CONJUNTOS E ÁLGEBRA

1º SEMESTRE

Neste curso, recordaremos inicialmente a teoria ingênua de conjuntos e um pouco de lógica. Depois, estudaremos alguns rudimentos de álgebra: relações de equivalência e de ordem, reticulados, grupos, anéis, módulos e categorias. Finalmente, aprenderemos um pouco de álgebra linear.

1. Símbolos lógicos e conjuntos

Batize o Bicho Papão para domesticá-lo.
Sabedoria infantil

A lógica matemática e a teoria de conjuntos são ciências bastante sérias. Tendo ajudado a superar uma "crise de contradições" no ínicio do século passado, estas passaram a constituir uma base sólida para a matemática moderna[1] e servem como uma linguagem para expressar conceitos, ideias e demonstrações.

Aqui, tratamos as mencionadas áreas de maneira simplificada (primitiva e ingênua), a qual é entretanto suficiente, tomando-se um certo cuidado, para o estudo da matemática (pelo menos, em áreas diferentes das próprias lógica e teoria de conjuntos). Assim, "recordamos" a matéria que é melhor talvez nomear *(pato)lógica* e *teoria ingênua de conjuntos.*

1.1. Significado de símbolos lógicos. Uma *proposição* P (=uma afirmação que faz sentido) pode ser *falsa* (=*inválida*), que denotamos por 0, ou *verdadeira* (=*válida*), que denotamos por 1. Dadas proposições P, P_1, P_2, podemos formar novas proposições:

$\neg P$, ou seja, a *negação* de P;
$P_1 \vee P_2$, ou seja, P_1 *ou* P_2;
$P_1 \wedge P_2$, ou seja, P_1 *e* P_2;
$P_1 \Rightarrow P_2$, ou seja, P_1 *implica* P_2;
$P_1 \Leftrightarrow P_2$, ou seja, P_1 *é equivalente a* P_2.

Em termos de validade/invalidade, temos

$$\neg 0 = 1,\ \neg 1 = 0;\quad 0 \vee 0 = 0,\ 0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1;\quad 0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0,\ 1 \wedge 1 = 1;$$

$$(1 \Rightarrow 0) = 0,\ (0 \Rightarrow 0) = (0 \Rightarrow 1) = (1 \Rightarrow 1) = 1;\quad (0 \Leftrightarrow 1) = (1 \Leftrightarrow 0) = 0,\ (0 \Leftrightarrow 0) = (1 \Leftrightarrow 1) = 1.$$

1.1.1. Exercício. Usando as "tabelas de multiplicação" acima, verifique as seguintes *leis de Morgan*:

$$\neg\neg P \leftrightarrow P,\ P \vee \neg P \leftrightarrow 1,\ P \wedge \neg P \leftrightarrow 0,\ P \vee P \leftrightarrow P,\ P \wedge P \leftrightarrow P,\ P_1 \vee P_2 \leftrightarrow P_2 \vee P_1,\ P_1 \wedge P_2 \leftrightarrow P_2 \wedge P_1,$$

$$(P_1 \vee P_2) \vee P_3 \leftrightarrow P_1 \vee (P_2 \vee P_3),\ (P_1 \wedge P_2) \wedge P_3 \leftrightarrow P_1 \wedge (P_2 \wedge P_3),\ P_1 \wedge (P_2 \vee P_3) \leftrightarrow (P_1 \wedge P_2) \vee (P_1 \wedge P_3),$$

$$P_1 \vee (P_2 \wedge P_3) \leftrightarrow (P_1 \vee P_2) \wedge (P_1 \vee P_3),\ \neg(P_1 \vee P_2) \leftrightarrow \neg P_1 \wedge \neg P_2,\ \neg(P_1 \wedge P_2) \leftrightarrow \neg P_1 \vee \neg P_2,$$

[1] Hoje em dia, a teoria de conjuntos está sendo pouco a pouco substituída pela teoria de categorias, uma língua mais moderna, eficiente e adequada para a matemática.

$$\neg P_1 \vee P_2 \leftrightarrow P_1 \Rightarrow P_2,\ P_1 \Leftrightarrow P_2 \leftrightarrow (P_1 \Rightarrow P_2) \wedge (P_1 \Leftarrow P_2),\ P_1 \Rightarrow P_2 \leftrightarrow \neg P_1 \Leftarrow \neg P_2,$$

onde P, P_1, P_2, P_3 são proposições e o símbolo $\leftrightarrow$ diz que as proposições envolvidas são simultaneamente válidas/inválidas.

Uma proposição $P(x)$ pode depender de um parâmetro x (por exemplo, $P(x)$ pode afirmar que "o número inteiro x é par"). Nestes casos, podemos formar novas proposições que independem do parâmetro x:

$\exists x\ P(x)$, ou seja, *existe x tal que vale $P(x)$*;
$\forall x\ P(x)$, ou seja, *para todo x, vale $P(x)$*.

Os últimos dois símbolos lógicos se chamam *quantificadores,* os restantes são *elementares.*

A proposição $\exists x\ P(x)$ se trata como verdadeira exatamente quando existe um x tal que a proposição $P(x)$ é válida. A proposição $\forall x\ P(x)$ é verdadeira exatamente quando, para todo x, a proposição $P(x)$ é válida. Os limites de variação do parâmetro x são normalmente claros pelo contexto ou podem ser indicados explicitamente. Por exemplo, a proposição "todo número inteiro é par" se escreve como $\forall x \in \mathbb{Z}\ P(x)$. De fato, as proposições $\exists x \in C\ P(x)$ e $\forall x \in C\ P(x)$ significam $\exists x\ x \in C \wedge P(x)$ e $\forall x\ x \in C \Rightarrow P(x)$, respectivamente.

A leitura dos símbolos lógicos no idioma usual admite tipicamente vários sinônimos. Por exemplo, as proposições $P_1 \Rightarrow P_2$ e $\forall x\ P(x)$ podem ser lidas como "P_2 vale sempre que P_1 vale" e "qualquer que seja x, vale $P(x)$". Do ponto de vista formal, a escolha de um sinônimo não altera o significado matemático.

1.1.2. Exercício. Seja P uma proposição que independe de x (isto significa que a validade de $P(x)$ sempre é a mesma, independente da escolha de x), seja C um conjunto e sejam $Q(x)$ e $R(x,y)$ proposições que dependem respectivamente de x e de x, y. Convença-se que

$$\exists x\, Q(x) \leftrightarrow \exists y\, Q(y),\ \forall x\, Q(x) \leftrightarrow \forall y\, Q(y),\ \exists x \exists y\, R(x,y) \leftrightarrow \exists y \exists x\, R(x,y),\ \forall x \forall y\, R(x,y) \leftrightarrow \forall y \forall x\, R(x,y),$$

$$\neg\forall x\, Q(x) \leftrightarrow \exists x\, \neg Q(x),\ \neg\exists x\, Q(x) \leftrightarrow \forall x\, \neg Q(x),\ P \vee \exists x\, Q(x) \leftrightarrow \exists x\, P \vee Q(x),\ P \vee \forall x\, Q(x) \leftrightarrow \forall x\, P \vee Q(x),$$

$$P \wedge \exists x\ Q(x) \leftrightarrow \exists x\ P \wedge Q(x),\ P \wedge \forall x\ Q(x) \leftrightarrow \forall x\ P \wedge Q(x),\ P \Rightarrow \exists x\ Q(x) \leftrightarrow \exists x\ P \Rightarrow Q(x),$$

$$P \Rightarrow \forall x\ Q(x) \leftrightarrow \forall x\ P \Rightarrow Q(x),\ \big(\exists x \forall y\ R(x,y)\big) \Rightarrow \forall y \exists x\ R(x,y),$$

onde o símbolo $\leftrightarrow$ diz que as proposições envolvidas são simultaneamente válidas/inválidas.

Quais das implicações

$$\big(\exists x \in C\ Q(x)\big) \Rightarrow \forall x \in C\ Q(x),\ \big(\forall x \in C\ Q(x)\big) \Rightarrow \exists x \in C\ Q(x),\ \big(\forall y \exists x\ R(x,y)\big) \Rightarrow \exists x \forall y\ R(x,y),$$

$$\Big(\big(\exists x \in C\ Q(x)\big) \Rightarrow P\Big) \Rightarrow \big(\exists x \in C\ Q(x) \Rightarrow P\big),\ \big(\exists x \in C\ Q(x) \Rightarrow P\big) \Rightarrow \Big(\big(\exists x \in C\ Q(x)\big) \Rightarrow P\Big),$$

$$\Big(\big(\forall x \in C\ Q(x)\big) \Rightarrow P\Big) \Rightarrow \big(\forall x \in C\ Q(x) \Rightarrow P\big),\ \big(\forall x \in C\ Q(x) \Rightarrow P\big) \Rightarrow \Big(\big(\forall x \in C\ Q(x)\big) \Rightarrow P\Big)$$

são sempre válidas e por quê?

1.1.3. Exercício. Seja $P(x)$ uma proposição dependente de x. Usando os símbolos lógicos introduzidos acima, expresse a proposição $\exists! x\ P(x)$ cujo significado é "existe um único x tal que $P(x)$".

Os Exercícios 1.1.1–2, que utilizaremos em seguida sem referência, servem como regras para manipular proposições formalmente. Isto é especificamente útil quando não há como (ou quando é muito difícil) perceber o sentido das afirmações envolvidas.

Observe que basta usar apenas os símbolos lógicos $\neg$, $\vee$, $\exists$, pois os restantes se expressam em termos de $\neg$, $\vee$, $\exists$ pelos Exercícios 1.1.1–2.

Além dos introduzidos, usaremos o símbolo := que significa “igual por definição”.

1.2. Conjuntos. Em vez de definir o que é um conjunto, aceitamos a visão ingênua de que é razoável imaginar um conjunto como um saco de elementos. Escrevemos $e \in E$ quando e é um elemento do conjunto E (e está no saco E). Para descrever um conjunto C usamos a notação $C := \big\{e \mid P(e)\big\}$ ou $C := \big\{e \in E \mid P(e)\big\}$, onde $P(x)$ é uma propriedade (de elementos) e E é um conjunto dado. Isto se lê assim: o conjunto C é formado por todos os e (ou por todos os elementos e do conjunto E) que satisfazem a propriedade $P(e)$.

1.2.1. Notação padrão.
$\mathbb{C} := \{c \mid c$ é um número complexo$\}$ é o conjunto de todos os números complexos;
$\mathbb{R} := \{r \mid r$ é um número real$\}$ é o conjunto de todos os números reais;
$\mathbb{Q} := \{q \in \mathbb{R} \mid q$ é um número racional$\}$ é o conjunto de todos os números racionais;
$\mathbb{Z} := \{z \in \mathbb{Q} \mid z$ é um número inteiro$\}$ é o conjunto de todos os números inteiros;
$\mathbb{N} := \{n \in \mathbb{Z} \mid n \geqslant 0\}$ é o conjunto de todos os números naturais;
$\mathbb{R}^{\geqslant 0} := \{r \in \mathbb{R} \mid r \geqslant 0\}$ é o conjunto de todos os números reais não-negativos;
$\mathbb{R}^{>0} := \{r \in \mathbb{R} \mid r > 0\}$ é o conjunto de todos os números reais positivos;
$[a,b] := \{r \in \mathbb{R} \mid a \leqslant r \leqslant b\}$, $(a,b) := \{r \in \mathbb{R} \mid a < r < b\}$, $[a,b) := \{r \in \mathbb{R} \mid a \leqslant r < b\}$, $(a,b] := \{r \in \mathbb{R} \mid a < r \leqslant b\}$ são os intervalos fechado, aberto e semiabertos entre $a,b \in \mathbb{R}$;
$(-\infty,b] := \{r \in \mathbb{R} \mid r \leqslant b\}$, $(-\infty,b) := \{r \in \mathbb{R} \mid r < b\}$, $[a,\infty) := \{r \in \mathbb{R} \mid a \leqslant r\}$, $(a,\infty) := \{r \in \mathbb{R} \mid a < r\}$, $(-\infty,\infty) := \mathbb{R}$ intervalos (semi)infinitos;
$\varnothing := \{e \mid e \neq e\}$ o conjunto vazio (saco vazio).

Note que $[a,b] = \varnothing$ se $a > b$.

1.2.2. Paradoxos. Na visão ingênua da teoria de conjuntos, há alguns perigos. Considere os seguintes paradoxos.

Paradoxo do barbeiro. *O* barbeiro *é um homem da cidade que faz a barba de todos aqueles, e somente daqueles, homens da cidade que não barbeiam a si mesmos. Quem barbeia o* barbeiro*?*
Paradoxo de Russell. *Definimos $C := \{x \mid x \notin x\}$. Se $C \in C$, então $C \notin C$. Se $C \notin C$, então $C \in C$.*
Paradoxo de Richard. *O menor número natural que não pode ser descrito por uma frase em Português contendo no máximo cem letras.*

A receita de como evitar os perigos deste tipo é simples. Basta não fazer auto-referências e não formar conjuntos de todas as coisas possíveis. Considerando, por exemplo, o paradoxo de Richard, imagine que escrevemos ao lado de cada frase que determina um número natural concreto este mesmo número e analise o que acontece quando chega a hora de associar um número à frase em questão.

Tomando tal cuidado, assumimos a convenção que as relações do tipo $x_1 \in x_2 \in \cdots \in x_n \in x_1$ são proibidas.[2]

1.2.3. Operações com conjuntos e relações entre conjuntos. Sejam C_1 e C_2 conjuntos. Dizemos que C_1 está *contido* em C_2 ou que C_2 *contém* C_1 ou que C_1 é um *subconjunto* de C_2 se $\forall x\ x \in C_1 \Rightarrow x \in C_2$ e escrevemos $C_1 \subset C_2$ ou $C_2 \supset C_1$. Em outras palavras, para verificar que $C_1 \subset C_2$, precisa-se provar a implicação $x \in C_1 \Rightarrow x \in C_2$.

Dois conjuntos C_1, C_2 são considerados como iguais se eles têm os mesmos elementos. Em outras palavras, $C_1 = C_2$ é equivalente a $C_1 \subset C_2 \wedge C_1 \supset C_2$.

Denotamos por $C_1 \cap C_2$ a *interseção* de C_1 e C_2, isto é, $C_1 \cap C_2 := \{x \mid x \in C_1 \wedge x \in C_2\}$.

Denotamos por $C_1 \cup C_2 := \{x \mid x \in C_1 \vee x \in C_2\}$ a *união* de C_1 e C_2. Caso $C_1 \cap C_2 = \varnothing$, temos a *união disjunta* $C_1 \sqcup C_2 := C_1 \cup C_2$, que é a união usual com ênfase na *disjunção* $C_1 \cap C_2 = \varnothing$.

[2]De fato, o axioma de regularidade padrão da axiomática de Zermelo-Fraenkel exige mais do que isto: para qualquer conjunto não-vazio $C \neq \varnothing$, existe um elemento $c \in C$ tal que $c \cap C = \varnothing$.

Denotamos por $C_1 \times C_2 := \big\{(c_1, c_2) \mid c_1 \in C_1 \wedge c_2 \in C_2\big\}$ o *produto cartesiano* de C_1 e C_2. Este produto é formado por todos os pares *ordenados* (c_1, c_2), onde $c_1 \in C_1$ e $c_2 \in C_2$. Não é necessário saber o que é um par ordenado. É suficiente saber apenas a propriedade que caracteriza este conceito: $(c_1, c_2) = (c_1', c_2') \Leftrightarrow (c_1 = c_1' \wedge c_2 = c_2')$. (Um exemplo: $[0,1] \times [0,1]$ pode ser visto como um quadrado.) De modo análogo, podemos definir o produto cartesiano $C_1 \times C_2 \times \cdots \times C_n$ de conjuntos $C_1, C_2, \dots, C_n$.

Denotamos por $C_1 \setminus C_2 := \{x \in C_1 \mid x \notin C_2\}$ o *complemento* de C_2 em C_1.

Para os fins de não poluir a notação, com frequência escrevemos p no lugar de $\{p\}$ quando não há grande perigo de confusão. Por exemplo, $\mathbb{R} \setminus 0$ é o conjunto de todos os números reais não-nulos, $\mathbb{R} \setminus 0 := \mathbb{R} \setminus \{0\}$.

Sejam C, C_1, C_2, C_3 conjuntos e $S, S_1, S_2 \subset C$ subconjuntos. As relações

$$C \setminus (C \setminus S) = S,\ S \sqcup (C \setminus S) = C,\ C \cup C = C,\ C \cap C = C,\ C_1 \cup C_2 = C_2 \cup C_1,\ C_1 \cap C_2 = C_2 \cap C_1,$$

$$(C_1 \cup C_2) \cup C_3 = C_1 \cup (C_2 \cup C_3),\ (C_1 \cap C_2) \cap C_3 = C_1 \cap (C_2 \cap C_3),\ C_1 \cap (C_2 \cup C_3) = (C_1 \cap C_2) \cup (C_1 \cap C_3),$$

$$C_1 \cup (C_2 \cap C_3) = (C_1 \cup C_2) \cap (C_1 \cup C_3),\ C \setminus (S_1 \cup S_2) = (C \setminus S_1) \cap (C \setminus S_2),\ C \setminus (S_1 \cap S_2) = (C \setminus S_1) \cup (C \setminus S_2),$$

$$(C \setminus S_1) \cup S_2 = C \Leftrightarrow S_1 \subset S_2,\ C_1 = C_2 \Leftrightarrow (C_1 \subset C_2) \wedge (C_1 \supset C_2),\ S_1 \subset S_2 \Leftrightarrow (C \setminus S_1) \supset (C \setminus S_2)$$

são consequências imediatas das correspondentes leis de Morgan e podem ser obtidas através da assim chamada "*demonstração por definição*". Já que qualquer definição é nada mais do que uma abreviação, tal método consiste simplesmente em "decifrar a abreviação". Para exemplificar, mostramos a identidade $C_1 \cup (C_2 \cap C_3) = (C_1 \cup C_2) \cap (C_1 \cup C_3)$. Por definição de união, $x \in C_1 \cup (C_2 \cap C_3)$ é equivalente a $x \in C_1 \vee x \in C_2 \cap C_3$. Por definição de interseção, isto pode ser reescrito como $x \in C_1 \vee (x \in C_2 \wedge x \in C_3)$. De forma análoga, $x \in (C_1 \cup C_2) \cap (C_1 \cup C_3)$ é equivalente a $(x \in C_1 \vee x \in C_2) \wedge (x \in C_1 \vee x \in C_3)$. Resta aplicar a correspondente lei de Morgan, onde P_i é $x \in C_i$ para $i = 1, 2, 3$.

1.2.4. Exercício. Prove as relações

$$\varnothing \in \{\varnothing\},\ \{\varnothing\} \neq \varnothing,\ \varnothing \subset \{\varnothing\},\ \{\varnothing \mid \varnothing \neq \varnothing\} = \varnothing,\ \varnothing \subset C,\ \varnothing \cup C = C,\ \varnothing \cap C = \varnothing,\ C \setminus C = \varnothing,$$

$$(C_1 \subset C_2 \wedge C_2 \subset C_3) \Rightarrow C_1 \subset C_3,\ C_1 \subset C_1 \cup C_2,\ C_1 \supset C_1 \cap C_2,\ (C_1 \subset C \wedge C_2 \subset C) \Rightarrow C_1 \cup C_2 \subset C,$$

$$(C \subset C_1 \wedge C \subset C_2) \Rightarrow C \subset C_1 \cap C_2,\ C_1 \cup C_2 = C_2 \Leftrightarrow C_1 \subset C_2 \Leftrightarrow C_1 \cap C_2 = C_1,$$

$$\varnothing \times C = \varnothing,\ (C_1 \times C_2) \cap (C_1' \times C_2') = (C_1 \cap C_1') \times (C_2 \cap C_2'),\ (C_1 \cup C_1') \times C = (C_1 \times C) \cup (C_1' \times C),$$

$$C \times (C_2 \cup C_2') = (C \times C_2) \cup (C \times C_2'),\ (C_1 \setminus C_1') \times C = (C_1 \times C) \setminus (C_1' \times C),$$

$$(C_1 \times C_2) \setminus (C_1' \times C_2') = \big((C_1 \setminus C_1') \times C_2\big) \sqcup \big((C_1 \cap C_1') \times (C_1' \setminus C_2')\big),\ C_1 \times C_2 = C_2 \times C_1 \neq \varnothing \Rightarrow C_1 = C_2.$$

para quaisquer conjuntos $C, C_1, C_1', C_2, C_2', C_3$.

1.2.5. Famílias de conjuntos. Seja I um conjunto (de índices). Se, para cada $i \in I$, é dado um conjunto C_i, temos uma *família* de conjuntos C_i, $i \in I$.

A *união* da família é o conjunto formado por todos os elementos que pertencem a pelo menos um dos membros da família, $\bigcup\limits_{i \in I} C_i := \{x \mid \exists i \in I\ x \in C_i\}$. Caso $C_i \cap C_{i'} = \varnothing$ para quaisquer distintos $i, i' \in I$, $i \neq i'$, isto é, caso a família seja *disjunta,* temos a *união disjunta* $\bigsqcup\limits_{i \in I} C_i := \bigcup\limits_{i \in I} C_i$, a união usual da família com a ênfase em que a família é disjunta.

A *interseção* da família é o conjunto formado por todos os elementos que pertencem a todos os membros da família, $\bigcap\limits_{i \in I} C_i := \{x \in U \mid \forall i \in I\ x \in C_i\}$. (Aqui U é um conjunto-universo. Se $I = \varnothing$, a restrição $x \in U$ é necessária, pois, sem esta, enfrentamos um paradoxo.)

Seja $C_i \subset X$, $i \in I$, uma família de conjuntos. Qualquer subconjunto $I' \subset I$ determina uma nova família C_i, $i \in I'$, chamada *subfamília* da original. Podemos considerar também uma família de subfamílias. Formalmente, seja $I_j \subset I$, $j \in J$, uma família de subconjuntos de I. Então temos uma família cujo j-ésimo membro é a família C_i, $i \in I_j$, onde j percorre J.

1.2.6. Exercício. Sejam C_i, $i \in I$, e $C'_{i'}$, $i' \in I'$, famílias de conjuntos, seja $I_j \subset I$, $j \in J$, uma família de subconjuntos de I e seja C um conjunto. Prove as seguintes fórmulas:

$$C \setminus \bigcup_{i\in I} C_i = \bigcap_{i\in I}(C \setminus C_i),\ C \setminus \bigcap_{i\in I} C_i = \bigcup_{i\in I}(C \setminus C_i),\ C \cap \bigcup_{i\in I} C_i = \bigcup_{i\in I}(C \cap C_i),\ C \cup \bigcap_{i\in I} C_i = \bigcap_{i\in I}(C \cup C_i),$$

$$\Big(\bigcup_{i\in I} C_i\Big) \cap \Big(\bigcup_{i'\in I'} C'_{i'}\Big) = \bigcup_{i\in I, i'\in I'} (C_i \cap C'_{i'}),\quad \Big(\bigcap_{i\in I} C_i\Big) \cup \Big(\bigcap_{i'\in I'} C'_{i'}\Big) = \bigcap_{i\in I, i'\in I'} (C_i \cup C'_{i'}),$$

$$\bigcup_{j\in J}\Big(\bigcup_{i\in I_j} C_i\Big) = \bigcup_{i\in \bigcup\limits_{j\in J} I_j} C_i,\qquad \bigcap_{j\in J}\Big(\bigcap_{i\in I_j} C_i\Big) = \bigcap_{i\in \bigcup\limits_{j\in J} I_j} C_i.$$

1.3. Funções. Uma *função* $f : D \to C$ de D para C é uma lei pela qual a cada elemento $d \in D$ está associado um único elemento $c \in C$, denotado por $c = f(d)$ e chamado a *imagem* de d. Escreve-se também $D \xrightarrow{f} C$. Dizemos que D é o *domínio* e C é o *codomínio* de f. Note que, por definição, consideramos duas funções $f : D \to C$ e $f' : D' \to C'$ como diferentes se os domínios ou codomínios são diferentes, isto é, se $D \neq D'$ ou $C \neq C'$, mesmo se a lei parece a mesma. Por exemplo, temos duas funções $f : \mathbb{R} \to \mathbb{R}$, $f : r \mapsto r^2$, e $f' : \mathbb{R} \to \mathbb{R}^{\geqslant 0}$, $f' : r \mapsto r^2$, que são diferentes embora dadas através da mesma lei $r \mapsto r^2$. (Escrevendo $f : d \mapsto c$, enfatizamos como f "age" sobre elementos; isto é equivalente a escrever $f(d) = c$.)

Seja $f : D \to C$ uma função. Denotamos por $\Gamma_f := \Big\{\big(d, f(d)\big) \in D \times C \mid d \in D\Big\}$ o *gráfico* da função f.

Seja $f : D \to C$ uma função e sejam $D' \subset D$ e $C' \subset C$. Então $fD' := \big\{f(d) \mid d \in D'\big\}$ é a *imagem* de D' por f e $f^{-1}C' := \big\{d \in D \mid f(d) \in C'\big\}$ é a *imagem inversa* (ou *pré-imagem*) de C' por f.

Definimos a *restrição* $f|_{D'} : D' \to C$ de f para $D' \subset D$ pela regra óbvia $f|_{D'} : d' \mapsto f(d')$. A função de *inclusão* $i : D' \hookrightarrow D$ é dada pela regra $i : d' \mapsto d'$ para todo $d' \in D'$.

Sejam $C_1 \xrightarrow{f_1} C_2 \xrightarrow{f_2} C_3$ duas funções dos formatos indicados. Definimos a função *composta* ou a *composição* $f_2 \circ f_1 : C_1 \to C_3$ pela regra $(f_2 \circ f_1)(x) := f_2\big(f_1(x)\big)$ para todo $x \in C_1$. Essa operação é associativa: é fácil verificar que $(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1)$ para funções $C_1 \xrightarrow{f_1} C_2 \xrightarrow{f_2} C_3 \xrightarrow{f_3} C_4$. Podemos observar também que a restrição $f|_{D'}$ da função $f : D \to C$ para $D' \subset D$ é a composição $f \circ i$, isto é, $f|_{D'} = f \circ i$, onde $i : D' \hookrightarrow D$ é a função de inclusão. Para qualquer conjunto C, temos a função *idêntica* $1_C : C \to C$ dada pela regra $1_C : c \mapsto c$. Essa função satisfaz as identidades $f_1 \circ 1_C = f_1$ e $1_C \circ f_2 = f_2$ para quaisquer funções $f_1 : C \to C_1$ e $f_2 : C_2 \to C$.

Uma função $f : D \to C$ é dita *injetora* ou uma *injeção* se $\forall d_1, d_2 \in D\ f(d_1) = f(d_2) \Rightarrow d_1 = d_2$. Enfatizando que uma função $f : D \to C$ é injetora, escrevemos $f : D \hookrightarrow C$. A função de inclusão considerada acima é um exemplo de uma função injetora. Uma função $f : D \to C$ é dita *sobrejetora* ou uma *sobrejeção* se todo elemento de C é a imagem por f de um elemento de D, isto é, se $\forall\ c \in C$ $\exists\ d \in D\ f(d) = c$. Equivalentemente, f é sobrejetora se e só se $fD = C$. Uma função $f : D \to C$ simultaneamente injetora e sobrejetora é dita *bijetora* ou uma *bijeção.*

1.3.1. Exercício. Sejam $f : D \to C$ e $C_1 \xrightarrow{f_1} C_2 \xrightarrow{f_2} C_3$ funções. Mostre que

- f é sobrejetora se e só se possui uma inversa à direita $g : D \leftarrow C$, isto é, $f \circ g = 1_C$;

• supondo que $D \neq \varnothing$, f é injetora se e só se possui uma inversa à esquerda $g : D \leftarrow C$, isto é, $g \circ f = 1_D$;
• f é bijetora se e só se possui uma inversa bilateral $g : D \leftarrow C$, isto é, $f \circ g = 1_C$ e $g \circ f = 1_D$; tal inversa é única se existir e é denotada por f^{-1};
• se f_1 e f_2 são bijeções, então $f_2 \circ f_1$ é uma bijeção e $(f_2 \circ f_1)^{-1} = f_1^{-1} \circ f_2^{-1}$.

1.3.2. Exercício. Sejam $f : D \to C$, $f' : C \to B$ funções, sejam $D_i \subset D$, $i \in I$, e $C_j \subset C$, $j \in J$, famílias de subconjuntos e sejam $D' \subset D$, $C' \subset C$ e $B' \subset B$ subconjuntos. Prove as seguintes fórmulas.

$$f \bigcup_{i\in I} D_i = \bigcup_{i\in I} fD_i,\ f \bigcap_{i\in I} D_i \subset \bigcap_{i\in I} fD_i,\ (f' \circ f)D' = f'(fD'),\ (f' \circ f)^{-1}B' = f^{-1}(f'^{-1}B'),$$

$$f^{-1} \bigcup_{j\in J} C_j = \bigcup_{j\in J} f^{-1}C_j,\ f^{-1} \bigcap_{j\in J} C_j = \bigcap_{j\in J} f^{-1}C_j,\ f^{-1}(C \setminus C') = D \setminus f^{-1}C'.$$

Planejando omitir em seguida demonstrações por definição, exemplificamos pela última vez como provar, digamos, a fórmula $(f' \circ f)^{-1}B' = f^{-1}(f'^{-1}B')$. Por definição de imagem inversa, a afirmação que $x \in f^{-1}(f'^{-1}B')$ significa que $x \in D \wedge f(x) \in f'^{-1}B'$ e, pela mesma razão, que $x \in D \wedge \Big(f(x) \in C \wedge f'\big(f(x)\big) \in B'\Big)$. Sendo $f(x) \in C$ para todo $x \in D$, podemos retirar essa parte, obtendo $x \in D \wedge (f' \circ f)(x) \in B'$ por definição de composta. Por definição de imagem inversa, isto significa que $x \in (f' \circ f)^{-1}B'$.

O produto cartesiano $C_1 \times C_2$ está munido de *projeções* $\pi_i : C_1 \times C_2 \to C_i$, $i = 1, 2$. Estas obviamente são sobrejetoras. Mais geralmente, seja C_i, $i \in I$, uma família de conjuntos. Definimos o *produto cartesiano* dessa família pela fórmula $\prod\limits_{i\in I} C_i := \Big\{I \xrightarrow{f} \bigcup\limits_{i\in I} C_i \mid \forall i \in I\ f(i) \in C_i\Big\}$. Os elementos de $\prod\limits_{i\in I} C_i$ são tipicamente denotados por $(c_i)_{i\in I}$ em vez de $I \xrightarrow{f} \bigcup\limits_{i\in I} C_i$, onde $c_i := f(i)$ para todo $i \in I$. Para cada $i \in I$, temos a *projeção* $\pi_i : \prod\limits_{i\in I} C_i \to C_i$ (claramente sobrejetiva).

1.3.3. Exercício. Seja $f_i : C \to C_i$, $i \in I$, uma família de funções. Mostre que existe uma única função $f : C \to \prod\limits_{i\in I} C_i$ tal que $\pi_i \circ f = f_i$ para todo $i \in I$. [diagrama]

1.3.4. Exercício. Seja C_i, $i \in I$, uma família disjunta de conjuntos e seja $f_i : C_i \to C$, $i \in I$, uma família de funções. Mostre que existe uma única função $f : \bigsqcup\limits_{i\in I} C_i \to C$ tal que $f \circ \iota_i = f_i$ para todo $i \in I$, onde $\iota_i : C_i \hookrightarrow \bigsqcup\limits_{i\in I} C_i$, $i \in I$, são as funções de inclusão. [diagrama]

1.3.5. Exercício. Seja $f : D \to C$ uma função e sejam $\iota : C' \hookrightarrow C$ e $\iota' : f^{-1}C' \hookrightarrow D$ funções de inclusão. Note que existe uma única função $f' : f^{-1}C' \to C'$ tal que $f \circ \iota' = \iota \circ f'$. Sejam $g : X \to C'$ $j : X \to D$ funções tais que $f \circ j = \iota \circ g$. Mostre que existe uma única função $h : X \to f^{-1}C'$ tal que $f' \circ h = g$ e $\iota' \circ h = j$. [diagrama]

1.4. Cardinalidade. Grosso modo, a cardinalidade de um conjunto mede quão grande é o conjunto, isto é, "quantos elementos" ele possui. Dizemos que os conjuntos C_1 e C_2 têm a mesma *cardinalidade* se existe uma bijeção entre C_1 e C_2. (Não importa se $C_1 \to C_2$ ou se $C_1 \leftarrow C_2$, pois a inversa de uma bijeção é uma bijeção; em símbolos, $C_1 \simeq C_2$ é uma bijeção entre C_1 e C_2.) Denotamos por $|C|$ ou por $\#C$ a cardinalidade de C.

Assim, os números naturais são as cardinalidades de conjuntos finitos. Por definição, o conjunto $\mathbb{N}$ é enumerável. Esta é a menor cardinalidade infinita. Dizemos que $|C_1| \leqslant |C_2|$ se existe uma função injetora $C_1 \hookrightarrow C_2$. É possível mostrar (mas não é trivial) que, dadas cardinalidades c_1, c_2, vale $c_1 \leqslant c_2$ ou $c_1 \geqslant c_2$.

Cardinalidades admitem várias operações: adição, multiplicação, potências, etc.: $|C_1|+|C_2| := |C_1 \sqcup C_2|$, $|C_1|\cdot|C_2| := |C_1 \times C_2|$, $|C_2|^{|C_1|} := |C_2^{C_1}|$, onde $C_2^{C_1} := \{C_1 \to C_2\}$. Na verdade, $|C_1|+|C_2| = |C_1|\cdot|C_2| = \max\big(|C_1|, |C_2|\big)$ se $|C_1| \neq 0$ e $|C_2|$ é infinita.

Denotamos por $2^C := \{X \mid X \subset C\}$ o conjunto das partes de C ou o *booleano* de C. A cada subconjunto $X \subset C$, podemos associar a *função característica* de X. Tal função $\chi_X : C \to \{0,1\}$ é dada pela regra $\chi_X : c \mapsto 0$ se $c \notin X$ e $\chi_X : c \mapsto 1$ se $c \in X$. A fórmula $f \mapsto f^{-1}1$ estabelece uma bijeção $2^C \simeq \{0,1\}^C$.

1.4.1. Exercício. Sejam C, C_1, C_2 conjuntos. Note que $2^{C_1 \cap C_2} = 2^{C_1} \cap 2^{C_2}$ e $C_1 \subset C_2 \Rightarrow 2^{C_1} \subset 2^{C_2}$. Estabeleça as seguintes bijeções:

$$2^C \simeq \{0,1\}^C,\ 2^{C_1 \sqcup C_2} \simeq 2^{C_1} \times 2^{C_2},\ C^{C_1 \sqcup C_2} \simeq C^{C_1} \times C^{C_2},\ (2^{C_1})^{C_2} \simeq 2^{C_1 \times C_2},\ (C^{C_1})^{C_2} \simeq C^{C_1 \times C_2}.$$

1.4.2. Exercício. Prove que $|2^C| \neq |C|$ para qualquer conjunto C. (Dica: se $b : C \to \{0,1\}^C$ é uma bijeção, então a função $f : C \to \{0,1\}$ dada pela regra $f : c \mapsto 1 - b(c)(c)$ deve ter a forma $f = b(c')$ para algum $c' \in C$; calculando o valor $f(c')$ chegamos a uma contradição. A ideia apresentada, o *argumento da diagonalização de Cantor,* foi de fato utilizada no paradoxo de Russell no item 1.2.2.)

1.4.3. Teorema (Cantor-Schröder-Bernstein). *Sejam A e B conjuntos tais que $|A| \leqslant |B|$ e $|A| \geqslant |B|$. Então $|A| = |B|$.*

Demonstração.[3] Temos duas bijeções $f : A \to B'$ e $g : A' \leftarrow B$, onde $A' \subset A$ e $B' \subset B$. Definamos indutivamente $C_0 := A \setminus A'$ e $C_{n+1} := gfC_n$. Sejam $C := \bigcup\limits_{n\in\mathbb{N}} C_n$ e $C' := \bigcup\limits_{n\in\mathbb{N}} C_{n+1}$. Segue de $A \setminus C = A' \setminus C'$ que

$$g^{-1}(A \setminus C) = g^{-1}\Big(A' \setminus \bigcup_{n\in\mathbb{N}} C_{n+1}\Big) = B \setminus \bigcup_{n\in\mathbb{N}} g^{-1}C_{n+1} =$$

$$= B \setminus \bigcup_{n\in\mathbb{N}} g^{-1}gfC_n = B \setminus \bigcup_{n\in\mathbb{N}} fC_n = B \setminus f\Big(\bigcup_{n\in\mathbb{N}} C_n\Big) = B \setminus fC.$$

Em outras palavras, g estabelece uma bijeção entre $B \setminus fC$ e $A \setminus C$ e f estabelece uma bijeção entre C e fC ■

1.5. Conjuntos enumeráveis. Se um conjunto C é finito ou tem a cardinalidade de $\mathbb{N}$, ele é dito *enumerável.*

1.5.1. Lema. $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Demonstração. Seja $\iota : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ a função definida pela regra $\iota : (m,n) \mapsto (2m+1)2^n$. Suponha que $(2m+1)2^n = (2m'+1)2^{n'}$ com $n \leqslant n'$. Então $2m+1 = (2m'+1)2^{n'-n}$. Daí concluímos que $n = n'$, pois, caso contrário, $2m+1$ seria par. Logo, $2m+1 = 2m'+1$, implicando $m = m'$. Em outras palavras, ι é injetora. Resta aplicar o Teorema 1.4.3 ■

Os seguintes exercícios podem ser resolvidos usando os Teorema 1.4.3 e Lema 1.5.1.

1.5.2. Exercício. Mostre que $C = \bigcup\limits_{n\in\mathbb{N}} C_n$ é enumerável se cada C_n é enumerável.

1.5.3. Exercício. Mostre que os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{Q}[x]$ são enumeráveis. Aqui $\mathbb{Q}[x]$ denota o conjunto de todos os *polinômios de uma variável x* com coeficientes em $\mathbb{Q}$, isto é, de todas expressões formais da forma $q_0 + q_1x + \cdots + q_nx^n$, onde $q_0, q_1, \dots, q_n \in \mathbb{Q}$ e $n \in \mathbb{N}$ estão variando.

[3]Esta demonstração explora uma ideia de Misha Verbitsky.

1.5.4. Exercício. Mostre que $|\mathbb{R}| = |2^{\mathbb{N}}|$.

1.6. Axioma da escolha. Tal axioma (AE) afirma que qualquer função sobrejetiva $f : D \to C$ possui inversa à direita $g : D \leftarrow C$, isto é, $f \circ g = 1_C$ (vide o Exercício 1.3.1). Em outras palavras, a função g efetua uma escolha $g(c)$ de um elemento na imagem inversa $f^{-1}c$ não-vazia para todo $c \in C$, ou seja, $g(c) \in f^{-1}c$. O AE parece óbvio. Porém, possui algumas consequências surpreendentes. Por exemplo, AE implica que uma bola de raio 1 em $\mathbb{R}^3$ pode ser decomposta na união disjunta de 5 subconjuntos, os quais, sendo movidos (como peças sólidas) dentro de $\mathbb{R}^3$, formam duas bolas disjuntas de raio 1 (o paradoxo de Banach-Tarski). Por outro lado, assumir AE não faz mal: se isto leva a uma contradição, então assumir a negação de AE também leva a uma contradição. Entretanto, vários matemáticos evitam usar AE, pois toda demonstração usando AE é não-construtiva, isto é, apela a objetos construídos implicitamente.

Em seguida, aceitamos AE.

2. Relações

Uma pessoa decente nunca escreveria
uma epígrafe sob tal título
P. Decente

Sejam $C_1, \dots, C_n$ conjuntos. Uma *correspondência n-ária* é simplesmente um subconjunto $R \subset C_1 \times \dots \times C_n$. Em vez de $(c_1, \dots, c_n) \in R$, podemos escrever $R(c_1, \dots, c_n)$, dizendo assim que $R(c_1, \dots, c_n)$ *vale*. Caso $C := C_1 = \dots = C_n$, obtemos uma *relação n-ária sobre C*. Para uma relação binária $R \subset C \times C$, podemos escrever $c_1 R c_2$ no lugar de $R(c_1, c_2)$. Associando a uma função $f : D \to C$ seu gráfico $\Gamma_f \subset D \times C$, de fato, tratamos a função como uma correspondência binária. Neste sentido, a relação binária de igualdade $=$ sobre um conjunto C, também chamada *diagonal* $\triangle := \triangle_C \subset C \times C$, corresponde à função idêntica $1_C : C \to C$.

2.1. Relações de equivalência. Com frequência, quando afirmamos que objetos matemáticos são iguais, não temos em mente uma igualdade plena. É bem possível que pensamos em "igualdade num certo sentido", considerando como irrelevantes alguns aspectos dos objetos em consideração. A relação binária de equivalência definida abaixo é uma formalização desta visão.

2.1.1. Definição. Seja $\sim$ uma relação binária sobre um conjunto C. Dizemos que $\sim$ é uma *relação de equivalência* (ou simplesmente *equivalência*) sobre C se ela é *reflexiva, simétrica* e *transitiva.* Isto quer dizer que

- $\forall c \in C\ c \sim c$ (*reflexividade*);
- $\forall c_1, c_2 \in C\ c_1 \sim c_2 \Rightarrow c_2 \sim c_1$ (*simetria*);
- $\forall c_1, c_2, c_3 \in C\ (c_1 \sim c_2 \wedge c_2 \sim c_3) \Rightarrow c_1 \sim c_3$ (*transitividade*).

Seja $\sim$ uma equivalência sobre C e seja $S \subset C$ um subconjunto. Então temos a *equivalência induzida* $\sim|_S$ sobre S. Frequentemente, tal equivalência se denota pelo mesmo símbolo $\sim$.

2.1.2. Definição. Uma *partição* do conjunto C é uma decomposição de C na união disjunta de subconjuntos não-vazios, $C = \bigsqcup\limits_{i \in I} C_i$, tal que $C_i \neq C_{i'}$ para quaisquer distinos $i, i' \in I$, $i \neq i'$. Equivalentemente, toda partição de C pode ser interpretada como uma função sobrejetiva $f : C \to I$, onde $C_i := f^{-1}i$ para todo $i \in I$.

2.1.3. Definição. Seja $\sim$ uma equivalência sobre C e seja $c \in C$. Então o subconjunto $[c] := \{x \in C \mid c \sim x\}$ é uma *classe de equivalência* de $\sim$ e $c \in [c]$ é um *representante* desta classe.

2.1.4. Lema. *Seja $\sim$ uma equivalência sobre C e sejam $K, K' \subset C$ classes de equivalência de $\sim$. Então*

1. $K \neq \varnothing$,
2. $K = [c']$ *para qualquer* $c' \in K$,
3. $K = K'$ *ou* $K \cap K' = \varnothing$.

Em outras palavras, as classes de equivalência formam uma partição de C.

Demonstração. **1.** Sendo $K = [c]$ para algum $c \in C$, temos $c \in K$ pela reflexividade de $\sim$.

2. Se $K = [c]$ e $c' \in K$, então $c \sim c'$. Mostraremos que $c \sim c'$ implica $[c] \supset [c']$. Com efeito, se $x \in [c']$, então $c' \sim x$ e, pela transitividade de $\sim$, obtemos $c \sim x$, ou seja, $x \in [c]$. Pela simetria de $\sim$, $c \sim c'$ implica $c' \sim c$. Logo, $[c] \subset [c']$.

3. Se $K \cap K' \neq \varnothing$, então existe um elemento $c' \in K \cap K'$. Pelo item 2, $K = [c'] = K'$ ■

2.1.5. Definição. Seja $\sim$ uma equivalência sobre C. A função sobrejetiva $\pi : C \to C/\sim$, $\pi : c \mapsto [c]$, relacionada com a partição de C nas classes da equivalência de $\sim$ é dita a *projeção canônica* do *quociente* $C/\sim$ de C pela equivalência $\sim$, onde o *quociente* $C/\sim$ é formado por todas as classes de equivalência, $C/\sim := \big\{[c] \mid c \in C\big\}$.

2.1.6. Resumo. Não há muita diferença entre equivalências, partições e funções sobrejetivas. É um mesmo conceito visto por diferentes ângulos.

2.1.7. Equivalência gerada por uma relação binária. Seja $E_i \subset C \times C$, $i \in I$, uma família de equivalências. É fácil ver que $\bigcap\limits_{i \in I} E_i$ é uma equivalência.

Seja $R \subset C \times C$ uma relação binária qualquer sobre C. Então $\hat{R} := \bigcap\limits_{\substack{\text{equiva-}\\\text{lência}\\E \supset R}} E$ é a menor equivalência que contém R. Tal $\hat{R}$ é dita a *equivalência gerada* por R.

Podemos descrever $\hat{R}$ explicitamente. Seja $R^{\mathrm{op}} := \big\{(c_1, c_2) \in C \times C \mid c_2 R c_1\big\}$. Então a relação $\bar{R} := \Delta_C \cup R \cup R^{\mathrm{op}}$ já é reflexiva e simétrica. Resta dizer que $c\hat{R}c'$ vale se e só se existem $n \in \mathbb{N}$ e $c_1, \dots, c_n \in C$ tais que $c = c_1$, $c_n = c'$ e valem $c_i \bar{R} c_{i+1}$ para todos $i = 1, \dots, n-1$. Deste modo, a equivalência gerada por R é simplesmente o fecho de R pelas reflexividade, simetria e transitividade.

2.2. Relações de ordem. Relações de ordem (parcial) aparecem com frequência. Um típico exemplo é a ordem dada pela inclusão de subconjuntos de um conjunto.

2.2.1. Definição. Seja $\leqslant$ uma relação binária sobre um conjunto C. Dizemos que $\leqslant$ é uma *relação de ordem parcial* (ou simplesmente *ordem*) sobre C e que C é um *conjunto* (*parcialmente*) *ordenado* se esta relação é *reflexiva, anti-simétrica* e *transitiva.* Isto quer dizer que

- $\forall c \in C\ c \leqslant c$ (*reflexividade*);
- $\forall c_1, c_2 \in C\ (c_1 \leqslant c_2 \wedge c_2 \leqslant c_1) \Rightarrow c_1 = c_2$ (*anti-simetria*);
- $\forall c_1, c_2, c_3 \in C\ (c_1 \leqslant c_2 \wedge c_2 \leqslant c_3) \Rightarrow c_1 \leqslant c_3$ (*transitividade*).

É imediato que a relação *dual* $\leqslant^{\mathrm{op}}$ também é uma ordem. Isto possibilita dualizar todos os conceitos, considerações, afirmações etc. sobre ordens, ou seja, fazer os mesmos para a ordem dual.

Há duas convenções típicas sobre relações de ordem. Convencionalmente, escreve-se às vezes $c_2 \geqslant c_1$ no lugar de $c_1 \leqslant c_2$. Além da relação $c_1 \leqslant c_2$, a gente usa a relação $c_1 < c_2$, cujo significado é $c_1 \leqslant c_2 \wedge c_1 \neq c_2$.

Seja $\leqslant$ uma ordem sobre C e seja $S \subset C$ um subconjunto. Então temos a *ordem induzida* $\leqslant|_S$ sobre S. Frequentemente, tal ordem se denota pelo mesmo símbolo $\leqslant$.

2.2.2. Definição. Para $S \subset C$ e $c \in C$, escrevemos $S \leqslant c$ e dizemos que c é uma *cota superior* de S se $\forall s \in S\ s \leqslant c$. Analogamente, definimos uma *cota inferior.* Escrever $S < c$ (analogamente, $c < S$) significa $\forall s \in S\ s < c$.

2.2.3. Definição. Um elemento $m \in C$ é *maximal* se $\forall c \in C\ m \leqslant c \Rightarrow m = c$. De modo semelhante, define-se um elemento *minimal.* Em alguns casos, quando temos $C \leqslant c$ para um óbvio elemento $c \in C$, as palavras "um elemento maximal de C" pressupõem um elemento maximal em $C \setminus c$.

2.2.4. Definição. Dizemos que uma ordem $\leqslant$ sobre C é *linear* ou que C é *linearmente ordenado* se $\forall c_1, c_2 \in C\ c_1 \leqslant c_2 \vee c_2 \leqslant c_1$. Um subconjunto $S \subset C$ é uma *cadeia* se S (com sua ordem induzida) é linearmente ordenado.

2.2.5. Definição. Dizemos que uma ordem $\leqslant$ sobre C satisfaz a *condição de cadeia descendente* ou a *condição de minimalidade* se qualquer subconjunto não-vazio S de C, $\varnothing \neq S \subset C$, possui um elemento minimal em S. Analogamente, formula-se a *condição de cadeia ascendente* ou a *condição de maximalidade.* Tais condições servem para agir (demonstrar, construir, etc.) por indução. Por exemplo, a ordem usual em $\mathbb{N}$ satisfaz a condição de minimalidade e aí baseia-se o glorioso método da indução matemática.

Uma ordem linear que satisfaz a condição de minimalidade é dita *total* e o correspondente conjunto é *totalmente ordenado.* Para um conjunto totalmente ordenado C com o elemento minimal $m \in C$, denotamos por $[m, c)_C := \{x \in C \mid m \leqslant x < c\}$ o *segmento inicial* de C limitado por $c \in C$.

2.2.6. Lema. *Seja $\leqslant$ uma ordem parcial sobre C. Então $\leqslant$ satisfaz a condição de maximalidade se e só se qualquer sequência crescente se estabiliza. Isto significa que, para qualquer família $c_i \in C$, $i \in \mathbb{N}$, com $c_i \leqslant c_{i+1}$ para todo $i \in \mathbb{N}$, existe $n \in \mathbb{N}$ tal que $c_j = c_n$ para todo $j \geqslant n$.*

Demonstração. Suponha que $\leqslant$ satisfaz a condição de maximalidade. Dada uma família $c_i \in C$, $i \in \mathbb{N}$, com $c_i \leqslant c_{i+1}$ para todo $i \in \mathbb{N}$, fazendo $S := \{c_i \mid i \in \mathbb{N}\}$, encontramos um elemento maximal $c_n \in S$. Obviamente, $c_j = c_n$ para todo $j \geqslant n$.

Reciprocamente, suponha que toda sequência crescente em C se estabiliza e seja $\varnothing \neq S \subset C$ um subconjunto não-vazio que não possui um elemento maximal. Segue de $S \neq \varnothing$ que existe $c_0 \in S$. Já que c_0 não é maximal em S, existe $c_1 \in S$ tal que $c_0 < c_1$, e assim por diante. Deste modo, construímos uma sequência crescente $c_0 < c_1 < \dots < c_i < c_{i+1} < \dots$ que não se estabiliza ∎

2.2.7. Teorema (lema de Zorn)**.** *Seja $(C, \leqslant)$ um conjunto parcialmente ordenado tal que qualquer cadeia totalmente*[4] *ordenada em C possui uma cota superior em C. Então, para todo $c_0 \in C$, existe um elemento maximal $m \in C$ com $c_0 \leqslant m$.*

Demonstração. Considerando o conjunto $\{x \in C \mid c_0 \leqslant x\}$ no lugar de C, basta supor que $c_0 \leqslant C$ e mostrar que C possui um elemento maximal. Suponha que não há tal elemento em C.

Denotamos por $\mathcal{T} \subset 2^C$ o conjunto de todas as cadeias totalmente ordenadas em C, $\mathcal{T} := \{T \in 2^C \mid T \text{ é uma cadeia totalmente ordenada}\}$. Pela hipótese do teorema, para todo $T \in \mathcal{T}$, existe um $c' \in C$ tal que $T \leqslant c'$. Mas c' não é maximal. Logo, existe $c \in C$ com $c' < c$, implicando $T < c$.

Como foi observado acima, a restrição $f : \mathcal{S} \to \mathcal{T}$ da projeção $\mathcal{T} \times C \to \mathcal{T}$ para o subconjunto $\mathcal{S} \subset \mathcal{T} \times C$ dado por $\mathcal{S} := \big\{(T, c) \in \mathcal{T} \times C \mid T < c\big\}$ é sobrejetiva. Pelo AE, existe uma função $g : \mathcal{S} \leftarrow \mathcal{T}$ com $f \circ g = 1_{\mathcal{T}}$. Compondo g com a projeção $\mathcal{T} \times C \to C$, obtemos uma função $c : \mathcal{T} \to C$ tal que $T < c(T)$ para todo $T \in \mathcal{T}$. Podemos supor que $c\varnothing = c_0$.

Seja $\mathcal{T}_0 := \big\{T \in \mathcal{T} \mid c_0 \in T \wedge \forall t \in T\ c[c_0, t)_T = t\big\}$. Então $\{c_0\} \in \mathcal{T}_0$, pois $c\varnothing = c_0$. Sejam $T, T' \in \mathcal{T}_0$. Então $[c_0, t)_T = [c_0, t')_{T'}$ implica $t = t'$ para quaisquer $t \in T$ e $t' \in T'$ pela definição de $\mathcal{T}_0$. Supondo que T e T' são distintos, $T \neq T'$, mostraremos que um dos T e T' é um segmento inicial do outro. (Em particular, $\mathcal{T}_0$ será uma cadeia relativamente à inclusão.)

Realmente, caso, por exemplo, $T \subset T'$, existe um elemento minimal $t' \in T' \setminus T$ pela condição de minimalidade para T'. Logo, $[c_0, t')_{T'} \subset T$. Se $[c_0, t')_{T'} \neq T$, existe um elemento minimal $t \in T \setminus [c_0, t')_{T'}$

[4]Na versão padrão do lema de Zorn, é exigida a existência de uma cota superior em C para qualquer cadeia em C, não necessariamente totalmente ordenada. A presente versão juntamente com sua demonstração pertencem a Misha Verbitsky.

pela condição de minimalidade para T. Então $[c_0,t')_{T'}=[c_0,t)_T$, pois $T\subset T'$; implicando $t=t'$ e uma contradição. Portanto, $T=[c_0,t')_{T'}$.

Caso $T\not\subset T'$ e $T'\not\subset T$, existem elementos minimais $t\in T\setminus T'$ e $t'\in T'\setminus T$ pela condição de minimalidade para T e T'. Logo, $[c_0,t)_T\subset T'$ e $[c_0,t')_{T'}\subset T$. Se $[c_0,t)_T=[c_0,t')_{T'}$, então $t=c[c_0,t)_T=c[c_0,t')_{T'}=t'\in T\cap T'$ pela definição de $\mathcal{T}_0$; uma contradição. Assim, pela simetria entre T e T', podemos supor que existe um elemento $t_0\in[c_0,t)_T\setminus[c_0,t')_{T'}$. Pela condição de minimalidade para T, podemos supor que t_0 é minimal com esta propriedade. Daí, $[c_0,t_0)_T\setminus[c_0,t')_{T'}=\varnothing$, ou seja, $[c_0,t')_{T'}\supset[c_0,t_0)_T$. De $t_0\notin[c_0,t')_{T'}$, $t_0\in[c_0,t)_T\subset T'$ e $t'\in T'\in\mathcal{T}$ segue $t'\leqslant t_0$. Concluímos de $[c_0,t')_{T'}\subset T$ que $[c_0,t')_{T'}\subset[c_0,t_0)_T$. Como acima, $[c_0,t')_{T'}=[c_0,t_0)_T$ implica $t'=t_0\in T$. Uma contradição.

Observemos agora que $T_0:=\bigcup\limits_{T\in\mathcal{T}_0}T\in\mathcal{T}_0$. Sendo $\mathcal{T}_0$ uma cadeia relativamente à inclusão, a ordem sobre T_0 é linear. Para mostrar a condição de minimalidade para T_0, usamos o fato dual ao Lema 2.2.6 : dada uma família $t_i\in T_0$, $i\in\mathbb{N}$, com $t_i\geqslant t_{i+1}$ para todo $i\in\mathbb{N}$, temos $t_0\in T$ para algum $T\in\mathcal{T}_0$; já que $t_i\in T'$ para algum $T'\in\mathcal{T}_0$ e um dos T e T' é um segmento inicial do outro (ou $T=T'$), concluímos que $t_i\in T$; a condição de minimalidade para T implica que a sequência em questão se estabiliza.

Resta notar que $T_0\not\subset T_0\sqcup\{cT_0\}\in\mathcal{T}_0$. Uma contradição ∎

2.2.8. Exercício (teorema de Zermelo)**.** Mostre que qualquer conjunto admite uma ordem total. (Dica: Dado um conjunto C, considere o conjunto $\mathcal{T}\subset 2^C$ de todos os subconjuntos não-vazios totalmente ordenados de C, isto é, $\mathcal{T}:=\big\{(T,\leqslant)\mid\varnothing\neq T\subset C\wedge\leqslant$ é uma ordem total sobre $T\big\}$. Introduza uma ordem em $\mathcal{T}$ escrevendo $(T_1,\leqslant)\prec(T_2,\leqslant)$ se e só se $T_1=[m,t)_{T_2}\subset T_2$ para algum $t\in T_2$ com a ordem em T_1 induzida pela ordem em T_2, onde m é o elemento minimal de T_2. Verifique a hipótese do lema de Zorn mostrando que a união de qualquer cadeia em $\mathcal{T}$ é uma cota superior desta cadeia.)

2.3. Pré-ordem. Omitindo a segunda exigência na Definição 2.2.1 de ordem, obtemos o conceito de *pré-ordem.* De fato, tal conceito é uma mistura dos conceitos de equivalência e de ordem. Com efeito, seja $\leqslant$ uma pré-ordem sobre C. É fácil verificar que a relação binária $c_1\leqslant c_2\wedge c_2\leqslant c_1$ (esta é a relação binária $\leqslant\cap\leqslant^{\mathrm{op}}$), denotada por $\sim$, é uma equivalência.

O quociente $C/\sim$ é naturalmente munido de uma ordem: $[c_1]\preccurlyeq[c_2]$ vale exatamente quando $c_1\leqslant c_2$. Tal definição está correta: se $c_1'\sim c_1$, $c_1\leqslant c_2$ e $c_2\sim c_2'$, então $c_1'\leqslant c_1$ e $c_2\leqslant c_2'$ implicam $c_1'\leqslant c_2'$. As reflexividade e transitividade de $\preccurlyeq$ se verificam no nível de representantes. Se $[c_1]\preccurlyeq[c_2]$ e $[c_2]\preccurlyeq[c_1]$, então $c_1\leqslant c_2$ e $c_2\leqslant c_1$, implicando $c_1\sim c_2$, ou seja, $[c_1]=[c_2]$.

Reciprocamente, se $f:D\to C$ é uma função sobrejetiva para um conjunto parcialmente ordenado $(C,\preccurlyeq)$, então a relação binária $d_1\leqslant d_2$, válida por definição se e só se $f(d_1)\preccurlyeq f(d_2)$, é uma pré-ordem sobre D cuja equivalência $\sim$ corresponde a f.

Grupos e suas ações