Grupos cíclicos de Jacobi

por Aron Simis (1)

I. Num trabalho recente [1], B. M. Puttaswamaiah afirmou que um grupo tem quando muito um endomorfismo não nulo de Jacobi.

Isto não é, contudo, verdade, como foi demonstrado por J. Morgado [2], estabelecendo que um grupo tem, quando muito, um automorfismo de Jacobi e mostrando ainda que um grupo G tem um endomorfismo não nulo de Jacobi se e sòmente se G é o produto semi-directo de um subgrupo normal próprio por um subgrupo abeliano com a propriedade da raiz quadrada única ([2], Th. 4).

Num seminário originado dos trabalhos acima, realizado no Instituto de Matemática do Recife (Abril, 1967), foi posta a questão de se determinar todos os grupos cíclicos que têm algum endomorfismo não nulo de Jacobi e apontar todos os endomorfismos de Jacobi dêsses grupos.

Nosso objectivo, neste trabalho, é resolver essa questão.

II. Lembramos que um *endomorfismo de Jacobi* de um grupo G é um endomorfismo σ de G tal que:

$$((ab)^\sigma c)^\sigma ((bc)^\sigma a)^\sigma ((ca)^\sigma b)^\sigma = 1, \forall\, a, b, c \in G.$$

É imediato que o endomorfismo nulo θ, definido por

$$a^\theta = 1, \forall\, a \in G,$$

é um endomorfismo de Jacobi.

Um grupo diz-se *de Jacobi* se admite pelo menos um endomorfismo não nulo de Jacobi.

Verifica-se, fàcilmente, que o grupo aditivo dos inteiros Z não é um grupo de Jacobi.

Com efeito, os únicos subgrupos de Z são $nZ = \{nx, x \in Z\}$, com n natural, os quais não possuem a propriedade seguinte:

$$\forall\, nx, \exists\, ny : ny + ny = nx$$

(esta é a «propriedade da raiz quadrada» traduzida em termos de uma operação aditiva).

Anàlogamente, o grupo cíclico $Z(2^n)$ dos inteiros mod 2^n não possui a propriedade da raiz quadrada, uma vez que qualquer de seus subgrupos não reduzido à identidade tem ordem igual a uma potência de 2 [3].

Teorema 1. *Os únicos grupos cíclicos de Jacobi são os grupos isomorfos a* $Z(2^n(2m+1))$, m *e* n *inteiros,* $n \geq 0$, $m \geq 1$.

Demonstração. Seja $2m+1 = p_1^{e_1} \cdots p_s^{e_s}$ a decomposição canónica de $2m+1$ em factores primos; então $p_i \neq 2$, $i = 1, \cdots, s$.

Tem-se ([4], pg. 148, por exemplo)

$$\begin{aligned} Z(2^n(2m+1)) &= Z(2^n) \oplus Z(p_1^{e_1}) \oplus \cdots \oplus Z(p_s^{e_s}) \\ &= (Z(2^n) \oplus Z(p_1^{e_1}) \oplus \cdots \oplus \\ &\quad \oplus Z(p_{s-1}^{e_{s-1}})) \oplus Z(p_s^{e_s}), \end{aligned}$$

onde $\oplus$ indica soma directa.

O subgrupo $Z(p_s^{e_s})$ possui a propriedade da raiz quadrada única, por ser de ordem

(1) Estudante do Mestrado em Matemática do Instituto de Matemática da Universidade Federal de Pernambuco.

ímpar ([2], Corollary to Th. 3). Por outro lado, o subgrupo $Z(2^n) \oplus Z(p_1^{e_1}) \oplus \cdots \oplus \oplus Z(p_{s-1}^{e_{s-1}})$ é próprio e normal; segue-se ([2], Th. 4) que $Z(2^n(2m+1))$ é um grupo de JACOBI.

A seguir veremos uma maneira de construir, efectivamente, todos os endomorfismos de JACOBI de $Z(2^n(2m+1))$.

Como $Z(2^n(2m+1))$ é cíclico, qualquer de seus endomorfismos é da forma

$$\sigma : x \to rx, r \in Z .$$

Por outro lado, σ é um endoformismo de JACOBI de $Z(2^n(2m+1))$, se e sòmente se $(2r^2 + r)x = 0$, $x \in Z(2^n(2m+1))$ ([2], Lemma 2). Portanto, encontrar todos os endomorfismos de JACOBI de $Z(2^n(2m+1))$ significa encontrar as soluções da congruência

$$(1) \quad 2r^2 + r \equiv 0 \mod 2^n(2m+1),$$

ou, equivalentemente, as soluções inteiras r da equação

$$(2) \quad r = \frac{-1 \pm \sqrt{1 + 2^{3+n}(2m+1)k}}{4},$$

para k inteiro positivo.

É imediato que $1 + 2^{3+n}(2m+1)k \geq 25$, para $n \geq 0, m \geq 1, k > 0$; portanto, se $1 + 2^{3+n}(2m+1)k$ admite uma raiz quadrada inteira, então (2) tem uma e uma só solução inteira. Trata-se, por conseguinte, de resolver a congruência

$$(3) \quad u^2 \equiv 1 \mod 2^{3+n}(2m+1),$$

a qual tem solução, se e sòmente se são solúveis as congruências

$$(4) \quad u^2 \equiv 1 \mod 2^{3+n}$$

e

$$(5) \quad u^2 \equiv 1 \mod p_i^{e_i}, i = 1, \cdots, s,$$

onde $2m + 1 = p_1^{e_1} \cdots p_s^{e_s}$ é a decomposição canónica de $2m + 1$.

Não é difícil ver que as soluções de (4) são $1, 2^{3+n} - 1, 2^{2+n} + 1$ e $2^{2+n} - 1$ e as de (5), 1 e $p_i^{e_i} - 1$ (entendendo-se por todas as soluções aquelas contidas num conjunto completo de resíduos). As soluções de (3) são obtidas a partir dessas por meio de combinações determinadas (v. [5], por exemplo).

Adiante veremos que o número de endomorfismos de JACOBI do grupo $Z(2^n(2m+1))$ é precisamente 2^s. Para o momento, verificaremos que tal número é $\geq 2^s$. Neste sentido, tem-se o seguinte

LEMA. *Os únicos subgrupos de* $Z(2^n(2m+1))$ *que são imagens de algum endomorfismo não nulo de* JACOBI *são os* p_i*-subgrupos de Sylow e somas directas destes subgrupos, onde* $2m + 1 = p_1^{e_1} \cdots p_s^{e_s}$ *é a decomposição canónica de* $2m + 1$.

DEMONSTRAÇÃO. É imediato que os p_i-subgrupos de SYLOW e somas directas arbitrárias dos mesmos são imagens de algum endomorfismo não nulo de JACOBI [2]; isto é o que, em essência, mostrou-se no Teorema I.

Suponhamos que existe um primo p que divide $2m + 1$ tal que existe algum p-subgrupo não de SYLOW que é imagem de algum endomorfismo de JACOBI; ter-se-ia, então

$$Z(2^n(2m+1)) = Z(p^{e-j}) \oplus (Z(p^j) \oplus G), \quad 0 < j < e,$$
$$= (Z(p^{e-j}) \oplus Z(p^j)) \oplus G,$$

onde G é um subgrupo de ordem

$$2^n(2m+1)/p^e .$$

Como só existe um subgrupo de ordem p^e, resulta

$$Z(p^e) = Z(p^{e-j}) \oplus Z(p^j),$$

o que constitui um absurdo, uma vez que os únicos subgrupos de $Z(p^e)$ são

$$Z(p^e) \supseteq Z(p^{e-1}) \supseteq \cdots \supseteq Z(p) \supseteq \{0\}.$$

COROLÁRIO. *O número de endomorfismos de* JACOBI *de* $Z(2^n(2m+1))$ *é* $\geq 2^s$.

TEOREMA 2. *O número de endomorfismos de* JACOBI *de* $Z(2^n(2m+1))$ *é precisamente* 2^s, *onde* s *é o número de factores primos de* $2m+1$.

DEMONSTRAÇÃO. Vimos acima que o número de endomorfismos de JACOBI de $Z(2^n(2m+1))$ é $\geq 2^s$. É suficiente mostrar agora que não se pode ter

$$Z(2^n(2m+1))^\sigma = Z(2^n(2m+1))^\tau,$$

com $\sigma \neq \tau, \sigma$ e τ endomorfismos de JACOBI de $Z(2^n(2m+1))$.

Ponhamos $G = Z(2^n(2m+1))$. Tem-se então ([2], Th 4):

$$\begin{aligned} G &= N_\sigma \oplus G, \quad N_\sigma = \ker \sigma \\ &= N_\tau \oplus G, \quad N_\tau = \ker \tau. \end{aligned}$$

Como G é cíclico finito e $G^\sigma = G^\tau$, resulta $N_\sigma = N_\tau$.

Seja $x \in G$; então tem-se ([2], Th 4):

$$\begin{aligned} x &= x_\sigma - 2rx, \quad x_\sigma \in N_\tau, \quad 2rx \in G^\sigma \\ &= x_\tau - 2sx, \quad x_\tau \in N_\tau, \quad 2sx \quad G^\tau, \end{aligned}$$

onde $\sigma : x \to rx$ e $\tau : x \to sx$. Das considerações acima resulta $rx = sx, \forall x \in G$; logo, $\sigma = \tau$.

III. Resumindo, obtivemos que os únicos grupos cíclicos de JACOBI são os isomorfos a $Z(2^n(2m+1)), m \geq 1, n \geq 0$; além disso, se s é o número de primos distintos que dividem $2m+1$, então $Z(2^n(2m+1))$ admite 2^s endomorfismos de JACOBI.

Observemos que o grupo $Z(p_i^{e_i}), p_i$ ímpar, possui exactamente um endomorfismo não nulo de JACOBI (que é um automorfismo). Com efeito, $Z(p_i^{e_i})$ tem um e um só *automorfismo* de JACOBI ([2], Corol. to Th 3). Suponhamos que σ fosse outro endomorfismo não nulo de JACOBI; então, como σ não é um automorfismo, resulta que é sua imagem um factor directo próprio. Mas, isto é absurdo, uma vez que $Z(p_i^{e_i})$ é indecomponível.

Como consequência obtemos uma maneira simples de escrever todos os endomorfismos de $Z(2^n(2m+1))$ a partir do endomorfismo não nulo de $Z(p_i^{e_i}), i = 1, \cdots, s$ e do endomorfismo nulo. Com efeito, a aplicação

$$\sigma : (x_0, x_1, \cdots, x_s) \to (0, x_1^{\sigma_1}, \cdots, x_s^{\sigma_s}),$$

onde σ_i ou é o automorfismo de JACOBI de $Z(p_i^{e_i})$ ou o endomorfismo nulo, é evidentemente um endomorfismo de JACOBI de $Z(2^n(2m+1))$. Obtemos, por este processo, 2^s endomorfismos de JACOBI distintos de $Z(2^n(2m+1))$. Pelo Teorema 2, estes são realmente todos os endomorfismos de JACOBI de $Z(2^n(2m+1))$.

Convém, talvez, observar que o processo de construir um endomorfismo de JACOBI para o grupo todo a partir de endomorfismos de JACOBI dos factores directos é válido para um grupo decomponível qualquer. Recìprocamente, dado um endomorfismo de JACOBI σ de um grupo decomponível, poderíamos pensar em verificar se ele induz um endomorfismo de JACOBI em cada factor directo. A resposta é afirmativa para os grupos cíclicos (o endomorfismo induzido podendo ser o endomorfismo nulo), uma vez que nesse caso tem-se $\sigma(H) \subseteq H$, onde H é um factor qualquer. Se a restricção $\bar{\sigma}$ de σ ao factor

directo H comuta com a projecção ε sobre H, então $\bar{\sigma}$ é um endomorfismo de JACOBI de H.

BIBLIOGRAFIA

[1] B. M. PUTTASWAMAIAH, *Jacobi Endomorphisms*, Amer. Math. Monthly, **73** (1966), pp. 741-4.

[2] J. MORGADO, *Note on Jacobi Endomorphisms*, a ser ser publicado.

[3] E. A. FAY, *Solution of the Problem E 1974, 1965, 545*, Amer. Math. Monthly, **73** (1966), p. 892.

[4] N. JACOBSON, *Lectures in Abstract Algebra*, Vol. I, D. Van Nostrand, N. Y., 1951.

[5] NIVEN and ZUCKERMAN, *An Introduction to the Theory of Numbers*, p. 38.

Nota a «Um novo método numérico de extração da raiz quadrada»

por Ruy Madsen Barbosa

Preliminares

Apresentamos no artigo acima, publicado *In* «Gazeta de Matemática», 98-99/1965, um algoritmo e seu ensino, baseado em propriedades das sucessões de ímpares e de pares.

O propósito desta Nota é apresentar uma modificação do algoritmo, utilizando sòmente a sucessão de ímpares: soma e ímpar sucessivo; e, ao final, provar que desta forma se chega ao algoritmo tradicional.

Modificações

Sejam Z ímpares no primeiro intervalo.

No segundo intervalo separemos a sucessão de ímpares da seguinte maneira:

$$2Z+1,\quad 2Z+3,\quad 2Z+5,\cdots$$

de onde teremos, no segundo intervalo, além das quantidades fixas $2Z$, uma nova sucessão de ímpares, também iniciando com a unidade.

Dividamos a diferença D (do segundo intervalo) por $2Z$, obtendo-se um número q possível de ímpares do intervalo, cuja soma é q^2.

Desde que $D = 2Z \cdot q + r$, o resto r deverá ser maior ou igual a q^2.

Satisfazendo essa condição, a raiz quadrada será $Z+q$ e o resto $R = r - q$.

Em caso contrário, diminue-se o valor de q.

EXEMPLO:

$\sqrt{3351}$

	1	3	
50 ímpares	100	100...	
2500	←	$D = 851$	→ 3351

851 : 100 é $q = 8$ e sobra $r = 51$; mas $q^2 = 64 > 51$; reduzimos q para 7 e sobra $r = 151$, e, o resto será $R = 151 - 49 = 102$.

Conclusão: $\sqrt{3351} = 50 + 7 = 57$.

Algoritmo Modificado

$\sqrt{3351}$	50	
2500	$\times$ 2	
851	$100\times 8=800$	$100\times 7=700$
800	Teste: $8^2=64$	Teste: $7^2=49$
51	(não serve)	Raiz $=50+7=57$
100+		
151		
49−		
R = 102		

Prova da identificação dos algoritmos

Da exposição resulta que para a extração da raiz quadrada de um número N, subtrae-se de N o quadrado de Z, procura-se um número q tal que seja o quociente de N pelo *dôbro de* Z, e ainda faz-se o teste da nova sucessão de ímpares, cuja soma é q^2, isto é, q é tal que $2Z\cdot q+q^2$ é o maior número inferior ao resto $N-Z^2$, que é justamente o que se faz no algoritmo tradicional: $(2Z+q)\,q$.

O que se fêz foi simplesmente separar o cálculo q^2 do teste para uma melhor aprendizagem.

EXEMPLO:

$\sqrt{3331}$	50		
2500	$\times$ 2		
851	100	100	Raiz $=50+7=57$
749	8+	7+	
102	108	107	
	$\times$ 8	$\times$ 7	
	864	749	

Ordered semigroups which contain zeroid elements

by **C. W. Leininger**

In [1] CLIFFORD and MILLER show that if a semigroup S has a zeroid element, then then its kernel is the subgroup K of zeroids of S. Furthermore K determines a partition G of S in a certain way. The purpose of this paper is to consider such a semigroup under the suppositions that K is a nondegenerate subset of S and there is a comparable pair of elements of S not both in the same set of G. We find that K inclndes a subchain Q of S which is o-isomorphic to the additive group of integers. Some aspects of the structure of ordered semigroups with zeroids elements are then investigated.

1. Introduction.

If z denotes the identity element of K, then the subsemigroug J such that

$$J=\{x : x\in S,\ xz=zx=z\}$$

is called the core of S and the set $J\cup K$ is called the frame of S. For convenience we summarize from [1, p. 121] the following properties pertaining to the gross structure of S: