UNIVERSIDADE FEDERAL DE SERGIPE
DEPARTAMENTO DE MATEMÁTICA - PROFMAT

Uma aplicação da teoria de Ramsey ao teorema de Schur

Dissertação apresentada ao Programa de Pós-Graduação em Matmática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Liliane Teixeira Pina Araujo

Orientador: Zaqueu Alves Ramos

São Cristóvão, 2019.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Araújo, Liliane Teixeira Pina
A663a Uma aplicação da teoria de Ramsey ao teorema de Schur / Liliane Teixeira Pina Araújo ; orientador Zaquel Alves Ramos. – São Cristóvão, SE, 2019.
35 f. : il.

Dissertação (mestrado em Matemática) – Universidade Federal de Sergipe, 2019.

1. Matemática – Estudo e ensino. 2. Álgebra. 3. Fermat, Último teorema de. 4. Teoria dos grafos. I. Ramos, Zaqueu Alves, orient. II. Título.

CDU 512

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Uma aplicação da teoria de Ramsey ao teorema de Schur

por

Liliane Teixeira Pina Araújo

Aprovada pela banca examinadora:

Prof. Zaqueu Alves Ramos - UFS
Orientador

Prof. Andre Vinicius Santos Doria - UFS
Primeiro Examinador

Prof. Fabio Lima Santos - UFRPE
Segundo Examinador

São Cristóvão, 12 de Julho de 2019

Cidade Universitária "Prof. José Aloísio de Campos" – Av. Marechal Rondon, s/no - Jardim Rosa Elze – Campus de São Cristóvão. Tel. (00 55 79) 3194-6887
CEP: 49100-000 - São Cristóvão – Sergipe - Brasil – E-mail: promat.ufs@gmail.com

Agradecimentos

Primeiramente quero agradecer a Deus por ter me dado sabedoria, forças e oportunidades em todos os momentos da minha vida, especialmente nesses dois últimos anos que me realizei profissionalmente e fui abençoada com chegada do meu filho Leonardo, o maior amor da minha vida.

Quero agradecer aos meus pais, Leandro e Solange, que me incentivaram nos estudos e sempre aplaudiram meu potencial.

Agradeço também ao meu esposo, José Valdo, que esteve o tempo todo ao meu lado, me apoiando e entendendo minha ausência em tantos momentos.

Aos meus irmãos, Lília e Evandro e aos meus cunhados Rafael e Grasielle que estavam na torcida pelo meu crescimento.

A melhor turma do Profmat, em especial a Ana Nery, Maurício, Vonicleiton, Marcos Sá, Luiz e Bebeto por tantas angústias e aprendizagens compartilhadas.

Ao meu orientador, professor Doutor Zaqueu por toda contribuição para que o êxito fosse alcançado.

A toda minha família e amigos que oram e torcem por mim, meu muito obrigada.

Conteúdo

Resumo

Nessa dissertação faremos uma breve introdução à teoria de Ramsey. Como aplicação dos resultados apresentados demonstraremos o teorema de uma versão do celebrado Último Teorema de Fermat no contexto dos corpos residuais $\mathbb{Z}_p$.

Palavras Chave: Teorema de Ramsey, Grafos, Grupos, Corpos Residuais

Abstract

In this dissertation, we will make a brief introduction to Ramsey's theory. As an application of the results presented we will demonstrate the theorem of a version of the celebrated Fermat's Last Theorem in the context of residual bodies $\mathbb{Z}_p$.

keywords: Ramsey's theorem, graphs, groups, residual bodies.

Lista de símbolos

Símbolo	Descrição
$\lvert A \rvert$	quantidade de elementos de um conjunto A
$\mathcal{O}(G)$	ordem de um grupo G
gH	classe lateral à esquerda de um elemento g de um grupo G
G/H	quociente de um grupo G por um subgrupo H
$\ker \varphi$	núcleo de um homomorfismo de grupos
$\mathrm{Im}\, \varphi$	imagem de um homomorfismo de grupos φ
$\mathbb{Z}_n$	anel de resíduos módulo n
$\mathbb{Z}_n^*$	conjunto dos elementos invertíveis de $\mathbb{Z}_n$
$V(G)$	conjunto dos vértices de um grafo G
$E(G)$	conjunto das arestas de um grafo G
$I(G)$	conjunto das incidências de um grafo G
K_n	grafo completo com n vértices
$[n]$	conjunto formado pelos números naturais de 1 a n

Introdução

O Último Teorema de Fermat, enunciado por Pierre de Fermat em 1637, é um dos capítulos mais célebres da história da matemática. Fermat escrevera uma anotação em um livro com os seguintes dizeres

"*É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como a soma de duas quartas potências ou, em geral, para qualquer número que é uma potência maior do que a segunda, ser escrito como a soma de duas potências com o mesmo expoente. Descobri uma demonstração maravilhosa desta proposição que, no entanto, não cabe nas margens deste livro*."

Em linguagem atual, o resultado proposto por Fermat pode ser encunciado como:

"*Não existem* $x_0, y_0, z_0 \in \mathbb{Z}$, *com* $x_0 y_0 z_0 \neq 0$, *que resolva a equação* $x^n + y^n = z^n$ *para* $n \geqslant 3$."

Não houve na história nenhum indício de que Fermat realmente tivesse demonstrado esse teorema. De fato, vários outros matemáticos proeminentes tentaram por mais de 3 séculos obter uma prova mas sem lograr êxito. Este resultado somente veio ser demonstrado completamente em 1994 pelo matemático britânico Andrew Wiles. As várias tentativas de demonstrar o Último Teorema de Fermat motivou o surgimento de diversas teorias e problemas inspirados nele.

Um dos problemas inspirados no Último Teorema de Fermat foi pensado pelo matemático Issai Schur por volta de 1916. O seu propósito era estudar a existência de soluções $x_0, y_0, z_0 \in \mathbb{Z}_p$, com $x_0 y_0 z_0 \neq 0$, que resolva a equação $x^n + y^n = z^n$, ou seja, ele estava interessado no problema de Fermat no contexto dos corpos residuais $\mathbb{Z}_p$. Diferentemente do problema original, em que é provado não existir soluções, na versão de Schur conclui-se que para todo p suficientemente grande a equação $x^n + y^n = z^n$ sempre possui solução independente de quem seja o n.

Nesse trabalho nosso objetivo principal é apresentar uma prova para o Teorema de Schur. Para isso, dividimos a dissertação em 2 capítulos os quais passamos a descrever.

No capítulo I fazemos os preliminares algébricos que são necessários para o entendimento do enunciado e da prova do teorema de Schur. Nessa parte do texto apresentamos: as definições de grupo, subgrupo, classe lateral, quociente de um grupo por um subgrupo; o teorema de Lagrange; as definições de homomorfismo, isomorfismo, subgrupo normal; o primeiro teorema dos isomor-

fismos; as definições de corpos e de anéis residuais módulo n.

No segundo e último capítulo iniciamos fazendo uma breve apresentação sobre a teoria geral de grafos. Em seguida, discutimos sobre a principal ferramenta para tratar do problema de Schur, a saber, a teoria de Ramsey. Concluída essa discussão exibimos a demonstração para a versão de Schur do Último Teorema de Fermat. Veremos que é uma prova belíssima em que são combinados de forma simples e elegante elementos de álgebra e de combinatória.

Capítulo 1

Preliminares algébricos

O objetivo desse capítulo é apresentar os conceitos e resultados algébricos que serão importantes para entender e demonstrar a versão do Último Teorema de Fermat para corpos residuais. A principal referência para a elaboração desse capítulo é o livro [2].

1.1 Grupos

A grosso modo, um grupo é uma estrutura formado por um conjunto não vazio e uma operação de composição que satisfaz propriedades operacionais básicas como associatividade, existência de identidade e existência de elemento invertível. De forma mais precisa, a definição pode ser dada da seguinte maneira.

Definição 1.1.1. Um *grupo* é uma estrutura formada por um conjunto não vazio G e uma operação $\circ : G \times G \to G$ sujeitos aos seguintes axiomas:

(a) Para quaisquer $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$.

(b) Existe $e \in G$ tal que $a \circ e = e \circ a = a$ para qualquer $a \in G$ (um elemento e com tal propriedade é chamado *identidade* ou *elemento neutro*).

(c) Para qualquer $a \in G$ existe um elemento $a' \in G$ tal que $a \circ a' = a' \circ a = e$ (um tal elemento a' é chamado de *inverso* de a).

Se além desses axiomas também for verificado que

(d) Para qualquer $a, b \in G$, $a \circ b = b \circ a$.

então dizemos que o grupo é *abeliano.*

Algumas consequências imediatas da definição são:

(1) *A indentidade de um grupo é única.* Com efeito, suponhamos $e, e' \in G$ duas identidades. Então $e = e \circ e' = e'$.

(2) *Para cada* $a \in G$*, o inverso de* a *é único.* Com efeito, suponhamos que a', a'' sejam inversos de a. Então $a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''$. Costumamos usar o símbolo a^{-1} para denotar o inverso de a.

Abaixo listamos alguns exemplos de grupos:

Exemplo 1.1.2. Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ equipados com suas operações usuais de adição são exemplos de grupos.

Exemplo 1.1.3. Os conjuntos $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$ equipados com suas operações usuais de multiplicação são exemplos de grupos.

Exemplo 1.1.4. O conjunto $M_{m\times n}(\mathbb{R})$ de todas as matrizes de ordem $m \times n$ com entradas em $\mathbb{R}$ com a operação usual de adição de matrizes.

Exemplo 1.1.5. O conjunto $Gl_n(\mathbb{R})$ de todas as matrizes invertíveis de $M_{n\times n}(\mathbb{R})$ com a operação de multiplicação de matrizes.

Exemplo 1.1.6. Seja X um conjunto não vazio. Definimos S_X sendo o conjunto de todas as funções $f : X \to X$ bijetoras. O conjunto S_X equipado com a operação de composição de funções é um grupo. Além disso é possível provar que esse grupo é abeliano, se e somente se, X é um conjunto com no máximo dois elementos. Na situação especial em que $X = \{1, \ldots, n\}$ usamos a notação S_n em vez de S_X. Chamamos S_n de *grupo das permutações de* n *letras*.

Notação: Dados um grupo G com operação $\circ$ e elementos $a, b \in G$, abreviaremos a notação escrevendo simplesmente ab em vez de $a \circ b$.

Uma das informações mais básicas sobre um grupo G é sua *ordem.*

Definição 1.1.7. Seja G um grupo. A quantidade de elementos de G é chamada de *ordem* de G. Se G tem uma quantidade infinita de elementos dizemos que sua ordem é infinita.

Notação: A ordem de um grupo G é denotada por $\mathcal{O}(G)$.

Exemplo 1.1.8. Os exemplos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $M_n(\mathbb{R})$ e $Gl_n(\mathbb{R})$ listados acima são grupos de ordem infinita. É fácil mostrar que o grupo S_X tem ordem infinita se, e somente se, X é infinito. Notemos que os elementos de S_n podem ser identificados com as permutações da sequência $(1, \ldots, n)$. Dessa maneira, $\mathcal{O}(S_n) = n!$.

Dado um grupo G, podemos procurar outros exemplos de grupos dentro do próprio grupo G. Para ver como isso pode ser feito necessitamos da seguinte definição:

Definição 1.1.9. Seja G um grupo. Um subconjunto H de G é chamado *subgrupo* de G se as seguintes condições forem verificadas:

(a) A identidade e de G pertence a H.

(b) Se $a, b \in H$ então $ab \in H$.

(c) Se $a \in H$ então $a^{-1} \in H$.

Observe que a condição (b) da definição garante que a operação $\circ : H \times H \to H$ está bem definida. Além disso, temos:

(i) Como $a(bc) = (ab)c$ para qualquer $a, b, c \in G$ então, por mais forte razão, $a(bc) = (ab)c$ para qualquer $a, b, c \in H$.

(ii) Como $ae = ea = a$ para qualquer $a \in G$ então, por mais forte razão, $ae = ea = a$ para qualquer $a \in H$.

(iii) Como para cada $a \in H$, $a^{-1} \in H$, então cada $a \in H$ tem um inverso em H.

Segue dessas três observações que ao restringirmos a operação de G a H temos um novo grupo.

Exemplo 1.1.10. Dado um grupo G, dois subgrupos óbvios de G são $\{e\}$ e o próprio G. Chamamos estes de *subgrupos triviais* de G.

Exemplo 1.1.11. Seja $\mathbb{R}_+$ o subconjunto de $\mathbb{R}^*$ formado pelos números reais positivos. Sabemos que: (i) $1 \in \mathbb{R}_+$; (ii) o produto de dois números positivos é também um número positivo; (iii) dado um número positivo a o seu inverso $1/a$ também é positivo. Assim, $\mathbb{R}_+$ é um subgrupo de $\mathbb{R}^*$.

Seja H um subgrupo de um grupo G. A *classe lateral à esquerda* de um elemento $g \in G$ com respeito ao subgrupo H, denotada gH, é:

$$gH := \{gh \mid h \in H\}.$$

Observação 1.1.12. Também podemos definir a *classe lateral à direita* de um elemento $g \in G$ com respeito ao subgrupo H, denotada Hg, como:

$$Hg := \{hg \mid h \in H\}.$$

O conjunto formado por todas classes laterais à esquerda gH é chamado *quociente de* G *por* H e é denotado por $\frac{G}{H}$ ou G/H. Observe em particular que G/H é, por definição, um subconjunto do conjunto das partes de G.

Observação 1.1.13. Seja H um subgrupo de um grupo G. Temos:

(a) Para cada $g \in G$, $gH \neq \emptyset$. De fato, temos que $g = ge \in gH$; logo, $gH \neq \emptyset$ como afirmado.

(b) Dados $g_1, g_2 \in G$, $g_1H = g_2H$ se, e somente se, $g_2^{-1}g_1 \in H$. Suponha $g_1H = g_2H$. Então $g_1 = g_1e \in g_1H = g_2H$; logo, existe $h \in H$ tal que $g_1 = g_2h$. Multiplicando os dois lados dessa igualdade por g_2^{-1} segue que $g_2^{-1}g_1 = h \in H$. Reciprocamente, suponhamos que $g_2^{-1}g_1 \in H$. Em particular, $g_1^{-1}g_2 \in H$ pois $g_1^{-1}g_2$ é o inverso de $g_2^{-1}g_1$ e H é subgrupo de G. Dado $a \in g_1H$, temos $a = g_1h$ para algum $h \in H$. Por outro lado, $a = g_2(g_2^{-1}g_1h) \in g_2H$. Desse modo, $g_1H \subset g_2H$. Agora suponha $b \in g_2H$. Então $b = g_2h$. Analogamente também temos $b = g_1(g_1^{-1}g_2h) \in g_1H$. Logo, $g_2H \subset g_1H$. Portanto, $g_1H = g_2H$.

(c) Dados $g_1, g_2 \in G$, $g_1H = g_2H$ se, e somente se, $g_1H \cap g_2H \neq \emptyset$. Com efeito, a igualdade $g_1H = g_2H$ obviamente implica $g_1H \cap g_2H \neq \emptyset$. Agora, suponha $g_1H \cap g_2H \neq \emptyset$, então existe $a \in g_1H \cap g_2H$. Logo, existem $h_1, h_2 \in H$ tais que $a = g_1h_1 = g_2h_2$; logo, $g_2^{-1}g_1 = h_2h_1^{-1} \in H$. Desse modo, pelo item (b) segue $g_1H = g_2H$ como desejado.

(d) $G = \bigcup_{gH \in G/H} gH$. A inclusão $\bigcup_{gH \in G/H} gH \subset G$ é óbvia. Para a inclusão contrária, considere $g \in G$. Como visto antes $g \in gH$. Assim, por mais forte razão, $g \in \bigcup_{gH \in G/H} gH$; logo, $G \subset \bigcup_{gH \in G/H} gH$.

Dado um conjunto X arbitrário, um subconjunto $\mathcal{S}$ do conjunto das partes de X é chamado uma *partição* de X se as seguintes condições são satisfeitas:

(i) Qualquer membro A de $\mathcal{S}$ é não vazio.

(ii) Quaisquer dois membros distintos de $\mathcal{S}$ são disjuntos.

(iii) A união de todos os membros de $\mathcal{S}$ é igual a X.

Os itens (a), (c) e (d) da Observação 1.1.13 nos diz que o conjunto quociente G/H é uma partição para o conjunto G. Em particular, se G é um grupo finito temos:

$$\mathcal{O}(G) = \#g_1H + \cdots + \#g_mH, \tag{1.1}$$

onde $g_1H, \ldots, g_mH$ são todas as classes laterais, duas a duas distintas, e $\#g_iH$ denota a quantidade de elementos de g_iH.

Proposição 1.1.14. *Seja* H *um subgrupo de um grupo* G. *Então, para cada* $g \in G$, *a correspondência*

$$\psi : H \to gH, \quad h \mapsto gh$$

é uma bijeção.

Prova. Observe que ψ é sobrejetora por construção. Assim, para concluir o desejado basta provar que ψ é injetora. Para isso, suponha $h_1, h_2 \in H$ tais que $\psi(h_1) = \psi(h_2)$. Então $gh_1 = gh_2$. Multiplicando os dois membros dessa igualdade por g^{-1} segue $h_1 = h_2$. Logo, ψ é injetora. □

Uma consequência imediata dessa proposição é o seguinte corolário.

Corolário 1.1.15. *Seja* H *um subgrupo de um grupo finito* G. *Então, para cada* $g \in G$, *temos:*

$$\mathcal{O}(H) = \#gH.$$

Definição 1.1.16. Seja G um grupo finito e H um subgrupo de G. O índice de H em G, denotado $[G : H]$, é a quantidade de elementos do conjunto quociente G/H.

Teorema 1.1.17 (Lagrange)**.** *Seja* G *um grupo finito e* H *um subgrupo de* G. *Então:*

$$\mathcal{O}(G) = \mathcal{O}(H) \cdot [G : H].$$

Em particular, a ordem de H *divide a ordem de* G.

Prova. Pela igualdade (1.1) e o corolário anterior temos o desejado. □

1.2 Homomorfismo de grupos

Definição 1.2.1. Sejam G e G' grupos. Uma função $f : G \to G'$ é chamada um *homomorfismo de grupos* se $f(ab) = f(a)f(b)$ para qualquer $a, b \in G$.

Exemplo 1.2.2. Seja G um grupo. Por razões óbvias, a aplicação identidade $\mathrm{Id}_G : G \to G$, $a \mapsto a$, é um homomorfismo de grupos.

Exemplo 1.2.3. A aplicação $\exp : \mathbb{R} \to \mathbb{R}^*$, $x \mapsto e^x$, é um homomorfismo de grupos.

Definição 1.2.4. Um homomorfismo de grupos $f : G \to G'$ é chamado *isomorfismo* se for uma bijeção. Dois grupos G e G' são ditos isomorfos se existe um isomorfismo $f : G \to G'$.

Notação: Usamos a notação $G \simeq G'$ para dizer que G e G' são isomorfos.

Dado um homomorfismo de grupos $f : G \to G'$, dois conjuntos importantes são:

$$\ker f := \{a \in G \mid f(a) = e'\},$$

onde e' denota a identidade de G', e

$$\operatorname{Im} f = \{y \in G' \mid y = f(a) \text{ para algum } a \in G\}.$$

Estes conjuntos são chamados, respectivamente, de *núcleo* e *imagem* do homomorfismo f.

Proposição 1.2.5. *Seja* $f : G \to G'$ *um homomorfismo de grupos. Então,* $\ker f$ *e* $\operatorname{Im} f$ *são subgrupos de* G *e* G', *respectivamente.*

Prova. Primeiro provaremos que $\ker f$ é subgrupo de G. Com efeito,

$$f(e) = f(ee) = f(e)f(e).$$

Assim,

$$f(e)^{-1}f(e) = f(e)^{-1}f(e)f(e),$$

ou seja,

$$f(e) = e'.$$

Logo, $e \in \ker f$. Agora suponhamos $a, b \in \ker f$. Então,

$$f(ab) = f(a)f(b) = e'e' = e'.$$

Logo, $ab \in \ker f$. Finalmente, suponha $a \in \ker f$. Temos

$$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) = e'f(a^{-1}) = f(a^{-1}).$$

Logo, $a^{-1} \in \ker f$. Portanto, $\ker f$ é subgrupo de G.

Agora provaremos que $\operatorname{Im} f$ é subgrupo de G'. Ao provarmos que $\ker f$ é um subgrupo G mostramos que $f(e) = e'$. Assim, $e' \in \operatorname{Im} f$. Suponhamos $y_1, y_2 \in \operatorname{Im} f$. Então, existem $a_1, a_2 \in G$ tais que $y_1 = f(a_1)$ e $y_2 = f(a_2)$. Logo, $y_1y_2 = f(a_1)f(a_2) = f(a_1a_2)$, ou seja, $y_1y_2 \in \operatorname{Im} f$. Para concluir, dado $y \in \operatorname{Im} f$ considere $a \in G$ tal que $y = f(a)$. Temos $yf(a^{-1}) = f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e'$. Da mesma forma, $f(a^{-1})y = e'$. Isso nos mostra que $f(a^{-1}) = y^{-1}$. Em particular, $y^{-1} \in \operatorname{Im} f$. □

Definição 1.2.6. Um subgrupo H de um grupo G é chamado *subgrupo normal* de G se $gH = Hg$ para qualquer $g \in G$.

Um fato que torna a definição de subgrupo normal importante é dado pela seguinte proposição:

Proposição 1.2.7. *Seja* H *um subgrupo normal de um grupo* G. *Então, a operação*

$$G/H \times G/H \to G/H, \quad (g_1H, g_2H) \mapsto g_1g_2H$$

está bem definida e a estrutura definida pelo conjunto G/H *e esta operação é um grupo.*

Prova. Para mostrar que a operação está bem definida suponhamos $g_iH = f_iH$ para $i = 1, 2$. Devemos provar que $g_1g_2H = f_1f_2H$, ou equivalentemente, que $(f_1f_2)^{-1}g_1g_2 \in H$. Observemos que $(f_1f_2)^{-1} = f_2^{-1}f_1^{-1}$. Assim, $(f_1f_2)^{-1}g_1g_2 = f_2^{-1}f_1^{-1}g_1g_2$. Como $g_1H = f_1H$ então $f_1^{-1}g_1 = h \in H$. Logo, $(f_1f_2)^{-1}g_1g_2 = f_2^{-1}hg_2$ Também temos $Hg_2 = g_2H = f_2H$. Desse modo, $\forall h \in H$ temos $h.g_2 = f_2h'$ para algum h, $h' \in H$, assim $f_2^{-1}.h.g_2 = h' \in H \Rightarrow f_2^{-1}Hg_2 \subset H$. Em particular, $(f_1f_2)^{-1}g_1g_2 = f_2^{-1}hg_2 \in H$. Portanto, segue que a operação está bem definida.

Agora mostraremos que G/H equipado com a operação em questão é um grupo. Dados $g_1H, g_2H, g_3H \in G/H$ temos

$$(g_1Hg_2H)g_3H = (g_1g_2H)g_3H = (g_1g_2)g_3H = g_1(g_2g_3)H = g_1H(g_2g_3)H = g_1H(g_2Hg_3H).$$

Para um $gH \in G/H$ arbitrário, temos

$$gHeH = geH = gH \quad \text{e} \quad eHgH = egH = gH.$$

Portanto eH é o elemento neutro de G/H Finalmente, dado $gH \in G/H$ temos

$$gHg^{-1}H = gg^{-1}H = eH \quad \text{e} \quad g^{-1}HgH = g^{-1}gH = eH.$$

Portanto, G/H é realmente um grupo. □

Proposição 1.2.8. *Seja* $f : G \to G'$ *um homomorfismo de grupos. Então* $H = \ker f$ *é um subgrupo normal de* G.

Prova. Dado um $g \in G$ arbitrário, devemos provar que $gH = Hg$. Suponhamos $a \in gH$. Então $a = gh$ para algum $h \in H$. Assim, $f(a) = f(gh) = f(g)f(h) = f(g)e' = f(g)$. Logo, $f(a)f(g^{-1}) = f(g)f(g^{-1})$, ou seja, $f(ag^{-1}) = e'$. Desse modo, $ag^{-1} \in H$. Logo, existe $h' \in H$ tal que $a.g^{-1} = h' \Rightarrow a = h'g$, ou seja, $a \in Hg$. Com isso concluímos que $gH \subset Hg$. A inclusão contrária é feita de forma análoga. □

Das Proposições 1.2.7 e 1.2.8 segue que se $f : G \to G'$ é um homomorfismo de grupos então G/H, $H = \ker f$, tem estrutura de grupo. É imediato verificar nessas circunstâncias que o mapa $\pi : G \to G/H$, $g \mapsto gH$, é um homomorfismo de grupos.

Teorema 1.2.9 (Primeiro teorema dos isomorfismos)**.** *Sejam* $f : G \to G'$ *um homomorfismo de grupos e* $H = \ker f$. *Então existe um único homomorfismo injetor* $\bar{f} : G/H \to G'$ *tal que* $f = \bar{f} \circ \pi$, *onde* $\pi : G \to G/H$ *é tal que* $g \mapsto gH$ *para cada* $g \in G$. *Em particular,* $\bar{f}$ *estabelece um isomorfismo de* $G/H \simeq \operatorname{Im} f$.

Prova. Primeiro provaremos a existência de $\bar{f} : G/H \to G'$. Para isso, definiremos $\bar{f}(gH) = f(g)$ para cada $gH \in G/H$. Afirmamos que $\bar{f}$ está bem definida. Com efeito, suponhamos que $gH = g'H$. Então $g^{-1}g' \in H$. Assim, $f(g)^{-1}f(g') = f(g^{-1})f(g') = f(g^{-1}g') = e'$. Logo, $f(g) = f(g')$.

Agora mostraremos que $\bar{f}$ é injetora. Para isso, digamos que $\bar{f}(gH) = \bar{f}(g'H)$. Então $f(g) = f(g')$. Logo, $e' = f(g)^{-1}f(g') = f(g^{-1})f(g') = f(g^{-1}g')$, ou seja, $g^{-1}g' \in H$. Logo, $gH = g'H$.

O fato de que $\bar{f}$ é homomorfismo segue de forma trivial.

Também temos, para cada $g \in G$, que

$$\bar{f} \circ \pi(g) = \bar{f}(\pi(g)) = \bar{f}(gH) = f(g).$$

Logo, $f = \bar{f} \circ \pi$ como desejado.

Para mostrar a unicidade suponhamos $\widetilde{f} : G/H \to G'$ tal que $f = \widetilde{f} \circ \pi$. Então, para cada $gH \in G/H$ temos:

$$\widetilde{f}(gH) = \widetilde{f}(\pi(g)) = \widetilde{f} \circ \pi(g) = f(g) = \bar{f}(gH).$$

Logo, $\widetilde{f} = \bar{f}$.

Por razões óbvias temos que $\operatorname{Im} \bar{f} = \operatorname{Im} f$. Como $\bar{f}$ é injetora, segue que ela é uma bijeção sobre sua imagem, portanto, um isomorfismo sobre a imagem. □

1.3 Corpos residuais

Definição 1.3.1. Um *corpo* é uma estrutura que consiste de um conjunto não vazio k, uma operação de *adição* $+ : k \times k \to k$ e uma operação de *multiplicação* $\cdot : k \times k \to k$ sujeitos às seguintes regras:

(a) **A adição é associativa:** para qualquer $a, b, c \in k$, $(a + b) + c = a + (b + c)$.

(b) **A adição é comutativa:** para qualquer $a, b \in k$, $a + b = b + a$.

(c) **Existe elemento neutro para a adição:** existe $0 \in k$ tal que para qualquer $a \in k$, $0 + a = a + 0 = a$.

(d) **Existência do elemento inverso para a adição:** Para cada $a \in k$ existe $-a \in k$ tal que $a + (-a) = (-a) + a = 0$.

(e) **A multiplicação é associativa:** para qualquer $a, b, c \in k$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(f) **A multiplicação é comutativa:** para qualquer $a, b \in k$, $a \cdot b = b \cdot a$.

(g) **Existe elemento neutro para a multiplicação:** existe $1 \in k$ tal que para qualquer $a \in k$, $a \cdot 1 = 1 \cdot a = a$.

(h) **Existência do elemento inverso para a multiplicação:** para cada $a \in k - \{0\}$ existe $a^{-1} \in k$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

(i) **A multiplicação é distributiva com relação à adição:** para qualquer $a, b, c \in k$, $a \cdot (b + c) = a \cdot b + a \cdot c$

Observamos que a definição não impede que tenhamos dois corpos distintos usando um mesmo conjunto k. Para isso, basta que se defina operações distintas de adição ou multiplicação no conjunto k. Todavia, para efeito de simplificar a escrita é comum fazer referência ao conjunto k para representar toda a estrutura. Esse abuso de notação não costuma causar confusão pois tipicamente as operações estão subentendidas. Também é hábito suprimir o símbolo que representa multiplicação, ou seja, em vez de escrever $a \cdot b$ escreve-se simplesmente ab.

Nota-se facilmente que a estrutura de corpo é uma abstração de estruturas que nos são familiares desde os tempos de escola. De fato, os racionais $\mathbb{Q}$, os reais $\mathbb{R}$ e os complexos $\mathbb{C}$ com suas operações usuais de adição e multiplicação são exemplos da estrutura de corpo. Notavelmente, o conjunto dos inteiros $\mathbb{Z}$ não é um corpo, uma vez que nem todo elemento de $\mathbb{Z}$ satisfaz a propriedade (h) da Definição 1.3.1.

1.4 Aritmética modular

Na seção anterior apresentamos o conceito de corpo. Vimos que exemplos de corpos são os racionais, os reais e os complexos. Todavia, todos esses são exemplos de corpos infinitos. Nessa seção mostraremos a existência de corpos finitos. Um ingrediente fundamental para esse propósito é a seguinte noção

Definição 1.4.1. Seja n um número inteiro positivo. Dizemos que um número inteiro a é *congruente módulo* n a um número inteiro b se n divide $a - b$.

Notação: Escrevemos $a \equiv b \mod n$ para denotar que a é congruente a b módulo n. Por outro lado, a notação $a \not\equiv b \mod n$ significa que a não é congruente a b módulo n.

Exemplo 1.4.2. Temos que 5 divide $16 - 1$. Logo, $16 \equiv 1 \mod 5$. Por outro lado, 5 não divide $16 - (-1)$. Logo, $16 \not\equiv -1 \mod 5$.

Proposição 1.4.3. *Seja n um inteiro positivo. Então congruência módulo n é uma relação de equivalência em $\mathbb{Z}$.*

Prova. Dado $a \in \mathbb{Z}$ temos que n divide $a - a = 0$. Logo, $a \equiv a \mod n$.

Agora suponhamos $a, b \in \mathbb{Z}$ tais que $a \equiv b \mod n$ então n divide $a - b$. Em particular, divide $-(a-b) = b - a$. Logo, $b \equiv a \mod n$.

Finalmente, consideremos $a, b, c \in \mathbb{Z}$ tais que $a \equiv b \mod n$ e $b \equiv c \mod n$. Então, n divide $a - b$ e $b - c$. Logo, n divide $(a-b)+(b-c) = a - c$, ou seja, $a \equiv c \mod n$. □

Representamos a classe de equivalência de um elemento $a \in \mathbb{Z}$ com respeito a relação de congruência módulo n, por $\overline{a}$ (lembre que, por definição, $\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \mod n\}$). O conjunto formado por todas as classes de equivalência de elementos de $\mathbb{Z}$ será denotado por $\mathbb{Z}_n$.

Proposição 1.4.4. *Seja n um inteiro positivo. Então, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Além disso, a cardinalidade de $\mathbb{Z}_n$ é n.*

Prova. Para provar a primeira parte da proposição é suficiente mostrar que a classe de um elemento $a \in \mathbb{Z}$ é necessariamente igual a classe de um inteiro compreendido entre 0 e $n-1$. Para isso, efetuamos a divisão euclidiana de a por n obtendo

$$a = nq + r$$

onde $0 \leqslant r \leqslant n-1$. Esta igualdade nos dá que $n | a - r$. Logo,

$$a \equiv r \mod n.$$

Logo, $\overline{a} = \overline{r}$ com $0 \leqslant r \leqslant n-1$. Assim, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ como queríamos mostrar.

Para a segunda parte da proposição devemos mostrar que os elementos do conjunto $\{\overline{0}, \ldots, \overline{n-1}\}$ são dois a dois distintos. Para isso, suponhamos que i, j são números inteiros entre 0 e $n-1$ distintos. Sem perda de generalidade, suponhamos $i < j$. Temos $0 < j - i \leqslant n-1$. Logo, $j - i$ é um número positivo menor que n. Em particular, n não divide $j - i$, ou seja, $j \not\equiv i \mod n$. Portanto, $\overline{i} \neq \overline{j}$. □

Podemos definir operações de adição e multiplicação em $\mathbb{Z}_n$ através das seguintes igualdades:

$$\overline{a_1} + \overline{a_2} := \overline{a_1 + a_2} \quad \text{e} \quad \overline{a_1} \cdot \overline{a_2} := \overline{a_1 \cdot a_2}$$

para cada $\overline{a_1}, \overline{a_2} \in \mathbb{Z}_n$.

Proposição 1.4.5. *As operações de adição e multiplicação em $\mathbb{Z}_n$ acima estão bem definidas. Além disso, as seguintes propriedades são verificadas:*

(a) *Para qualquer* $\overline{a_1}, \overline{a_2}, \overline{a_3} \in \mathbb{Z}_n$, $(\overline{a_1} + \overline{a_2}) + \overline{a_3} = \overline{a_1} + (\overline{a_2} + \overline{a_3})$.

(b) *Para qualquer* $\overline{a_1}$, $\overline{a_2} \in \mathbb{Z}_n$, $\overline{a_1} + \overline{a_2} = \overline{a_2} + \overline{a_1}$.

(c) $\overline{0} \in \mathbb{Z}_n$ *é tal que para qualquer* $\overline{a_1} \in \mathbb{Z}_n$, $\overline{0} + \overline{a_1} = \overline{a_1} + \overline{0} = \overline{a_1}$.

(d) *Para cada* $\overline{a_1} \in \mathbb{Z}_n$ *existe* $\overline{-a_1} \in \mathbb{Z}_n$ *tal que* $\overline{a_1} + (\overline{-a_1}) = (\overline{-a_1}) + \overline{a_1} = \overline{0}$.

(e) *Para qualquer* $\overline{a_1}, \overline{a_2}, \overline{a_3} \in \mathbb{Z}_n$, $(\overline{a_1} \cdot \overline{a_2}) \cdot \overline{a_3} = \overline{a_1} \cdot (\overline{a_2} \cdot \overline{a_3})$.

(f) *Para qualquer* $\overline{a_1}, \overline{a_2} \in \mathbb{Z}_n$, $\overline{a_1} \cdot \overline{a_2} = \overline{a_2} \cdot \overline{a_1}$.

(g) *Existe* $1 \in \mathbb{Z}_n$ *tal que para qualquer* $\overline{a_1} \in \mathbb{Z}_n$ $\overline{a_1} \cdot 1 = 1 \cdot \overline{a_1} = I$.

(h) *Para qualquer* $\overline{a_1}, \overline{a_2}, \overline{a_3} \in \mathbb{Z}_n$, $\overline{a_1} \cdot (\overline{a_2} + \overline{a_3}) = \overline{a_1} \cdot \overline{a_2} + \overline{a_1} \cdot \overline{a_3}$.

Prova. Primeiro provaremos que as operações de adição e multiplicação de $\mathbb{Z}_n$ estão bem definidas. Para isso, suponhamos $\overline{a_1}, \overline{a_2}, \overline{b_1}, \overline{b_2} \in \mathbb{Z}_n$ tais que

$$\overline{a_1} = \overline{b_1} \quad \text{e} \quad \overline{a_2} = \overline{b_2}.$$

Em particular, n divide $a_1 - b_1$ e n divide $a_2 - b_2$. Logo, n divide $(a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$, ou seja, $\overline{a_1 + a_2} = \overline{b_1 + b_2}$. Segue desse argumento que a adição está bem definida.

Agora vamos provar que a multiplicação também está bem definida. Como n divide $a_1 - b_1$ e n divide $a_2 - b_2$ então n divide $a_2(a_1 - b_1)$ e n divide $b_1(a_2 - b_2)$. Logo, n divide $a_2(a_1 - b_1) + b_1(a_2 - b_2) = a_1a_2 - b_1b_2$, ou seja, $\overline{a_1a_2} = \overline{b_1b_2}$. Assim, a multiplicação também está bem definida.

A prova de todas as propriedades acima segue do fato de que dentro da barra a conta é realizada em $\mathbb{Z}$, e em $\mathbb{Z}$ tais propriedades são verificadas. □

Observe da proposição acima que, com exceção da propriedade da existência do elemento inverso para a multiplicação, $\mathbb{Z}_n$ satisfaz todas as demais propriedades da definição de corpo. De modo geral, podemos dizer que $\mathbb{Z}_n$ é um exemplo da estrutura de *anel comutativo com identidade*. Chamamos $\mathbb{Z}_n$ de *anel dos resíduos módulo* n. Na próxima proposição damos uma caracterização de quando $\mathbb{Z}_n$ é corpo.

Proposição 1.4.6. $\mathbb{Z}_n$ *é corpo se, e somente se,* n *é primo.*

Prova. Primeiro suponhamos que n é primo. Então, dado um inteiro $1 \leqslant a \leqslant n - 1$ temos que $mdc(a, n) = 1$. Logo, existem inteiros x, y tais que $ax + yn = 1$. Assim:

$$\overline{a}.\overline{x} = \overline{a}.\overline{x} + \overline{y}.\overline{n} = \overline{a.x} + \overline{y.n} = \overline{ax + yn} = \overline{1}.$$

Isso nos mostra que qualquer elemento em $\mathbb{Z}_n \setminus \{\overline{0}\}$ é invertível. Portanto, $\mathbb{Z}_n$ é corpo.

Reciprocamente, suponhamos que $\mathbb{Z}_n$ é corpo. Para mostrar que n é primo é suficiente mostrarmos que n não é divisível pelos elementos do conjunto $\{2, \ldots, n-1\}$.

Assim, consideremos $a \in \{2, \ldots, n-1\}$. Temos então que $\overline{a} \neq \overline{0}$. Como $\mathbb{Z}_n$ é corpo, existe $\overline{x} \in \mathbb{Z}_n \setminus \{0\}$ tal que $\overline{a}.\overline{x} = 1$. Logo, $ax - 1$ é divisível por n. Logo, existe $y \in \mathbb{Z}$ tal que $ax + yn = 1$. Logo, $mdc(a, n) = 1$. Logo, a não divide n. Logo n é primo. □

Dado um número primo p usaremos $\mathbb{Z}_p^*$ para denotar o conjunto $\mathbb{Z}_p \setminus \{\overline{0}\}$. Uma consequência do fato de $\mathbb{Z}_p$ ser corpo é que o conjunto $\mathbb{Z}_p^*$ é um grupo. O grupo $\mathbb{Z}_p^*$ será bastante importante na demonstração do principal resultado desse trabalho.

Capítulo 2

O teorema de Ramsey e a equação de Fermat para corpos finitos

Iniciamos esse capítulo tratando de algumas noções básicas em torno do conceito de grafos. Estas noções serão necessárias para podermos abordar a primeira versão do celebrado Teorema de Ramsey. Também apresentamos aqui uma versão mais geral desse teorema envolvendo o conceito de coloração. Finalizamos o capítulo com os principais resultados desse trabalho, i. e., o teorema de Schur e a versão do Último Teorema de Fermat para corpos residuais. As principais referências para essa parte do texto são [1] e [3].

2.1 Noções de teoria de grafos

Definição 2.1.1. Um *grafo G* é uma terna (V, E, I), onde V e E são conjuntos finitos e $I \subseteq V \times E$ satisfaz

$$1 \leqslant |\{v \in V : (v, e) \in I\}| \leqslant 2, \tag{2.1}$$

para qualquer $e \in E$.

Em algumas situações é útil denotarmos V, E e I, respectivamente, por $V(G)$, $E(G)$ e $I(G)$. Os elementos desses conjuntos são chamados, nesta ordem, de *vértices*, *arestas* e *incidências* do grafo G.

Dizemos que uma aresta e é *incidente* a um vértice v no grafo G quando $(v, e) \in I$. Dois vértices no grafo G são ditos *adjacentes* se existe uma aresta que incide a ambos.

Quando uma aresta é incidente a exatamente um vértice de G, então é chamada de *laço*. Dizemos que duas arestas e e f de uma grafo *G*, estão em *paralelo* quando ambas são incidentes a vértices u e v, com $u \neq v$ e $e \neq f$.

Definição 2.1.2. Um grafo G é dito *simples* quando não possui laços e nem arestas em paralelo.

A representação geométrica de um grafo no plano dar-se da seguinte maneira: cada vértice corresponde a um ponto e cada aresta a uma linha, cujo extremos representam os vértices incidentes a esta aresta.

Exemplo 2.1.3. Seja G um grafo onde

$$V(G) = \{v_1, \ldots, v_{11}\}, \quad E(G) = \{e_1, \ldots, e_{17}\}$$

e

$$I(G) = \{(v_1, e_1), (v_2, e_1), (v_2, e_2), (v_4, e_2), (v_4, e_3), (v_9, e_3), (v_2, e_4), (v_9, e_4), (v_2, e_5), (v_{10}, e_5),$$

$$(v_6, e_6), (v_9, e_6), (v_3, e_7), (v_6, e_7), (v_3, e_8), (v_5, e_8), (v_5, e_9), (v_7, e_9), (v_6, e_{10}), (v_8, e_{10}), (v_7, e_{11}),$$

$$(v_8, e_{11}), (v_8, e_{12}), (v_{10}, e_{12}), (v_{10}, e_{13}), (v_{11}, e_{13}), (v_8, e_{14}), (v_{11}, e_{14}), (v_1, e_{15}), (v_3, e_{16}), (v_4, e_{16}),$$

$$(v_3, e_{17}), (v_4, e_{17}), (v_9, e_{18}), (v_{10}, e_{18})\}.$$

A representação geométrica deste grafo é dada pela seguinte figura:

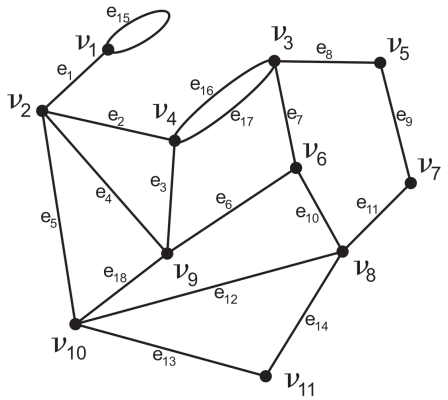


Figura 2.1: Exemplo de grafo

Observe que este grafo G possui um laço, aresta e_{15}, e duas arestas em paralelo, arestas e_{16} e e_{17}. Sendo assim, G não é simples.

Exemplo 2.1.4. Seja G um grafo onde

$$V(G) = \{v_1, v_2, \ldots, v_{10}\}, \quad E(G) = \{e_1, e_2, \ldots, e_{15}\}$$

e

$$I(G) = \{(v_1, e_1), (v_1, e_9), (v_1, e_{10}), (v_2, e_2), (v_2, e_1), (v_3, e_2), (v_3, e_3), (v_3, e_4), (v_3, e_7), (v_3, e_5),$$

$$(v_4, e_4), (v_4, e_8), (v_5, e_3), (v_5, e_{14}), (v_5, e_6), (v_6, e_8), (v_6, e_9), (v_6, e_{11}), (v_7, e_7), (v_7, e_{12}), (v_7, e_{13}),$$

$$(v_7, e_6), (v_8, e_{15}), (v_8, e_{12}), (v_8, e_{11}), (v_8, e_{10}), (v_8, e_5), (v_9, e_{15}), (v_{10}, e_{13}), (v_{10}, e_{14})\}.$$

A representação geométrica desse grafo é dada pela seguinte figura:

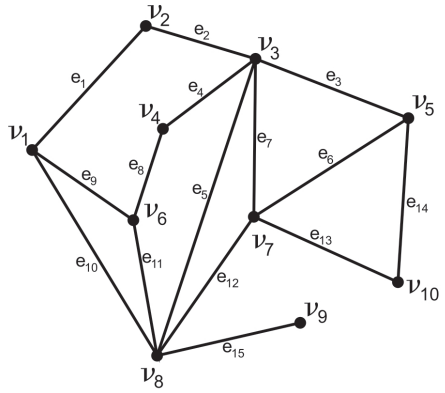


Figura 2.2: Exemplo de grafo

Observe que este grafo G não possui laço nem aresta em paralelo. Assim, G é um exemplo de grafo simples.

Uma razão para a estrutura de grafo ser tão importante é a quantidade de situações que podem ser modeladas por ela. Existem várias aplicações para os grafos, dentre elas podemos citar: logística de transporte, distância entre cidades, fluxo de um jogo, conexões de comunicação ligando satélites, linhas de metrô e árvores genealógicas. Vejamos alguns exemplos:

Exemplo 2.1.5. Seja $k[X_1, \ldots, X_n]$ um anel de polinômios com coeficientes sobre um corpo k e em n variáveis. Dado um subconjunto $A \subset \{1, \ldots, n\} \times \{1, \ldots, n\}$, considere o ideal $J = (\{X_i X_j \mid (i, j) \in A\})$. Para um tal ideal podemos associar um grafo G da seguinte forma:

$$V(G) := \text{conjunto das variáveis que aparecem como fator de algum gerador de} J;$$

$$E(G) := \{X_i X_j \mid X_i X_j \in I\}$$

(obviamente, $E(G)$ já determina $I(G)$).

Exemplo 2.1.6. Um grupo de n pessoas pode ser pensado como um grafo simples onde cada pessoa corresponde a um vértice e dois vértices desse grafo são adjacentes se as respectivas pessoas se conhecem.

Exemplo 2.1.7. Dado um mapa de um país (região, estado, etc) podemos pensar cada estado desse país como um vértice e que dois desses vértices são adjacentes se os respectivos estados possuírem fronteiras. Na figura temos o grafo do mapa da região nordeste do Brasil.

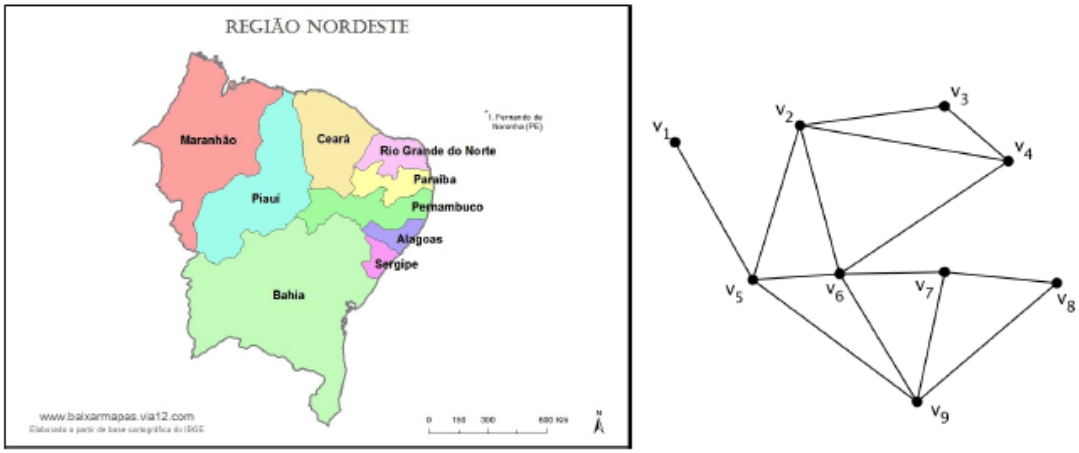


Figura 2.3: Mapa da região do Nordeste do Brasil e o grafo que lhe representa

Definição 2.1.8. Um grafo simples $G = (V, E, I)$ é dito *completo* se cada par de vértices em G é adjacente.

Veja abaixo, alguns exemplos de grafos completos:

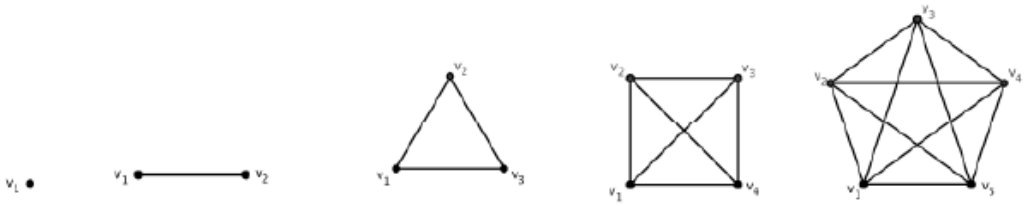


Figura 2.4: K_1, K_2, K_3, K_4 e K_5, respectivamente

A notação usual para um grafo simples completo com n vértices é K_n. Esta notação é uma homenagem ao matemático polonês Kasemir Kuratowski, que foi o primeiro a obter, em 1930, uma caracterização completa de planaridade, por meio deste tipo de grafo.

Outras noções importantes em teoria dos grafos, e que faremos uso nesse trabalho, são as de subgrafo, clique e independente de um grafo, cujas definições seguem abaixo.

Definição 2.1.9. Um *subgrafo* de um grafo G é qualquer grafo H tal que $V(H) \subseteq V(G)$,$E(H) \subseteq E(G)$ e $I(H) \subseteq I(G)$. Um subgrafo H de G é dito *subgrafo induzido* se cada par de vértices $u, v \in H$ adjacentes em G são também adjacentes em H.

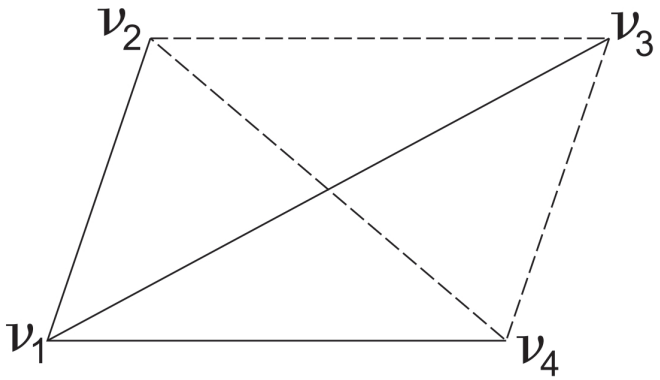
Definição 2.1.10. Seja $G = (V, E, I)$ um grafo.

(a) Um *clique* em G é um subgrafo completo de G.

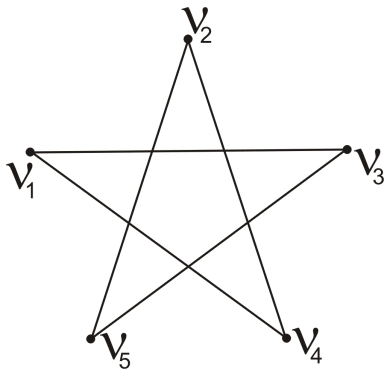
(b) Um *independente* de G é um subgrafo induzido H de G tal que nenhum par de vértices é adjacente.

Exemplo 2.1.11. Todo grafo com seis vértices contém um clique ou um independente com 3 vértices.

Para verificar essa afirmação, faremos a seguinte representação: quando dois vértices forem adjacentes utilizaremos linha cheia e caso contrário usaremos linha tracejada. Fixemo-nos em um vértice v_1 de tal grafo. Nesse vértice incidem 5 linhas onde, pelo princípio da casa dos pombos, devemos ter pelo menos 3 dessas linhas do mesmo tipo. Digamos, sem perda de generalidade, que estas sejam linhas cheias e que elas vão para os vértices v_2, v_3 e v_4. Se uma das linhas no triângulo $v_2v_3v_4$ for cheia, por exemplo a linha ligando v_2 a v_3, então temos um K_3 formado pelo triângulo $v_1v_2v_3$, caso contrário temos um independente formado pelos vértices v_2, v_3 e v_4 como mostra a Figura abaixo:



Podemos ver ainda que seis é o menor número n com a propriedade de que todo grafo com n vértices contém um clique ou um independente com 3 vértices. De fato, o grafo abaixo tem 5 vértices e não contém clique nem independente com 3 vértices



Observação 2.1.12. Observemos que, na perspectiva do Exemplo 2.1.6, o exemplo anterior pode ser enunciado da seguinte maneira: *Qualquer grupo de seis pessoas possuirá ou 3 pessoas que se conhecem mutuamente ou 3 pessoas que se desconhecem mutuamente.*

A afirmação contida no Exemplo 2.1.11 pode ser generalizada de diversas formas, e são estas generalizações o conteúdo da teoria de Ramsey tal como veremos em seguida.

2.2 A versão original do Teorema de Ramsey

O Teorema de Ramsey é um resultado clássico obtido por Frank Plumpton Ramsey no ano de 1930. Com o decorrer do tempo, outras versões (que também iremos apresentar) foram surgindo, todavia a original é esta que segue.

Teorema 2.2.1 (Ramsey 1930)**.** *Para cada* $r \in \mathbb{N}$ *existe um* $n \in \mathbb{N}$ *tal que cada grafo de ordem pelo menos* n *contém um clique ou um independente com* r *vértices.*

Prova. Para $r = 1$, o teorema é trivial. Suponhamos então que $r \geqslant 2$ e definamos $n := 2^{2r-3}$. Suponha G um grafo arbitrário de ordem pelo menos n.

Afirmação 1: *Existe uma sequência de conjuntos* $V_1, \ldots, V_{2r-2}$ *e de vértices* $v_i \in V_i$ *satisfazendo as seguintes condições:*

(i) $|V_i| = 2^{2r-2-i}$ $(i = 1, \ldots, 2r-2)$.

(ii) $V_i \subset V_{i-1} \setminus \{v_{i-1}\}$ $(i = 2, \ldots, 2r-2)$.

(iii) v_{i-1} *é adjacente a todo ou a nenhum vértice em* V_i $(i = 2, \ldots, 2r-2)$.

Podemos considerar $V_1 \subset V(G)$ sendo qualquer subconjunto de cardinalidade 2^{2r-3}. Obviamente, para qualquer $v_1 \in V_1$ teremos as condições (i)-(iii). Agora, para $1 < i \leqslant 2r-2$, suponhamos v_{i-1} e V_{i-1} construídos satisfazendo (i)-(iii). Como $|V_{i-1} \setminus \{v_{i-1}\}| = 2^{2r-1-i} - 1$,

então ou pelo menos 2^{2r-2-i} vértices em $V_{i-1} \setminus \{v_{i-1}\}$ são adjacentes a v_{i-1} ou pelo menos 2^{2r-2-i} vértices em $V_{i-1} \setminus \{v_{i-1}\}$ não são adjacentes a v_{i-1}. Dessa coleção com pelo menos 2^{2r-2-i} vértices podemos escolher um subconjunto V_i com 2^{2r-2-i} elementos e fixando um $v_i \in V_i$ temos o desejado para concluir a afirmação.

Afirmação 2: *Sejam* A *e* B *subconjuntos de* $\{v_1, \ldots, v_{2r-3}\}$*, tais que* A *é formado pelos vértices que são adjacentes a* v_{2r-2} *e* B *é formado pelos vértices que não são adjacentes a* v_{2r-2}*. Então,* $|A| \geqslant r-1$ *ou* $|B| \geqslant r-1$.

Suponhamos que ocorra o contrário. Então, $|A| \leqslant r-2$ e $|B| \leqslant r-2$. Logo, $|A|+|B| \leqslant 2r-4$. Mas isso é um absurdo já que $|A| + |B| = 2r-3$. Portanto, temos a afirmação 2.

À luz dessa afirmação, podemos concluir a existência de um subconjunto C de $\{v_1, \ldots, v_{2r-2}\}$ com exatamente $r-1$ vértices onde ou todos são adjacentes a v_{2r-2} ou todos não são adjacentes a v_{2r-2}.

Afirmação 3: $C \cup \{v_{2r-2}\}$ *induz um clique ou um independente com* r *vértices em* G.

Suponhamos que todo vértice de C seja vizinho a v_{2r-2}. Digamos que $C = \{v_{i_1}, \ldots, v_{i_{r-1}}\}$ com $1 \leqslant i_1 < \cdots < i_{r-1} \leqslant 2r-3$. Notemos que v_{i_1} é adjacente a cada vértice de V_{i_1+1} ou a nenhum, isso pela maneira que definimos os v_i e V_i. Como já sabemos que v_{i_1} é adjacente a v_{2r-2} e cada $\{v_{i_2}, \ldots, v_{i_{r-1}}\} \cup \{v_{2r-2}\} \subset V_{i_1+1}$ então temos em particular que v_{i_1} se liga a todos os demais vértices de C. Repetimos o mesmo argumento agora para v_{i2} e observamos que este também se liga a todos os demais vértices de C. Repetindo esse argumento até $v_{i_{r-1}}$ temos que C induz um clique com r vértices em G. Se tivéssemos suposto que nenhum vértice de C é vizinho a v_{2r-2} obteríamos de forma análoga que C induz um independente com r vértices em G. □

O menor número natural n associado a r como no teorema acima é chamado o *número de Ramsey* de r e o denotamos por $R(r)$. Percebemos na demonstração acima que para cada inteiro positivo r, o número 2^{2r-3} é uma cota superior para $R(r)$. A busca por cotas superiores e inferiores para o número de Ramsey é de grande interesse, uma vez que a determinação exata do seu valor é um problema bastante difícil. Para se ter ideia da dificuldade, os únicos valores de r para os quais se conhece o valor exato de $R(r)$ são $r = 1, 2, 3$ ou 4.

Notemos em particular que a partir do teorema de Ramsey acima temos:

Corolário 2.2.2. Dado um número inteiro positivo r e duas cores distintas fixadas então existe $n \in \mathbb{N}$ tal que, independente da maneira de colorirmos as arestas de K_n com essas duas cores, existirá um subgrafo completo de K_n com vértices cujas arestas possuem a mesma cor.

Na seção seguinte apresentaremos uma generalização para esse corolário.

2.3 Algumas generalizações do Teorema de Ramsey

Para cada inteiro positivo n, usaremos o símbolo $[n]$ para denotar o conjunto $\{1, \ldots, n\}$. Dados um inteiro positivo k e um conjunto não vazio A, a notação $[A]^k$ significará o conjunto de todos os subconjuntos de A com exatamente k elementos. Abreviadamente, chamaremos os elementos de $[A]^k$ de k-subconjuntos de A. Portanto sempre que nos reportarmos a um k-conjunto ou k-subconjunto, estamos nos referindo respectivamente a conjuntos e subconjuntos com k elementos.

Definição 2.3.1. Seja c um inteiro positivo e X um conjunto com pelo menos c elementos. Uma c-coloração de X é uma função $\varphi : X \to [c]$ sobrejetiva.

Note que podemos pensar numa c-coloração de X como uma partição de X em c classes onde cada classe é distinguida pela cor.

Definição 2.3.2. Sejam X um conjunto não vazio, k um inteiro positivo e $\varphi : [X]^k \to [c]$ uma c-coloração de $[X]^k$. Um subconjunto Y de X é dito *monocromático* se todos os elementos de $[Y]^k$ possuem a mesma cor.

Exemplo 2.3.3. Seja $X = \{a_1, a_2, a_3, a_4\}$. Temos nesse caso que

$$[X]^2 = \{\{a_1, a_2\}, \{a_1, a_3\}, \{a_1, a_4\}, \{a_2, a_3\}, \{a_2, a_4\}, \{a_3, a_4\}\}$$

Consideremos a 3-coloração $\varphi : [X]^2 \to [1, 2, 3]$ tal que

$$\varphi(\{a_1, a_2\}) = 1, \quad \varphi(\{a_1, a_3\}) = 1, \quad \varphi(\{a_1, a_4\}) = 2,$$
$$\varphi(\{a_2, a_3\}) = 1, \quad \varphi(\{a_2, a_4\}) = 3, \quad \varphi(\{a_3, a_4\}) = 1.$$

Para o subconjunto $Y = \{a_1, a_2, a_3\}$ de X, temos

$$[Y]^2 = \{\{a_1, a_2\}, \{a_1, a_3\}, \{a_2, a_3\}\}.$$

Além disso, todo elemento de $[Y]^2$ tem cor igual a 1. Logo, Y é monocromático. Por outro lado, consideremos o subconjunto $Y_1 = \{a_2, a_3, a_4\}$ de X. Observe neste caso que

$$[Y_1]^2 = \{\{a_2, a_3\}, \{a_2, a_4\}, \{a_3, a_4\}\}.$$

Como $\{a_2, a_3\}$ e $\{a_2, a_4\}$ são elementos de $[Y_1]^2$ com cores distintas segue que Y_1 não é monocromático.

A primeira generalização que faremos do teorema de Ramsey é:

Teorema 2.3.4. *Sejam* k *e* c *inteiros positivos e* X *um conjunto infinito. Se* $[X]^k$ *é colorido com* c *cores, então* X *contém um subconjunto infinito monocromático.*

Prova. Provaremos o teorema aplicando indução sobre k com c fixado. Para $k = 1$ a afirmação segue trivialmente. Suponhamos então $k > 1$.

Vamos construir uma sequência infinita $X_0, X_1, ...$ de subconjuntos infinitos de X e elementos $x_i \in X_i$ com as seguintes propriedades:

(i) $X_{i+1} \subset X_i - \{x_i\}$.

(ii) todos os k-subconjuntos $\{x_i\} \cup Z$ com $Z \in [X_{i+1}]^{k-1}$ tem a mesma cor, a qual associaremos a x_i.

Definamos $X_0 := X$ com $x_0 \in X$ qualquer. Suponhamos definido X_i onde a cor de $Z \in [X_i - \{x_i\}]^{k-1}$ é igual a cor de $\{x_i\} \cup Z$ em $[X]^k$. Então, por hipótese de indução, $[X_i - \{x_i\}]^{k-1}$ com esta coloração possui um subconjunto infinito monocromático que definiremos como X_{i+1}. Notemos em particular que X_{i+1} e $x_{i+1} \in X_{i+1}$ arbitrários satisfazem (i) e (ii).

Como c é finito, existem infinitos x_i associados a uma mesma cor. A totalidade desses x_i nos dá um subconjunto infinito monocromático de X. □

Observação 2.3.5. Notemos que a coloração de $[X_i - \{x_i\}]^{k-1}$ fornecida na demonstração acima pode eventualmente usar menos que c cores. Contudo, se o resultado vale para c a *fortiori* valerá para um número menor de cores.

Lema 2.3.6. *Sejam* $V_0, V_1, \ldots$ *uma sequência infinita de conjuntos finitos não vazios e* G *um grafo sobre a união deles. Assumamos que cada vértice* v *em um conjunto* V_n *com* $n \geqslant 1$ *tem um vizinho* $f(v)$ *em* V_{n-1}. *Então* G *contém um caminho infinito* $v_0v_1 \ldots$ *com* $v_n \in V_n$ *para cada* n.

Prova. Seja P o conjunto de todos os caminhos da forma $vf(v)f(f(v))\ldots$ encerrando em V_0. Como V_0 é finito e P é infinito então uma quantidade infinita de caminhos em P encerram num mesmo vértice $v_0 \in V_0$. Destes caminhos também uma quantidade infinita passam por um vértice $v_1 \in V_1$, pois V_1 é finito. Destes, uma quantidade infinita passam por um vértice $v_2 \in V_2$ e assim sucessivamente. De etapa em etapa sempre sobra uma quantidade infinita de conjuntos a considerar e dessa forma, para cada n definimos um $v_n \in V_n$. Da forma que definimos, cada v_n é vizinho de v_{n-1}, assim $v_0v_1 \ldots$ é precisamente um caminho como da conclusão do lema. □

Teorema 2.3.7. *Para todo* $k, c, r \geqslant 1$ *existe um inteiro* $n \geqslant k$ *tal que cada* n*-conjunto* X *contém um* r*-subconjunto monocromático com respeito a qualquer* c*-coloração de* $[X]^k$.

Prova. Podemos supor $X = [n]$. Digamos que o teorema falhe para alguma terna (k, c, r). Então, para cada $n \geqslant k$ existe uma c-coloração $[n]^k \to [c]$ tal que $[n]$ não contém r-subconjunto monocromático. Se chamarmos tal coloração de **ruim**, estamos assumindo que para todo $n \geqslant k$ existe uma coloração ruim de $[n]^k$. Nosso objetivo é associar a estas colorações ruins de $[n]^k$ uma coloração de $[\mathbb{N}]^k$ que irá contradizer o Teorema.

Para todo $n \geqslant k$ consideremos $V_n \neq \emptyset$ o conjunto de todas as colorações ruins de $[n]^k$. Para $n > k$, as restrições $f(g)$ de qualquer $g \in V_n$ a $[n-1]^k$ ainda são ruins e, por conseguinte ruins em V_{n-1}. Pelo Lema , existe uma sequência infinita $g_k, g_{k+1}, \ldots$ de colorações ruins $g_n \in V_n$ tais que $f(g_n) = g_{n-1}$ para todo $n > k$. Para cada $m \geqslant k$, todas as g_n colorações, com $n \geqslant m$, também são colorações ruins quando restritas a $[m]^k$. Assim, para cada $Y \in [\mathbb{N}]^k$ o valor de $g_n(Y)$ coincide para todo $n > max(Y)$. Seja $g(Y)$ o valor comum de $g_n(Y)$. Então g é uma coloração ruim de $[\mathbb{N}]^k$: cada r-conjunto $S \subset \mathbb{N}$ está contido em algum $[n]$, para n suficientemente grande. Sendo assim, S não pode ser monocromático, pois g coincide sobre $[n]^k$ com a coloração ruim g_n. □

2.4 Aplicação

Um resultado crucial para deduzirmos a versão do Último Teorema de Fermat para corpos residuais é o seguinte Lema :

Lema 2.4.1. *Seja* c *um inteiro positivo. Então existe* $n \in \mathbb{N}$ *tal que para cada* c*-coloração* $\varphi : [n] \to [c]$ *existem* $x, y, z \in [n]$ *com* $\varphi(x) = \varphi(y) = \varphi(z)$ *e* $x + y = z$.

Prova. Pelo Teorema de Ramsey, existe $n \in \mathbb{N}$ tal que toda c-coloração de $[n]^2$ admite um 3-subconjunto de $[n]$ monocromático. Dada uma c-coloração $\varphi : [n] \to [c]$ definimos uma c-coloração $\varphi' : [n]^2 \to [c]$ por

$$\varphi'(\{a, b\}) = \varphi(|a - b|).$$

Logo, existe um 3-subconjunto $\{a, b, c\}$ de $[n]$ que é monocromático. Desse modo, $\varphi(|b - a|) = \varphi(|c - a|) = \varphi(|b - c|)$. Digamos que $a < b < c$. Então, fazendo $x = c - b$, $y = b - a$ e $z = c - a$ temos o desejado. □

Observação 2.4.2. Seja c e n como no Lema 2.4.1.

(a) Se $c' \leqslant c$ então para cada c'-coloração $\varphi : [n] \to [c']$ existem $x, y, z \in [n]$ com $\varphi(x) = \varphi(y) = \varphi(z)$ e $x + y = z$, i.e., o Lema 2.4.1 funciona substituindo c por qualquer $c' \leqslant c$. Para provar isso, é suficiente argumentar para $c' = c - 1$ (os demais caso seguem usando indução decrescente). Suponhamos que exista uma $(c-1)$-coloração $\varphi : [n] \to [c-1]$

que não satisfaz as condições desejadas. Note que deve haver pelo menos dois elementos $1 \leqslant i, j \leqslant c-1$, com $i \neq j$, tais que $\varphi(i) = \varphi(j)$. Definimos agora uma c-coloração $\widetilde{\varphi} : [n] \to [c]$ da seguinte maneira:

$$\widetilde{\varphi}(a) = \begin{cases} \varphi(a) & \text{se } a \neq j \\ c & \text{se } a = j. \end{cases}$$

Desse modo, $\widetilde{\varphi}$ é uma c-coloração que não satisfaz a conlusão do Lema 2.4.1. Mas isso é um absurdo de acordo com a escolha feita para c e n.

(b) Se $n' \geqslant n$ então para cada c-coloração $\varphi : [n'] \to [c]$ existem $x, y, z \in [n]$ com $\varphi(x) = \varphi(y) = \varphi(z)$ e $x + y = z$, i.e., o Lema 2.4.1 funciona substituindo n por qualquer $n' \geqslant n$. Com efeito, considere $\varphi : [n'] \to [c]$ uma c-coloração. Então $\varphi|_{[n]} : [n] \to \varphi([n])$ é uma c'-coloração, com $c' = |\varphi([n])| \leqslant c$. Logo, pelo item (a) desta observação segue que existem $x, y, z \in [n] \subset [n']$ tais que $x + y = z$ e $\varphi(x) = \varphi(y) = \varphi(z)$.

Finalmente, chegamos ao célebre resultado de Schur.

Teorema 2.4.3 (Schur, 1916)**.** *Para todo $m \in \mathbb{N}$ a equação*

$$x^m + y^m = z^m$$

tem solução não trivial em $\mathbb{Z}_p$ para todo primo p suficientemente grande.

Prova. Considere $H := \{x^m \mid x \in \mathbb{Z}_p^*\}$. Obviamente, H é um subgrupo de $\mathbb{Z}_p^*$. Seja c a quantidade de elementos de $\mathbb{Z}_p^*/H$. Segue do Teorema de Lagrange (ver Teorema 1.1.17) a seguinte igualdade:

$$\mathcal{O}(\mathbb{Z}_p^*) = \mathcal{O}(H) \cdot c \tag{2.2}$$

Agora consideremos o seguinte homomorfismo de grupos

$$\psi : \mathbb{Z}_p^* \to H, \quad x \mapsto x^m.$$

Por construção, ψ é um homomorfismo sobrejetor. Assim, pelo Primeiro Teorema dos Isomorfismos 1.2.9,

$$\mathbb{Z}_p^*/\ker\psi \simeq H.$$

Em particular,

$$\mathcal{O}(H) = |\mathbb{Z}_p^*/\ker\psi|. \tag{2.3}$$

Mais uma vez usando o teorema de Lagrange segue que

$$|\mathbb{Z}_p^*/\ker\psi| = \frac{\mathcal{O}(\mathbb{Z}_p^*)}{\mathcal{O}(\ker\psi)},$$

ou seja,

$$\mathcal{O}(H) = \frac{\mathcal{O}(\mathbb{Z}_p^*)}{\mathcal{O}(\ker\psi)}. \tag{2.4}$$

Desse modo, substituindo (2.4) em (2.2) e efetuando cancelamentos obtemos que $c = \mathcal{O}(\ker\psi)$. Mas, $\ker\psi = \{x \in \mathbb{Z}_p^* \,|\, x^m = 1\}$, ou seja, $\ker\psi$ pode ser visto como o conjunto solução, em $\mathbb{Z}_p^*$, da equação polinomial $x^m - 1 = 0$. Em particular, $\ker\psi$ tem no máximo m elementos. Logo, $c \leqslant m$.

Consideremos n tal que qualquer m-coloração $\varphi : [n] \to [m]$ existam x, y, z com $\varphi(x) = \varphi(y) = \varphi(z)$ e $x + y = z$. Utilizando a Observação 2.4.2, segue que para cada primo $p \geqslant n + 1$ tem-se que para qualquer c-coloração $\varphi : [p-1] \to [c]$ existem $x, y, z \in [p-1]$ tais que $\varphi(x) = \varphi(y) = \varphi(z)$. Observemos que a aplicação

$$\pi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*/H, \quad a \mapsto aH$$

pode ser pensada como uma c-coloração. Assim, existem $x_0, y_0, z_0 \in \mathbb{Z}_p^*$ tais que $x_0 + y_0 = z_0$ e $x_0H = y_0H = z_0H$. Em particular, $z_0^{-1}x_0 = x^m$ e $z_0^{-1}y_0 = y^m$ para certos $x, y \in \mathbb{Z}_p^*$. Dessa forma,

$$x^m + y^m = z_0^{-1}(x_0 + y_0) = z_0^{-1}z_0 = 1,$$

e com isso concluímos o desejado. □

Bibliografia

[1] DIESTEL, Reinhard; Graph theory, Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.

[2] GARCIA, A.; LEQUAIN, Y.; Elementos de Álgebra. Rio de Janeiro: Associação IMPA, 2003. 326 p.

[3] LEMOS, Manoel, Interação entre grafos e matróides, Pernambuco, 2009. PP 1-14.

[4] MOREIRA, Carlos Gustavo T. de A.; KAHAYAKAWA, Yoshiharu, Tópicos em combinatória contemporânea, PP 03–34. Notas de aulas, Rio de Janeiro, 2001.

[5] SANTOS, José Plínio O.; MELLO, Margarida P.; MURARI, Idani T. C; Introdução à análise combinatória, PP 297–329. Ciência Moderna, Rio de Janeiro, 2007.