**Comparando o número de aneis finitos de ordem $n$ com o número de grupos finitos de ordem $n$.**

**Thiago Dias - UFRPE**

Folheando artigos da revista *Mathematical Monthly* me deparo com o excelente artigo escrito pelo professor Desmond Machele [5] cujo título traz a seguinte questão: "Há mais anéis finitos do que grupos finitos?". A pergunta é bastante interessante e a resposta também. Inspirados fortemente no artigo do Machale, fazemos um breve passeio pelo que se sabe sobre o número de grupos finitos e sobre o número de anéis finitos.

**Exercício 1.** *Quantas classes de isomorfismos de aneis de ordem p , não necessariamente com unidade, existem?*

**Teorema 1.** *Todo anel finito (não necessariamente com unidade) é soma direta de aneis de ordem p.*

*Demonstração.* Uma vez que $R$ é finito, suponha que $|R| = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_n^{s_n}$, a fatoração em primos de $|R|$.

Para cada $i = 1, 2, \ldots, n$, defina $R_i = \{r \in R \mid p^{s_i} r = 0 \text{ para algum } s \in \mathbb{N}^+\}$.

**Exercício 2.** *Verifique que $R_i$ é um ideal em $R$ e que $R_i \cap (R_1 \cap \ldots \cap R_{i-1} \cap R_{i+1} \cap \ldots \cap R_n) = \emptyset$.*

Considere o grupo aditivo finito abeliano $(R, +)$, pelo Teorema Fundamental dos Grupos Abeliano Finitamente Gerados, temos $(R, +) \cong (\mathbb{Z}_{p_1^{s_1}}, +) \oplus (\mathbb{Z}_{p_2^{s_2}}, +) \oplus \ldots \oplus (\mathbb{Z}_{p_n^{s_n}}, +)$. Isso implica em

1. Para todo $r \in R$, $r = r_1 + r_2 + \ldots + r_n$, onde a ordem aditiva de $r_i$ é uma potência de $p_i$. Então, $R = R_1 + R_2 + \ldots + R_n$.

2. Existem exatamente $p_i^{s_i}$ elementos em $R$ cuja ordem aditiva é uma potência de $p_i$. Logo, $|R_i| = p_i^{s_i}$.

Portanto, $R \cong R_1 \oplus R_2 \oplus \ldots \oplus R_n$

□

Se $R$ é um anel finito, então seu grupo aditivo é um grupo abeliano finito e, portanto, é um produto direto de grupos cíclicos. Suponha que esses tenham geradores $g_1, \ldots, g_k$ de ordens $m_1, \ldots, m_k$. A estrutura do anel é então determinada pelos $k^2$ produtos

$$g_i g_j = \sum_{t=1}^{k} c_{ij}^{(t)} g_t, \quad \text{com } c_{ij}^{(t)} \in \mathbb{Z}_{m_t} \quad (1)$$

e, assim, pelos $k^3$ coeficientes de estrutura $c_{ij}^{(t)}$. Introduzimos uma notação conveniente, motivada pela teoria dos grupos, para descrever a estrutura de um anel finito. Uma apresentação para um anel finito $R$ consiste em um conjunto de geradores $g_1, \ldots, g_k$ do grupo aditivo de $R$ juntamente com relações. As relações são de dois tipos:

(i) $m_i g_i = 0$ para $i = 1, \ldots, k$, indicando a ordem aditiva de $g_i$, e

(ii) $g_i g_j = \sum_{t=1}^{k} c_{ij}^{(t)} g_t$ com $c_{ij}^{(t)} \in \mathbb{Z}_{m_t}$ para $i = 1, \ldots, k$, $j = 1, \ldots, k$, $t = 1, \ldots, k$.

Se o anel $R$ possui a apresentação acima, escrevemos

$$R\langle g_1, \ldots, g_k; m_i g_i = 0 \text{ para } i = 1, \ldots, k, g_i g_j = \sum_{t=1}^{k} c_{ij}^{(t)} g_t \rangle.$$

Por exemplo, o anel $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = (a, b; 2a = 2b = 0, a^2 = a, b^2 = b, ab = ba = 0)$, enquanto o corpo finito de ordem 4 é $(a, b; 2a = 2b = 0, a^2 = a, ab = b, b^2 = a + b)$.

Note que se o grupo aditivo é cíclico com gerador $g$, a estrutura do anel é completamente determinada por $g^2$. Portanto, o anel $\mathbb{Z}_4 = (a; 4a = 0, a^2 = a)$.

**Exercício 3.** *Dado um número primo $p$ em um polinômio mônico $q(x) \in \mathbb{F}_p[x]$ de grau $n$ e irredutível. Seja $A$ a matriz companheira de $q(x)$.*

*Mostre que $F = \{r(A) \mid r \in \mathbb{F}_p[x]\}$ é um corpo finito. .*

**Teorema 2.** *Existem 11 classes de isomorfismos de aneis (que não necessariamente possuem unidade) de ordem $p^2$. Mais precisamente, os 11 anéis são dados por*

1. $A = \langle a; p^2 a = 0, a^2 = a \rangle = \mathbb{Z}$,
2. $B = \langle a; p^2 a = 0, a^2 = pa \rangle$
3. $C = \langle a; p^2 a = 0, a^2 = 0 \rangle = \mathbb{C}_{p^2}(0)$
4. $D = \langle a, b; pa = pb = 0, a^2 = a, b^2 = b, ab = ba = 0 \rangle = \mathbb{Z}_p \oplus \mathbb{Z}_p$
5. $E = \langle a, b; pa = pb = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$
6. $F = \langle a, b; pa = pb = 0, a^2 = a, b^2 = b, ab = b, ba = a \rangle$
7. $G = \langle a, b; pa = pb = 0, a^2 = 0, b^2 = b, ab = a, ba = a \rangle$
8. $H = \langle a, b; pa = pb = 0, a^2 = 0, b^2 = b, ab = ba = 0 \rangle = \mathbb{Z}_p \oplus \mathbb{C}_p(0)$
9. $I = \langle a, b; pa = pb = 0, a^2 = b, ab = 0 \rangle$
10. $I = \langle a, b; pa = pb = 0, a^2 = b^2 = 0 \rangle = \mathbb{C}_p(0) \oplus \mathbb{C}_p(0)$

11. *$K = GF(p^2)$ = corpo finito de ordem $p^2 = \langle a, b; pa = pb = 0, a^2 = a, b^2 = ja, ab = b, ba = b\rangle$ para o qual $j$ não é um quadrado em $\mathbb{Z}_p$, se $p \nmid 2$ e $\langle a, b; 2a = 2b = 0, a^2 = a, b^2 = a + b, ab = b, ba = b\rangle$, se $p = 2$., onde $C_p(0)$ é o anel que é o grupo cíclico de ordem $p$ com respeito a soma e possui multiplicação trivial*

*Demonstração.* Consulte [1]. □

**Lema 1.** *(Hölder 1893) Se $p$, $q$ e $r$ são primos, com $p < q < r$, então*

$$f(pqr) = \begin{cases} p+4 & \text{se } r \equiv 1 \pmod p,\ r \equiv 1 \pmod q \text{ e } q \equiv 1 \pmod p \\ p+2 & \text{se } r \equiv 1 \pmod p,\ r \not\equiv 1 \pmod q \text{ e } q \equiv 1 \pmod p \\ 4 & \text{se } r \equiv 1 \pmod p,\ r \equiv 1 \pmod q \text{ e } q \not\equiv 1 \pmod p \\ 2 & \text{se } r \equiv 1 \pmod p,\ r \not\equiv 1 \pmod q \text{ e } q \not\equiv 1 \pmod p \\ 3 & \text{se } r \not\equiv 1 \pmod p,\ r \equiv 1 \pmod q \text{ e } q \equiv 1 \pmod p \\ 2 & \text{se } r \not\equiv 1 \pmod p,\ r \not\equiv 1 \pmod q \text{ e } q \equiv 1 \pmod p \\ 2 & \text{se } r \not\equiv 1 \pmod p,\ r \equiv 1 \pmod q \text{ e } q \not\equiv 1 \pmod p \\ 1 & \text{se } r \not\equiv 1 \pmod p,\ r \not\equiv 1 \pmod q \text{ e } q \not\equiv 1 \pmod p \end{cases}$$

*Note que esses oito casos cobrem todas as possibilidades.*

Do ponto de vista histórico é interessante consultar o artigo original do Hölder [2]. Para uma prova detalhada da enumeração, consulte [4]. Para saber o estado da arte sobre o que a humanidade sabe sobre enumeração de grupos finitos consulte [3].

**Teorema 3.** *Existe um $n$ tal que $f(n) > g(n)$*

*Demonstração.* Considere $p = 5$, $q = 11$, $r = 661$. Observe que $11 \equiv 1 \pmod 5$, $661 \equiv 1 \pmod 5$ e $661 \equiv 1 \pmod{11}$. Existem $g(5 \cdot 11 \cdot 661) = g(5)g(11)g(661) = 2^3 = 8$ anéis isomorfos com $6 \cdot 11 \cdot 665$ elementos. Por outro lado, existem $f(6 \cdot 11 \cdot 665) = 5 + 4 = 9$ elementos. □

**Exercício 4.** *Existem infinitos primos tais que $f(n) > g(n)$. Mais ainda, o valor de $f(n) - g(n)$ pode ser tomado arbitrariamente grande.*

**Lema 2.** *(Hölder 1893) Se $p$ e $q$ são primos distintos, então*

$$f(pq^2) = \begin{cases} 5 & \text{se } p = 2 \text{ ou se } p = 3,\ q = 2 \text{ ou } 1 \\ \frac{1}{2}(p+9) & \text{se } p \text{ é ímpar e } q \equiv 1 \pmod p \\ 5 & \text{se } p \equiv 1 \pmod{q^2} \\ 4 & \text{se } p > 3,\ p \equiv 1 \pmod q \text{ e } p \not\equiv 1 \pmod{q^2} \\ 3 & \text{se } p > 2, q > 3 \text{e } p \equiv -1 \pmod q \\ 2 & \text{em todos os outros casos.} \end{cases}$$

Para a demonstração desse resultado sugerimos a leitura de [3] e [4].

**Teorema 4.** *Se $p$ e $q$ são primos, com $p$ sendo ímpar, $p > 35$, $q \equiv 1 \ (mod\ p)$, então $f(n) > g(n)$*

*Demonstração.* $g(pq^2) = g(p)g(q^2) = 2 \cdot 11 = 22$, então precisamos de $f(n) = f(pq^2) = \frac{1}{2}(p+9) > g(n) = 22$. Portanto, $p > 35$. □

**Exemplo 1.** *Para $p = 37$, o menor primo $q$ que podemos escolher é $q = 149$. Assim, para $n = 37 \cdot 149^2 = 821437$, temos $f(n) = \frac{1}{2}(37+9) = 23 > 22 = 2 \cdot 11 = g(n)$.*

Para $n = 41$, $2 \cdot 41 + 1 = 83$ é primo, e obtemos $f(n) = f(41 \cdot 83^2) = f(282449) = \frac{1}{2}(41+9) = 25$, enquanto $g(n) = 22$.

**Exercício 5.** *Mostre que $f(n) - g(n)$ pode ser tão grande quando se queira tomando $n$ da forma $n = pq^2$ e $q \equiv 1 \ (mod\ p)$.*

Finalizamos o texto com algumas conjecturas e um exercício.

1. $f$ é sobrejetora em $\mathbb{N}$
2. É 36355 o menor valor de $n$ para o qual $f(n) > g(n)$?
3. É verdade que $g(p^r) > f(p^r)$ para todos os primos $p$ e números naturais $r$?
4. É verdade que, para $n > 1$, existem mais anéis finitos de ordem no máximo $n$ do que grupos de ordem no máximo $n$?
5. Existe um $n > 1$ tal que $f(n) = g(n)$?

**Exercício 6.** *A função $g$ não é sobrejetora*

# Referências


[1] FINE, Benjamin. Classification of finite rings of order $p^2$. Mathematics magazine, v. 66, n. 4, p. 248-252, 1993.

[2] HÖLDER, Otto. Die Gruppen der Ordnungen $p^3$, $pq^2$, $pqr$, $p^4$. Mathematische Annalen, v. 43, p. 301-412, 1893.

[3] BLACKBURN, Simon R.; NEUMANN, Peter M.; VENKATARAMAN, Geetha. Enumeration of finite groups, 2007.

[4] GANEV, Iordan. Groups of a square-free order. Rose-Hulman Undergraduate Mathematics Journal, v. 11, n. 1, p. 7, 2010.

[5] MACHALE, Desmond. Are There More Finite Rings than Finite Groups?. The American Mathematical Monthly, v. 127, n. 10, p. 936-938, 2020.