[Conclusão da aula anterior: exemplos de polinómios resolúveis e polinómios não resolúveis]

4. Corpos finitos

Neste capítulo final vamos estudar as propriedades fundamentais dos corpos finitos e descrever algumas das suas muitas aplicações (à teoria dos códigos, teoria dos números e teoria matemática dos jogos).

O corpo $\mathbb{F}_p = (\mathbb{Z}_p, \oplus_p, \otimes_p)$ dos inteiros módulo p (p primo) é, evidentemente, o exemplo mais familiar de corpo finito. Muitas das suas propriedades generalizam-se aos corpos finitos arbitrários. Os corpos $\mathbb{F}_p$ representam um papel muito importante na teoria dos corpos pois, como vimos, todo o corpo de característica p contém uma cópia isomorfa de $\mathbb{F}_p$ (como seu subcorpo primo) e pode então ser visto como uma extensão de $\mathbb{F}_p$. Esta observação, conjuntamente com o facto óbvio de que todo o corpo finito tem característica finita (prima), é fundamental para a classificação dos corpos finitos.

Além dos corpos $\mathbb{F}_p$, de ordem prima p, já encontrámos (na Aula 17) outros exemplos de corpos finitos: um corpo de ordem $4 = 2^2$, definido pelas tabelas

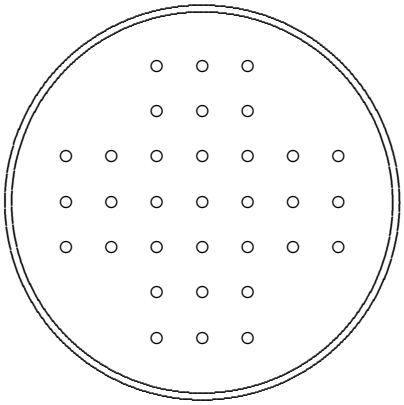
$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

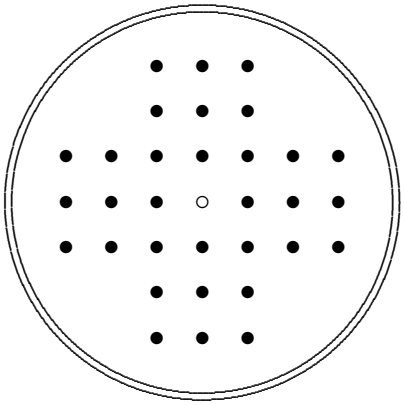
e um corpo de ordem $16 = 2^4$. Haverá algum corpo de ordem 6? Veremos em seguida que não, ao provarmos que a ordem de qualquer corpo finito é necessariamente da forma p^n para algum primo p e algum natural n, e que, para cada número dessa forma existe, a menos de isomorfismo, exactamente um corpo com esse número de elementos.

Antes de avançarmos para a prova desses resultados que permitem classificar os corpos finitos, vejamos uma aplicação do corpo com 4 elementos acima referido, que se pode encontrar em [N. de Bruijn, *A solitaire game and its relation to a finite field*, J. Recreational Math. 5 (1972) 133].

O jogo do solitário é jogado num tabuleiro como a figura representa



Inicialmente, em cada buraco, com excepção do central, coloca-se uma bola (32 bolas no total):



O jogo desenrola-se movimentando uma bola por cima de outra adjacente (na vertical ou na horizontal) para um buraco vazio; a bola sobre a qual se saltou é então removida do jogo. O objectivo do jogador é chegar a uma situação em que só reste uma bola no tabuleiro.

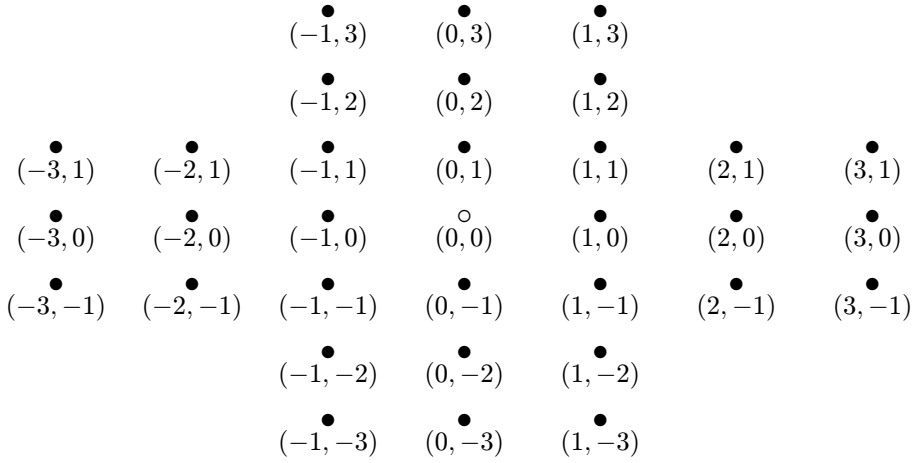
`[Frequentemente, esta última bola acaba por ficar no buraco central; experimente!]`

Poderá ficar noutro buraco que não o central?

Se jogarmos algumas vezes observaremos que sim, mas também nos convenceremos que talvez não possa ocupar qualquer posição.

Quais são as posições possíveis?

A ideia de de Bruijn é usar o corpo acima referido para determinar tais posições. Para isso, consideremos os buracos do tabuleiro referenciados por pares de inteiros (i, j), com o buraco central em $(0, 0)$:

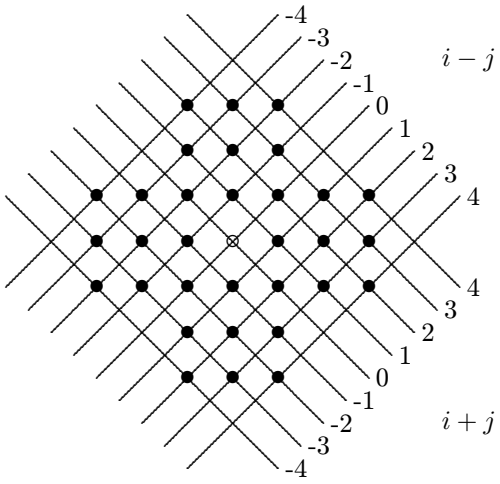


Definamos, para cada conjunto X de bolas colocadas no tabuleiro, os números

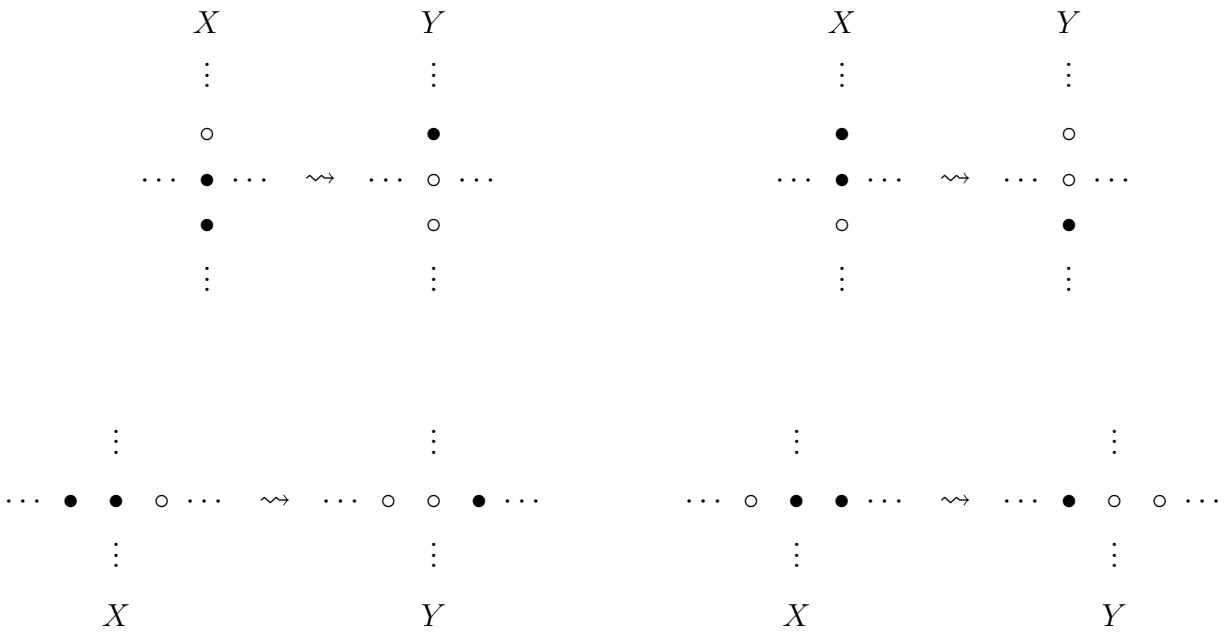
$$A(X) = \sum_{(i,j)\in X} \alpha^{i+j}, \qquad B(X) = \sum_{(i,j)\in X} \alpha^{i-j}.$$

Por exemplo, para a posição inicial X_1 do jogo, é fácil de ver (observe a figura abaixo) que

$$\begin{aligned} A(X_1) = B(X_1) &= 2\alpha^4 + 4\alpha^3 + 5\alpha^2 + 4\alpha^1 + 2\alpha^0 + 4\alpha^{-1} + 5\alpha^{-2} + 4\alpha^{-3} + 2\alpha^{-4} \\ &= 0 + 0 + 5\beta + 0 + 0 + 0 + 5\alpha + 0 + 0 \\ &= \alpha + \beta = 1. \end{aligned}$$



Cada jogada, que transforma um conjunto X de bolas no tabuleiro num conjunto Y, é necessariamente de um dos quatro tipos seguintes:



É fácil de ver que, em qualquer um desses tipos de jogada, se tem $A(Y) = A(X)$ e $B(Y) = B(X)$. Por exemplo, no primeiro tipo, se supusermos que a bola a movimentar está inicialmente na posição (i, j) (e portanto, após a jogada, vai ficar na posição $(i, j + 2)$), então

$$A(X) - A(Y) = \alpha^{i+j} + \alpha^{i+j+1} - \alpha^{i+j+2} = \alpha^{i+j}(1 + \alpha + \alpha^2) = 0,$$

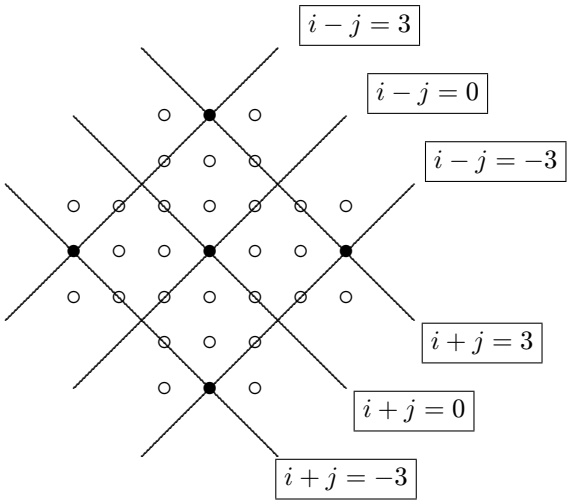
$$B(X) - B(Y) = \alpha^{i-j} + \alpha^{i-j-1} - \alpha^{i-j-2} = \alpha^{i-j}(1 + \beta + \beta^2) = 0.$$

Portanto, o par $(A(X), B(X))$ é invariante ao longo do jogo.

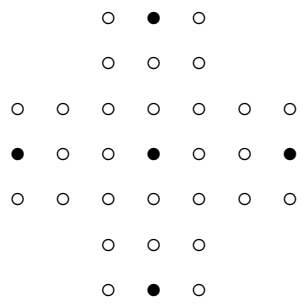
Assim, se o jogo terminar com uma só bola no tabuleiro, na posição (i, j), teremos necessariamente $A(\{(i, j)\}) = 1$ e $B(\{(i, j)\}) = 1$, isto é, $\alpha^{i+j} = 1$ e $\alpha^{i-j} = 1$. Como as sucessivas potências de α são

$$\alpha^{-4} = \beta, \boxed{\alpha^{-3} = 1}, \alpha^{-2} = \alpha, \alpha^{-1} = \beta, \boxed{\alpha^0 = 1}, \alpha^1 = \alpha, \alpha^2 = \beta, \boxed{\alpha^3 = 1}, \alpha^4 = \alpha,$$

a posição (i, j) da bola final terá que satisfazer $i+j \in \{-3, 0, 3\}$ e $i-j \in \{-3, 0, 3\}$:



Em conclusão, as únicas posições finais possíveis são $(-3,0)$, $(0,-3)$, $(0,0)$, $(0,3)$ e $(3,0)$:



Por experimentação, é possível concluir que todas elas podem ser, de facto, obtidas.

[Por simetria, basta mostrar que se consegue atingir as posições $(0,0)$ e $(3,0)$]