O Teorema de Ramsey e o Último Teorema de Fermat em Corpos Finitos.

Leandro Cioletti *　　Eduardo A. Silva †

12 de setembro de 2011

Resumo

O objetivo deste texto é apresentar a prova do Último Teorema de Fermat em corpos finitos. Este resultado é obtido a partir de um dos teoremas fundamentais da teoria de Ramsey, que é exposto em todos os detalhes. Salientamos que este trabalho introdutório é baseado em resultados clássicos da Teoria de Ramsey e não possui nenhum conteúdo inovador.

AMS 2000 subject classification: 05DXX, 05D10, 05C15.

Palavras-chaves: Teoria de Ramsey, Coloração, O Último Teorema de Fermat em $\mathbb{Z}_p$.

1 Introdução

O objetivo destas notas é apresentar com todos os detalhes e de forma auto-contida a prova de um dos teoremas fundamentais da teoria de Ramsey e em seguida, como aplicação apresentar o argumento de Issai Schur usado para provar a existência de soluções não-triviais para a equação $x^n + y^n \equiv z^n$ em $\mathbb{Z}_p$, para p suficientemente grande.

De maneira simplificada podemos dizer que a teoria de Ramsey lida com o problema de encontrar ordem no caos. A motivação escolhida neste texto para apresentar a teoria de Ramsey vem de problemas antigos em teoria dos números.

O problema de resolver equações em $\mathbb{Z}$ é um dos problemas mais antigos em matemática. Por exemplo, a equação de Pell

$$x^2 - ny^2 = \pm 1$$

foi estudada por Brahmagupta no Século VII. Um outro exemplo mais famoso é Último Teorema de Fermat. Este problema ficou em aberto por mais de 300 anos e finalmente em 1995, Andrew Wiles provou que a equação

$$x^n + y^n = z^n$$

*Departamento de Matemática, UnB, 70910-900 Brasília, Brasil.
leandro.mat@gmail.com

†Departamento de Matemática, UnB, 70910-900 Brasília, Brasil.
eduardo23maf@gmail.com

não possui solução (não-trivial) se $n \geq 3$, solucionando assim o problema em questão.

Alguns dos resultados apresentados aqui estão relacionados a resolução de equações em subconjuntos dos inteiros, por isto começamos introduzindo as seguintes notações: $\mathbb{N} = \{1, 2, \ldots\}$ e $[n] = \{1, \ldots, n\}$, onde $n \in \mathbb{N}$. A cardinalidade de um conjunto X qualquer será denotada por $|X|$ e a densidade de um subconjunto $X \subset \mathbb{N}$ será definida por

$$d(X) = \liminf_{n\to\infty} \frac{|X \cap [n]|}{n}.$$

Com a notação introduzida acima, podemos colocar de maneira precisa a questão que será nosso ponto de partida.

Questão 1. *Qual é a densidade máxima de um conjunto $A \subset \mathbb{N}$ que não possui solução para a equação $x + y = z$?*

A primeira observação que podemos fazer a cerca da resposta da pergunta acima é que a densidade de A deve ser no mínimo $1/2$, já que o conjunto dos números ímpares não é fechado com relação a operação de soma. Por outro lado, a cota superior para densidade de A pode ser obtida pelo seguinte argumento. Para cada $n \in \mathbb{N}$ considere os seguintes conjuntos $A_n = A \cap [n]$ e $n - A_n = \{n - a : a \in A_n\}$. Afirmamos que se $n \in A$ então $A_n \cap (n - A_n) = \emptyset$. De fato, se existe algum elemento $a \in A_n \cap (n - A_n)$ então existe $\tilde{a} \in A$ tal que $a = n - \tilde{a}$, mas isto contradiz o fato de A ser livre de somas. Já que $d(A) \geq 1/2$ temos que $|A| = \infty$. Portanto A contém uma sequência crescente $(n_k)_{k\in\mathbb{N}}$. Como A_{n_k} e $n_k - A_{n_k}$ são subconjuntos disjuntos de $\{0, 1, \ldots, n_k\}$ com mesma cardinalidade segue que $|A_{n_k}| \leq (n_k + 1)/2$, logo

$$d(A) = \liminf_{n\to\infty} \frac{|A \cap [n]|}{n} \leq \liminf_{k\to\infty} \frac{|A \cap [n_k]|}{n_k} \leq \frac{1}{2},$$

o que nos permite concluir que a densidade máxima de um subconjunto de $\mathbb{N}$ livre de somas é exatamente $1/2$.

Nem todas perguntas semelhantes a esta são tão simples de serem respondidas, entretanto é possível também determinar

$$\kappa_3 = \sup_{A\subset\mathbb{N}} d(A)$$

onde A é um conjunto livre de soluções não triviais($x = y = z$) da equação $x+z = 2y$. Isto significa que se $A \subset \mathbb{N}$ é tal que $d(A) > \kappa_3$ então A necessariamente possui uma progressão aritmética de comprimento três. De fato, como $d(A) > \kappa_3$, existe em A uma tripla $\{x, y, z\}$ tal que $x + z = 2y$. Desta equação decorre que $x - y = y - z$. Observe que $z < y$ ou $x < y$. Sem perda de generalidade, podemos supor que $x < y$ e assim a progressão aritmética de comprimento três dada por $\{x, x + (y - x), x + 2(y - x)\}$ é exatamente a tripla $\{x, y, z\}$.

2 O Teorema de Ramsey

Uma coloração de um conjunto S não-vazio com $r \in \mathbb{N}$ cores será apenas uma maneira de nos referir a uma função $c : S \to [r]$. Neste contexto os números $\{1, \ldots, r\}$ serão chamados de cores e diremos que $s \in S$ está pintado com a cor $i \in [r]$ se $c(s) = i$. Um conjunto monocromático é um subconjunto $X \subset S$ cujo os elementos são todos pintados com a mesma cor.

Dado um conjunto X arbitrário denotaremos a coleção de todos os subconjuntos de X de cardinalidade k por $\binom{X}{k}$. Para tornar mais simples a compreensão do enunciado do Teorema de Ramsey vamos pensar em $\mathbb{N}$ e $\binom{\mathbb{N}}{2}$ como um grafo $G = (V, E)$, onde o conjunto de vértices $V = \mathbb{N}$ e o conjunto de aresta $E = \binom{\mathbb{N}}{2}$.

Teorema 1 (Ramsey)**.** *Seja $r \geq 1$. Para qualquer coloração $c : \binom{\mathbb{N}}{2} \to [r]$ das arestas do grafo $G = \left(\mathbb{N}, \binom{\mathbb{N}}{2}\right)$, existe pelo menos uma cor $i \in [r]$ e um subconjunto $A \subset \mathbb{N}$ tal que $|A| = \infty$ e para todo par $\{a_1, a_2\} \subset A$, temos que $c(\{a_1, a_2\}) = i$.*

Prova. Se $c : \binom{\mathbb{N}}{2} \to [r]$ uma coloração, $i \in [r]$ uma cor e $v \in \mathbb{N}$ um vértice, denotaremos por $N_i(v) = \{w \in \mathbb{N} : c(\{v, w\}) = i\}$. Mostraremos agora como construir o conjunto A mencionado no enunciado indutivamente.

Sejam $x_1 = 1$ e $X_1 = \mathbb{N}$. Pelo princípio de Dirichlet existe $c_1 \in [r]$ tal que $|N_{c_1}(x_1)| = \infty$. Tome $X_2 = N_{c_1}(x_1)$

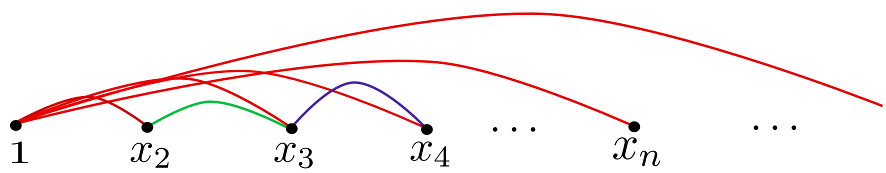

Figura 1: $N_{c_1}(x_1)$ com arestas representadas em vermelho.

Dado o conjunto infinito X_2, escolhemos $x_2 \in X_2$ arbitrariamente satisfazendo $x_2 > x_1$. Novamente pelo princípio de Dirichlet temos que existe $c_2 \in [r]$ tal que $|N_{c_2}(x_2) \cap X_1| = \infty$. Tomamos $X_3 = N_{c_2}(x_2) \cap X_2$.

De um modo geral para $n \geq 2$, escolhidos $(x_1, \ldots, x_{n-1})$ e um conjunto infinito X_n, escolhemos em seguida $x_n \in X_n$ arbitrariamente satisfazendo $x_n > x_{n-1}$. Pelo princípio de Dirichlet sabemos que existe $c_n \in [r]$ tal que $|N_{c_n}(x_n) \cap X_n| = \infty$ e assim definimos $X_{n+1} = N_{c_n}(x_n) \cap X_n$.

Claramente para todo $n \in \mathbb{N}$ temos que $X_{n+1} \subset X_n$ e desta continência segue que $c(\{x_i, x_j\}) = c_i$ para todo $j > i$. Como r é finito a sequência de cores $\{c_1, c_2, \ldots\}$ possui um subsequência monocromática infinita que será denotada por $\{c_{n_1}, c_{n_2}, \ldots, c_{n_k}, \ldots\}$.

A construção acima nos fornece um subconjunto infinito $A = \{x_{n_1}, x_{n_2}, \ldots\} \subset \mathbb{N}$ com $\binom{A}{2} \subset \binom{\mathbb{N}}{2}$ infinito monocromático.

$\square$

Observação 1. *O Teorema acima é de fato um caso particular do teorema obtido por Ramsey. O resultado realmente provado por Frank Ramsey é enunciado abaixo.*

Teorema 2 (Ramsey para hipergrafos)**.** *Sejam $r, k \geq 1$. Para qualquer coloração $c : \binom{\mathbb{N}}{k} \to [r]$ das arestas do hipergrafo $G = \left(\mathbb{N}, \binom{\mathbb{N}}{k}\right)$, existe pelo menos uma cor $i \in [r]$ e um subconjunto $A \subset \mathbb{N}$ tal que $|A| = \infty$ e para todo $\{a_1, \ldots, a_k\} \subset A$ de cardinalidade k temos $c(\{a_1, \ldots, a_k\}) = i$.*

Prova. Indução em k.

3 Teorema de Schur

Em 1916 em seus trabalhos relacionados ao Último Teorema de Fermat em $\mathbb{Z}_p$, Issai Schur se deparou (e resolveu!) com a seguinte questão.

Questão 2. *Suponha que os inteiros positivos sejam coloridos arbitrariamente com r cores. Podemos afirmar que sempre existe uma solução monocromática da equação $x + y = z$?*

Veremos nesta seção como resolver esta questão proposta por Schur, usando o Teorema de Ramsey.

Diremos que uma tripla ordenada de números inteiros positivos (x, y, z), é uma tripla de Schur se estes três números formam uma solução da equação $x + y = z$.

Teorema 3 (Schur-1916)**.** *Toda coloração $c : \mathbb{N} \to [r]$ contém uma tripla de Schur monocromática.*

Prova. Dada a coloração $c : \mathbb{N} \to [r]$ definimos uma coloração $c' : \binom{\mathbb{N}}{2} \to [r]$ por

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

Pelo Teorema de Ramsey (Teorema 1) existe um triângulo c' monocromático, isto é, existe $\{x, y, z\} \subset \mathbb{N}$ tal que $c'(\{x, y\}) = c'(\{x, z\}) = c'(\{y, z\})$. Sem perda de generalidade podemos supor que $x < y < z$. Pela definição da coloração c' segue que $c(y - x) = c(z - x) = c(z - y)$ e assim $(y - x, z - y, z - x)$ é a tripla de Schur desejada.

$\square$

4 O Último Teorema de Fermat em $\mathbb{Z}_p$

O principal resultado desta seção é um teorema provado por Schur em 1916. Este teorema foi a principal motivação para propor e provar o Teorema 3 da seção anterior.

Teorema 4 (Schur-1916)**.** *Para todo $n \in \mathbb{N}$ a equação*

$$x^n + y^n \equiv z^n \pmod{p}$$

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

Prova. Fixamos $n \in \mathbb{N}$ e p um primo que será escolhido em seguida. Considere o subgrupo $H_n = \{x^n : x \in \mathbb{Z}_p^*\} \leq \mathbb{Z}_p^*$ e a seguinte partição de $\mathbb{Z}_p^*$ em classes laterais:

$$\mathbb{Z}_p^* = a_1 H_n \cup \ldots \cup a_r H_n. \tag{1}$$

Afirmamos que $r \leq n$. De fato, considere o homomorfismo $\varphi : \mathbb{Z}_p^* \to H_n$ dado por $\varphi(x) = x^n$. Pelo Primeiro Teorema dos Homomorfismos temos que

$$\frac{\mathbb{Z}_p^*}{\ker(\varphi)} \cong \varphi(\mathbb{Z}_p^*) = H_n. \tag{2}$$

De (1) e (2) segue que $|\mathbb{Z}_p^*| = |H_n| \cdot r$ e $|\mathbb{Z}_p^*| = |\ker(\varphi)| \cdot |H_n|$, respectivamente. Logo $|\ker(\varphi)| = r$. Mas já que $\ker(\varphi) = \{x \in \mathbb{Z}_p^* : x^n = 1\}$ e o polinômio $x^n - 1$ tem no máximo n raízes em $\mathbb{Z}_p^*$, segue que $r = |\ker(\varphi)| \leq n$. Observe que em geral, $r = r(p)$ e $H_n = H_n(p)$ mas a cota obtida para r é uniforme em p, isto é, para qualquer primo p temos $r(p) \leq n$.

Para cada p primo fixado, defina a coloração $c_p : \{1, \ldots, p-1\} \to [n]$ por

$$c_p(k) = i,$$

onde i é o único índice satisfazendo $1 \leq i \leq r(p) \leq n$ e $\overline{k} \in a_i H_n$. Para terminar a prova apelamos agora para técnicas de compacidade. Defina $\tilde{c}_p : \mathbb{N} \to \{0, 1, \ldots, n\}$ por

$$\tilde{c}_p(k) = \begin{cases} c_p(k) & \text{, se } 1 \leq k \leq p-1; \\ 0 & \text{, caso contrário.} \end{cases}$$

Vamos olhar para $\tilde{c}_p$ como um elemento do espaço $\{0, 1, \ldots, n\}^{\mathbb{N}}$. Munindo este espaço da topologia produto segue do teorema de Tychonoff que $\{0, 1, \ldots, n\}^{\mathbb{N}}$ é compacto. Podemos mostrar que a topologia produto de $\{0, 1, \ldots, n\}^{\mathbb{N}}$ é gerada pela métrica

$$d(f, g) = \frac{1}{\min\{n : f(n) \neq g(n)\}}.$$

Portanto, usando que $\{0, 1, \ldots, n\}^{\mathbb{N}}$ é sequencialmente compacto, podemos afirmar que existe uma sequência crescente infinita de primos $(p_j)_{j \in \mathbb{N}}$ tal que

$$\tilde{c}_{p_j} \to \tilde{c} \in \{0, 1, \ldots, n\}^{\mathbb{N}}.$$

Podemos, na verdade, provar um fato um pouco mais forte, isto é, mostrar que $\tilde{c} \in [n]^{\mathbb{N}}$. Para isto basta observar que fixado $k \in \mathbb{N}$ e $\varepsilon = 1/k$, existe j_0 tal que para todo $j > j_0$ temos

$$d(\tilde{c}_{p_j}, \tilde{c}) < \frac{1}{k}.$$

Tomando $j > j_0$ com $p_j > k$ e usando a definição da distância segue que $\tilde{c}(k) = \tilde{c}_{p_j}(k) \in [n]$. Desta maneira $\tilde{c}$ é uma coloração de $\mathbb{N}$ em n cores. Pelo Teorema de Schur (Teorema 3) existe uma tripla de Schur $(\tilde{x}, \tilde{y}, \tilde{z})$ para a coloração $\tilde{c}$. Tome p_j tal que $p_j > \tilde{z}$ e $d(\tilde{c}_{p_j}, \tilde{c}) < 1/\tilde{z}$. Desta forma temos que $\tilde{c}_{p_j}(\tilde{x}) = \tilde{c}_{p_j}(\tilde{y}) = \tilde{c}_{p_j}(\tilde{z}) = i \in [r(p_j)]$. Mas como $\tilde{x}, \tilde{y}, \tilde{z} < p_j$, temos que nestes três pontos $\tilde{c}_{p_j}$ coincide com

c_{p_j}. Portanto $(\tilde{x}, \tilde{y}, \tilde{z})$ é uma tripla de Schur para a coloração c_{p_j}. Pela definição de c_{p_j} segue finalmente que existem $x, y, z \in \{1, \ldots, p_j - 1\}$ tal que

$$a_i x^n + a_i y^n = a_i z^n$$

Mas a_i é invertível, logo $x^n + y^n = z^n \pmod{p}$

$\square$

5 Apendice 1 - Teorema de Tychonoff

Topologia

Definição 1. *Uma topologia num conjunto X é uma coleção $\mathcal{T}$ de subconjuntos de X cujos elementos são chamados abertos e tais que*

(a) X e o $\varnothing$ são abertos;

(b) A união de quaisquer famílias de abertos ainda é aberto;

(c) A interseção de um número finito de abertos ainda é aberto;

Um par $(X, \mathcal{T})$, consistindo de um conjunto X e uma topologia $\mathcal{T}$ em X é dito um espaço topológico. Sempre que não houver confusão omitiremos a topologia e diremos simplesmente que X é um espaço topológico. Seja X um espaço topológico, $p \in X$, e S um subconjunto qualquer de X,

- Uma *vizinhaça* de p é qualquer conjunto aberto contendo p. Analogamente uma vizinhaça de S é qualquer conjunto aberto contendo S;
- S é dito *fechado* se $X \setminus S$ for um conjunto aberto;
- O *interior* de S, denotado por $\mathrm{Int}S$, é a união de todos os abertos contidos em S;
- O *fecho* de S denotado por $\overline{S}$ é definido como a interseção de todos os subconjuntos fechados de X contendo S.

Definição 2. *Seja X um conjunto. Uma base para uma topologia em X é uma coleção $\mathcal{B}$ de subconjuntos de X tais que*

(a) $X = \bigcup_{B \in \mathcal{B}} B$

(b) Se B_1, e B_2 estão em $\mathcal{B}$ e $x \in B_1 \cap B_2$, então existe B_3 em $\mathcal{B}$ tal que $x \in B_3 \subset B_1 \cap B_2$.

É um exercício para o leitor notar que a coleção $\mathcal{T}$ de todas as uniões de elementos de $\mathcal{B}$ é uma topologia para X.

Agora vamos definir um conceito extremamente importante, a saber, o conceito de funções contínuas entre espaços topológicos.

Definição 3. *Sejam X e Y espaços topológicos. Uma aplicação $f : X \to Y$ é dita contínua quando para todo aberto U de Y a imagem inversa $f^{-1}(U)$ é aberta em X.*

Com essa definição os seguintes fatos são praticamente observações

- a composição de duas funções contínuas é contínua
- a restrição de uma função contínua ainda é contínua se considerarmos a topologia induzida

Com efeito, seja $A \subset X$ e considere em A a topologia induzida por X. Então se U é um aberto em Y temos

$$(f|A)^{-1}(U) = A \cap f^{-1}(U)$$

que é aberto em A, portanto $f|A$ é contínua. Reciprocamente se para todo $A \subset X$ a restrição $f|A$ é contínua então f é contínua em X.

Teorema 5. *Sejam X e Y espaços topológicos e $f : X \to Y$ uma aplicação. As seguintes afirmações são equivalentes:*

(a) A aplicação f é contínua.

(b) A imagem inversa de fechado é fechado.

(c) A imagem inversa de cada elemento de uma base para a topologia de Y é aberto.

(d) Para cada $x \in X$ a imagem inversa de toda vizinhança de $f(x)$ é uma vizinhança de x.

5.1 A topologia induzida por uma família de funções

Seja X um conjunto arbitrário, Y um espaço topológico e $\mathcal{F}$ uma família de aplicações $f_\lambda : X \to Y$ com índices em um certo conjunto $\mathcal{I}$. Considere a família $\mathcal{B}$ de todos os subconjuntos de X obtidos através das interseções finitas:

$$f_{\lambda_1}^{-1}(U) \cap \ldots \cap f_{\lambda_k}^{-1}(U)$$

onde U é aberto em Y.

Proposição 6. *São verdadeiras as seguintes afirmações:*

a) $\mathcal{B}$ é a base para uma topologia em X;

b) Esta topologia é a menor topologia que torna cada aplicação $f_\lambda : X \to Y$ de $\mathcal{F}$ contínua. Esta topologia é chamada de topologia fraca em X determinada por $\mathcal{F}$.

Agora vamos tentar generalizar esta noção, ao invés de considerar apenas um espaço topológico Y, nós vamos considerar uma família arbitraria $(Y_\lambda)_{\lambda \in \mathcal{I}}$ de espaços topológicos. Se $\mathcal{F} = \{f : X \to Y_\lambda \,; \lambda \in \mathcal{I}\}$ é uma família de aplicações então a família $\mathcal{B}$ de todos os subconjuntos de X obtidos através das interseções finitas

$$f_{\lambda_1}^{-1}(U_{\lambda_1}) \cap \ldots \cap f_{\lambda_k}^{-1}(U_{\lambda_i}),$$

onde os U_{λ_i} são abertos em Y_{λ_i}, é uma base de uma topologia em X.

Proposição 7. *São verdadeiras as seguintes afirmações:*

a) $\mathcal{B}$ é uma base para uma topologia em X;

b) Esta topologia é a menor topologia que torna cada aplicação $f_\lambda : X \to Y_\lambda$ de $\mathcal{F}$ contínua. Esta topologia é chamada de topologia fraca em X determinada por $\mathcal{F}$;

c) Se as f_λ separam pontos e cada Y_λ é Hausdorff então a topologia induzida em X pelas f_λ é Hausdorff;

d) Uma aplicação $g : Z \to X$ é continua se, e somente se, cada uma das aplicações $f_\lambda \circ g : X \to Y_\lambda$ é continua.

5.2 Espaços Produto

Nesta seção vamos mostrar como munir o produto cartesiano de espaços topológicos com uma topologia adequada para nossas finalidades. Vamos iniciar esta construção, por questão de simplicidade, considerando o produto cartesiano de apenas dois espaços topológicos.

Sejam X e Y espaços topológicos, seja $\mathcal{B}$ a coleção de todos os produtos cartesianos $U \times V$, onde U é aberto em X e V é aberto em Y. Vamos mostrar que $\mathcal{B}$ é uma base para uma topologia em $X \times Y$. Primeiro note que

$$(U \times V) \cap (U_1 \times V_1) = (U \cap U_1) \times (V \cap V_1)$$

(terminar depois)

5.3 Produtos com infinitos fatores

Seja $\mathcal{I}$ um conjunto de índices e $(X_\lambda)_{\lambda\in\mathcal{I}}$ uma família de espaços topológicos. Vamos tentar introduzir uma topologia no produto cartesiano

$$X = \prod_{\lambda\in\mathcal{I}} X_\lambda.$$

- Um elemento $x \in X$ é uma função $x : \mathcal{I} \to \bigcup X_\lambda$, onde para cada $\lambda \in \mathcal{I}$ temos $x(\lambda) \in X_\lambda$.

- Para cada X_λ podemos considerar uma projeção natural de X sobre X_λ

  $$\pi_\lambda : X \to X_\lambda$$

  dada por $\pi_\lambda(x) = x(\lambda)$ que pode ser compreendida como a λ-ésima coordenada de x.

- Uma observação muito útil e que se para todo $\lambda \in \mathcal{I}$ tivermos $X_\lambda = X$ então $X = \prod_{\lambda\in\mathcal{I}} X_\lambda$ coincide com o o conjunto $\mathcal{F}(\mathcal{I}; X)$ de todas as funções de $\mathcal{I}$ em X. Por exemplo, se considerarmos o conjunto de índices $\mathcal{I} = [0, 1]$ e a família $(\mathbb{R}_t)_{t\in\mathcal{I}}$ com $\mathbb{R}_t = \mathbb{R}$ para todo $t \in [0, 1]$, então

  $$\mathcal{F}([0, 1]; X) = \prod_{\lambda\in[0,1]} \mathbb{R}_t$$

Certamente esta topologia torna contínua cada uma das projeções $\pi_\lambda : X \to X_\lambda$ mas por motivos óbvios não estaremos muito interessados quando ela for a topologia discreta.

Vamos agora considerar em em X a topologia induzida pelas projeções $\{\pi_\lambda : X \to X_\lambda,\ \lambda \in \mathcal{I}\}$, isto é, a topologia que tem como base os abertos:

$$\pi_{\lambda_1}^{-1}(U_{\lambda_1}) \cap \ldots \cap \pi_{\lambda_k}^{-1}(U_{\lambda_k}) = U_{\lambda_1} \times \ldots \times U_{\lambda_k} \times \prod_{\lambda \neq \lambda_i} X_\lambda$$

Onde $U_{\lambda_1} \subset X_{\lambda_1}, \ldots, U_{\lambda_k} \subset X_{\lambda_k}$ são abertos. Por definição esta é a menor topologia em X que torna todas as projeções $\pi_\lambda : X \to X_\lambda$ contínuas. Os abertos da forma

$$U_{\lambda_1} \times \ldots \times U_{\lambda_k} \times \prod_{\lambda \neq \lambda_i} X_\lambda$$

são chamados os abertos elementares. Esta topologia será chamada a topologia produto em X.

Proposição 8. *A topologia produto em $X = \prod_{\lambda \in \mathcal{I}} X_\lambda$ tem as seguintes propriedades:*

a) As projeções $\pi_\lambda : X \to X_\lambda$ são continuas e abertas;

b) Dado um espaço topologico Z, para que uma aplicação $f : Z \to X$ seja contínua num ponto $a \in Z$ é necessário e suficiente que, para todo índice λ, a aplicação $f_\lambda = \pi_\lambda \circ f : Z \to X_\lambda$ seja contínua no ponto a;

c) Se para cada λ, F_λ é um subconjunto fechado de X_λ, então $F = \prod F_\lambda$ é fechado em $X = \prod_{\lambda \in \mathcal{I}} X_\lambda$.

Prova. A prova do item a) decorre diretamente das definições. Para provar b), vamos considerar um conjunto V aberto contendo $f(a)$. Como V é a união de abertos elementares podemos supor que $V = U_{\lambda_1} \times \ldots \times U_{\lambda_k} \times \prod_{\lambda \neq \lambda_i} X_\lambda$.

Como cada f_λ é contínua e temos que para cada λ_i existe um aberto $B_{\lambda_i} \ni a$ em Z tal que $f_{\lambda_i}(B_{\lambda_i}) \subset U_{\lambda_i}, \quad i = 1, \ldots, k$. Agora considere o aberto $B = \cap_{i=1}^{k} B_{\lambda_i}$. Já que $f_{\lambda_i}(B) \subset U_{\lambda_i}$, segue que

$$f(B) \subset f_{\lambda_1}(B) \times \ldots \times f_{\lambda_k}(B) \times \prod_{\lambda \neq \lambda_i} X_\lambda \subset U_{\lambda_1} \times \ldots \times U_{\lambda_k} \times \prod_{\lambda \neq \lambda_i} X_\lambda$$

fato que finaliza a demonstração.

1- Revisar este argumento;

2- Incluir a prova do ítem c).

Proposição 9. *As seguintes afirmações são equivalentes a respeito da topologia produto em $X = \prod_{\lambda \in \mathcal{I}} X_\lambda$*

a) é a menor topologia que torna todas as projeções $\pi_\lambda : X \to X_\lambda$ contínuas.

b) Uma aplicação $f : Z \to X$ é contínua se, e somente se, cada uma das funções $f_\lambda = \pi_\lambda \circ f : Z \to X_\lambda$ é contínua.

6 Conjuntos compactos

Nesta seção vamos definir a noção de espaço topológico compacto e provar o teorema de Tychonoff que diz que o produto arbitrário de uma família de espaços topológicos compactos ainda é um espaço topológico compacto quando equipado com a topologia produto.

Definição 4. *Um espaço topológico X é compacto se toda cobertura por abertos de X possui uma subcobertura finita.*

Seja X um espaço topológico e $\{F_\alpha\}_{\alpha\in A}$ uma família de subconjuntos de X. Diremos que esta família tem a propriedade da interseção finita se para quaisquer número finito de índices $\alpha_1, \alpha_2, \ldots, \alpha_n$ a interseção

$$F_{\alpha_1} \cap F_{\alpha_2} \cap \ldots \cap F_{\alpha_n}$$

é não vazia. A próxima proposição caracteriza compacidade usando conjuntos fechados.

Proposição 10. *Um espaço topológico X é compacto se e somente se para toda família $\{F_\alpha\}_{\alpha\in A}$ de fechados com a propriedade da interseção finita a interseção*

$$\bigcap_{\alpha\in A} F_\alpha$$

é não vazia.

Prova. Seja X compacto e $\{F_\alpha\}_{\alpha\in A}$ uma família de fechados com a propriedade da interseção finita. Suponha que a interseção

$$\bigcap_{\alpha\in A} F_\alpha$$

seja vazia. Isto significa que a família dos complementos $\{F_\alpha^c\}_{\alpha\in A}$ forma uma cobertura aberta de X, usando a compacidade de X podemos extrair uma subcobertura aberta finita

$$X = F_{\alpha_1}^c \cup F_{\alpha_2}^c \cup \ldots \cup F_{\alpha_n}^c$$

o que é um absurdo pois isto implica

$$F_{\alpha_1} \cap F_{\alpha_2} \cap \ldots \cap F_{\alpha_n} = \emptyset$$

o que contradiz a hipótese de $\{F_\alpha\}_{\alpha\in A}$ ter a propriedade da interseçao finita. Reciprocamente seja $\{F_\alpha\}$ uma cobertura aberta de X, isto significa que

$$\bigcap_{\alpha\in A} F_\alpha^c = \emptyset$$

portanto a família $\{F_\alpha^c\}_{\alpha\in A}$ não tem a propriedade da interseção finita, donde existem índices $\alpha_1, \alpha_2, \ldots, \alpha_n$ tais que a interseção

$$F_{\alpha_1}^c \cap F_{\alpha_2}^c \cap \ldots \cap F_{\alpha_n}^c = \emptyset$$

tomando o complementar na interseção acima obtemos uma subcobertura aberta finita de X, sendo assim X é compacto.

$\square$

Proposição 11. *A imagem de um conjunto compacto por uma função contínua ainda é um conjunto compacto.*

O próximo teorema é altamente não-trivial, diz que o produto de espaços topológicos compactos ainda é compacto na topologia produto.

Teorema 12 (Tychonoff)**.** *Se é $\{X_\alpha\}_{\alpha\in A}$ uma família arbitrária de espaços topológicos compactos, então o espaço produto*

$$X = \prod_{\alpha\in A} X_\alpha$$

é compacto na topologia produto.

Prova. Seja $\mathcal{F} = \{F_i\}_{i\in I}$ uma família se subconjuntos fechados de X tendo a propriedade da interseção finita. Agora considere a família Λ definida da seguinte maneira:

a) Os elementos de Λ são famílias cujos elementos contém $\mathcal{F} = \{F_i\}_{i\in I}$;

b) Cada elemento de Λ tem a propriedade da interseção finita.

Considere em Λ a ordem da inclusão. Usando o Lema se Zorn, podemos encontrar um elemento maximal $\mathcal{F}^*$ em Λ que possui a propriedade da interseção finita.

Seja $\pi : X \to X_\alpha$ a projeção sobre o α-ésimo fator. Para cada α fixo considere a família $\overline{\pi_\alpha(F)}$, com $F \in \mathcal{F}^*$. Observe que:

a) a família $\overline{\pi_\alpha(F)}_{F\in\mathcal{F}^*}$ herda a propriedade da interseção finita de $\mathcal{F}^*$;

b) X_α é compacto.

Assim segue da proposição anterior que a interseção

$$\bigcap_{F\in\mathcal{F}^*} \overline{\pi_\alpha(F)}$$

é não vazia. Logo para cada escolha de α temos que $x_\alpha \in \cap\overline{\pi_\alpha(F)}$. Se definimos $x = (x_\alpha)$ e mostramos que x pertence a todos os elementos F de $\mathcal{F}^*$, encerramos a demonstração.

Antes de prosseguir observamos que $\mathcal{F}^*$ é fechado para a interseção devido a sua maximalidade.

Seja U um aberto de X contendo x então U é da forma

$$U = U_{\alpha_1} \times \ldots \times U_{\alpha_n} \times \prod_{\alpha\neq\alpha_i} X_\alpha,$$

onde cada U_{α_i} é um aberto de X_{α_i}. Isto significa que U_{α_i} contém x_{α_i} para cada i. Portando fixado i, U_{α_i} contém um ponto de $\pi_{\alpha_i}(F)$ para todo $F \in \mathcal{F}^*$, então

$$\pi^{-1}(U_{\alpha_i}) = U_{\alpha_i} \times \prod_{\alpha_i\neq\alpha} X_\alpha$$

contém um ponto de F para cada $F \in \mathcal{F}^*$.

□

(terminar depois)