Aplicações do Axioma da Escolha

João Paulos

17 de Fevereiro de 2013

Resumo

São expostas algumas aplicações elementares do Axioma da Escolha, em tópicos desde a Topologia à Álgebra. Descreve-se ainda a construção dos números ordinais e cardinais, culminando num resultado sobre módulos que utiliza ferramentas elementares de aritmética de cardinais.

Conteúdo

Capítulo Zero

O principal objectivo deste projecto feito no âmbito da disciplina *Projecto em Matemática* presente no plano curricular da LMAC, é o de explorar o Axioma da Escolha e apresentar os conceitos de número ordinal e número cardinal. Serão expostas algumas aplicações importantes do Axioma da Escolha em áreas distintas da Matemática, revelando deste modo um pouco do seu poder enquanto ferramenta fundamental.

Não é exagero afirmar que em Análise Real, em Topologia, em Análise Funcional ou em Álgebra, muitos resultados fundamentais dependem do Axioma da Escolha. Dado o carácter desta disciplina, não será feita uma exposição exaustiva destas ligações surpreendentes com o Axioma da Escolha, no entanto, espera-se motivar o interesse e estimular a curiosidade de um leitor que tenha algum conhecimento elementar em Matemática.

O tema *infinito* é omnipresente neste projecto. Não só por o Axioma da Escolha ser uma asserção que extende ao infinito o bom comportamento de conjuntos finitos, mas também porque a construção dos números ordinais e dos números cardinais será abordada no projecto. Muitas vezes, a forma de pensar e a intuição que temos sobre conjuntos finitos perde-se ao tentarmos estudar conjuntos infinitos. Os objectos infinitos são por vezes exóticos e podem levar a construções aparentemente paradoxais. De facto, no quotidiano os objectos matemáticos com os quais lidamos, costumam ser finitos. Se adoptarmos a postura de que a Matemática, enquanto linguagem criada por humanos, assenta em princípios formulados apartir de uma intuição criada por via empírica, parece-nos natural que alguns *problemas* possam surgir enquanto lidamos com objectos não finitos. Um exemplo muito simples de como factos *obviamente verdadeiros* sobre conjuntos finitos não são necessariamente verdadeiros em conjuntos infinitos pode ser dado do seguinte modo : Suponha-se que temos um conjunto de rebuçados e um conjunto de crianças e que, para evitar conflitos, cada criança come e um e um só rebuçado. Se tivermos 50 rebuçados e os distribuirmos deste modo por 20 crianças, sabemos que sobram rebuçados. Se, por outro lado tivermos 50 crianças, não sobra nenhum. No entanto, imagine-se que temos um conjunto infinito de rebuçados e que, distribuindo desta forma os doces, os rebuçados se esgotam e que todas as crianças recebem um e só um doce. Seria de esperar que, se chegásse mais uma crinça a este conjunto, esta ficaria sem rebuçado. Seria ainda de esperar que, se uma criança saísse do nosso conjunto, sobraria um rebuçado. Pois bem, o que acontece é que,

qualquer um destes dois últimos casos não difere da situação em que cada criança recebeu um e só um rebuçado. Considere-se ainda outra situação. Imaginemos uma fila de espera. Se na fila estiverem 49 pessoas, quando chegar outra pessoa, existe uma mudança fundamental na fila : definiu-se uma nova posição na ordem da fila, nomeadamente a posição 50. O que é que acontece quando a fila é infinita? Suponha-se que alguém chega a uma fila de espera infinita. Será que alguma coisa muda na fila com a chegada dessa pessoa? De facto, se estivermos a falar da ordem da fila, algo muda. Aqui a nossa intuição está correcta e é extendida do caso finito. Mas então, qual é a diferença entre os dois casos mencionados ? A diferença reside no que se está a *medir* nos conjuntos. No exemplo do conjunto de rebuçados, definimos uma correspondência um-por-um para medirmos o tamanho do conjunto. No exemplo da fila de espera, o conceito que abstrai a nossa intuição sobre as filas, é o da ordem. Estas ideias podem ser materializadas nos números cardinais e nos números ordinais, que serão construídos ao longo do projecto.

Gostaria ainda de agradecer a paciência, a dedicação e a disponibilidade do Professor Gustavo Granja, que orientou este projecto.

1 Axioma da Escolha

1.1 Axiomatização da Teoria dos Conjuntos

Será que os objectos matemáticos existem num plano transcendente à Natureza que a percepção dos nossos sentidos permite alcançar? Esta é uma questão profunda que nos levaria a ponderar sobre a existência de um mundo platónico, onde a verdade absoluta poderia ser definida como uma verdade matemática. Não obstante, e sendo um pouco mais pragmático, o que define algo como verdadeiro em Matemática ? Uma asserção é válida se puder ser deduzida apartir de uma sequência finita de passos, encadeados entre si, interdependentes e sem contradições lógicas. Ao contrário da maioria das ciências que se regem por hipóteses impostas pela Natureza, em Matemática, como linguagem formal, existe uma plasticidade e liberdade únicas na escolha das hipóteses. O processo de validação de uma teoria em Matemática, é também diferente, nao se baseando em constatação empírica, mas fazendo-se intrinsecamente na própria linguagem, provando-se os factos pelas deduções mencionadas acima. Mas então, surge uma necessidade gritante de não estarmos a trabalhar no vazio, de tudo não deixar de

ser uma grande recursão sem base! Como as hipóteses não foram observadas num mundo não platónico, temos de estabelecer a priori o que entendemos como verdade inquestionável em Matemática, de modo a que qualquer sequência de passos que justifica uma prova, não esteja num vácuo misterioso e mal definido. As verdades que permitem a construção dos objectos matemáticos, designam-se por **axiomas**. Pode colocar-se agora outra questão : Como escolher os axiomas ? Isto é uma questão que diverge muito rapidamente do carácter elementar deste projecto e como tal, vamos assumir que temos a legitimidade de encarar o modelo axiomático apresentado neste texto, como uma espécie de mandamentos que regem o mundo platónico da Matemática. A abordagem, especialmente nos capítulos onde se constroem os números ordinais, usará uma formulação equivalente ao modelo axiomático mais usado na matemática usual - o modelo ZFC. À formulação que vamos adoptar, costuma dar-se o nome de axiomas Bernays-Gödel-von Neumann. Assume-se que o leitor se sinta confortável com conceitos primitivos como o da relação de pertença, contido ou de igualdade, classe, operações habituais com conjuntos (como união, interseção ou produto cartesiano), conectivos proposicionais e função.

Apresentemos então os axiomas para futura referência!

Axioma I. $x \in A \wedge x = y \Rightarrow y \in A$. Dada uma *classe* A e um elemento x que pertença a A, se $y = x$, então y também pertence a A.

Definição 1 *A classe A designa-se por* ***conjunto*** *se existe uma classe B tal que* $A \in B$.

Este axioma sugere que *existem colecções na nossa linguagem que não são conjuntos.* Dito de outro modo, nem tudo o que conceptualmente é uma colecção de objectos, pode ser tratado formalmente como um conjunto. Deste modo, o paradoxo de Russell que historicamente abalou as fundações da Matemática, motivando uma maior preocupação com a definição formal dos objectos em Matemática, é evitado : A classe de Russell não é um conjunto por esta definição e pelo próximo axioma ! Aconselha-se ao leitor interessado uma pesquisa sobre a importância do Paradoxo de Russell [JvH].

II.Axioma da Formação. Existe uma classe A cujos elementos são os conjuntos com a propriedade p, ou seja $x \in A \Leftrightarrow (x \text{ é conjunto}) \wedge p(x)$.

Os seguintes axiomas destinam-se a garantir que podem ser efectuadas algumas das construções usuais com conjuntos :

III.Axioma do Conjunto Vazio. $\emptyset$ é um conjunto.

IV. Axioma do Emparelhamento. Dados A e B conjuntos distintos , então $C = \{x : x = A \wedge x = B\}$ é um conjunto, usualmente denotados por $\{A, B\}$.

V. Axioma da União. Se $\{A_\alpha : \alpha \in J\}$ é uma família de conjuntos, então $\bigcup_{\alpha \in J} \{A_\alpha\}$ é conjunto.

Axioma VI. Se A é um conjunto e $f : A \to A$ é uma aplicação, então $f(A)$ é um conjunto.

Axioma VII. Se A é um conjunto, para qualquer classe C temos que $A \cap C$ é conjunto.

Embora não se tenha definido o que é um subconjunto, usa-se o termo com a conotação habitual. Recorde-se que dado um conjunto A, o conjunto das partes de A, denota-se por P(A). Simbolicamente, P(A) = $\{B : (B \text{ é conjunto}) \wedge B \subset A\}$.

Axioma VIII. Se A é um conjunto, então a colecção dos subconjuntos de A, $P(A)$, é ainda um conjunto.

IX.Axioma da Fundação. Se A é um conjunto não vazio, $\exists x \in A$ tal que $x \cap A = \emptyset$

Este último axioma tem duas consequências importantes : Por um lado, nenhum conjunto pertence a si próprio. Por outro lado, se A e B são conjuntos não vazios, não é possível que $A \in B$ e $B \in A$. De facto, sendo A um conjunto, pelo Axioma VIII, $\{A\}$ é ainda um conjunto. Se $A \in A$, então $A \cap \{A\} \neq \emptyset$ e violaríamos o Axioma da Fundação. Em relação à segunda asserção, procede-se de modo perfeitamente análogo, considerando o conjunto $\{A, B\}$.
O próximo axioma garante a existência de um conjunto *infinito*.

X. Axioma do Infinito. Existe um conjunto A tal que $\emptyset \in A$ e tal que se $a \in A$ então $a \cup \{a\} \in A$.

Estes axiomas capturam a intuição daquilo que deverá ser a noção de *colecção de objectos* e como é que ela se deve comportar de forma coerente, distinguindo à partida as colecções *demasiado grandes* para serem formalmente conjuntos. Por último, o Axioma da Escolha. Apesar de, à primeira vista, ser *obviamente verdadeiro* ou *inquestionavelmente evidente*, revela-se

extraordinariamente controverso, pois *alguns* resultados *impossíveis* ou extremamente contra-intuitivos são consequência deste ou até mesmo, de modo mais chocante, equivalentes. No entanto, dada a sua *omnipresença* e utilidade em várias áreas da Matemática, particularmente nas suas formas equivalentes, é aceite pela maioria dos matemáticos. Nem que seja por ser tão *óbvio* :

XI. Axioma da Escolha. Dada uma família $\{A_\alpha : \alpha \in J\}$ não vazia, de conjuntos não vazios, existe um conjunto C ao qual pertence exactamente um elemento de cada A_α. Por outras palavras, o produto cartesiano de uma família não vazia de conjuntos não vazios, é ainda não vazio.

1.2 Algumas formulações equivalentes do Axioma da Escolha

Nesta secção serão provadas algumas formas equivalentes ao Axioma da Escolha. Algumas delas são muito surpreendentes e todas elas são muito úteis em diversas instâncias da construção matemática. Na próxima secção serão expostas algumas aplicações importantes destas formas equivalentes.

Definição 2 *Uma relação binária R num conjunto A é designada por ordem parcial se é reflexiva (i.e.* $\forall a : aRa$ *), transitiva (*$aRb \wedge bRc \Rightarrow aRc$*) e ainda anti-simétrica (*$aRb \wedge bRa \Rightarrow a = b$*). Neste caso, A diz-se parcialmente ordenado por R, denotando-se por (A,R). Por fim, uma ordem parcial R numa cadeia A (i.e. um conjunto parcialmente ordenado tal que quaisquer* $a, b \in A$ *estão relacionados por R), diz-se uma ordem total.*

Definição 3 *Seja (A,*$\preccurlyeq$*) com uma ordem parcial. Se* $\forall a : m \preccurlyeq a \Rightarrow a \preccurlyeq m$*, então* $m \in A$ *diz-se maximal em A. Se* $B \subset A$ *e* $m_0 \in A$ *é tal que* $\forall b \in A$ *se tem que* $b \preccurlyeq m_0$*, diz-se que* m_0 *é um majorante de B.*

Definição 4 *Um conjunto totalmente ordenado W diz-se bem-ordenado (ou um ordinal) se para* $B \subset W$ *tal que* $B \neq \emptyset$*, existe* $b_0 \in B$ *tal que* $b_0 \preccurlyeq b$ *para todo* $b \in B$*, i.e. todo o subconjunto não vazio de W, tem um mínimo (*b_0*).*

Teorema 5 *As seguintes afirmações são equivalentes :*

1. *Axioma da Escolha.*

2. *Lema de Zorn : Seja X um conjunto parcialmente ordenado onde cada cadeia tem um majorante. Então existe elemento um maximal em X.*

3. *Teorema de Zermelo : Todo o conjunto pode ser bem-ordenado.*

4. *Teorema de Tychonoff : Seja* $\{A_\alpha\}_{\alpha\in J}$ *uma família de espaços topológicos compactos. Então,* $\Pi_{\alpha\in J}(A_\alpha)$ *com a topologia produto, é compacto.*

A seguinte citação expressa bem como o teorema anterior é surpreendente : 'The Axiom of Choice is obviously true, the Well-Ordering Principle (Zermelo's Theorem) obviously false, and who can tell about Zorn's Lemma?' - Jerry Bona [1]

Prova: (1) $\Rightarrow$ (2) : A prova é omitida, não por ser difícil, mas por ser muito extensa. Ao leitor interessado aconselham-se duas boas referências : [Du, pg.32-34] ou [Hal, pg.63-65]

(2) $\Rightarrow$ (3) : Seja X um conjunto qualquer. É claro que existem subconjuntos de X que podem ser bem-ordenados ($\emptyset$, por exemplo). Seja então, $F = \{(A, \preccurlyeq_A) : A \subset X$ e $\preccurlyeq_A$ é uma boa ordenação de A $\}$. Pela observação anterior, sabemos que $F \neq \emptyset$. Podemos ordenar F da seguinte maneira : $(A, \preccurlyeq_A) \preccurlyeq (B, \preccurlyeq_B)$ se :

(i) $A \subset B$

(ii) $\preccurlyeq_B$ induz $\preccurlyeq_A$, restringindo $\preccurlyeq_B$ a A

(iii) $(y \in B \setminus A) \wedge (x \in A) \Rightarrow x \prec_B y$

É fácil verificar que na verdade F é um conjunto parcialmente ordenado. Seja C $= \{(A_\alpha, \preccurlyeq_\alpha) : \alpha \in J\}$, uma cadeia em $(F, \preccurlyeq)$. Resta provar que C tem um majorante em F. Defina-se U $= \bigcup_{\alpha\in J}(A_\alpha)$ e considera-se a boa ordem $\preccurlyeq_U$ em U, definida da seguinte maneira : dados $a, b \in \bigcup_\alpha(A_\alpha)$, seja α tal que $a, b \in A_\alpha$ (que existe porque C é uma cadeia). Define-se então $a \preccurlyeq_U b$ se e só se $a \preccurlyeq_\alpha b$. Note-se que $\preccurlyeq_U$ está bem definida (ou seja, é independente da escolha de α, por (ii)) e é imediato que $\preccurlyeq_U$ é uma ordem parcial, restando verificar que é uma boa ordem. Ora, por (i) e por (iii), $\preccurlyeq_U$ tem a seguinte propriedade : $(y \in A_\alpha) \wedge (x \preccurlyeq_U y) \Rightarrow (x \in A_\alpha)$. Então, se $Q \subset \bigcup_\alpha(A_\alpha)$ é não vazio, existe α tal que $Q \cap A_a \neq \emptyset$ e o elemento mínimo dessa intersecção é mínimo em Q. Claramente para todo $\alpha \in A$ se tem que $(A_\alpha, \preccurlyeq_\alpha) \preccurlyeq (\bigcup_\alpha(A_\alpha), \preccurlyeq_U)$ e como tal, concluimos que U é um majorante da cadeia C, em (F,$\preccurlyeq$). Portanto, pelo Lema de Zorn, *existe* $(M, \preccurlyeq_M)$ **maximal** em $(F, \preccurlyeq)$. Se $M \neq X$, existiria $a_0 \in X \setminus M$. Neste caso, considerando $M' = M \cup \{a_0\}$, com $\preccurlyeq_{M'}$ definida por restrição em M e por $m \preccurlyeq'_M a_0$ para

todo $m \in M$, temos que $M \cup \{a_0\}$ é bem ordenado e que $(M, \preccurlyeq_M) \preccurlyeq (M', \preccurlyeq_{M'})$, o que é uma contradição. Logo, M = X e $\preccurlyeq_M$ é boa ordem em X.

(3) $\Rightarrow$ (1) Seja $\{A_\alpha : \alpha \in J\}$ família não vazia de conjuntos não vazios. Por (3) é possível impôr uma boa ordem em $\bigcup_\alpha (A_\alpha)$ e defina-se então, $c(\alpha)$ como o primeiro elemento em A_α. Desde modo, $(c(\alpha))_{\alpha \in J}$ é um elemento de $\prod_{\alpha \in J} A_\alpha$, que é portanto não vazio.

(2) $\Rightarrow$ (4) Comecemos por provar o seguinte resultado

Teorema 6 *(**Teorema da Sub-base de Alexander**) Seja (X, T) um espaço topológico e S uma sub-base para T. Se qualquer cobertura de X por elementos de S tem uma subcobertura finita, então X é compacto.*

Prova: Suponha-se, por contradição, que toda a cobertura de X por abertos em S tem uma subcobertura finita e ainda assim, X não é compacto. Então, F = {coberturas abertas de X sem subcobertura finita} $\neq \emptyset$ e é parcialmente ordenado por inclusão. Seja $\{C_\alpha\}$ uma cadeia em F e defina-se C = $\bigcup_\alpha C_\alpha$. Vamos verificar que C é um majorante de $\{C_\alpha\}$ em F, bastando provar que C não contém subcobertura finita de X. Considere-se uma subcolecção finita $U_1, \cdots, U_n$ de C. Como $\{C_\alpha\}$ é uma cadeia, existe α_0 tal que $U_j \subset C_{\alpha_0}$ para todo $j \in \{1, \cdots, n\}$. Então, como C_{α_0} não tem subcobertura finita de X, o mesmo se passa com C. Assim sendo, pelo *Lema de Zorn* existe um elemento maximal M em F.

Seja $Z = M \cap S$. Se mostrarmos que Z cobre X, chegaremos a uma contradição pois $Z \subset S$ e como tal, tem subcobertura finita, mas por outro lado $Z \subset M$, e portanto não pode ter uma subcobertura finita. Voltemos à prova que Z cobre X. Suponha-se, por contradição, que Z não cobre X e seja $x \in X$ um elemento que não pertence a nenhum elemento de Z. Como M cobre X, existe $O \in M$ tal que $x \in O$ e como S é uma sub-base, existem $V_1 \cdots V_n$ em S tal que $x \in \bigcap_{j=1}^n (V_j) \subset O$. Nenhum destes conjuntos V_j estão em M, caso contrário, x seria elemento de algum membro de Z. Pelo facto de M ser maximal, cada $M \cup \{V_j\}$ contém uma subcobertura finita de X; digamos $X = V_j \cup W_j$ com W_j uma união finita de subconjuntos de M. Então, $X \subset \bigcap_{j=1}^n (V_j \cup W_j) \subset O \bigcup (\cup_{j=1}^n W_j)$. *Mas isto é impossível* pela definição de M, que não admite subcobertura finita. Conclui-se que Z cobre X, o que implica, como notado anteriormente, que X é compacto. ■

Lema 7 *Seja $\{(X_\alpha, T_\alpha) : \alpha \in J\}$ uma família de espaços topológicos compactos. Qualquer*

cobertura aberta de $X = \prod_{\alpha \in A} X_\alpha$ *por conjuntos da forma* $\pi_\alpha^{-1}(U)$ *com* U *um aberto de* (X_α, T_α)*, contém uma subcobertura finita de* X*.*

Prova: Seja C uma cobertura por elementos da forma $\pi_\alpha^{-1}(U)$ e seja, para cada $\alpha \in C$, $C_\alpha = \{U \in T_\alpha : \pi_\alpha^{-1}(U) \in C\}$. Vamos provar que existe $\alpha \in J$ tal que C_α cobre X_α. Ora, se não fôsse esse o caso, para cada $\alpha \in J, \exists x_\alpha \in X_\alpha$ tal que x_α não pertence a nenhum dos elementos de C_α. Seja $x \in X$ tal que $\pi_\alpha(x) = x_\alpha$. Então chegamos à contradição que C não cobre X, pois tal x não pertenceria a nenhum do elementos de C. Escolha-se então α tal que C_α cobre X_α. Por compacidade de X_α, existe uma subcobertura finita $\{U_1, \cdots, U_n\} \subset C_\alpha$. Temos então que $\{\pi_\alpha^{-1}(U_1), \cdots, \pi_\alpha^{-1}(U_n)\} \subset C$ é uma subcobertura finita de X. ■

Corolário 8 ***(Teorema de Tychonoff)***

Prova: O Teorema de Tychonoff é uma consequência imediata do Teorema 6 e do Lema 7. Basta notar que os elementos da sub-base de X na topologia produto são da forma $\pi_\alpha^{-1}(U)$, com U aberto de (X_α, T_α). ■

Deste modo, acabámos de provar a implicação (2) ⇒ (4). Para acabar a prova do teorema, resta-nos a última implicação :

(4) ⇒ (1) Seja $\{A_\alpha : \alpha \in J\}$ uma família não vazia de conjuntos não vazios. O objectivo é mostrar que de facto, $\prod_{\alpha \in J} A_\alpha \neq \emptyset$. Para cada $\alpha \in J$ defina-se $X_\alpha = A_\alpha \cup \{a\}$ e seja $X = \prod_{\alpha \in J} X_\alpha$. Considere-se uma *topologia cofinita modificada* nos conjuntos X_α, cujos abertos são os subconjuntos cofinitos de X_α, o conjunto vazio e o conjunto singular $\{a\}$, em cada X_α. É imediato que X_α é compacto e portanto, pelo Teorema de Tychonoff, temos que X com a topologia produto é compacto. Como cada aplicação de projecção $\pi_\alpha : X \to X_\alpha$ é contínua e cada A_α é fechado (porque é complementar do aberto $\{a\}$ em T_α), então cada $\pi_\alpha^{-1}(A_\alpha)$ é um fechado de X. Além disso, $\bigcap_\alpha \pi_\alpha^{-1}(A_\alpha) = \prod A_\alpha$ e basta portanto provar que a família $\{\pi_\alpha^{-1}(A_\alpha)\}$ tem a propriedade da intersecção finita. Sendo X compacto, concluimos que $\prod_{\alpha \in J} A_\alpha \neq \emptyset$. Seja então $\{\alpha_1, \cdots, \alpha_N\} \subset J$. O objectivo é mostrar que $\bigcap_{k=1}^N (\pi_{\alpha_k}^{-1}(A_{\alpha_k})) \neq \emptyset$. Ora, $\prod_{k=1}^N (A_{\alpha_k}) \neq \emptyset$ (*note-se que não é necessário invocar o Axioma da Escolha, pois trata-se de um subconjunto finito de índices*). Logo podemos escolher $x' = (x_1, \cdots, x_N)$ pertencente a esse produto cartesiano. Seja $x \in \prod_{\alpha \in J} A_\alpha$ definido por : $x_\alpha = \begin{cases} x_k, \alpha = \alpha_k \\ x_\alpha = a, \text{caso contrário} \end{cases}$. Ora, por construção, esta extensão de x' pertence a $\bigcap_{k=1}^N \pi_{\alpha_k}^{-1}(A_{\alpha_k})$. ■

Note-se que a construção desta topologia cofinita modificada foi crucial para que fôsse possível prolongar x', **sem** necessidade de invocar o Axioma da Escolha.

É de salientar o quão bizarro nos parece o inocente Axioma da Escolha, na sua versão equivalente de Teorema de Zermelo. É extremamente difícil imaginar uma *boa ordenação num conjunto não contável*. No entanto, o Teorema de Zermelo não é apenas um resultado estranho e contra-intuitivo. Tem muitas aplicações importantes, como a demonstração do Teorema de Metrização de Nagata-Smirnov e a construção dos ordinais, que será abordada neste trabalho. Para um exemplo de aplicação, o leitor interessado deve consultar [Mu, pg. 244-52]. É ainda extremamente elegante a ligação tão profunda entre o Axioma da Escolha e o Teorema de Tychonoff. Esta ligação ocorre ainda como **muitas** outras ferramentas da Topologia, Análise e Álgebra. Dada a natureza deste projecto, infelizmente não iremos desenvolver muito mais o assunto. No entanto, ao leitor interessado aconselha-se [Her].

1.3 Algumas aplicações do Axioma da Escolha

Nesta secção serão expostas algumas consequências importantes do Axioma da Escolha :

Teorema 9 *Todo o espaço vectorial não nulo tem uma base.*

Prova: Seja M um espaço vectorial tal que $M \neq \{0\}$. Seja F a família dos subconjuntos linearmente independentes de M, com a ordem parcial dada pela inclusão. Note-se que $F \neq \emptyset$ (*pois* $\exists a \in M \setminus \{0\}$ *e claro que* $\{a\} \in F$ *: se* $r \neq 0$ *e* $ra = 0$*, como r é um elemento de um corpo e não é o zero, tem inversa e chegamos à contradição que* $a = 0$). Seja $C = \{C_\alpha : \alpha \in J\}$ uma cadeia em F. Vamos provar que C é majorada pela escolha natural $\bigcup_{\alpha \in J} C_\alpha$. De facto, por C ser uma cadeia, dados $\{a_1, \cdots, a_n\} \subset \bigcup_{\alpha \in J}(C_\alpha)$, $\exists \alpha : \{a_1, \cdots, a_n\} \subset C_\alpha$. Como C_α é linearmente independente, $\sum_{i=1}^{n} r_i a_i = 0 \Rightarrow r_i = 0$, para todo o i. Deste modo, concluimos que $\bigcup_{\alpha \in J} C_\alpha \in F$ e portanto, estamos nas condições de aplicar o Lema de Zorn, que nos garante a existência de um elemento maximal em F, que designaremos por B. Por um lado, B é por construção um conjunto linearmente independente. Por outro lado, B é um conjunto gerador de M : Suponhamos, por contradição, que existe $m \in M$ tal que $m \notin \langle B \rangle$. Se assim fôr, vamos provar que $r.m + r_1.b_1 + \cdots + r_n.bn = 0 \Rightarrow r = 0 \wedge r_i = 0$ e portanto, $B \cup \{m\}$ é linearmente independente, o que é impossível, pois contraria a maximalidade de B. Ora por um lado, dada uma combinação linear como acima temos necessariamente $r = 0$. Caso contrário como r é um elemento de um corpo, admite inversa e temos que $m = r^{-1}((-r_1)b_1 + \cdots + (-r_n)b_n)$, o que

é impossível pois admitimos que $m \notin \langle B \rangle$. Assim sendo, como B é linearmente independente, concluimos que $r_i = 0$ para todo o i. ■

Teorema 10 *Existência de Ideais Maximais num anel com identidade.*

Prova: Seja $R \neq \{0\}$ um anel com unidade e seja $F = \{I \subsetneq R \text{ e } I \text{ é ideal }\}$. Claro que $F \neq \emptyset$, pois $\{0\} \in F$ e note-se ainda que podemos ordenar F parcialmente por inclusão. Seja $C = \{I_\alpha : \alpha \in J\}$ uma cadeia de ideais em F. Vamos verificar que $\bigcup_{\alpha \in J} I_\alpha$ é um majorante. É claro que $C \subset \bigcup_{\alpha \in J} I_\alpha$. Embora a união de ideais não seja um ideal em geral, neste caso como C é uma cadeia, temos que o nosso candidato a majorante é de facto um ideal. Além disso, $\bigcup_{\alpha \in J} I_\alpha \neq R$, caso contrário, $1_R \in \bigcup_{\alpha \in J} I_\alpha \Rightarrow \exists \alpha \in J : 1_R \in I_\alpha \Rightarrow I_\alpha = R$, o que contradiz a definição de F. Então, o Lema de Zorn garante a existência de elemento maximal de F, digamos M. Por definição, M é um ideal maximal de R. ■

Lema 11 *Seja R um anel com identidade. Qualquer ideal $I \subsetneq R$ está contido num ideal maximal*

Prova: A prova é perfeitamente análoga à prova do teorema anterior, bastando considerar a família F de ideais $J \subsetneq R$ que contêm I. Como $I \subsetneq R$ e $I \subset I$, $F \neq \emptyset$ e a aplicação do Lema de Zorn é perfeitamente análoga. ■

Teorema 12 *Seja K um corpo. Então K admite uma extensão algebricamente fechada.*

Comecemos por provar um resultado simples :

Lema 13 *Seja K um corpo e $p(x) \in K[x]$. Então p(x) tem um zero em $K[x]/\langle p(x) \rangle$.*

Prova: Tome-se $\alpha = x + \langle p(x) \rangle \in K[x]/\langle p(x) \rangle$. Seja $p(x) = \sum_{i=0}^{n} k_i x^i \in K[x]$ e note-se que $p(\alpha) = k_0 + k_1(x + < p(x) >) + \cdots + k_n(x + < p(x) >)^n = p(\alpha) = (k_0 + k_1 x + \cdots + k_n x^n) + < p(x) >= 0 + < p(x) >$, pois $\sum_{i=0}^{n}(k_i x^i) = p(x) \in < p(x) >$. ■

Saliente-se que embora $K[x]/\langle p(x) \rangle$ seja uma extensão de K, é um corpo se e só se $p(x)$ fôr irredutível em $K[x]$. Provemos então a asserção do Teorema 12 :

Prova: (i) *Seja K um corpo. Então existe uma extensão L_1 na qual todo $p(x) \in K[x]$ com $deg(p(x)) > 1$ tem uma raíz* : Seja $p(x) \in K[x], deg(p(x)) > 1$ e considere-se uma variável x_p para cada polinómio $p(x)$. Seja S o conjunto das indeterminadas x_p. Considere-se $K[S] = \{$ polinómios nas indeterminadas $x_p\}$ e seja I o ideal gerado por todos os $p(x_p) \in K[S]$, i.e.

$I = \{p_1(x_{p_1}).g_1 + \cdots + p_n(x_{p_n}).g_n\}$, com $g_j \in K[S]$. Vamos usar o teorema anterior para ver que I está contido num ideal maximal M. Para tal, temos de provar que $I \subsetneq K[S]$. Suponhamos, por contradição, que $1 = g_1 p_1(x_{p_1}) + \cdots + g_m p_m(x_{p_m})$. Pelo lema anterior, aplicado iteradamente, existe uma extensão de K onde $p_i(x)$ tem uma raíz em α_i para todo i. Substituindo x_{p_i} por α_i, obtemos que $1 = 0$, o que é falso. Como I é ideal próprio de $K[S]$, está contido nalgum ideal maximal M. Considere-se então $L_1 = K[S]/M$. Como M é maximal, então L_1 é corpo. Além disso, $h : K \to K[S]/M$ definido por $k \mapsto k + M$ é um homomorfismo de corpos não nulo, logo injectivo. Pelo Teorema de Isomorfismo de Anéis, temos que $K \approx h(K) \subset L_1$ e portanto, L_1 é uma extensão de K. Além disso, $p(x) \in K[x]$ tem $r = x_p + M \in L_1$ como raíz em L_1, pois $p(r) = k_0 + k_1 r + \cdots + k_n r^n = k_0 + k_1(x_p + M) + \cdots + k_n(x_p + M)^n = [k_0 + k_1(x_p) + \cdots + k_n(x_p)^n] + M = p(x_p) + M = 0$, pois $p(x_p) \in I \subset M$.

(ii) Usando *(i)*, podemos construir indutivamente uma cadeia $L_1 \subset \cdots \subset L_n \subset \cdots$ de extensões de K, de tal forma que um polinómio de grau superior a um de $L_k[x]$ tenha sempre uma raíz em $L_{k+1}[x]$.

(iii) Tome-se $L = \bigcup_i (L_i)$. Como $\{L_i\}$ é uma cadeia podemos definir a soma e o produto em L do seguinte modo : dados $a, b \in L$, seja j o índice de um conjunto da cadeia que contém ambos os elementos. Definimos $a + b$ e $a * b$ do mesmo modo que a soma e o produto entre esses dois elementos estão definidos em L_j. Então, L é um corpo.

(iv) Conclui-se que L é uma extensão algebricamente fechada de K : seja $p(x) \in L[x]$ tal que $deg(p(x)) > 1$. Então, existe k tal que $p(x) = \sum_{i=0}^{n} \alpha_i x^i$ com $\alpha_i \in L_k$. Assim, $p(x) \in L_k[x]$ e portanto, $p(x)$ tem uma raíz em $L_{k+1} \subset L$. ■

Teorema 14 *Compacidade da Lógica Proposicional.*

Recorde-se que uma assinatura proposicional P é um conjunto não vazio de variáveis proposicionais. Apartir de P, é usual definir $\triangle$, um conjunto de fórmulas da lógica proposicional, indutivamente pela introdução da negação e das implicações. Recorde-se ainda que as interpretações proposicionais (ou valorações), que atribuem a condição de *verdade* às variáveis proposicionais, são aplicações $v : P \to \{0, 1\}$. Diz-se que $\triangle$ é *adequado* (em inglês, *sound*), se existe uma interpretação v tal que $v(\alpha) = 1, \forall \alpha \in \triangle$.

Prova: Temos a provar que, se qualquer subconjunto finito de $\triangle$ é adequado, então $\triangle$ também o é. Ora, para qualquer $\triangle$ defina-se o conjunto das valorações $S(\triangle) = \{v \in \{0, 1\}^P :$

$v(\alpha) = 1, \forall \alpha \in \triangle\}$. É imediato verificar que

$$S(\bigcup\{\triangle_i : i \in I\}) = \bigcap\{S(\triangle_i) : i \in I\} \tag{1}$$

Considere-se $B = \{0, 1\}$ com a topologia discreta e B^P com a topologia produto. Como B é compacto, pelo Teorema de Tychonoff temos que B^P é compacto. Ora, para qualquer $A \subset \triangle$ finito, temos que $S(A)$ é fechado em B^P, pois as palavras são sequências finitas e portanto só contêm um número finito de variáveis proposicionais. Suponhamos agora que qualquer subconjunto *finito* de $\triangle$ é adequado, isto é, $S(A) \neq \emptyset$, para $A \in \triangle$. Seja $C = \{S(A) : A \in \triangle\}$. Cada elemento de C é fechado e por hipótese e pela igualdade (1), qualquer intersecção finita de elementos de C é não-vazia. Como B^P é compacto, pela propriedade da intersecção finita, temos que $\bigcap C \neq \emptyset$, mas então, de novo por (1), temos que $\bigcap C = S(\triangle)$. Concluimos então que $S(\triangle) \neq \emptyset$, ou seja, $\triangle$ é adequado. ■

É importante notar que habitualmente o conjunto das variáveis proposicionais é contável. Neste caso, podemos provar a compacidade da lógica proposicional sem usar o Teorema de Tychonoff, argumentando que $\{0, 1\}^P$ é homeomorfo ao conjunto de Cantor e portanto, é compacto. No entanto, se o conjunto das variáveis proposicionais não é contável, não podemos proceder invocando tal homeomorfismo.

2 Ordinais

Neste capítulo são apresentadas algumas propriedades dos ordinais que nos permitirão definir posteriormente, com rigor, o conceito de número ordinal.

2.1 Propriedades Básicas

Definição 15 *Seja W um conjunto bem ordenado. Diz-se que $S \subset W$ é um ideal de W se $S = \emptyset$ ou se $\forall x : (x \in S) \wedge (y \preccurlyeq x) \Rightarrow (y \in S)$. Para cada $a \in W$, o conjunto $W(a) = \{x \in W : (x \prec a) \wedge (x \neq a)\}$ designa-se por intervalo inicial determinado por a.*

W e $\emptyset$ são ambos ideais de W mas apenas $\emptyset$ é um intervalo inicial. O seguinte resultado clarifica a relação entre estes dois conceitos :

Lema 16

(a) A intersecção e a união de ideais de W, é ainda um ideal de W

(b) Seja I(W) o conjunto dos ideais de W e J(W) o conjunto dos intervalos iniciais de W. Então $J(W) = I(W) \setminus \{W\}$.

Prova: A prova de *(a)* é imediata (embora se trate de uma propriedade útil dos ideias). A afirmação *(b)* diz-nos em particular que o único ideal que não é um intervalo inicial é o próprio W. Claramente $J(W) \subset I(W)$, por definição. Reciprocamente, seja $I \neq W$ um ideal. Vamos mostrar que $I = W(\alpha)$ para algum $\alpha \in W$. Ora, $W \setminus I \neq \emptyset$ e como W é um ordinal, tem um mínimo α. Por um lado, $W(\alpha) \subset I$, pois $x \in W(\alpha) \Rightarrow x \in I$, já que α é o *primeiro* elemento de W que não pertence a I. Por outro lado, $I \subset W(\alpha)$, pois se $x \notin W(\alpha)$, então $\alpha \prec x$ e como tal, $x \notin I$ (caso contrário, sendo I um ideal, temos que $\alpha \in I$). Conclui-se que $I = W(\alpha)$ ■

Numa dada categoria, os morfismos têm que preservar a estrutura dos objectos. Por exemplo, num contexto algébrico, interessa-nos estudar os homomorfismos. Em Topologia, as funções contínuas. Mas, no contexto dos ordinais, o que é que nos interessa preservar? Um ordinal é pois um conjunto totalmente ordenado, com uma propriedade adicional que o caracteriza - a existência de mínimo num qualquer seu subconjunto não vazio. Assim sendo, devemos ter isto em conta na definição dos morfismos. É apropriado definir os morfismos entre ordinais, como aplicações que preservam a ordem, i.e. $f : (X, \prec) \to (Y, \prec')$ *tal que* $(x \prec x') \Rightarrow (f(x) \prec' f(x'))$. *Deste modo, a propriedade de mínimo é preservada com esta definição de morfismo. Tais aplicações, se forem injectivas designam-se por monomorfismos e se forem sobrejectivas, por epimorfismos. Por último, neste contexto, a uma aplicação bijectiva e que preserva a ordem, damos o nome de isomorfismo.*

Lema 17 *O conjunto* $I(W)$ *de todos os ideais de um ordinal, é bem ordenado por inclusão.*

Prova: Provamos primeiro que $J(W)$ é bem ordenado : É imediato que se $a, b \in W$ e $a \preccurlyeq b$, então $W(a) \subset W(b)$ e portanto ordenando $J(W)$ por inclusão, a aplicação $a \mapsto W(a)$ preserva a ordem. É ainda claro que esta aplicação é sobrejectiva. Se $a \neq b$, então $W(a) \neq W(b)$, logo a aplicação é um isomorfismo. Como W é bem ordenado, concluimos que $J(W)$ é bem ordenado. Pelo lema anterior, $I(W) = J(W) \cup \{W\}$. Ordenando os ideais de W por inclusão do mesmo modo que o fizemos em $J(W)$ e como W é o máximo de $I(W)$ (i.e. $K \preccurlyeq W$, para todo $K \in I(W)$), concluimos que $I(W)$ é bem ordenado. ■

Definição 18 *Seja W um ordinal. Uma família* $B \subset I(W)$ *diz-se indutiva se satisfaz :*

(i) B é fechado para a união

(ii) $W(\alpha) \in B \Rightarrow (W(\alpha) \cup \{\alpha\}) \in B$

.

Teorema 19 *Seja B uma família indutiva de ideais de W. Então, B = I(W).*

Prova: Suponha-se, por contradição, que $B \neq I(W)$. Pelo Lema 17, existe o mais pequeno ideal $S \notin B$. Existem dois casos a considerar : ou S tem um último elemento, ou S não tem um último elemento. No primeiro caso, seja α o último elemento de S. Então, temos que $S = W(\alpha) \cup \{\alpha\}$ e como $W(\alpha)$ é um ideal e $W(\alpha) \prec S$, então $W(\alpha) \in B$. Assim sendo, $S = W(\alpha) \cup \{\alpha\}$ também pertence a B (*porque B é indutivo*), o que é uma contradição. No segundo caso, $S = \bigcup_\alpha \{W(\alpha) : W(\alpha) \subset S\}$ e sendo B indutivo, $S \in B$, o que é uma contradição. Concluimos então que $B = I(W)$. ■

2.2 Comparabilidade dos Ordinais

Nesta secção vamos mostrar que dois ordinais são sempre *comparáveis* no sentido em que ou são isomorfos ou um é isomorfo a um intervalo inicial do outro.

Lema 20 *Sejam W e X ordinais e* $\psi : W \to X$ *um isomorfismo tal que* $\psi(W)$ *é um ideal de X. Então, qualquer monomorfismo* $f : W \to X$*, é tal que* $\forall w : \psi(w) \preccurlyeq f(w)$.

Prova: Suponhamos que $X = \{w \in W : (f(w) \prec \psi(w))\} \neq \emptyset$. Vamos ver que neste caso, $\psi(W)$ não é um ideal de X. Como X não é vazio, tem mínimo w_0. Então, ψ não pode tomar o valor de $f(w_0)$, pois se $w \prec w_0$ temos que $\psi(w) \preccurlyeq f(w) \prec f(w_0)$ e se $w_0 \prec w$, então $f(w_0) \prec \psi(w_0) \preccurlyeq \psi(w)$. Como $f(w_0) \prec \psi(w_0)$, concluimos que $\psi(W)$ não é um ideal. ■

Observação 1 : Segue-se do Lema 20 que se existe um isomorfismo entre ideais $I_1 \subset W$ e $I_2 \subset X$ ele é sempre único : Se $\psi_1 : I_1 \to I_2$ e $\psi_2 : I_1 \to I_2$ são isomorfismos, então são também monomorfismos. Pelo Lema 20, temos $\psi_1(w) \preccurlyeq \psi_2(w)$ e $\psi_2(w) \preccurlyeq \psi_1(w)$, para todo $w \in I_1$ e portanto, $\psi_1 = \psi_2$.

Teorema 21 *Sejam W e X ordinais. Então, uma e só uma das seguintes afirmações é verdadeira :*

(i) Existe um único isomorfismo entre W e X

(ii)Existe um único isomorfismo de W sobre um intervalo inicial de X

(iii) Existe um único isomorfismo de X sobre um intervalo inicial de W

Prova: Comecemos por mostrar que as afirmações são mutuamente exclusivas. Os casos são todos semelhantes e por isso vamos mostrar apenas que (ii) e (iii) não podem ocorrer simultaneamente. Se existem isomorfismos $g : X \to W(w_0)$ e $h : W \to X(x_0)$, então temos um monomorfismo $g \circ h : W \to W(w_0)$, que satisfaz $g \circ h(w_0) \prec w_0$. Tomando $id : W \to W$, o isomorfismo dado pela identidade, obtemos uma contradição com o Lema 20. Resta então provar que uma das três coisas acontece *sempre*. Seja $B \subset I(W)$ o conjunto dos ideais de W que são isomorfos a ideais de X. Primeiro, verifica-se que B é fechado para uniões : Seja $\{S_\alpha : \alpha \in J\}$ uma família de elementos de B e sejam $\Psi_\alpha : S_\alpha \to X$ os respectivos isomorfismos para ideais de X. Pelo Lema 16, $S_\alpha \cap S_\beta$ é ainda um ideal de B e pela Observação 1, temos que $\Psi_\alpha | S_\alpha \cap S_\beta = \Psi_\beta | S_\alpha \cap S_\beta$, para todos os pares $(\alpha, \beta) \in J \times J$. Existe então uma aplicação única $\Psi : \bigcup_\alpha S_\alpha \to \bigcup_\alpha \Psi_\alpha(S_\alpha)$ [1]. É fácil de verificar que Ψ é um isomorfismo : dados $w_1 \neq w_2$ em $\bigcup_\alpha S_\alpha$, como $I(W)$ é bem ordenado por inclusão, existe $\alpha_0 \in J$ tal que $w_1, w_2 \in S_{\alpha_0}$ e como Ψ_{α_0} é um isomorfimso é imediato que $\Psi(w_1) \neq \Psi(w_2)$. De novo, pelo Lema 16, como $\bigcup_\alpha S_\alpha$ e $\bigcup_\alpha \Psi_\alpha(S_\alpha)$ são ideais, concluimos que $\bigcup_\alpha S_\alpha \in B$. Note-se que se $W \in B$, verifica-se uma das duas primeiras alíneas do teorema. Alternativamente, se $W \notin B$, então pelo Teorema 19, como B não pode ser indutivo, existe $S_\alpha = W(w_0) \in B$ com $W(w_0) \cup \{w_0\} \notin B$. Vamos ver então que $\Psi_\alpha(S_\alpha) = X$ e portanto verifica-se (iii). Suponhamos por absurdo que $\Psi_\alpha = X(x_0)$. Podemos então prolongar Ψ_α definindo $\Psi_\alpha(w_0) = x_0$ e temos então que $W(w_0) \cup \{w_0\} \in B$, o que é uma contradição. A unicidade de isomorfismos, é consequência da Observação 1. ■

Corolário 22 *Qualquer subconjunto bem-ordenado A de um ordinal W é isomorfo a W ou a intervalo inicial de W. Nenhum intervalo inicial de W é isomorfo a W*

Prova: Pelo Teorema 21 basta provar que W não pode ser isomorfo a um intervalo inicial de A. Suponha-se que existe um isomorfismo $g : W \to A(\alpha_0)$. Sendo $i : A \hookrightarrow W$ a aplicação de inclusão, temos que $g \circ i : A \to A$ satisfaz $g \circ i(\alpha_0) \prec \alpha_0$, o que contraria o Lema 20, escolhendo $\psi = id_A$. A segunda afirmação resulta directamente do Teorema 21. ■

Considere-se agora uma partição nos ordinais induzida por classes de isomorfismo.

[1] Seja $\{A_\alpha : \alpha \in J\}$ uma família de conjuntos com $\{f_\alpha : A_\alpha \to B, \alpha \in J\}$ família de funções tais que $f_\alpha | A_\alpha \cap A_\beta = f_\beta | A_\alpha \cap A_\beta$, para quaisquer $(\alpha, \beta) \in J \times J$. Então, podemos definir de forma única, uma função $f : \bigcup_{\alpha \in J} A_\alpha \to B$ que é uma extensão de cada f_α. Basta definir para cada $x \in \bigcup_{\alpha \in J} A_\alpha$, $f(x) = f_\alpha(x)$, onde α é um índice tal que $x \in A_\alpha$. É imediato que f é uma extensão de f_α e bem definida pois se $x \in A_\alpha \cap A_\beta$, então $f_\alpha(x) = f_\beta(x)$. Além disso, qualquer outra função g que seja uma extensão de f_α, terá de assumir os mesmos valores para $x \in A_\alpha$ e como tal, f é única.

Definição 23 *Sejam W e X ordinais. Diz-se que $W \preccurlyeq X$ se W fôr isomorfo a um ideal de X e escreve-se $W = X$, se W e X são isomorfos.*

Corolário 24 *A relação $\preccurlyeq$ da definição 23 é uma boa ordem na classe dos ordinais.*

Prova: Deve ser claro que $\preccurlyeq$ é uma relação reflexiva e transitiva. É ainda uma ordem parcial, pois pelo Teorema 21 , temos que $(X \preccurlyeq W) \wedge (W \preccurlyeq X) \Rightarrow W = X$. Por fim, é de facto uma boa-ordem : Seja C um conjunto não vazio de ordinais e seja $W \in C$. Como cada $X \in C$ que precede W é isomorfo a um ideal de W e porque $I(W)$ é bem-ordenado, existe um primeiro elemento em C. ■

2.3 Indução Transfinita

Teorema 25 *(Princípio da Indução Transfinita) Seja W um ordinal e seja Q um subconjunto de W. Se $W(x) \subset Q \Rightarrow x \in Q$ para todo $x \in W$, então $Q = W$*

Prova: Seja 0 o elemento mínimo de W. Note-se que, como $W(0) = \emptyset \subset Q$, então Q não é vazio. Suponhamos, por contradição, que $W \setminus Q \neq \emptyset$ e seja x_0 o primeiro elemento de $W \setminus Q$. Então, $W(x_0) \subset Q$ e logo, $x_0 \in Q$, o que é uma contradição. Conclui-se que $Q = W$. ■

O teorema anterior é uma extensão do princípio de indução finita.

Teorema 26 *Seja W um ordinal e C uma classe. Suponha-se que, para cada $x \in W$, existe uma regra R_x que associa a cada $\Psi : W(x) \to C$ um único $R_x(\Psi) \in C$. Então, existe uma e uma só função $F : W \to C$ tal que $F(x) = R_x(F|W(x))$ para cada $x \in W$.*

Prova: Primeiro prova-se que se tal F existir, tem de ser único : Suponha-se que F e G são duas funções diferentes satisfazendo a condição do enunciado. Então, existe o primeiro elemento x_0 de $\{x \in W : F(x) \neq G(x)\}$. Como $F|W(x_0) = G|W(x_0)$, temos que $F(x_0) = G(x_0)$, contrariando a escolha de x_0. Resta então provar a existência : Seja $B = \{S \subset W :$ S é um ideal de W e existe $\Psi_S : S \to C$ satisfazendo a propriedade do enunciado$\}$. A unicidade implica que $\Psi_S|(S \cap S') = \Psi_{S'}|(S \cap S')$ e daqui se conclui, como na demonstração do Teorema 21, que a união de elementos de B ainda pertence a B. Dado $S = W(x) \in B$, podemos extender Ψ_S a $W(x) \cup \{x\}$, definindo $\Psi_S(x) = R_x(\Psi_S|W(x))$. Logo $W(x) \cup \{x\} \in B$. Conclui-se que B é uma família indutiva e o Teorema 19 mostra que $W \in B$. ■

O teorema anterior, que nos permite fazer construções por recorrência transfinita, será uma ferramenta essencial nas construções dos próximos capítulos.

2.4 Números Ordinais

Estamos em condições de definir o que se entende por um número ordinal. Como vimos anteriormente, podemos identificar dois ordinais que sejam isomorfos, pois se o isomorfismo existir, é único. Considerámos ainda uma partição na classe dos ordinais induzida pela relação de equivalência de isomorfismo. A cada classe de equivalência de isomorfismo de ordinais, dá-se o nome de *número ordinal*.

Nesta secção formalizaremos a noção de número ordinal e iremos concluir que de facto, a motivação dada no capítulo zero, pode ser materializada na linguagem matemática. Será mostrado que existe uma classe bem-ordenada L, unicamente definida tal que cada ordinal é isomorfo a um seu intervalo inicial.

Definição 27 *Um número ordinal é um conjunto não vazio $\underline{\alpha}$ com as propriedades :*
(1) $(x \in \underline{\alpha}) \wedge (y \in \underline{\alpha}) \Rightarrow (x \in y) \vee (y \in x) \vee (y = x)$
(2) $(x \in y) \wedge (y \in \underline{\alpha}) \Rightarrow (x \in \underline{\alpha})$

Note-se que $\in$ induz uma relação de ordem estrita : a transitividade é garantida pelo axioma *2* e o Axioma IX garante a irreflexibilidade, uma vez $x \notin x$. Podemos explorar algumas propriedades importantes da relação $\in$ nos números ordinais :

Lema 28 *Seja $\underline{\alpha}$ um número ordinal. Então verificam-se as seguintes afirmações :*
(a) Seja $A \neq \emptyset$ tal que $A \subset \underline{\alpha}$. Então existe um único $s \in A$ tal que para qualquer $x \in A$, $(s \in x) \vee (s = x)$. Diz-se que s é o primeiro elemento de A.
(b) O primeiro elemento em $\underline{\alpha}$ é $\emptyset$
(c) Se $z \in \underline{\alpha}$, então z é um número ordinal

Prova:

(a) Pelo Axioma IX, existe $s \in A$ tal que $s \cap A = \emptyset$. Então, se $x \in A$, temos que $x \notin s$. Logo, por *1* da definição 27, ou $s \in x$ ou $s = x$. Deste modo, s é o primeiro elemento de A. Vejamos que é único : caso existisse outro $t \in A$ com a mesma propriedade de s, teriamos que $s \in t$ e $t \in s$ eram verificados, o que contradiria o Axioma IX.

(b) Suponha-se que $b \neq \emptyset$ é o primeiro elemento de $\underline{\alpha}$. Ora, neste caso, existe $x \in b$ e por (2) da definição 27, concluimos que $x \in \underline{\alpha}$, o que contraria a condição de b ser o mínimo de $\underline{\alpha}$.

(c) Vamos provar que z verifica as duas condições da definição 27. Sejam $x, y \in z$. Então, $(x, y \in z) \wedge (z \in \underline{\alpha}) \Rightarrow (x, y \in \underline{\alpha})$. Logo por (1) da definição 27 temos que $x \in y$ ou $y \in x$ ou $x = y$. Resta verificar que a condição (2) da definição 27 é satisfeita : Sejam $(x \in y)$ e $(y \in z)$. Ora, $(y \in z) \wedge (z \in \underline{\alpha}) \Rightarrow (y \in \underline{\alpha})$ e deste modo, se $(x \in y)$, então temos que $x \in \underline{\alpha}$ e portanto, $x, y \in \underline{\alpha}$. Assim sendo, uma de três coisas acontece : ou $x \in z$, ou $z \in x$ ou $z = x$. No entanto, se $z = x$, temos que $(x \in y) \wedge (y \in x)$, o que é impossível. Por outro lado, se $z \in x$, ao considerarmos $A = \{x, y, z\} \subset \underline{\alpha}$, notamos que não existe o primeiro elemento, pois $z \in x$, $x \in y$ e $y \in z$. Como provámos que teria de existir um primeiro elemento em A, concluimos que $x \in z$.

■

Lema 29 *(a) Se $\underline{\alpha}, \underline{\beta}$ são números ordinais e $\underline{\alpha} \neq \underline{\beta}$, então $\underline{\alpha} \subset \underline{\beta}$ se e só $\underline{\alpha} \in \underline{\beta}$*
(b) Se $\underline{\alpha}$ e $\underline{\beta}$ são números ordinais, ou $\underline{\alpha} \subset \underline{\beta}$ ou $\underline{\beta} \subset \underline{\alpha}$.

Prova:

(a) Suponha-se que $\underline{\alpha} \in \underline{\beta}$. Pela condição (2) da definição 27, se $x \in \underline{\alpha}$, então $x \in \underline{\beta}$, o que nos permite concluir que $\underline{\alpha} \subset \underline{\beta}$. Reciprocamente, suponha-se que $\underline{\alpha} \subsetneq \underline{\beta}$ e seja $x_0 \in \underline{\beta} \setminus \underline{\alpha}$ o primeiro elemento de $\underline{\beta} \setminus \underline{\alpha}$. Se $y \in x_0$, não podemos ter $y \in \underline{\beta} \setminus \underline{\alpha}$, pois x_0 é o primeiro elemento de $\underline{\beta} \setminus \underline{\alpha}$. Logo, $y \in x_0 \Rightarrow y \in \underline{\alpha}$ e como tal, $x_0 \subset \underline{\alpha}$. Por outro lado, seja $y \in \underline{\alpha}$. Se $x_0 \in y$ ou $x = y$, então $x_0 \in \underline{\alpha}$ (já que $(x_0 \in y) \wedge (y \in \underline{\alpha}) \Rightarrow (x_0 \in \underline{\alpha})$), o que é impossível. Assim sendo, $y \in \underline{\alpha} \Rightarrow y \in x_0$. Conclui-se que $\underline{\alpha} = x_0$. Logo, $\underline{\alpha} \subset \underline{\beta}$.

(b) É fácil verificar que $\underline{\alpha} \cap \underline{\beta}$ tem as propriedades (1) e (2) da definição 27 e portanto é um ordinal. Resta-nos mostrar que $\underline{\alpha} \cap \underline{\beta} = \underline{\alpha}$ ou que $\underline{\alpha} \cap \underline{\beta} = \underline{\beta}$. De facto, se não fôsse esse o caso, $\underline{\alpha} \cap \underline{\beta}$ estaria estritamente contido em $\underline{\alpha}$ e em $\underline{\beta}$ e por *(a)*, tinhamos que $(\underline{\alpha} \cap \underline{\beta}) \in (\underline{\alpha} \cap \underline{\beta})$, o que é impossível pelo Axioma IX.

■

Teorema 30 *Seja L a classe dos números ordinais e defina-se $\underline{\alpha} \prec \underline{\beta}$ se $\underline{\alpha} \subsetneq \underline{\beta}$.*
(1) L é bem ordenada por $\prec$.
(2) Para cada $\underline{\alpha} \in L$, o intervalo inicial $L(\underline{\alpha})$ é igual a $\underline{\alpha}$.

(3) Qualquer ordinal W é isomorfo a um intervalo inicial $L(\underline{\alpha})$. A $\underline{\alpha}$ chama-se o número ordinal de W e que se denota por ord(W)

Prova:

(1) : Deve ser claro que $\prec$ é uma ordem parcial. Verifiquemos que é uma boa ordem. Seja $E \subset L$ um conjunto não-vazio. Vamos mostrar que E tem um primeiro elemento. Escolha-se $\underline{\alpha_0} \in E$ e defina-se $A = \underline{\alpha_0} \cap E$. Se $A = \emptyset$, pelo Lema 29 *(a)*, temos que $x \in E \Rightarrow x \nsubseteq \underline{\alpha_0}$ e pelo Lema 29 *(b)*, temos que $(x \nsubseteq \underline{\alpha_0}) \Rightarrow (\underline{\alpha_0} \subset x)$. Deste modo podemos concluir que $\underline{\alpha_0}$ é o primeiro elemento de E. Se, alternativamente, $A \neq \emptyset$, então pelo Lema 28 *(a)* existe um primeiro elemento s de A, isto é, existe $s \in A$ tal que para todo $x \in A$ se tem que $(s \in x) \vee (s = x)$. Assim, temos $s \in E$ e $s \subset x$ para cada $x \in \underline{\alpha_0} \cap E$. Como $s \in \underline{\alpha_0}$ e como $\underline{\alpha_0} \subset y$ para cada $y \in E \setminus (\underline{\alpha_0} \cap E)$, também temos que $s \subset y$ para cada $y \in E \setminus (\underline{\alpha_0} \cap E)$ e portanto, s é o primeiro elemento de E.

(2) Dado $\underline{\alpha} \in L$ temos que, por definição de intervalo inicial e pelo Lema 29, $L(\underline{\alpha}) = \{\underline{\beta} : \underline{\beta} \in L \wedge \underline{\beta} \in \underline{\alpha}\}$. Como pelo Lema 28 *(c)*, a condição $\underline{\beta} \in L$ é redundante (já que $\underline{\beta} \in \underline{\alpha}$) concluimos que $L(\underline{\alpha}) = \{\underline{\beta} : \underline{\beta} \in \underline{\alpha}\} = \underline{\alpha}$.

(3) Começamos por provar que L não tem máximo. Suponha-se, por contradição, que $\underline{\alpha}$ é o máximo dos números ordinais. Temos que $\underline{\alpha} \cup \{\underline{\alpha}\}$ é ainda um número ordinal, pois verifica as condições da definição 27. Além disso, $\underline{\alpha} \prec \underline{\alpha} \cup \{\alpha\}$, o que é impossível. Observamos ainda que dado $X \subset L$ tal que X é não vazio, temos que $\{X\} \cup \bigcup\{\underline{\alpha} \in X\}$ é sempre um número ordinal maior do que qualquer $\underline{\alpha} \in X$. Como $\prec$ é uma boa ordem, dado um subconjunto X de L, existe sempre o menor dos números ordinais que são maiores que todos os números ordinais de X. A este número ordinal chama-se o supremo de X. Defina-se para cada $x \in W$ e cada função $\Psi : W(x) \to L$, $R_x(\Psi)$ como sendo o supremo de $\Psi(W(x))$. Esta definição é válida, pois pelo Axioma VI, $\Psi(W(x))$ é um conjunto e podemos aplicar o raciocínio do início da prova desta alínea. Pelo Teorema 26, existe uma aplicação $F : W \to L$ tal que $F(x) = R_x(F|W(x))$ para todo $x \in W$. Pela definição da regra $R_x(\Psi)$, verifica-se que $F(x)$ é um monomorfismo, já que se $x_1 \prec x_2$ temos que $F(x_1) \subsetneq F(x_2)$. De novo, existe $\underline{\beta} \in L$ tal que $F(W) \subset L(\underline{\beta})$ e portanto, pelo corolário 22 do capítulo anterior, concluimos que W é isomorfo a $L(\underline{\alpha})$ para algum $\underline{\alpha}$

. ■

Concluimos a secção com uma observação : L não é um conjunto. Se L fôsse um conjunto, as condições da definição 27 eram verificadas, o que levaria à contradição com o Axioma IX ($L \in L$). Sejam $x \in L$ e $y \in L$. Ou $x = y$, ou pelo Lema 29 temos que $x \subset y$ e portanto $x \in y$, ou então $y \subset x$ e portanto $y \in x$. Além disso, $(x \in y) \wedge (y \in L) \Rightarrow (x \in L)$.

3 Números Cardinais

Estamos agora em condições de definir o que é um número cardinal. Como tinhamos motivado no capítulo zero, a noção de *tamanho* de um conjunto é algo independente de um processo de contagem.

Definição 31 *Dois conjuntos X e Y têm o mesmo cardinal se existe uma bijecção entre ambos. Diz-se também que X e Y são conjuntos equipotentes e escrevemos* $\mathrm{card}(X) = \mathrm{card}(Y)$.

Podemos definir classes de equivalência, induzindo uma partição na classe dos conjuntos, por relação de equipotência. Mas o que é ao certo o número cardinal de um conjunto ? Queremos catalogar os conjuntos de acordo com o seu *tamanho*, ou seja, identificar um representante de uma classe que equipotência. Considere-se uma classe de equipotência C. Pelo Teorema da Boa Ordenação, todos os conjuntos desta classe podem ser bem-ordenados e pelo Teorema 30.(3), identificados com um número ordinal. Assim sendo, e como a classe dos ordinais é bem ordenada, existe o mínimo destes dos números ordinais.

Definição 32 *Seja X um conjunto. Dizemos que $\aleph(X) = min\{\alpha \in L : \alpha$ é equipotente a $X\}$ é o número cardinal de X.*

Definição 33 *Dados dois conjuntos X e Y, escrevemos* $\mathrm{card}(X) \leqslant \mathrm{card}(Y)$ *se existe $f : X \to Y$ injectiva.*

Lema 34 *(a) Se $A \subset X$,* $\mathrm{card}(A) \leqslant \mathrm{card}(X)$
(b) Se existe $f : X \to Y$ sobrejectiva, $\mathrm{card}(Y) \leqslant \mathrm{card}(X)$

Prova: *(a)* Basta considerar a aplicação de inclusão $A \hookrightarrow X$.
(b) Seja c uma função de escolha para $P(X)$. Então $y \mapsto c(f^{-1}(y))$ é uma função injectiva de Y para X. ■

Teorema 35 $\mathrm{card}(X) \leqslant \mathrm{card}(Y)$ *se e só se* $\aleph(X) \preccurlyeq \aleph(Y)$

Prova: Suponha-se que $\aleph(X) \preccurlyeq \aleph(Y)$. Como tal, $\aleph(X) \subseteq \aleph(Y)$. Existem bijecções $\Phi : X \to \aleph(X)$, $\Psi : Y \to \aleph(Y)$ e $j : \aleph(X) \hookrightarrow \aleph(Y)$. Assim, $\Psi^{-1} \circ j \circ \Phi : X \to Y$ é uma função injectiva e concluimos que $\text{card}(X) \leqslant \text{card}(Y)$. Se, por outro lado, $\text{card}(X) \leqslant \text{card}(Y)$, existe uma função injectiva $f : X \to \aleph(Y)$, podemos ver X como subconjunto de $\aleph(Y)$ e pelo Corolário 22 podemos concluir que $ord(X) \preccurlyeq \aleph(Y)$. Como $\aleph(X) \preccurlyeq ord(X)$, por transitividade temos que de facto $\aleph(X) \preccurlyeq \aleph(Y)$. ■

Nota: Sejam X e Y dois conjuntos tais que $\aleph(X) \preccurlyeq \aleph(Y)$ e $\aleph(Y) \preccurlyeq \aleph(X)$. Então, $\aleph(X) = \aleph(Y)$ e como tal, X e Y são equipotentes, isto é, $\text{card}(X) = \text{card}(Y)$.

Corolário 36 *(Teorema de Schröder-Bernstein): Se existem funções injectivas $X \to Y$ e $Y \to X$, então existe uma bijecção entre X e Y.*

Prova: Do Teorema 35, temos que $\aleph(X) \preccurlyeq \aleph(Y)$ e que $\aleph(Y) \preccurlyeq \aleph(X)$. Logo $\aleph(X) = \aleph(Y)$. Assim sendo, X e Y pertencem à mesma classe de equipotência e portanto, $\text{card}(X) = \text{card}(Y)$. ■

Nota: Se X e Y são conjuntos tais que $\text{card}(X) \leqslant \text{card}(Y)$ e $\text{card}(Y) \leqslant \text{card}(X)$, então pelo Teorema de Schröder-Bernstein temos que $\text{card}(X) = \text{card}(Y)$ e como tal, X e Y são equipotentes, isto é, $\aleph(X) = \aleph(Y)$.

Teorema 37 *(Cantor) Não existe uma função sobrejectiva entre X e P(X).*

Prova: Seja $Y = \{x \in X : x \notin \Psi(x)\} \in P(X)$. Suponha-se, por contradição, que Ψ é sobrejectiva. Então, $\exists x_0 \in X$ tal que $\Psi(x_0) = Y$. Mas vejamos que isto conduz a uma contradição : Ora, ou $x_0 \in Y$ ou $x_0 \notin Y$. No entanto, nenhum dos dois é possível ! Se $x_0 \in Y = \Psi(x_0)$, por definição de Y temos que $x_0 \notin Y$, o que é absurdo. Se, por outro lado, $x_0 \notin Y = \Psi(x_0)$, de novo por definição de Y temos que $x_0 \in Y$, o que é igualmente absurdo.■

Definição 38 *Um conjunto X diz-se **finito** se existir uma bijecção entre X e uma secção dos números naturais, caso contrário diz-se que X é **infinito**. Se X é um conjunto infinito, diz-se que $\aleph(X)$ é um número cardinal infinito.*

O Teorema de Cantor implica que existem *infinitos maiores que outros.* Dados dois conjuntos X e Y, se não existir uma função sobrejectiva $f : X \to Y$, escreve-se que $\text{card}(X) < \text{card}(Y)$. Observe-se que isto é equivalente à negação de $\text{card}(X) \geqslant \text{card}(Y)$. De facto, se não existe

uma função sobrejectiva $f : X \to Y$, então não pode existir uma função injectiva $h : Y \to X$, caso contrário $f : X \to Y$ tal que $f(x) = \begin{cases} h^{-1}(x), x \in h(Y) \\ y_0, \text{caso contrário} \end{cases}$, com $y_0 \in Y$, seria uma função sobrejectiva. Por outro lado, se não existe $g : Y \to X$ injectiva, então também não existe uma função $f : X \to Y$ sobrejectiva, caso contrário podiamos definir $g : Y \to X$, injectiva, impondo $g(y) \in f^{-1}(y)$.

Em particular, o Teorema de Cantor implica que o conjunto dos naturais não é *suficientemente grande* para listar todos os elementos do conjunto das suas partes. A qualquer conjunto *demasiado grande* para poder ser listado pelo conjunto dos naturais, no sentido de não existir uma função sobrejectiva dos naturais para o conjunto, chama-se conjunto *não contável*. Todos os outros conjuntos dizem-se *contáveis*. Na nossa terminologia, X diz-se contável se $\aleph(X) \preccurlyeq \aleph(\mathbb{N})$ e diz-se não contável se $\aleph(X) > \aleph(\mathbb{N})$. Ao número cardinal da classe de equipotência dos conjuntos contáveis não finitos, atribui-se usualmente o símbolo $\aleph_0$. Sabemos então que dado X infinito e contável, temos que $\aleph(X) \prec \aleph(P(X))$. Será que existe um número cardinal estritamente maior que $\aleph(X)$, mas estritamente menor que $\aleph(P(X))$? A Hipótese do Contínuo Generalizada diz que não.

Kurt Gödel provou que se os axiomas I-XI são consistentes, a negação da Hipótese do Contínuo Generalizada não pode ser provada com estes axiomas [2]. Por seu turno, J.P.Cohen provou que a Hipótese do Contínuo Generalizada não pode ser provada com os axiomas I-XI [Coh]. Como tal, a Hipótese de Contínuo (HC) é independente dos axiomas I-XI. A título de curiosidade, Sierpinski provou que o Axioma da Escolha poderia ser derivado apenas dos Axiomas I-X e da HC. Uma boa referência para as provas de independência é [Ku].

Teorema 39 *Seja κ a classe dos números cardinais*
(1) κ é bem-ordenada com a ordem induzida por L, a classe dos ordinais.
(2) $\aleph_0$ é o mais pequeno dos números cardinais infinitos.

Prova:

(1) Notando que $\kappa \subset L$, a asserção é uma consequência do facto de que qualquer subconjunto não vazio de um conjunto bem ordenado, com a ordem induzida, ser ainda um conjunto bem ordenado.

(2) Seja X um conjunto infinito. Ora, se X é um conjunto infinito, então existe $f : \mathbb{N} \to X$ injectiva e como tal, $\text{card}(\mathbb{N}) \leqslant \text{card}(X)$ [Mu, pg.57]. Portanto, pelo teorema 35 temos que $\aleph_0 \preccurlyeq \aleph(X)$, ficando provado que $\aleph_0$ é o mais pequeno dos cardinais infinitos.

■

Terminamos a secção com duas observações importantes :
(1) Não existe o maior dos números cardinais : Suponha-se, por contradição, que α é o maior dos números cardinais e seja X um representante. Pelo Teorema de Cantor, não existe função sobrejectiva $f : X \to P(X)$ e como tal, $\text{card}(P(X)) > \text{card}(X)$. Mas, pelo Teorema 35, temos que $\alpha \prec \aleph(P(X))$, o que é uma contradição.
(2) κ não é um conjunto : Suponha-se, por contradição, que κ é um conjunto. Então, $X = \bigcup_{\aleph \in \kappa} \aleph$ é um conjunto pelo Axioma V. O mesmo se sucede com $P(X)$, que é conjunto pelo Axioma VIII. Mas, $\aleph(P(X)) \subset X$, o que implica que $\text{card}(P(X)) \leqslant \text{card}(X)$, contrariando o Teorema 37.

3.1 Aritmética de Cardinais

Nesta secção, exploramos alguns resultados elementares da aritmética de cardinais. Como aplicação, mostra-se que a cardinalidade da base de um R-módulo livre com base infinita, está bem definida.

Definição 40 *Sejam $\aleph_1$ e $\aleph_2$ dois números ordinais, com representantes X e Y respectivamente. Define-se $\aleph_1 + \aleph_2 = \aleph(X \cup Y)$. Define-se ainda $\aleph_1 \aleph_2 = \aleph(X \times Y)$.*

Teorema 41 *Seja F um conjunto finito e X um conjunto infinito. Então, $\aleph(X) + \aleph(F) = \aleph(X)$.*

Prova: Como X é um conjunto infinito, existe uma função injectiva $f : \mathbb{N} \to X$. Seja $F = \{y_1, \cdots, y_m\}$. Podemos considerar a função $g : X \to X \cup F$, definida por : $g(x) = x$, se $x \notin f(N)$; $g(x) = y_j$, se $x = f(j)$ com $1 \leqslant j \leqslant m$ e $g(x) = f(j - m)$, se $x = f(j)$ com $m \leqslant j$. Então g é uma bijecção entre X e $X \cup F$ e consequentemente, $\aleph(X) = \aleph(X \cup F)$. ■

Teorema 42 *Sejam α e β números cardinais tais que $\beta \preccurlyeq \alpha$ e α é infinito. Então, $\alpha + \beta = \alpha$.*

Prova: Basta provar que $\alpha + \alpha = \alpha$ (de facto, $\alpha \preccurlyeq \alpha + \beta \preccurlyeq \alpha + \alpha = \alpha \Rightarrow \alpha + \beta = \alpha$, pelo Teorema de Schröder-Bernstein). Seja A tal que $\aleph(A) = \alpha$ e F a colecção dos pares (f, X) tais que $X \subset A$ e que $f : X \times \{0,1\} \to X$ é bijectiva. Vamos verificar que $F \neq \emptyset$: Seja $\Psi_1 : \mathbb{N} \times \{0,1\} \to \mathbb{N}$ a função bijectiva definida por $\Psi_1(n,0) = 2n$ e $\Psi_1(n,1) = 2n+1$. Considere-se agora uma bijecção $\Psi_2 : \mathbb{N} \to D$, para $D \subset A$. Esta função existe porque A é infinito. Então $\Psi_2 \circ \Psi_1 \circ (\Psi_2^{-1} \times \{0,1\})$ é um elemento de F. Ordene-se parcialmente F por *prolongamento*, isto é, $(f_1, X_1) \preccurlyeq (f_2, X_2)$ se e só se $X_1 \subseteq X_2$ e $f_{2|X_1} = f_1$. O Lema de Zorn garante então a existência de um elemento maximal $(g, C) \in F$. Sejam $C_0 = \{(c,0) : c \in C\}$ e $C_1 = \{(c,1) : c \in C\}$. Então C_0 e C_1 são disjuntos e $\text{card}(C_0) = \text{card}(C_1) = \text{card}(C)$. Como $g : C \times \{0,1\} \to C$ é uma bijecção, temos que $\text{card}(C) = \text{card}(C \times \{0,1\}) = \text{card}(C_0 \cup C_1)$. Então, $\aleph(C) = \aleph(C_0) + \aleph(C_1) = \aleph(C) + \aleph(C)$. Resta ver que $\aleph(C) = \alpha$: Se $A \setminus C$ fôr infinito, existe $B \subset A \setminus C$ tal que $\text{card}(B) = \text{card}(N)$ e portanto, como antes, existe uma bijecção $\Phi : B \times \{0,1\} \to B$. Pode então definir-se uma bijecção $\Gamma : (C \cup B) \times \{0,1\} \to (C \cup B)$, com $\Gamma(x) = g(x)$ para $x \in C \times \{0,1\}$ e $\Gamma(x) = \Phi(x)$ para $x \in B \times \{0,1\}$. Chegamos a uma contradição, pois $(g, C) \prec (h, C \cup B)$. Concluimos então que $A \setminus C$ é finito e pelo Teorema 41 temos que $\aleph(C) = \aleph(C \cup (A \setminus C)) = \aleph(A) = \alpha$.■

Teorema 43 *Sejam A e B dois conjuntos tais que $\aleph(A) = \alpha$ e $\aleph(B) = \beta$, com $B \neq \emptyset$. Então, se $\beta \preccurlyeq \alpha$ e α é infinito, temos que $\alpha\beta = \alpha$.*

Prova: Como na prova do Teorema 42, basta provar que $\alpha\alpha = \alpha$. Seja $\aleph(A) = \alpha$ e seja F a família parcialmente ordenada por prolongamento dos pares (f, X) tais que $f : X \times X \to X$ é uma bijecção, com $X \subset A$ infinito. Vamos verificar que $F \neq \emptyset$: Como A é infinito, existe $D \subset A$ tal que $\aleph(D) = \aleph_0$ e escolhendo uma bijecção entre $\mathbb{N}$ e $\mathbb{N} \times \mathbb{N}$ (ver por exemplo [HSW]) podemos definir uma bijecção entre D e $D \times D$. O Lema de Zorn garante então a existência de elemento maximal $(g, B) \in F$. Por definição, $\aleph(B \times B) = \aleph(B)$ e basta provar que $\aleph(B) = \aleph(A) = \alpha$. Ora, suponhamos que $\text{card}(A \setminus B) > \text{card}(B)$ e seja $C \subset A \setminus B$ tal que $\aleph(C) = \aleph(B)$. Então, $\aleph((B \cup C) \times (B \cup C)) = \aleph((B \times B) \cup (B \times C) \cup (C \times B) \cup (C \times C)) = \aleph(B \times B) + \aleph(B \times C) + \aleph(C \times B) + \aleph(C \times C)$. Como por hipótese $\aleph(B) = \aleph(C)$ e $\aleph(B \times B) = \aleph(C)$, temos que $\aleph((B \cup C) \times (B \cup C)) = (\aleph(B) + \aleph(B)) + (\aleph(C) + \aleph(C)) = \aleph(B) + \aleph(C) = \aleph(B \cup C)$, onde a penúltima igualdade é justificada pelo Teorema 42. Logo, existe uma bijecção entre $(B \cup C) \times (B \cup C)$ e $B \cup C$, o que contraria a hipótese de maximalidade de (g, B). Logo, $\aleph(A \setminus B) \preccurlyeq \aleph(B)$ e pelo Teorema 42, $\aleph(B) = \aleph(A \setminus B) + \aleph(B) = \aleph((A \setminus B) \cup B) = \aleph(A) = \alpha$.
■

Note-se em particular que , para α infinito, temos que $\alpha\aleph_0 = \alpha$. Note-se também que se α é infinito, prova-se por indução que $\alpha^n = \alpha$.

Teorema 44 *Seja A um conjunto. Então,* $\aleph(\bigcup_{n\in\mathbb{N}}(A^n)) = \aleph_0\aleph(A)$.

Prova: O resultado é claro se $A = \emptyset$. Se A é infinito, existem bijecções $f_n : A^n \to A$ pelo teorema anterior e então, $\Lambda : \bigcup_{n\in\mathbb{N}} A^n \to \mathbb{N} \times A$ definida por $u \mapsto (n, f_n(u))$ para $u \in A^n$, é uma bijecção. Conclui-se que $\aleph(A \times \mathbb{N}) = \aleph(\bigcup_{n\in\mathbb{N}} A^n)$ e como tal, $\aleph(A)\aleph_0 = \aleph(\bigcup_{n\in\mathbb{N}} A^n)$. Se A é finito e não-vazio, seja $h : N \to \bigcup_{n\in\mathbb{N}} A^n$ uma função tal que $h(n) \in A^n$. Então, h é injectiva e portanto, $\text{card}(\mathbb{N}) \leqslant \text{card}(\bigcup_{n\in\mathbb{N}} A^n)$. Por outro lado, existem funções injectivas $g_n : A^n \to \mathbb{N}$ para cada $n \in \mathbb{N}$, logo $g : \bigcup_{n\in\mathbb{N}}(A^n) \to \mathbb{N} \times \mathbb{N}$ definida por $g(u) = (n, f_n(u))$ para $u \in A^n$, é injectiva e deste modo, $\text{card}(\bigcup_{n\in\mathbb{N}} A^n) \leqslant \text{card}(\mathbb{N} \times \mathbb{N}) = \text{card}(\mathbb{N})$. Logo, pelo Teorema de Schröder-Bernstein, concluimos que $\aleph(\bigcup_{n\in\mathbb{N}} A^n) = \aleph_0 = \aleph_0\aleph(A)$, pelo Teorema 43 com $\alpha = \aleph_0$ ■

Definição 45 *Seja A um conjunto. O conjunto dos subconjuntos finitos de A, denota-se por* $P_{fin}(A)$.

Corolário 46 *Seja A um conjunto infinito. Então,* $\text{card}(A) = \text{card}(P_{fin}(A))$.

Prova: Considerando a função injectiva $\Psi : A \to P_{fin}(A)$ definida por $a \mapsto \{a\}$, concluimos que $\text{card}(A) \leqslant \text{card}(P_{fin}(A))$. Sendo $\Phi : P_{fin}(A) \to \bigcup_{n\in\mathbb{N}} A^n$ a função que atribui um subconjunto finito de A, $\{a_1, \cdots, a_k\}$ a si próprio mas enquanto elemento de A^k, obtemos uma função injectiva entre $P_{fin}(A)$ e $\bigcup_{n\in\mathbb{N}} A^n$. Como A é infinito, o teorema anterior garante que $\text{card}(\bigcup_{n\in\mathbb{N}} A^n) = \text{card}(A)$. Logo, concluimos que $\text{card}(P_{fin}(A)) \leqslant \text{card}(A)$. Pelo Teorema de Schröder-Bernstein, temos que $\text{card}(P_{fin}(A)) = \text{card}(A)$. ■.

Para concluir, vamos aplicar os resultados enunciados acima para obter um resultado fundamental sobre módulos. Seja M um R-módulo livre, finitamente gerado. Se o anel R é comutativo, sabemos que todas as bases de M têm o mesmo número de elementos [Hun]. No entanto, se R não fôr comutativo, tal pode não acontecer. Tal facto pode ser observado no contra-exemplo do teorema 47. No entanto, quando as bases são infinitas, têm sempre a mesma cardinalidade.

Teorema 47 *Seja $\mathbb{R}$ o corpo dos reais e $\mathbb{R}^\infty = \bigoplus_{i=1}^{\infty} \mathbb{R}$. Seja $A = Hom_{\mathbb{R}}(\mathbb{R}^\infty, \mathbb{R}^\infty)$ o anel das transformações $\mathbb{R}$-lineares de $\mathbb{R}^\infty$. Então, A enquanto A-módulo, tem uma base com um elemento e uma base com dois elementos.*

Prova: Seja $f : \bigoplus_{i=1}^{\infty} \mathbb{R} \to \bigoplus_{i=1}^{\infty} \mathbb{R}$ definida por $(x_1, x_2, x_3, \cdots) \mapsto (x_1, x_3, x_5, \cdots)$ e seja $g : \bigoplus_{i=1}^{\infty} \mathbb{R} \to \bigoplus_{i=1}^{\infty} \mathbb{R}$ definida por $(x_1, x_2, x_3, \cdots) \mapsto (x_2, x_4, x_6, \cdots)$. Como f e g são $\mathbb{R}$-lineares, temos que $f, g \in A$. Seja id a função identidade em $\mathbb{R}^{\infty}$. Vamos ver que $\{f, g\}$ e $\{id\}$ são bases para A. Como estamos a considerar A enquanto A-módulo, $\{id\}$ é uma base. Em relação ao conjunto $\{f, g\}$, primeiro provamos que f e g geram A : Basta encontrar $h_1, h_2 \in A$ tais que $h_1 f + h_2 g = id$. Para este efeito, escolha-se $h_1 : \bigoplus_{i=1}^{\infty} \mathbb{R} \to \bigoplus_{i=1}^{\infty} \mathbb{R}$ definida por $(x_1, x_2, \cdots) \mapsto (x_1, 0, x_2, 0, \cdots)$ e $h_2 : \bigoplus_{i=1}^{\infty} \mathbb{R} \to \bigoplus_{i=1}^{\infty} \mathbb{R}$ definida por $(x_1, x_2, \cdots) \mapsto (0, x_1, 0, x_2, 0, \cdots)$. Resta agora provar que f e g são linearmente independentes : Suponha-se que existem $h_1, h_2 \in A$ tais que $h_1 f + h_2 g = 0$, onde 0 é a função identicamente nula. Então, em particular para quaisquer $(x_1, x_3, x_5, \cdots) \in \mathbb{R}^{\infty}$, temos que $(h_1 f + h_2 g)(x_1, 0, x_3, 0, x_5, \cdots) = (0, 0, 0, \cdots)$, o que implica que $h_1(x_1, x_3, x_5, \cdots) = (0, 0, 0, \cdots)$ e portanto h_1 é a função identicamente nula. De forma análoga, $(h_1 f + h_2 g)(0, x_2, 0, x_4, 0, x_6, \cdots)$, concluimos que h_2 é a função identicamente nula. Logo, $\{f, g\}$ é uma base para A enquanto A-módulo. ■

Teorema 48 *Seja R um anel e M um R-módulo livre que não é finitamente gerado. Então, se $\{m_\alpha\}_{\alpha \in A}$ e $\{m_\beta\}_{\beta \in B}$ são bases de M, tem-se que* $\mathrm{card}(A) = \mathrm{card}(B)$.

Prova: Seja M um R-módulo e sejam $\{m_i\}_{i \in I}$ e $\{n_j\}_{j \in J}$ bases de M, com I infinito.

(1) J é infinito : Suponha-se, por contradição, que J é finito. Seja $J = \{1, \cdots, m\}$. Então, existem $c_{j_t} \in R$ tais que $n_j = \sum_{t=1}^{k_j} c_{j_t} m_{i_t}$. Note-se que as expressões para os elementos n_j em termos da base $\{m_i\}_{i \in I}$, só envolvem um número finito de elementos dessa base, digamos $X = \{m_{i_1}, \cdots, m_{i_w}\}$. Logo, X gera M e em particular, como X é finito e I é infinito, escolhendo $m_{i_0} \in \{m_i\}_{i \in I} \setminus X$, podemos escrever $m_{i_0} = \sum_{k=1}^{z} c_k m_{i_k}$, o que é impossível porque $\{m_i\}_{i \in I}$ é linearmente independente.

(2) Existe uma função $\Phi : I \to P_{fin}(J) \times \mathbb{N}$ injectiva: Seja $\Psi : I \to P_{fin}(J)$ a função que a $i \in I$ associa um conjunto de índices $\{j_1, \cdots, j_m\} \in P_{fin}(J)$ tais que $m_i = a_{j_1} n_{j_1} + \cdots + a_{j_m} n_{j_m}$, para alguns $a_{ji} \in R \setminus \{0\}$. A função está bem definida porque sendo $\{n_j\}_{j \in J}$ uma base, estas combinações lineares são únicas. Considere-se agora $P \subset P_{fin}(J)$. Então, $\Psi^{-1}(P)$ é finito : seja S o subconjunto finito de $\{n_j\}_{j \in J}$ indexado por P. Sejam $i : I \to \{m_i\}_{i \in I}$ e $j : P_{fin}(J) \to \{n_j\}_{j \in J}$ as funções que indexam vectores e conjuntos finitos de vectores das bases. Seja $\rho : \{m_i\}_{i \in I} \to \{n_j\}_{j \in J}$ tal que $\rho(v) = j \circ \Psi \circ i^{-1}(v)$. Ora $\rho^{-1}(S) \subset \langle S \rangle$ e como S é finito, existe um subconjunto finito $T \subset \{m_i\}_{i \in I}$ tal que $S \subset \langle T \rangle$ (construído de modo análogo ao que se fez em (1)). Deste modo, $\rho^{-1}(S) \subset \langle T \rangle$ e como tal, $\rho^{-1}(S) \subset T$, caso contrário $\{m_i\}_{i \in I}$ não seria linearmente independente. Como T é finito, concluimos que $\rho^{-1}(S)$ é finito

e consequentemente, $\Psi^{-1}(P)$ é finito. Podemos escolher uma ordenação em I e assim induzir uma ordenação em cada $\Psi^{-1}(P)$. Deste modo, seja $\Phi : I \to P_{fin}(J) \times \mathbb{N}$ a função definida por $\Phi(i) = (\Psi(i), \alpha)$, onde α é tal que i é o α-ésimo elemento de $\Psi^{-1}(\Psi(i))$. Para ver que Φ é injectiva, suponha-se que $\Phi(i_1) = \Phi(i_2)$. Assim, $\Psi(i_1) = \Psi(i_2)$ e se $i_1 \neq i_2$, a segunda coordenada de $\Phi(i_1)$ é diferente da segunda coordenada de $\Phi(i_2)$. Deste modo concluimos que $i_1 = i_2$ e portanto, Φ é uma função injectiva.

(3) Os cardinais de J e I são iguais: Pela alínea anterior, $\text{card}(I) \leqslant \text{card}(P_{fin}(J) \times N)$. Como J é infinito, $\text{card}(P_{fin}(J)) \geqslant \text{card}(N)$ e pelo Teorema 42, temos que $\text{card}(P_{fin}(J) \times N) = \text{card}(P_{fin}(J))$. Por sua vez, pelo corolário 45, temos que $\text{card}(P_{fin}(J)) = \text{card}(J)$ e portanto, $\text{card}(I) \leqslant \text{card}(J)$. De modo perfeitamente análogo, $\text{card}(J) \leqslant \text{card}(I)$ e pelo Teorema de Schröder-Bernstein, concluimos que $\text{card}(J) = \text{card}(I)$, como pretendido. ■

Referências

[JvH] Jean van Heijenoort, *From Frege to Gödel: A Source Book in Mathematical Logic*, Harvard University Press, 1976

[1] http://mathoverflow.net/questions/7155/famous-mathematical-quotes

[2] http://people.brandeis.edu/ lian/GCH-Summer03.PDF

[Coh] Paul J. Cohen, *Set Theory and the Continuum Hypothesis*, Dover Publications, 2008

[HSW] M. Holz, K. Steffens, E. Weitz ,*Introduction to Cardinal Arithmetic*, Birkhäuser, 1999

[Hun] Thomas W. Hungerford, *Algebra*, Springer, 1980

[Her] Herrlich, *Axiom of Choice*, Springer, 2006.

[Mu] J. Munkres, *Topology*, Pearson, 2000.

[Du] J. Dugundji, *Topology*, William C Brown Pub, 1966.

[Hal] P. Halmos, *Naive Set Theory*, Springer, 1974.

[Ku] K. Kunen, *Set Theory. An Introduction to Independence Proofs*, College Publications, 2011.