



Universidade de Brasília

Dinâmica da aplicação quadrada em grupos finitos

Pedro Luís Souto Silva

Departamento de Matemática
Universidade de Brasília

Dissertação apresentada como requisito parcial para obtenção do grau
de
Mestre em Matemática

Brasília, 11 de Dezembro de 2025

Pedro Luís Souto Silva ¹

DINÂMICA DA APLICAÇÃO QUADRADA EM GRUPOS FINITOS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. Raimundo de Araújo Bastos Júnior

¹Autor financiado pelo CAPES

Agradecimentos

Agradeço a minha família, que me deu toda a chance e oportunidade e incentivo para estudar desde a minha infância.

Agradeço a meu orientador, por toda sua paciência e instrução em nossos anos de trabalho juntos.

Agradeço a meus colegas, pelo apoio e conforto em meio aos estresses do processo.

Abstract

In this work we study the dynamics of the square mapping in some families of groups, by exposing the iteration of the mapping as an action on a set of points generating a directed graph. The action of the square mapping on cyclic and abelian groups is well known and is established, as well as the action in finite 2-groups with cyclic maximal subgroup and groups of exponent p .

keywords: *finite groups, discrete dynamical systems, directed graphs, finite p -groups.*

Resumo

Nesse trabalho estudamos a dinâmica de aplicações de potência em algumas famílias de grupos. Resultados bem estabelecidos para grupos cíclicos e abelianos são enunciados e demonstrados. Estudamos também a dinâmica da aplicação potência quadrado para grupos de expoente p e 2-grupos de grupo maximal cíclico, expondo a dinâmica discreta da aplicação como um grafo direcionado finito.

Palavras-Chave: *Grupos finitos, sistemas dinamicos discretos, grafos direcionados, p -grupos finitos*

Conteúdo

1	Introdução	1
2	Conceitos preliminares sobre grafos	3
2.1	Grafos direcionados	3
2.2	Grafos Gerados por Funções	4
2.3	Árvores e Ciclos	6
2.4	Produtos tensoriais	12
2.5	Grafos de Endomorfismos	15
3	Dinâmica em grupos abelianos	19
3.1	Preliminares	19
3.2	Grupos cíclicos	20
3.3	Grupos cíclicos de ordem ímpar	20
3.4	Grupos cíclicos de ordem par	22
3.5	Produtos Tensoriais e Árvores Elementares	26
3.6	Grupos Abelianos	30
4	Alguns grupos não abelianos	33
4.1	Grupos Diedrais	34
4.2	Grupos Quatérnios Generalizados	36
4.3	2-grupos	38
4.4	2-grupos com subgrupo cíclico maximal	40
4.5	Grupos de Expoente p	44
5	Considerações finais	49

Capítulo 1

Introdução

Um **sistema dinâmico finito** é o estudo de iterações de uma aplicação $f : X \rightarrow X$, onde X é um conjunto finito. O estudo de sistemas dinâmicos finitos possui aplicações em áreas como criptografia, engenharia e biologia (veja por exemplo [8] para uma coletânea de aplicações). Quando o conjunto X possui estruturas adicionais, como sendo um grupo, anel ou corpo, e f for uma aplicação que é bem comportada com essa estrutura, por exemplo, um endomorfismo, então é possível fazer uma análise adicional utilizando as propriedades algébricas de X .

O estudo de aplicações polinomiais em grupos finitos pode ser visto em [5], [6], [13], [15], entre outros. Os dois primeiros estavam interessados no estudo de Corpos finitos: quando $\mathbb{F}_{p^n}$ é um corpo finito, seu subconjunto de elementos inversíveis $\mathbb{F}_{p^n}^*$ é um grupo cíclico, o que proporciona uma motivação natural para o estudo de aplicações em grupos (cíclicos).

Em uma direção distinta de trabalhos como [1], [6], [10] e [11] que buscaram estudar a dinâmica de diferentes classes de polinômios em corpos finitos (e portanto grupos cíclicos), esse trabalho se preocupará com o estudo do mapa $f : G \rightarrow G$, $f(x) = x^2$ para diferentes classes de grupos. O estudo dessa função particular foi feita em [15] para grupos cíclicos e em [13] para grupos abelianos e grupos de flores.

Uma poderosa ferramenta no estudo de dinâmica finita é o **Grafo Direcionado**. Grafos direcionados permitem a visualização da dinâmica de uma aplicação em um conjunto finito de uma maneira concisa e prática. Utilizando grafos também podemos fazer perguntas sobre a conexidade do grupo sob a função. Devido a ubiquidade de grafos direcionados nesse trabalho, o **Capítulo 2** é dedicado a definição formal desses, e o estabelecimento de notações úteis. Os grafos estudados no texto serão predominantemente **grafos definidos por funções**, que tornam a dinâmica da aplicação visível. Grafos definidos por funções tomam a forma de uniões disjuntas de grafos

da forma $Cyc(k, \mathcal{T})$, que são ciclos cujos vértices são raízes de árvores isomorfas a $\mathcal{T}$. Iremos introduzir esses três conceitos. Por fim, trataremos de **produtos tensoriais**: uma forma de combinar diferentes grafos que será central no final do Capítulo 3.

No **Capítulo 3** iremos estudar a dinâmica de grupos abelianos. Pelo teorema fundamental de grupos abelianos finitos, todo grupo abeliano pode ser escrito como o produto direto de grupos cíclicos. Por [15], possuímos a estrutura de grafo relacionado com grupos cíclicos, e por [13] temos uma operação de grafos compatível com o produto direto de grupos: o produto tensorial de grafos. Com esses dois resultados, é possível determinar o grafo funcional da aplicação quadrada para qualquer grupo abeliano finito, embora algum trabalho extra será feito para obter uma representação isomorfa ao produto tensorial que seja conveniente. Iremos classificar os grafos funcionais de grupos cíclicos de ordem ímpar, inicialmente, e em seguida de ordens gerais, como foi feito em [15]. Com isso, podemos obter uma descrição do grafo correspondente a um grupo abeliano utilizando produtos tensoriais.

No **Capítulo 4** a escolha de especializar-nos na aplicação $f(x) = x^2$ se mostrará vantajosa. Classes de grupos finitos que possuem um subgrupo maximal cíclico cujo índice é uma potência de 2 são comuns na literatura: Grupos Diedrais, Quatérnios Generalizados, Semidiedrais, entre outros. Sob a ação da nossa função, esses grupos são bem próximos de grupos cíclicos, que já foram classificados no Capítulo 2. Nesse capítulo também investigaremos grupos de expoente primo, onde uma propriedade similar se revela: o grafo relacionado a um grupo de expoente p consiste em várias cópias do grafo relacionado ao grupo C_p .

Capítulo 2

Conceitos preliminares sobre grafos

2.1 Grafos direcionados

Seja V um conjunto não vazio. Um **grafo direcionado** é um par (V, A) onde A é um subconjunto de $V \times V$. Iremos permitir que pares do tipo $(v, v) \in V \times V$ estejam em A . O conjunto V é chamado de **conjunto de vértices** e o conjunto A é dito o **conjunto de arestas**. Neste trabalho, **todo grafo será direcionado**, e portanto omitiremos o termo "direcionado" pelo resto do texto.

Representamos visualmente um grafo com um ponto para cada vértice e uma seta de a para b para cada par (a, b) em A . Por exemplo:

Exemplo 2.1.1. Seja $V = \{1, 2, 3, 4\}$ e seja $A = \{(1, 2), (1, 3), (2, 3)\}$. Então teremos a seguinte representação visual do grafo (V, A) :

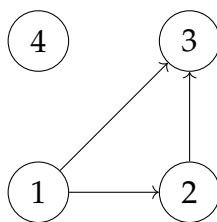


Figura 2.1 : Grafo (V, A)

O conjunto de vértices pode ser qualquer conjunto. Porém, nos casos onde V é infinito, a representação visual do grafo é inviável. Nesse trabalho, salvo menção em contrário, V corresponderá a um conjunto finito, portanto não teremos este problema.

Um fato importante relativo a grafos é que a representação visual não é única. Antes de formalizarmos esse princípio, vejamos o seguinte exemplo:

Seja $V_1 = \{a, b, c, d\}$ e $A_1 = \{(a, b), (a, c), (b, c)\}$. Temos o grafo:

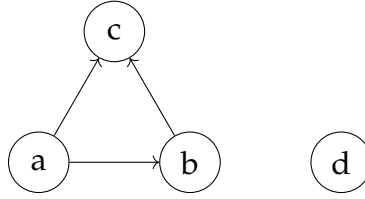


Figura 2.2 : Grafo (V_1, A_1)

É possível notar que os grafos (V, A) e (V_1, A_1) acima são semelhantes em estrutura, mesmo que $V_1 \neq V$ e as representações gráficas utilizadas são distintas. De fato, eles são o "mesmo" grafo, um conceito formalizado utilizando **Isomorfismos de grafos**:

Definição 2.1.1 (Isomorfismo de Grafos). Sejam $\mathcal{G}_1 = (V_1, A_1)$ e $\mathcal{G}_2 = (V_2, A_2)$ grafos. Uma bijeção $\varphi : V_1 \rightarrow V_2$ tal que $(u, v) \in A_1$ se e somente se $(\varphi(u), \varphi(v)) \in A_2$ é chamada de **Isomorfismo de Grafos**. Se um tal isomorfismo existe, dizemos que $\mathcal{G}_1$ é **Isomorfo** a $\mathcal{G}_2$, com a notação $\mathcal{G}_1 \cong \mathcal{G}_2$.

Diversas vezes cometeremos o abuso de referir a grafos isomorfo usando termos como "iguais" ou "o mesmo grafo". Assim como isomorfismos entre estruturas algébricas (grupos, anéis, corpos, etc), é possível mostrar que $\mathcal{G}_1 \cong \mathcal{G}_2$ é uma relação de equivalência entre grafos.

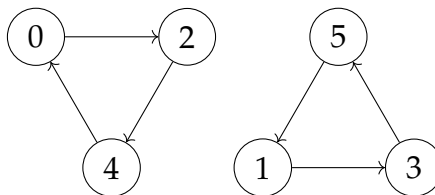
2.2 Grafos Gerados por Funções

Os grafos que estaremos interessados nesse trabalho são **Grafos gerados por funções**:

Definição 2.2.1. Sejam V um conjunto e $f : V \rightarrow V$ uma função. O **grafo gerado por f** , denotado por $\mathcal{G}(V, f)$ é o grafo (V, A) onde $A = \{(a, f(a)) \mid a \in V\}$.

Vejamos alguns exemplos.

Exemplo 2.2.1. Seja $V = \mathbb{Z}/6\mathbb{Z}$, e defina a função $f : V \rightarrow V$, por $f(x) = x + 2$. Então o grafo $\mathcal{G}(V, f)$ é dado abaixo:

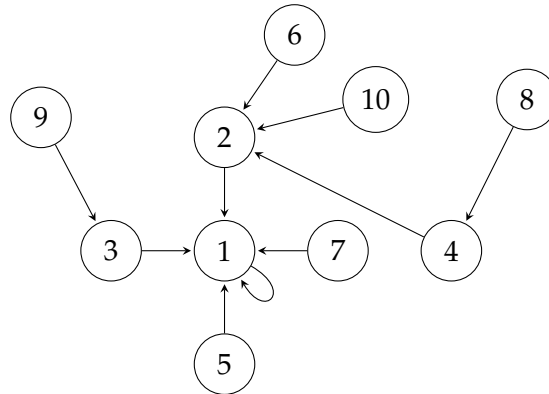


É possível notar algumas características de grafos gerados por funções nesse exemplo. Em específico, todos os vértices tem grau de saída, isto é, para todo $a \in V$ existe apenas um elemento de forma $(a, b) \in A$. Isto é uma consequência direta da definição de funções: para todo $a \in V$ existe apenas um $f(a)$. Isso não impede de termos múltiplas arestas "entrando" em um vértice, como ilustrado no próximo exemplo.

Exemplo 2.2.2. Seja $V = \mathbb{N}$ e definamos uma função $f : V \rightarrow V$ da seguinte maneira:

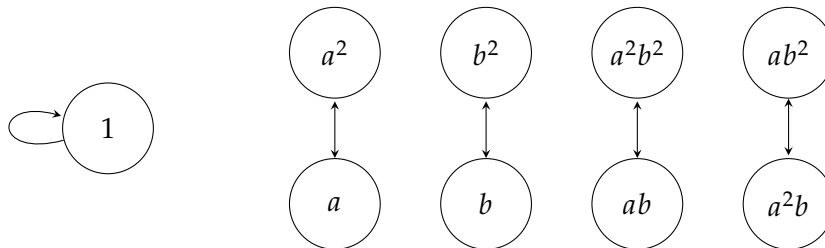
$$f(n) = \begin{cases} 1, & \text{se } n = 1; \\ n/p_n, & \text{caso contrário, onde } p_n \text{ é o maior primo dividindo } n \end{cases}.$$

Como V é um conjunto infinito, não podemos representar o grafo completo. Vamos representar apenas os vértices de 1 a 10:



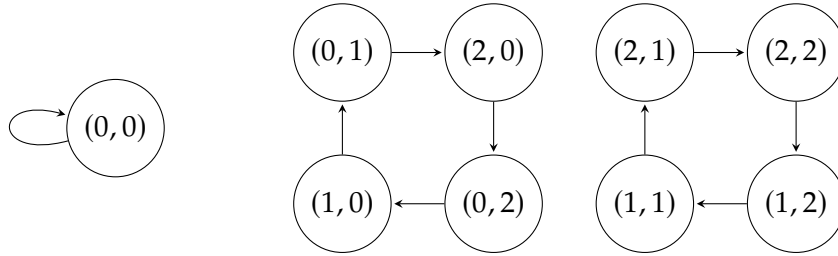
Todos os números primos estão adjacentes com o vértice 1. Note que 1 é um ponto fixo da função f , logo $(1, 1) \in A$. Para todo natural n , existe $k \in \mathbb{N}$ tal que $f^k(n) = 1$.

Exemplo 2.2.3. Vejamos um exemplo agora de grafo em um grupo. Seja $V = C_3 \times C_3$ com C_3 sendo o grupo cíclico de ordem 3. Seja $f : V \rightarrow V$ a função dada por $f(x) = x^2$. Então se tomarmos a apresentação $C_3 \times C_3 \cong \langle a, b | a^3, b^3, [a, b] \rangle$, temos o seguinte grafo $\mathcal{G}(V, f)$:

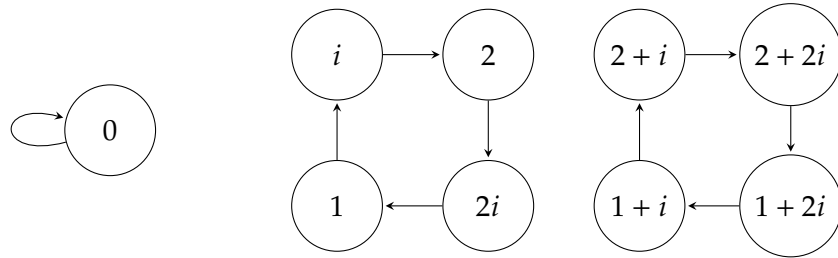


Como a ordem do grupo é ímpar, o único elemento cuja ordem é uma potência de 2 é a identidade, de ordem 2^0 . No grafo isso corresponde com nenhum elemento sendo direcionado para a identidade. O mapa corresponde ao automorfismo de ordem dois $x \rightarrow x^{-1}$.

Exemplo 2.2.4. Seja $V = \mathbb{F}_9$ o corpo finito de 9 elementos, cuja representação que usaremos é $\mathbb{F}_9 \cong \mathbb{F}_3/(X^2 + 1) = \{a + bi : a, b \in \mathbb{F}_3, i^2 = 2\}$. O corpo $\mathbb{F}_9$ é um espaço vetorial de Dimensão 2 sobre $\mathbb{F}_3$, onde $a + bi$ corresponde com o vetor (a, b) . Seja T a transformação linear nesse espaço vetorial dada por $T(a, b) = (2b, a)$. Então o grafo $\mathcal{G}(V, T)$ é dado por:



Exemplo 2.2.5. Seja novamente $V = \mathbb{F}_9$, com $f : \mathbb{F}_9 \rightarrow \mathbb{F}_9$, a aplicação $f(x) = i \cdot x$, onde $i^2 = 2$ como acima. Temos o grafo:



É possível notar, comparando os grafos dos exemplos 5 e 6 acima, que ambos são isomórficos, e o isomorfismo de grafos é o isomorfismo natural de $\mathbb{F}_9$ visto como um corpo e como um espaço vetorial.

2.3 Árvores e Ciclos

Iremos introduzir algumas notações e operações de grafos que serão frequentemente utilizados no decorrer desse trabalho.

Definição 2.3.1 (ciclos). Para $k \geq 1$, um **ciclo de comprimento** k , denotado por $\text{Cyc}(k)$ é um grafo isomorfo a (V, A) com $V = \{v_1, v_2, \dots, v_k\}$ e $A = \{(v_i, v_{i+1}) : i = 1, 2, \dots, k-1\} \cup \{(v_k, v_1)\}$.

Exemplo 2.3.1. Seguem representações dos grafos $\text{Cyc}(i)$, com $i \in \{3, 4, 5\}$



Figura 2.3 : Grafos $\text{Cyc}(1)$ e $\text{Cyc}(2)$ respectivamente

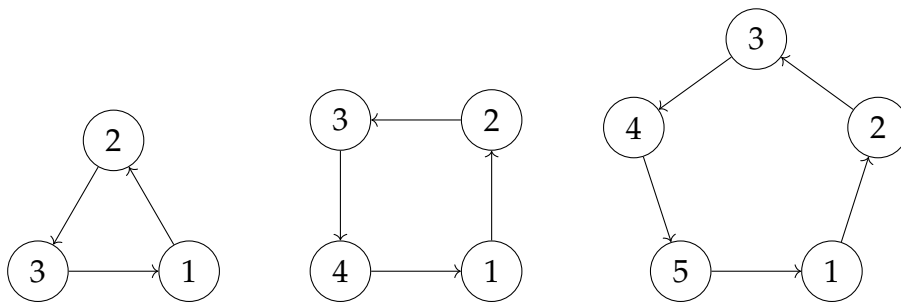


Figura 2.4 : Grafos $\text{Cyc}(3)$, $\text{Cyc}(4)$, $\text{Cyc}(5)$, respectivamente

Vamos definir algumas operações úteis em grafos:

Definição 2.3.2 (Soma direta). Se $\mathcal{G}_1$ e $\mathcal{G}_2$ são grafos, a **soma direta** de $\mathcal{G}_1$ e $\mathcal{G}_2$, denotada por $\mathcal{G}_1 \oplus \mathcal{G}_2$ é a união disjunta de $\mathcal{G}_1$ e $\mathcal{G}_2$. Usaremos a notação $k \times \mathcal{G} = \bigoplus_{i=1}^k \mathcal{G}_i$ onde cada um dos $\mathcal{G}_i$ é isomorfo a $\mathcal{G}$.

O grafo no Exemplo 2.2.1 acima é uma união disjunta de dois ciclos; a saber, $\mathcal{G} = 2 \times \text{Cyc}(3)$. O grafo no Exemplo 2.2.3 acima é a soma direta $\text{Cyc}(1) \oplus (4 \times \text{Cyc}(2))$.

Definição 2.3.3 (Árvores). Uma **árvore** é um grafo (V, A) que possui um vértice especial $v_0 \in V$ chamado de **raiz** tal que para todo vértice $v \in V$ existe um único caminho direcionado de v para v_0 .

Observação 2.3.4. no estudo de grafos não direcionados, a definição usual de árvore é notavelmente mais simples, a dizer, um grafo conexo que não possui ciclos. A nossa

definição requer adicionalmente que . Um exemplo dessa diferença é observado nos três grafos com conjunto de vértices $V = \{a, b, c\}$ abaixo, com conjuntos de arestas distintas $A_1 = \{(a, b), (c, b)\}$, $A_2 = \{(b, a), (c, b)\}$ e $A_3 = \{(b, c), (b, a)\}$. Os grafos (V, A_1) e (V, A_2) são árvores com raízes b e a respectivamente, enquanto o grafo (V, A_3) não é uma árvore pois não possui raiz. Do ponto de vista de grafos não direcionados os três grafos são isomorfos e portanto são todos árvores.

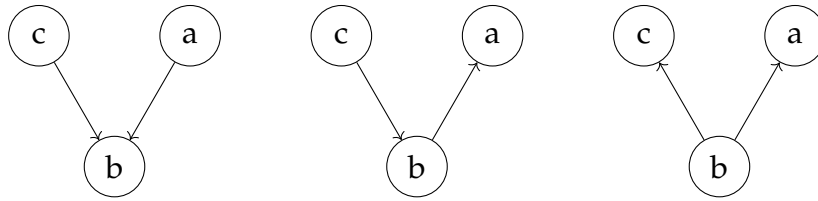


Figura 2.5 : Grafos (V, A_1) , (V, A_2) , e (V, A_3) respectivamente.

O grafo no Exemplo 2.2.2 anterior é uma árvore de infinitos vértices. A sua raiz corresponde com o vértice 1.

Definição 2.3.5 (Floresta). uma **floresta** é uma união disjunta de árvores

Definição 2.3.6 (Árvores geradas). Seja $\mathcal{G} = \bigoplus_{i=1}^n \mathcal{T}_i$ uma floresta onde v_i é a raiz de $\mathcal{T}_i$, $i = 1, 2, \dots, n$. Então $\langle \mathcal{G} \rangle$ é a árvore obtida com a união de $\mathcal{G}$ com um novo vértice v_0 , e arestas (v_i, v_0) , $i = 1, \dots, n$.

Exemplo 2.3.2.

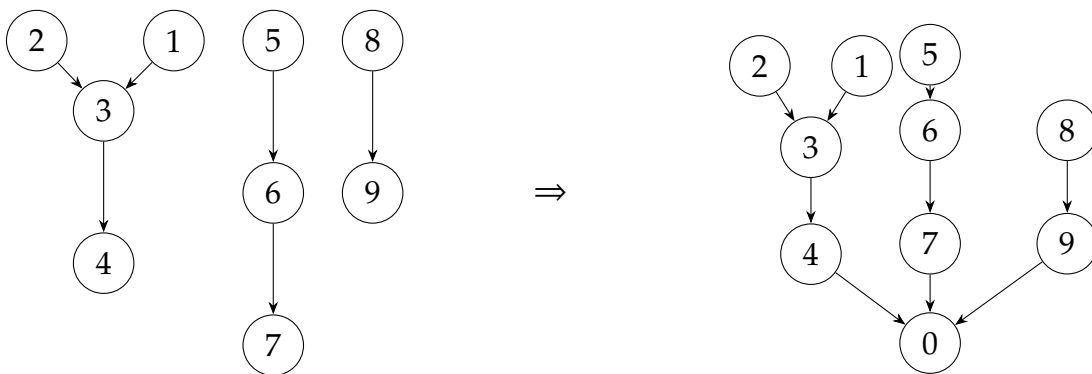


Figura 2.6 : A árvore à direita é gerada pelas árvores à esquerda

Uma família importante de árvores é o conjunto das árvores binárias.

Definição 2.3.7 (Árvores binárias). Uma **árvore binária** de profundidade k , denotada por $\mathcal{T}^k$ é definida recursivamente da seguinte forma: $\mathcal{T}^0$ é o grafo com apenas um vértice, $\mathcal{T}^1$ é um grafo isomorfo a $(\{\alpha, \beta\}, \{(\beta, \alpha)\})$ e para $k \geq 1$ $\mathcal{T}^{k+1}$ é obtido de $\mathcal{T}^k$ e $\mathcal{T}^1$ identificando o vértice β com as raízes de duas cópias disjuntas de $\mathcal{T}^k$.

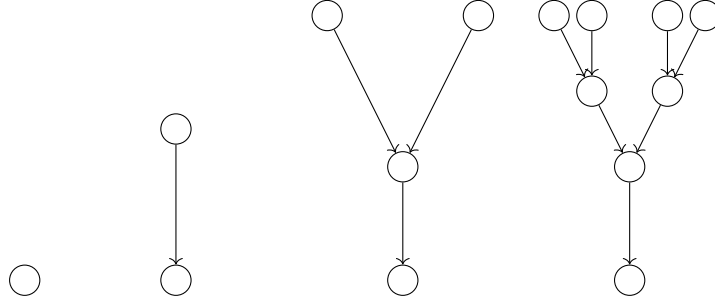


Figura 2.7 : :árvores binárias $\mathcal{T}^0, \mathcal{T}^1, \mathcal{T}^2$, e $\mathcal{T}^3$

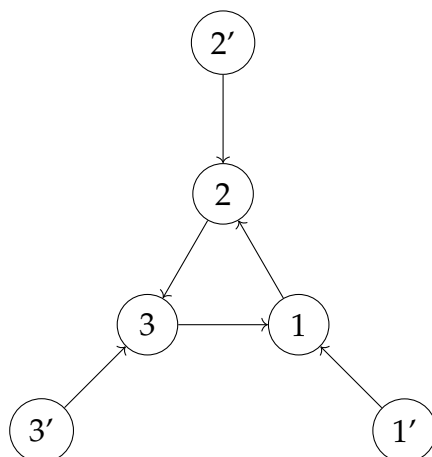
Note que $\mathcal{T}^k$ possui 2^k vértices no total.

Uma árvore binária é um exemplo de uma **árvore elementar**, que será definida no capítulo 3, onde servirá como uma notação compacta para o grafo de grupos abelianos.

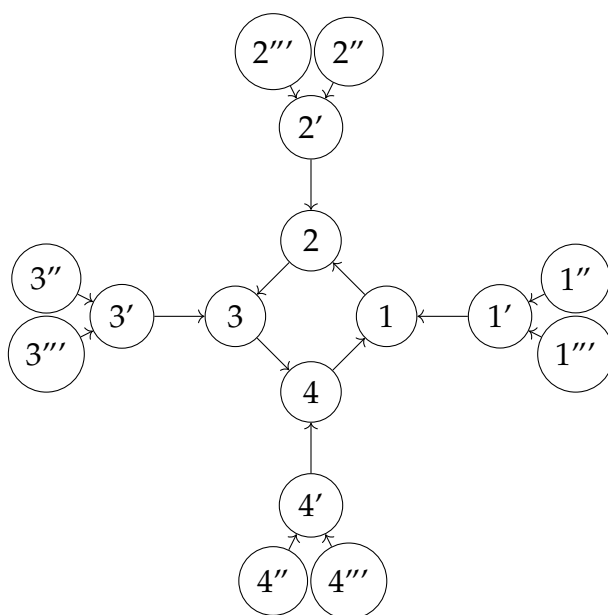
Definição 2.3.8. Seja $\mathcal{T}$ uma árvore. O grafo $\text{Cyc}(k, \mathcal{T})$ é obtido identificando os vértices de $\text{Cyc}(k)$ por raízes de árvores isomorfas à $\mathcal{T}$.

Para esse trabalho, esse é o tipo de grafo mais importante definido: grafos gerados por funções em conjuntos finitos naturalmente são formados por uniões de grafos do tipo $\text{Cyc}(k, \mathcal{T})$ como veremos posteriormente. No caso $\text{Cyc}(1, \mathcal{T})$ o grafo consiste na árvore $\mathcal{T}$ com um laço na identidade, e no caso $\mathcal{T} = \mathcal{T}^0$ é a árvore trivial, então convencionamos $\text{Cyc}(n, \mathcal{T}^0) = \text{Cyc}(n)$

Exemplo 2.3.3.

Figura 2.8 : Grafo $\text{Cyc}(3, \mathcal{T}^1)$

Exemplo 2.3.4.

Figura 2.9 : Grafo $\text{Cyc}(4, \mathcal{T}^2)$

Exemplo 2.3.5.

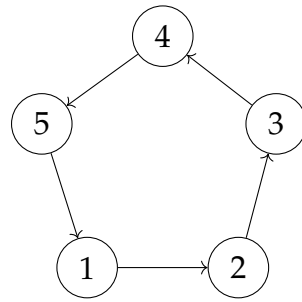
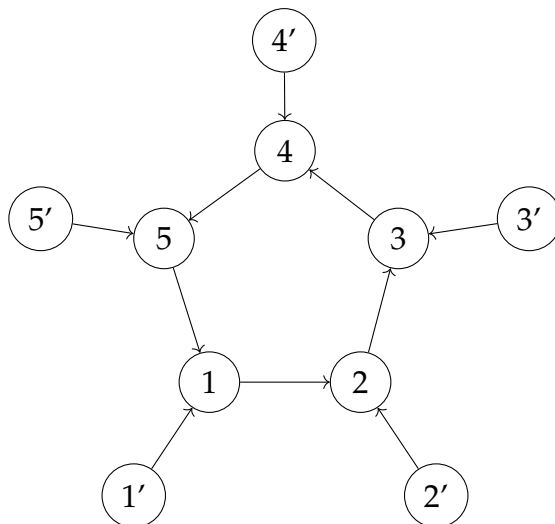


Figura 2.10 : Grafo $\text{Cyc}(5, \mathcal{T}^0) = \text{Cyc}(5)$

Exemplo 2.3.6.Figura 2.11 : : Grafo $\text{Cyc}(5, \mathcal{T}^1)$ **2.4 Produtos tensoriais**

Definição 2.4.1. Sejam $\mathcal{G}_1 = (V_1, A_1)$ e $\mathcal{G}_2 = (V_2, A_2)$ grafos. O **produto tensorial** $\mathcal{G}_1 \otimes \mathcal{G}_2$ é o grafo $(V_1 \times V_2, A)$ onde $A = \{((v_1, v_2), (w_1, w_2)) : (v_1, w_1) \in A_1 \text{ e } (v_2, w_2) \in A_2\}$.

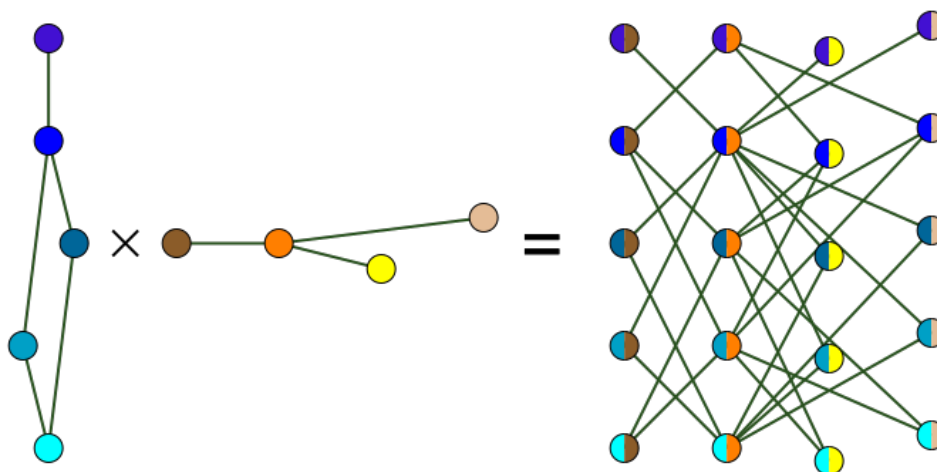
Exemplo 2.4.1.

Figura 2.12 : Produto tensorial de grafos. Na figura a direita, pares ordenados são representados como misturas de cores. (Crédito da imagem: David Eppstein, obtido de Wikipédia em inglês: Tensor Product of Graphs, Imagem em Domínio Público)

Exemplo 2.4.2. Seja $\mathcal{G}_1 = (V_1, A_1)$ onde $V_1 = \{a, b, c\}$, $A_1 = \{(a, b), (b, c), (c, c)\}$ (à esquerda na figura 2.13), e $\mathcal{G}_2 = (V_2, A_2)$ é o grafo de ciclo $\text{Cyc}(3)$, com $V_2 = \{1, 2, 3\}$, $A_2 = \{(1, 2), (2, 3), (3, 1)\}$ (no centro da figura 2.13). Denotaremos os pares ordenados de maneira simplificada, por exemplo $(a, 1) = a1$, $(b, 3) = b3$ etc. Se $\mathcal{G} = \mathcal{G}_1 \otimes \mathcal{G}_2 = (V, A)$ (à direita na figura 2.13), então $V = \{a1, a2, a3, b1, b2, b3, c1, c2, c3\}$ e $A = \{(a1, b2), (a2, b3), (a3, b1), (b1, c2), (b2, c3), (b3, c1), (c1, c2), (c2, c3), (c3, c1)\}$. Note que se $\mathcal{T}$ é a árvore isomorfa a $\mathcal{G}_1$, então $\mathcal{G}$ é isomorfo a $\text{Cyc}(3, \mathcal{T})$; Isto não é uma coincidência, como veremos no lema abaixo.

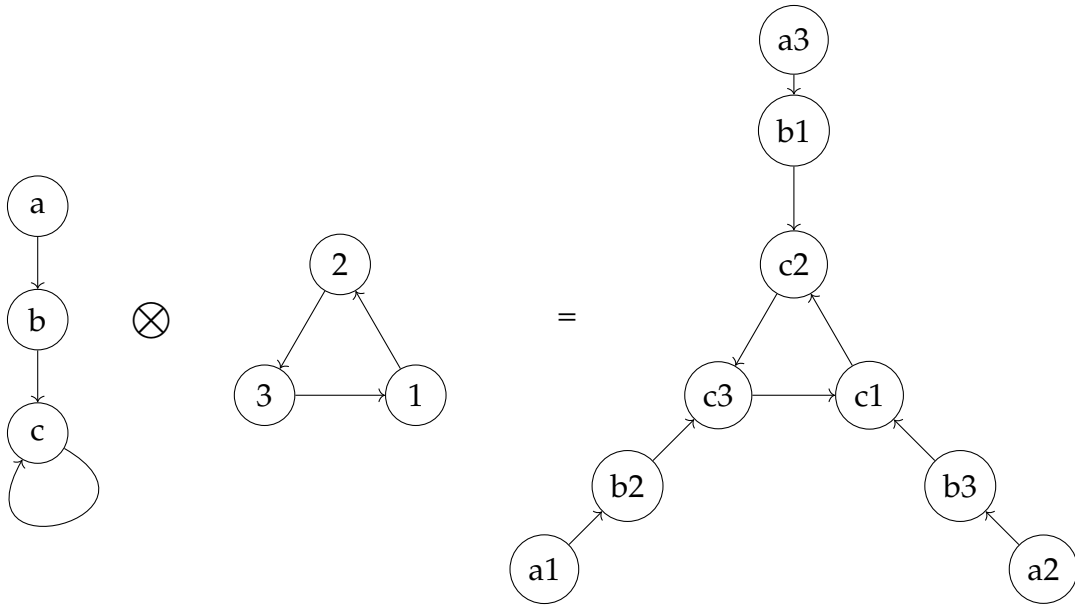


Figura 2.13 : Produto $\mathcal{G}_1 \otimes \mathcal{G}_2$

Lema 2.4.2 ([12], Lema 3.4). *Sejam X, Y conjuntos finitos e $(X, f), (Y, g)$ grafos gerados pelas aplicações f e g . Se $f \times g : X \times Y \rightarrow X \times Y$ é a aplicação $(x, y) \rightarrow (f(x), g(y))$ então o seguinte isomorfismo de grafos é válido:*

$$\mathcal{G}(X \times Y, f \times g) \cong \mathcal{G}(X, f) \otimes \mathcal{G}(Y, g)$$

Demonstração. Seja $\mathcal{G}_1 = \mathcal{G}(X \times Y, f \times g)$ e $\mathcal{G}_2 = \mathcal{G}(X, f) \otimes \mathcal{G}(Y, g)$. Os conjuntos de vértices são iguais, então basta mostrar que os conjuntos de arestas são iguais a menos de isomorfismos. De fato, seja A_1 o conjunto de arestas de $\mathcal{G}_1$ e A_2 o conjunto de arestas de $\mathcal{G}_2$. Por definição $A_1 = \{((x, y), (f(x), g(y))) : x \in X, y \in Y\}$ e $A_2 = \{((x, y), (x', y')) : (x, x') \in X \times f(X), (y, y') \in Y \times f(Y)\} = A_1$. $\square$

Para o próximo lema, vamos definir o nível de uma árvore:

Definição 2.4.3. Seja $\mathcal{T} = (V, A)$ um grafo de árvore direcionada. Para todo $v \in V$ definimos o **nível** indutivamente: se v_0 é a raiz da árvore, o nível de v_0 é 0. Se $(v, w) \in A$ então o nível de v é o sucessor do nível de w .

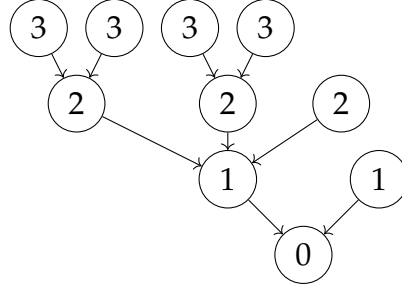


Figura 2.14 : Exemplos de níveis em uma árvore direcionada

A definição acima faz sentido pois na definição de árvore direcionada utilizada, temos apenas uma raiz e todos os outros vértices tem uma sequência de arestas direcionando à raiz.

Lema 2.4.4 ([12], Lema 3.5). Se $k \in \mathbb{Z}_{>0}$ e $\mathcal{T}$ é uma árvore, então o seguinte isomorfismo de grafos é válido:

$$\text{Cyc}(k, \mathcal{T}) \cong \text{Cyc}(k) \otimes \mathcal{T}$$

Demonstração. Seja $\text{Cyc}(k) = (V, A)$ onde $V = \{a_1, \dots, a_k\}$, $A = \{(a_i, a_{i+1}), \forall i < k\} \cup \{(a_k, a_1)\}$, e considere também $\mathcal{T} = (V', A')$, onde

$$V' = \{b_0, b_{1,1}, \dots, b_{1,r_1}, \dots, b_{n,1}, \dots, b_{n,r_n}\}$$

e b_0 é a raiz, n é o número de níveis da árvore e r_ℓ é o número de vértices de nível k . Isto é, para todo $1 \leq i \leq n, 1 \leq \ell \leq r_\ell$ existe um único $s, 1 \leq s \leq r_{i-1}$ tal que $(b_{i,\ell}, b_{i-1,s}) \in A'$.

Podemos escrever os grafos acima como grafos definidos por funções fazendo

$$f : V \rightarrow V$$

$$f(a_i) = \begin{cases} a_{i+1}, & \text{se } i < k \\ a_1, & \text{se } i = k \end{cases}$$

e

$$\begin{aligned} g : V' &\rightarrow V' \\ g(b_{1,\ell}) &= b_0, \forall 1 \leq \ell \leq r_1 \\ g(b_{s,\ell}) &= b_{s-1,\ell^*}, \forall 1 < s \leq n, 1 \leq \ell \leq r_s \end{aligned}$$

tal que $(b_{s,\ell}, b_{s-1,\ell^*}) \in A'$. Então pelo lema 2.4.2 temos que $\text{Cyc}(k) \otimes \mathcal{T} = \mathcal{G}(V \times V', f \times g)$. Aplicando repetidamente $f \times g$ temos o grafo $\text{Cyc}(k, \mathcal{T})$.

□

2.5 Grafos de Endomorfismos

O caso onde G é um grupo e f é um endomorfismo de G nos revela a importância de grafos do tipo $\text{Cyc}(k, \mathcal{T})$. Usemos o lema abaixo:

Lema 2.5.1 (Fitting). *Sejam G um grupo, f um endomorfismo de G tal que exista ℓ o menor inteiro tal que $\ker(f^\ell) = \ker(f^{\ell+1})$, e defina $\ker(f^\ell) = K$ e $\text{Im}(f^\ell) = I$. Então $G = K \rtimes I$, $f|_K$ é nilpotente de grau ℓ e $f|_I$ é um automorfismo. Ademais, se G é abeliano, $G = K \times I$*

Demonstração. Seja $g = f^\ell$. Seja $x \in \ker(g) \cap \text{Im}(g)$. Então $x = f^\ell(y)$ para algum $y \in G$. Mas então $1 = f(x) = f^{\ell+1}(y) = f^\ell(y) = x$, e portanto $K \cap I = \{1\}$. Por outro lado f^ℓ é um automorfismo em G/K , e portanto $G = K \rtimes I$.

Como $f^\ell(k) = 1$, para todo $k \in K$, temos que $f|_K$ é nilpotente. Como $f^\ell|_I$ é sobrejetora e I é finito, segue que $f^\ell|_I$ é bijetora e portanto $f|_I$ é isomorfismo. □

O lema 2.5.1 pode ser interpretado no ponto de vista de grafos. Se G é um conjunto finito e f é uma bijeção, então $\mathcal{G}(G, f)$ é uma união de ciclos disjuntos. Se f possui um "ponto terminal" x_0 tal que $f^n(x) = x_0, \forall x \in G$, como é o caso de endomorfismos nilpotentes, então o grafo $\mathcal{G}(G, f)$ é uma árvore de raiz x_0 . Observamos então que no caso onde G é um grupo finito e f é um endomorfismo, então $\mathcal{G}(G, f)$ é a união disjunta de grafos da forma $\text{Cyc}(k, \mathcal{T})$.

Exemplo 2.5.1. Seja $G = S_3$ o grupo simétrico de ordem 3. Sabemos que $G = \langle (12), (123) \rangle$, e portanto qualquer endomorfismo de G é determinado pelas imagens de $\sigma = (12)$ e $\pi = (123)$. Seja $f : S_3 \rightarrow S_3$ tal que $f(\pi) = \pi^2$ e $f(\sigma) = 1$. Então temos que todos os conjugados de σ , os 2-ciclos, tem imagem 1 e $f(\pi^2) = \pi^4 = \pi$, isto é:

$x \in S_3$	$f(x)$
1	1
(12)	1
(13)	1
(23)	1
(123)	(132)
(132)	(123)

O grafo $\mathcal{G}(G, f)$ é dado por:

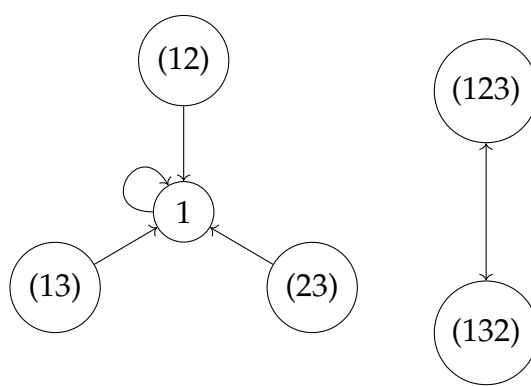
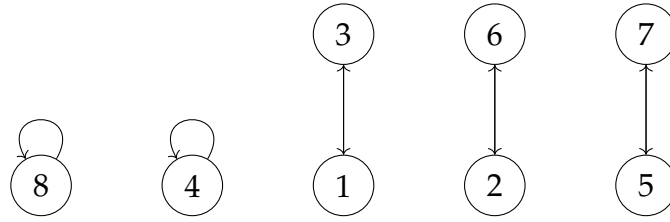


Figura 2.15 : Grafo $\mathcal{G}(S_3, f)$

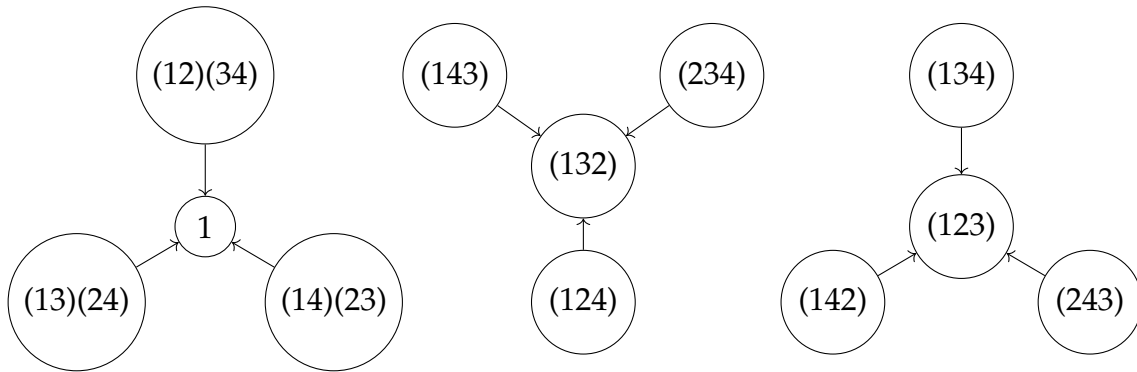
Note que o grafo $\mathcal{G}(S_3, f)$ é a união disjunta de uma árvore e $Cyc(2)$.

No caso onde f é um automorfismo de um grupo finito G , f é um elemento de $Sym(G)$, isto é, o grupo de permutações dos símbolos em G (aqui, G é visto como conjunto, sem preocupar com a estrutura de grupo). Neste caso, pela teoria de grupos simétricos, f é uma união de ciclos disjuntos. No ponto de vista de grafos, $\mathcal{G}(G, f)$ também será uma união de ciclos disjuntos, pois a definição de um ciclo em um grupo simétrico é feita pela ação de permutação dos elementos.

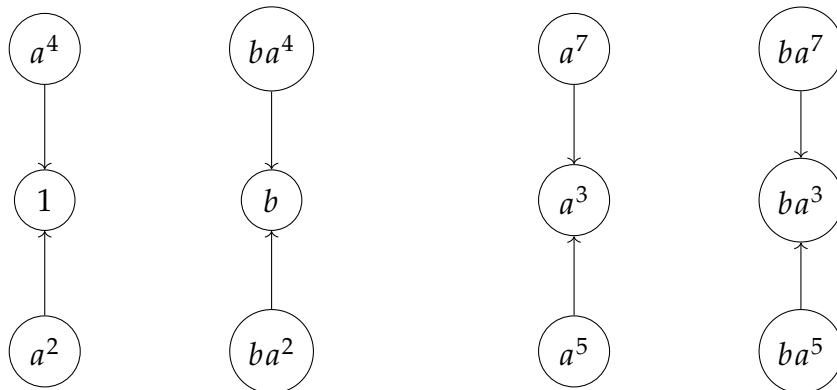
Exemplo 2.5.2. Seja $G = \mathbb{Z}/8\mathbb{Z}$ $f : G \rightarrow G$, $f(x) = 3x$. Então f é um automorfismo pois 3 é coprimo com 8. Usando notação de permutações nos símbolos $\{1, 2, 3, 4, 5, 6, 7, 8\}$, temos que $f = (13)(26)(57)$ e temos o seguinte grafo $\mathcal{G}(G, f)$:

Figura 2.16 : Grafo $\mathcal{G}(C_8, f)$

Exemplo 2.5.3. Tomemos $G = A_4$. O grupo de Klein $K_4 = \langle (12)(34), (13)(24) \rangle$ é um subgrupo normal de A_4 e $A_4/K_4 \cong C_3$ que é isomorfo ao subgrupo $\{1, (123), (132)\}$. Pelo teorema de isomorfismo, temos um endomorfismo $f : A_4 \rightarrow A_4$ de núcleo $\{1, (12)(34), (13)(24), (14)(23)\}$ e imagem $\{1, (123), (132)\}$. Seu grafo corresponde à:

Figura 2.17 : Grafo do endomorfismo de A_4

Exemplo 2.5.4. Seja $G = D_6$. Existe $H \trianglelefteq G$ tal que $H \cong C_3$. Tome, por exemplo, $H = \langle a^2 \rangle$ onde a é o gerador de ordem 6. O quociente $G/H \cong K_4$ o grupo de Klein que é isomorfo ao subgrupo $\langle a^3, b \rangle$ onde b é a involução de G . Temos então um endomorfismo $f : G \rightarrow G$ com grafo:

Figura 2.18 : Grafo do endomorfismo de D_6

Capítulo 3

Dinâmica em grupos abelianos

3.1 Preliminares

Nesse capítulo estudaremos a dinâmica da aplicação quadrada em grupos abelianos finitos. Em grupos abelianos, a aplicação quadrada é um endomorfismo, então o lema [2.5.1](#) garante que o grafo $\mathcal{G}(G, f)$ será a união disjunta de grafos da forma $\text{Cyc}(n_i, \mathcal{T})$, $i = 1, \dots, k$.

Nessa sessão e no resto do trabalho iremos assumir alguns conceitos e notações estudadas em cursos introdutórios de teoria dos números: Divisibilidade, congruências, e números primos, e a função φ de Euler. Também utilizaremos a noção de **ordem multiplicativa**:

Definição 3.1.1 (Ordem multiplicativa). Seja k um inteiro qualquer e n um número coprimo com k . Então a **ordem multiplicativa de k modulo n** , notada como $\text{ord}_n(k)$ é a ordem de k visto como um elemento do grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$, isto é, o menor inteiro positivo x tal que $k^x \equiv 1 \pmod{n}$. Definimos também $\text{ord}_1(k) = 1$ para todo k .

Exemplo 3.1.1. $\text{ord}_{27}(2) = 18$. De fato, $\varphi(27) = 18$. Podemos calcular, sempre módulo 27, que $2^2 \equiv 4$, $2^3 \equiv 8$, $2^6 \equiv 10$, $2^9 \equiv 26$, e portanto $2^{18} \equiv 1$.

Exemplo 3.1.2. $\text{ord}_{125}(32) = 20$. Temos que $\varphi(125) = 100$ e $(\mathbb{Z}/125\mathbb{Z})^* \cong \mathbb{Z}/100\mathbb{Z}$ é cíclico. Então $\text{ord}_{125}(32) | 100$. $32^{10} \equiv 124$, e $32^{20} \equiv 1$.

As notações utilizadas serão, quando possível, as mesmas de [\[13\]](#).

3.2 Grupos cíclicos

O primeiro resultado estabelecendo a estrutura de grafos para grupos cíclicos foi apresentado em [15], e também pode ser observado em [6], [13]. Os artigos de Rogers e Chou apresentavam um interesse em estudar corpos finitos. Se $\mathbb{F}$ é um corpo finito, $\mathbb{F} \setminus \{0\}$ é um grupo cíclico (Veja, por exemplo, [4], 15.3 Teorema 6), portanto o estudo da dinâmica de aplicações que preservam o 0 em corpos finitos se reduz ao estudo do mesmo em um grupo cíclico. Estaremos interessados na generalização do estudo dessa aplicação para outros grupos.

3.3 Grupos cíclicos de ordem ímpar

A partir da Proposição 2.5.1, temos que os grafos $\mathcal{G}(G, f)$, quando G é um grupo e f é um endomorfismo tem estrutura de uniões disjuntas de grafos da forma $\text{Cyc}(n_i, \mathcal{T})$. A menos que indiquemos o contrário, f será a aplicação quadrada no grupo, isto é $f(x) = x^2$ em notação multiplicativa, e $f(x) = 2x$ em notação aditiva. Como a aplicação $f(x) = x^2$ é um endomorfismo no caso onde G é cíclico, obtemos o primeiro resultado estabelecendo a estrutura de grafos. Vejamos alguns exemplos antes:

Exemplo 3.3.1. Seja $G = C_{15}$. Vamos tomar notação aditiva; nesse caso $f(x) = 2x$. Temos que $f(0) = 0$ pois f é um endomorfismo. Além disso, temos as seguintes sequências de aplicações:

$$\begin{aligned} 1 &\rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 1 \\ 3 &\rightarrow 6 \rightarrow 12 \rightarrow 9 \rightarrow 3 \\ 7 &\rightarrow 14 \rightarrow 13 \rightarrow 11 \rightarrow 7 \\ 5 &\rightarrow 10 \rightarrow 5 \end{aligned}$$

Temos então $\mathcal{G}(G, f)$ consiste na união disjunta de três 4-ciclos, um 2-ciclo e um 1-ciclo com a identidade

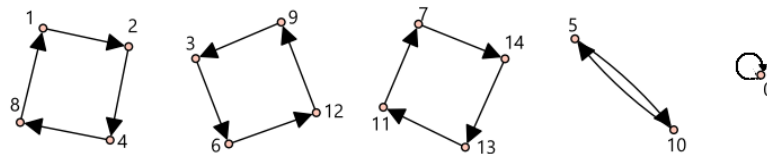


Figura 3.1 : Grafo do grupo C_{15} utilizando notação aditiva.

Exemplo 3.3.2. Seja $G = C_{21}$. Então temos as seguintes sequências de aplicações:

$$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow 11 \rightarrow 1$$

$$3 \rightarrow 6 \rightarrow 12 \rightarrow 3$$

$$5 \rightarrow 10 \rightarrow 20 \rightarrow 19 \rightarrow 17 \rightarrow 13 \rightarrow 5$$

$$7 \rightarrow 14 \rightarrow 7$$

$$9 \rightarrow 18 \rightarrow 15 \rightarrow 9$$

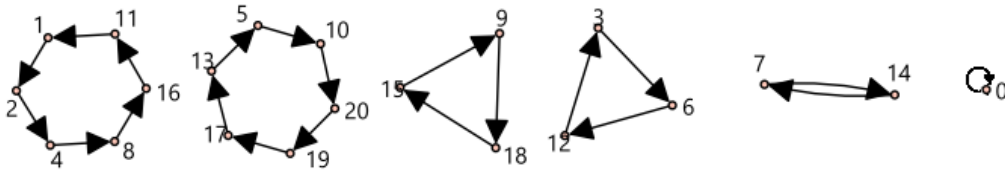


Figura 3.2 : Grafo do grupo C_{21} utilizando notação aditiva.

Proposição 3.3.1 ([15], Teorema 1). *Seja $G = C_n$ o grupo cíclico de ordem n ímpar. Seja $f : G \rightarrow G$, $f(x) = x^2$. Seja φ a função de Euler e $\text{ord}_k(2)$ a ordem multiplicativa de 2 modulo k . Então o grafo $\mathcal{G} = \mathcal{G}(G, f)$ é:*

$$\mathcal{G} = \bigoplus_{d|n} \frac{\varphi(d)}{\text{ord}_d(2)} \times \text{Cyc}(\text{ord}_d(2))$$

Demonstração. Como n é ímpar, f é um automorfismo de C_n , de onde segue que é uma permutação dos n símbolos de C_n e portanto seu grafo é uma união de ciclos.

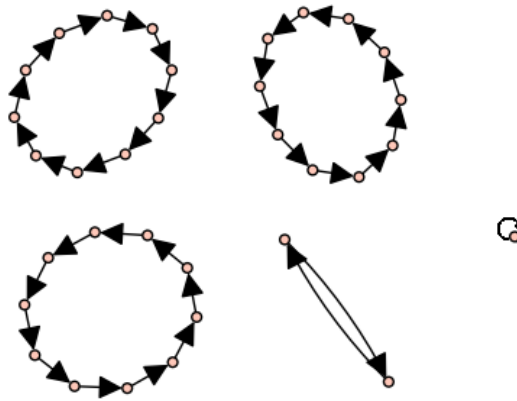
Seja $G = \bigcup_{d|n} G_d$ onde G_d é o subconjunto de elementos de ordem d em G . Temos que f permuta elementos de cada G_d entre si: de fato se $x \in G_d$ então

$$(f(x))^d = (x^2)^d = (x^d)^2 = 1$$

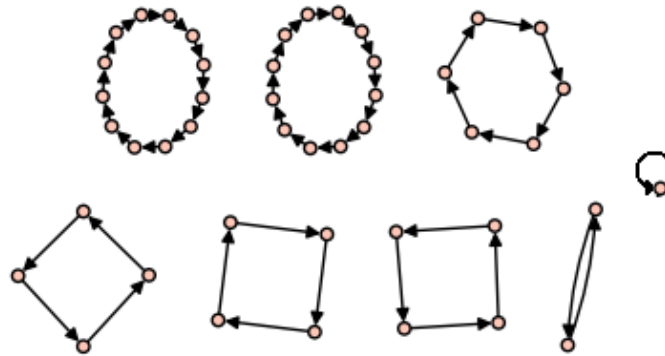
e se $o(x^2) < o(x)$ então $2|d$, absurdo pois d é ímpar.

Seja $x \in G_d$. Como f é uma permutação em G_d , temos que existe um menor ℓ tal que $f^\ell(x) = x^{2^\ell} = x$. Neste caso $d|2^\ell - 1$ e portanto $2^\ell \equiv 1 \pmod{d}$ isto é, $\text{ord}_d(2)|\ell$. Por minimalidade de ℓ , $\ell = \text{ord}_d(2)$. Segue que cada G_d é a união de ciclos de tamanho $\text{ord}_d(2)$. Como $|G_d| = \varphi(d)$, temos o resultado. $\square$

Exemplo 3.3.3. Seja $G = C_{33}$. O conjunto de divisores de 33 é $\{1, 3, 11, 33\}$ cujas imagens por φ são 1, 2, 10, 20, respectivamente. Temos também que $\text{ord}_1(2) = 1, \text{ord}_3(2) = 2, \text{ord}_{11}(2) = 10, \text{ord}_{33}(2) = 10$. Temos então um 2-ciclo, e três 10-ciclos, e a identidade.

Figura 3.3 : Grafo de C_{33} .

Exemplo 3.3.4. Seja $G = C_{45}$. Então o conjunto de divisores de 45 é $\{1, 3, 5, 9, 15, 45\}$. Suas imagens por φ são $\{1, 2, 4, 6, 8, 24\}$, respectivamente. Temos também que as ordens multiplicativas são $\text{ord}_1(2) = 1, \text{ord}_3(2) = 2, \text{ord}_5(2) = 4, \text{ord}_9(2) = 6, \text{ord}_{15}(2) = 4, \text{ord}_{45}(2) = 12$. Temos então um 2-ciclo, três 4-ciclos, um 6-ciclo, e dois 12-ciclos.

Figura 3.4 : Grafo de C_{45} .

3.4 Grupos cíclicos de ordem par

Podemos generalizar o resultado para grupos cíclicos de ordem qualquer. Isto se dá na proposição 3.4.1. Vejamos alguns exemplos antes:

Exemplo 3.4.1. Seja $G = C_{28}$. Em notação aditiva temos as seguintes sequências para a aplicação $f(x) = 2x$:

$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow 4$
 $3 \rightarrow 6 \rightarrow 12 \rightarrow 24 \rightarrow 20 \rightarrow 12$
 $5 \rightarrow 10 \rightarrow 20 \rightarrow 12 \rightarrow 24 \rightarrow 20$
 $7 \rightarrow 14 \rightarrow 0$
 $9 \rightarrow 18 \rightarrow 8 \rightarrow 16 \rightarrow 4 \rightarrow 8$
 $11 \rightarrow 22 \rightarrow 16 \rightarrow 4 \rightarrow 8 \rightarrow 16$
 $13 \rightarrow 26 \rightarrow 24 \rightarrow 20 \rightarrow 12 \rightarrow 24$
 $15 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow 4$
 $17 \rightarrow 6 \rightarrow 12 \rightarrow 24 \rightarrow 20 \rightarrow 12$
 $19 \rightarrow 10 \rightarrow 20 \rightarrow 12 \rightarrow 24 \rightarrow 20$
 $21 \rightarrow 14 \rightarrow 0$
 $23 \rightarrow 18 \rightarrow 8 \rightarrow 16 \rightarrow 4 \rightarrow 8$
 $25 \rightarrow 22 \rightarrow 16 \rightarrow 4 \rightarrow 8 \rightarrow 16$
 $27 \rightarrow 26 \rightarrow 24 \rightarrow 20 \rightarrow 12 \rightarrow 24$

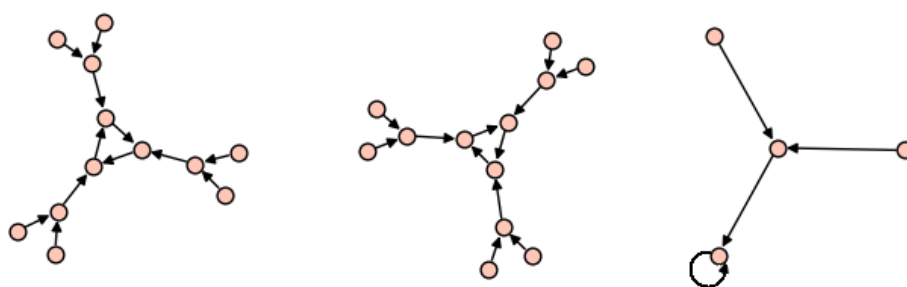


Figura 3.5 : Grafo de C_{28}

Exemplo 3.4.2. Seja $G = C_{30}$. Temos as seguintes sequências de aplicações:

$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow 2$
 $3 \rightarrow 6 \rightarrow 12 \rightarrow 24 \rightarrow 18 \rightarrow 6$
 $5 \rightarrow 10 \rightarrow 20 \rightarrow 10$
 $7 \rightarrow 14 \rightarrow 28 \rightarrow 26 \rightarrow 22 \rightarrow 14$
 $9 \rightarrow 18 \rightarrow 6 \rightarrow 12 \rightarrow 24 \rightarrow 18$
 $11 \rightarrow 22 \rightarrow 14 \rightarrow 28 \rightarrow 26 \rightarrow 22$
 $13 \rightarrow 26 \rightarrow 22 \rightarrow 14 \rightarrow 28 \rightarrow 26$
 $15 \rightarrow 0$
 $17 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow 2 \rightarrow 4$
 $19 \rightarrow 8 \rightarrow 16 \rightarrow 2 \rightarrow 4 \rightarrow 8$
 $21 \rightarrow 12 \rightarrow 24 \rightarrow 18 \rightarrow 6 \rightarrow 12$
 $23 \rightarrow 16 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16$
 $25 \rightarrow 20 \rightarrow 10 \rightarrow 20$
 $27 \rightarrow 24 \rightarrow 18 \rightarrow 6 \rightarrow 12 \rightarrow 24$
 $29 \rightarrow 28 \rightarrow 26 \rightarrow 22 \rightarrow 14 \rightarrow 28 \rightarrow 26$

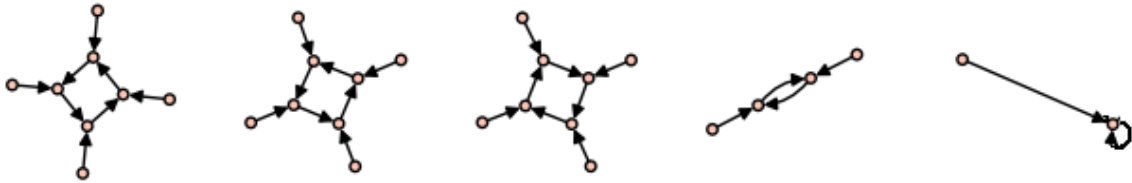


Figura 3.6 : Grafo de C_{30}

Proposição 3.4.1 ([15] Teorema 2). *Seja $G = C_n$ o grupo cíclico de ordem $n = 2^k m$, onde m é ímpar. Seja $f : G \rightarrow G$, $f(x) = x^2$. Então o grafo $\mathcal{G} = \mathcal{G}(G, f)$ é:*

$$\mathcal{G} = \bigoplus_{d|m} \frac{\varphi(d)}{\text{ord}_d(2)} \times \text{Cyc}(\text{ord}_d(2), \mathcal{T}^k).$$

Demonstração. Usaremos o fato que m é ímpar para escrever $C_n \cong C_{2^k} \times C_m$ e usaremos o isomorfismo natural $C_{2^k} \times C_m \cong \mathbb{Z}_{2^k} \oplus \mathbb{Z}_m = \overline{G}$ para escrever o grupo em notação aditiva. Neste caso, os elementos de $\overline{G}$ são da forma (x, y) , $x \in \mathbb{Z}_{2^k}, y \in \mathbb{Z}_m$. A

aplicação f em C_n possui uma aplicação equivalente $\bar{f}$ em $\bar{G}$, pois os grupos são isomorfos. $\bar{f}(x, y) = (2x, 2y)$ por definição. Iremos omitir as linhas em G e f por simplicidade.

Como $o(x)$ é uma potência de 2, temos que existe ℓ tal que $f^\ell(x, y) = (0, y')$. Por outro lado, como f aplica coordenada a coordenada, $(0, y')$ e $(0, y)$ estão no mesmo ciclo. Portanto basta definirmos quantos elementos de cada ordem estão em $\mathbb{Z}_{2^k}$, que nos darão a árvore conectada com o grafo já determinado de $\mathbb{Z}_m$.

Em um grupo de ordem 2^k , temos $\varphi(2) = 1$ elemento de ordem 2, $\varphi(4) = 2$ elementos de ordem 4, $\varphi(8) = 4$ elementos de ordem 8, e, em geral, $\varphi(2^k) = 2^k - 2^{k-1}$ elementos de ordem 2^k . Logo para cada elemento do cíclico C_m temos uma árvore binária acoplada. $\square$

Exemplo 3.4.3. Seja $G = C_{56}$. $56 = 2^3 \cdot 7$ e temos que $\varphi(7) = 6$, $ord_7(2) = 3$, portanto o grafo $\mathcal{G}(G, f)$ é $2 \times \text{Cyc}(3, \mathcal{T}^3) \oplus \text{Cyc}(1, \mathcal{T}^3)$. Note que a diferença entre esse grafo e o de C_{28} é a profundidade de cada árvore

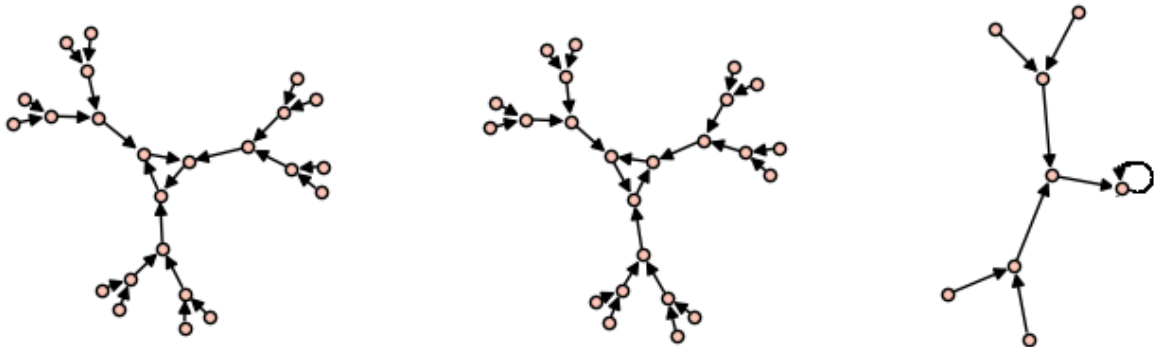
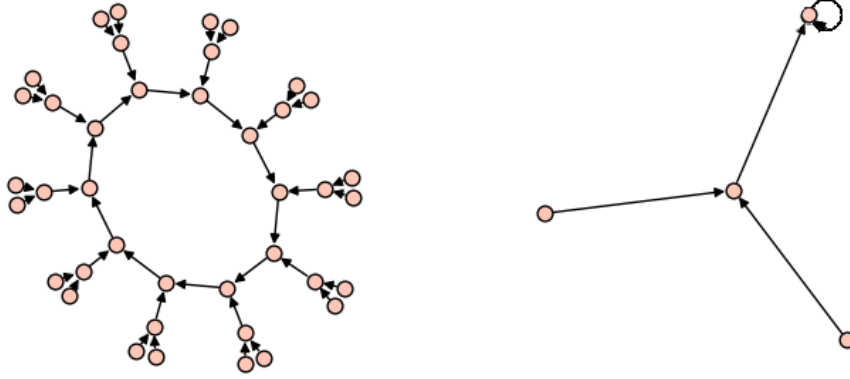


Figura 3.7 : Grafo de C_{56}

Exemplo 3.4.4. Seja $G = C_{44}$. Temos que $44 = 2^2 \cdot 11$. Como 11 é primo, o grafo de C_{11} é $\text{Cyc}(10) \oplus \text{Cyc}(1)$ e portanto o grafo $\mathcal{G}(G, f)$ é de $\text{Cyc}(10, \mathcal{T}^2) \oplus \mathcal{T}^2$.

Figura 3.8 : Grafo de C_{44}

3.5 Produtos Tensoriais e Árvores Elementares

Podemos agora estabelecer a estrutura do grafo $\mathcal{G}(G, f)$ onde G é um grupo abeliano qualquer. Isso se dá pelo fato do teorema de classificação de grupos abelianos finitos garantir que todo grupo abeliano finito é isomorfo ao produto direto de grupos cíclicos. Pelo Lema 2.4.2, podemos representar o grafo associado à um grupo abeliano finito como um produto tensorial de vários grafos. Essa representação é pouco conveniente, visto que produtos tensoriais de grafos são difíceis de representar e visualizar. Para obter uma representação mais conveniente, vamos estudar propriedades do produto tensorial, com o objetivo de obter representações mais simples deste.

Já vimos que $\text{Cyc}(k, \mathcal{T}) = \text{Cyc}(k) \otimes \mathcal{T}$. Por construção, temos:

Lema 3.5.1. *O produto tensorial de grafos possui as seguintes propriedades:*

1. É comutativo, isto é, $\mathcal{G}_1 \otimes \mathcal{G}_2$ é isomorfo a $\mathcal{G}_2 \otimes \mathcal{G}_1$
2. É distributivo sobre $\oplus$, isto é $\mathcal{G}_1 \otimes (\mathcal{G}_2 \oplus \mathcal{G}_3)$ é isomorfo a $(\mathcal{G}_1 \otimes \mathcal{G}_2) \oplus (\mathcal{G}_1 \otimes \mathcal{G}_3)$

Demonstração. As propriedades são consequências diretas da definição.

Seja $\mathcal{G}_i = (V_i, A_i)$, $i \in \{1, 2, 3\}$. Então $\mathcal{G}_1 \otimes \mathcal{G}_2 = (V_1 \times V_2, A_1 \times A_2) \cong (V_2 \times V_1, A_2 \times A_1) = \mathcal{G}_2 \otimes \mathcal{G}_1$, o que dá a propriedade 1.

Para a propriedade 2, $\mathcal{G}_1 \otimes (\mathcal{G}_2 \oplus \mathcal{G}_3) = (V_1 \times (V_2 \cup V_3), A_1 \times (A_2 \cup A_3)) \cong (V_1 \times V_2 \cup V_1 \times V_3, A_1 \times A_2 \cup A_1 \times A_3)$ □

Vamos então estudar o produto tensorial de ciclos e de árvores:

Lema 3.5.2. *Sejam $r_1, \dots, r_k$ inteiros positivos. Então temos:*

$$\bigotimes_{i=1}^k \text{Cyc}(r_i) = \frac{r_1 r_2 \cdots r_k}{\text{mmc}(r_1, \dots, r_k)} \times \text{Cyc}(\text{mmc}(r_1, \dots, r_k))$$

Demonstração. Seja $s_i : \mathbb{Z}_{r_i} \rightarrow \mathbb{Z}_{r_i}$, $s_i(x) = x + 1$. Então $\text{Cyc}(r_i) = (\mathbb{Z}_{r_i}, s_i)$ e pelo Lema 2.4.2, temos que $\bigotimes_{i=1}^k \text{Cyc}(r_i) = (\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_k}, s_1 \times \cdots \times s_k)$. Este grafo é a união de ciclos disjuntos pois $S = s_1 \times \cdots \times s_k$ é uma bijeção.

Vistos como subconjuntos, cada um desses ciclos corresponde com uma classe lateral de $H = \langle (1, 1, \dots, 1) \rangle$ no grupo $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_k}$; De fato, se $(a_1, \dots, a_k)$, seja r o maior número de elementos entre $a_1, \dots, a_k$ que são iguais entre si (r pode ser 1.). Então esse número, que determina as classes laterais de H , é preservado por S . Essas classes laterais possuem $|H| = \text{mmc}(r_1, \dots, r_k)$ elementos. $\square$

Exemplo 3.5.1. Considere os ciclos $C_1 = \text{Cyc}(8)$ e $C_2 = \text{Cyc}(12)$. Então $C_1 \otimes C_2 = 4 \times \text{Cyc}(24)$. Note a diferença com $C_1 \oplus C_2 = \text{Cyc}(8) \oplus \text{Cyc}(12)$

Exemplo 3.5.2. Vamos estudar o produto de ciclos isomorfos. Se $r_1 = r_2 = \cdots = r_k = r$, então:

$$\bigotimes_{i=1}^k \text{Cyc}(r_i) = \frac{r^k}{r} \times \text{Cyc}(r) = r^{k-1} \times \text{Cyc}(r).$$

Para estudar o produto tensorial de árvores, vamos antes definir uma família de árvores mais geral que as árvores binárias: as **árvores elementares**. Na definição abaixo, lembre a definição de árvores geradas $\langle \mathcal{G} \rangle$ em 2.3.6 e que $k \times \mathcal{G} = \bigoplus_{i=1}^k \mathcal{G}$

Definição 3.5.3 (Árvore elementar). Seja $\mathbf{v} = (v_1, \dots, v_d)$ uma sequência não crescente de inteiros positivos, isto é $v_1 \geq v_2 \geq \cdots \geq v_d \geq 1$. Definimos a **árvore elementar** $\mathcal{T}_{\mathbf{v}}$ pela relação recursiva abaixo:

$$\begin{cases} \mathcal{T}_{\mathbf{v}}^0 = \bullet, \text{ (o grafo com um só vértice);} \\ G_{\mathbf{v}}^k = v_k \times \mathcal{T}_{\mathbf{v}}^{k-1} \oplus \bigoplus_{i=1}^{k-1} (v_i - v_{i+1}) \times \mathcal{T}_{\mathbf{v}}^{i-1}; \text{ e } \mathcal{T}_{\mathbf{v}}^k = \langle G_{\mathbf{v}}^k \rangle, \text{ Para } 1 \leq k < d \\ G_{\mathbf{v}} = (v_d - 1) \times \mathcal{T}_{\mathbf{v}}^{d-1} \oplus \bigoplus_{i=1}^{d-1} (v_i - v_{i+1}) \times \mathcal{T}_{\mathbf{v}}^{i-1}; \text{ e } \mathcal{T}_{\mathbf{v}} = \langle G_{\mathbf{v}} \rangle \end{cases}$$

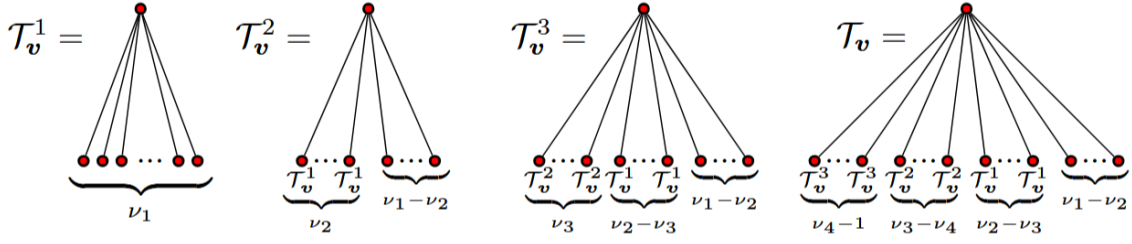


Figura 3.9 : Construção de uma árvore elementar onde $d = 4$. Imagem obtida de [13]

Vejamos alguns exemplos de árvores elementares para construir uma intuição sobre a construção acima. Primeiramente note que se uma sequência é da forma $\mathbf{v} = (v_1, \dots, v_k, 1, \dots, 1)$, então a árvore elementar de $\mathbf{v}$ é a mesma que a árvore elementar de $\tilde{\mathbf{v}} = (v_1, \dots, v_k)$. As duas sequências são ditas **equivalentes**. Outra intuição para o fato que adicionar sequências de 1 não altera a árvore pode ser vista no resultado abaixo:

Lema 3.5.4. *Seja $\mathbf{v} = (v_1, \dots, v_d)$. Então a árvore elementar $\mathcal{T}_{\mathbf{v}}$ possui $\prod_{i=1}^d v_i$ vértices.*

Demonstração. Vamos mostrar que para $1 \leq k < d$, a quantidade de vértices de $\mathcal{T}_{\mathbf{v}}^k$, denotada $|V_k|$, é $1 + v_1 + v_1 v_2 + \dots + v_1 \dots v_k$. Por indução, suponha que o resultado valha para to índice menor que k . Então o número de vértices em $G_{\mathbf{v}}^k$ é:

$$v_k(1 + v_1 + v_1 v_2 + \dots + v_1 v_2 \dots v_{k-1}) + \sum_{i=1}^{k-1} (v_i - v_k)(1 + v_1 + \dots + v_1 \dots v_{i-1})$$

Seja $\xi_0 = 1$ e $\xi_n = v_1 \dots v_n$. Então temos:

$$\begin{aligned} & v_k(\xi_0 + \xi_1 + \dots + \xi_{k-1}) + \sum_{i=1}^{k-1} (v_i - v_k)(\xi_0 + \xi_1 + \dots + \xi_{i-1}) = \\ & \xi_0(v_k + v_1 - v_2 + v_2 - v_3 + \dots + v_{k-1} - v_k) + \\ & \xi_1(v_k + v_2 - v_3 + v_3 - v_4 + \dots + v_{k-1} - v_k) + \\ & \dots + \xi_{k-2}(v_k + v_{k-1} - v_k) + \xi_{k-1}(v_k) = \\ & = \xi_0 v_1 + \xi_1 v_2 + \dots + \xi_{k-1} v_k = v_1 + v_1 v_2 + \dots + v_1 \dots v_k \end{aligned}$$

E como $|V_k|$ possui uma raiz a mais que $G_{\mathbf{v}}^k$, temos o que queríamos.

Agora um calculo similar mostra que:

$$1 + (v_d - 1)(1 + v_1 + \cdots + v_1 \dots v_{d-1}) + \sum_{i=1}^{d-1} (v_i - v_{i+1})(1 + v_1 + \cdots + v_1 \dots v_{i-1}) = v_1 \dots v_d$$

□

Um exemplo já visto anteriormente de árvores elementares são as árvores binárias: Na notação anterior a árvore binária $\mathcal{T}^k$ corresponde agora com a árvore elementar $\mathcal{T}_{\mathbf{v}}$ onde $\mathbf{v} = (2, 2, \dots, 2)$ é uma sequência de comprimento $d = k$, que possui 2^k vértices pelo lema acima.

Exemplo 3.5.3. Consideremos $\mathcal{T}_{\mathbf{v}}$ onde $\mathbf{v} = (3, 2, 2)$. Iremos construir a árvore pela definição. Temos que $d = 3$ e $v_1 = 3$, $v_2 = v_3 = 2$.

$G_{\mathbf{v}}^1 = 3 \times \bullet$, $\mathcal{T}_{\mathbf{v}}^1 \langle G_{\mathbf{v}}^1 \rangle =$. Temos no 1o passo:



Figura 3.10 : Grafo $G_{\mathbf{v}}^1$ à esquerda e $\mathcal{T}_{\mathbf{v}}^1$ à direita

para o 2o passo temos $G_{\mathbf{v}}^2 = 2 \times \mathcal{T}_{\mathbf{v}}^1 \oplus (3 - 2) \times \bullet$ e $\mathcal{T}_{\mathbf{v}}^2 = \langle G_{\mathbf{v}}^2 \rangle$.

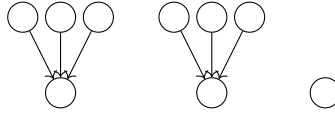


Figura 3.11 : Grafo $G_{\mathbf{v}}^2$

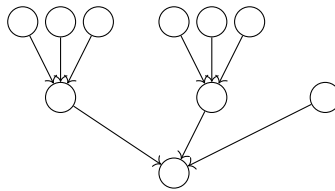
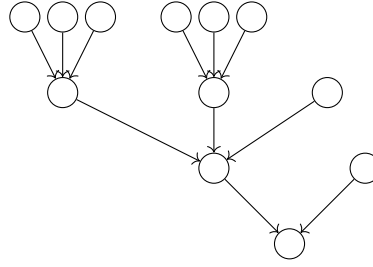


Figura 3.12 : Grafo $\mathcal{T}_{\mathbf{v}}^2$

Para o passo final temos que $G_{\mathbf{v}} = \mathcal{T}_{\mathbf{v}}^2 \oplus \mathcal{T}_{\mathbf{v}}^0$ e $\mathcal{T}_{\mathbf{v}}$ é a árvore gerada por essas duas árvores:

Figura 3.13 : Grafo $\mathcal{T}_v$

Definição 3.5.5. Definimos o produto $\mathbf{uv}$ como sendo o produto coordenada a coordenada. Se as sequências tem comprimentos diferentes, então trocamos a de comprimento menor por uma equivalente de mesmo comprimento. Simbolicamente: Seja $\mathbf{u} = (u_1, \dots, u_k)$ e $\mathbf{v} = (v_1, \dots, v_\ell)$ com $k \leq \ell$. Então $\mathbf{uv} = (u_1v_1, \dots, u_kv_k, v_{k+1}, \dots, v_\ell)$.

Temos o seguinte resultado sobre o produto tensorial de árvores elementares:

Proposição 3.5.6 ([12], Proposição 2.10). *Dadas sequências $\mathbf{v}$ e $\mathbf{u}$ não crescentes e positivas, temos que $\mathcal{T}_v \otimes \mathcal{T}_u = \mathcal{T}_{vu}$*

3.6 Grupos Abelianos

Podemos agora classificar o teorema de classificação para grafos gerados por grupos abelianos. Vamos introduzir notações: Para uma sequência $\mathbf{d} = (d_1, \dots, d_k)$ iremos notar $\mathbf{d}|\mathbf{w}$ para indicar que $d_i|w_i, \forall i$; $\varphi(\mathbf{d}) = \prod_i \varphi(d_i)$ e $o_{\mathbf{d}}(2) = \text{mmc}\{\text{ord}_{d_i}(2), 1 \leq i \leq k\}$.

Teorema 3.6.1 ([13] Proposição 2.7). *Seja G um grupo abeliano, $f : G \rightarrow G, f(x) = x^2$ e escreva $G = C_{r_1} \times \dots \times C_{r_k}$, um produto de grupos cíclicos. Tome $r_i = v_i w_i$ onde w_i é o maior divisor de r_i coprimo com 2 (equivalentemente, v_i é a maior potência de 2 que divide r_i). Escreva $\mathbf{v} = (v_1, \dots, v_k)$ e $\mathbf{w} = (w_1, \dots, w_k)$. Seja $v_i = 2^{\ell_i}$ e $\mathbf{v}_i = (2, 2, \dots, 2)$ uma sequência de comprimento ℓ_i . Seja $\mathbf{v} = \prod_{i=1}^k \mathbf{v}_i$.*

Então, o grupo G possui $\prod_{i=1}^k w_i$ elementos em ciclos, e o grafo funcional $\mathcal{G} = \mathcal{G}(G, f)$ é dado por:

$$\mathcal{G} = \bigoplus_{\mathbf{d}|\mathbf{w}} \frac{\varphi(\mathbf{d})}{o_{\mathbf{d}}(2)} \times \text{Cyc}(o_{\mathbf{d}}(2), \mathcal{T}_v) \quad (3.1)$$

Demonstração. Suponha que a equação 3.1 é verdadeira. Neste caso o número de elementos em ciclos é

$$\sum_{\mathbf{d}|\mathbf{w}} \frac{\varphi(\mathbf{d})}{o_{\mathbf{d}}(2)} \times o_{\mathbf{d}}(2) = \sum_{\mathbf{d}|\mathbf{w}} \varphi(\mathbf{d})$$

Ou seja:

$$\sum_{\mathbf{d}|\mathbf{w}} \prod_{d_i} \varphi(d_i) = \prod_{i=1}^k \sum_{d_i|w_i} \varphi(d_i) = \prod_{i=1}^k w_i$$

Para provar a fórmula, primeiro tomemos a equação do grafo como um produto de grupos cíclicos:

$$\mathcal{G} = \bigotimes_{i=1}^k \mathcal{G}(C_{r_i}, f) = \bigotimes_{i=1}^k \bigoplus_{d_i|w_i} \frac{\varphi(d_i)}{\text{ord}_{d_i}(2)} \times \text{Cyc}(\text{ord}_{d_i}(2), \mathcal{T}_{v_i})$$

Usando comutatividade e distributividade do produto tensorial, podemos rearranjar os termos e obter:

$$\mathcal{G} = \bigoplus_{\mathbf{d}|\mathbf{w}} \bigotimes_{i=1}^k \frac{\varphi(d_i)}{\text{ord}_{d_i}(2)} \times \text{Cyc}(\text{ord}_{d_i}(2), \mathcal{T}_{v_i})$$

Agora utilizando as fórmulas de produto tensorial obtidas em 3.5.2 e 3.5.6, temos:

$$\begin{aligned} \mathcal{G} &= \bigoplus_{\mathbf{d}|\mathbf{w}} \left(\prod_{i=1}^k \frac{\varphi(d_i)}{\text{ord}_{d_i}(2)} \right) \times \left(\bigotimes_{i=1}^k \text{Cyc}(\text{ord}_{d_i}(2)) \right) \otimes \left(\bigotimes_{i=1}^k \mathcal{T}_{v_i} \right) = \\ &= \bigoplus_{\mathbf{d}|\mathbf{w}} \frac{\varphi(\mathbf{d})}{o_{\mathbf{d}}(2)} \times \text{Cyc}(o_{\mathbf{d}}(2), \mathcal{T}_{\mathbf{v}}) \end{aligned}$$

□

Exemplo 3.6.1. Seja $G = C_2 \times C_4 \times C_3 \times C_5$ um grupo abeliano de ordem 120. Podemos escrever $G = C_2 \times C_{60}$ utilizando os isomorfismos bem conhecidos de grupos abelianos. temos então $r_1 = 2 = 2 \cdot 1 = v_1 w_1$ e $r_2 = 60 = 4 \cdot 15 = r_2 w_2$. Temos que $v_1 = (2)$, $v_2 = (2, 2)$, e $\mathbf{v} = (4, 2)$. $\mathbf{w} = (1, 15)$, cujos divisores $\mathbf{d}$ são $\{(1, 1), (1, 3), (1, 5), (1, 15)\}$. Para cada um temos os valores de φ e o : $\{1, 2, 4, 8\}$, $\{1, 2, 4, 4\}$, ou seja temos que $\left\{ \frac{\varphi(\mathbf{d})}{o_{\mathbf{d}}(2)} : \mathbf{d}|\mathbf{w} \right\} = \{1, 1, 1, 2\}$. Temos então que:

$$\begin{aligned} \mathcal{G} &= \text{Cyc}(1, \mathcal{T}_{(4,2)}) \oplus \text{Cyc}(2, \mathcal{T}_{(4,2)}) \oplus \text{Cyc}(4, \mathcal{T}_{(4,2)}) \oplus 2 \times \text{Cyc}(4, \mathcal{T}_{(4,2)}) = \\ &= \mathcal{T}_{(4,2)} \oplus \text{Cyc}(2, \mathcal{T}_{(4,2)}) \oplus 3 \times (4, \mathcal{T}_{(4,2)}) \end{aligned}$$

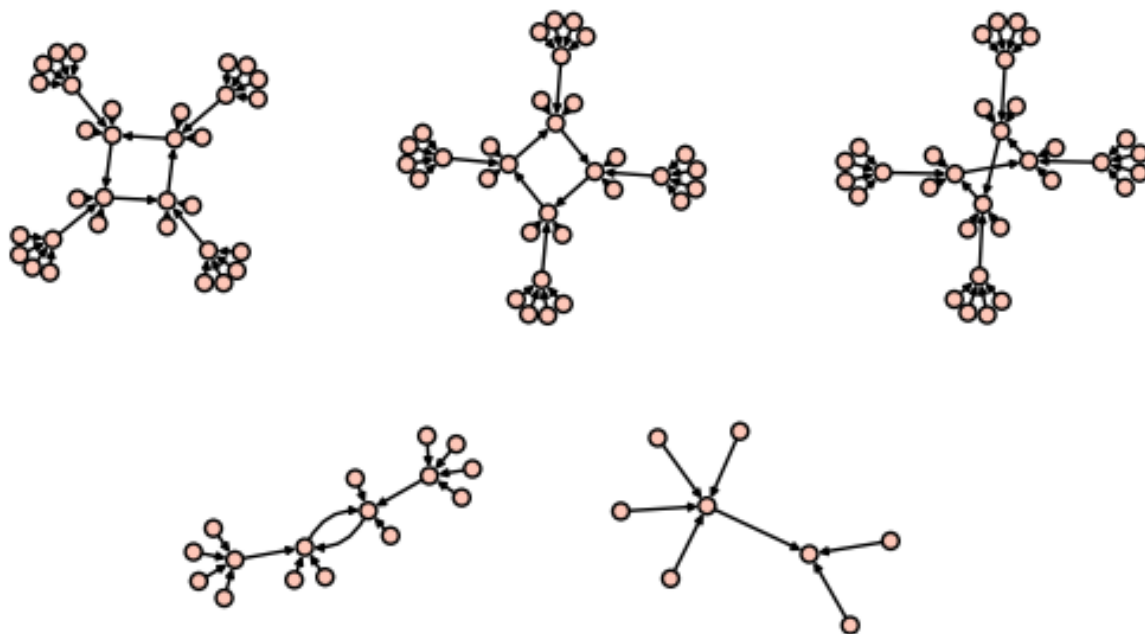


Figura 3.14 : Grafo do grupo abeliano $C_2 \times C_{60}$. Laço na identidade não representado por clareza visual.

Capítulo 4

Alguns grupos não abelianos

Nesse capítulo iremos aplicar resultados do Capítulo 3, generalizando para grupos não abelianos. Nessa parte do trabalho o nosso enfoque na dinâmica da aplicação $f(x) = x^2$, $\forall x \in G$ irá se provar valiosa: Se x é um involução em G , temos que $f(x) = 1$. Portanto, se G é um grupo possuindo um subgrupo $N \trianglelefteq G$ normal cíclico tal que G/N possui apenas involuções ou é um 2-grupo de ordem pequena, o grafo associado terá uma estrutura próxima da estrutura do grafo associado ao grupo cíclico N . O primeiro exemplo desse fenômeno que iremos estudar são grupos Diedrais: Tais grupos possuem um subgrupo normal cíclico de índice 2, e portanto para todo $x \in G$, pelo menos um elemento do par (x, x^2) estará no subgrupo cíclico normal.

Salvo menção contrária, os resultados desse capítulo foram obtidos pelo autor. Por uma questão de completude e reconhecimento alguns dos grafos funcionais de alguns dos grupos estudados aqui já foram estudados em trabalhos como [13], em particular em grupos de flores, estudados na seção 3 deste artigo; a abordagem utilizada nesta dissertação distingue-se na análise baseada na existência de subgrupos maximais cíclicos.

Iremos introduzir uma nova notação:

Definição 4.0.1. Seja $\mathcal{T}$ uma árvore direcionada. Denotaremos por $\mathcal{T}^\backslash$ a floresta gerada eliminando a raiz de $\mathcal{T}$, isto é, $\langle \mathcal{T}^\backslash \rangle = (\langle \mathcal{T} \rangle)^\backslash = \mathcal{T}$. A composição de operações, nos casos onde a composição é bem definida, isto é, quando $\mathcal{T}^\backslash$ é uma árvore, usará notação usual: $\mathcal{T}^{\backslash\backslash} = (\mathcal{T}^\backslash)^\backslash$

Exemplo 4.0.1.

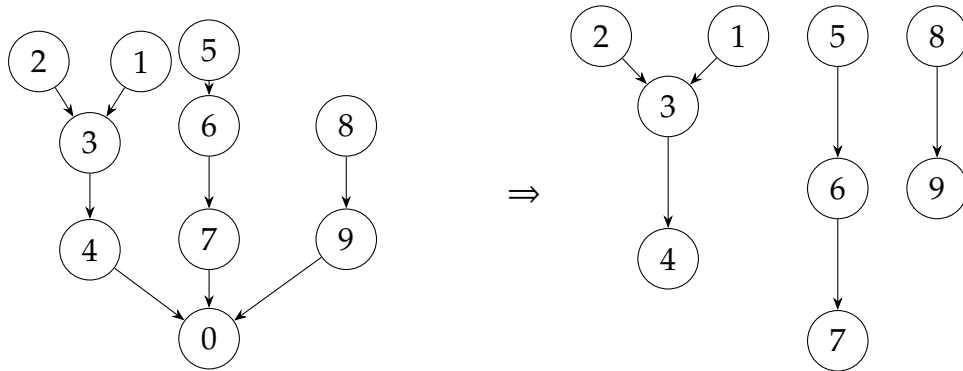


Figura 4.1 : A floresta à direita é gerada eliminando a raiz da árvore à esquerda

4.1 Grupos Diedrais

Uma vantagem do foco dado nesse trabalho à aplicação $f(x) = x^2$ é que involuções - elementos do grupo de ordem 2 - são levados para a identidade. Essa vantagem será ilustrada nos exemplos abaixo, e depois generalizada na proposição:

Exemplo 4.1.1. Seja $D_3 = \langle a, b : a^3, b^2, (ab)^2 \rangle$ o grupo diedral de ordem 6. Então pela proposição 3.4.1, sabemos que o grafo do subgrupo $\langle a \rangle$ é isomorfo a $\text{Cyc}(1) \oplus \text{Cyc}(2)$. Todos os outros elementos são involuções, e portanto são levados à identidade. Note também que o grafo é isomorfo à o exemplo 2.5.1 do grup S_3 , acima. Isto ocorre pois os grupos são isomorfos.

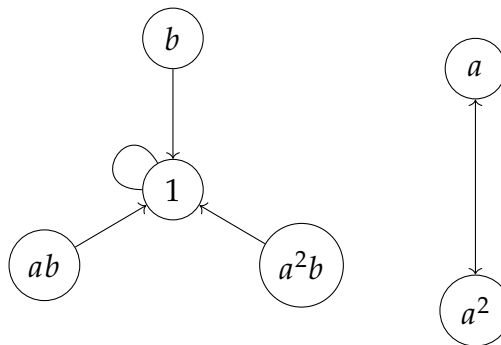


Figura 4.2 : Grafo (D_3, f)

Observação 4.1.1. Nesse capítulo, em geral não representaremos os laços no vértice correspondendo com a identidade do grupo para evitar poluição visual.

Exemplo 4.1.2. Seja $D_4 = \langle a, b : a^4, b^2, (ab)^2 \rangle$ o grupo diedral de ordem 8. Então pela proposição 3.4.1, sabemos que o grafo do subgrupo $\langle a \rangle$ é isomorfo a $\mathcal{T}_{(2,2)}$. Todos os outros elementos são involuções, e portanto são levados à identidade.

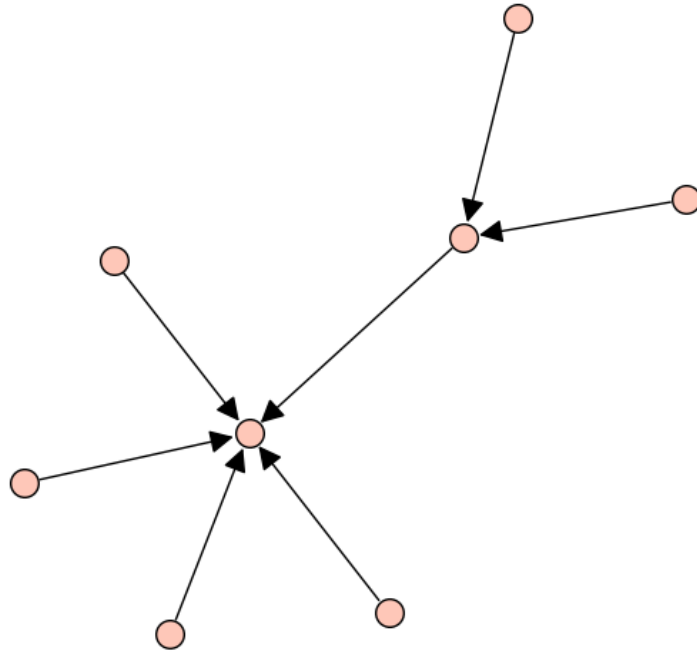


Figura 4.3 : Grafo (D_4, f)

Exemplo 4.1.3. Seja $D_5 = \langle a, b : a^5, b^2, (ab)^2 \rangle$ o grupo diedral de ordem 10. Então pela proposição 3.4.1, sabemos que o grafo do subgrupo $\langle a \rangle$ é isomorfo a $Cyc(1) \oplus Cyc(4)$. Todos os outros elementos são involuções, e portanto são levados à identidade.

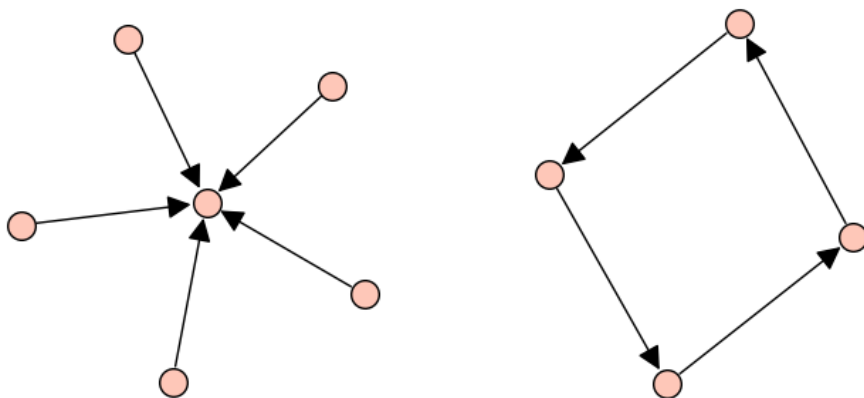


Figura 4.4 : Grafo (D_5, f)

Proposição 4.1.2. *Seja $G = D_n = \langle a, b : a^n, b^2, (ab)^2 \rangle$ o grupo diedral de ordem $2n$, $f : G \rightarrow G$, $f(x) = x^2$. Se $n = 2^k m$, com m ímpar e $\mathbf{v} = (2, 2, \dots, 2)$ de comprimento k , então o grafo $\mathcal{G} = \mathcal{G}(G, f)$ é dado por:*

$$\mathcal{G} = \mathcal{T}_1 \oplus \bigoplus_{1 \neq d|m} \frac{\varphi(d)}{\text{ord}_d(2)} \times \text{Cyc}(\text{ord}_d(2), \mathcal{T}_{\mathbf{v}})$$

Onde $\mathcal{T}_1 = \langle \mathcal{T}_{\mathbf{v}} \setminus \oplus (n \times \text{Cyc}(1)) \rangle$ é a árvore binária $\mathcal{T}^k = \mathcal{T}_{\mathbf{v}}$, $\mathbf{v} = (2, 2, \dots, 2)$ com n vértices adicionais conectados à raiz.

Demonstração. G possui subgrupo normal $\langle a \rangle$ de índice 2, e portanto podemos particionar G como $\langle a \rangle \cup b \langle a \rangle$. Nessa partição, todos os n elementos de $b \langle a \rangle$ tem ordem 2 e portanto o grafo correspondente à restrição de f em $b \langle a \rangle$ é a árvore com n vértices conectados à uma raiz (a identidade): $\mathcal{T}_{(n+1)}$. Os outros elementos estão em $\langle a \rangle$, um grupo cíclico de ordem n , e portanto o grafo será como na proposição 3.4.1, exceto na componente conexa do vértice 1. $\square$

O grupo diedral D_n é, de um certo modo, "próximo" do grupo cíclico C_n , pois é a extensão de C_n por C_2 . Como involuções do grupo possuem estrutura simples no grafo $\mathcal{G}(G, f)$, a estrutura do grafo é bem próxima da estrutura do grafo em grupos cíclicos.

4.2 Grupos Quatérnios Generalizados

O grupo quatérnio generalizado de ordem $4n$ é o grupo:

$$Q_{4n} = \langle a, b : a^n = b^2, a^{2n} = 1, a^b = a^{-1} \rangle$$

Alguns resultados sobre essa família podem ser vistos em [9] 2.5. Todo elemento de Q_{4n} pode ser escrito da forma $a^i b^j$ com $0 \leq i \leq 2n - 1$ e $0 \leq j \leq 1$. Temos que $(a^i b)^2 = a^i b a^i b = a^i b a^i b^{-1} b^2 = a^i a^{-i} b^2 = b^2 = a^n$, portanto o grafo de Q_{4n} é muito próximo do grafo de C_{2n} . A diferença ocorre com os $2n$ elementos na classe lateral $b \langle a \rangle$; todos eles são levados para o vértice de a^n , o único vértice conectado com 1. Visto de outra forma, é um grafo similar ao de D_{2n} , porém com vértices conectados a a^n em vez de 1.

Exemplo 4.2.1. Vamos analisar os grafos de Q_8 , Q_{12} , e Q_{20} . Temos subgrupos cíclicos maximais de ordens 4, 6, e 10 respectivamente, cujos grafos serão isomórficos a

$\mathcal{T}_{(2,2)}, \mathcal{T}_{(2)} \oplus Cyc(2, \mathcal{T}_{(2)})$ e $\mathcal{T}_{(2)} \oplus Cyc(4, \mathcal{T}_{(2)})$ respectivamente. Em todos os casos, o grupo cíclico possui ordem par, e portanto existe um elemento de ordem 2. Em cada caso, todos os outros vértices se conectam com o elemento de ordem 2. Temos então os seguintes grafos:

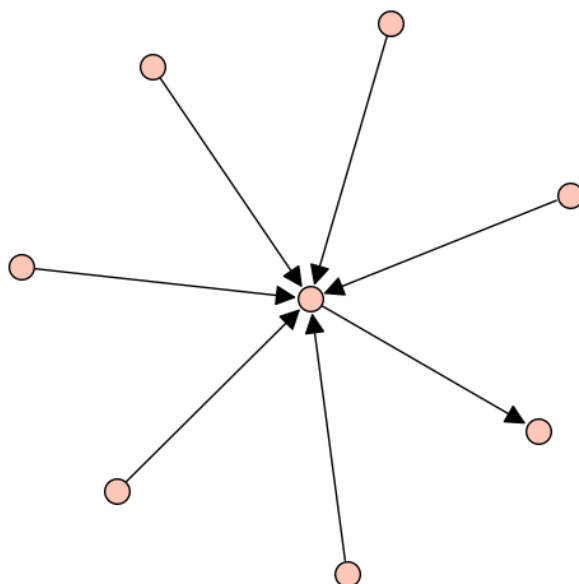


Figura 4.5 : Grafo (Q_8, f)

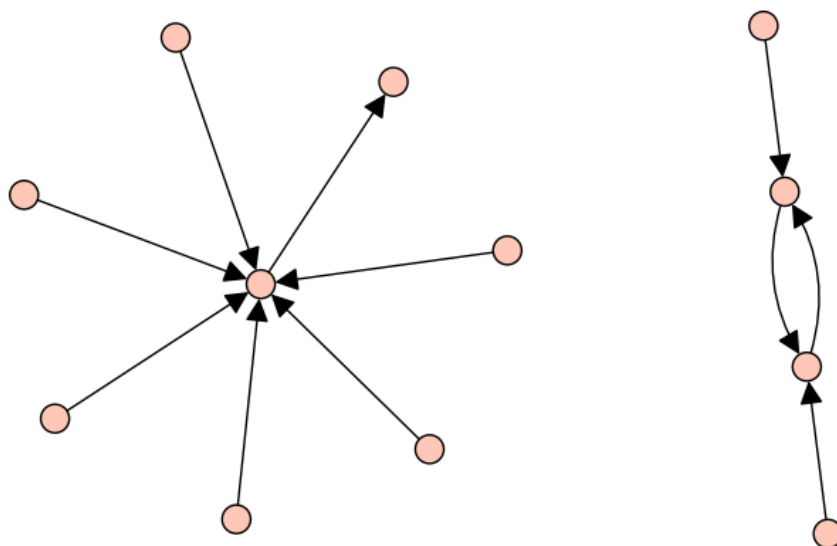
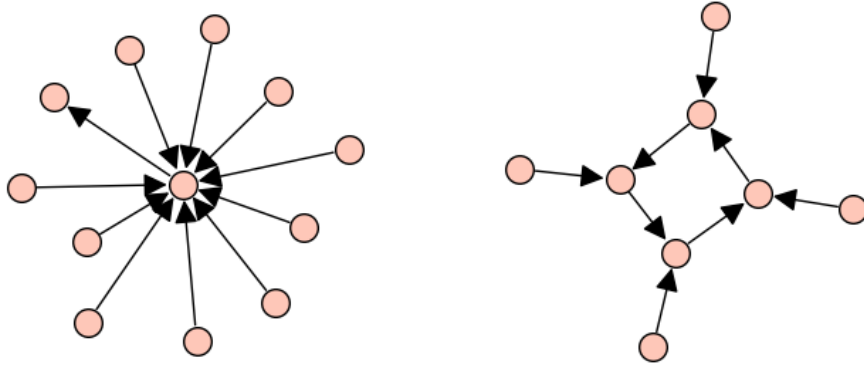


Figura 4.6 : Grafo (Q_{12}, f)

Figura 4.7 : Grafo (Q_{20}, f)

Proposição 4.2.1. *Seja $G = Q_{4n}$, e $f : G \rightarrow G$, $f(x) = x^2$. Tome também $2n = 2^k m$ e $\mathcal{G}_0$ o grafo dado por:*

$$\mathcal{G}_0 = \bigoplus_{d|m} \frac{\varphi(d)}{\text{ord}_d(2)} \times \text{Cyc}(\text{ord}_d(2), \mathcal{T}^k)$$

Isto é, o grafo correspondente ao grupo cíclico C_{2n} . A componente conexa da identidade no grafo é $\mathcal{T}^k = \mathcal{T}_0$. Seja $\mathcal{T}_1 = \left\langle \left\langle \mathcal{T}_0^{\setminus \setminus} \oplus 2n \times \text{Cyc}(1) \right\rangle \right\rangle$ Então o grafo $\mathcal{G} = \mathcal{G}(G, f)$ é dado por:

$$\mathcal{G} = \mathcal{T}_1 \oplus \bigoplus_{1 \neq d|m} \frac{\varphi(d)}{\text{ord}_d(2)} \times \text{Cyc}(\text{ord}_d(2), \mathcal{T}^k)$$

Demonstração. A maior parte da demonstração foi discutida no parágrafo anterior. Basta mostrar que $\mathcal{T}_1$ é o grafo que precisamos. De fato, para os vértices que estão em $\langle a \rangle$, a combinação de duas operações do tipo $\setminus$ e $\langle \rangle$ se cancelam, não alterando a estrutura da árvore. Para os outros $2n$ vértices introduzidos, eles estarão conectados ao único vértice conectado à raiz, como requerido. $\square$

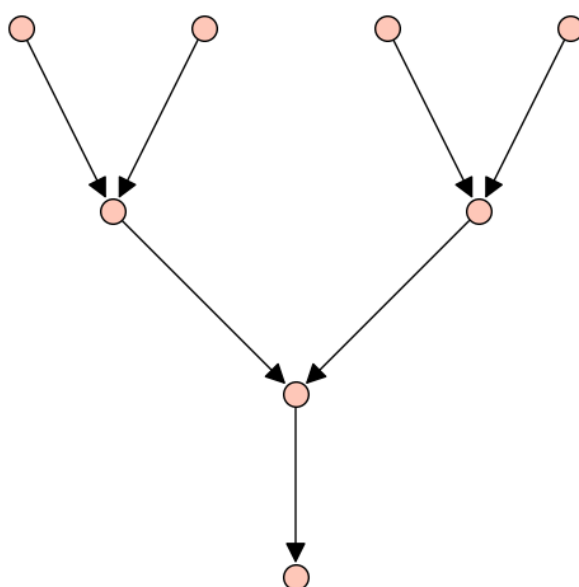
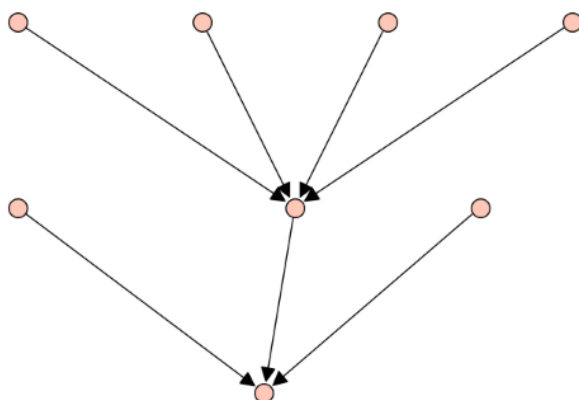
4.3 2-grupos

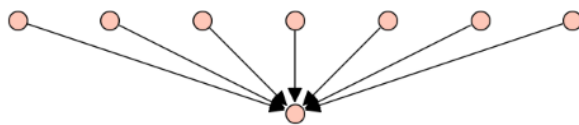
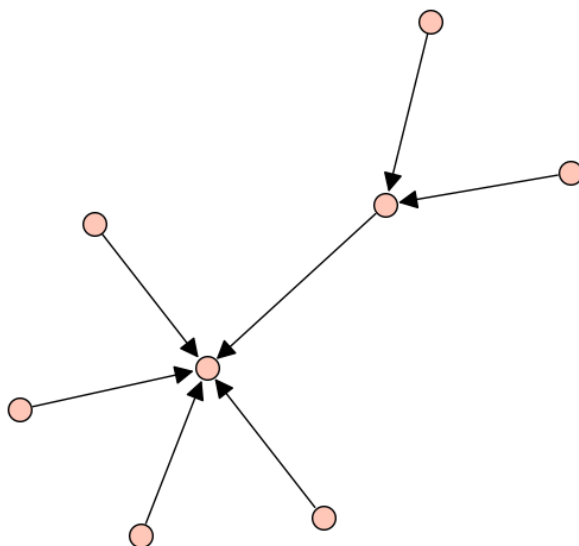
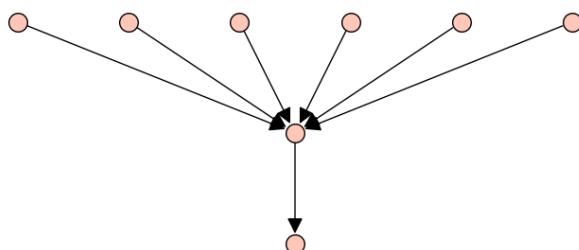
Lembramos que um p -grupo finito é um grupo cuja ordem é uma potência de um primo p . O estudo de p -grupos é uma área extensa e profunda na Teoria de Grupos. Para o nosso interesse, um tipo especial de p -grupos se destaca: os 2-grupos, cuja ordem é uma potência de 2.

O grafo funcional de um 2-grupo é sempre uma única árvore pois todos os elementos tem como ordem uma potência de 2. Abaixo temos, por exemplo, os diferentes grafos dos 5 grupos de ordem 8:

Grupo	Árvore
C_8	$\mathcal{T}_{(2,2,2)}$
$C_4 \times C_2$	$\mathcal{T}_{(4,2)}$
$C_2 \times C_2 \times C_2$	$\mathcal{T}_{(8)}$
D_4	$\langle 4 \times \mathcal{T}_{(1)} \oplus \mathcal{T}_{(3)} \rangle$
Q_8	$\langle \mathcal{T}_{(7)} \rangle$

Tabela 4.1 : Os grafos dos grupos de ordem 8

Figura 4.8 : Grafo do grupo C_8 Figura 4.9 : Grafo do grupo $C_4 \times C_2$

Figura 4.10 : Grafo do Grupo C_2^3 Figura 4.11 : Grafo do grupo D_4 Figura 4.12 : Grafo do grupo Q_8

4.4 2-grupos com subgrupo cíclico maximal

Como vimos no caso de grupo diedrais, grupos que são "próximos" a grupos cíclicos tem estruturas mais simples. Entre os 2-grupos, essa propriedade é caracterizada pela presença de um subgrupo cíclico maximal. O Teorema 5.3.4 de [14] nos dá a seguinte classificação desses grupos:

Teorema 4.4.1 ([14] 5.3.4 para $p = 2$). *Seja G um grupo de ordem 2^n com subgrupo cíclico maximal. Então G é de um dos seguintes tipos:*

1. Cíclico C_{2^n}
2. Produto $C_{2^{n-1}} \times C_2$
3. Diedral $D_{2^{n-1}} = \langle a, x : a^{2^{n-1}}, x^2, a^x = a^{-1} \rangle, n \geq 3$
4. Quatérnio $Q_{2^n} = \langle a, x : a^{2^{n-1}}, a^x = a^{-1}, a^{2^{n-2}} = x^2 \rangle, n \geq 3$
5. Semidiedral $SD_{2^n} = \langle a, x : a^{2^{n-1}}, x^2, a^x = a^{2^{n-2}-1} \rangle, n \geq 4$
6. Modular máximo $M_{2^n} = \langle a, x : a^{2^{n-1}}, x^2, a^x = a^{2^{n-2}+1} \rangle, n \geq 4$

Já determinamos a estrutura de grafo para os casos 1, 2, 3 e 4 no teorema acima: no caso 1, temos um grupo cíclico de ordem par, estudado na Proposição 3.4.1; no caso 2 temos um grupo abeliano, visto no Teorema 3.6.1; estudamos grupos diedrais e quatérnios generalizados no Teorema 4.1.2 e na Proposição 4.2.1 respectivamente. Para os grupos SD_{2^n} e M_{2^n} , temos os seguintes resultados:

Lema 4.4.2. *Sejam $n \geq 3$ e $SD_{2^n} = \langle a, x : a^{2^{n-1}}, x^2, a^x = a^{2^{n-2}-1} \rangle$ o grupo semidiedral de ordem 2^n . Então todo elemento é da forma $x^i a^j$ com $0 \leq i \leq 1$; $0 \leq j \leq 2^{n-1} - 1$. Além disso, temos que:*

$$(xa^k)^2 = \begin{cases} 1, & \text{se } k \equiv 0 \pmod{2} \\ a^{2^{n-2}}, & \text{se } k \equiv 1 \pmod{2} \end{cases}$$

Demonstração. A primeira afirmação vem do fato que $ax = xa^{2^{n-2}-1}$. Para a segunda afirmação, seja $k = 2m + r$ com $m \in \mathbb{Z}$ e $r \in \{0, 1\}$. Então:

$$(xa^k)^2 = xa^k xa^k = (a^{2^{n-2}-1})^k a^k = a^{k2^{n-2}} = a^{m2^{n-1}} a^{r2^{n-2}} = a^{r2^{n-2}}$$

Os dois valores correspondem com os dois casos de r . □

Lema 4.4.3. *Seja $G = M_{2^n}$, para $n \geq 4$. Então:*

1. podemos particionar $G = G_0 \cup xG_0$ onde G_0 é o subgrupo cíclico maximal $\langle a \rangle$.
2. Seja $g \in G$. Então se $o(g) = 2^{n-1}$ não existe $h \in xG_0$ tal que $h^2 = g$; Caso contrário, existem exatamente dois elementos $h_1, h_2 \in xG_0$ tais que $h_i^2 = g$. e $h_i = xa^{k_i}$

Demonstração. A primeira afirmação segue do fato que G_0 é um subgrupo normal de G de índice 2. Portanto todo elemento de G é da forma a^k ou xa^k , e seu quadrado está em G_0 pois $G/G_0 \cong C_2$. Tomemos xa^k e apliquemos a função quadrado:

$$(xa^k)^2 = xa^k xa^k = (a^{2^{n-2}+1})^k a^k = a^{2k(2^{n-3}+1)}$$

Então obter os valores de k para que $(xa^k)^2 = a^t$ para algum $g = a^t$ dado corresponde a solucionar em k a congruência linear:

$$2k(2^{n-3} + 1) \equiv t \pmod{2^{n-1}}$$

Como $2^{n-3} + 1$ é ímpar, o número de soluções é 0 se $\text{mdc}(t, 2^{n-1}) = 1$ e 2 caso contrário (veja, por exemplo, [2] teorema 5.14) $\square$

Relembremos a definição de nível, em 2.4.3: Seja $\mathcal{T} = (V, A)$ um grafo de árvore direcionada. Para todo $v \in V$ definimos o **nível** indutivamente: se v_0 é a raiz da árvore, o nível de v_0 é 0. Se $(v, w) \in A$ então o nível de v é o sucessor do nível de w .

Definição 4.4.4. Seja $\mathcal{T} = (V, A)$ um grafo de árvore direcionada. Definimos o grafo $\mathcal{T}^{+(k)}$, chamada k -estrelada, como sendo o novo grafo de árvore, onde para cada vértice de nível não maximal em $\mathcal{T}$, adicionamos k vértices conectados a ele.

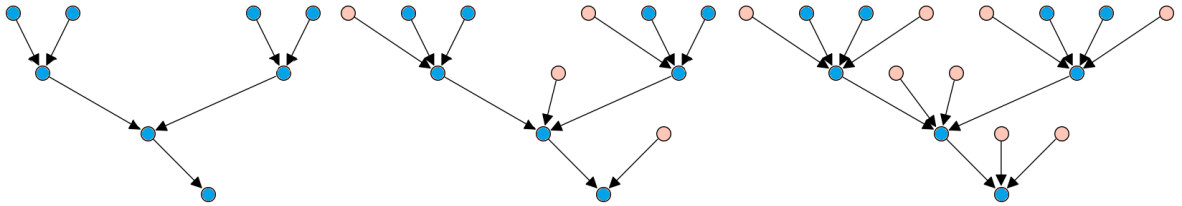


Figura 4.13 : Exemplo do processo de árvore estrelada. Da esquerda pra direita: árvore $\mathcal{T}$ original, árvore $\mathcal{T}^{+(1)}$, e árvore $\mathcal{T}^{+(2)}$.

Com esse resultados estabelecidos, temos então as ferramentas para classificar os grafos de 2-grupos com subgrupo cíclico maximal. Esse resultado está sumariado no teorema abaixo:

Teorema 4.4.5. *Seja G um 2-grupo de ordem 2^n com um subgrupo cíclico maximal. Adotando as notações do Teorema 4.4.1, seja $f : G \rightarrow G$, $f(x) = x^2$. Então a estrutura do grafo $\mathcal{G}(G, f)$ para as diferentes classes de G estão na tabela abaixo, onde as sequências $\mathbf{v}$ de índice $\mathcal{T}_{\mathbf{v}}$ possuem comprimento k no primeiro caso e $k - 1$ em todos os outros:*

Grupo	Grafo
C_{2^n}	$\mathcal{T}_{(2,2,\dots,2)}$
$C_{2^{n-1}} \times C_2$	$\mathcal{T}_{(4,2,\dots,2)}$
$D_{2^{n-1}}$	$\left\langle \mathcal{T}_{(2,2,\dots,2)}^\setminus \oplus (2^{n-1} \times \bullet) \right\rangle$
Q_{2^n}	$\left\langle \left\langle \mathcal{T}_{(2,2,\dots,2)}^{\setminus\setminus} \oplus (2^{n-1} \times \bullet) \right\rangle \right\rangle$
SD_{2^n}	$\left\langle \left\langle \mathcal{T}_{(2,2,\dots,2)}^{\setminus\setminus} \oplus (2^{n-2} \times \bullet) \right\rangle \oplus (2^{n-2} \times \bullet) \right\rangle$
M_{2^n}	$\mathcal{T}_{(2,2,\dots,2)}^{+(2)}$

Demonstração. A única informação nova são os grafos de $SD_{2^{n-1}}$ e $M_{2^{n-1}}$. Em ambos temos um subgrupo normal cíclico de índice 2 gerado por a ; portanto basta estudar os quadrados dos elementos xa^k . Para $SD_{2^{n-1}}$, o Lema 4.4.2 nos dá que metade dos elementos xa^k quando elevados ao quadrado são iguais a 1 e a outra metade é igual a $a^{2^{n-2}}$. Para $M_{2^{n-1}}$, se a^r é tal que $\text{mdc}(r, 2^{n-1}) = 1$, então $o(a^r) = 2^{n-1}$ e não existe "raiz quadrada" de a^r da forma xa^k . Caso contrário, existem dois elementos xa^k tais que $(xa^k)^2 = a^r$. $\square$

Abaixo seguem os grafos dos grupos de ordem 16 com um subgrupo cíclico maximal. Nelas, o subgrupo cíclico está destacado em azul:

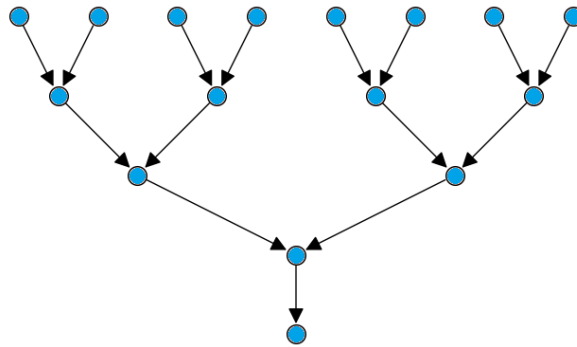


Figura 4.14 : Grafo de C_{16}

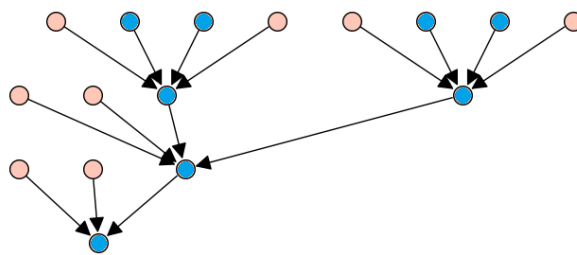
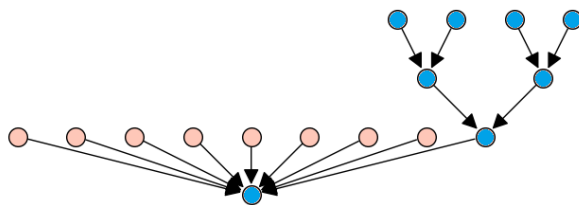
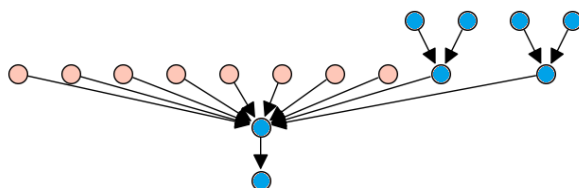
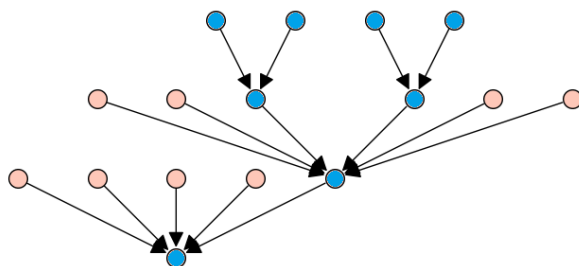
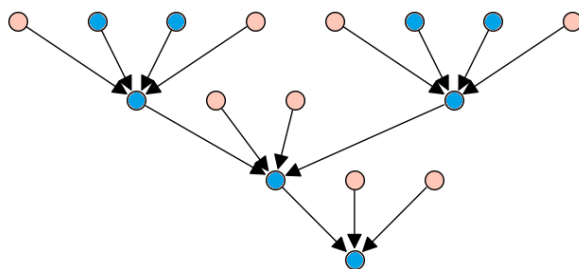


Figura 4.15 : Grafo de $C_8 \times C_2$

Figura 4.16 : Grafo de D_8 Figura 4.17 : grafo de Q_{16} Figura 4.18 : Grafo de SD_{16} Figura 4.19 : Grafo de M_{16}

4.5 Grupos de Expoente p

Dado um grupo finito G , o **Expoente** do grupo, escrito $\exp(G)$, é o menor natural n tal que $g^n = 1, \forall g \in G$. Equivalentemente, $\exp(G)$ é $\text{mmc}\{o(g) : g \in G\}$, o menor

múltiplo comum das ordens de elementos de G . Se $\exp(G)$ é um primo p , então $o(g) = p$ para todo $g \neq 1$.

O exemplo clássico de grupos de expoente p são os grupos **Abelianos Elementares**: $C_p \times C_p \times \cdots \times C_p$. Um exemplo de grupo de expoente p não abeliano é o **Grupo de Heisenberg Módulo 3**, o subgrupo de $GL(3, \mathbb{F}_3)$ dado por:

$$\left\{ \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{F}_3 \right\}$$

É possível mostrar que esse grupo é isomorfo ao grupo de apresentação

$$\langle a, b, c : a^3, b^3, c^3, [a, c], [b, c], [a, b] = c \rangle.$$

Nessa apresentação, todo elemento é de forma $a^i b^j c^k$ e

$$(a^i b^j c^k)(a^\ell b^m c^n) = a^{i+\ell} b^{j+m} c^{n+k+j\ell}.$$

Portanto, $(a^i b^j c^k)^3 = a^{3i} b^{3j} c^{3k+ij+2ij} = 1$ e segue que o grupo de Heisenberg módulo 3 tem expoente 3.

Grupos de expoente p podem possuir estruturas bastante complexas: no estudo do Problema de Burnside, isto é, se “um grupo finitamente gerado de expoente finito é necessariamente finito?”, Novikov e Adjan (1968) mostraram que o grupo livre de Burnside $B(n, e)$ é infinito para todo $n > 1$ e $e \geq 665$ ímpar. Para esse trabalho, basta o corolário desse resultado, que existem grupos 2-gerados de expoente primo infinitos para primos grandes o suficiente. Para uma exposição mais detalhada do problema de Burnside, ver [14].

Para $f : G \rightarrow G, f(g) = g^2$, a estrutura do grafo $\mathcal{G}(G, f)$ quando $\exp(G)=p$ não é complexa. No caso $p = 2$, G é um 2-grupo, e como foi discutido na seção 4.3, o grafo será uma árvore, cuja estrutura é definida na proposição abaixo (O primeiro resultado é bem conhecido, e será enunciado por completude):

Proposição 4.5.1. *Seja G um grupo de ordem n tal que $\exp(G) = 2$, e seja $f : G \rightarrow G, f(g) = g^2$. Então o grupo G é abeliano e o grafo $\mathcal{G} = \mathcal{G}(G, f)$ é dado por:*

$$\mathcal{G} = \mathcal{T}_{(n)} = \langle (2n - 1) \times \bullet \rangle$$

Demonstração. É suficiente mostrar que quaisquer dois elementos comutam. De fato se $a, b \in G$ são não triviais, $a^2 = b^2 = (ab)^2 = 1$ e portanto $abab = a^2 b^2 \implies ba = ab$.

Se $g \in G$ e $g \neq 1$ então $f(g) = 1$; segue que $\mathcal{G}$ é uma árvore de $n - 1$ vértices conectadas à raiz 1. $\square$

O caso onde p é ímpar temos um argumento similar:

Proposição 4.5.2. *Seja G um grupo de ordem n tal que $\exp(G) = p$, um primo ímpar, e seja $f : G \rightarrow G, f(g) = g^2$. Então o grafo $\mathcal{G} = \mathcal{G}(G, f)$ é dado por:*

$$\mathcal{G} = \text{Cyc}(1) \oplus \frac{n-1}{\text{ord}_p(2)} \times \text{Cyc}(\text{ord}_p(2))$$

Demonstração. A divisão $(n-1)/\text{ord}_p(2)$ faz sentido pois $\text{ord}_p(2)|p-1$ e como G é um grupo de expoente p , em particular é um p -grupo, e portanto $n = p^k$ e $p-1|p^k-1 \implies \text{ord}_p(2)|n-1$. Se $g \in G, g \neq 1$, então por definição $k = \text{ord}_p(2)$ é o menor inteiro positivo tal que $g^k = 1$. Logo os elementos de g distintos de 1 estão em ciclos de ordem $\text{ord}_p(2)$, e a quantidade desses ciclos é $(n-1)/\text{ord}_p(2)$. $\square$

Uma consequência da proposição acima é que o número de componentes conexas do grafo é de

$$1 + \frac{n-1}{\text{ord}_p(2)}.$$

Um caso interessante ocorre quando 2 é uma raiz primitiva módulo p , isto é $\text{ord}_p(2) = p-1$. Este é o caso minimal, onde o número de componentes conexas é:

$$1 + \frac{n-1}{p-1} = 1 + \frac{p^k-1}{p-1} = p^{k-1} + \dots + p + 2,$$

que é portanto uma cota inferior para o número de componentes conexas que depende apenas de p . Determinar os casos onde essa cota inferior é ótima, ou equivalentemente, determinar os casos onde 2 é uma raiz primitiva módulo p é um problema difícil de teoria dos números. Um resultado relacionado é a aberta Conjectura de Artin, que postula que infinitos tais primos existem e sua densidade assintótica. (Para mais detalhes, ver [7]). Os primos menores que 200 para qual essa cota é ótima são: 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197 (fonte: OEIS Foundation Inc (2025) entrada A001122 na On-line Encyclopedia of Integer Sequences <https://oeis.org/A001122>).

Exemplo 4.5.1. Seja $H_3 = \langle a, b, c : a^3, b^3, c^3, [a, c], [b, c], [a, b] = c \rangle$ o grupo de Heisenberg módulo 3. O grupo possui ordem 27. Então $26/\text{ord}_3(2) = 13$ e temos 14 componentes conexas, e o grafo é $\text{Cyc}(1) \oplus 13 \times \text{Cyc}(2)$.

Exemplo 4.5.2. Seja $G = C_3 \times C_3 \times C_3$ o grupo abeliano elementar de ordem 27. O grupo possui ordem 27. Então $26/\text{ord}_3(2) = 13$ e temos 14 componentes conexas, e o grafo é $\text{Cyc}(1) \oplus 13 \times \text{Cyc}(2)$. Note que o grafo é isomorfo ao grafo de H_3 .

Exemplo 4.5.3. Seja G um grupo de expoente 5 e ordem 125. Exemplos incluem C_5^3 e o grupo de Heisenberg módulo 5 $\langle a, b, c : a^5, b^5, c^5, [a, c], [b, c], [a, b] = c \rangle$. Nesse caso temos $124/\text{ord}_5(2) = 31$ e portanto temos o grafo $\text{Cyc}(1) \oplus 31 \times \text{Cyc}(4)$ de 32 componentes conexas.

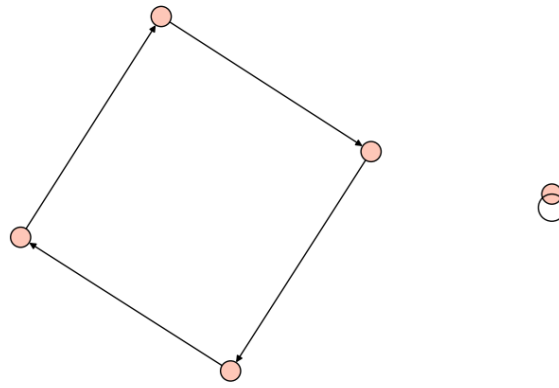


Figura 4.21 : Tipos de componentes conexas nos grafos de expoente 5. No caso de H_5 e C_5^3 a componente da esquerda aparece 31 vezes.



Figura 4.20 : Grafo de H_3 e de C_3^3

Capítulo 5

Considerações finais

No trabalho, estudamos profundamente a aplicação $f(x) = x^2$. Para potências positivas distintas, resultados similares aos do capítulo 2 podem ser observados em [13]; por exemplo:

Teorema 5.0.1 ([13], Proposição 2.2). *Seja $G = C_n$ o grupo cíclico de ordem n e $f : G \rightarrow G$, $f(x) = x^t$. Tome $n = vw$ onde w é o maior divisor de n coprimo a t e $\text{mdc}_t(v) = (v_1, \dots, v_D)$ é o mdc iterado de v e t . Então temos o isomorfismo de grafos:*

$$\mathcal{G}(G, f) = \bigoplus_{d|w} \left(\frac{\varphi(d)}{\text{ord}_d(t)} \times \text{Cyc}(\text{ord}_d(t), \mathcal{T}_{\text{mdc}_t(v)}) \right),$$

onde o mdc iterado é definido em [13] seção 2.2.

Podemos também afirmar para a aplicação $f(x) = x^{-1}$ onde para qualquer grupo G de ordem n o grafo $\mathcal{G}(G, f) = r \times \text{Cyc}(1) \oplus \frac{n-r}{2} \times \text{Cyc}(2)$ onde r é o número de elementos de G tais que $x = x^{-1}$, isto é, involuções e a identidade.

No capítulo 4 definimos a notação $\mathcal{T}^{+(k)}$ para árvores k -estreladas e utilizamos essa notação para o grafo de M_{2^n} . É possível mostrar *a posteriori* que essa notação é supérflua, pois os grafos de M_{2^n} e $C_{x^{n-1}} \times C_2$ são isomorfos. De fato:

Proposição 5.0.2. *Os grafos (M_{2^n}, f) , e $(C_{x^{n-1}} \times C_2, g)$ são isomorfos para $f(x) = x^2$ e $g(x) = x^2$.*

Demonstração. Basta que para $v = (2, 2, \dots, 2)$ temos $\mathcal{T}_{(4,2,\dots,2)} \cong \mathcal{T}_v^{+(2)}$. De fato $\mathcal{T}_{(4,2,\dots,2)} = \mathcal{T}_{(2)} \otimes \mathcal{T}_v$. Na definição de produto tensorial, temos que todo elemento x no conjunto de vértices de $\mathcal{T}_v$ que possui uma aresta direcionada a ele, temos mais dois vértices direcionados. Isto é a definição de $\mathcal{T}_v^{+(2)}$. $\square$

Nesse trabalho demos ênfase para a classificação das estruturas de grafo na dinâmica da função $f(x) = x^2$. Um possível direcionamento em futura análise seria utilizar ferramentas da teoria de grafos - como por exemplo a computação de invariantes como B-polinômios (ver [3]) - para obter informações dos grupos.

Bibliografia

- [1] T. Alden Gassert. “Chebyshev action on finite fields”. Em: *Discrete Mathematics* 315-316 (2014), pp. 83–94. ISSN: 0012-365X. DOI: <https://doi.org/10.1016/j.disc.2013.10.014>. URL: <https://www.sciencedirect.com/science/article/pii/S0012365X1300441X>.
- [2] Tom M Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag, 1976.
- [3] Jordan Awan e Olivier Bernardi. “Tutte polynomials for directed graphs”. Em: *Journal of Combinatorial Theory, Series B* 140 (2020), pp. 192–247. ISSN: 0095-8956. DOI: <https://doi.org/10.1016/j.jctb.2019.05.006>. URL: <https://www.sciencedirect.com/science/article/pii/S0095895619300553>.
- [4] Garrett Birkhoff e Saunders Mac Lane. *A survey of modern algebra*. A K Peters/CRC Press, 2017.
- [5] A. Bors. “On the dynamics of endomorphisms of finite groups”. Em: *AAECC* 28, 205–214 (2017).
- [6] Wun-Seng Chou e Igor E Shparlinski. “On the cycle structure of repeated exponentiation modulo a prime”. Em: *Journal of Number Theory* 107.2 (2004), pp. 345–356. ISSN: 0022-314X. DOI: <https://doi.org/10.1016/j.jnt.2004.04.005>. URL: <https://www.sciencedirect.com/science/article/pii/S0022314X04000745>.
- [7] Christopher Hooley. Em: *Journal für die reine und angewandte Mathematik* 1967.225 (1967), pp. 209–220. DOI: [doi:10.1515/crll.1967.225.209](https://doi.org/10.1515/crll.1967.225.209). URL: <https://doi.org/10.1515/crll.1967.225.209>.
- [8] Abdul Salam Jarrah et al. “Reverse-engineering of polynomial dynamical systems”. Em: *Advances in Applied Mathematics* 39.4 (2007), pp. 477–489. ISSN: 0196-8858. DOI: <https://doi.org/10.1016/j.aam.2006.08.004>. URL: <https://www.sciencedirect.com/science/article/pii/S0196885806001205>.
- [9] D L Johnson. *Presentation of Groups*. Cambridge University Press, 1990.
- [10] José Alves Oliveira e F. E. Brochero Martínez. “Dynamics of polynomial maps over finite fields”. Em: *Des. Codes Cryptography* 92.5 (nov. de 2023), pp. 1113–1125. ISSN: 0925-1022. DOI: [10.1007/s10623-023-01332-3](https://doi.org/10.1007/s10623-023-01332-3). URL: <https://doi.org/10.1007/s10623-023-01332-3>.
- [11] Daniel Panario e Lucas Reis. “The functional graph of linear maps over finite fields and applications”. Em: *Designs, Codes and Cryptography* 87 (mar. de 2019). DOI: [10.1007/s10623-018-0547-5](https://doi.org/10.1007/s10623-018-0547-5).

- [12] Claudio Qureshi e Lucas Reis. "Dynamics of the a -map over residually finite Dedekind domains and applications". Em: *Journal of Number Theory* 204 (2019), pp. 134–154. ISSN: 0022-314X. DOI: <https://doi.org/10.1016/j.jnt.2019.03.018>. URL: <https://www.sciencedirect.com/science/article/pii/S0022314X19301234>.
- [13] Claudio Qureshi e Lucas Reis. "On the functional graph of the power map over finite groups". Em: *Discrete Mathematics* 346.7 (2023), p. 113393. ISSN: 0012-365X. DOI: <https://doi.org/10.1016/j.disc.2023.113393>. URL: <https://www.sciencedirect.com/science/article/pii/S0012365X23000791>.
- [14] Derek J S Robinson. *A Course in the theory of Groups*. Springer-Verlag, 1996.
- [15] Thomas D. Rogers. "The graph of the square mapping on the prime fields". Em: *Discrete Mathematics* 148.1 (1996), pp. 317–324. ISSN: 0012-365X. DOI: [https://doi.org/10.1016/0012-365X\(94\)00250-M](https://doi.org/10.1016/0012-365X(94)00250-M). URL: <https://www.sciencedirect.com/science/article/pii/0012365X9400250M>.