pelo Teorema de Cauchy e pelas relações (2.24) temos que $[px, y] = p[x, y] = [x, py] = 0$, para todos $x \in X$ e $y \in G$. Assim, por $\mathcal{NC}$, X, Y e $Z(G)$ têm expoente p. Mas como X, Y e $Z(G)$ são grupos abelianos com expoente p, então são abelianos elementares. Portanto, como estes grupos possuem a mesma ordem p^n, $X \cong Y \cong Z(G) \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ termos}}$. Desta forma, se $S \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ termos}}$, existem isomorfismos σ, τ e θ, onde

$$X = S^\tau,\ Y = S^\sigma \ \text{ e } \ Z(G) = S^\theta.$$

Além disso, como $[Y, X] = [X, Y] = Z(G)$, segue que

$$[S^\sigma, S^\tau] = S^\theta.$$

Assim, utilizando a adição sobre os elementos de S em notação usual, podemos definir uma nova operação $\star$ sobre os elementos de S por

$$(a \star b)^\theta = [a^\sigma, b^\tau].$$

Agora G ser nilpotente de classe 2 implica em

$$(a + c) \star b = a \star b + c \star b \ \text{ e } \ b \star (a + c) = b \star a + b \star c, \ \ \forall\, a, b, c \in S;$$

e a condição $\mathcal{NC}$ implica em

$$(a \star b = 0) \Longleftrightarrow (a = 0 \text{ ou } b = 0).$$

Conseqüentemente, $(S,\ +,\ \star)$ é um pré-semicorpo e, pelas observações anteriores,

$$(a_1^\tau + b_1^\sigma + c_1^\theta) + (a_2^\tau + b_2^\sigma + c_2^\theta)$$

$$= a_1^\tau + b_1^\sigma + a_2^\tau + b_2^\sigma + (c_1 + c_2)^\theta$$

$$= a_1^\tau + (a_2^\tau + b_1^\sigma) - (a_2^\tau + b_1^\sigma) + b_1^\sigma + a_2^\tau + b_2^\sigma + (c_1 + c_2)^\theta$$

$$= (a_1 + a_2)^\tau + b_1^\sigma + [b_1^\sigma, a_2^\tau] + b_2^\sigma + (c_1 + c_2)^\theta$$

$$= (a_1 + a_2)^\tau + b_1^\sigma + (b_1 \star a_2)^\theta + b_2^\sigma + (c_1 + c_2)^\theta$$

$$= (a_1 + a_2)^\tau + (b_1 + b_2)^\sigma + (c_1 + c_2 + b_1 \star a_2)^\theta.$$

□

Capítulo 3

Hipercubos Não-singulares

3.1 Hipercubos e suas operações elementares

Definição 13. *Um* **hipercubo** m**-dimensional** *(ou, simplesmente, um* m**-cubo**$)$ A, $m \geq 1$, *é um vetor de* n^m *elementos pertencentes a um corpo; os elementos são denotados por* $A_{ij\cdots r}$, *onde existem* m *índices, e cada índice varia de* 1 *a* n. *Consideraremos* n *fixo durante toda a discussão.*

Seja σ uma permutação dos elementos $1, 2, \cdots, m$. Então A^σ representará o m-cubo A com seus índices permutados por σ, ou seja, o $k\sigma$-ésimo índice de A^σ é o k-ésimo índice de A, onde $k\sigma$ indica a imagem de k pela permutação σ. Esta é uma generalização do conceito de transposição de matrizes: se A é uma matriz ($m = 2$), $A^T = A^{(1\,2)}$. No caso tridimensional, se $A = (A_{ijk})$, então se $B = A^{(1\,2\,3)} = (B_{ijk})$ temos $B_{ijk} = A_{jki}$, para todos i, j, k. Temos também a lei geral $(A^\sigma)^\tau = A^{\sigma\tau}$.

Se A é um m-cubo, $m > 1$, podemos obter um subcubo $(m-1)$-dimensional de A, denotado por $A^{[\,t\,]}$, como a seguir:

$$B = A^{[\,t\,]} = (B_{ij\cdots r}) \longleftrightarrow B_{ij\cdots r} = A_{tij\cdots r}. \tag{3.1}$$

Aqui $1 \leq t \leq n$. Subcubos adicionais com outras posições fixas podem ser formados combinando as operações A^σ e $A^{[\,t\,]}$ descritas aqui; na verdade, todos os subcubos concebíveis podem ser obtidos desta maneira.

3.2 Somas e Produtos de Hipercubos

A soma de dois m-cubos A e B é simplesmente definida como o m-cubo consistindo das somas das componentes:

$$C = A + B = (C_{ij\cdots r}) \longleftrightarrow A_{ij\cdots r} + B_{ij\cdots r} = C_{ij\cdots r} \tag{3.2}$$

O produto de um d-cubo B vezes um m-cubo A, resulta em um $(m + d - 2)$-cubo definido como a seguir:

$$C = B \overset{1}{\times} A = (C_{i\cdots jk\cdots r}) \longleftrightarrow C_{i\cdots jk\cdots r} = \sum_t B_{i\cdots jt} A_{tk\cdots r}.$$

Podemos definir m tais produtos, da seguinte maneira:

$$C = B \overset{l}{\times} A = (C_{i\cdots jk\cdots qr\cdots s}) \longleftrightarrow C_{i\cdots jk\cdots qr\cdots s} = \sum_t B_{k\cdots qt} A_{i\cdots jtr\cdots s} \tag{3.3}$$

onde "$i \cdots j$" representa $l - 1$ índices e "$r \cdots s$" representa $m - l$.

Note que se $B = (B_k) = (\delta_{kt})$ e A é um m-cubo então

$$(B \overset{1}{\times} A)_{i\cdots j} = \sum_k B_k A_{ki\cdots j} = \sum_k \delta_{kt} A_{ki\cdots j} = A_{ti\cdots j},$$

ou seja, $B \overset{1}{\times} A = A^{[t]}$, onde "$i \cdots j$" representa $m - 1$ índices.

Se A, B, C são matrizes, $B \overset{1}{\times} A = BA$ e $C \overset{2}{\times} A = AC^T$. De fato,

$$(B \overset{1}{\times} A)_{ij} = \sum_t B_{it} A_{tj} = (BA)_{ij}$$

e

$$(C \overset{2}{\times} A)_{ij} = \sum_t C_{jt} A_{it} = \sum_t A_{it} C^T_{tj} = (AC^T)_{ij}.$$

A lei associativa para a multiplicação de matrizes, $(BA)C^T = B(AC^T)$, pode ser escrita na forma

$$C \overset{2}{\times} (B \overset{1}{\times} A) = B \overset{1}{\times} (C \overset{2}{\times} A).$$

Esta relação é um caso especial de uma regra geral para produtos de hipercubos.

Teorema 16 (Lei associativa generalizada)**.** *Se $u < v$ e a dimensão de C é $f + 2$, então*

$$C \overset{u}{\times} (B \overset{v}{\times} A) = B \overset{v+f}{\times} (C \overset{u}{\times} A) \tag{3.4}$$

Demonstração. Sejam m e p as dimensões de A e B, respectivamente. Assim,

$$C \overset{u}{\times} (B \overset{v}{\times} A) = (C_{j_1 j_2 \cdots j_{f+2}}) \overset{u}{\times} \left((B_{k_1 k_2 \cdots k_p}) \overset{v}{\times} (A_{i_1 i_2 \cdots i_m}) \right)$$

$$= \left(C_{j_1 \cdots j_{f+2}}\right) \overset{u}{\times} \left(\sum_h B_{k_1 \cdots k_{p-1} h} A_{i_1 \cdots i_{v-1} h i_{v+1} \cdots i_m} \right)$$

$$= \left(\sum_t C_{j_1 \cdots j_{f+1} t} \left\{ \sum_h B_{k_1 \cdots k_{p-1} h} A_{i_1 \cdots i_{u-1} t i_{u+1} \cdots i_{v-1} h i_{v+1} \cdots i_m} \right\} \right)$$

$$= \left(\sum_h B_{k_1 \cdots k_{p-1} h} \left\{ \sum_t C_{j_1 \cdots j_{f+1} t} A_{i_1 \cdots i_{u-1} t i_{u+1} \cdots i_{v-1} h i_{v+1} \cdots i_m} \right\} \right)$$

$$= \left(B_{k_1 \cdots k_p}\right) \overset{v+f}{\times} \left(\sum_t C_{j_1 \cdots j_{f+1} t} A_{i_1 \cdots i_{u-1} t i_{u+1} \cdots i_m} \right)$$

$$= (B_{k_1 \cdots k_p}) \overset{v+f}{\times} \left((C_{j_1 \cdots j_{f+2}}) \overset{u}{\times} (A_{i_1 \cdots i_m}) \right) = B \overset{v+f}{\times} (C \overset{u}{\times} A)$$

□

Corolário 2. *Seja m a dimensão de A, e sejam $B_1, B_2, \cdots, B_m$ matrizes. Então as m multiplicações por A, $B_i \overset{i}{\times} A$, podem ser efetuadas em qualquer ordem, ou seja, se β é uma permutação de $\{1, 2, \cdots, m\}$, então*

$$B_1 \overset{1}{\times} (B_2 \overset{2}{\times} (\cdots (B_m \overset{m}{\times} A) \cdots)) = B_{1\beta} \overset{1\beta}{\times} (B_{2\beta} \overset{2\beta}{\times} (\cdots (B_{m\beta} \overset{m\beta}{\times} A) \cdots)). \tag{3.5}$$

Demonstração. Se a dimensão é 2, então f no Teorema 16 é sempre zero, e o resultado segue da aplicação repetida daquele teorema. □

Escreveremos

$$[B_1, B_2, \cdots, B_m] \times A$$

para denotar as operações de multiplicação expressas na Eq. (3.5).

A seguinte regra generaliza a equação matricial $(CA)^T = A^T C^T$:

Teorema 17. *Se C é uma matriz, e se σ é uma permutação, então*

$$(C \overset{u}{\times} A)^\sigma = C \overset{u\sigma}{\times} A^\sigma. \tag{3.6}$$

Demonstração. Como $(A^\sigma)_{i_1 i_2 \cdots i_m} = A_{i_{1\sigma} i_{2\sigma} \cdots i_{m\sigma}}$ e

$$(C \overset{u}{\times} A)_{i_1 i_2 \cdots i_m} = \sum_{t=1}^{n} C_{i_u t} A_{i_1 \cdots i_{u-1} t i_{u+1} \cdots i_m},$$

segue que

$$\begin{aligned}(C \overset{u\sigma}{\times} A^\sigma)_{i_1 i_2 \cdots i_m} &= \sum_t C_{i_{u\sigma} t} (A^\sigma)_{i_1 \cdots i_{u\sigma-1} t i_{u\sigma+1} \cdots i_m} \\ &= \sum_t C_{i_{u\sigma} t} A_{i_{1\sigma} \cdots i_{(u-1)\sigma} t i_{(u+1)\sigma} \cdots i_{m\sigma}},\end{aligned}$$

donde $(C \overset{u}{\times} A)^\sigma = C \overset{u\sigma}{\times} A^\sigma$. □

Outras leis associativas podem ser formuladas para incluir os casos não mencionados na hipótese do Teorema 16; ou seja, quando temos um produto $C \overset{u}{\times} (B \overset{v}{\times} A)$ tal que $u \geq v$ e $u + 2 - dim(C) \leq v$. Mas somente uma dessas leis é de nosso interesse:

Teorema 18. *Para quaisquer matrizes $B_1, \cdots, B_m$, $C_1, \cdots, C_m$ e qualquer m-cubo A,*

$$[C_1, C_2, \cdots, C_m] \times ([B_1, B_2, \cdots, B_m] \times A) = [C_1 B_1, C_2 B_2, \cdots, C_m B_m] \times A. \quad (3.7)$$

Demonstração. Pelo Teorema 17, temos

$$\left[C \overset{k}{\times} (B \overset{k}{\times} A^{(1\,k)})\right]^{(1\,k)} = C \overset{1}{\times} (B \overset{1}{\times} A)$$

e

$$\left[(CB) \overset{k}{\times} A^{(1\,k)}\right]^{(1\,k)} = (CB) \overset{1}{\times} A,$$

quando C e B são matrizes. Portanto, pelo Teorema 16, é suficiente mostrar que

$$C \overset{1}{\times} (B \overset{1}{\times} A) = (CB) \overset{1}{\times} A,$$

onde C e B são matrizes e A é um m-cubo. Como

$$C \overset{1}{\times} (B \overset{1}{\times} A) = (D_{ij\cdots r})$$

e

$$(CB) \overset{1}{\times} A = (E_{ij\cdots r}),$$

com

$$D_{ij\cdots r} = \sum_t C_{it} \left\{ \sum_h B_{th} A_{hj\cdots r} \right\} = \sum_h \left\{ \sum_t C_{it} B_{th} \right\} A_{hj\cdots r} = E_{ij\cdots r},$$

obtemos

$$C \overset{1}{\times} (B \overset{1}{\times} A) = (CB) \overset{1}{\times} A.$$

□

Proposição 2. *Sejam A um m-cubo, B um vetor, $\sigma = (23 \cdots m)$ e $\tau = (12 \cdots (m-1))$. Então*

i) $B \overset{1}{\times} A^{(1\,2)} = B \overset{2}{\times} A$;

ii) $(B \overset{1}{\times} A)^{\tau} = B \overset{1}{\times} (A^{\sigma})$.

Demonstração. Basta mostrar que as entradas são iguais.

i)

$$(B \overset{1}{\times} A^{(1\,2)})_{i_1 i_2 \cdots i_{(m-1)}} = \sum_t B_t A^{(1\,2)}_{t i_1 \cdots i_{(m-1)}} = \sum_t B_t A_{i_1 t i_2 \cdots i_{(m-1)}} = (B \overset{2}{\times} A)_{i_1 i_2 \cdots i_{(m-1)}}.$$

ii)

$$[(B \overset{1}{\times} A)^{\tau}]_{i_1 i_2 \cdots i_{(m-1)}} = (B \overset{1}{\times} A)_{i_{1\tau} i_{2\tau} \cdots i_{(m-1)\tau}} = (B \overset{1}{\times} A)_{i_2 i_3 \cdots i_{(m-1)} i_1}$$

$$= \sum_t B_t A_{t i_2 i_3 \cdots i_{(m-1)} i_1}.$$

$$(B \overset{1}{\times} (A^{\sigma}))_{i_1 i_2 \cdots i_{(m-1)}} = \sum_t B_t A^{\sigma}_{t i_1 i_2 \cdots i_{(m-1)}} = \sum_t B_t A_{t i_2 i_3 \cdots i_{(m-1)} i_1}.$$

□

3.3 Hipercubos Não-singulares

O conceito de matriz não-singular pode ser generalizado procedendo-se indutivamente, da seguinte forma:

Definição 14. *Dizemos que um vetor, ou 1-cubo, A, é* **singular** *se, e somente se, $A = 0$. Para $m > 1$, dizemos que um m-cubo A é* **singular** *se, e somente se, existe um vetor não-singular B tal que $B \overset{1}{\times} A$ é singular. Equivalentemente, A é não-singular se, para todo vetor B tal que $B \overset{1}{\times} A$ é singular, tem-se que $B = 0$.*

Outra maneira de estabelecermos esta definição é que um m-cubo A é **não-singular** se a seguinte condição é satisfeita:

"$x_1A^{[1]} + x_2A^{[2]} + \cdots + x_nA^{[n]}$ singular implica em $x_1 = x_2 = \cdots = x_n = 0$."

Em outras palavras, qualquer combinação linear não nula de subcubos $A^{[t]}$ deve ser não-singular. Obviamente, esta definição inclui a definição de matriz não-singular, no caso especial em que $m = 2$: uma matriz A é não-singular se, e somente se, suas linhas são linearmente independentes.

Teorema 19. *Seja A um m-cubo e σ uma permutação de $\{1, 2, \cdots, m\}$. Então A é não-singular se, e somente se, A^σ é não-singular.*

Demonstração. Utilizaremos indução sobre m. Para $m = 1$ é trivial, e para $m = 2$ é o caso especial do teorema que afirma que "o posto-linha e o posto-coluna de uma matriz são iguais". Assumiremos, portanto, que $m > 2$.

Sem perda de generalidade assumiremos que σ seja da forma $(1\,2)$ ou $(2\,3\,\cdots\,m)$, já que estas duas permutações geram todas as $m!$ permutações.

Se $\sigma = (1\,2)$, argumentamos como a seguir, onde B e C denotam vetores:

A é não-singular
$\leftrightarrow (C \neq 0 \rightarrow C \overset{1}{\times} A$ é não-singular)
$\leftrightarrow (C \neq 0 \rightarrow (B \neq 0 \rightarrow B \overset{1}{\times} (C \overset{1}{\times} A)$ é não-singular)) já que $m > 2$
$\leftrightarrow (B \neq 0 \rightarrow (C \neq 0 \rightarrow B \overset{1}{\times} (C \overset{1}{\times} A)$ é não-singular))
$\leftrightarrow (B \neq 0 \rightarrow (C \neq 0 \rightarrow C \overset{1}{\times} (B \overset{2}{\times} A)$ é não-singular)) pelo Teorema 16
$\leftrightarrow (B \neq 0 \rightarrow B \overset{2}{\times} A$ é não-singular)
$\leftrightarrow (B \neq 0 \rightarrow B \overset{1}{\times} A^\sigma$ é não-singular) já que $B \overset{1}{\times} A^{(1\,2)} = B \overset{2}{\times} A$ pela Proposição 2, parte (i))
$\leftrightarrow A^\sigma$ é não-singular.

Por outro lado, se $\sigma = (2\,3\,\cdots\,m)$, seja $\tau = (1\,2\,\cdots\,(m-1))$. Então, já que $(B \overset{1}{\times} A)^\tau = B \overset{1}{\times} (A^\sigma)$, pela Proposição 2, parte (ii), argumentamos como segue:

$$\begin{aligned} A \text{ é não-singular} &\leftrightarrow (B \neq 0 \rightarrow B \overset{1}{\times} A \text{ é não-singular}) \\ &\leftrightarrow (B \neq 0 \rightarrow (B \overset{1}{\times} A)^\tau \text{ é não-singular}) \text{ por indução} \\ &\leftrightarrow (B \neq 0 \rightarrow B \overset{1}{\times} (A^\sigma) \text{ é não-singular}) \\ &\leftrightarrow A^\sigma \text{ é não-singular.} \end{aligned}$$

□

Teorema 20. *Seja A um m-cubo e sejam $C_1, C_2, \cdots, C_m$ matrizes não-singulares. Então A é não-singular se, e somente se,*

$$[C_1, C_2, \cdots, C_m] \times A$$

é não-singular.

Demonstração. Para $m = 1$ é meramente a definição de uma matriz não-singular C_1. Para $m > 1$, é suficiente mostrar que A é singular se, e somente se, $C \overset{2}{\times} A$ é singular, por causa dos Teoremas 17 e 19. Agora,

$C \overset{2}{\times} A$ é não-singular
$\leftrightarrow (B \neq 0 \rightarrow B \overset{1}{\times} (C \overset{2}{\times} A)$ é não-singular)
$\leftrightarrow (B \neq 0 \rightarrow C \overset{1}{\times} (B \overset{1}{\times} A)$ é não-singular) pelo Teorema 16
$\leftrightarrow (B \neq 0 \rightarrow B \overset{1}{\times} A$ é não-singular) por indução

$\leftrightarrow A$ é não-singular. □

Finalmente, definimos uma relação de equivalência $\equiv$ entre m-cubos como a seguir:

$$A \equiv B \quad \text{se, e somente se,} \quad A = [C_1, C_2, \cdots, C_m] \times B \tag{3.8}$$

para matrizes não-singulares $C_1, C_2, \cdots, C_m$. Pelos Teoremas 18 e 20 esta é uma relação de equivalência que preserva a não-singularidade.

3.4 Pré-semicorpos representados por 3-cubos

A partir de agora especializamos a discussão para o caso $m = 3$. Seja S um pré-semicorpo de característica p. De acordo com o capítulo 1, S é um espaço vetorial sobre $F = GF(p)$. Seja $\{x_1, x_2, \cdots, x_n\}$ uma base de S sobre F. Podemos escrever a multiplicação em termos dos elementos da base:

$$x_i x_j = \sum_k A_{ijk} x_k. \tag{3.9}$$

Disto origina um 3-cubo, $A = (A_{ijk})$, com entradas em F. A é chamado **cubo correspondendo** a S.

A multiplicação em S é completamente determinada pelo produto entre os elementos da base, de acordo com as leis distributivas, uma vez que

$$\left\{\sum_i b_i x_i\right\}\left\{\sum_j c_j x_j\right\} = \sum_i \sum_j b_i c_j x_i x_j = \sum_i \sum_j \sum_k b_i c_j A_{ijk} x_k. \tag{3.10}$$

Teorema 21. *Um cubo correspondendo a um pré-semicorpo é não-singular. Reciprocamente, se A é um 3-cubo não-singular, podemos definir um pré-semicorpo S pela Eq. (3.10), tendo os x_i's como elementos de uma base do espaço vetorial subjacente a S.*

Demonstração. Por causa das primeiras observações deste capítulo necessitamos mostrar apenas que a multiplicação definida pela Eq. (3.10) satisfaz ao axioma **A2** se, e somente se, A é não-singular.

Sejam B e C os vetores correspondentes aos coeficientes de a e b na base $\{x_1, x_2, \cdots, x_n\}$. Assim

$$a = \sum_i B_i x_i, \quad b = \sum_j C_j x_j$$

e

$$a \cdot b = \left\{\sum_i B_i x_i\right\}\left\{\sum_j C_j x_j\right\} = \sum_i \sum_j B_i C_j x_i x_j$$

$$= \sum_i \sum_j \sum_k B_i C_j A_{ijk} x_k = \sum_k \sum_i \sum_j B_i C_j A_{ijk} x_k.$$

Fazendo $d = a \cdot b$, se $D = (D_k)$ é o vetor correspondente aos coeficientes de d na base $\{x_1, x_2, \cdots, x_n\}$, temos

$$d = a \cdot b = \sum_k D_k x_k, \quad \text{onde} \quad D_k = \sum_i \sum_j B_i C_j A_{ijk}.$$

Olhando agora para a demonstração do Teorema 19, vemos que A é não-singular se, e somente se, $B \neq 0$ e $C \neq 0 \rightarrow C \overset{1}{\times} (B \overset{1}{\times} A) \neq 0$ (no caso $m = 3$). Mas $C \overset{1}{\times} (B \overset{1}{\times} A)$ é o vetor $D = (D_k)$ acima descrito,

$$D_k = \sum_i \sum_j B_i C_j A_{ijk};$$

entretanto esta é, precisamente, a condição de que $(a \neq 0 \text{ e } b \neq 0) \rightarrow ab \neq 0$. □

Podemos observar também que um 4-cubo pode corresponder a um sistema algébrico com uma multiplicação ternária, satisfazendo três leis distributivas e com nenhum divisor próprio do zero. Em geral, um m-cubo não-singular poderá levar a uma operação $(m-1)$-ária.

Se mudarmos para uma base diferente $\{y_1, y_2, \cdots, y_n\}$ de S sobre F, temos

$$y_i = \sum_j C_{ij} x_j,$$

onde $C = (C_{ij})$ é uma matriz não-singular.

Isto introduz uma correspondente mudança em A; seja B o novo cubo. Então, como

$$\sum_l C_{kl}^{-1} y_l = \sum_l C_{kl}^{-1} \sum_j C_{lj} x_j = \sum_l \sum_j C_{kl}^{-1} C_{lj} x_j = \sum_j \left\{ \sum_l C_{kl}^{-1} C_{lj} \right\} x_j = \sum_j \delta_{kj} x_j = x_k,$$

obtemos

$$y_i y_j = \left\{ \sum_r C_{ir} x_r \right\} \left\{ \sum_s C_{js} x_s \right\} = \sum_r \sum_s \sum_k C_{ir} C_{js} A_{rsk} x_k$$

$$= \sum_r \sum_s \sum_k \sum_l C_{ir} C_{js} A_{rsk} C_{kl}^{-1} y_l = \sum_l \sum_r \sum_s \sum_k C_{ir} C_{js} C_{kl}^{-1} A_{rsk} y_l.$$

Agora B_{ijl} é o coeficiente de y_l; portanto

$$B = [C, C, C^{-T}] \times A, \tag{3.11}$$

onde $-T$ denota a transposta inversa. Conseqüentemente, $B \equiv A$.

Definiremos agora uma nova operação $\star$ sobre os elementos de S da seguinte maneira:

$$(a \star b)H = (aF)(bG) \tag{3.12}$$

onde F, G, H são transformações lineares não-singulares arbitrárias de S sobre si mesmo. Isto nos dá outro pré-semicorpo S', que é dito ser *isotópico* a S.

Seja B um cubo correspondendo ao pré-semicorpo S'. Podemos admitir que S' tenha a mesma base $\{x_1, x_2, \cdots, x_n\}$ como S, e que A seja o cubo de S com esta base. Considere F, G, H como matrizes; ou seja,

$$x_i F = \sum_r F_{ir} x_r. \tag{3.13}$$

Então

$$x_i \star x_j = ((x_i F)(x_j G))\, H^{-1} = \left(\left(\sum_r F_{ir} x_r\right)\left(\sum_s G_{js} x_s\right)\right) H^{-1}$$

$$= \left\{\sum_r \sum_s \sum_t F_{ir} G_{js} A_{rst} x_t\right\} H^{-1}$$

$$= \sum_r \sum_s \sum_t \sum_k F_{ir} G_{js} H^{-1}_{tk} A_{rst} x_k.$$

Assim

$$B = [F, G, H^{-T}] \times A. \tag{3.14}$$

Isto prova o seguinte teorema fundamental:

Teorema 22. *Sejam S e S' pré-semicorpos, A e A' cubos correspondendo a S e S'. Então S é isotópico a S' se, e somente se, $A \equiv A'$ (onde a equivalência é definida na Eq. (3.8)).*

3.5 Semicorpos e Pré-semicorpos equivalentes.

A discussão anterior é aplicada a semicorpos como caso especial de pré-semicorpos. Se S é um semicorpo, podemos assumir que sua base seja da forma $\{1, x_2, \cdots, x_n\}$. O cubo A correspondendo a S tem uma propriedade especial.

Para começar, escrevemos

$$A^{r**} = A^{[r]}, \quad A^{*r*} = B^{[r]} \quad \text{e} \quad A^{**r} = \widehat{B}^{[r]}, \quad \text{onde} \quad B = A^{(1\,3\,2)} \quad \text{e} \quad \widehat{B} = A^{(1\,2\,3)}.$$

Assim,

$$B = (B_{kij}) = \left(A^{(1\,3\,2)}_{kij}\right) = (A_{jki}) \longleftrightarrow B^{[r]} = (B_{rij}) = (A_{jri})$$

e

$$\widehat{B} = \left(\widehat{B}_{kij}\right) = \left(A^{(1\,2\,3)}_{kij}\right) = (A_{ijk}) \longleftrightarrow \widehat{B}^{[r]} = \left(\widehat{B}_{rij}\right) = (A_{ijr})\,.$$

Em outras palavras, A^{r**}, A^{*r*} e A^{**r} são as matrizes (A_{rij}), (A_{jri}) e (A_{ijr}), respectivamente. Além disso, como

$$x_k A^{r**} = x_k\,(A_{rij}) = \sum_t A_{rkt} x_t = x_r \cdot x_k = x_k L_{x_r}$$

e

$$x_k \left(A^{*r*}\right)^T = x_k \left(A_{jri}\right)^T = x_k \left(A_{irj}\right) = \sum_t A_{krt} x_t = x_k \cdot x_r = x_k R_{x_r},$$

então A^{r**} é a matriz L_{x_r} da multiplicação à esquerda por x_r e A^{*r*} é a transposta da matriz para a multiplicação à direita, R_{x_r}. Demonstraremos agora as seguintes fórmulas:

$$\begin{aligned}
&(\mathbf{a}) \quad ([F,G,H] \times A)^{r**} = F_{r1}(GA^{1**}H^T) + \cdots + F_{rn}(GA^{n**}H^T) \\
&(\mathbf{b}) \quad ([F,G,H] \times A)^{*r*} = G_{r1}(HA^{*1*}F^T) + \cdots + G_{rn}(HA^{*n*}F^T) \\
&(\mathbf{c}) \quad ([F,G,H] \times A)^{**r} = H_{r1}(FA^{**1}G^T) + \cdots + H_{rn}(FA^{**n}G^T).
\end{aligned} \tag{3.15}$$

Demonstração. **(a)**

$$\begin{aligned}
([F,G,H] \times A)_{rij} &= \sum_k \sum_s \sum_t F_{rk} G_{is} H_{jt} A_{kst} = \sum_k F_{rk} \left\{ \sum_s \sum_t G_{is} H_{jt} A_{kst} \right\} \\
&= \sum_k \left\{ \sum_s \sum_t G_{is} A_{kst} H^T_{tj} \right\} = \sum_k F_{rk} (GA^{k**}H^T)_{ij}
\end{aligned}$$

(b)

$$\begin{aligned}
([F,G,H] \times A)_{jri} &= \sum_k \sum_s \sum_t F_{jk} G_{rs} H_{it} A_{kst} = \sum_s G_{rs} \left\{ \sum_k \sum_t F_{jk} H_{it} A_{kst} \right\} \\
&= \sum_s G_{rs} \left\{ \sum_k \sum_t F_{jk} H_{it} A^{*s*}_{tk} \right\} = \sum_s G_{rs} \left\{ \sum_k \sum_t H_{it} A^{*s*}_{tk} F^T_{kj} \right\} \\
&= \sum_s G_{rs} (HA^{*s*}F^T)_{ij}
\end{aligned}$$

(c)

$$\begin{aligned}
([F,G,H] \times A)_{ijr} &= \sum_k \sum_s \sum_t F_{ik} G_{js} H_{rt} A_{kst} = \sum_t H_{rt} \left\{ \sum_k \sum_t F_{ik} G_{js} A^{**t}_{ks} \right\} \\
&= \sum_t H_{rt} \left\{ \sum_k \sum_t F_{ik} A^{**t}_{ks} G^T_{sj} \right\} = \sum_t H_{rt} (FA^{**t}G^T)_{ij}
\end{aligned}$$

□

Definição 15. *Dizemos que A está na* **forma padrão** *se $A^{1**} = A^{*1*} = I$.*

Teorema 23. *Seja S um semicorpo com base $\{1, x_2, \cdots, x_n\}$. Então o cubo correspondendo a S é não-singular e está na forma padrão; reciprocamente, todo 3-cubo não singular na forma padrão produz um semicorpo se a multiplicação estiver definida por (3.10).*

Demonstração. Pelo Teorema 21, precisamos apenas mostrar que a forma padrão é equivalente ao axioma **A4.** Mas isto é evidente, porque a forma padrão nada mais é do que a condição de que $L_1 = R_1 = I$. □

Teorema 24. *Sejam S e S' semicorpos com correspondentes cubos A e A'. Então S e S' coordenatizam o mesmo plano projetivo se, e somente se, $A \equiv A'$. Planos coordenatizados por semicorpos estão em correspondência biunívoca com as classes de equivalência dos 3-cubos não-singulares.*

Demonstração. Aplicação dos Teoremas 22 e 12. □

Teorema 25. *Se A é um cubo correspondendo a um semicorpo próprio S, o grupo dos automorfismos de S é isomorfo ao grupo de todas as triplas de matrizes (F, G, H) tais que*

$$[F, G, H] \times A = A. \tag{3.16}$$

Demonstração. Segue da Eq. (3.14). □

Note que o mesmo resultado vale para um 3-cubo qualquer B com $B \equiv A$, mesmo que B não esteja na forma padrão, já que os grupos correspondentes são conjugados.

Agora voltaremos a questão de construirmos um semicorpo a partir de um pré-semicorpo. Esta é meramente a questão de encontrarmos três matrizes não-singulares, F, G e H, tais que $[F, G, H] \times A$ está na forma padrão. Tal construção pode ser feita de diversas formas; por exemplo:

1. Tome $H = I,\ G = (A^{1**})^{-1}$ e $F = (B^{*1*})^{-T}$, onde $B = G \overset{1}{\times} A$.

2. Tome $H = I,\ F = (A^{*1*})^{-T}$ e $G = (B^{1**})^{-1}$, onde $B = F \overset{1}{\times} A$,

3. Tome $G = I,\ H = (A^{1**})^{-T}$ e $F = A^{1**}(A^{*1*})^{-T}$.

4. Tome $F = I,\ H = (A^{*1*})^{-1}$ e $G = (A^{*1*})^T (A^{1**})^{-1}$.

As demonstrações de que as escolhas acima fazem o trabalho são análogas, usando a Eq. (3.15). Considerando o método 3, por exemplo:

$$F = \begin{pmatrix} a_{111} & a_{112} & \cdots & a_{11n} \\ a_{121} & a_{122} & & a_{12n} \\ . & . & & . \\ . & . & & . \end{pmatrix} \cdot \begin{pmatrix} a_{111} & a_{211} & \cdots & a_{n11} \\ a_{112} & a_{212} & \cdots & a_{n12} \\ . & . & & . \\ . & . & & . \end{pmatrix}^{-T}$$

$$= \begin{pmatrix} a_{111} & a_{112} & \cdots & a_{11n} \\ a_{121} & a_{122} & & a_{12n} \\ . & . & & . \\ . & . & & . \end{pmatrix} \cdot \begin{pmatrix} a_{111} & a_{112} & \cdots & a_{11n} \\ a_{211} & a_{212} & \cdots & a_{21n} \\ . & . & & . \\ . & . & & . \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ . & . & & . \\ . & . & & . \\ . & . & & . \end{pmatrix}.$$

Conseqüentemente

$$([F, G, H] \times A)^{1**} = GA^{1**}H^T = I;$$

e

$$([F, G, H] \times A)^{*1*} = HA^{*1*}F^T = I.$$

Estes métodos podem ser traduzidos em termos algébricos; aqui é o método 3 nesta forma:

Teorema 26. *Seja $(S, +, \circ)$ um pré-semicorpo e $u \in S$. Então se definirmos uma nova multiplicação $*$ pela regra*

$$(a \circ u) * (u \circ b) = a \circ b \tag{3.17}$$

obtemos um semicorpo $(S, +, *)$ com unidade $u \circ u$.

Note que se $(S, +, \circ)$ é comutativo, então $(S, +, *)$ também é comutativo.

A fórmula (3.17) é um caso particular da Eq. (2.10) com $H = I,\ F = R_u^{-1}$ e $G = L_u^{-1}$, já que

$$(a \circ u) * (u \circ b) = (a \circ u)F \circ (u \circ b)G = (a \circ u)R_u^{-1} \circ (u \circ b)L_u^{-1} = a \circ b.$$

Uma maneira menos simétrica de escrevermos esta fórmula pode ser interpretada diretamente do método 3: fazendo $\widehat{G} = I,\ \widehat{H} = A^{1**} = L_u$ e $\widehat{F} = A^{1**}(A^{*1*})^{-T} =$

$L_u R_u^{-1}$ temos $(a \bullet b)\widehat{H} = a\widehat{F} \circ b\widehat{G}$, pela Eq. (2.10), donde segue que $(a \bullet b)L_u = aL_u R_u^{-1} \circ bI$. Daí

$$u \circ (a \bullet b) = (u \circ a)R_u^{-1} \circ b$$

e encontramos um semicorpo $(S, +, \bullet)$ com unidade u. Mas $(S, +, *) \cong (S, +, \bullet)$, pois

$$(u \circ u)F = u\widehat{F} = u \quad \text{e} \quad (u \circ u)G = u\widehat{G} = u$$

(Veja demonstração do Teorema 5).
O método 4 proporciona outro sistema isomorfo $(S, +, \odot)$, "dual" ao sistema $(S, +, \bullet)$, com unidade u e fórmula

$$(a \odot b) \circ u = a \circ (b \circ u)L_u^{-1}.$$

Podemos obter, deste modo, semicorpos a partir de pré-semicorpos de diversas maneiras; em cada método que encontramos fomos capazes de permitir que F, G ou H seja igual a identidade.

O grau de liberdade extra que vimos ter neste processo de padronização indica que devemos buscar uma forma "mais padronizada" que a forma padrão. Algo sugestivo seria requerermos que $A^{**1} = I$ também. Veremos se com esta restrição obtemos uma forma canônica.

Se S é um corpo com p^2 elementos, então pode sempre ser representado na forma

$$A^{1**} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad A^{2**} = \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix},$$

se a é escolhido tal que $x^2 - ax - 1$ é irredutível $\pmod p$.

Adotando a convenção de escrevermos $A^{1**}, A^{2**}, \cdots$ nesta ordem, o corpo $GF(8)$ pode ser representado nas formas:

$$\begin{array}{ccc} 100 & 010 & 001 \\ 010 & 101 & 011 \\ 001 & 011 & 111 \end{array} \quad \text{ou} \quad \begin{array}{ccc} 100 & 010 & 001 \\ 010 & 111 & 011 \\ 001 & 011 & 110 \end{array}.$$

No caso de $GF(8)$ representado como

$$\begin{array}{ccc} 100 & 010 & 001 \\ 010 & 101 & 011 \\ 001 & 011 & 111 \end{array},$$

admitimos que $GF(8) = \mathbb{Z}_2(\alpha)$, onde α satisfaz $\alpha^3 + \alpha + 1 = 0$, e a base escolhida na forma $\{1, \alpha + 1, \alpha^2\}$. No caso de $GF(8)$ representado como

$$\begin{array}{ccc} 100 & 010 & 001 \\ 010 & 111 & 011 \\ 001 & 011 & 110 \end{array},$$

admitimos que $GF(8) = \mathbb{Z}_2(\beta)$, onde β satisfaz $\beta^3 + \beta^2 + 1 = 0$, e a base escolhida na forma $\{1, \beta + 1, \beta^2 + \beta + 1\}$.

Pode ser facilmente verificado que nos exemplos acima temos que

$$A^{1**} = A^{*1*} = A^{**1} = I,$$

mas não está claro que esta forma é possível em geral. Estes exemplos mostram que não temos uma forma canônica; mas, se for verdade que todos os cubos não-singulares puderem ser escolhidos desta maneira, será bastante útil para eliminarmos alguns casos na construção de semicorpos.

Uma maneira bastante útil de usarmos a liberdade extra é ajustarmos a matriz A^{2**} para que seu polinômio característico seja irredutível. Se este ajuste puder ser feito, o semicorpo resultante poderá ser visto como um espaço vetorial com base da forma 1, x, x^2, $x(x^2)$, $x(x(x^2))$, etc. Operações deste tipo podem ser exploradas na construção de todos os possíveis semicorpos de uma dada ordem.

Capítulo 4

Transposição de um plano

Neste capítulo discutiremos um interessante relacionamento entre alguns planos coordenatizados por semicorpos. O relacionamente é um tanto peculiar já que tem significado algébrico mas não parece ter significado geométrico.

Definição 16 (Plano Transposto)**.** *Sejam π um plano projetivo, S um semicorpo que coordenatiza π, e A um cubo correspondendo a S. Sejam, ainda, S_1 o pré-semicorpo descrito por $A^{(2\,3)}$ e S_2 o semicorpo construído por S_1 por isotopia. Então definimos π^T, o* **plano transposto** *de π, como o plano coordenatizado por S_2.*

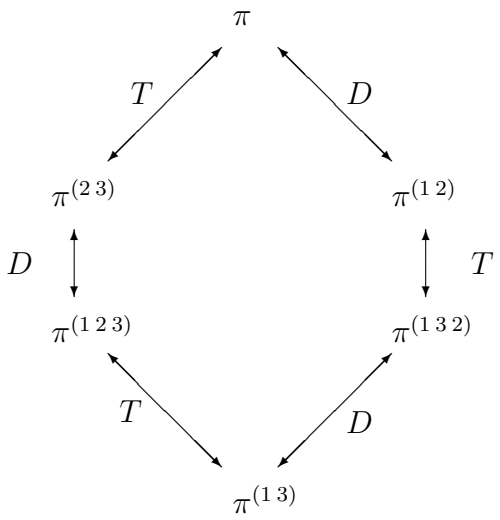
Teorema 27. *π^T é unicamente definido.*

Demonstração. Como nenhuma restrição sobre a escolha de S é feita, os A's resultantes poderão ser equivalentes, pelo Teorema 24. O 3-cubo $A^{(2\,3)}$ é não-singular, pelo Teorema 19. Se $A \equiv B$, então $A^{(2\,3)} \equiv B^{(2\,3)}$, pelo Teorema 17. Portanto $A^{(2\,3)}$ é unicamente determinado, a menos de equivalência, e o plano π^T é unicamente determinado. □

Corolário 3. $(\pi^T)^T = \pi$.

Definição 17 (Plano Dual)**.** *O* **dual π^D de um plano** *coordenatizado por um semicorpo é bem conhecido, sendo determinado pela construção do semicorpo anti-isomorfo, i.e., substituindo ab por ba no semicorpo. Esta definição pode ser expressa da mesma maneira que a definição de π^T, usando $A^{(1\,2)}$ no lugar de $A^{(2\,3)}$.*

Teorema 28. *As operações de dualidade e transposição geram uma série de, no máximo, seis planos, de acordo com o seguinte esquema:*



Demonstração. Este teorema é óbvio da maneira em que plano transposto e plano dual foram definidos. □

Corolário 4. *Se $\pi = \pi^D \neq \pi^T$ então existe um terceiro plano π^{TD} diferente de π e de π^T.*

Demonstração. Se $\pi^{TD} = \pi$ então $\pi^T = \pi^D = \pi$. Se $\pi^{TD} = \pi^T$, então $\pi^{TD} = (\pi^D)^{TD} = \pi^{(1\,3)} = (\pi^{TD})^T = \pi^{TT} = \pi$. □

4.1 Colineações

Teorema 29. *O grupo das colineações de π^T tem a mesma ordem que o grupo das colineações de π.*

Demonstração. Trata-se do Teorema 13. Os grupos das translações e os grupos dos *shears* são isomorfos. Os grupos dos autotopismos também são isomorfos, pelo Teorema 17, já que

$$[F, G, H] \times A \equiv A \longleftrightarrow [F, H, G] \times A^{(2\,3)} \equiv A^{(2\,3)}.$$

Portanto, os grupos de colineações têm a mesma ordem. As inter-relações entre autotopismos, translações e *shears* são, contudo, diferentes como as Eq. (2.21) mostram. □

4.2 Exemplos

O transposto de um plano desarguesiano é desarguesiano, pois todas as matrizes de multiplicação à esquerda são potências da mesma matriz, e esta propriedade é preservada por transposição.

Os planos coordenatizados por semicorpos de ordem 32 foram calculados por R. J. Walker [18]. Além do plano Desarguesiano, existem cinco outros planos.

O plano $P(1)$ tem a representação por 3-cubos:

$$\begin{array}{ccccc} 10000 & 01000 & 00100 & 00010 & 00001 \\ 01000 & 00100 & 00010 & 00001 & 10100 \\ 00100 & 00010 & 01001 & 10100 & 00101 \\ 00010 & 00001 & 11010 & 11110 & 10111 \\ 00001 & 10010 & 11011 & 10000 & 01110 \end{array} . \tag{4.1}$$

Este plano foi descoberto em Dezembro de 1961 por R.J. Walker com um programa de computador escrito em um Burroughs 220.

Não existe nenhum autotopismo exceto a identidade; conseqüentemente, o grupo de colineações de $P(1)$ é gerado somente pelas translações e *shears*. Este é o único plano coordenatizado por um semicorpo (exceto o seu dual) com esta propriedade. Uma conseqüencia adicional é que existem 31^2 distintos semicorpos, isotópicos mas não-isomorfos (veja Eq. (2.17)).

O plano $P(2)$ é o dual e também o transposto de $P(1)$, e tem as mesmas propriedades.

O plano $P(3)$ é construído do semicorpo binário de ordem 32 (veja Seção 5.6). Este plano tem a seguinte representação por 3-cubos:

$$
\begin{array}{ccccc}
10000 & 01000 & 00100 & 00010 & 00001 \\
01000 & 00100 & 00010 & 00001 & 11000 \\
00100 & 00010 & 11001 & 01010 & 00111 \\
00010 & 00001 & 01010 & 11011 & 11100 \\
00001 & 11000 & 00111 & 11100 & 10111
\end{array} . \tag{4.2}
$$

Este representante particular tem cinco automorfismos e cinco autotopismos; existem 192 outros sistemas isotópicos a este e nenhum desses têm automorfismos não-triviais. Isto é compatível com a Eq. (2.17):

$$31^2 = \left(\frac{5}{5}\right) + 192 \cdot \left(\frac{5}{1}\right) .$$

O plano $P(3)$ é auto-dual, já que seu semicorpo é comutativo, mas não é auto-transposto. Conseqüentemente (Corolário 4), existem dois outros planos, $P(4) = P(3)^T$, e $P(5) = P(4)^D$. Cada um destes planos também contém um sistema com cinco automorfismos e 192 outros sistemas sem automorfismos não-triviais.

R. J. Walker mostrou, por exaustivas enumerações em um computador, que estes cinco planos constituem o conjunto de todos os semicorpos próprios de ordem 32.

Capítulo 5

Alguns semicorpos conhecidos

Neste capítulo, discutiremos alguns semicorpos conhecidos e consideraremos quais são as possíveis ordens para semicorpos próprios. Neste capítulo p será sempre um número primo.

5.1 Ordens excluídas

Vimos que os semicorpos têm ordem da forma p^n. Para todo primo p e n natural existe um único corpo com p^n elementos. O que podemos dizer sobre semicorpos próprios ?

Se a ordem do semicorpo é p, então este semicorpo é o corpo $GF(p)$. Além disso, se a ordem do semicorpo for p^2, então este semicorpo precisa ser o corpo $GF(p^2)$: Seja $\{1, x\}$ uma base para o semicorpo; a multiplicação é determinada pela definição de $x^2 = ax+b$. Mas o polinômio x^2-ax-b não possui raízes em $GF(p)$, pois teríamos $(x-r)(x-s) = x^2 - ax - b = 0$ com r e s em $GF(p)$, contradizendo o axioma **A2.** Conseqüentemente, $x^2 - ax - b$ é irredutível em $GF(p)$, e a multiplicação é aquela de $GF(p^2)$.

Se a ordem do semicorpo é 8, verificaremos que o único semicorpo possível é o corpo $GF(8)$. Seja $\{1, x, y\}$ uma base para o semicorpo sobre $GF(2)$ e L a matriz A^{2**} da multiplicação à esquerda por x. Se a equação característica de L é $\lambda^3+a\lambda^2+b\lambda+c = 0$ então L satisfaz esta equação. Assim, encontramos $x(x^2)+ax^2+bx+c = 0$. Mas este polinômio é irredutível, já que não pode ter fatores lineares; portanto este polinômio

é uma das duas formas: $x(x^2) + x^2 + 1 = 0$ ou $x(x^2) + x + 1 = 0$. Substituindo x por $x+1$, se necessário, podemos assumir que $x(x^2)+x+1 = 0$. Em particular, $\{1, x, x^2\}$ é uma base para o semicorpo.

Para o restante da demonstração consideraremos as seguintes possibilidades:

I. Se $x^2x = 1$, então $(x^2 + x + 1)(x + 1) = 0$.

II. Se $x^2x = x$, então $(x^2 + 1)x = 0$.

III. Se $x^2x = x^2$, então $x^2(x + 1) = 0$.

IV. Se $x^2x = x^2 + x$, então $(x^2 + x + 1)x = 0$.

V. Se $x^2x = x^2 + x + 1$, então $(x^2 + 1)(x + 1) = 0$.

VI. Se $x^2x^2 = 1$, então $(x^2 + 1)^2 = 0$.

VII. Se $x^2x^2 = x + 1$, então $(x^2 + x)x^2 = 0$.

VIII. Se $x^2x^2 = x^2$, então $(x^2 + 1)x^2 = 0$.

IX. Se $x^2x^2 = x^2 + x + 1$, então $(x^2 + x + 1)x^2 = 0$.

X. Se $x^2x = x^2 + 1$ e $x^2x^2 = x$, então $(x^2 + x)^2 = 0$.

XI. Se $x^2x = x^2 + 1$ e $x^2x^2 = x^2 + 1$, então $x^2(x + x^2) = 0$.

XII. Se $x^2x = x^2 + 1$ e $x^2x^2 = x^2 + x$, então $(x^2 + 1)(x^2 + x + 1) = 0$.

XIII. Se $x^2x = x + 1$ e $x^2x^2 = x$, então $(x^2 + x)(x^2 + x + 1) = 0$.

XIV. Se $x^2x = x + 1$ e $x^2x^2 = x^2 + 1$, então $(x^2 + 1)(x^2 + x) = 0$.

XV. Se $x^2x = x + 1$ e $x^2x^2 = x^2 + x$, então temos o corpo $GF(8)$.

Provamos, então, o seguinte teorema:

Teorema 30. *Um semicorpo próprio tem ordem p^n, onde $n \geq 3$ e $p^n \geq 16$.*

Mostraremos pelas construções desta seção que a condição *necessária* que obtemos sobre a ordem é também *suficiente.*

5.2 Semicorpos de ordem 16

Os semicorpos de ordem 16 foram calculados em [11] por Kleinfeld. Existem 23 semicorpos próprios não-isomorfos de ordem 16. Todos são isotópicos ou ao sistema V ou ao sistema W da Seção 1.2; conseqüentemente, dois planos projetivos podem ser formados.

O primeiro plano, consistindo dos semicorpos isotópicos a V, contém 18 semicorpos distintos. Existe um (o próprio V) com 6 automorfismos, outro com 3 automorfismos, 8 com 2 automorfismos, e 8 com somente o automorfismo identidade. Conseqüentemente, existem 18 autotopismos pela fórmula (2.17):

$$15^2 = 18\left(\frac{1}{6} + \frac{1}{3} + \frac{8}{2} + \frac{8}{1}\right). \tag{5.1}$$

O segundo plano tem somente cinco semicorpos distintos. Um destes tem 4 automorfismos, um (W) tem 3, e os outros três restantes têm 2 automorfismos. Também, pela fórmula (2.17), existem 108 autotopismos, e

$$15^2 = 108\left(\frac{1}{4} + \frac{1}{3} + \frac{3}{2}\right). \tag{5.2}$$

Já que o número de autotopismos é diferente, podemos concluir que cada plano é auto-dual e auto-transposto.

5.3 O trabalho precursor de Dickson

O estudo de semicorpos aparentemente foi introduzido por L. E. Dickson em 1905 [6]. Em dois artigos iniciais sobre o assunto, Dickson construiu todos os possíveis semicorpos de ordem p^3, e todos os possíveis semicorpos comutativos de ordem p^4, onde p é ímpar.

Segundo D. Knuth [12], talvez a maneira mais simples para construir semicorpos próprios seja análoga a construção de V e W na Seção 1.2; iniciando com um corpo $GF(p^m)$ e construindo um semicorpo de ordem p^{2m}, tendo elementos

$$a + \lambda b, \quad \text{com} \quad a, b \in GF(p^m).$$

Para isto a multiplicação será definida, simplesmente, por

$$(a + \lambda b)(c + \lambda c) = f(a, b, c, d) + \lambda g(a, b, c, d),$$

onde f e g são lineares em todas as quatro variáveis, e onde

$$f(a,b,c,d) = g(a,b,c,d) = 0$$

implica em $a = b = 0$ ou $c = d = 0$. Existem muitas maneiras de fazer isto.

Dickson [7] encontrou uma construção particular de um semicorpo *comutativo* deste tipo para p ímpar, com multiplicação definida por

$$(a + \lambda b)(c + \lambda d) = (ac + b^\sigma d^\sigma f) + \lambda(ad + bc), \tag{5.3}$$

onde σ é um automorfismo e f não é um quadrado do corpo $GF(p^m)$. A condição de que f necessariamente é um elemento não-quadrado é clara, porque se $f = a^2$, escolhendo b tal que $b^\sigma = a^{-1}$, temos $(1+\lambda b)(1-\lambda b) = 0$. Para verificar que a condição é suficiente, suponha que $(a + \lambda b) \neq 0$ e $(c + \lambda d) \neq 0$, mas $(a + \lambda b)(c + \lambda d) = 0$. Então, em primeiro lugar, temos

$$ac + b^\sigma d^\sigma f = 0;$$

isto implica que existe um elemento $x \neq 0$ em F tal que

$$a = xd^\sigma \quad \text{e} \quad c = -x^{-1}b^\sigma f.$$

A outra condição é que

$$ad + bc = 0,$$

i.e.,

$$xd^{\sigma+1} - x^{-1}b^{\sigma+1}f = 0.$$

Conseqüentemente, como p é um primo ímpar, então $\sigma + 1$ é par; assim, f seria um quadrado, contradizendo a hipótese.

Os números complexos são um caso particular do sistema (5.3), embora f ser um não-quadrado não seja suficiente no caso infinito. O sistema (5.3) é associativo se, e somente se, $\sigma = I$.

5.4 Corpos Deformados.

A seguinte construção é devida a A. A. Albert [1, 2, 4]. Defina um nova multiplicação sobre os elementos de $GF(p^n)$ por

$$x \circ y = xy^q - cx^q y, \tag{5.4}$$

onde $q = p^m,\ 1 \leq m < n$, e $c \neq a^{q-1}$ para $a \in GF(p^n)$. Então obtemos um pré-semicorpo, já que $x^q + y^q = (x+y)^q$, e já que $x \circ y = 0$ implica em $x = 0$ ou $y = 0$ ou $c = (y/x)^{q-1}$. Agora utilize (3.17) para obter um semicorpo. Este semicorpo resultante é chamado *corpo deformado.*

A construção pode ser levada a cabo somente se c existe sujeito as condições requeridas. Este será o caso quando $(q-1, p^n-1) > 1$, i.e., quando $q-1$ e p^n-1 têm um fator comum, já que $x^{p^n-1} = 1$ para todo $x \in GF(p^n) - \{0\}$. De fato, se $(q-1, p^n-1) = 1$ e $x^{p^n-1} = 1$ para todo $x \in GF(p^n) - \{0\}$, então existe um inteiro α com $(x^\alpha)^{q-1} = x$ para todo $x \in GF(p^n)$; ou seja, não podemos ter $c \neq a^{q-1}$ para todo $a \in GF(p^n)$. Mas se p é ímpar, existe sempre o fator comum $p-1$; se $p = 2$ temos $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$, assim necessitamos de $(m,n) > 1$. Se $n = mk$, onde $k > 2$, pode ser mostrado que o semicorpo construído é não-associativo.

Corpos deformados existem para quase todas as ordens não excluídas pelo Teorema 30. As ordens que faltam são 2^4 e 2^p, onde p é um primo maior que 3.

5.5 Construção de Sandler

Uma classe interessante de semicorpos foi construída por R. Sandler [17] em 1962. Existem p^{nm^2} elementos nesses semicorpos, onde m é maior que 1.

Para a construção de Sandler, seja $q = p^n$; os elementos de S são

$$a_0 + \lambda a_1 + \cdots + \lambda^{m-1} a_{m-1},\ a_i \in GF(q^m).$$

A multiplicação é definida como a seguir:

$$(\lambda^i x)(\lambda^j y) = \lambda^{i+j} x^{q^i} y, \quad 0 \leq i < m,\ 0 \leq j < \infty$$
$$\lambda^m = \delta,$$

com a convenção de que λ^k denota as potências à esquerda de λ, i.e., $\lambda^{k+1} = \lambda\lambda^k$. Se δ for escolhido não satisfazendo a nenhum polinômio de grau menor que m sobre $GF(q)$, temos um semicorpo.

Por exemplo, vamos construir um tal sistema F de ordem 2^9. Os elementos são da forma

$$a + \lambda b + \lambda^2 c, \ \text{ onde } \ a, b, c \in GF(8).$$

A multiplicação é definida pela regra

$$(a+\lambda b+\lambda^2 c)(d+\lambda e+\lambda^2 f) = ad+\lambda a^2 e+\lambda^2 a^4 f+\delta b^4 f+\lambda bd \\ +\lambda^2 b^2 e+\delta c^2 e+\lambda\delta c^4 f+\lambda^2 cd.$$

Note a semelhança entre esta e a definição do sistema W da Seção 1.2. A multiplicação definida acima pode ser escrita na forma matricial, já que S é um espaço vetorial sobre $GF(8)$; a matriz da multiplicação à esquerda por $(a+\lambda b+\lambda^2 c)$ é

$$L = \begin{bmatrix} a & \delta c^2 & \delta b^2 \\ b & a^2 & \delta c^4 \\ c & b^2 & a^4 \end{bmatrix}.$$

O determinante de L é

$$a^7+\delta b^7+\delta^2 c^7-\delta(a^2 b^4 c+ab^2 c^4+a^4 bc^2) = r+s\delta+t\delta^2.$$

Já que $r^2=r$, $s^2=s$ e $t^2=t$, então o determinante de L é um polinômio de grau menor ou igual a 2 sobre $GF(2)$. Este determinante não pode ser nulo por hipótese, a menos que todos os coeficientes sejam nulos; mas isto requer que $a=b=c=0$.

5.6 Semicorpos binários de Knuth

Seja $K=GF(2^{mn})$, onde n é ímpar, $n>1$; seja K_0 o subcorpo $GF(2^m)$. Considerando K como um espaço vetorial sobre K_0, seja f um funcional linear qualquer de K sobre K_0, i.e.,

$$f(\lambda a+\mu b) = \lambda f(a)+\mu f(b), \tag{5.5}$$

para todos $a,b\in K$ e todos $\lambda,\ \mu\in K_0$.

Defina uma nova multiplicação em K como a seguir:

$$a\circ b = ab+\left(f(a)b+f(b)a\right)^2. \tag{5.6}$$

Teorema 31. *O sistema algébrico $(K,+,\circ)$ é um pré-semicorpo.*

Demonstração. Como f é um funcional linear e a aplicação $a\to a^2$ é um automorfismo de K, o produto $a\circ b$ é linear em ambas as variáveis e, deste modo, ambas as leis

distributivas se verificam. Portanto, precisamos mostrar apenas que não existem divisores do zero.

Suponhamos que $a \circ b = 0$, com $a,\ b \neq 0$, e faça $x = ab^{-1}$. Isto implica em

$$x + f(a)^2 + f(b)^2 x^2 = 0.$$

Temos uma equação quadrática com coeficientes em K_0; mas como o grau de K/K_0 é ímpar, esta equação precisa ser redutível. Conseqüentemente, $x \in K_0$. Mas então, $a = xb$ implica em

$$a \circ b = ab + [f(xb)b + f(b)xb]^2 = ab \neq 0,$$

e esta contradição completa a demonstração. □

No Capítulo 3 vimos que existem várias maneiras de convertermos o pré-semicorpo $(K, +, \circ)$ em um semicorpo. Uma dessas maneiras é definirmos um novo produto $*$ como na equação (3.17),

$$(1 \circ a) * (1 \circ b) = a \circ b. \tag{5.7}$$

Desta forma $(K, +, *)$ é um semicorpo comutativo, já que $(K, +, \circ)$ é um pré-semicorpo comutativo.

Note que agora definimos três diferentes "multiplicações"sobre os elementos de K : ab, $a \circ b$, e $a * b$. É importante mantermos esta discussão em mente, já que todas as três multiplicações serão utilizadas simultaneamente nas próximas demonstrações desta seção. As potências de um elemento, a^2, a^3, etc., serão sempre referidas a multiplicação do *corpo.*

Teorema 32. *Se $mn > 3$, é possível escolher a função f de (5.5) de tal maneira que o sistema $(K, +, *)$ seja um semicorpo próprio.*

Demonstração. Seja $\{1, x, x^2, \cdots, x^{n-1}\}$ uma base de K sobre K_0; faça

$$f(1) = f(x) = \cdots = f(x^{n-2}) = 0,\ f(x^{n-1}) = 1. \tag{5.8}$$

Com esta definição, para $\lambda \in K_0$,

$$1 \circ \lambda = \lambda,\ 1 \circ \lambda x = \lambda x, \cdots, 1 \circ \lambda x^{n-2} = \lambda x^{n-2},\ 1 \circ \lambda x^{n-1} = \lambda x^{n-1} + \lambda^2;$$

e, portanto, para todos $a,\ b \in K$ temos

$$1 \circ (1 \circ a) = a,\ (a * b) = (1 \circ a) \circ (1 \circ b).$$

Agora se $n > 3$, seja $k = (n-1)/2$; então $1 < k < n-2$, e

$$x * (x^k * x^k) = x * x^{n-1} = x^n + x^2 + x \neq x^n = x^{k+1} * x^k = (x * x^k) * x^k.$$

Conseqüentemente, a multiplicação não é associativa neste caso.

Se $n = 3$, seja λ um elemento de K_0; temos

$$(x * x) * \lambda x = x^2 * \lambda x = (x^2 + 1) \circ \lambda x = \lambda x(x^2 + 1) + \lambda^2 x^2.$$

$$x * (x * \lambda x) = x * \lambda x^2 = x \circ (\lambda x^2 + \lambda^2) = (\lambda x^2 + \lambda^2)x + \lambda^2 x^2.$$

Assim, a multiplicação não é associativa a menos que $\lambda^2 = \lambda$. Mas podemos sempre escolher $\lambda \neq \lambda^2$ já que $K = GF(8)$ está excluído, por hipótese. □

A condição $mn > 3$ será assumida no restante desta seção.

Agora consideraremos o efeito de escolhermos diferentes funções f na equação (5.5).

Lema 1. *Se f e g são funcionais lineares não-nulos de K em K_0 então existe um elemento $z \in K$ tal que $f(az) = g(a)$, para todo a em K.*

Demonstração. Um simples argumento de contagem provará este lema.

Se $\{x_1, x_2, \cdots, x_n\}$ é uma base de K sobre K_0, um funcional linear f é completamente determinado pelas n escolhas de $f(x_i) \in K_0$, $1 \leq i \leq n$, e estas escolhas são independentes com a condição de que estes funcionais são todos não-nulos. Portanto, existem $2^{mn} - 1$ funcionais lineares.

Suponha que f seja um funcional linear não-nulo; então se definirmos $g(a) = f(az)$, para $z \neq 0 \in K$, g é também um funcional linear não-nulo. Como existem $2^{mn}-1$ escolhas para z precisamos mostrar apenas que para duas dessas escolhas temos funções diferentes. Mas se $f(az_1) = f(az_2)$ para todo a, temos $f(a(z_1 - z_2)) = 0$ para todo a, conseqüentemente $z_1 - z_2 = 0$. □

Teorema 33. *Para um dado K e K_0, quaisquer dois semicorpos $(K, +, *)$ determinados por diferentes funcionais f em (5.5) são isotópicos.*

Demonstração. Já que todo semicorpo é isotópico ao seu pré-semicorpo correspondente, necessitamos apenas mostrar que quaisquer dois dos pré-semicorpos são isotópicos. Suponha que

$$a \circ b = ab + [f(a)b + f(b)a]^2 \text{ e}$$

$$a \cdot b = ab + [g(a)b + g(b)a]^2.$$

Aplicando o Lema 1, encontramos $z \in K$ com $f(za) = g(a)$ para todo $a \in K$. Então

$$az \circ bz = abz^2 + [g(a)bz + g(b)az]^2 = (a \cdot b)z^2.$$

□

Corolário 5. *Se $mn > 3$, então todos os sistemas $(K, +, *)$ definidos nesta seção são semicorpos próprios.*

Demonstração. Segue do Teorema 32 e do fato de que nenhum corpo é isotópico a um semicorpo próprio. Além disso, pelo Teorema 12, dois semicorpos coordenatizam o mesmo plano se, e somente se, são isotópicos. Enquanto um corpo coordenatiza um plano desarguesiano, um semicorpo coordenatiza um plano não-desarguesiano. □

O semicorpo binário de K/K_0

Nesta subseção mostraremos que se o funcional f é escolhido apropriadamente então obtermos um semicorpo possuindo pelo menos mn automorfismos. Este semicorpo particular, com f definido pelo Teorema 34, será chamado o semicorpo binário de K/K_0.

Teorema 34. *Seja $q = 2^m$, e seja f tal que $f(a) = \lambda$ sempre que*

$$a = \lambda + b + b^q, \quad \lambda \in K_0, \ b \in K. \tag{5.9}$$

Então f é um funcional linear de K em K_0, e $f(a^2) = f(a)^2$.

Demonstração. Primeiro mostraremos que f está bem definido. Suponha que $\lambda + b + b^q = \mu + c + c^q$ para $\lambda \neq \mu \in K_0$; então $(b+c)^q = (b+c) + \lambda + \mu$, i.e., $a^q = a + z$ para algum $a \in K$, $z \in K_0$. Aplicando a regra anterior, obtemos

$$a^{q^2} = a^q + z^q = a^q + z = a.$$

Como n é ímpar, $a^{q^{n+1}} = a$. Daí, como $a^{q^{n+1}} = a^q$, segue que $z = 0$. Portanto $f(x + b + b^q)$ está bem definido.

Além disso, todo elemento de K pode ser representado na forma $\lambda + b + b^q$, pois existem precisamente q elementos $c \in K$ para os quais $b+b^q = c+c^q$ e $(b+c) = (b+c)^q$ se, e somente se, $b+c \in K_0$. Conseqüentemente f é unicamente definida. Finalmente,

$$\begin{aligned} f(\lambda + b + b^q + \mu + c + c^q) &= f(\lambda + \mu + (b + c) + (b + c)^q) = \lambda + \mu \\ &= f(\lambda + b + b^q) + f(\mu + c + c^q), \end{aligned}$$

$$f(\mu(\lambda + b + b^q)) = f(\mu\lambda + \mu b + (\mu b)^q) = \mu\lambda = \mu f(\lambda + b + b^q),$$

e

$$f((\lambda + b + b^q)^2 = f(x^2 + b^2 + (b^2)^q) = x^2 = f(x + b + b^q)^2.$$

□

Teorema 35. *O semicorpo binário de K/K_0 tem o automorfismo $a \to a^2$; conseqüentemente existem pelo menos mn automorfismos do semicorpo binário.*

Demonstração. Primeiro mostraremos que $a \to a^2$ é um automorfismo do pré-semicorpo.

$$\begin{aligned} (a \circ b)^2 &= (ab + [f(a)b + f(b)a]^2)^2 \\ &= a^2b^2 + [f(a)^2b^2 + f(b)^2a^2]^2 \\ &= a^2b^2 + [f(a^2)b^2 + f(b^2)a^2]^2 = a^2 \circ b^2. \end{aligned}$$

O automorfismo é herdado para o semicorpo, já que

$$\begin{aligned} ((1 \circ a) * (1 \circ b))^2 &= (a \circ b)^2 = a^2 \circ b^2 \\ &= (1 \circ a^2) * (1 \circ b^2) \\ &= (1^2 \circ a^2) * (1^2 \circ b^2) = (1 \circ a)^2 * (1 \circ b)^2. \end{aligned}$$

O restante da demonstração segue por composição de automorfismos. □

Knuth [13] demonstra que os únicos automorfismos do semicorpo $(GF(2^{mn}), +, *)$ são exatamente os mn automorfismos gerados pelo automorfismo $a \to a^2$, e que este semicorpo possui exatamente $mn(2^m - 1)$ autotopismos.

Os semicorpos de Knuth, juntamente com os outros semicorpos vistos neste capítulo, dão exemplos de semicorpos próprios de todas ordens não excluídas pelo Teorema 30.

Referências Bibliográficas

[1] ALBERT, A. A., *On non-associative division algebras,* Trans. Am Math. Soc. **72** (1952), 296-309.

[2] ALBERT, A. A., *Finite non-associative division algebras,* Proc. Am. Math. Soc. **9** (1958), 928-932.

[3] ALBERT, A. A., *On the collineation groups of certain non-Desarguesian planes,* Portugal. Math. **18** (1959), 207-224.

[4] ALBERT, A. A.,*Finite division algebras and finite planes,* Proc. Sym. Appl. Math. **10** (1960), 53-70.

[5] DICKSON, L. E., *Linear algebras in which division is always uniquely possible,* Trans. Am. Math. Soc. **7** (1906), 370-390, 514-527.

[6] DICKSON, L. E., *Linear algebras with associativity not assumed,* Duke Math. J. **1** (1935), 113-125.

[7] HALL, M., J_R., *Theory of Groups,* 2a ed., Chelsea, New York, 1976.

[8] HUGHES, D. R. & KLEINFELD, E., *Semi-nuclear extensions of Galois fields,* Am. J. Math. **82** (1960), 389-392.

[9] HUGHES, D. R., *Colineation groups of non-Desarguesian planes II,* Am. J. Math. **82** (1960), 113-119

[10] HUGHES, D. R. & PIPER, F. C., *Projective Planes,* Springer, New York, 1973.

[11] KLEINFELD, E., *Techniques for enumerating Veblen-Wedderburn system,* J. Assoc. Comp. Mach. **7** (1960), 330-337.

[12] KNUTH, D. E., *Finite Semifields and Projective Planes,* J. Algebra **2** (1965), 182-217.

[13] KNUTH, D. E., *A class of projective planes,* Trans. Amer. Math. Soc. **115** (1965), 541-549.

[14] MAZUROV, V. D. & KHUKHRO, E. I., *The Kourovka Notebook - Unsolved Problems in Group Theory*, Institute of Mathematics, SO RAN - Novosibirski - Russia, 1992.

[15] PEDOE, D., *An Introduction to Projective Geometry,* Macmillan, New York, 1963.

[16] ROCCO, N. R., *Relações entre Comutadores e Certos Produtos Regulares de Grupos,* Encontro de Álgebra - IME/USP, MT - MAT **93-15**, 1993, 36-41.

[17] SANDLER, R., *Autotopism groups of some finite non-associative algebras,* Am. J. Math. **84** (1962), 239-264.

[18] WALKER, R. J., *Determination of division algebras with 32 elements,* Proc. Symp. Appl. Math. AMS **15** (1962), 83-85.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo