2019-12-11T14:14:41-03:00

Projeto de monitoria FMCn 2017–2019

AulaBook

http://fmc.imd.ufrn.br/

Monitores

Bianca Rodrigues Cesarino (2017–2019)
Josenaldo Júnior (2018–2019)
João Pedro de Amorim Paula (2018.2–2019)
Giordano Rodrigues (2018.2)
João Pedro Holanda (2017.2–2018.1)
Victor Rafael Santos Silva (2017.1)

Coordenador

Thanos Tsouanas (2017–2019)

Sumário

1 2017.1

11/04/2017 (Bianca)

Exercício 1.1. Seja A conjunto finito não-vazio com $A \subseteq \mathbb{R}$. Prove que A tem máximo e mínimo.

18/04/2017 (Bianca)

Exercício 1.2. Prove que para todo $n \in \mathbb{N}$

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Exercício 1.3. Encontre uma fórmula para $1 + 3 + 5 + \cdots + (2n - 1)$ para $n \leq 1$ e prove que sua fórmula é correta.

Exercício 1.4. Prove que para todo $n \in \mathbb{Z}$, tal que $n \geq 5$

$$n^2 < 2^n.$$

25/04/2017 (Bianca)

Exercício 1.5. Prove que para todo $n \in \mathbb{N}$

$$0^2 + 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Exercício 1.6. Prove que para todo $n \in \mathbb{N}$ e todo ímpar $k \in \mathbb{Z}$, k^n é ímpar.

Exercício 1.7. Usando o PBO, prove que não existe inteiro k tal que

$$0 < k < 1.$$

27/04/2017 (Bianca)

Exercício 1.8. Prove que a relação $a \mid b$ é de ordem parcial se $a, b \in \mathbb{N}$.

Exercício 1.9. Prove que $a \equiv b \pmod{m}$ é uma relação de equivalência nos inteiros.

04/05/2017 (Bianca)

Definição 1.10. Seja $x \in \mathbb{R}$. O x é *irracional* sse existem $p, q \in \mathbb{Z}$ tais que:

$$x = \frac{p}{q}.$$

Exercício 1.11. Prove que $\sqrt{2}$ é irracional.

Exercício 1.12. Que alterações devem ser feitas no 1.11 para provar que $\sqrt{3}$ é irracional?

Exercício 1.13. Mostre que existem irracionais x, y com x^y racional.

Homework 1.1. Prove que o $\sqrt[3]{2}$ é irracional.

09/05/2017 (Bianca)

Exercício 1.14. Uma sequência $a_0, a_1, a_2, \ldots$ é definida recursivamente da seguinte forma:

$$a_0 = 0$$
$$\text{para todo } n \in \mathbb{N}, \quad a_{n+1} = 2a_n + n$$

Prove que para todo $n \in \mathbb{N}$, $a_n = 2^n - n - 1$.

Exercício 1.15. Para todos os naturais n e m, se $m > 0$, então existem naturais q e r tais que $n = mq + r$ e $r < m$.

Exercício 1.16. Todo inteiro $n > 1$ é primo ou um produto de primos.

16/05/2017 (Bianca)

Exercício 1.17. Sejam $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Então:

(i) $a + c \equiv b + d \pmod{m}$

(ii) $ac \equiv bd \pmod{m}$

(iii) $a - c \equiv b - d \pmod{m}$

Exercício 1.18. Sejam $a \equiv b \pmod{m}$. Prove que $ac \equiv bc \pmod{m}$ para qualquer $c \in \mathbb{Z}$.

Exercício 1.19. Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$ para qualquer inteiro positivo n.

18/05/2017 (Bianca)

Definição 1.20 (Divisão de Euclides)**.** Dados inteiros a e b com $b > 0$, existem inteiros q e r tais que

$$a = bq + r, \qquad 0 \leq r < b.$$

Além disso, os q e r são determinados unicamente.

Exercício 1.21. Prove a unicidade dos q e r.

Exercício 1.22. Se $a, b \in \mathbb{Z}$ com $b > 0$, então $(a, b) = (b, r)$, onde r é o resto da divisão de a por b.

Definição 1.23 (Algoritmo de Euclides)**.** Sejam a, b inteiros positivos. Para encontrar o (a, b), aplicamos a *Divisão de Euclides* (1.20) repetidamente até chegar em resto 0. O (a, b) será igual ao último resto diferente de 0 que foi obtido.

– Por que o *Algoritmo de Euclides* sempre termina?

Exercício 1.24. Usando o *Algoritmo de Euclides* (1.23), encontre o $(101, 73)$.

Definição 1.25 (Algoritmo Estendido de Euclides)**.** O máximo divisor comum (a, b) de dois inteiros a e b pode ser escrito como uma combinação linear de a e b. Usamos o *Algoritmo Estendido de Euclides* para encontrar os inteiros $s, t \in \mathbb{Z}$ que satisfazem a

$$(a, b) = as + bt.$$

Exercício 1.26. Continuando o 1.24, encontre $t, s \in \mathbb{Z}$ tais que

$$(101, 73) = 101t + 73s.$$

Homework 1.2. Prove a corretude do *Algoritmo de Euclides* (1.23).

25/05/2017 (Bianca)

Definição 1.27 (Inverso módulo m)**.** Sejam $a, a', m \in \mathbb{Z}$. Chamamos a' o inverso (multiplicativo) de a módulo m sse

$$aa' \equiv 1 \pmod{m}.$$

– O inverso é único;

– O a tem inverso módulo m sse $(a, b) = 1$.

Exercício 1.28. Prove a unicidade do inverso módulo m.

Exercício 1.29. Usando o Teorema Chinês do Resto, ache todos os inteiros $x \in \mathbb{Z}$ que satisfazem o sistema de congruências:

$$\begin{cases} x \equiv 2 \pmod 9 \\ x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 4 \end{cases}$$

Exercício 1.30. Ache todos os inteiros $x \in \mathbb{Z}$ com $|x| < 64$ que satisfazem o sistema de congruências:

$$\begin{cases} x \equiv 1 \pmod 3 \\ 3x \equiv 1 \pmod 4 \\ 4x \equiv 2 \pmod 5 \end{cases}$$

Homework 1.3. Use o Teorema Chinês do Resto para resolver os sistemas de congruências:

(a) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$ (b) $\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 9 \\ x \equiv 5 \pmod{13} \end{cases}$ (c) $\begin{cases} x \equiv 3 \pmod 4 \\ 5x \equiv 1 \pmod 7 \\ x \equiv 2 \pmod 9 \end{cases}$

Homework 1.4. Encontre o menor inteiro positivo que deixa os restos 8, 7 e 11 quando dividido por 7, 11 e 15, respectivamente.

30/05/2017 (Bianca)

Lema 1.31 (Lema de Euclides)**.** *Sejam m, n inteiros e p um primo. Se $p \mid ab$, então $p \mid m$ ou $p \mid n$.*

30/05/2017 (Victor)

Nos exercícios abaixo G é grupo, H e K são subgrupos de G e p é primo.

Exercício 1.32. A ordem de $H \cap K$ é um divisor comum da ordem de H e da ordem de K.

Exercício 1.33. A ordem de $H \cap K$ é um divisor comum da ordem de H e da ordem de K. Se ordem de $H = m$, ordem de $K = n$ e $(m, n) = 1$, mostrar que $H \cap K = \{e\}$.

Exercício 1.34. A ordem de $H \cap K$ é um divisor comum da ordem de H e da ordem de K. Se G possui um elemento de ordem p e um elemento de ordem q, onde p e q são primos distintos, mostrar que a ordem de G é múltiplo de pq.

Exercício 1.35. A ordem de $H \cap K$ é um divisor comum da ordem de H e da ordem de K. Se a ordem de G é n, mostrar que $x^n = e$ para todo x em G.

Exercício 1.36. A ordem de $H \cap K$ é um divisor comum da ordem de H e da ordem de K. $H \neq K$ e H e K possuem mesma ordem p, mostrar que que $H \cap K = \{e\}$.

01/06/2017 (Bianca)

Exercício 1.37. Se $a < 0$ e $a \mid b$, então $(a, b) = a$.

Exercício 1.38. Se $ab \equiv 0 \pmod{p}$, onde p é um primo, então $a \equiv 0 \pmod{p}$ ou $b \equiv 0 \pmod{p}$.

Exercício 1.39. $ax + by = c$ tem soluções sse $(a, b) \mid c$.

Definição 1.40 (Teorema de Fermat)**.** Seja p um primo. Então

$$a^{p-1} \equiv 1 \pmod{p}$$

para todo $a \not\equiv 0 \pmod{p}$.

Definição 1.41. $\varphi(n)$ é o número de inteiros positivos menores do que n que são coprimos com n.

Definição 1.42 (Teorema de Euler)**.** Se a e n são coprimos

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Exercício 1.43. Se p é primo, encontre $\varphi(p)$. Use isso para deduzir o *Teorema de Fermat* (1.40) a partir do *Teorema de Euler* (1.42).

Homework 1.5. Prove que $(a, 0) = a$, se $a > 0$.

Homework 1.6. Se $(a, c) = 1$ e $c \mid ab$, então $c \mid b$.

06/06/2017 (Bianca)

Exercício 1.44. No "meio" de uma "cidade infinita", tem um motorista no seu carro. Ele está parado numa interseção onde há 3 opções: virar à esquerda; dirigir reto; virar à direita. Em seu tanque tem a unidades de combustível, e sempre gasta 1 para dirigir até a próxima interseção. De quantas maneiras diferentes ele pode dirigir até seu combustível acabar?

Exercício 1.45. Aleco e Bego são dois sapos. Eles estão na frente de uma escada com 11 degraus. No 6º degrau, tem Cátia, uma cobra, com fome. Aleco pula 1 ou 2 degraus para cima. Bego, 1, 2 ou 3. E ele é tóxico: se Cátia o comer, ela morre na hora.

(1) Por enquanto, Cátia está dormindo profundamente.
   (a) De quantas maneiras Aleco pode subir a escada toda?
   (b) De quantas maneiras Bego pode subir a escada toda?

(2) Cátia acordou!
   (a) De quantas maneiras Aleco pode subir a escada toda?
   (b) De quantas maneiras Bego pode subir a escada toda?

(3) Bego começou a subir a escada... Qual é a probabilidade que Cátia morra? (Considere que antes de começar, ele já decidiu seus saltos e não tem percebido a existência da cobra.)

Exercício 1.46. Prove que para todos os inteiros positivos n e r temos

$$C(n, r) = C(n - 1, r) + C(n - 1, r - 1).$$

Homework 1.7. Prove que

$$P(n, n) = P(n, n - 1)$$

para todos os inteiros positivos n.

Homework 1.8. Prove que

$$P(n,1) + P(m,1) = P(n+m,1)$$

para todos os inteiros positivos m e n.

06/06/2017 (Victor)

Nos exercícios abaixo, G e H sempre serão grupos.

Exercício 1.47. Seja $f : G \to H$ um homomorfismo, J um subgrupo de H e defina B como sendo a imagem inversa de J por f. Prove que B é subgrupo de G e também que $\ker f$ é subconjunto de B.

Exercício 1.48. Seja $f : G \to H$ homomorfismo e m um inteiro relativamente primo com a ordem de H. Mostre que se x^m é elemento de $\ker f$ então x é elemento de $\ker f$.

Exercício 1.49. Seja $f : G \to H$ homomorfismo sobrejetor. Prove que se todo elemento de G possui ordem finita, então todo elemento de H possui ordem finita.

Exercício 1.50. Seja A um anel. Prove que se o grupo aditivo de A é cíclico, então A é um anel comutativo.

08/06/2017 (Bianca)

Exercício 1.51. Se G tem ordem n, então $x^n = e$ para todo x em G.

Exercício 1.52. Seja G de ordem pq, onde p e q são primos. Ou G é cíclico, ou todo elemento $x \neq e$ em G tem ordem p ou q.

Exercício 1.53. Se $f : G \to H$ é um homomorfismo com kernel K, então f é injetiva sse $K = \{e\}$.

13/06/2017 (Bianca)

Exercício 1.54. Dado um conjunto a, mostre que o conjunto de todos os singletons de elementos de a é um conjunto.

Exercício 1.55. Traduza as frases seguintes para a FOL da teoria de conjuntos.

(1) Existe conjunto com pelo menos dois membros.

(2) Os x e y têm exatamente um membro em comum.

(3) Todos os conjuntos têm o x como membro.

(4) Existe conjunto que pertence nele mesmo.

(5) O y consiste em todos os subconjuntos de x com exatamente 2 elementos.

(6) Existe conjunto com exatamente dois membros.

(7) Para todos os conjuntos a e b, sua interseção é conjunto.

(8) A união de a e b é um conjunto.

(9) O x não pertence em nenhum conjunto.

(10) Existem conjuntos tais que cada um pertence ao outro.

(11) Existe conjunto que não é igual a ele mesmo.

20/06/2017 (Bianca)

Definição 1.56 (Isomorfismo de ordem)**.** Dizemos que P e Q são isomorfos de ordem se existe um mapeamento bijetivo φ de P para Q tal que $x \leq y$ em P se e somente se $\varphi(x) \leq \varphi(y)$ em Q.

Definição 1.57 (A relação de cobertura)**.** Seja P um poset e sejam $x, y \in P$. Dizemos que x é coberto por y, e escrevemos $x \prec y$, se $x < y$ e $x \leq z < y$ implica $z = x$.

Exercício 1.58. Sejam P e Q posets finitos e seja $\varphi : P \to Q$ um mapeamento bijetivo. Então, os seguintes são equivalentes:

(i) φ é um isomorfismo de ordem;

(ii) $x < y$ em P se e somente se $\varphi(x) < \varphi(y)$ em Q;

(iii) $x \prec y$ em P se e somente se $\varphi(x) \prec \varphi(y)$.

Exercício 1.59. Dois posets finitos P e Q são isomorfos de ordem se e somente se podem ser desenhados com diagramas idênticos.

Exercício 1.60. Existe uma lista de 16 diagramas de posets de quatro elementos, tal que todo poset de quatro elementos pode ser representado por um dos diagramas nessa lista. Encontre essa lista.

22/06/2017 (Bianca)

Exercício 1.61. Prove que $\langle \mathbb{N} \,;\, | \rangle$ é um poset.

- Ele é linear?
- Ache o máximo e o mínimo (se tiver).

Exercício 1.62. Seja $D_{12} = \{d \in \mathbb{N} \mid d \mid 12\}$. Desenhe o diagrama Hasse do poset $\langle D_{12} \,;\, | \rangle$.

2 2017.2

08/08/2017 (Jp)

Exercício 2.1. Defina o conjunto dos números naturais usando BNF.

Exercício 2.2. Defina a operação de adição sobre os números naturais como definidos acima.

Exercício 2.3. Demonstre que a adição definida no exercício anterior é associativa. Isso é, mostre que para todo m, n, p naturais, $m+(n+p) = (m+n)+p$.

Definição 2.4 (Lema 1 da adição)**.** Para todo n natural, $n + 0 = n$.

Definição 2.5 (Lema 2 da adição)**.** Para todo m, n naturais, $S(m + n) = m + Sn$.

Homework 2.1. Demonstre 2.4 (p. 9) e 2.5 (p. 9).

Exercício 2.6. Demonstre que a adição é comutativa (ou seja, que para todo m, n naturais, $m + n = n + m$). Use coisas que demonstramos anteriormente.

10/08/2017 (Bianca)

Exercício 2.7. Prove que para todo inteiro positivo n, uma grid de 2^n x 2^n com qualquer um dos quadrados removidos pode ser coberto por peças em forma de L.

Exercício 2.8. Use indução para mostrar que para todo $n \geq 1$

$$n! \geq 2^{n-1}$$

Exercício 2.9. A sequência Fibonacci é a sequência de inteiros $F_1, F_2, F_3, \ldots$ definida como segue

$$\begin{cases} F_1 = 1; \\ F_2 = 1; \\ F_{n+2} = F_{n+1} + F_n \end{cases}$$

para todos os inteiros positivos n. Use indução para provar que para todo $n > 0$,

$$F_{n+1}F_{n+2} - F_nF_{n+3} = (-1)^n$$

15/08/2017 (Jp)

Exercício 2.10. Temos uma malha de pontos m por n. Chamamos o ponto superior direito de $S = (0, 0)$ e o inferior direito de $D = (m - 1, n - 1)$. De quantas maneiras conseguimos caminhar de S a D, usando somente movimentos para baixo e para a direita?

Exercício 2.11. Demonstre que, para todo conjunto A finito, $|\wp A| = 2^{|A|}$.

Exercício 2.12. Demonstre que, para todo n,

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

.

Exercício 2.13. Formule um argumento informal para a asserção do exercício 2.12, considerando o resultado do exercício 2.11.

17/08/2017 (Bianca)

Exercício 2.14. Suponha que A, B e C são conjuntos. Então $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Exercício 2.15. Suponha que A, B e C são conjuntos. Prove que se $A \subseteq C$ e $B \subseteq C$, então $A \cup B \subseteq C$.

Exercício 2.16. Suponha A, B e C conjuntos, $A \setminus B \subseteq C$ e x arbitrário. Prove que se $x \in A \setminus C$, então $x \in B$.

Exercício 2.17. Suponha A, B e C conjuntos. Prove que $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

17/08/2017 (Jp)

Exercício 2.18. Determine quais dos seguintes conjuntos são definidos intensionalmente vs extensionalmente.
(a) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
(b) $\{x \in \mathbb{Z} \mid x \text{ é par}\}$
(c) $\{x \text{ par} \mid x = p + q, \text{ onde } p, q \text{ são primos}\}$

Exercício 2.19. Demonstre que, dados $A, B, C \subseteq U$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

21/08/2017 (Jp)

Exercício 2.20. Faça um esboço de prova e em seguida escreva uma demonstração em linguagem natural para os seguintes teoremas:

1. Sejam A, B e U conjuntos tais que $A, B \subset U$. Mostre que $A \subset B$ se e somente se $(U - A) \cup B = U$.
2. Para todo a, b e n naturais, $a - b \mid a^n - b^n$

23/08/2017 (Jp)

Exercício 2.21. Prove que, para quaisquer conjuntos A, B, $(A \cup B) - B \subset A$. Mostre que a recíproca não vale.

Exercício 2.22. Prove que, se p^2 é par, então p é par. Dica: use a forma contrapositiva.

Exercício 2.23. Prove que $\sqrt{2}$ é irracional. Você pode usar o resultado do exercício 2.22 acima. Dica: tente provar por absurdo.

Exercício 2.24. Prove que, para todo n natural, $n^3 - n$ é múltiplo de 3. Faça uma prova por indução, e outra utilizando propriedades da aritmética modular. Compare os dois métodos, para este caso.

24/08/2017 (Bianca)

Exercício 2.25. Algumas definições de funções recursivas são:

$$x + 0 = x \quad \text{(a1)} \qquad x^0 = S0 \quad \text{(e1)}$$
$$x + Sy = S(x + y) \quad \text{(a2)} \qquad x^{Sy} = x^y \cdot x \quad \text{(e2)}$$

$$x \cdot 0 = 0 \quad \text{(m1)} \qquad x \Uparrow 0 = S0 \quad \text{(t1)}$$
$$x \cdot Sy = (x \cdot y) + x \quad \text{(m2)} \qquad x \Uparrow Sy = x^{x \Uparrow y} \quad \text{(t2)}$$

(a) Calcule o valor $2 \Uparrow 4$.

(b) Dados os lemas:

$$a + b = b + a \quad \text{(a-com)}$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \text{(m-ass)}$$

prove por indução as seguintes propriedades, indicando para cada passo o que foi usado:

(i) $a \cdot S0 = a$ (ii) $a^{x+y} = a^x \cdot a^y$ (iii) $a^{x \cdot y} = (a^x)^y$.

28/08/2017 (Jp)

Exercício 2.26. Defina o conjunto $\mathcal{L}_A$ das listas de elementos de um tipo A usando BNF.

Exercício 2.27. Defina a operação $\mathit{append} : \mathcal{L}_A \times \mathcal{L}_A \to \mathcal{L}_A$ de concatenação de duas listas.

Exercício 2.28. Demonstre que a *append* definida no exercício anterior é associativa.

Homework 2.2. Defina a operação $\mathit{reverse} : \mathcal{L}_A \to \mathcal{L}_A$, que faz a inversão de uma lista. Prove que *reverse* é involutiva, ou seja, que $\mathit{reverse} \circ \mathit{reverse} = \mathit{id}$.

29/08/2017 (Bianca)

Exercício 2.29. Para toda função $f : X \to Y$ e todos os $A, B \subseteq X$,

$$f[A \cup B] = f[A] \cup f[B].$$

Exercício 2.30. Para toda função injetiva $f : X \rightarrowtail Y$ e todos os $A, B \subseteq X$,

$$f[A \cap B] = f[A] \cap f[B].$$

Mostre também que essa identidade não funciona sempre se f não é injetiva.

Exercício 2.31. Cada uma das funções seguintes é uma função $f : \mathbb{R} \to \mathbb{R}$. Determine

(a) se f é injetiva ou não.

(b) se f é sobrejetiva ou não.

Prove sua resposta.

(i) $f(x) = 2x$

(ii) $f(x) = |x|$

30/08/2017 (Jp)

Exercício 2.32. Mostre que, se $f : A \to B$ e $g : B \to C$ possuem inversa, então $g \circ f : A \to C$ também possui inversa.

Exercício 2.33. Sejam $f : A \to B$ e $g : B \to A$ tais que $g \circ f = id_A$. Prove que:

a) g é sobrejetora;

b) f é injetora.

31/08/2017 (Bianca)

Exercício 2.34. Prove que composição de injeções é uma injeção, a composição de sobrejeções é uma sobrejeção, e consequentemente a composição de bijeções é uma bijeção.

04/09/2017 (Jp)

Definição 2.35 (Lema 1)**.** Para todo m e n inteiros não-nulos, se $m > 0$ e $n > 0$, então $m \cdot n > 0$.

Definição 2.36 (Lema 2)**.** Para todo m e n inteiros não-nulos, se $m > 0$ e $m \cdot n > 0$, então $n > 0$.

Exercício 2.37. Seja R uma relação binária nos inteiros não-nulos dada por $R(u, v)$ sse $u \cdot v > 0$. Mostre que R é uma relação de equivalência (ou seja, que é reflexiva, simétrica e transitiva). (Você pode usar os lemas acima).

Homework 2.3. Dada a definição $a > b$ sse existe k positivo tal que $a = b+k$, prove os lemas 2.35 e 2.36

05/09/2017 (Bianca)

Exercício 2.38. Prove que a relação $|$ é uma ordem parcial no $\mathbb{N}$.

Exercício 2.39. Prove que $\bullet \equiv \bullet \pmod{m}$ é uma relação de equivalência nos inteiros.

06/09/2017 (Jp)

Exercício 2.40. Mostre que para todo $n \geq 12$, n pode ser escrito como uma combinação de 4 e 5 (ou seja, $n = 4 \cdot a + 5 \cdot b$, onde a, b são naturais)

Exercício 2.41. Seja R_ϵ a relação dada por $R(x, y)$ sse $|x - y| < \epsilon$, onde $\epsilon \in (0, 1]$. R_ϵ é uma relação de equivalência? Prove ou refute.

11/09/2017 (Jp)

Exercício 2.42. Dadas as relações

$$f \overset{\forall\exists}{=} g \overset{\text{def}}{\iff} (\forall n \in \mathbb{N})(\exists x \geq n)[f(x) = g(x)]$$
$$f \overset{\exists\forall}{=} g \overset{\text{def}}{\iff} (\exists n \in \mathbb{N})(\forall x \geq n)[f(x) = g(x)]$$

Prove ou refute, para cada uma, se é uma relação de equivalência.

Exercício 2.43. Dado um conjunto A com n elementos, determine o número de funções idempotentes sobre A.

12/09/2017 (Bianca)

Exercício 2.44. Proposição: Seja $X \neq \emptyset$ e $\sim$ uma relação no X. Se $\sim$ é simétrica e transitiva, então ela é reflexiva.

Prova: Como ela é simétrica, de $x \sim y$, concluímos que $y \sim x$ também. Usando a transitivdade, de $x \sim y$ e $y \sim x$, concluímos a $x \sim y$, que mostra que $\sim$ é reflexiva também.

Ache o erro na prova acima e prove que a proposição é falsa.

Exercício 2.45. Seja R uma relação binária num conjunto A. O.s.s.e.:

(i) R é uma relação de equivalência;

(ii) R é reflexiva e circular;

(iii) R é reflexiva e right-euclidean.

Exercício 2.46. Sejam $\sim$ uma relação de equivalência num conjunto X, e $x, y \in X$. O.s.s.e.:

(i) $x \sim y$

(ii) $[x] = [y]$

(iii) $[x] \cap [y] \neq \emptyset$

13/09/2017 (Jp)

Exercício 2.47. Para cada relação binária abaixo, mostre que é uma relação de equivalência e descreva alguns dos elementos de sua partição correspondente.

- $\approx$ sobre $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ tal que $\langle a, b\rangle \approx \langle c, d\rangle$ sse $a\,d = b\,c$
- $\sim$ sobre $\mathbb{Q}$ tal que $r \sim s$ sse $r - s \in \mathbb{Z}$
- $\sim$ sobre $\mathbb{R}$ tal que $x \sim y$ sse $x - y \in \mathbb{Q}$

14/09/2017 (Bianca)

Exercício 2.48. Seja $\mathcal{P}$ o conjunto de todas as pessoas. Considere as relações no $\mathcal{P}$ definidas pelas:

$$\text{Parent}(x, y) \overset{\text{def}}{\iff} x \text{ é a mãe ou pai de } y$$

$$\text{Child}(x, y) \overset{\text{def}}{\iff} x \text{ é filho ou filha de } y.$$

Prove ou refute: $\text{Child} \circ \text{Parent} \overset{?}{=} \text{Parent} \circ \text{Child}$.

Exercício 2.49. Suponha as propriedades de adição para os números naturais, mas que multiplição não é conhecida. Então, o seguinte pode ser usado como uma definição recursiva de multiplicação:

$$1 \cdot b = b \quad \text{(i)}$$

$$(a+1) \cdot b = a \cdot b + b \quad \text{(ii)}$$

Prove o seguinte:

(a) $a \cdot (b+c) = a \cdot b + a \cdot c$

(b) $a \cdot 1 = a$

(c) $a \cdot b = b \cdot a$

18/09/2017 (Jp)

Exercício 2.50. Para cada operação binária sobre $\mathbb{R}$ abaixo, determine se: é comutativa; é associativa; tem identidade; tem inversa.

- $x \star y = x + 2y + 4$
- $x \star y = x + 2y - xy$
- $x \star y = |x + y|$
- $x \star y = |x - y|$
- $x \star y = xy + 1$
- $x \star y = maxx, y$
- $x \star y = \frac{xy}{x+y+1}$ (sobre o conjunto dos reais positivos)

19/09/2017 (Bianca)

Exercício 2.51. Se uma nova adição para números reais, denotada pelo símbolo temporário $\boxplus$, é definida por

$$\alpha \boxplus \beta = 2\alpha + 2\beta,$$

ela é comutativa? É associativa?

Exercício 2.52. Se uma nova adição para números reais, denotada pelo símbolo temporário $\boxplus$, é definida por

$$\alpha \boxplus \beta = 2\alpha + \beta,$$

ela é comutativa? É associativa?

Exercício 2.53. Se uma operação para inteiros positivos, denotada pelo símbolo temporário $*$, é definida por

$$\alpha * \beta = \alpha^{\beta},$$

ela é comutativa? É associativa?

Exercício 2.54. Se uma operação para pares ordenados de números reais, denotada pelo símbolo temporário $\boxdot$, é definida por

$$(\alpha, \beta) \boxdot (\gamma, \delta) = (\alpha\gamma - \beta\delta, \alpha\delta + \beta\gamma),$$

ela é comutativa? É associativa?

Exercício 2.55. Se uma operação para pares ordenados de números reais, denotada mais uma vez pelo $\boxdot$, é definida por

$$(\alpha, \beta) \boxdot (\gamma, \delta) = (\alpha\gamma, \alpha\delta + \beta),$$

ela é comutativa? É associativa?

20/09/2017 (Jp)

Definição 2.56. Denotamos por S_n o conjunto das permutações em n elementos, ou, equivalentemente, o conjunto das funções bijetoras sobre $\{0, 1, \ldots, n\}$. Usaremos a notação $\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$ para nos referirmos à permutação $\sigma \in S_n$.

Definição 2.57. Definimos as permutações $\phi, \psi \in S_3$, onde

$$\phi := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$\psi := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Exercício 2.58. Calcule $\psi \circ \psi^2$ e justifique que é igual à $\psi^2 \circ \psi$.

Exercício 2.59. Calcule $\phi \circ \psi^2$ e a $\psi^2 \circ \phi$.

Exercício 2.60. Prove ou refute a validade das seguintes propriedades para a operação $\circ$ sobre S_3

- Associatividade
- Comutatividade
- Tem identidade
- Tem inversa

Exercício 2.61. Calcule as inversas de cada um dos elementos de S_3.

21/09/2017 (Bianca)

Exercício 2.62. Considere a função recursiva $\alpha : \mathbb{N}^2 \to \mathbb{N}$ definida pelas equações:

$$\alpha(0, x) = x + 1 \qquad \text{(K1)}$$
$$\alpha(n + 1, 0) = \alpha(n, 1) \qquad \text{(K2)}$$
$$\alpha(n + 1, x + 1) = \alpha(n, \alpha(n + 1, x)) \qquad \text{(K3)}$$

(i) Seguindo as definições recursivas, calcule os valores $\alpha(1, 1)$ e $\alpha(2, 1)$.

(ii) Prove que para todo $x \in \mathbb{N}$, $\alpha(1, x) = x + 2$.

(iii) Prove que para todo $x \in \mathbb{N}$, $\alpha(2, x) = 2x + 3$.

25/09/2017 (Jp)

Exercício 2.63. Seja $\langle G, \cdot, e, ^{-1} \rangle$ um grupo, e sejam $x, a, b \in G$. Demonstre cada uma das asserções abaixo:

1. $\left(b\, a\, b^{-1}\right)^n = b\, a^n\, b^{-1}$
2. Se $a\, b = b\, a$, então $(a\, b)^n = a^n\, b^n$
3. Se $x\, a\, x = e$, então $(x\, a)^{2n} = a^n$
4. Se $a^3 = e$ então a tem raíz quadrada (existe um y tal que $y^2 = a$)

5. Se $a^2 = e$ então a tem raíz cúbica
6. Se a^{-1} tem raíz cúbica, então a também tem
7. Se $x^2\, a\, x = a^{-1}$, então a tem raíz cúbica
8. Se $x\, a\, x = b$, então $a\, b$ tem raíz quadrada

26/09/2017 (Bianca)

Exercício 2.64. Prove que $(a^2)^{-1} = (a^{-1})^2$. Generalize para n natural $(a^n)^{-1} = (a^{-1})^n$.

Exercício 2.65. Sejam G um grupo e a, b, c elementos de G e e o elemento neutro de G. Prove que se $ab = e$, então $ba = e$.

Exercício 2.66. Sejam G um grupo e a, b, c elementos de G e e o elemento neutro de G. Prove que se $abc = e$, então $cab = e$ e $bca = e$.

Exercício 2.67. Prove que se $xay = a^{-1}$, então $yax = a^{-1}$.

Exercício 2.68. Sejam a, b, c iguais aos seus próprios inversos. Prove que se $ab = c$, então $bc = a$ e $ca = b$.

27/09/2017 (Jp)

Definição 2.69. Seja $\langle G, *, e, {}^{-1} \rangle$ um grupo, e H é um subconjunto de G que possui as seguintes propriedades:

- H é fechado sobre $*$
- H é fechado sobre ${}^{-1}$

Dizemos que H é um *subgrupo* de G.

Exercício 2.70. Para cada item, mostre que H é um subgrupo de G.

- $G = \langle \mathbb{R}, + \rangle$, $H = \{\log a \mid a \in \mathbb{Q}, a > 0\}$
- $G = \langle \mathbb{R}^*, \cdot \rangle$, $H = \{2^n\, 3^m \mid n, m \in \mathbb{Z}\}$

Exercício 2.71. Denotamos por *centro* do grupo $\langle G, * \rangle$ o conjunto dos elementos de G que comutam com todos os elementos de G. Ou seja,

$$C = \{a \in G \mid \text{para todo } x \in G,\ a\,x = x\,a\}$$

Mostre que C é subgrupo de G.

Exercício 2.72. Seja $\langle G, * \rangle$ um grupo, e H, K subconjuntos de G. Mostre que, se H e K são subgrupos de G, então $H \cap K$ também é subgrupo de G.

Exercício 2.73. Calcule a tabela de Cayley para o grupo $G = \{e, a, b, b^2, b^3, a\,b, a\,b^2, a\,b^3\}$ onde

$$a^2 = e \quad b^4 = e \quad b\,a = a\,b^3$$

Exercício 2.74. Monte o diagrama de Cayley para o grupo G do exercício 2.73.

28/09/2017 (Bianca)

Exercício 2.75. Sejam G grupo e $a \in G$, e suponha $o(a) = n \in \mathbb{N}$. Existem exatamente n potências diferentes de a.

Sejam a, b elementos de um grupo G. Prove o seguinte:

Exercício 2.76. $o(a) = 1$ sse $a = e$.

Exercício 2.77. Se $o(a) = n$, então $a^{n-r} = (a^r)^{-1}$.

Exercício 2.78. $o(a) = o(bab^{-1})$.

Exercício 2.79. A ordem de ab é a mesma que a ordem de ba.

02/10/2017 (Jp)

Exercício 2.80. Recorde a definição para a^n:

$$a^0 = e$$
$$a^{n+1} = a \cdot a^n$$

Abaixo temos uma definição alternativa, executando o passo recursivo à esquerda:

$$a^0 = e$$
$$a^{n+1} = a^n \cdot a$$

Mostre que essa nova definição é equivalente à usual.

Exercício 2.81. Prove que, se a é o único elemento de G com ordem k, então a está no centro de G. (Recorde a definição de centro dada no exercício 2.71)

04/10/2017 (Jp)

Seja G um grupo, a um elemento de G.

Definição 2.82 (Teorema)**.** Para todo $n, m \in \mathbb{Z}$, $a^m = a^n$ se e somente se $m \equiv n \pmod{o(a)}$.

Exercício 2.83. Prove o teorema 2.82.

Para os exercícios abaixo, assuma que as variáveis não-introduzidas são inteiros quaisquer.

Exercício 2.84. Prove que $o(a^k) \mid o(a)$.

Exercício 2.85. Seja p um primo. Prove que se $a \neq e$ e $a^p = e$, então $o(a) = p$.

Exercício 2.86. Seja n um número ímpar. Prove que se $o(a) = n$, então $o(a^2) = n$.

Exercício 2.87. Prove que se $o(a) = km$, então $o(a^k) = m$.

Exercício 2.88. Prove que se $o(a) = km$ e $a^{rk} = e$, então $m \mid r$.

Exercício 2.89. Prove que se $m \nmid o(a)$, então $m \nmid o(a^k)$.

05/10/2017 (Bianca)

Exercício 2.90. Seja G grupo e $H \leq G$. Defina:

$$a \sim b \overset{\text{def}}{\iff} ab^{-1} \in H.$$

(a) Prove que $\sim$ é uma relação de equivalência.

(b) Prove que para todos os $a, b \in G$:

(i) se $a \in H$ e $b \in H$, então $a \sim b$.

(ii) se $a \in H$ e $b \notin H$, então $a \not\sim b$.

Exercício 2.91. Se G é um grupo de ordem n. Prove que G é cíclico sse G tem um elemento de ordem n.

Exercício 2.92. Prove que todo grupo cíclico é abeliano.

Exercício 2.93. Se $G = <a>$ e $b \in G$, a ordem de b é um fator da ordem de a.

09/10/2017 (Bianca)

Exercício 2.94. Seja G grupo e $\emptyset \neq H \subseteq G$. Prove que

$$H \leq G \iff (\forall a, b \in H)[ab^{-1} \in H].$$

Exercício 2.95. Mostre que $\leq$ é uma relação de ordem:

(i) $G \leq G$.

(ii) $K \leq H \ \& \ H \leq K \implies K \leq G$.

(iii) $H \leq G \ \& \ G \leq H \implies H = G$.

Exercício 2.96. Prove que a ordem de a^{-1} é a mesma que a ordem de a.

Exercício 2.97. Sejam G grupo, $a \in G$ e $m \in \mathbb{Z}$. Prove que

$$a^m = e \iff o(a) \mid m.$$

Exercício 2.98. Se $a^p = e$ onde p é um número primo, então a tem ordem p $(a \neq e)$.

Exercício 2.99. A ordem de a^k é um divisor (fator) da ordem de a.

09/10/2017 (Jp)

Exercício 2.100. Seja $\mathcal{H}$ uma família de subgrupos de G. Mostre que sua interseção $\bigcap \mathcal{H}$ é um subgrupo de G.

Exercício 2.101. Prove que G é abeliano se e somente se, para todo a e b em G, $(a\,b)^{-1} = a^{-1}\,b^{-1}$.

Exercício 2.102. Enumere todos os subgrupos cíclicos de $\langle \mathbb{Z}_1 0, + \rangle$

Exercício 2.103. Mostre que $\mathbb{Z}_1 0$ é gerado por 2 e 5.

Exercício 2.104. Suponha que um grupo G é gerado por dois elementos a e b. Prove que se $a\,b = b\,a$ então G é abeliano.

11/10/2017 (Jp)

Exercício 2.105. Seja G um grupo e a, b elementos de G tal que $b = a^k$ para algum $k \in \mathbb{Z}$. Prove as seguintes afirmações:

- $\langle b \rangle \subseteq \langle a \rangle$
- $o(b) \mid o(a)$
- $\langle a \rangle = \langle b \rangle$ se e somente se $a \in \langle b \rangle$
- $\langle a \rangle = \langle b \rangle$ se e somente se $o(a) = o(b)$
- $\langle a \rangle = \langle b \rangle$ se e somente se k e $o(a)$ são coprimos.

16/10/2017 (Jp)

Exercício 2.106. Para cada um dos itens abaixo, enumere as coclasses de H.

- $H \leq S_3$, $H = \{id, \varphi\}$
- $H \leq S_3$, $H = \left\{id, \psi, \psi^2\right\}$
- $H \leq \mathbb{Z}_{15}$, $H = \langle 5 \rangle$
- $H \leq \mathbb{Z}$, $H = \langle 3 \rangle$
- $H \leq \mathbb{R}$, $H = \mathbb{Z}$
- $H \leq \mathbb{R}^*$, $H = \{2^n \mid n \in \mathbb{Z}\}$
- $H \leq \mathbb{R}^*$, $H = \left\langle \frac{1}{2} \right\rangle$

17/10/2017 (Bianca)

Exercício 2.107. Prove que se $a \in Hb$, então $Ha = Hb$.

Exercício 2.108. Prove que $Ha = H$ sse $a \in H$.

Exercício 2.109. Seja G grupo finito. Se G tem ordem n, então $x^n = e$ para todo $x \in G$.

Exercício 2.110. Prove que $\sqrt{2}$ é irracional.

Exercício 2.111. Prove que:

(i) $a \mid b \;\&\; a \mid c \implies a \mid b + c$

(ii) $a \mid b \implies a \mid -b$

(iii) $a \mid b \;\&\; b \mid c \implies a \mid c$.

18/10/2017 (Jp)

Exercício 2.112. Suponha que G tem ordem pq, onde p e q são primos. Mostre que G é cíclico ou todo elemento de G tem ordem p ou q.

Exercício 2.113. Seja G um grupo de ordem 4. Mostre que G é cíclico ou todo elemento de G é o próprio inverso. Conclua que G é abeliano.

Exercício 2.114. Suponha que G tem um elemento de ordem p e um elemento de ordem q, onde p e q são primos distintos. Mostre que a ordem de G é múltiplo de pq.

Exercício 2.115. Suponha que G tem um elemento de ordem k e um elemento de ordem n. Mostre que a ordem de G é múltiplo de $mmc(k, n)$.

Exercício 2.116. Seja p um primo. Prove que, em qualquer grupo finito, o número de elementos de ordem p é múltiplo de $p - 1$.

19/10/2017 (Bianca)

Exercício 2.117. Prove os seguintes:

(i) se $a \mid b$, então $|a| \leq |b|$, com $b \neq 0$

(ii) se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$, para $x, y \in \mathbb{Z}$.

Exercício 2.118. Mostre que a soma de três números consecutivos é divisível por 3.

Exercício 2.119. Prove que para qualquer inteiro n ímpar, n^2 é da forma $8m + 1$, para algum inteiro m.

23/10/2017 (Jp)

Exercício 2.120. Verifique se as seguintes funções definem homomorfismos. Nos casos em que forem homomorfismos, determine o kernel.

- $\mathbb{R}^*$ é o grupo multiplicativo dos reais não-nulos. $\phi : \mathbb{R}^* \to \mathbb{R}^*$, $\phi(x) = x^2$.
- $\phi : \mathbb{R}^* \to \mathbb{R}^*$, $\phi(x) = 2^x$.
- Seja G um grupo abeliano. $\phi : G \to G$, $\phi(x) = x^5$.

Exercício 2.121. Seja G um grupo, e g um elemento fixo de G. Defina $\phi : G \to G$ onde $\phi(x) = gxg^{-1}$. Prove que ϕ é um isomorfismo de G em G.

24/10/2017 (Bianca)

Exercício 2.122. Se $H \leq G$ de índice 2, então $H \trianglelefteq G$.

Exercício 2.123. Se $H \leq G$ e $N \trianglelefteq G$, então $H \cap N \trianglelefteq H$.

Exercício 2.124. Se $(a, c) = 1$ e $c \mid ab$, então $c \mid b$.

Exercício 2.125. Se $a \mid m$, $b \mid m$ e $(a, b) = 1$, então $ab \mid m$.

Exercício 2.126. Prove que $ax + by = c$ tem soluções sse $(a, b) \mid c$.

Exercício 2.127. Se $a > 0$ e $a \mid b$, então $(a, b) = a$.

Exercício 2.128. Se $ab \equiv 0 \pmod{p}$, onde p é primo, então $a \equiv 0 \pmod{p}$ ou $b \equiv 0 \pmod{p}$.

26/10/2017 (Bianca)

Exercício 2.129. Seja G grupo e $H, K \leq G$. Prove que

$$HK = KH \iff HK \leq G$$

Exercício 2.130. Seja G grupo e N um subgrupo normal de G. Prove que para todo $x \in G$, $x^2 \in N$ sse todo elemento de G/N é seu próprio inverso.

Exercício 2.131. Se $\varphi : G \to H$ é um homomorfismo, prove que para todo elemento $a \in G$, a ordem de $\varphi(a)$ é um divisor da ordem de a.

Exercício 2.132. Se $\varphi : G \to H$ é um epimorfismo, prove que:

(i) Se G é abeliano, então H é abeliano.

(ii) Se G é cíclico, então H é cíclico.

(iii) Se todo elemento em G é o seu próprio inverso, então todo elemento em H é o seu próprio inverso.

30/10/2017 (Jp)

Notações:

- $\mathbb{R}$ é o grupo aditivo dos reais.
- $\mathbb{R}^*$ é o grupo multiplicativo dos reais.
- $\mathcal{F}(\mathbb{R})$ é o grupo das funções de $\mathbb{R}$ em $\mathbb{R}$ com a operação $+$, onde $(f + g)(x) = f(x) + g(x)$.
- $\mathcal{D}(\mathbb{R})$ é o subgrupo de $\mathcal{F}(\mathbb{R})$ das funções deriváveis/diferenciáveis.
- $\mathbb{R}\times\mathbb{R}$ é o grupo aditivo dos pares ordenados de reais, com $(a, b)+(x, y) = (a + x, b + y)$
- $M_{2\times2}$ é o grupo multiplicativo das matrizes reais 2×2 inversíveis.

Prove que cada uma das seguintes funções é um homomorfismo de grupos, e descreva seu kernel.

Exercício 2.133. A função $\phi : \mathcal{F}(\mathbb{R}) \to \mathbb{R}$ dada por $\phi(f) = f(0)$.

Exercício 2.134. A função $\phi : \mathcal{D}(\mathbb{R}) \to \mathcal{F}(\mathbb{R})$ dada por $\phi(f) = \frac{df}{dx}$.

Exercício 2.135. A função $\phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ dada por $\phi(x, y) = x + y$.

Exercício 2.136. A função $\phi : M_{2\times2} \to \mathbb{R}^*$, dada por $\phi(A) = det(A)$.

31/10/2017 (Bianca)

Exercício 2.137. Se n é um inteiro composto, então existe um a natural com $a \leq \sqrt{n}$ tal que $a \mid n$.

Exercício 2.138. Para todo $n \in \mathbb{N}$ e todo ímpar $k \in \mathbb{Z}$, k^n é ímpar.

Exercício 2.139. Prove ou refute:

(i) $a \mid b+c \;\&\; a \mid b-c \implies a \mid b$

(ii) $a \mid b+c \;\&\; a \mid b+2c \implies a \mid b$.

Exercício 2.140. Sejam $a, b \in \mathbb{Z}$. Prove que:

$$(a, b) = (a, a+b)\,.$$

01/11/2017 (Jp)

Exercício 2.141. Denotamos por $\mathbb{B}^*$ como o conjunto de todas as palavras binárias. Uma definição recursiva para esse conjunto é a seguinte:

$$\mathbb{B}^* ::= \lambda \mid \mathbb{B}^* 0 \mid \mathbb{B}^* 1$$

Definimos também uma operação de concatenação para esse conjunto, dada por $\cdot : \mathbb{B}^* \times \mathbb{B}^* \to \mathbb{B}^*$ onde

1. $x \cdot \lambda = x$
2. $x \cdot (w0) = (x \cdot w)0$
3. $x \cdot (w1) = (x \cdot w)1$

Mostre que $\langle \mathbb{B}^*, \cdot\,, \lambda \rangle$ é um monóide.

Exercício 2.142. Tome $\phi : \mathbb{B}^* \to \mathbb{N}$ dado por

1. $\phi(\lambda) = 0$
2. $\phi(w0) = w + w$
3. $\phi(w1) = w + w + 1$

Determine se ϕ é um homomorfismo de monóides de $\langle \mathbb{B}^*, \cdot\,, \lambda \rangle$ em $\langle \mathbb{N}, +, 0 \rangle$.

Exercício 2.143. Sejam $\langle G, \cdot_G \rangle$ e $\langle H, \cdot_H \rangle$ dois grupos.

- Mostre que o conjunto dado pelo produto cartesiano $G \times H$ com a operação $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$ também é um grupo.
- Mostre que existe um subgrupo de $G \times H$ isomórfico a G. (São duas tarefas: a primeira é mostrar que o subconjunto encontrado é um subgrupo; a segunda é mostrar que esse subgrupo é isomórfico a G)

Exercício 2.144. Seja $\mathcal{G} = \left\langle G, \cdot\,, e, {}^{-1} \right\rangle$ um grupo. Defina uma nova operação $\cdot^{op} : G \times G \to G$ tal que $x \cdot^{op} y = y \cdot x$. Mostre que $\mathcal{G}^{op} = \left\langle G, \cdot^{op}, e, {}^{-1} \right\rangle$ é um grupo, e que é isomórfico a $\mathcal{G}$.

06/11/2017 (Jp)

Definição 2.145. Teorema Fundamental da Aritmética: todo inteiro maior que 1 pode ser escrito como um único produto de primos.

Exercício 2.146. Forneça uma prova para o Teorema Fundamental da Aritmética.

07/11/2017 (Bianca)

Sejam G, H e K grupos. Prove os seguintes:

Exercício 2.147. Se $\varphi : G \to H$ e $\psi : H \to K$ são homomorfismos, então sua composição $\psi \circ \varphi : G \to K$ é um homomorfismo.

Exercício 2.148. Para qualquer grupo G, a função $\varphi : G \to G$ dada por $\varphi(x) = e$ é um homomorfismo.

Exercício 2.149. A função $\varphi : G \to G$ dada por $\varphi(x) = x^2$ é um homomorfismo sse G é abeliano.

Exercício 2.150. Seja H um subgrupo de G. H é normal sse ele tem a seguinte propriedade: Para todos os $a, b \in G$, $ab \in H$ sse $ba \in H$.

Exercício 2.151. Se a é um elemento arbitrário de G, $<a>$ é um subgrupo normal de G sse a tem a seguinte propriedade: Para todo $x \in G$, existe um inteiro positivo k tal que $xa = a^k x$.

Exercício 2.152. Prove que em qualquer anel, $a(b-c) = ab-ac$ e $(b-c)a = ba - ca$.

Exercício 2.153. Prove que em qualquer anel, se $ab = -ba$, então $(a+b)^2 = (a-b)^2 = a^2 + b^2$.

08/11/2017 (Jp)

Exercício 2.154. Definimos $\tau_{a,b} : \mathbb{R} \to \mathbb{R}$ como a função $\tau_{a,b}(x) = ax + b$. Seja $G = \{\tau_{a,b} \mid a, b \in \mathbb{R} \wedge a \neq 0\}$.

- Mostre que G com a operação de composição de funções forma um grupo.
- Seja $N = \{\tau_{1,b} \in G\}$. Mostre que N é um subgrupo normal de G.
- Mostre que G/N é isomórfico ao $\mathbb{R}^*$, o grupo multiplicativo dos reais.

09/11/2017 (Bianca)

Exercício 2.155. Usando o Algoritmo Estendido de Euclides, encontre o m.d.c. dos seguintes inteiros e escreva-o como uma combinação linear deles:

(i) $14, 35$

(ii) $11, 15$

(iii) $180, 252$

(iv) $1001, 7655$

Exercício 2.156. Se $a, b \in \mathbb{Z}$ com $b > 0$, então $(a, b) = (b, r)$, onde r é o resto da divisão de a por b.

13/11/2017 (Jp)

Exercício 2.157. Prove cada item:

- $\mathbb{R} =_c \mathbb{R}^+$.
- $[a, b] =_c [c, d]$, onde $a < b$ e $c < d$.
- $\mathbb{N} \times \mathbb{N} =_c \mathbb{N}$.

Exercício 2.158. Para cada item abaixo, descreva uma estratificação que permita enumerar os respectivos conjuntos:

- O conjunto das palavras geradas pelo alfabeto $\Sigma = \{a, b, \ldots, z\}$.
- O conjunto de triplas de naturais, $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$.

Exercício 2.159. Seja G um grupo cíclico infinito. Mostre que G é contável.

Exercício 2.160. Seja A um conjunto infinito contável. Mostre que $A \times A =_c A$.

16/11/2017 (Bianca)

Exercício 2.161. Se A é contável e existe uma injeção $f : B \rightarrowtail A$, então B também é contável.

Exercício 2.162. Se A é contável e existe uma sobrejeção $f : A \twoheadrightarrow B$, então B também é contável.

Exercício 2.163. Suponha que $\mathbb{N} \leq_c A$. Mostre que A é infinito.

Exercício 2.164. Prove que os seguintes são equivalentes para todo conjunto A:

(1) A é contável

(2) $A \leq_c \mathbb{N}$

(3) Ou $A = \emptyset$, ou A tem uma enumeração.

22/11/2017 (Jp)

Exercício 2.165. Sejam A e B conjuntos tais que $A \subseteq B$. Mostre que $A \leq_c B$.

Exercício 2.166. Sejam A e B conjuntos. Suponha que A e B tem pelo menos dois elementos cada $(*)$.

- Prove que $A \cup B \leq_c A \times B$.
- A hipótese $(*)$ é necessária? Reflita e argumente.

23/11/2017 (Bianca)

Exercício 2.167. Usando o Teorema Chinês do Resto, ache todos os inteiros $x \in \mathbb{Z}$ que satisfazem o sistema de congruências:

$$\begin{cases} x \equiv 2 \pmod 9 \\ x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 4 \end{cases}$$

Exercício 2.168. Ache todos os inteiros $x \in \mathbb{Z}$ com $|x| < 64$ que satisfazem o sistema de congruências:

$$\begin{cases} x \equiv 1 \pmod 3 \\ 3x \equiv 1 \pmod 4 \\ 4x \equiv 2 \pmod 5 \end{cases}$$

Exercício 2.169. Sejam a, b conjuntos. Mostre que $\{b, \{\emptyset, \{a\}\}\}$ é conjunto.

Exercício 2.170. Sejam a, b, c, d conjuntos. Mostre pelos axiomas que os seguintes também são:

$$A = \{a, b, c, d\}$$
$$B = \{a, b, \{c, d\}\}$$
$$C = \{x \mid x \subseteq a \cup b \cup c \cup d \ \& \ x \text{ tem exatamente 2 membros}\}.$$

27/11/2017 (Jp)

Exercício 2.171. Traduza para português as seguintes fórmulas:

- $\forall x \exists y (x \notin y)$
- $\forall x \forall y ((x \in y \wedge y \in z) \Rightarrow x \in z)$

Exercício 2.172. Expresse cada um dos seguintes itens como uma fórmula:

- O conjunto x contêm pelo menos um elemento.
- Existe um conjunto com exatamente um elemento.

Exercício 2.173. Mostre que para quaisquer conjuntos x e y, existe um único conjunto cujos elementos são exatamente x e y.

Exercício 2.174. Seja x um conjunto. Mostre que existe um único conjunto y cujos elementos são todos os subconjuntos de x.

Exercício 2.175. Sejam $x_1, x_2, \ldots, x_n$ conjuntos, para algum natural $n \geq 1$.

- Mostre que existe um conjunto cujos elementos são exatamente os $x_1, x_2, \ldots, x_n$.
- Mostre que $x_1 \cup x_2 \cup \cdots \cup x_n$ é um conjunto.

28/11/2017 (Bianca)

Definição 2.176 (Adição e Multiplicação)**.** A função de adição nos números naturais é definida pela recursão

$$\begin{aligned} n + 0 &= n, && \text{(a1)} \\ n + (Sm) &= S(n + m). && \text{(a2)} \end{aligned}$$

e a multiplicação é definida em seguida, usando adição, pela recursão

$$\begin{aligned} n \cdot 0 &= 0, && \text{(m1)} \\ n \cdot Sm &= (n \cdot m) + n. && \text{(m2)} \end{aligned}$$

Exercício 2.177. Prove que adição é associativa, ou seja, satisfaz a identidade

$$(n + m) + k = n + (m + k).$$

Exercício 2.178. Mostre que, para todo natural n, $0 + n = n$.

Exercício 2.179. Prove que, para todos n, m, $n + Sm = Sn + m$.

Exercício 2.180. Prove que adição é comutativa, ou seja, satisfaz a identidade

$$n + m = m + n.$$

29/11/2017 (Jp)

Exercício 2.181. Defina recursivamente a função $d : \mathbb{N} \to \mathbb{N}$ que dobra sua entrada. Verifique que $d(3) = 6$.

Exercício 2.182. Defina recursivamente a multiplicação $\_ \cdot \_ : \mathbb{N}^2 \to \mathbb{N}$. Verifique que $2 \cdot 3 = 6$.

Exercício 2.183. Demonstre as seguintes propriedades para a multiplicação:

- Associatividade
- Comutatividade
- Distributividade sobre adição $(+)$

Exercício 2.184. Mostre que $d(n) = 2 \cdot n$, para todo natural n.

30/11/2017 (Bianca)

Exercício 2.185. Exponenciação nos números naturais é definida pela seguinte recursão no m:

$$n^0 = 1, \qquad (e1)$$
$$n^{Sm} = n^m \cdot n. \quad (e2)$$

Mostre que ela satisfaz as seguintes identidades (para $n \neq 0$):

$$n^{(m+k)} = m^m \cdot n^k,$$
$$n^{(m \cdot k)} = (n^m)^k.$$

Exercício 2.186. Defina recursivamente o fatorial

$$f(n) = 1 \cdot 2 \cdots (n-1) \cdot n.$$

Exercício 2.187. Suponha que $(\mathbb{N}_1, 0_1, S_1)$ e $(\mathbb{N}_2, 0_2, S_2)$ são dois sistemas Peano, $+_1, \cdot_1, +_2, \cdot_2$ são as funções de adição e multiplicação nesses sistemas, e $\pi : \mathbb{N}_1 \rightarrowtail \mathbb{N}_2$ é o isomorfismo "canônico" entre eles definido por

$$\pi(0_1) = 0_2,$$
$$\pi(S_1 n) = S_2 \pi(n) \ (n \in \mathbb{N}_1).$$

Mostre que π é um isomorfismo com respeito à adição e também à multiplicação, ou seja, para todos $n, m \in \mathbb{N}_1$,

$$\pi(n +_1 m) = \pi(n) +_2 \pi(m), \ \pi(n \cdot_1 m) = \pi(n) \cdot_2 \pi(m).$$

Definição 2.188. A relação de ordem $\leq$ nos números naturais é definida pela equivalência

$$n \leq m \iff^{\text{def}} (\exists s)[n + s = m].$$

Exercício 2.189. Suponha que $(\mathbb{N}_1, 0_1, S_1)$ e $(\mathbb{N}_2, 0_2, S_2)$ são dois sistemas Peano, $\leq_1, \leq_2$ são as respectivas boas ordens e $\pi : \mathbb{N}_1 \rightarrowtail \mathbb{N}_2$ é o isomorfismo canônico. Mostre que π é ordem-preservante, ou seja, para todos $n, m \in \mathbb{N}_1$,

$$n \leq_1 m \iff \pi(n) \leq_2 \pi(m).$$

04/12/2017 (Jp)

Exercício 2.190. Dizemos que um conjunto C é cofinito em um conjunto A sse $A \backslash C$ é finito. Para qualquer conjunto A definimos $\wp_{cof} A \stackrel{\text{def}}{=} \{C \subset A \mid C \text{ é cofinito no } A\}$. Qual a cardinalidade do $\wp_{cof}\mathbb{N}$?

Exercício 2.191. Para qualquer conjunto A definimos $\wp_\infty A \stackrel{\text{def}}{=} \{C \subseteq A \mid C \text{ é infinito}\}$. Qual a cardinalidade do $\wp_\infty \mathbb{N}$?

05/12/2017 (Bianca)

Exercício 2.192. Sem usar o (ZF3), mostre que para qualquer conjunto a existe um conjunto que tem a como seu único elemento.

Exercício 2.193. Considere a seguinte versão mais fraca do (ZF3):

Dados quaisquer conjuntos a e b, existe um conjunto u tal que $a \in u$ e $b \in u$.

Chame-a de (ZF3′). Prove que é possível substituir o (ZF3) pelo (ZF3′) sem perder nada. Ou seja, dados objetos a, b, mostre que existe o conjunto $\{a, b\}$ que consiste exatamente nesses objetos.

Exercício 2.194. Dado um conjunto a, justifique (usando os axiomas ZF) a existência do conjunto $\{\{x\} \mid x \in a\}$.

Exercício 2.195. Para $n \in \mathbb{N}$, definimos o poset $\mathcal{D}_n \stackrel{\text{def}}{=} \langle D_n \,;\, | \rangle$ onde $D_n \stackrel{\text{def}}{=} \{d \in \mathbb{N} \mid d \mid n\}$.

(i) Desenhe o diagrama Hasse de $\mathcal{D}_{30}$.

(ii) Ache conjunto A tal que $\mathcal{D}_{30} \cong \langle \wp A \,;\, \subseteq \rangle$, e defina um isomorfismo $\varphi : D_{30} \to \wp A$.

(iii) Existe conjunto B tal que $\mathcal{D}_0 \cong \langle \wp B \,;\, \subseteq \rangle$? Se sim, ache o B e defina um isomorfismo $\varphi : D_0 \to \wp B$. Se não, prove que é impossível.

(iv) Verdadeiro ou falso? $\mathcal{D}_0 \cong \langle \{D_n \mid n \in \mathbb{N}\} \,;\, \subseteq \rangle$.

06/12/2017 (Jp)

Exercício 2.196. Seja A um conjunto e $\sim$ uma relação de equivalência em A. Mostre que $A/\!\sim \leq_c A$.

07/12/2017 (Bianca)

Definição 2.197. Um conjunto estruturado $\mathcal{L} = \langle L \,;\, \vee, \wedge \rangle$ é um lattice sse para todo $a, b, c \in L$:

(Ass1)	$a \vee (b \vee c) = (a \vee b) \vee c$	$a \vee a = a$	(Idem1)
(Ass2)	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$	$a \wedge a = a$	(Idem2)
(Com1)	$a \vee b = b \vee a$	$(a \vee b) \wedge a = a$	(Abs1)
(Com2)	$a \wedge b = b \wedge a$	$(a \wedge b) \vee a = a$	(Abs2)

Exercício 2.198. Seja $\mathcal{L} = \langle L\ ;\ \vee, \wedge \rangle$ um lattice. Prove que:

(i) $a \vee b = b \iff a \wedge b = a$

(ii) Defina $\leq$ no L por $a \leq b$ se $a \vee b = b$. Então $\leq$ é uma relação de ordem.

Exercício 2.199. Seja $\mathcal{L} = \langle L\ ;\ \leq \rangle$ um poset tal que $\bigwedge H$ existe para todo $H \subseteq L$. Mostre que $\mathcal{L}$ é um lattice.

Exercício 2.200. Prove que podemos inferir as leis (Idem1)-(Idem2) pelas outras.

Exercício 2.201. Sejam P e Q posets finitos e seja $\varphi : P \rightarrowtail\!\!\!\!\!\rightarrow Q$ um mapeamento bijetivo. Então, os seguintes são equivalentes:

(i) φ é um isomorfismo de ordem;

(ii) $x < y$ em P se e somente se $\varphi(x) < \varphi(y)$ em Q;

(iii) $x \prec y$ em P se e somente se $\varphi(x) \prec \varphi(y)$ em Q.

3 2018.1

05/03/2018 (Jp)

Definição 3.1 (Naturais)**.** Definimos o conjunto dos naturais recursivamente, da seguinte forma: $\langle \mathbf{Nat} \rangle\ ::=\ O\ \mid\ S\ \langle \mathbf{Nat} \rangle$

Exercício 3.2. Defina a operação de adição sobre os números naturais como definidos acima.

Exercício 3.3. Demonstre que a adição definida no exercício anterior é associativa. Isso é, mostre que para todo m, n, p naturais, $m+(n+p) = (m+n)+p$.

Definição 3.4 (Lema 1 da adição)**.** Para todo n natural, $n + 0 = n$.

Definição 3.5 (Lema 2 da adição)**.** Para todo m, n naturais, $S(m + n) = m + Sn$.

Homework 3.1. Demonstre 3.4 (p. 35) e 3.5 (p. 35).

Exercício 3.6. Demonstre que a adição é comutativa (ou seja, que para todo m, n naturais, $m + n = n + m$). Use coisas que demonstramos anteriormente.

Homework 3.2. Defina a multiplicação, e prove sua associatividade e comutatividade

06/03/2018 (Bianca)

Exercício 3.7. Algumas definições de funções recursivas são:

$$\begin{aligned} x + 0 &= x \quad \text{(a1)} & x \cdot 0 &= 0 \quad \text{(m1)} \\ x + Sy &= S(x + y) \quad \text{(a2)} & x \cdot Sy &= (x \cdot y) + x \quad \text{(m2)} \end{aligned}$$

$$\begin{aligned} x^0 &= S0 \quad \text{(e1)} \\ x^{Sy} &= x^y \cdot x \quad \text{(e2)} \end{aligned}$$

Dados os lemas:

$$\begin{aligned} a + b &= b + a \quad \text{(a-com)} \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c \quad \text{(m-ass)} \end{aligned}$$

prove por indução as seguintes propriedades, indicando para cada passo o que foi usado:

$$\text{(i)} \quad a \cdot S0 = a \qquad \text{(ii)} \quad a^{x+y} = a^x \cdot a^y \qquad \text{(iii)} \quad a^{x \cdot y} = (a^x)^y.$$

07/03/2018 (Jp)

Exercício 3.8. Traduza as seguintes frases para a lógica de primeira ordem da teoria de conjuntos.

1. Existe conjunto sem membros;
2. O conjunto x não tem membros;
3. Existe conjunto com membros;
4. Existe conjunto com exatamente um membro;
5. Os conjuntos x e y tem exatamente um membro em comum;
6. Para todos conjuntos a e b, sua união é um conjunto;
7. Existe conjunto que não é igual com ele mesmo

08/03/2018 (Bianca)

Exercício 3.9. Suponha que A, B e C são conjuntos. Então $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Exercício 3.10. Suponha que $A \subseteq B$, e A e C são disjuntos. Prove que $A \subseteq B \setminus C$.

Exercício 3.11. Suponha que A, B e C são conjuntos. Prove que se $A \subseteq C$ e $B \subseteq C$, então $A \cup B \subseteq C$.

Exercício 3.12. Suponha A, B e C conjuntos, $A \setminus B \subseteq C$ e x arbitrário. Prove que se $x \in A \setminus C$, então $x \in B$.

Exercício 3.13. Use indução para mostrar que para todo $n \geq 1$

$$n! \geq 2^{n-1}$$

Exercício 3.14. Suponha as propriedades de adição para os números naturais, mas que multiplição não é conhecida. Então, o seguinte pode ser usado como uma definição recursiva de multiplicação:

$$1 \cdot b = b \qquad \text{(i)}$$
$$(a+1) \cdot b = a \cdot b + b \qquad \text{(ii)}$$

Prove o seguinte:

(a) $a \cdot (b + c) = a \cdot b + a \cdot c$

(b) $a \cdot 1 = a$

(c) $a \cdot b = b \cdot a$

12/03/2018 (Jp)

Exercício 3.15. Prove que, para todos os conjuntos A, B e C,

- $C - (A \cup B) = (C - A) \cap (C - B)$
- $C - (A \cap B) = (C - A) \cup (C - B)$

Definição 3.16 (Diferença simétrica)**.** Dados A e B conjuntos, definimos $A \triangle B$ tal que

$$x \in A \triangle B \overset{\text{def}}{\iff} x \text{ pertence a exatamente um dos } A, B$$

Exercício 3.17. Prove que, para todos os conjuntos A e B,

$$A \triangle B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

Definição 3.18 (Produto cartesiano)**.** Dados A e B conjuntos, definimos

$$A \times B = \{\langle a, b\rangle \mid a \in A, b \in B\}$$

Exercício 3.19. Prove que, para todos os conjuntos A e B não-vazios, se $A \times B = B \times A$ então $A = B$.

13/03/2018 (Bianca)

Exercício 3.20. Para quaisquer três conjuntos A, B, C:

(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(iii) $A \setminus (A \cap B) = A \setminus B$

(iv) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$

(v) $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$

Exercício 3.21. Para qualquer conjunto C e qualquer sequência de conjuntos $\{A_n \mid n \in \mathbb{N}\}$:

(i) $C \setminus (\bigcup_{n=0}^{\infty} A_n) = \bigcap_{n=0}^{\infty} (C \setminus A_n)$

(ii) $C \setminus (\bigcap_{n=0}^{\infty} A_n) = \bigcup_{n=0}^{\infty} (C \setminus A_n)$

14/03/2018 (Jp)

Exercício 3.22. Prove que, para qualquer conjunto A, $\cup \wp A = A$.

Exercício 3.23. Demonstre ou exiba contra-exemplos para cada uma das seguintes asserções, onde A e B são conjuntos:

- $\varnothing \in \wp A$
- $\varnothing \in A$
- $\wp(A \cup B) = \wp(A) \cup \wp(B)$
- $\wp(A \cap B) = \wp(A) \cap \wp(B)$

15/03/2018 (Bianca)

Exercício 3.24. $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Exercício 3.25. $A \times (B \cup C) = (A \times B) \cup (A \times C)$

Exercício 3.26. $(A \times B) \cap (A \times D) = (A \cap C) \times (B \cap D)$

Exercício 3.27. $A \times (B \setminus D) = (A \times B) \setminus (A \times D)$

19/03/2018 (Jp)

Exercício 3.28. Sejam P, Q e R conjuntos. Considere as seguintes asserções:

(a) $P \subseteq R$

(b) $P \cup (Q \cap R) = (P \cup Q) \cap R$

(c) $(P \cap Q) \cup R = R$

Verifique (isto é, demonstre ou refute) as seguintes asserções:

- (1a) implica (1b)
- (1b) implica (1a)
- (1a) implica (1c)
- (1c) implica (1a)

20/03/2018 (Bianca)

Exercício 3.29. Os nũmeros Fibonacci são definidos recursivamente assim:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n \end{aligned}$$

Prove que para todo $n \in \mathbb{N}$,

$$\sum_{i=0}^{n} F_i = F_{n+2} - 1.$$

Exercício 3.30. Sejam $n \in \mathbb{N}$ com $n \geq 2$ e n conjuntos $A_1, A_2, \ldots, A_n$. Seja

$$A = A_1 \triangle A_2 \triangle \cdots \triangle A_n$$

Observe que como a operação $\triangle$ é (i) associativa e (ii) comutativa, o A é bem definido. Prove que

$$A = \{a \mid a \text{ pertence a uma quantidade ímpar de } Ai\text{'s}\}.$$

21/03/2018 (Jp)

Exercício 3.31. Defina formalmente os operadores unários $\wp(-)$, $\bigcap$ e $\bigcup$.

Exercício 3.32. Seja A_n uma família de conjuntos. Mostre que $C \setminus \bigcup_{n=0}^{\infty} A_n = \bigcap_{n=0}^{\infty} (C \setminus A_n)$.

Exercício 3.33. Seja A um conjunto, e A_n uma sequência de subconjuntos de A. Defina:

$$A_* = \bigcup_{i=0}^{\infty} \bigcap_{j=i}^{\infty} A_j$$

$$A^* = \bigcap_{i=0}^{\infty} \bigcup_{j=i}^{\infty} A_j$$

- Como descrever os elementos dos A_* e A^*?
- É verdade que um desses conjuntos é subconjunto do outro? São iguais? São disjuntos?

22/03/2018 (Bianca)

Exercício 3.34. Prove ou refute a afirmação:
para todos os conjuntos A, B, C, se $A \subseteq B$ e $A \subseteq C$, então $A \subseteq B \cap C$.

Exercício 3.35. Prove ou refute a afirmação:
para todos os conjuntos A, B, C, se $A \subsetneq B$ e $A \subsetneq C$, então $A \subsetneq B \cap C$.

Exercício 3.36. Sejam $\{A_n\}_n$ e $\{B_n\}_n$ duas sequências de conjuntos tais que, para todo $n \in \mathbb{N}$, $A_n \subsetneq B_{n+1}$.

(a) Prove que

$$\bigcup_{n=0}^{\infty} A_n \subseteq \bigcup_{n=0}^{\infty} B_n.$$

(b) Mostre que, em geral, não podemos concluir que

$$\bigcup_{n=0}^{\infty} A_n \subsetneq \bigcup_{n=0}^{\infty} B_n.$$

Exercício 3.37. Prove que se $(A \times B) \cap (C \times D) = \emptyset$, então $A \cap C = \emptyset$ ou $B \cap D = \emptyset$.

27/03/2018 (Bianca)

Exercício 3.38. Prove que a relação $|$ é uma ordem parcial no $\mathbb{N}$.

Exercício 3.39. Prove que para todo $n \in \mathbb{Z}$, se $3 \nmid n$, então $3 \mid n^2 - 1$.

Exercício 3.40. Se $f : X \to Y$ e $A, B \subseteq X$, então

$$f[A \cup B] = f[A] \cup f[B].$$

28/03/2018 (Jp)

Definição 3.41 (Partição)**.** Dado um conjunto A, uma *partição* de A é um conjunto $\mathcal{A}$ de subconjuntos de A que satisfaz as seguintes propriedades:

(i) $\bigcup \mathcal{A} = A$

(ii) para todos $X, Y \in \mathcal{A}$, $X \cap Y = \emptyset$

(iii) $\emptyset \notin \mathcal{A}$

Exercício 3.42. Dado $A = \{0, 1, 2, 3, 4, 5, 6\}$, determine para cada item abaixo se o mesmo configura uma partição de A.

- $\mathcal{A}_1 = \{\{0, 1, 2\}, \{3\}, \{4, 5, 6\}\}$
- $\mathcal{A}_2 = \{\{0, 1, 2\}, \{2, 3, 4\}, \{4, 5, 6\}\}$
- $\mathcal{A}_3 = \{\{0, 1, 2\}, \{3, 4\}, \{5, 6, 7\}\}$

- $\mathcal{A}_4 = \{\{0,1\}, \emptyset, \{2,3,4\}, \{5,6\}\}$

Exercício 3.43. Dado $\mathcal{A} = \{\{0,1\}, \{2\}, \{3,4,5\}\}$ partição de $A = \{0,1,2,3,4,5\}$, determine a relação de equivalência sobre A induzida por $\mathcal{A}$

Exercício 3.44. Verifique a seguinte asserção: dadas duas relações de equivalência R e S sobre um conjunto A, sua composição é também uma relação de equivalência.

02/04/2018 (Jp)

Exercício 3.45. Para cada item abaixo, verifique se o mesmo é bem-definido e determina uma função:

- $f : \mathbb{R} \to \mathbb{R}$, onde $f(x)$ é o y tal que $y^2 = x$.
- $g : \mathbb{Z} \to \mathbb{Z}$, onde $g(n)$ é o m tal que $n = m + 1$.
- $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, onde $f(n, m)$ é o natural que divide n e m simultaneamente.
- $m : \mathcal{P} \to \mathcal{P}$, onde $\mathcal{P}$ é o conjunto das pessoas, e $m(p)$ é a mãe de p.

03/04/2018 (Bianca)

Exercício 3.46. Sejam A, B conjuntos diferentes, e $f : A \to B$. Para cada uma das igualdades, decida se ela é válida ou não, justificando sua resposta.

(1) $f = f \circ \mathrm{id}_A$

(2) $f = f \circ \mathrm{id}_B$

(3) $f = \mathrm{id}_A \circ f$

(4) $f = \mathrm{id}_B \circ f$

Exercício 3.47. A, B, C são três conjuntos diferentes; f, g, h e k são funções com os seguintes domínios e contra-domínios:

$$f : A \to B, \qquad g : B \to A, \qquad h : A \to C, \qquad k : C \to B.$$

Duas das expressões abaixo fazem sentido. Encontre-as e determine seus respectivos domínios e contra-domínios.

(a) $k \circ h \circ g \circ f$

(b) $k \circ f \circ g$

(c) $g \circ f \circ g \circ k \circ h$

Exercício 3.48. A e B são conjuntos, $f : A \times B \to B \times A$ é definida pela $f(x, y) = (y, x)$.

Encontre a $g \circ f$ e seu domínio e contra-domínio.

Exercício 3.49.

$f : \mathbb{R} \to \mathbb{R}$ é definida pela $f(x) = sen(x)$.
$g : \mathbb{R} \to \mathbb{R}$ é definida pela $g(x) = \mathrm{e}^x$.

Encontre $f \circ g$ e $g \circ f$.

Exercício 3.50. $A = \{a, b, c, d\}$; f e g são funções de A para A; elas são definidas, na forma tabular, pelas

$$f = \begin{pmatrix} a & b & c & d \\ a & c & a & c \end{pmatrix} \quad g = \begin{pmatrix} a & b & c & d \\ b & a & b & a \end{pmatrix}$$

Encontre $f \circ g$ e $g \circ f$ na mesma forma tabular.

Exercício 3.51. Verdade ou falso? (Prove sua resposta).

Se $g \circ f$ é constante, então pelo menos uma das f, g também é.

04/04/2018 (Jp)

Exercício 3.52. Dados A e B conjuntos, seja X um conjunto com as seguintes propriedades:

(i) $A \subseteq X$ e $B \subseteq X$

(ii) para todo conjunto Y, se $A \subseteq Y$ e $B \subseteq Y$ então $X \subseteq Y$

Mostre que $X = A \cup B$.

Exercício 3.53. Formule e prove uma caraterização análoga à do exercício anterior para a interseção $A \cap B$.

Exercício 3.54. Dados $A, B \subseteq U$, prove:

- $A \cap B = \emptyset$ sse $A \subseteq \widetilde{B}$
- $A \cup B = U$ sse $\widetilde{A} \subseteq B$

05/04/2018 (Bianca)

Exercício 3.55. Cada um dos seguintes é uma função $f : \mathbb{R} \to \mathbb{R}$. Determine:

(a) se f é ou não injetiva, e

(b) se f é ou não sobrejetiva.

Prove sua resposta em qualquer um dos casos.

(i) $f(x) = 2x$

(ii) $f(x) = x^2$

(iii) $f(x) = 3x + 4$

(iv) $f(x) = \begin{cases} 2x & \text{se } x \text{ é um inteiro} \\ x & \text{caso contrário} \end{cases}$

Exercício 3.56. A e B são conjuntos e $A \times B$ denota o conjunto de todos os pares ordenados (x, y), onde $x \in A$ e $y \in B$. Determine se cada um das funções seguintes é ou não (a) injetiva e (b) sobrejetiva. Proceda como no exercício 3.55.

(i) $f : A \times B \to A$, definida por $f(x, y) = x$.

(ii) $f : A \times B \to B \times A$, definida por $f(x, y) = (y, x)$

(iii) $f : A \to A \times B$, definida por $f(x) = (x, b)$, onde b é um elemento fixo de B.

Exercício 3.57. Sejam A, B, C conjuntos, $f : A \to B$ e $g : B \to C$.

(i) Prove que se $g \circ f$ é injetiva, então f é injetiva.

(ii) Prove que se $g \circ f$ é sobrejetiva, então f é sobrejetiva.

09/04/2018 (Jp)

Exercício 3.58. Dada uma função $f : A \to B$

(a) Prove que se tem $f[X] \setminus f[Y] \subseteq f[X \setminus Y]$ para todos $X, Y \subseteq A$.

(b) Mostre que, se f for injetiva, se tem $f[X] \setminus f[Y] = f[X \setminus Y]$ para todos $X, Y \subseteq A$.

Exercício 3.59. Mostre que uma função $f : A \to B$ é injetiva sse $f[X] \setminus f[Y] = f[X \setminus Y]$ para todos $X, Y \subseteq A$.

10/04/2018 (Bianca)

Definição 3.60 (Isomorfismo)**.** Uma função $f : A \to B$ é dita um isomorfismo se existe uma função $g : A \to B$ tal que:

$$g \circ f = \mathrm{id}_A$$
$$f \circ g = \mathrm{id}_B$$

Definição 3.61 (Inversa)**.** Uma função g relacionada a f satisfazendo as equações do 3.60 é chamada uma inversa de f.

Exercício 3.62. Mostre que:

(a) Mostre que id_A é um isomorfismo.

(b) Mostre que se $f : A \to B$ é um isomorfismo, e $g : B \to A$ é uma inversa de f, então g também é um isomorfismo.

(c) Mostre que se $f : A \to B$ e $k : B \to C$ são isomorfismos, $k \circ f : A \to C$ também é um isomorfismo.

Exercício 3.63. Suponha que $g : B \to A$ e $k : B \to A$ são ambas inversas de $f : A \to B$. Mostre que $g = k$.

Exercício 3.64. Se f tem uma inversa, então f satisfaz as duas leis de cancelamento:

(a) Se $f \circ h = f \circ k$, então $h = k$

(b) Se $h \circ f = k \circ f$, então $h = k$

Exercício 3.65. Mostre que em geral não podemos afirmar que se $h \circ f = f \circ k$, então $h = k$.

11/04/2018 (Jp)

Definição 3.66 (Função constante)**.** Uma função $f : A \to B$ é dita constante se, para todos $x, y \in A$, temos $f(x) = f(y)$.

Exercício 3.67. Tome a seguinte definição alternativa para função constante: Uma função $f : A \to B$ é dita constante se existe um $y \in B$ tal que para todo $x \in A$, temos $f(x) = y$.

Verifique se as duas definições são equivalentes.

Exercício 3.68. Para cada item abaixo, construa um λ-termo com o tipo correspondente.

- $\mathbb{R} \to \mathbb{R}$
- $\mathbb{R} \to (\mathbb{R} \to \mathbb{R})$
- $(\mathbb{R} \to \mathbb{R}) \to \mathbb{R}$
- $(\mathbb{R} \to \mathbb{R}) \to (\mathbb{R} \to \mathbb{R})$
- $(\mathbb{R}^2 \to \mathbb{R}) \to \mathbb{R}$
- $(\mathbb{R}^2 \to \mathbb{R}) \to (\mathbb{R} \to (\mathbb{R} \to \mathbb{R}))$

Exercício 3.69. Verifique a validade da seguinte afirmação: Dados $f : A \to B$ e $g : B \to C$, se $g \circ f$ é constante então pelo menos uma das f, g também é.

12/04/2018 (Bianca)

Definição 3.70. Se $f : A \to B$:
Uma retração de f é uma função $r : B \to A$ tal que $r \circ f = \mathrm{id}_A$.
Uma seção de f é uma função $s : B \to A$ tal que $f \circ s = \mathrm{id}_B$.

Exercício 3.71. Se uma função $f : A \to B$ tem uma seção, então, para todo T e para toda função $y : T \to B$, existe uma função $x : T \to A$ tal que $f \circ x = y$.

Exercício 3.72. Se a função $f : A \to B$ tem uma retração, então, para toda função $g : A \to T$, existe uma função $t : B \to T$ tal que $t \circ f = g$.

Exercício 3.73. Suponha que uma função $f : A \to B$ tem uma retração. Então, para qualquer conjunto T e para qualquer par de funções $x_1 : T \to A$, $x_2 : T \to A$ de qualquer conjunto T para A: se $f \circ x_1 = f \circ x_2$ então $x_1 = x_2$.

Exercício 3.74. Se a função $f : A \to B$ tem uma retração, então f é injetiva.

Homework 3.3. Suponha que a função $f : A \to B$ tem uma seção, Então, para qualquer conjunto T e qualquer par $t_1 : B \to T$, $t_2 : B \to T$ de funções de B para T, se $t_1 \circ f = t_2 \circ f$ então $t_1 = t_2$.

Exercício 3.75. Se a função $f : A \to B$ tem uma seção, então f é sobrejetiva.

Exercício 3.76. Se $f : A \to B$ tem uma retração e se $g : B \to C$ tem uma retração, então $g \circ f : A \to C$ tem uma retração.

Homework 3.4. Prove que a composição de duas funções, cada uma tendo seções tem, também, uma seção.

Definição 3.77 (Função idempotente)**.** Uma função $f : A \to A$ é chamada de idempotente se $f \circ f = f$

Exercício 3.78. Suponha que r é uma retração de f (equivalentemente, f é uma seção de r) e seja $e = f \circ r$. Mostre que e é idempotente. Mostre que se f é um isomorfismo, então e é a identidade.

Exercício 3.79. Se f tem tanto uma retração r quanto uma seção s então $r = s$.

16/04/2018 (Jp)

Exercício 3.80. Prove que:

- $f : B \to C$ é injetora sse para todos $h, k : A- > B$, se $f \circ h = f \circ k$ então $h = k$.
- $g : A \to B$ é sobrejetora sse para todos $h, k : B- > C$, se $h \circ g = k \circ g$ então $h = k$.

17/04/2018 (Bianca)

Exercício 3.81. Prove que a composição de injeções é uma injeção, a composição de sobrejeções é uma sobrejeção, e consequentemente, a composição de bijeções é uma bijeção.

Exercício 3.82. Sejam $A \neq \emptyset$ um conjunto e $f : A \to \mathcal{P}A$ definida pela equação:

$$f(a) = \{a\}$$

(a) f é injetora?

(b) f é sobrejetora?

Exercício 3.83. Seja S o conjunto de todos os strings não-vazios de um alfabeto Σ, com $|\Sigma| \geq 2$. Considere a função $f : S \times \{0, 1\} \to S$ definida pela:

$$f(w, i) = \begin{cases} ww & \text{, se } i = 0 \\ w' & \text{, se } i = 1 \end{cases}$$

onde w' é o string reverso de w, e onde denotamos a concatenação de strings por justaposição.

(a) f é injetora?

(b) f é sobrejetora?

Exercício 3.84. Sejam $n \in \mathbb{N}$, e $I = \{i \in \mathbb{N} \mid i < n\}$. Considere a função $\pi : I \times A^n \to A$ definida por:

$$\pi(i, \alpha) = \text{o iésimo elemento da tupla } \alpha = \alpha_i$$

(a) π é injetora?

(b) π é sobrejetora?

18/04/2018 (Jp)

Exercício 3.85. Prove que:

- $f : A \to B$ é injetora sse existe $g : B \to A$ tal que $g \circ f = id_A$
- $g : B \to A$ é sobrejetora sse existe $f : A \to B$ tal que $g \circ f = id_A$

Exercício 3.86. Mostre que o morfismo identidade id_A de uma dada Σ-álgebra $\mathcal{A} = \langle A, \cdot_{\mathcal{A}} \rangle$ é um Σ-homomorfismo.

19/04/2018 (Bianca)

Nas questões 3.87 a 3.89, sejam A, B, C conjuntos e sejam $f : A \to B$ e $g : B \to C$ funções.

Exercício 3.87. Prove que se $g \circ f$ é injetiva, então f é injetiva.

Exercício 3.88. Prove que se $g \circ f$ é sobrejetiva, então f é sobrejetiva.

Exercício 3.89. As questões 3.87 e 3.88, juntas, nos dizem que se $g \circ f$ é bijetiva, então f é injetiva e g é sobrejetiva. A recíproca dessa proposição é verdade? Se f é injetiva e g sobrejetiva, a $g \circ f$ é bijetiva?

Exercício 3.90. Sejam $f : A \to B$ e $g : B \to A$ funções. Suponha que $y = f(x)$ sse $x = g(y)$. Prove que f é bijetiva, e $g = f^{-1}$.

Exercício 3.91. Para toda $f : X \to Y$, e todos $A, B \subseteq Y$,

(a) $f^{-1}[A \cup B] = f^{-1}[A] \cup f^{-1}[B]$

(b) $f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$

(c) $f^{-1}[A \setminus B] = f^{-1}[A] \setminus f^{-1}[B]$

Exercício 3.92. Para toda $f : X \to Y$ e todas as sequências de conjuntos $A_n \subseteq X$, $B_n \subseteq Y$,

(a) $f^{-1}[\bigcup_{n=0}^{\infty} B_n] = \bigcup_{n=0}^{\infty} f^{-1}[B_n]$

(b) $f^{-1}[\bigcap_{n=0}^{\infty} B_n] = \bigcap_{n=0}^{\infty} f^{-1}[B_n]$

(c) $f[\bigcup_{n=0}^{\infty} A_n] = \bigcup_{n=0}^{\infty} f[A_n]$

23/04/2018 (Jp)

Definição 3.93. Dada $f : A \to B$, chamamos de **núcleo** de f a relação $=_f$ definida por $x =_f y$ sse $f(x) = f(y)$.

Exercício 3.94. Mostre que, para toda função f, seu núcleo é uma relação de equivalência.

Exercício 3.95. Caracterize as classes de equivalência dos núcleos das funções abaixo:

- $g : \mathbb{Z} \to \mathbb{Z}$; $g(x) = x^2$
- $h : P \to P$ onde P é o conjunto das pessoas; $h(x) =$ o pai de x

Exercício 3.96. Seja f uma função injetiva. O que podemos dizer do núcleo de f?

Exercício 3.97. Dado $k > 2$ natural, definimos $mod_k : \mathbb{N} \to \mathbb{N}$ tal que $mod_k(n) = n \mod k$. Como podemos caracterizar o núcleo de mod_k?

25/04/2018 (Jp)

Exercício 3.98. Para cada relação, determine quais das propriedades abaixo são satisfeitas

- reflexividade
- simetria
- transitividade
- assimetria
- antissimetria
- irreflexividade
- ciclicidade

(a) $F : \mathbf{Rel}(P, P)$, onde P é o conjunto das pessoas, e $F(x, y)$ sse x é pai de y.

(b) $D : \mathbf{Rel}(\mathbb{N}, \mathbb{N})$, onde $D(m, n)$ sse m divide n.

(c) $I : \mathbf{Rel}(Prop, Prop)$, onde $Prop$ é o conjunto das proposições, e $I(p, q)$ sse p implica q.

(d) $R : \mathbf{Rel}(\mathbb{R}^2, \mathbb{R}^2)$, onde $R(p, q)$ sse p é o reflexo de q pelo eixo y.

Exercício 3.99. É possível uma relação binária ser simétrica e assimétrica ao mesmo tempo? Prove ou refute.

Exercício 3.100. Dado $\varepsilon \in (0, 1)$, definimos a relação $\sim_\varepsilon$ tal que $x \sim_\varepsilon y$ sse $|x - y| < \varepsilon$. Essa relação é reflexiva? Simétrica? Transitiva?

26/04/2018 (Bianca)

Exercício 3.101. Proposição: Seja $X \neq \emptyset$ e $\sim$ uma relação no X. Se $\sim$ é simétrica e transitiva, então ela é reflexiva.

Prova: Como ela é simétrica, de $x \sim y$, concluímos que $y \sim x$ também. Usando a transitivdade, de $x \sim y$ e $y \sim x$, concluímos a $x \sim y$, que mostra que $\sim$ é reflexiva também.

Ache o erro na prova acima e prove que a proposição é falsa.

Exercício 3.102. Seja R uma relação binária num conjunto A. O.s.s.e.:

(i) R é uma relação de equivalência;

(ii) R é reflexiva e circular;

(iii) R é reflexiva e left-euclidean;

(iv) R é reflexiva e right-euclidean.

Exercício 3.103. Sejam $\sim$ uma relação de equivalência num conjunto X, e $x, y \in X$. O.s.s.e.:

(i) $x \sim y$

(ii) $[x] = [y]$

(iii) $[x] \cap [y] \neq \emptyset$

03/05/2018 (Bianca)

Exercício 3.104. Se uma nova adição para números reais, denotada pelo símbolo temporário $\boxplus$, é definida por

$$\alpha \boxplus \beta = 2\alpha + 2\beta,$$

ela é comutativa? É associativa?

Exercício 3.105. Se uma nova adição para números reais, denotada pelo símbolo temporário $\boxplus$, é definida por

$$\alpha \boxplus \beta = 2\alpha + \beta,$$

ela é comutativa? É associativa?

Exercício 3.106. Se uma operação para inteiros positivos, denotada pelo símbolo temporário $*$, é definida por

$$\alpha * \beta = \alpha^{\beta},$$

ela é comutativa? É associativa?

Exercício 3.107. Cada uma das seguintes é uma operação $*$ em $\mathbb{R}$. Indique se:

- $*$ é comutativa;
- $*$ é associativa;
- $\mathbb{R}$ tem um elemento identidade com respeito a $*$;
- todo $x \in \mathbb{R}$ tem uma inversa com respeito a $*$.

(a) $x * y = x + y + 1$

(b) $x * y = x + 2y + 4$

(c) $x * y = |x - y|$

Exercício 3.108. Seja $*$ uma operação definida por

$$(a, b) * (c, d) = (ac, bc + d)$$

no conjunto $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \neq 0\}$. Proceda como no exercício anterior.

08/05/2018 (Bianca)

Exercício 3.109. Sejam a, b, c e x elementos de um grupo G. Em cada um dos seguintes, encontre o valor de x em termos de a, b e c.

(i) $axb = c$

(ii) $x^2b = xa^{-1}c$

Exercício 3.110. Se a e b estão em G e $ab = ba$, dizemos que a e b comutam. Supondo que a e b comutam, prove os seguintes.

(i) $a^{-`}$ e b^{-1} comutam.

(ii) a e b^{-1} comutam.

(iii) a comuta com ab.

(iv) xax^{-1} comuta com xbx^{-1}, para qualquer $x \in G$.

Exercício 3.111. Se G é um grupo e a, b são elementos de G, mostre que $(ab)^{-1} = b^{-1}a^{-!}$.

Exercício 3.112. Sejam G grupo, e $a, b \in G$. Prove os seguintes.

(i) $(bab^{-1})^n = ba^nb^{-1}$, para todo $n \in \mathbb{N}$.

(ii) Se $ab = ba$, então $(ab)^n = a^nb^n$, para todo $n \in \mathbb{N}$.

(iii) Se $xax = e$, então $(xa)^{2n} = a^n$.

10/05/2018 (Bianca)

Exercício 3.113. Seja A um conjunto. Mostre que $\wp A$ com a operação $\triangle$ é um grupo.

Exercício 3.114. Sejam $B = \{2^m \mid m \in \mathbb{Z}\}$ e $B_0 = B \cup \{0\}$. Considere os conjuntos estruturados

(i) $\langle B\ ;\ + \rangle$

(ii) $\langle B\ ;\ \cdot \rangle$

(iii) $\langle B_0\ ;\ + \rangle$

(iv) $\langle B_0\ ;\ \cdot \rangle$

Para cada um deles, decida se satisfaz cada uma das leis $\langle G0 \rangle - \langle G3 \rangle$.

Exercício 3.115. Sejam G grupo, a, b, c elementos de G e e o elemento neutro de G.

(i) Prove que se $ab = e$, então $ba = e$.

(ii) Sejam a, b iguais aos seus próprios inversos. Prove que ba é o inverso de ab.

Exercício 3.116. Se G e H são dois grupos, seu produto direto é denotado por $G \times H$, e definido da seguinte forma: $G \times H$ consiste em todos os pares ordenados (x, y) onde $x \in G$ e $y \in H$. Ou seja,

$$G \times H = \{(x, y) \mid x \in G \text{ e } y \in H\}$$

A operação $G \times H$ consiste na multiplicação de elementos correspondentes:

$$(x, y) \cdot (x', y') = (x \cdot x', y \cdot y')$$

Prove que $G \times H$ é um grupo.

15/05/2018 (Bianca)

Exercício 3.117. Seja a elemento de um grupo G. Prove os seguintes:

(i) $o(a) = 1$ sse $a = e$.

(ii) Se $o(a) = n$, então $a^{n-r} = (a^r)^{-1}$.

(iii) A ordem de a^{-1} é a mesma que a ordem de a.

Exercício 3.118. Sejam G grupo, $a \in G$ e $m \in \mathbb{Z}$. Prove que

$$a^m = e \iff o(a) \mid m$$

onde $o(a)$ denota a ordem de a no G.

Exercício 3.119. Seja a elemento de ordem finita de um grupo G. Prove os seguintes:

(i) Se $a^k = e$, onde k é ímpar, então a ordem de a é ímpar.

(ii) Se $a^p = e$, onde p é um número primo, então a tem ordem p ($a \neq e$).

(iii) A ordem de a^k é um divisor da ordem de a.

(iv) Se $o(a) = km$, então $o(a^k) = m$.

22/05/2018 (Bianca)

Exercício 3.120. Mostre que $\leq$ é uma relação de ordem:

(1) $G \leq G$

(2) $K \leq H \ \ \& \ \ H \leq G \implies K \leq G$

(3) $H \leq G \ \ \& \ \ G \leq H \implies H = G$

Exercício 3.121. Nos próximos exercícios, seja G um grupo abeliano.

(i) Se $H = \left\{x \in G \mid x = x^{-1}\right\}$, isto é, H consiste em todos os elementos de G que são seus próprios inversos, prove que H é um subgrupo de G.

(ii) Seja n um inteiro fixo, e seja $H = \{x \in G \mid x^n = e\}$. Prove que H é um subgrupo de G.

(iii) Suponha que H e K são subgrupos de G, e defina HK da seguinte maneira:

$$HK = \{hk \mid h \in H \text{ e } k \in K\}$$

Prove que HK é um subgrupo de G.

Exercício 3.122. O centro de um grupo é o conjunto de todos os elementos de G que comutam como todo elemento de G, isto é,

$$C = \{c \in G \mid cg = gc \text{ para todo } g \in G\}$$

Prove que C é um subgrupo de G.

24/05/2018 (Bianca)

Exercício 3.123. Se G é um grupo de ordem n, G é cíclico sse G tem um elemento de ordem n.

Exercício 3.124. Todo subgrupo cíclico é abeliano.

Exercício 3.125. Seja G grupo e sejam $a, b \in G$. Prove que se a é uma potência de b, isto é, $a = b^k$, então $\langle a \rangle \subseteq \langle b \rangle$.

Exercício 3.126. Seja G grupo e $\emptyset \neq H \subseteq G$. Prove que

$$H \leq G \iff (\forall a, b \in H)[ab^{-1} \in H]$$

Exercício 3.127. Seja G grupo e $H \leq G$. Defina:

$$a \sim b \overset{\text{def}}{\iff} ab^{-1} \in H$$

(i) Prove que $\sim$ é uma relação de equivalência.

(ii) Prove que para todo $a, b \in G$

(a) Se $a \in H$ e $b \in H$, então $a \sim b$.

(b) Se $a \in H$ e $b \notin H$, então $a \not\sim b$.

29/05/2018 (Bianca)

Exercício 3.128. Seja G grupo e $H, K \leq G$. Prove que:

$$HK = KH \iff HK \leq G$$

Exercício 3.129. Seja G um grupo finito. Prove os seguintes:

1. Se G tem ordem n, então $x^n = e$ para todo $x \in G$.
2. Seja $o(G) = pq$ onde p, q são primos. Ou G é cíclico, ou todo elemento $x \neq e$ em G tem ordem p ou q.

05/06/2018 (Bianca)

Exercício 3.130. Prove que todo subgrupo de um grupo abeliano é normal.

Exercício 3.131. Prove que o centro de qualquer grupo G é um subgrupo normal de G.

Exercício 3.132. Seja G um grupo arbitrário e $H \leq G$. Mostre que H é normal sse ele tem a seguinte propriedade:
Para todo $a, b \in G$, $a, b \in H$ sse $ba \in G$

Exercício 3.133. Se $H \leq G$ e $N \trianglelefteq G$, então $H \cap N \trianglelefteq H$.

14/06/2018 (Bianca)

Exercício 3.134. Seja $\langle R; 0; +; \cdot \rangle$ anel. Prove que:

(i) $0x = 0 = x0$

(ii) $(-x)y = -(xy) = x(-y)$

(iii) $(-x)(-y) = xy$

Exercício 3.135. Um anel $\langle B; 0; +; \cdot \rangle$ com unidade é booleano sse $p^2 = p$ para todo $p \in B$. Prove que:

(i) $p + p = 0$ para todo $p \in B$. (Dica: calcule o $(p + q)^2$)

(ii) B é um anel comutativo.

Definição 3.136 (Domínio de integridade)**.** Um anel comutativo D tal que para todo $x, y \in D$,

$$\text{se } xy = 0, \text{ então } x = 0 \text{ ou } y = 0 \quad (NZD)$$

é chamado domínio de integridade.

Definição 3.137 (Domínio de cancelamento)**.** Um anel comutativo D tal que para todo $a, x, y \in D$,

$$ax = ay \ \& \ a \neq 0 \implies x = y \quad (CL)$$

é chamado domínio de cancelamento.

Exercício 3.138. Mostre que:

D é um domínio de integridade $\iff$ D é um domínio de cancelamento.

19/06/2018 (Bianca)

Exercício 3.139. Mostre que $<_c$ é

(i) irreflexiva

(ii) transitiva

Exercício 3.140. Mostre que $A \leq_c B \iff (\exists f)[f : A \rightarrowtail B]$.

Exercício 3.141. Mostre que se $A =_c B$, então $\wp A =_c \wp B$.

21/06/2018 (Bianca)

Exercício 3.142. Mostre que A é contável sse $A \leq_c \mathbb{N}$.

Exercício 3.143. Mostre que A é contável sse $A = \emptyset$ ou A tem uma enumeração, isto é, uma sobrejeção $g : \mathbb{N} \twoheadrightarrow A$.

26/06/2018 (Bianca)

Exercício 3.144. Se A é contável e existe uma injeção $f : B \rightarrowtail A$, então B também é contável; em particular, todo subconjunto de um conjunto contável é contável.

Exercício 3.145. Se A é contável e existe uma sobrejeção $f : A \twoheadrightarrow B$, então B é contável.

Exercício 3.146. Sejam a, b conjuntos. Mostre que $\{b, \{\emptyset, \{a\}\}\}$ é conjunto.

Exercício 3.147. Sejam a, b, c, d conjuntos. Mostre pelos axiomas que os seguintes também são:

$$A = \{a, b, c, d\}$$
$$B = \{a, b, \{c, d\}\}$$
$$C = \{x \mid x \subseteq a \cup b \cup c \cup d \ \& \ x \text{ tem exatamente 2 membros}\}.$$

Exercício 3.148. Dado um conjunto a, justifique (usando os axiomas de ZF) a existência do conjunto $\{\{x\} \mid x \in a\}$.

Exercício 3.149. Considere o axioma seguinte:

$$\forall h \forall t \exists s \forall x (x \in s \leftrightarrow x = h \vee x \in t) \quad \text{(ZF3*)}$$

No sistema ZF1+ZF2+ZF3*, prove o ZF3 como teorema.

4 2018.2

09/08/2018 (Bianca)

Definição 4.1 (Adição)**.** A função de adição nos números naturais é definida pela recursão

$$n + 0 = n, \qquad \text{(a1)}$$
$$n + (Sm) = S(n + m). \quad \text{(a2)}$$

Exercício 4.2. Prove que adição é associativa, ou seja, satisfaz a identidade

$$(a + b) + c = a + (b + c).$$

Exercício 4.3. Prove que adição é comutativa, ou seja, satisfaz a identidade

$$a + b = b + a.$$

Exercício 4.4. O que as afirmações seguintes significam? Elas são verdadeiras ou falsas? (O universo é $\mathbb{N}$).

(a) $\forall x \exists y (x < y)$

(b) $\exists y \forall x (x < y)$

(c) $\exists x \forall y (x < y)$

(d) $\forall y \exists x (x < y)$

(e) $\exists x \exists y (x < y)$

(f) $\forall x \forall y (x < y)$

09/08/2018 (Giordano)

Exercício 4.5. Demonstre que para quaisquer inteiros a e b, valem

(i) $0 \mid a$

(ii) $a \mid a$

Exercício 4.6. Demonstre que para qualquer inteiro n, vale que n é par se e somente se n^2 é par.

10/08/2018 (Jplinha)

Exercício 4.7. Traduza as seguintes frases para fórmulas de lógicas.

a) João foi ao supermercado, ou ficaremos sem ovos.

b) Joel vai sair de casa e não voltará.

Exercício 4.8. Traduza para frases em português as seguintas fórmulas de lógica.

a) $(\neg s \wedge l) \vee s$, onde $s :=$ "Giordano é burro"e $l :=$ "Giordano é preguiçoso".

b) $\neg s \wedge (l \vee s)$, onde s e l tem a mesma definição.

c) $\neg(s \wedge l) \vee s$, onde s e l tem a mesma definição.

Exercício 4.9. Analise as fórmulas lógicas nas seguintes afirmações.

a) Vamos ter um livro para ler ou tarefa para casa, mas não vamos ter tarefas para casa e uma prova.

b) Você não vai esquiar, ou você vai e não terá neve.

c) $\sqrt{7} \nleq 2$

Exercício 4.10. Mostre que

(i) $p \wedge (p \vee q) \iff p$

(ii) $p \vee (p \wedge q) \iff p$

14/08/2018 (Josenaldo)

Definição 4.11 (divisibilidade natural)**.** Sejam $a, b \in \mathbb{N}^*$. Dizemos que a *divide* b quando existe $n \in \mathbb{N}^*$ tal que $a \cdot n = b$, e denotamos esse fato por $a \mid b$.

Exercício 4.12. Mostre que se o dígito das unidades de um número natural é par, então o próprio número também o é.

Exercício 4.13. Prove ou refute as seguintes afirmações:

(i) $(\exists x \in \mathbb{N}^*)(\forall y \in \mathbb{N}^*)[y \mid x]$

(ii) $(\forall x \in \mathbb{N}^*)(\exists y \in \mathbb{N}^*)[y \mid x]$

Homework 4.1. Prove ou refute as seguintes afirmações:

(i) $(\exists x \in \mathbb{N}^*)(\forall y \in \mathbb{N}^*)[x \mid y]$

(ii) $(\forall x \in \mathbb{N}^*)(\exists y \in \mathbb{N}^*)[x \mid y]$

14/08/2018 (Jplinha)

Definição 4.14 (Naturais)**.** Definimos o conjunto dos naturais recursivamente, usando a notação BNF, da seguinte forma:

$$\langle \mathbf{Nat} \rangle \ ::= \ 0 \mid S \ \langle \mathbf{Nat} \rangle$$

Exercício 4.15. Defina a operação de adição sobre o $\langle \mathbf{Nat} \rangle$ definido acima.

Exercício 4.16. Mostre que a adição sobre o $\langle \mathbf{Nat} \rangle$ do exercício anterior é associativa. Ou seja, para todos a, b, c naturais, $a + (b + c) = (a + b) + c$.

Homework 4.2. Mostre que a adição sobre o ⟨**Nat**⟩ é comutativa. Ou seja, para todos m, n naturais, $m + n = n + m$.

Homework 4.3. Ainda sobre o ⟨**Nat**⟩, defina a operação de multiplicação e tente provar sua distributividade, associatividade e comutatividade.

16/08/2018 (Bianca)

Exercício 4.17. Prove que a relação $\mid$ é uma ordem parcial no $\mathbb{N}$.

Exercício 4.18. Prove que para todo $n \in \mathbb{Z}$, se $3 \nmid n$, então $3 \mid n^2 - 1$.

Exercício 4.19. Os números Fibonacci são definidos recursivamente assim:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n \end{aligned}$$

Prove que para todo $n \in \mathbb{N}$,

$$\sum_{i=0}^{n} F_i = F_{n+2} - 1.$$

Homework 4.4. Prove que $\bullet \equiv \bullet \pmod{m}$ é uma relação de equivalência nos inteiros.

16/08/2018 (Giordano)

Exercício 4.20. Prove que para todo $n \in \mathbb{N}$, $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Exercício 4.21. Prove que para todo $n \in \mathbb{N}$, se $n \geq 4$, então $n^2 \leq 2^n$

16/08/2018 (Jplinha)

Definição 4.22 (Adição sobre ⟨**Nat**⟩)**.** Definimos a operação de adição sobre o ⟨**Nat**⟩, definido anteriormente, da seguinte forma:

$$n + 0 = n \tag{a1}$$
$$n + Sm = S(n + m) \tag{a2}$$

Exercício 4.23. Prove que a adição sobre $\langle \mathbf{Nat} \rangle$ é comutativa, isto é

$$(\forall n, m \in \langle \mathbf{Nat} \rangle)[n + m = m + n]$$

Homework 4.5.

Definição 4.24 (Multiplicação sobre $\langle \mathbf{Nat} \rangle$)**.** Definimos a operação de multiplicação sobre o $\langle \mathbf{Nat} \rangle$ através das seguintes equações:

$$n \cdot 0 = n \tag{m1}$$
$$n \cdot Sm = S(n \cdot m) + n \tag{m2}$$

Dado a definição de multiplicação sobre $\langle \mathbf{Nat} \rangle$ acima, prove que ela é

(i) Distributiva

(ii) Associativa

(iii) Comutativa

17/08/2018 (Jplinha)

Definição 4.25 (Multiplicação sobre $\langle \mathbf{Nat} \rangle$)**.** Definimos a operação de multiplicação sobre o $\langle \mathbf{Nat} \rangle$ através das seguintes equações:

$$n \cdot 0 = n \tag{m1}$$
$$n \cdot Sm = S(n \cdot m) + n \tag{m2}$$

Exercício 4.26. Mostre que a multiplicação como definida acima é

(i) Distributiva

(ii) Associativa

(iii) Comutativa

Homework 4.6 (Lema α)**.** Prove que

$$(\forall m \in \langle \mathbf{Nat} \rangle)[0 \cdot m = 0]$$

Homework 4.7 (Lema β)**.** Prove que

$$(\forall n, m \in \langle \mathbf{Nat} \rangle)[Sn \cdot m = (n \cdot m) + m]$$

21/08/2018 (Bianca)

Exercício 4.27. Suponha que A, B e C são conjuntos. Então

$$A \cap (B \setminus C) = (A \cap B) \setminus C.$$

Exercício 4.28. Suponha que A, B e C são conjuntos. Prove que se $A \subseteq C$ e $B \subseteq C$, então

$$A \cup B \subseteq C.$$

Exercício 4.29. Suponha que $A \subseteq B$, e A e C são disjuntos. Prove que

$$A \subseteq B \setminus C.$$

Exercício 4.30. Para quaisquer três conjuntos A, B, C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Homework 4.8. Mostre que para quaisquer três conjuntos A, B, C,

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Homework 4.9. Suponha que A, B, C são conjuntos. Prove que se $A \subseteq C$ e $B \subseteq C$, então

$$A \cup B \subseteq C.$$

23/08/2018 (Bianca)

Definição 4.31 (Multiplicação)**.** A função de multiplicação nos números naturais é definida pela recursão

$$\begin{aligned} n \cdot 0 &= 0, && \text{(m1)} \\ n \cdot Sm &= (n \cdot m) + n. && \text{(m2)} \end{aligned}$$

Exercício 4.32. Mostre que a multiplicação é associativa, ou seja, que para todos $a, b, c \in \mathbb{N}$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Exercício 4.33. Mostre que a multiplicação é comutativa, ou seja, que para todos $a, b \in \mathbb{N}$,

$$a \cdot b = b \cdot a$$

24/08/2018 (Jplinha)

Exercício 4.34. Prove que

$$\forall x(x \cdot S0 = x = S0 \cdot x) \ (id*)$$

Exercício 4.35. Defina a exponenciação nos $\mathbb{N}$ recursivamente.

Exercício 4.36. Dado a definição da questão anterior, prove que

1. $\forall x \forall a \forall b(x^{a+b} = x^a + x^b)$
2. $\forall x \forall a \forall b(x^{a \cdot b} = (x^a)^b)$

Definição 4.37 ($\leq$ no $\mathbb{N}$)**.** Definimos a relação $\leq$ assim:

$$n \leq m \iff (\exists k \in \mathbb{N})[n + k = m]$$

Exercício 4.38. Prove que

$$\forall n \forall m(n \leq Sm \iff n \leq moun = Sm)$$

28/08/2018 (Bianca)

Exercício 4.39. Para quaisquer conjuntos A, B, C,

$$A \setminus (A \cap B) = A \setminus B.$$

Exercício 4.40. Para quaisquer conjuntos A, B, C,

(i) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$

(ii) $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$.

Exercício 4.41. Prove ou refute a afirmação:

Para todos os conjuntos A, B, C se $A \subseteq B$ e $A \subseteq C$, então $A \subseteq B \cap C$.

Homework 4.10. Prove ou refute a afirmação:

Para todos os conjuntos A, B, C, se $A \subsetneq B$ e $A \subsetneq C$, então $A \subsetneq B \cap C$.

30/08/2018 (Bianca)

Exercício 4.42. Para qualquer conjunto C e qualquer sequência de conjuntos $\{A_n \mid n \in \mathbb{N}\}$:

(i) $C \setminus (\bigcup_{n=0}^{\infty} A_n) = \bigcap_{n=0}^{\infty}(C \setminus A_n)$

(ii) $C \setminus (\bigcap_{n=0}^{\infty} A_n) = \bigcup_{n=0}^{\infty}(C \setminus A_n)$

Exercício 4.43. Sejam $\mathcal{A}, \mathcal{B}$ famílias de conjuntos com $\mathcal{A} \cap \mathcal{B} \neq \emptyset$. Prove ou refute a afirmação

$$\bigcap \mathcal{A} \subseteq \bigcup \mathcal{B}.$$

Exercício 4.44. Sejam A, B, C conjuntos. Mostre que

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

Exercício 4.45. Prove que se $(A \times B) \cap (C \times D) = \emptyset$, então $A \cap C = \emptyset$ ou $B \cap D = \emptyset$.

30/08/2018 (Giordano)

Exercício 4.46. Seja A conjunto, prove que

a) $\emptyset \subseteq A$

b) $A \subseteq A$

Exercício 4.47. Sejam A e B conjuntos, prove que

$$A \cup B = B \iff A \subseteq B \iff A \cap B = A$$

30/08/2018 (Jplinha)

Exercício 4.48. Sejam $n \in \mathbb{N}$ com $n \geq 2$ e n conjuntos $A_1, A_2, \ldots, A_n$. Seja

$$A := A_1 \triangle A_2 \triangle \ldots \triangle A_n$$

Observe que como a operação $\triangle$ é associativa e comutativa, o A é bem definido. Prove que:

$$A = \{a \mid a \text{ pertence numa quantidade ímpar de } A_i\text{'s}\}.$$

31/08/2018 (Jplinha)

Exercício 4.49. Sejam $\{A_n\}_n$ e $\{B_n\}_n$ duas sequências de conjuntos t.q.

$$\text{para todo número par } m, A_m \subseteq B_{m/2}$$

Exercício 4.50. Prove que

$$C \setminus \bigcap_{n=0}^{\infty} A_n = \bigcap_{n=0}^{\infty} (C \setminus A_n)$$

04/09/2018 (Bianca)

Exercício 4.51. Sejam I, J conjuntos de índices e para cada $k \in I \cup J$. Seja A_k um conjunto. A afirmação

$$\bigcup_{k \in I \cap J} A_k = \bigcup_{k \in I} A_k \cap \bigcup_{k \in J} A_k$$

é verdadeira? Responda... (1) "sim", e prove; (2) "não"e refute; ou (3) "depende", e demonstre dois exemplos, um onde a afirmação é verdadeira, e outro onde não é.

Exercício 4.52. Sejam A, B conjuntos diferentes, e $f : A \to B$. Para cada uma das igualdades, decida se ela é válida ou não, justificando sua resposta.

(1) $f = f \circ \mathrm{id}_A$

(2) $f = f \circ \mathrm{id}_B$

(3) $f = \mathrm{id}_A \circ f$

(4) $f = \mathrm{id}_B \circ f$

04/09/2018 (Josenaldo)

Exercício 4.53. Sejam A, B conjuntos. Prove que $\wp(A \cup B) = \wp(A) \cup \wp(B)$ implica que $A \subseteq B$ ou $B \subseteq A$.

06/09/2018 (Giordano)

Exercício 4.54. Prove que para todos $a, b, c \in \mathbb{N}$, se $a \mid b$ e $a \mid c$, então $a \mid bx + cy$ para quaisquer $x, y \in \mathbb{Z}$

Exercício 4.55. Prove que para todo $n \in \mathbb{N}$, vale $3 \nmid 2n + 3$

Exercício 4.56. Sejam $a, b, c \in \mathbb{N}$, prove que

$$a \mid b \ \& \ a \nmid c \implies a \nmid b + c$$

Exercício 4.57. Sejam $f : A \to B$ e $g : B \to C$, prove que

(i) f, g injetivas $\implies$ $g \circ f$ injetiva

(ii) f, g sobrejetivas $\implies$ $g \circ f$ sobrejetiva

Exercício 4.58. Defina uma $f : \mathbb{N} \to \mathbb{Z}$ função bijetiva, isto é, prove que sua definição realmente define uma função, e que é bijetiva.

06/09/2018 (Jplinha)

Exercício 4.59. Prove ou refute: Para todo conjunto A e toda sequência de conjuntos $\{B_n\}_n$

$$A \cup \bigcap_{n=0}^{\infty} B_n = \bigcap_{n=0}^{\infty} (A \cup B_n)$$

Exercício 4.60. Sejam I, J conjuntos de índices e para cada $k \in I \cup J$ seja A_k um conjunto. Prove ou refute:

$$\bigcup_{k \in I \cap J} A_k = \bigcup_{k \in I} A_k \cap \bigcup_{k \in J} A_k$$

11/09/2018 (Bianca)

Exercício 4.61. Sejam $f : A \to B$, $h : B \to A$. Suponha que f tem inversa. Mostre que f satisfaz as duas leis de cancelamento.

(a) Se $f \circ h = f \circ k$, então $h = k$

(b) Se $h \circ f = k \circ f$, então $h = k$

Exercício 4.62. Sejam $A \neq \emptyset$ um conjunto e $f : A \to \mathcal{P}A$ definida pela equação:

$$f(a) = \{a\}$$

(a) f é injetora?

(b) f é sobrejetora?

Exercício 4.63. Mostre que se f tem uma inversa, então ela é única.

11/09/2018 (Josenaldo)

Exercício 4.64. Seja $f : A \to B$ injetiva. Prove que, para todo $Y \subseteq B$ unitário, o conjunto $f^{-1}[Y]$ tem menos de dois elementos.

Homework 4.11. No Exercício 4.64, prove que, se f é sobrejetiva, então $f^{-1}[Y] \neq \emptyset$. Conclua que f ser bijetiva e Y ser unitário implicam que $f^{-1}[Y]$ é unitário.

13/09/2018 (Bianca)

Exercício 4.65. Se $f : X \to Y$ e $A, B \subseteq X$, então

$$f[A \cup B] = f[A] \cup f[B].$$

Exercício 4.66. Para toda $f : X \to Y$, e todos $A, B \subseteq Y$,

$$f^{-1}[A \setminus B] = f^{-1}[A] \setminus f^{-1}[B].$$

Exercício 4.67. Sejam $f : X \rightarrowtail Y$ e $A, B \subseteq X$. Mostre que

$$f[A \setminus B] = f[A] \setminus f[B].$$

Exercício 4.68. Para toda $f : X \to Y$ e todas as sequências de conjuntos $A_n \subseteq X$, $B_n \subseteq Y$,

(a) $f^{-1}[\bigcup_{n=0}^{\infty} B_n] = \bigcup_{n=0}^{\infty} f^{-1}[B_n]$

(b) $f^{-1}[\bigcap_{n=0}^{\infty} B_n] = \bigcap_{n=0}^{\infty} f^{-1}[B_n]$

(c) $f[\bigcup_{n=0}^{\infty} A_n] = \bigcup_{n=0}^{\infty} f[A_n]$

13/09/2018 (Giordano)

Exercício 4.69. Seja $f : A \rightarrowtail B$, defina a $f^{-1} : B \to A$ pela

$$f^{-1}(y) = x \overset{\text{def}}{\iff} f(x) = y.$$

Prove que a f^{-1} é função com esta definição, em seguida, prove sua bijetividade.

13/09/2018 (Jplinha)

Exercício 4.70. Seja $f : X \to Y$. Prove que

1) f injetiva $\iff$ para todo $A \subseteq X, A = f^{-1}[f[A]]$

2) f sobrejetiva $\iff$ para todo $B \subseteq Y, B = f[f^{-1}[B]]$

Exercício 4.71. Defina as funções f e g com os seguintes tipos

$$f : A \rightarrowtail \wp A$$
$$g : \wp A \twoheadrightarrow A$$

14/09/2018 (Jplinha)

Exercício 4.72. Defina as funções f e g com os seguintes tipos

$$f : A \rightarrowtail \wp A$$
$$g : \wp A \twoheadrightarrow A$$

Sabendo que $A \neq \emptyset$, prove as seguintes afirmações:

(i) A f é injetiva.

(ii) A f não é sobrejetiva.

(iii) A g é sobrejetiva.

(iv) A g não é injetiva.

Exercício 4.73. Sejam $f : A \to A$. O $x \in A$ é um *fixpoint* (ponto fixo) da f sse $f(x) = x$. Seja F o conjunto de todos os *fixpoints* de f definido abaixo

$$F = \{x \in A \mid x \text{ é um fixpoint da } f\}$$

Prove a (i) e refute a (ii)

(i) $F \subseteq f^{-1}[F]$

(ii) $f^{-1}[F] \subseteq F$

Agora, supondo que f é injetiva, prove a (ii).

Exercício 4.74. Sejam $f : A \to B$, e duas famílias indexadas de conjuntos $(A_i)_{i\in I}$ feita por subconjuntos de A e $(B_j)_{j\in J}$ feita de subconjuntos de B. Ou seja, para todo $i \in I$, e para todo $j \in J$, temos $A_i \subseteq A$ e $B_j \subseteq B$. Mostre que

(1) $f[\bigcup_{i\in I} A_i] = \bigcup_{i\in I} f[A_i]$

(2) $f[\bigcap_{i\in I} A_i] \stackrel{?}{=} \bigcap_{i\in I} f[A_i]$

(3) $f^{-1}[\bigcup_{j\in J} B_j] = \bigcup_{j\in J} f^{-1}[B_j]$

(4) $f^{-1}[\bigcap_{j\in J} B_j] = \bigcap_{j\in J} f^{-1}[B_j]$

Onde aparece $\stackrel{?}{=}$ prove que a igualdade em geral não é válida, mas umas das $(\subseteq)$ e $(\supseteq)$ é. Prove-a, e, supondo que f é injetora, prove a outra também.

18/09/2018 (Bianca)

Exercício 4.75. Sejam $A \neq \emptyset$ um conjunto e $f : A \to \mathcal{P}A$ definida pela equação:

$$f(a) = \{a\}$$

(a) f é injetora?

(b) f é sobrejetora?

Exercício 4.76. Seja S o conjunto de todos os strings não-vazios de um alfabeto Σ, com $|\Sigma| \geq 2$. Considere a função $f : S \times \{0, 1\} \to S$ definida pela:

$$f(w, i) = \begin{cases} ww & \text{, se } i = 0 \\ w' & \text{, se } i = 1 \end{cases}$$

onde w' é o string reverso de w, e onde denotamos a concatenação de strings por justaposição.

(a) f é injetora?

(b) f é sobrejetora?

Exercício 4.77. Verdade ou falso? (Prove sua resposta).

Se $g \circ f$ é constante, então pelo menos uma das f, g também é.

18/09/2018 (Josenaldo)

Exercício 4.78. Sejam A e B conjuntos e $f : A \to B$ bijetiva. Mostre que, para todo $Y \subseteq B$, a imagem de Y pela f^{-1} é igual à pré-imagem de Y pela f. Conclua que o conjunto $f^{-1}[Y]$ é bem-definido.

20/09/2018 (Bianca)

Exercício 4.79. Seja R uma relação binária num conjunto A. O.s.s.e.:

(i) R é uma relação de equivalência;

(ii) R é reflexiva e circular;

(iii) R é reflexiva e left-euclidean.

20/09/2018 (Jplinha)

Exercício 4.80. Sejam B, C, D conjuntos, $g, h : C \to D$ e $f : B \twoheadrightarrow C$. Prove a afirmação

$$g \circ f = h \circ f \implies g = h$$

Exercício 4.81. Seja $f : A \to B$. As afirmações seguintes

(i) f sobrejetiva $\implies$ $f^{-1}[-]$ injetiva

(ii) f sobrejetiva $\impliedby$ $\inf f[-]$ injetiva

são verdadeiras?

Exercício 4.82. Sejam $n \in \mathbb{N}$ e $succ : \mathbb{N} \to \mathbb{N}$ a função *sucessor*. Supondo que o leitor não sabe o que são iterações de uma função, defina a função $succ^n$ de um jeito simples e em seguida prove que as n iterações de $succ$, ou seja, $succ^n$, é igual a função que você definiu.

Homework 4.12. Qual é (a extensão d)o conjunto $\bigcup_{n=0}^{\infty} succ^n[\mathbb{N}]$? Prove sua afirmação.

04/10/2018 (Bianca)

Exercício 4.83. Sejam $\sim$ uma relação de equivalência num conjunto X, e $x, y \in X$. O.s.s.e.:

(i) $x \sim y$

(ii) $[x] = [y]$

(iii) $[x] \cap [y] \neq \emptyset$

Exercício 4.84. Defina no $(\mathbb{N} \to \mathbb{N})$ as relações seguintes:

$$f \overset{\exists\forall}{=} g \iff_{\text{def}} (\exists n \in \mathbb{N})(\forall x \geq n)[f(x) = g(x)]$$
$$f \overset{\forall\exists}{=} g \iff_{\text{def}} (\forall n \in \mathbb{N})(\exists x \geq n)[f(x) = g(x)]$$

Para cada uma das relações acima, decida se ela é relação de equivalência (prove ou refute). Se é, descreva esse conjunto quociente.

04/10/2018 (Giordano)

Exercício 4.85. Prove que para todo natural $n \geq 4$, vale $2^n < n!$.

Exercício 4.86. Prove que se A é um conjunto finito, então $|\wp A| = 2^{|A|}$.

04/10/2018 (Jplinha)

Exercício 4.87. Defina no $\mathbb{Z} \times \mathbb{Z}_{\neq 0}$ a seguinte relação

$$\langle a, b\rangle \approx \langle c, d\rangle \iff_{\text{def}} ad = bc$$

mostre que essa relação é de equivalência e descreva suas classes de equivalência e conjunto quociente.

Exercício 4.88. Dadas as seguintes relações no $(\mathbb{Z} \to \mathbb{Z})$

$$f \sim g \iff_{\text{def}} (\exists u \in \mathbb{Z})(\forall x \in \mathbb{Z})[f(x) = g(x + u)] \tag{1}$$
$$f \approx g \iff_{\text{def}} (\exists u \in \mathbb{N})(\forall x \in \mathbb{Z})[f(x) = g(x + u)] \tag{2}$$
$$f \wr g \iff_{\text{def}} (\exists u \in \mathbb{Z})(\forall x \in \mathbb{Z})[f(x) = g(x) + u] \tag{3}$$
$$f \wr\!\wr g \iff_{\text{def}} (\exists u \in \mathbb{N})(\forall x \in \mathbb{Z})[f(x) = g(x) + u] \tag{4}$$

decida se cada uma é (ir)reflexiva, transitiva ou (a(nti)s)simétrica.

Homework 4.13. Sabendo que a (2) do exercício anterior não é nem simétrica nem antissimétrica, construa contraexemplos que mostrem essa afirmação.

09/10/2018 (Bianca)

Exercício 4.89. Seja R uma preordem num conjunto A. Prove que R é idempotente, ou seja, $R = R \circ R$.

Exercício 4.90. Seja S uma relação binária no $\mathbb{R}$ tal que

$$(S \circ S^{\partial}) \text{ é irreflexiva.}$$

Qual é o gráfico da S? Prove tua resposta.

Exercício 4.91. Defina com texto completo o conjunto quociente.

Exercício 4.92. Defina com texto completo o que é uma partição.

Exercício 4.93. Seja $\sim$ uma relação de equivalência num conjunto A. Prove que o conjunto quociente $A/\sim$ é uma partição de A.

11/10/2018 (Giordano)

Exercício 4.94. Sejam $a, b, c \in \mathbb{N}$, demonstre que

$$a \mid b \ \& \ a \mid c \implies a \mid bx + cy \text{ para quaisquer } x, y \in \mathbb{Z}$$

Definição 4.95 (Máximo Divisor Comum)**.** Considere a, b e $d \in \mathbb{Z}$, defina $mdc(a, b) = d$ se, e somente se:

(i) $d \geq 0$ (não negativo)

(ii) $d \mid a \ \& \ d \mid b$ (divisor comum)

(iii) $(\forall n \in \mathbb{N})[(n \mid a \ \& \ n \mid b) \implies n \mid d]$ (maior em relação à divisibilidade)

Exercício 4.96. Seja $a \in \mathbb{N}$, demonstre que valem os seguintes itens:

(a) $mdc(a, a) = a$

(b) $mdc(0, a) = a$

18/10/2018 (Giordano)

Exercício 4.97 (Divisão de Euclides)**.** Dados inteiros a e b com $b > 0$, demonstre que existem únicos inteiros q e r tais que

$$a = bq + r, \qquad 0 \leq r < b.$$

Dica: Demonstre primeiro a existência no caso $a > 0$.

25/10/2018 (Giordano)

Exercício 4.98 (lema de Bézout)**.** Considere $a, b \in \mathbb{Z}$, demonstre que $mdc(a, b) = ax + by$ para alguns $x, y \in \mathbb{Z}$.

25/10/2018 (Jplinha)

Exercício 4.99. Seja G conjunto e $H \leq G$. Defina no G a relação R pela

$$a \ R \ b \overset{\text{def}}{\iff} ab^{-1} \in H$$

Prove que R é uma relação de equivalência.

Definição 4.100. Dado um grupo G, definimos seu centro $Z(G)$ como o conjunto de todos os membros de G que "comutam com todos os membros de G":

$$Z(G) \overset{\text{def}}{=} \{z \in G \mid \text{para todo } g \in G,\ zg = gz\}$$

Exercício 4.101. Seja G grupo. Dada a definição de $Z(G)$ acima, prova que $Z(G) \leq G$.

26/10/2018 (Josenaldo)

Exercício 4.102. Sejam G grupo e $\emptyset \neq H \subseteq G$. Prove que se $ab^{-1} \in H$ para todos $a, b \in H$, então $H \leq G$.

Exercício 4.103. Prove que se G é um grupo, então, para todos $a, b \in G$,

$$ab = ba \implies ab^{-1} = b^{-1}a$$

Homework 4.14. Prove a conversa do Exercício 4.103.

01/11/2018 (Jplinha)

Exercício 4.104. Sejam $m, a, b \in \mathbb{Z}$. Prove que, se $a \equiv b \pmod{m}$, então para todo $x \in \mathbb{Z}$,

(i) $a + x \equiv b + x \pmod{m}$

(ii) $ax \equiv bx \pmod{m}$

(iii) $-a \equiv -b \pmod{m}$

Exercício 4.105. Sejam $m, a, k \in \mathbb{Z}$ e seja $c \in \mathbb{Z}$ tal que $(c, m) = 1$. Prove que

$$ca \equiv cb \pmod{m} \implies a \equiv b \pmod{m}$$

Exercício 4.106. Sejam G grupo, $a \in G$ e $m \in \mathbb{Z}$. Então $a^m = e \iff o(a) \mid m$.

Exercício 4.107. Sejam G grupo e $a \in G$. Se $o(a) = km$, então $o(a^k) = m$.

Exercício 4.108. Seja G grupo. Prove que para todo $a \in G$, $\langle a \rangle \leq G$.

08/11/2018 (Giordano)

Exercício 4.109. Demonstre que se $a, b, c \in \mathbb{Z}$, então

$$mdc(a, mdc(b, c)) = mdc(a, b, c)$$

Dica: considere $d = mdc(a, b, c)$ e tente provar que d satizfas as condições de ser o mdc de a e $mdc(b, c)$.

16/11/2018 (Josenaldo)

Exercício 4.110. Sejam G grupo e $\varphi : G \to G$ com lei de formação $\varphi(x) = x^2$. Prove que φ é um homomorfismo sse G é abeliano.

Exercício 4.111. Sejam G grupo e $N \trianglelefteq G$. Mostre que existem grupo G' e homomorfismo $\varphi : G \to G'$ tais que $N = \ker \varphi$.

22/11/2018 (Josenaldo)

Exercício 4.112. Sejam G grupo e $a \in G$. Prove, a partir dos axiomas de grupos e sem usar lemas auxiliares, que $\left(a^{-1}\right)^{-1} = a$.

Exercício 4.113. Sejam G e H grupos, $\varphi : G \to H$ homomorfismo e $B \leq H$. Prove que $\varphi^{-1}[B] \leq G$.

Exercício 4.114. Seja F um corpo ordenado. Prove que, para todos $a, b \in F$, exatamente uma das seguintes afirmações é válida:

$$a < b;$$
$$a = b;$$
$$b < a.$$

23/11/2018 (Josenaldo)

Exercício 4.115. Sejam F um corpo ordenado e $a, b \in F$. Mostre que se $ab > 0$, então a e b são ambos negativos ou ambos positivos.

Exercício 4.116. Sejam F um corpo ordenado e $x \in F$. Mostre que se x tem a propriedade de que $0 \leq x < \epsilon$ para todo $\epsilon > 0$, então $x = 0$.

27/11/2018 (Bianca)

Exercício 4.117. Mostre que

$$A \leq_c B \iff (\exists f)[f : A \rightarrowtail B].$$

Exercício 4.118. Mostre que se $A \neq \emptyset$, então:

$$A \leq_c B \iff (\exists g)[g : B \twoheadrightarrow A].$$

30/11/2018 (Josenaldo)

Exercício 4.119. Dado A conjunto, prove que 1 implica 2 e que 2 implica 3.

1. A é contável;
2. $A = \emptyset$ ou existe função sobrejetiva $f : \mathbb{N} \to A$;
3. Existe função injetiva $f : A \to \mathbb{N}$.

07/12/2018 (Josenaldo)

Exercício 4.120. Considere o axioma seguinte:

ZF3* $\forall a \forall b \forall c\,((a \neq b \wedge b \neq c \wedge c \neq a) \rightarrow \exists s \forall x(x \in s \leftrightarrow x = a \vee x = b \vee x = c))$

a) No sistema ZF1+ZF2+ZF3+ZF4+ZF5+ZF6, construa um conjunto de cardinalidade 3.

b) Prove que o ZF3 pode ser substituído pelo ZF3* "sem perder nada"; isto é, prove, no sistema ZF1+ZF2+ZF3*+ZF4+ZF5+ZF6, que se a e b são conjuntos então $\{a, b\}$ também é.

c) O resultado do item anterior permanece válido quando se remove o ZF5 do sistema?

Exercício 4.121. Considere o axioma seguinte:

CONS $\forall h \forall t \exists s \forall x(x \in s \leftrightarrow x = h \vee x \in t)$

a) No sistema ZF1+ZF2+CONS, prove o ZF3 como teorema.

b) Mostre que é impossível provar o CONS no sistema ZF1+ZF2+ZF3.

c) No sistema ZF1+ZF2+ZF3+ZF4+ZF5+ZF6, prove o CONS como teorema.

14/12/2018 (Josenaldo)

Exercício 4.122. Sejam $f : A \rightarrow A$ e $F = \{x \in A : f(x) = x\}$. Mostre que:

a) $f[F] \subseteq F$;

b) $f^{-1}[F] \subseteq F$, se f é injetiva.

Exercício 4.123. Prove que $\mathbb{Q}$ é um conjunto contável.

Exercício 4.124. Prove que, para todo A conjunto, $A <_C \wp A$.

5 2019.1

13/03/2019 (Bianca)

Exercício 5.1. Para quaisquer conjuntos A, B, C,

$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B).$$

Exercício 5.2. Para qualquer conjunto C e qualquer sequência de conjuntos $\{A_n \mid n \in \mathbb{N}\}$:

$$C \setminus (\bigcup_{n=0}^{\infty} A_n) = \bigcap_{n=0}^{\infty} (C \setminus A_n).$$

Exercício 5.3. Para quaisquer conjuntos A, B, C,

$$A \setminus (A \cap B) = A \setminus B.$$

Exercício 5.4. Prove ou refute a afirmação:

Para todos os conjuntos A, B, C se $A \subseteq B$ e $A \subseteq C$, então $A \subseteq B \cap C$.

14/03/2019 (Josenaldo)

Exercício 5.5. Sejam C conjunto e $\mathscr{A}$ uma família de conjuntos tal que todos contêm o C. Prove que $C \subseteq \bigcap \mathscr{A}$.

Exercício 5.6. Sejam $\mathscr{A}$ e $\mathscr{B}$ famílias de conjuntos tais que $\mathscr{A} \cap \mathscr{B} \neq \emptyset$. Prove ou refute:

$$\bigcap \mathscr{A} \subseteq \bigcup \mathscr{B}$$

Exercício 5.7. Seja $\mathscr{A}$ uma família de conjuntos tal que $\bigcup \mathscr{A} = \bigcap \mathscr{A}$. O que se pode concluir a respeito de $\mathscr{A}$?

15/03/2019 (Josenaldo)

Exercício 5.8. Sejam $\{A_n\}_n$ e $\{B_n\}_n$ duas sequências de conjuntos tais que para todo m par, $A_m \subseteq B_m$. Prove que

$$\bigcap_{n=0}^{\infty} A_n \subseteq \bigcap_{n=0}^{\infty} B_n$$

.

Exercício 5.9. Sejam $n \in \mathbb{N}$, com $n \geq 2$, e n conjuntos $A_1, \ldots, A_n$. Além disso, seja $A = A_1 \triangle A_2 \triangle \ldots \triangle A_n$ (observe que, como $\triangle$ é uma operação associativa e comutativa, o conjunto A é bem-definido). Prove que

$$A = \{a \mid a \text{ pertence em uma quantidade ímpar de } A_i\text{'s}\}$$

.

19/03/2019 (Bianca)

Exercício 5.10. Seja $\{A_n\}_n$ uma sequência (infinita) de conjuntos.

(a) Defina recursivamente uma sequência de conjuntos $\{D_n\}_n$ tal que (informalmente):

$$D_k = A_0 \cup A_1 \cup \cdots \cup A_{k-1} \text{ para todo } k \in \mathbb{N}.$$

(b) Demonstre que para todo $n \in \mathbb{N}$:

$$D_n \subseteq \bigcup_{m=0}^{\infty} A_m.$$

Exercício 5.11. Sejam A, B conjuntos diferentes e $f : A \to B$. Para cada uma das igualdades abaixo, decida se ela é válida ou não, justificando sua resposta.

(i) $f = f \circ id_A$

(ii) $f = f \circ id_B$

(iii) $f = id_A \circ f$

(iv) $f = id_B \circ f$

Exercício 5.12. Seja $\mathcal{A}$ uma família de conjuntos tal que

$$\bigcup \mathcal{A} = \bigcap \mathcal{A}$$

O que mais (interessante) podes concluir sobre o $\mathcal{A}$? (Demonstre tua afirmação).

22/03/2019 (Josenaldo)

Definição 5.13. Dados $f : A \to B$ e $x \in A$, x é um ponto fixo de f se $f(x) = x$.

Definição 5.14. Dada $f : A \to A$, definem-se as iterações f^n como:

$$f^0 = id_A$$
$$f^{n+1} = f \circ f^n$$

Exercício 5.15. Sejam $f : A \to A$ e $x \in A$. Prove que:

$$x \text{ é ponto fixo de } f \iff \text{para todo } n \in \mathbb{N},\ x \text{ é ponto fixo de } f^n$$

Exercício 5.16. Seja $f : \mathbb{N} \to \mathbb{N}$. Prove que:

$$f \text{ é sobrejetiva} \iff \text{existe } g : \mathbb{N} \to \mathbb{N} \text{ tal que } f \circ g = id_A$$

26/03/2019 (Bianca)

Exercício 5.17. Prove que a composição de injeções é uma injeção; a composição de sobrejeções é uma sobrejeção; e consequentemente, a composição de bijeções é uma bijeção.

Exercício 5.18. Nas questões seguintes, sejam A, B, C conjuntos e sejam $f : A \to B$ e $g : B \to C$ funções.

(i) Mostre que se $g \circ f$ é injetora, então f é injetora.

(ii) Mostre que se $g \circ f$ é sobrejetora, então f é sobrejetora.

(iii) Questões (i) e (ii), juntas, nos dizem que se $g \circ f$ é bijetora, então f é injetora e g é sobrejetora. A recíproca dessa afirmação é verdadeira?

Exercício 5.19. Sejam $A \neq \emptyset$ conjunto, $n \in \mathbb{N}_{>0}$, e $I = \{i \in \mathbb{N} \mid i < n\}$. Considere a função $\pi : I \times A^n \to A$ definida por:

$$\pi(i, \alpha) = \pi_i(\alpha) \qquad (= \text{o iésimo elemento da tupla } \alpha)$$

(a) π é injetora?

(b) π é sobrejetora?

28/03/2019 (Bianca)

Exercício 5.20. Seja $f : A \to B$. A afirmação

$$f \text{ bijetora} \iff \text{para todo } b \in B,\ f^{-1}[\{b\}] \text{ é um conjunto unitário}$$

é verdadeira? Prove ou refute.

Exercício 5.21. Sejam $f : X \to Y$ e $\{B_n\}_n$ uma sequência de subconjuntos de Y. Prove que:

$$f^{-1}\big[\bigcap_{n=0}^{\infty} B_n\big] = \bigcap_{n=0}^{\infty} f^{-1}[B_n]$$

Exercício 5.22. Sejam $f : A \to A$ um endomapa e $x \in A$. Chamamos o $x \in A$ um fixpoint da f sse $f(x) = x$. Prove ou refute a afirmação:

$$x \text{ é um fixpoint da } f \iff \text{para todo } n \in \mathbb{N},\ x \text{ é um fixpoint da } f^n.$$

Exercício 5.23. Seja $f : A \to A$ e seja F o conjunto de todos os fixpoints da f:

$$F = \{x \in A \mid x \text{ é um fixpoint da } f\}.$$

Prove uma das afirmações seguintes e encontre um contraexemplo para a outra:

(i) $f^{-1}[F] \subseteq F$

(ii) $f^{-1}[F] \supseteq F$

Prove que se f é injetora, ambas as afirmações são verdadeiras.

28/03/2019 (Josenaldo)

Exercício 5.24. Seja $f : A \to B$. Prove que existem conjunto C e funções $e : A \rightarrowtail C$ injetiva e $m : C \twoheadrightarrow B$ sobrejetiva tais que $f = m \circ e$.

Exercício 5.25. Sejam $f : A \rightarrowtail\!\!\!\!\twoheadrightarrow B$ bijetiva e $Y \subseteq B$. Prove que

$$f^{-1}[Y] \subseteq \left\{f^{-1}(y) \mid y \in Y\right\}$$

.

Homework 5.1. Prove a outra inclusão do Exercício 5.25, isso é, mostre que

$$\left\{f^{-1}(y) \mid y \in Y\right\} \subseteq f^{-1}[Y]$$

29/03/2019 (Josenaldo)

Exercício 5.26. Seja $f : A \to B$. Prove que:

$$f(-) \text{ é sobrejetiva} \iff f^{-1}[-] \text{ é injetiva}$$

Exercício 5.27. Sejam $f : A \to A$ e F, o conjunto de todos os pontos fixos de f, isso é,

$$F = \{x \in A \mid f(x) = x\}$$

Para cada uma das afirmações a seguir, demonstre-a ou prove que, em geral, não é válida:

$$f^{-1}[F] \subseteq F$$
$$f^{-1}[F] \supseteq F$$

01/04/2019 (Jplinha)

Definição 5.28. Definimos os *numerais* `Nat` para representar os números naturais com uma definição indutiva:

- 0 é um `Nat`;
- Se n é um `Nat`, então Sn é um `Nat`;
- Nada mais é `Nat`.

Alternativamente, podemos usar a notação BNF para definir o `Nat` como segue:

$$\langle \texttt{Nat} \rangle ::= 0 \mid S \langle \texttt{Nat} \rangle$$

Exercício 5.29. Defina recursivamente as operações de adição e multiplicação no `Nat`.

Exercício 5.30. Descreva formalmente (com fórmulas de lógica), o que significa afirmar que a adição (definida no exercício anterior) é associativa e em seguida demonstre que ela realmente é.

02/04/2019 (Bianca)

Exercício 5.31. Seja $f : A \to B$ tal que $f[A]$ é um singleton (conjunto unitário) ou $f^{-1}[B]$ é um singleton. O que interessante podes concluir sobre a f? (Demonstre tua afirmação).

Exercício 5.32. Seja função $f : A \to B$. Demonstre se f tem um $\circ$-inverso pela esquerda f^L, então f é injetora. O converso é válido...Sempre? Nunca? Quando? (Justifique sua resposta). Se adicionalmente, o inverso esquerdo f^L é injetivo, podemos concluir que f é bijetora?

Exercício 5.33. Seja $f : A \to A$ endomapa tal que $f^3 = \mathrm{id}_A$.

(i) Dê um exemplo disso com $f \neq \mathrm{id}_A$.

(ii) A afirmação "f é bijetora" é verdadeira? Se sim, demonstre; se não, refute; se os dados não são suficientes para concluir, mostre um exemplo e um contraexemplo.

02/04/2019 (Jplinha)

Exercício 5.34. Defina no $\mathbb{Z} \times \mathbb{Z}_{\neq 0}$ a relação

$$\langle a, b\rangle \approx \langle c, d\rangle \overset{\text{def}}{\iff} ad = bc$$

Mostre que a $\approx$ é uma relação de equivalência e descreva suas classes de equivalência: $\mathbb{Z} \times \mathbb{Z}_{\neq 0}$"="?

Exercício 5.35. Defina no $(\mathbb{N} \to \mathbb{N})$ as relações seguintes:

$$f \overset{\exists\forall}{=} g \overset{\text{def}}{\iff} (\exists n \in \mathbb{N})(\forall x \geq n)[f(x) = g(x)]$$

$$f \overset{\forall\exists}{=} g \overset{\text{def}}{\iff} (\forall n \in \mathbb{N})(\exists x \geq n)[f(x) = g(x)]$$

Para cada uma das relações acima, decida se ela é relação de equivalência (demonstre caso seja, refute caso contrário). Se é relação de equiavalência, descreva seu conjunto quociente.

04/04/2019 (Bianca)

Exercício 5.36. Seja R uma preordem num conjunto A. Prove que R é idempotente, ou seja, $R = R \circ R$.

Exercício 5.37. Proposição: Seja $X \neq \emptyset$ e $\sim$ uma relação no X. Se $\sim$ é simétrica e transitiva, então ela é reflexiva.

Prova: Como ela é simétrica, de $x \sim y$, concluímos que $y \sim x$ também. Usando a transitivdade, de $x \sim y$ e $y \sim x$, concluímos a $x \sim y$, que mostra que $\sim$ é reflexiva também.

Ache o erro na prova acima e prove que a proposição é falsa.

Exercício 5.38. Considere a $\circ$ como uma operação binária nas relações binárias num conjunto A. Ela tem identidade? Ou seja, existe alguma relação binária I no A tal que para toda relação R no A,

$$I \circ R = R = R \circ I?$$

Se sim, defina essa relação I e prove que realmente é. Se não, prove que não existe.

Exercício 5.39. Defina formalmente as "potências" R^n de uma dada relação binária R em um conjunto, informalmente definida por:

$$x(R^n)y \overset{\text{"def"}}{\iff} x(R \circ \cdots \circ R)y,$$

válida para todo $n \in \mathbb{N}$.

Exercício 5.40. Seja S uma relação binária no $\mathbb{R}$ tal que

$$(S \circ S^{\partial}) \text{ é irreflexiva.}$$

Qual é o gráfico da S? Prove tua resposta.

05/04/2019 (Josenaldo)

Definição 5.41. Dados A e B conjuntos, e R e S relações de A para B, definem-se:

$$R \leq S \overset{\text{def}}{\iff} (\forall a \in A)(\forall b \in B)[a \; R \; b \implies a \; S \; b]$$

$$\text{Dom}(R) \overset{\text{def}}{=} \{a \in A \mid \text{existe } b \in B \text{ tal que } a \; R \; b\}$$

$$\text{Ran}(R) \overset{\text{def}}{=} \{b \in B \mid \text{existe } a \in A \text{ tal que } a \; R \; b\}$$

Exercício 5.42. Dados A e B conjuntos, e R uma relação de A para B, prove que $\mathrm{Dom}(R) \subseteq \mathrm{Ran}(R^\partial)$.

Homework 5.2. Prove a inclusão contrária no Exercício 5.42.

Exercício 5.43. Sejam A e B conjuntos, e R e S, relações de A para B. Mostre que:

$$R \leq S \iff R^\partial \leq S^\partial$$

Homework 5.3. No contexto do Exercício 5.43, prove que $R^\partial \leq S^\partial \iff R \leq S$.

Definição 5.44. Dados A e B conjuntos, define-se a relação $0_{A,B}$ de A para B tal que, para todos $a \in A$ e $b \in B$,

$$0_{A,B}(a,b) \overset{\text{def}}{\iff} a \neq a$$

Exercício 5.45. Sejam A, B e C conjuntos, e R e S relações de A para B e B para C, respectivamente. Prove que:

$$\mathrm{Ran}(R) \cap \mathrm{Dom}(S) = \emptyset \implies R \circ S = 0_{A,C}$$

Homework 5.4. Prove a afirmação conversa do Exercício 5.45.

09/04/2019 (Bianca)

Exercício 5.46. Sejam $\sim$ uma relação de equivalência num conjunto X, e $x, y \in X$. O.s.s.e.:

(i) $x \sim y$

(ii) $[x] = [y]$

(iii) $[x] \cap [y] \neq \emptyset$

Exercício 5.47. Seja $f : A \to B$ uma função. Defina $\sim$ por $a \sim b$ sse $f(a) = f(b)$. Prove que $\sim$ é uma relação de equivalência em A e descreva suas classes de equivalência.

Exercício 5.48. No conjunto $\mathbb{R}$, defina $\sim$ por $a \sim b$ sse $a - b \in \mathbb{Z}$. Mostre que $\sim$ é uma relação de equivalência e descreva suas classes de equivalência.

Exercício 5.49. Seja R uma relação binária num conjunto A. O.s.s.e.:

(i) R é uma relação de equivalência;

(ii) R é reflexiva e circular;

(iii) R é reflexiva e right-euclidean.

11/04/2019 (Bianca)

Exercício 5.50. Defina com texto completo o conjunto quociente.

Exercício 5.51. Defina com texto completo o que é uma partição.

Exercício 5.52. Seja $\sim$ uma relação de equivalência num conjunto A. Prove que o conjunto quociente $A/\sim$ é uma partição de A.

Exercício 5.53. Considere as relações seguintes no $(\mathbb{Z} \to \mathbb{Z})$:

$$f \sim g \iff^{\text{def}} (\exists u \in \mathbb{Z})(\forall x \in \mathbb{Z})[f(x) = g(x+u)]$$

$$f \wr\!\wr\, g \iff^{\text{def}} (\exists v \in \mathbb{Z})(\forall x \in \mathbb{Z})[f(x) = g(x) + v]$$

Prove que uma delas é uma relação de equivalência e que a outra é uma relação de ordem.

11/04/2019 (Josenaldo)

Exercício 5.54. Seja R uma relação binária num conjunto A. Prove que, se R é transitiva, então $\text{Graph}(R \circ R) \subseteq \text{Graph}(R)$.

Exercício 5.55. Seja $\sim$ uma relação de equivalência num conjunto A. Prove que $A/\sim$ é uma partição de A.

12/04/2019 (Josenaldo)

Exercício 5.56. Seja $\mathscr{A}$ uma partição de um conjunto A. Prove que existe relação de equivalência $\sim$ tal que $\mathscr{A} = A/\sim$.

16/04/2019 (Bianca)

Exercício 5.57. Seja D um conjunto. Mostre que $\langle \wp D, \triangle \rangle$ é um grupo.

Exercício 5.58. Sejam G grupo e $a, b \in G$. Mostre que $(bab^{-1})^n = ba^n b^{-1}$, para todo $n \in \mathbb{N}$.

Exercício 5.59. Se G e H são dois grupos, seu produto direto é denotado por $G \times H$, e definido da seguinte forma: $G \times H$ consiste em todos os pares ordenados (x, y) onde $x \in G$ e $y \in H$. Ou seja,

$$G \times H = \{(x, y) \mid x \in G \text{ e } y \in H\}$$

A operação $G \times H$ consiste na multiplicação de elementos correspondentes:

$$(x, y) \cdot (x', y') = (x \cdot x', y \cdot y')$$

Prove que $G \times H$ é um grupo.

23/04/2019 (Bianca)

Exercício 5.60. Seja a elemento de um grupo G. Prove os seguintes:

(i) $o(a) = 1$ sse $a = e$.

(ii) A ordem de a^{-1} é a mesma que a ordem de a.

Exercício 5.61. Sejam G grupo e $\mathcal{H}$ uma família de subgrupos de G. Mostre que $\bigcap \mathcal{H} \leq G$.

Exercício 5.62. Seja G grupo e $H \leq G$. Defina:

$$a \sim b \overset{\text{def}}{\iff} ab^{-1} \in H.$$

(a) Prove que $\sim$ é uma relação de equivalência.

(b) Prove que para todo $a, b \in G$:

(i) se $a \in H$ e $b \in H$, então $a \sim b$.

(ii) se $a \in H$ e $b \notin H$, então $a \not\sim b$.

25/04/2019 (Bianca)

Exercício 5.63. Se G é um grupo de ordem n, G é cíclico sse G tem um elemento de ordem n.

Exercício 5.64. Todo subgrupo cíclico é abeliano.

Exercício 5.65. Sejam G grupo e $H \leq G$. Sejam $a, b \in G$. Mostre que:

(i) $a \in Hb \iff Ha = Hb$

(ii) $Ha = Hb \iff a \equiv b \pmod{H}$

(iii) $aH = Ha \;\&\; bH = Hb \implies (ab)H = H(ab)$

29/04/2019 (Jplinha)

Exercício 5.66. Sejam $a, b, c, x, y, m \in \mathbb{Z}$, demonstre os seguintes:

(1) $1 \mid a$

(2) $a \mid 0$

(3) $a \mid b \implies a \mid bx$

(4) $a \mid b \implies a \mid -b \;\&\; -a \mid b$

(5) $a \mid b \;\&\; a \mid c \implies a \mid b + c$

(6) $a \mid b \;\&\; a \mid c \implies a \mid bx + cy$

(7) $a \mid b \;\&\; b \neq 0 \implies |a| \leq |b|$

(8) Se $m \neq 0$, então: $a \mid b \iff ma \mid mb$

Exercício 5.67. Para todos $a, b, c \in \mathbb{Z}$, demonstre que

$$a \mid a$$

$$a \mid b \;\&\; b \mid c \implies a \mid c$$

Se $a, b \in \mathbb{N}$, demonstre que

$$a \mid b \;\&\; b \mid a \implies a = b$$

30/04/2019 (Josenaldo)

Exercício 5.68. Seja G grupo. Prove que, para todo $a, b \in G$,

$$ab = e \implies ba = e$$

Exercício 5.69. Seja G grupo. Prove que $\left\{x \in G \mid x = x^{-1}\right\} \leq G$.

09/05/2019 (Josenaldo)

Exercício 5.70. Sejam A e B grupos. Prove que se φ é um homomorfismo de A para B, então:

(i) $\varphi(e_A) = e_B$

(ii) $\varphi\left(x^{-1}\right) = (\varphi(x))^{-1}$

Exercício 5.71. Considere os grupos $\boldsymbol{R} = \langle \mathbb{R} \setminus \{0\}; \cdot \rangle$ e $\boldsymbol{Z} = \langle \mathbb{Z} \setminus \{0\}; + \rangle$, e $\langle 2 \rangle_{\boldsymbol{R}}$ e $\langle 2 \rangle_{\boldsymbol{Z}}$ os subgrupos de $\boldsymbol{R}$ e $\boldsymbol{Z}$, respectivamente, gerados por 2. Prove que $\langle 2 \rangle_{\boldsymbol{R}}$ e $\langle 2 \rangle_{\boldsymbol{Z}}$ são isomorfos.

10/05/2019 (Josenaldo)

Exercício 5.72. Seja G grupo e $\emptyset \neq H \subseteq G$. Prove que se $ab^{-1} \in H$ é válido para todos $a, b \in H$, então $H \leq G$.

Exercício 5.73. Sejam G grupo e $N \trianglelefteq G$. Prove que a operação $*$ tal que, para todos $a, b \in G$,

$$(Na) * (Nb) \stackrel{\text{def}}{=} N(ab)$$

é bem-definida.

13/05/2019 (Jplinha)

Exercício 5.74 (Lema de Euclides)**.** Sejam $a, b \in \mathbb{Z}$ com $b > 0$, então $(a, b) = (b, r)$, onde r é o resto da divisão de a por b.

14/05/2019 (Jplinha)

Exercício 5.75. Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid b$ e $(a, b) = 1$, então $a \mid c$.

Exercício 5.76. Sejam $a, b \in \mathbb{Z}$. Se $a = bq + r$, para alguns $q, r \in \mathbb{Z}$, então $(a, b) = (b, r)$.

16/05/2019 (Josenaldo)

Exercício 5.77. Sejam $a, b \in \mathbb{N}$ tais que $a > b$. Prove que $\text{mdc}(a, b) = \text{mdc}(b, a \; mod \; b)$, em que $a \; mod \; b$ denota o resto da divisão de a por b.

17/05/2019 (Josenaldo)

Exercício 5.78. Sejam F um corpo ordenado e $a, b \in F$. Mostre que exatamente uma das seguintes afirmações é válida:

$$a < b; \qquad a = b; \qquad b < a$$

Exercício 5.79. Sejam F um corpo ordenado e $a, b, c \in F$. Mostre que:

$$a < b \;\&\; c > 0 \implies ac < bc$$

.

Exercício 5.80. Sejam F um corpo ordenado e $x \in F$. Mostre que, se $0 \leq x < \epsilon$ para todo $\epsilon \in F$ tal que $\epsilon > 0$, então $x = 0$.

20/05/2019 (Jplinha)

Exercício 5.81. Sejam $a, b, p \in \mathbb{Z}$. Se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Exercício 5.82 (Teorema Fundamental da Aritmética)**.** Todo $n \in \mathbb{N}$, com $n > 1$, pode ser escrito como um único produtório de primos, a menos de ordem.

21/05/2019 (Jplinha)

Exercício 5.83. A sequência dos primos é infinita.

Exercício 5.84. Seja $n \in \mathbb{N}_{>1}$ tal que n não é primo. Logo, n possui um fator primo menor ou igual a $\sqrt{n}$.

23/05/2019 (Josenaldo)

Exercício 5.85. Prove que, para todos $k \geq 1$ e $n \geq 2$, é válido que $(n-1) \mid n^k - 1$.

Exercício 5.86. Mostre que $n^5 - n$ é divisível por 30 para todo inteiro n.

Exercício 5.87. Mostre que, para todos $n \in \mathbb{N}$, $k \in \mathbb{N}^*$,

$$n^k - 1 = (n-1)\Big(n^{k-1} + n^{k-2} + \cdots + n^1 + 1\Big)$$

Exercício 5.88. Mostre que, para todos $a, b, c \in \mathbb{Z}$ tais que $ab \neq 0$ e $(a+c)b \neq 0$, se $b \mid c$ então $(a+c, b) = (a, b)$.

24/05/2019 (Josenaldo)

Exercício 5.89. Prove que $\wp\mathbb{N}$ não é enumerável.

Exercício 5.90. Seja $\sim$ uma relação de equivalência em $\mathbb{N}$. Prove que $\mathbb{N}/\sim$ é enumerável.

27/05/2019 (Jplinha)

Definição 5.91. Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}_{>0}$. Dizemos que a é *congruente* a b *módulo* m se, e somente se, $m \mid (a-b)$. Denotamos essa relação por $a \equiv b \pmod{m}$ ou $a \equiv_m b$.

Exercício 5.92. Se a, b são inteiros, temos que $a \equiv_m b$ se, e somente se, $a = b + mk$, para algum $k \in \mathbb{Z}$.

Exercício 5.93. Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 0$. As seguintes sentenças são verdadeiras:

(i) $a \equiv_m a$;

(ii) Se $a \equiv_m b$, então $b \equiv_m a$;

(iii) Se $a \equiv_m b$ e $b \equiv_m c$, então $a \equiv_m c$.

Homework 5.5. Sejam $a, b, c \in \mathbb{Z}$ e $m \in \mathbb{N}_{>0}$ tal que $a \equiv_m b$, então:

(i) $a + c \equiv_m b + c$

(ii) $a - c \equiv_m b - c$

(iii) $ac \equiv_m bc$

28/05/2019 (Josenaldo)

Exercício 5.94. Sejam $a, b, m \in \mathbb{Z}$, com $m > 0$. Considere as seguintes definições de congruência:

$$a \equiv b \ (mod\ m) \overset{\text{def}}{\iff} m \mid (b - a) \tag{5}$$

$$\overset{\text{def}}{\iff} b \text{ é o resto da divisão de } a \text{ por } m \tag{6}$$

Para cada uma das perguntas seguintes, responda "sim", "não" ou "depende":

1. 5 $\implies$ 6?
2. 6 $\implies$ 5?

Exercício 5.95. Prove que $(\mathbb{R} \to \mathbb{R}) =_{\text{c}} \wp\mathbb{R}$.

30/05/2019 (Josenaldo)

Exercício 5.96. Sejam a, b, k e m inteiros tais que $m > 0$ e $a \equiv b \pmod{m}$. Mostre que $a^k \equiv b^k \pmod{m}$.

Exercício 5.97. Considere o axioma seguinte:

CONS $\forall h \forall t \exists s \forall x (x \in s \leftrightarrow x = h \vee x \in t)$

a) No sistema ZF1+ZF2+CONS, prove o ZF3 como teorema.

b) Mostre que é impossível provar o CONS no sistema ZF1+ZF2+ZF3.

c) No sistema ZF1+ZF2+ZF3+ZF4+ZF5+ZF6, prove o CONS como teorema.

Exercício 5.98. Mostre que $\wp_\infty\mathbb{N}$ não é enumerável, em que $\wp_\infty A = \{X \subseteq A \mid X \text{ é infinito}\}$ para qualquer conjunto A.

03/06/2019 (Jplinha)

Definição 5.99. Se a e b são dois inteiros com $a \equiv_m b$, dizemos que b é resíduo de a módulo m.

Definição 5.100. O conjunto dos inteiros $\{r_0, \ldots, r_{s-1}\}$ é um *sistema completo de resíduos módulo* m se

(i) $r_i \not\equiv_m r_j$ para $i \neq j$

(ii) para todo inteiro n existe um r_i tal que $n \equiv_m r_i$.

Exercício 5.101. Se k inteiros $r_0, \ldots, r_{k-1}$ formam um sistema completo de resíduos módulo m, então $k = m$.

04/06/2019 (Jp)

Exercício 5.102. Usando os ZF1+ZF2+ZF3+ZF5, podemos construir conjunto com cardinalidade finita, arbitrariamente grande?

Exercício 5.103. Usando os ZF1+ZF2+ZF3+ZF5, podemos construir conjunto com cardinalidade finita, qualquer?

Exercício 5.104. Usando os ZF1+ZF2+ZF4+ZF5, podemos construir conjunto com cardinalidade finita, qualquer?

06/06/2019 (Josenaldo)

Exercício 5.105. Considere o axioma seguinte:

CONS $\forall h \forall t \exists s \forall x (x \in s \leftrightarrow x = h \vee x \in t)$

Mostre que, no sistema ZF1+ZF2*+ZF3+ZF4+ZF5+ZF6, o ZF2 é um teorema.

Exercício 5.106. Seja a conjunto. Prove que, no sistema ZF1+ZF2+ZF4+ZF5+ZF6, $\{a\}$ também o é.

Exercício 5.107. Sejam a, b, c e d conjuntos. Prove, pelos axiomas ZFC, que os seguintes também o são:

a) $A = \{a, b, c, d\}$;

b) $B = \{a, b, \{c, d\}\}$;

c) $C = \{x \mid x \subseteq a \cup b \cup c \cup d \;\&\; x \text{ tem exatamente dois membros}\}$.

06/06/2019 (Jp)

Exercício 5.108. Prove os seguintes itens:

- $0 \in \mathbf{N}$
- $S : \mathbf{N} \to \mathbf{N}$

Homework 5.6. Prove os seguintes itens:

- S é injetiva.
- Para todo $X \subseteq \mathbf{N}$, se X satisfaz

  (i) $0 \in X$

  (ii) se $n \in X$, então $n^+ \in X$

  então $X = \mathbf{N}$.

Teorema 5.109. *Para todos $a, b, n, m \in \mathbb{N}$, se $a \equiv_m b$, então $a^n \equiv_m b^n$.*

Exercício 5.110. Usando o teorema acima, prove que $13 \mid 2^{70} + 3^{70}$.

07/06/2019 (Josenaldo)

Exercício 5.111. Sejam $a_1, \ldots, a_n$ conjuntos, em que $n > 0$. Prove, usando os axiomas ZFC, que existe um conjunto cujos membros são os $a_1, \ldots, a_n$.

Exercício 5.112. Considere a seguinte definição:

$$\langle a, b \rangle \stackrel{\text{def}}{=} \{x, \{y\}\}$$

.

Prove que ela não pode ser usada como uma "implementação" de tuplas, de fato.

Exercício 5.113. Prove que $\wp_{\text{cof}}\mathbb{N} =_{\text{c}} \mathbb{N}$, em que $\wp_{\text{cof}}A = \{C \subseteq A \mid A \setminus C \text{ é finito}\}$.

10/06/2019 (Jplinha)

Exercício 5.114. Mostrar que $2(p-3)! \equiv_p -1$ para p primo ímpar.

Exercício 5.115. Se a e b são inteiros, temos que $a \equiv_m b$ se, e somente se, $a = b + km$ para algum k inteiro.

Homework 5.7. Mostre que para todo $a \in \mathbb{Z}$, $a^7 \equiv_{27} a$.

11/06/2019 (Jp)

Exercício 5.116. Sejam P poset e $A \subseteq P$. Prove que $\uparrow A$ é um upset e $\downarrow A$ é um downset.

Exercício 5.117. Sejam P poset e $x, y \in P$. Prove que os seguintes são equivalentes:

- $x \leq y$
- $\downarrow x \subseteq \downarrow y$
- Para todo downset $D \subseteq P$ com $y \in D$ temos $x \in D$

Exercício 5.118. Prove que $\mathbf{N}$ satisfaz o princípio da indução, ou seja: para todo $X \subseteq \mathbf{N}$, se $0 \in X$ e para todo $n \in X$ temos $n^+ \in X$, então $X = \mathbf{N}$.

11/06/2019 (Jplinha)

Exercício 5.119. Demonstre ou refute "Se a e m são inteiros e $(a, m) = 1$, então $m \mid (1 + a^1 + \cdots + a^{\phi(m)-1})$."

Exercício 5.120. Sejam p, q primos tais que $p \geq q \geq 5$, então $p^2 - q^2 \equiv_{24} 0$.

13/06/2019 (Josenaldo)

Exercício 5.121. Mostre que, se $n > 0$ é tal que $(n-1)! \equiv -1 \pmod{n}$, então n é primo.

Exercício 5.122. Sejam p primo e $a > 0$. Mostre que $a^p \equiv a \pmod{p}$.

Exercício 5.123. Sejam P poset, $A \subseteq P$ e $u \in A^{\mathrm{U}} \cap A$. Mostre que $u = \mathrm{lub}A = \mathrm{max}A$.

Exercício 5.124. Seja A um conjunto e R uma relação binária em A irreflexiva e transitiva. Mostre que a relação

$$x \leq y \overset{\text{def}}{\iff} x \leq y \text{ ou } x = y$$

é uma ordem parcial.

13/06/2019 (Jp)

Exercício 5.125. Para cada conjunto estruturado abaixo, verifique se é um poset, e prove ou refute em acordo.

- $\langle \mathbb{N}; \perp \rangle$, $n \perp m \overset{\text{def}}{\iff} \gcd(n, m) = 1$
- $\langle \mathbb{R}; \square \rangle$, $x \square y \overset{\text{def}}{\iff} |x| \leq |y|$
- $\langle \mathbb{R}^2; \propto \rangle$, $p \propto q \overset{\text{def}}{\iff} (\exists t \in \mathbb{R}_{\geq 1})[\, q = t \cdot p \,]$

Exercício 5.126. Sejam $\langle B; \leq \rangle$ poset e $f : A \rightarrowtail B$. Definimos

$$x \leq_f y \overset{\text{def}}{\iff} f(x) \leq f(y)$$

Mostre que $\langle A; \leq_f \rangle$ é um poset.

Exercício 5.127. Sejam $\langle P; \leq \rangle$ poset, $A \subseteq P$ e $x \in A$. Quais das seguintes implicações são válidas? Prove ou refute cada uma.

- x é minimal de $A \implies x$ é mínimo de A
- x é mínimo de $A \implies x$ é minimal de A

Homework 5.8. Seja $\langle P; \leq \rangle$ poset. Prove que, se $A \subseteq P$ é uma cadeia, então para todo $x \in A$, x é minimal de A sse x é mínimo de A.

17/06/2019 (Jplinha)

Exercício 5.128. Mostre que p é o menor primo que divide $(p-1)! + 1$.

Exercício 5.129. Seja S o conjunto de sequências finitas de números naturais. Descreva um método para "codificar" os elementos de S com os elementos de $\mathbb{N} \setminus \{0\}$. Teu método deve ser revertível, no sentido que cada sequência finita

$$s = \langle s_0, s_1, \ldots, s_{k_s} \rangle \in S$$

deve corresponder em exatamente um número natural $n_s \in \mathbb{N}\backslash\{0\}$, e, dado esse número $n_s \in \mathbb{N}_{>0}$, deveria ser possível "extrair" a sequência s cuja codificação é o n_s. Não se preocupe se existem naturais que não são codificações de nenhuma sequência.

18/06/2019 (Jp)

Teorema 5.130. *Se $a \perp m$ e $ax \equiv_m b$, então $x \equiv_m a^{\varphi(m)-1} \cdot b$.*

Exercício 5.131. Sabendo que $7x \equiv_{11} 8$, descubra o resto da divisão de x por 11.

21/06/2019 (Jp)

Exercício 5.132. Sejam A, B, C conjuntos. Prove que

$$(A \times B \to C) =_{\mathrm{c}} (A \to (B \to C))$$

Exercício 5.133. Prove ou refute: para todos conjuntos A, B, temos

$$(A \times B) \leq_{\mathrm{c}} (A \to B)$$

Exercício 5.134. Seja $\phi : L \to K$ um homomorfismo de reticulados. Prove os seguintes itens:

- se $M \leq L$, então $\phi[M] \leq K$.
- se $N \leq K$, então $\phi^{-1}[N] \leq L$.

25/06/2019 (Josenaldo)

Exercício 5.135. Sejam P e Q cadeias. Mostre que $P \times Q$ é uma cadeia na ordem lexicográfica.

Exercício 5.136. Sejam P e Q cadeias. Mostre que $P \times Q$ é uma cadeia na ordem coordenada-a-coordenada se, e somente se, no máximo um dos P e Q tiver mais de um elemento.

25/06/2019 (Jplinha)

Definição 5.137. Os números de *Fibonacci* e os números de *Lucas* são definidos recursivamente como segue, respectivamente

$$\begin{aligned} F_0 &= 0 & L_0 &= 2 \\ F_1 &= 1 & L_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n & L_{n+2} &= L_{n+1} + L_n \end{aligned}$$

Exercício 5.138. Definimos a função $l\colon \mathbb{N} \setminus \{0\} \to \mathbb{N}$ pela equação

$$l(n) = F_{n-1} + F_{n+1}$$

Demonstre, para todo $n \in \mathbb{N}_{\geq 1}$, que $l(n) = L_n$.

Exercício 5.139. Sejam $a, b \in \mathbb{Z}$ e $k, m \in \mathbb{N}_{>0}$, tal que $a \equiv_m b$. Demonstre que $a^k \equiv_m b^k$.

27/06/2019 (Jp)

Definição 5.140. Seja $f : A \to B$ uma função. Dizemos que f é preimagem-finita sse para todo $Y \subseteq B$ finito, $f^{-1}[Y]$ também é finito.

Exercício 5.141. Seja $f : A \rightarrowtail B$ injetiva. Podemos dizer que f é preimagem-finita?

Exercício 5.142. Seja $f : A \to B$ preimagem-finita. Podemos dizer que f é injetiva?

Exercício 5.143. Sejam $f : A \to B$ e $g : B \to C$ preimagem-finitas. Prove que $g \circ f$ é preimagem-finita.

28/06/2019 (Jp)

Exercício 5.144. Seja $\langle G; e, * \rangle$ um conjunto estruturado satisfazendo os seguintes axiomas:

(G0) $(\forall a, b \in G)[a * b \in G]$

(G1) $(\forall a, b, c \in G)[a * (b * c) = (a * b) * c]$

(G2L) $(\forall a \in G)[e * a = a]$

(G3L) $(\forall a \in G)(\exists y \in G)[y * a = e]$

Prove que $\langle G; e, * \rangle$ é um grupo.

Exercício 5.145. Se trocarmos o (G2L) acima pelo

(G2R) $(\forall a \in G)[a * e = a]$

Ainda podemos afirmar que $\langle G; e, * \rangle$ é um grupo?

Exercício 5.146. Seja G um grupo e $a \in G$. Prove que $\langle a \rangle$ é um subgrupo de G.

Exercício 5.147. Sejam M, N monoides, e $\phi : M \twoheadrightarrow N$ sobrejetiva que respeita a operação. Prove que ϕ é homomorfismo de monoides.

6 2019.2

12/08/2019 (Jplinha)

Definição 6.1. Definimos os `Nat` com grámatica BNF da seguinte forma

$$\texttt{Nat} ::= 0 | S \langle \texttt{Nat} \rangle$$

Exercício 6.2. Defina e demonstra a associatividade da adição nos `Nat`.

Homework 6.1. Defina com fórmulas de lógica a comutatividade nos `Nat`.

13/08/2019 (Jplinha)

Exercício 6.3. Demonstre a associatividade da adição nos `Nat`.

Homework 6.2. Defina e demonstre a comutatividade da adição nos `Nat`

19/08/2019 (Jplinha)

Exercício 6.4. Demonstre a comutatividade da adição nos `Nat`.

20/08/2019 (Jplinha)

Exercício 6.5. Defina a multiplicação nos `Nat`.

Exercício 6.6. Defina a exponenciação nos `Nat`.

Exercício 6.7. Prove que a multiplicação é distributiva nos `Nat`.

Exercício 6.8. Prove que a multiplicação é associativa nos `Nat`.

Homework 6.3. Prova que a multiplicação é comutativa nos `Nat`.

16/09/2019 (Jplinha)

Exercício 6.9. Prove que a $\leq$ nos $\mathbb{N}$ é uma boa-ordem, isto é

$$\text{para todo } A \subseteq \mathbb{N}, \text{ se } A \neq \emptyset \text{ então } A \text{ tem um mínimo}$$

Definição 6.10. Definimos a relação de ordem $\preceq$ nos $\mathbb{N}$ pelas

$$\begin{array}{ll} \text{(LE1)} & 0 \preceq m \iff \mathsf{True} \\ \text{(LE2)} & Sn \preceq 0 \iff \mathsf{False} \\ \text{(LE3)} & Sn \preceq Sm \iff n \preceq m \end{array}$$

Exercício 6.11. Prove que as duas relações de ordem, $\leq$ e $\preceq$ são equivalentes, isto é

$$\text{para todos } n, m \in \mathbb{N},\ n \leq m \iff n \preceq m$$

04/11/2019 (Jplinha)

Exercício 6.12. (Lema de Euclides) Sejam $a, b \in \mathbb{Z}$ e p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Exercício 6.13. Sejam $a \in \mathbb{Z}$ e p primo. Se $p \not| a$, então $gcda, p = 1$.

Homework 6.4. Sejam $a \in \mathbb{Z}$ e p primo. Se $a \mid p$, então $a = 1$ ou $a = p$.

25/11/2019 (Jplinha)

Exercício 6.14. Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{Z}_{>0}$. Se $a \equiv b \pmod{m}$, então para todo $x \in \mathbb{Z}$ temos:

(i) $a + x \equiv b + x \pmod{m}$

(ii) $ax \equiv bx \pmod{m}$

(iii) $-a \equiv -b \pmod{m}$

27/11/2019 (Jplinha)

Exercício 6.15 (Lei de cancelamento módulo m)**.** Seja $c \in \mathbb{Z}$ tal que $(c, m) = 1$. Se $ca \equiv cb \pmod{m}$, então $a \equiv b \pmod{m}$.

Homework 6.5 (Inverso módulo m)**.** Sejam $a, m \in \mathbb{Z}$ tal que $m > 0$. Dizemos que a tem inverso módulo m se, e somente se, $(a, m) = 1$.

02/12/2019 (Jplinha)

Exercício 6.16. Sejam $a, b, c, d \in \mathbb{Z}$, com $c \neq 0$. Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.

Exercício 6.17. Sejam p, q primos distintos. Prove que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Índice Remissivo