UMA NOTA SOBRE A ESTRUTURA DO GRUPO MULTIPLICATIVO DE UM CORPO

Norai Romeu Rocco

1. Introdução

É notável em Matemática, especialmente no estudo de estruturas algébricas, como o número de elementos de um conjunto restringe qualitativamente a estrutura que desejamos considerar sobre aquele conjunto. É assim por exemplo quando verificamos logo num primeiro curso de Álgebra da graduação que *o anel dos inteiros módulo n é um corpo se e somente se n é um número primo* [4, pág. 183]. Indo além, observamos que restrições consideráveis em geral ocorrem numa estrutura quando simplesmente exigimos a finitude do conjunto a ela subjacente. Para citar apenas dois exemplos dessa natureza, temos um conhecido teorema elementar assegurando que *todo domínio de integridade finito é um corpo* [4, pág. 183], ou então o célebre teorema de Wedderburn(1) afirmando que *todo anel de divisão*(2) *finito é necessariamente um corpo* [2, cap. 7]. A finitude em ambos os exemplos é condição essencial visto que, no primeiro caso, o anel dos inteiros constitui um domínio de integridade, enquanto que os quaternios reais, com adição e multiplicação de quaternios, formam um anel de divisão cuja multiplicação não é comutativa [5, pág. 44].

Vale observar que os resultados acima fazem implicações somente à parte multiplicativa das estruturas em apreço e daqui por diante vamos restringir nossas considerações à parte multiplicativa de um *corpo* K ou seja, ao grupo abeliano (ou comutativo) K^*, consis

(1) Jospeh Henry Maclagan Wedderburn (1882-1948) nasceu em Forfar, na Escócia. Deixou importantes contribuições na área de Álgebra. Em [2, cap. 7] são apresentados 2 demonstrações desse seu Teorema.

(2) Entendemos por Anel de Divisão (ou corpo não comutativo) uma estrutura cujas operações (adição e multiplicação) satisfazem as mesmas condições de um corpo, com exceção da comutatividade da multiplicação.

tindo dos elementos não nulos de K munidos da operação de multiplicação do corpo.

Uma vez mais invocando a finitude obtemos o importante resultado: *Se K é um corpo com apenas um número finito de elementos, então K^* é um grupo cíclico* [2, pág. 382].

Dizer que um grupo é cíclico é dizer que todos os seus elementos podem ser descritos como potências inteiras de um de seus membros, chamado o *gerador* do grupo; o grupo será então finito ou infinito conforme ocorram ou não repetições entre duas potências do gerador com expoentes distintos. Um fato fundamental que ocorre nesses grupos é que todo subgrupo é também cíclico; se o grupo é infinito, todo subgrupo não trivial é também infinito. Neste ponto abrimos um parenteses para citar a seguinte caracterização de grupos cíclicos finitos: *Se um grupo abeliano finito A, com identidade e, é tal que a equação $x^n = e$ tem no máximo n soluções em A para todo inteiro positivo n, então A é um grupo cíclico.* Esta caracterização, da qual segue imediatamente o resultado acima, tem uma demonstração bastante elementar baseada apenas em rudimentos da aritmética dos inteiros, [cf. 3, pág. 69].

2. Uma questão surge naturalmente

Pelo que temos observado anteriormente é natural perguntarmos se grupos cíclicos podem aparecer como grupos multiplicativos em corpos infinitos. Em outras palavras, podemos colocar a seguinte questão:

(P) Pode um grupo cíclico infinito ser o grupo multiplicativo de um corpo?

A motivação do autor em escrever este artigo deve-se ao fato de a pergunta acima (ou uma generalização da mesma, cf. 4 adiante) ter surgido naturalmente quando da investigação de certos grupos duplamente transitivos.

A resposta é *não* e existem várias maneiras de se verificar isto, muito embora este fato não apareça explícitamente na literatura.

O propósito desta nota é demonstrar essa negação de maneira bastante elementar, de modo a torná-la apreciável ao leitor que tem visto apenas as primeiras noções de estruturas algébricas. Fazemos isto no próximo parágrafo.

No parágrafo 4, usando já alguns conceitos da teoria dos corpos, generalizamos essa situação provando que os grupos abelianos finitamente gerados só aparecem como grupos multiplicativos em corpos finitos.

No parágrafo 5, deixamos ao leitor interessado um exercício com intuito de reforçar o método utilizado no parágrafo 3.

3. Um Lema e a resposta de (P)

Numa primeira tentativa de responder a pergunta (P) é natural observarmos o grupo multiplicativo de certos corpos conhecidos. O primeiro corpo infinito que nos vem em mente é sem dúvida o corpo Q, dos números racionais, do qual podemos destacar o conjunto binário $\{1,-1\}$ e imediatamente verificar que este subconjunto constitui um subgrupo de Q^*. Ora, já observamos anteriormente que um grupo cíclico infinito não contém subgrupos finitos não triviais. Assim, o corpo Q fica descartado de nossa análise.

De modo geral, denotando por 1 a identidade multiplicativa de um corpo genérico K, vemos que o subconjunto $\{1,-1\}$ constituirá um subgrupo de K^* e pelas mesmas razões acima só poderá ser o subgrupo trivial, ou seja, $1 = -1$ em K. Um corpo no qual esta última igualdade é válida, i.e., onde $1+1 = 0$, é dito ter *característica* 2; num tal corpo vale também a igualdade $a+a = 0$ para todo elemento a.

Portanto, para responder (negativamente) a (P) precisamos verificar a não existência de um corpo (infinito), de característica 2, cujo grupo multiplicativo seja cíclico.

Por absurdo, suponhamos a existência de um tal corpo K e seja x um gerador de K^*, de modo que K^* consiste das potências x^m onde m percorre o conjunto $\mathbb{Z}$ dos números inteiros, $x^m = x^n$ se e somente se $m = n$, e $x^0 = 1$ (continuamos denotando por 1 tanto o elemento identidade de K^* como o menor inteiro positivo). Desde que $1+x^i = 0$ se e somente se $i = 0$ e como todo elemento não nulo de K^* é uma potência de x, obtemos, para todo $i \in \mathbb{Z}-\{0\}$:

$$1+x^i = x^{\alpha(i)} \quad ; \quad (1+x^{-i})^{-1} = x^{\beta(i)} \tag{1}$$

onde $\alpha(i)$ e $\beta(i)$ são inteiros *não-nulos*, bem determinados por i (dado a unicidade de representação dos elementos de K^*). Em outras palavras, as expressões em (1) definem funções α e β em $\mathbb{Z}-\{0\}$.

Lema. As funções α e β acima definidas satisfazem as seguintes condições, para todo $i \in \mathbb{Z}-\{0\}$:

I) $\alpha(i) + \beta(i) = i$;

II) $\alpha(\alpha(i)) = i = \beta(\beta(i))$;

III) $\alpha(2i) = 2\alpha(i)$, $\beta(2i) = 2\beta(i)$.

Vamos propor a demonstração do Lema para concluir nossa argumentação. Ora, se a existência de K nos leva à existência das funções acima, a negação de (P) estará provada se pudermos verificar que semelhantes funções α e β não podem ser definidas em $\mathbb{Z}-\{0\}$. De fato, as três condições do Lema são contraditórias. Com efeito, por I) temos $\alpha(1)+\beta(1) = 1$, de modo que os inteiros $\alpha(1)$ e $\beta(1)$ têm paridades distintas. Por simetria podemos supor que $\alpha(1)$ seja par, digamos $\alpha(1) = 2r$. Agora, usando II) e III) obtemos:

$1 = \alpha(\alpha(1)) = \alpha(2r) = 2\alpha(r)$, isto é, 1 é par. Absurdo.

Demonstração do Lema:

I) Das definições de α e β temos:

$$x^{\alpha(i)+\beta(i)} = x^{\alpha(i)} \cdot x^{\beta(i)} = (1+x^{i})(1+x^{-i})^{-1} =$$

$$= \frac{1+x^{i}}{1+x^{-i}} = \frac{x^{i}(1+x^{-i})}{1+x^{-i}} = x^{i}.$$

Logo $\alpha(i)+\beta(i) = i$, desde que K^{*} é infinito por hipótese.

II) Como $1+1 = 0$ em K, usando a definição de α duas vezes podemos escrever:

$$x^{i} = 1+1+x^{i} = 1+x^{\alpha(i)} = x^{\alpha(\alpha(i))}$$

e novamente pela unicidade de representação dos elementos de K^{*}, temos $\alpha(\alpha(i)) = i$. Para β, como $1+x^{-i} = x^{-\beta(i)}$ segue que $x^{-i} = 1+x^{-\beta(i)}$. Invertendo e usando a definição de β vem:

$$x^{i} = (1+x^{-\beta(i)})^{-1} = x^{\beta(\beta(i))}, \quad \text{o que dá} \quad \beta(\beta(i)) = i.$$

III) Uma vez mais usando que K tem caracterização 2, vemos que $(a+b)^{2} = a^{2}+b^{2}$ para todo $a, b \in K$. Logo,

$$x^{2\alpha(i)} = (x^{\alpha(i)})^{2} = (1 + x^{i})^{2} = 1 + x^{2i} = x^{\alpha(2i)},$$

ou, $\alpha(2i) = 2i$. Para β o procedimento é análogo e assim fica demonstrado o lema.

4. Cíclico ou Finitamente Gerado

Como vimos nos parágrafos anteriores, a ciclicidade do grupo multiplicativo caracteriza os corpos finitos. Mas, o que há de tão especial nos grupos cíclicos para garantir-lhes esta propriedade?

A resposta a esta pergunta já apareceu anteriormente: - "todo subgrupo é do mesmo tipo". Ora, esta não é uma particularidade só dos grupos cíclicos, uma vez que *todos os subgrupos de um grupo abeliano finitamente gerado*(3) *gozam dessa "hereditariedade"*. Sendo assim, é natural esperarmos a finitude de um corpo sempre que seu grupo multiplicativo por finitamente gerado.

Proposição: *Se K é um corpo tal que K^* é finitamente gerado, então K é finito.*

Demonstração: Suponhamos K^* gerado por n elementos $x_1,\ldots,x_n$. Vemos então de imediato que K é uma extensão finitamente gerada do seu corpo primo P: $K = P(x_1,\ldots,x_n)$. Desde que P^* é um subgrupo de K^*, segue-se que P^* é também finitamente gerado e com isto vamos concluir que P não pode ser o corpo dos racionais Q. Com efeito, consideremos qualquer subconjunto finito $\left\{\frac{r_1}{s_1},\ldots,\frac{r_m}{s_m}\right\} \subset Q^*$. Como um inteiro qualquer tem apenas um número finito de fatores primos, o conjunto S, constituído pelos primos que aparecem nas decomposições dos r_i's e s_i's, $i=1,\ldots,m$, é finito, digamos $S = \{p_1,\ldots,p_t\}$. Seja q um primo divisor de $1+p_1\ldots p_t$. Claramente $q \notin S$ e assim *não* pode ser escrito na forma

$$q = \left(\frac{r_1}{s_1}\right)^{\alpha_1} \ldots \left(\frac{r_m}{s_m}\right)^{\alpha_n},$$

ou seja, Q^* não é finitamente gerado como grupo abeliano. Isto mostra que o corpo primo P só pode ser da forma $\mathbb{Z}_p$ para algum primo p, i.e., $K = \mathbb{Z}_p(x_1,\ldots,x_n)$. Como o corpo K pode ser atingido através da *torre* de corpos:

---

(1) Um grupo abeliano (multiplicativo) A é "finitamente gerado" se existem um número natural n e elementos $x_1,\ldots,x_n$ em A tal que todo elemento x em A é da forma $x = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ com $\alpha_i \in \mathbb{Z}$, $i=1,\ldots,n$. Neste caso dizemos que $x_1,\ldots,x_n$ geram A.

$$\mathbb{Z}_p \subset \mathbb{Z}_p(x_1) \subset \mathbb{Z}_p(x_1,x_2) \subset \ldots \subset \mathbb{Z}_p(x_1,\ldots,x_n) = K$$

cada um sendo uma extensão simples do precedente, teremos concluído nosso argumento se soubermos que cada x_i é algébrico sobre $\mathbb{Z}_p$, para $i=1,\ldots,n$, pois nesse caso teremos o *grau* $[K:\mathbb{Z}_p]$ finito e consequentemente K será finito. Vamos então mostrar que nenhum dos geradores $x_1,\ldots,x_n$ pode ser transcendente sobre $\mathbb{Z}_p$. Ora, se um deles, x_1 digamos, fosse transcendente, teríamos o subcorpo $\mathbb{Z}_p(x_1)$ isomorfo ao corpo das frações racionais com coeficientes em $\mathbb{Z}_p$, qual seja, todo elemento de $\mathbb{Z}_p(x_1)$ pode ser identificado com uma fração $\frac{f(t)}{g(t)}$ onde $f(t)$, $g(t)$ são polinômios em t com coeficientes em $\mathbb{Z}$ e $g(t) \neq 0$. Mas sendo $\mathbb{Z}_p(x_1)^*$ um subgrupo de K^*, deve ser finitamente gerado como tal, o que *não* acontece, fato este cuja demonstração segue de maneira análoga àquela utilizada para $\mathbb{Q}^*$ acima, bastando para tanto trocar inteiro (primo) respectivamente por polinômio (irredutível). Vamos omitir os detalhes. Portanto, a proposição segue.

5. Exercício

Usando o método utilizado no parágrafo 2, mostrar que um produto direto de 2 grupos cíclicos infinitos *não* pode ser o grupo multiplicativo de um corpo. (Sugestão: definir funções $\alpha,\beta: \mathbb{Z}\times\mathbb{Z} - \{(0,0)\} \to \mathbb{Z}\times\mathbb{Z} - \{(0,0)\}$ que satisfaçam condições análogas às do Lema anterior. Note que as funções α e β definidas anteriormente satisfazem também as seguintes propriedades adicionais:

a) $\alpha(-i) = -\beta(i)$; $\beta(-i) = -\alpha(i)$, $\forall\, i \in \mathbb{Z}-\{0\}$;

b) $\alpha(i)+\alpha(\beta(i)) = 0 = \beta(i) + \beta(\alpha(i))$, $\forall\, i \in \mathbb{Z}-\{0\}$;

c) Se $i,j \in \mathbb{Z}-\{0\}$ são tais que $i+j \neq 0$, então $\alpha(i) + \beta(j) \neq 0 \neq \alpha(j) + \beta(i)$ e valem:

$$\alpha(i+j) = \alpha(i)+\alpha[\beta(i)+\alpha(j)] = \alpha(j)+\alpha[\beta(j)+\alpha(i)],$$

$$\beta(i+j) = \beta(i) + \beta[\alpha(i)+\beta(j)] = \beta(j) + \beta[\beta(i) + \alpha(j)].$$

Referências Bibliográficas

1. A. Gonçalves, *Introdução à Álgebra*, Projeto Euclides - IMPA (1979).

2. I.N. Herstein, *Tópicos de Álgebra*, Edusp/Ed. Polígono (1970).

3. B.W. Jones, *An Introduction to Modern Algebra*, Macmillan (1975).

4. L.H. Jacy Monteiro, *Elementos de Álgebra*, Ao livro Técnico S.A. (1969).

5. B.L. Van der Waerden, *Modern Algebra*, vol. I, Frederick Ungar (1948).

Departamento de Matemática
Universidade de Brasília
70.910 Brasília, D.F.