NOTAS DE AULA PARA MATEMÁTICA DISCRETA I

ANDREAS B.M. BRUNNER
UFBA

Salvador-Bahia
Julho de 2013

Sumário

Comentário inicial

Estas notas de aula para *Matemática Discreta I* devem ajudar aos estudantes a entender conceitos básicos em matemática e fornecer um primeiro contato com a linguagem e a apresentação de noções matemáticas. A minha ideia de elaborar notas de aula para as disciplinas de Matemática Discreta I e II, já existe bastante tempo. Como estas duas disciplinas foram criadas para o estudante se familiarizar em noções fundamentais da matemática e nenhum livro abrange todos estes assuntos, notas de aulas devem ser bem vindos. E aqui vem a primeira parte.

Quase todos os assuntos nestas notas de aula são abordados nos livros [4], [8] e [15]. Os últimos dois livros abordam um monte de assuntos acerca da matemática discreta, inclusive muitos assuntos do curso oferecido na UFBA, Matemática Discreta II.

O conteúdo das notas de aulas, foi tirado de vários livros matemáticos (todos citados na bibliografia) e deve facilitar ao estudante cursar a disciplina de MATA42 - Matemática Discreta I, oferecida pelo departamento de Matemática da UFBA.

Basicamente abrangemos em seguida uma curta reflexão sobre o trabalho de um matemático - em geral o estudante não tem nenhuma ideia sobre o funcionamento da matemática. Para isso, falamos um pouco acerca do método axiomático em matemática. Depois disso, vejamos alguns conceitos da lógica proposicional clássica, como tabelas de verdade para fórmulas bem formadas, os conceitos da tautologia, contradição e fórmulas satisfatíveis. Com isso podemos explicar métodos de demonstrações em matemática, como prova direta, indireta e por contraposição. A teoria ingênua de conjuntos, introduz conceitos básicos para conjuntos e algumas propriedades. Introduzimos também o produto Cartesiano de conjuntos e assim relações e funções. Vejamos algumas funções específicas e inversas à direita e à esquerda. Introduzimos via axiomática de Peano a noção de número natural e discutimos demonstrações por indução como também recursão. Além disso, introduzimos relações específicas e relações de equivalência, partição de um conjunto e a conexão entre os dois últimos conceitos. Também introduzimos fechos reflexivo e transitivo de relações, conceitos importantes para a teoria da computação. Terminamos esta parte da Matemática Discreta I, explicando noções básicas da combinatória, como os princípios da adição e da multiplicação e como estes princípios fundamentam a combinatória.

Observemos que as noções abordadas nestas notas se direcionam a estudantes a partir do primeiro semestre, cursando algum curso na área das ciências exatas, principalmente aos estudantes das áreas da ciência da computação, sistemas de informação, engenharia da computação, mas acreditamos que também estudantes *novatos* de matemática - licenciatura e bacharelado - podem tirar bastante aproveito destas notas. Claramente, devem servir estas notas também a estudantes interessados e curiosos em matemática de qualquer área. As notas são escritas numa maneira elementar tal que qualquer pessoa com segundo grau completo deve ser capaz de entender os conceitos.

Em breve notas de aula acerca da *Matemática Discreta II* devem aparecer.

Salvador, 31 de julho de 2013.

Capítulo 1

Conceitos básicos da lógica matemática proposicional

Para poder exibir alguns conceitos importantes acerca da lógica matemática clássica, queremos numa primeira seção discutir o *funcionamento da matemática.* Vejamos que o matemático não é sempre interessado em calcular, porém em demonstrar resultados matemáticos, em entender estes resultados matemáticos e em conexar resultados de áreas diferentes. Para isso, é preciso entender como um matemático trabalha no seu dia a dia. Isto, tentamos esclarecer na primeira seção 1.1, antes de discutir conceitos lógicos.

O leitor interessado tem livros para acompanhar esta seção listados na bibliografia, por exemplo, [1, 3, 4, 6, 14]. Também nos livros [8] e [15], estes assuntos são tratados de uma ou outra maneira.

1.1 O método axiomático em matemática

Queremos nos perguntar inicialmente, como é que funciona a matemática? Ou seja, como um matemático trabalha? Sabemos que em áreas como biologia ou física experimental, por exemplo, o biológo ou o físico estão elaborando experimentos e através destes conseguem algum resultado acerca de uma questão feita. Para questões matemáticas, será que os matemáticos também podem elaborar estes *experimentos*? Num certo sentido, o matemático pode sim fazer digamos *experimentos mentais* acerca de um assunto da matemática. Mas assim, é preciso perguntar como o matemático pode *abstrair* os conceitos para fazer os seus experimentos mentais e conseguir resultados, quais devem ser sempre válidos.

Um exemplo muito simples e ingênuo, seria perguntar: Por que, é que $1+1=2$? Será que isso somente é uma convenção? Ou um resultado por uma força maior, talvez deus? Para poder responder isso, é preciso perguntar de antemão, como é definido 1, e $=$ e como 2? Assim, já temos uma pergunta aparentemente difícil e também chata, pois o número 1 é simplesmente um, e o 2 é dois. Enquanto a igualdade é igualdade no sentido de Leibniz:

Dois objetos A e B são ditos iguais se, e somente se, os dois objetos têm as mesmas propriedades P,
i.e. em lógica de segunda ordem, $A = B \quad \text{sse} \quad \forall P,\, P(A) \text{ sse } P(B)$.

Leia para $P(A)$ simplesmente, A tem a propriedade P. Mais tarde vejamos que podemos de fato esclarecer estas questões usando a axiomática de Peano, cf. 3. Aí, o número 1 é simplesmente o sucessor de 0, e o 2 o sucessor de 1 e assim adiante obtemos todos os naturais. A igualdade, vejamos que estará sendo tratado como símbolo lógico, e este símbolo lógico satisfaz axiomas, cf. 1.2.2.

Assim, um ponto de partida para descobrir como a matemática funciona é tentar ter clareza sobre os objetos ou conceitos matemáticos. Para ter esta clareza, devemos usar *definições.* Estas definições explicam os conceitos matemáticos. Tratando da geometria Euclideana plana, poderíamos por exemplo definir triângulo

ABC da seguinte forma:

Dados três pontos não colineares A, B e C no plano Euclideano, dizemos que estes três pontos determinam um triângulo, abreviado por ABC com os lados dados pelos segmentos AB, BC e AC.

Mas aí, temos uma nova pergunta que poderia ser: O que é o plano Euclideano? O que são pontos colineares? O que é segmento? E o que é ponto? Então vamos definir pontos colineares da seguinte forma:

Dizemos que três pontos A, B e C são colineares se, e somente se, pelos três pontos não passa nenhuma reta.

Esta nova definição nos leva a uma nova pergunta: O que é reta? É preciso definir então reta.

Uma reta é a linha determinada por dois pontos no plano.

Novamente, temos novas perguntas: O que é linha? O que é ponto? Assim, é preciso definir estes conceitos. Pensando bem, podemos concluir que sempre vamos usar palavras para definir os conceitos em jogo. Assim aparecem duas possibilidades, se quisermos definir todas as entidades matemáticas:
(i) Ou exibimos uma cadeia infintamente descendo de definições, pois nas definições sempre ocorrem novos conceitos, ou
(ii) exibimos uma cadeia finita de definições, qual é circular, ou seja, numa linha definimos o objeto A usando o objeto B, e na linha seguinte, definimos B usando A. Consequentemente (pense sobre isso!), deste modo não definimos nem objeto A nem objeto B.

Concluimos assim, que não é possível definir **todas** as entidades matemáticas. Assim, vai ser preciso que existam objetos digamos **básicos** dentro de cada teoria matemática, e estes objetos básicos não vamos definir. É claro que gostaríamos de deixar o número destes objetos básicos o menor possível, pois um objeto básico tem um certo caráter de incerteza matemática. E incertezas na matemática queremos excluir. Além disso, deixando o número de objetos básicos pequeno, a teoria matemática qual desenvolvemos será aplicável em mais casos concretos. Tendo então consciência quais objetos não definiremos, podemos começar a definir os demais objetos matemáticos, usando os objetos básicos e objetos já definidos.

Na seção, onde introduzimos a axiomática de G.Peano, vejamos que o conjunto dos naturais $\mathbb{N}$, o número 0 e a aplicação de sucessor S são os conceitos básicos, satisfazendo três axiomas. E isso nos leva a mais uma questão acerca do funcionamento da matemática. O que é um axioma? Esclarecemos que para falar de um assunto matemático, primeiramente, é preciso saber de quais objetos falamos, e definir estes objetos ou tomar como objetos básicos. Agora queremos estabelecer resultados acerca destes objetos. Isto é, queremos *demonstrar* teoremas, proposições, lemas e corolários dentro da teoria matemática considerada. Para isso, é preciso ter consciência de que somente com a lógica matemática clássica não será possível demonstrar os teoremas da geometria Euclideana, ou da teoria de números, ou de uma outra área da matemática. É preciso ter certas afirmações quais **não** demonstramos, ou seja, postulados quais aceitamos como *plausíveis* dentro de uma teoria matemática. Por exemplo, na geometria Euclideana plana, é plausível postular, que dado dois pontos no plano, então passa uma única reta por estes pontos. Na aritmética de Peano, é plausível postular que o número 0 não pode ser escrita como um natural n somando mais 1. Mas existem também postulados quais não são tão plausíveis, e mesmo assim aceitamos como axioma ou postulado. Um exemplo temos na geometria não-Euclideana, onde negamos o quinto postulado qual postula que dado uma reta e um ponto fora da reta, existe exatamente uma única reta passando por este ponto e paralela a reta dada: dado uma reta e um ponto não pertencente a essa reta, a existência de mais de uma reta paralela (na geometria hiperbólica) ou de nenhuma reta paralela (na geometria Riemanniana). Estes exemplos mostram que temos sim, liberdade na escolha dos postulados matemáticos. Porém, muitas vezes já temos algo em mente na hora de escolher certos axiomas. E esta *liberdade* também acaba logo em seguida, após a escolha dos axiomas; pois apartir daí, é preciso seguir rigorosamente os axiomas e definições escolhidos.

Por que escolhemos este ou o outro postulado, é explicado muitas vezes na teoria qual queremos desenvolver, como também nas aplicações matemáticas, ou se existe modelo para certos axiomas. Mas a princípio podemos escolher qualquer axioma, somente que uma vez escolhido um axioma é preciso ser respeitado, ou seja, aplicado e tomado de certeza absoluta.

Resumindo, temos, trabalhando numa teoria matemática, conceitos básicos e definidos. Além disso, temos axiomas ou postulados. Estamos agora em boas condições de começar trabalhar nesta área de matemática. Falta somente um detalhe acerca das demonstrações. Como é que funcionam as demonstrações matemáticas? Por que uma afirmação demonstra um teorema? O fundamento para as demonstrações é dado pela *lógica matemática clássica* e esta lógica clássica vem digamos de deduções naturais do dia e dia. Na próxima seção devemos falar um pouco mais detalhada desta lógica clássica. Antes disso, podemos então fazer a seguinte tentativa de definição:

Definição 1.1.1. *O* **método axiomático** *para uma teoria matemática consiste de*
(a) escolha de conceitos básicos na teoria,
(b) definições dos demais conceitos, usando os básicos e os já definidos,
(c) escolha dos axiomas e finalmente
(d) lógica matemática, para podermos demonstrar os teoremas.

O leitor interessado na filosofia da matemática pode consultar [3], um bom livro explicando problemas e filosofia da matemática.

1.2 Princípios da lógica clássica

Nesta seção falamos sobre conceitos básicos da lógica matemática clássica. Observemos que existem outras lógicas, as ditas **não clássicas**. A existência de lógicas não clássicas foi possibilitado pela distinção entre síntaxe e semântica em lógica, basicamente a partir das pesquisas de D. Hilbert (1862 - 1943) por volta de 1900. A lógica clássica tem três características quais usamos também no dia e dia em nossas argumentações.

Observação 1.2.1. *Enunciamos os três princípios básicos da lógica clássica.*
(a) o princípio da **Identidade***, i.e.,* $\forall x, \quad x = x$*.*
(b) o princípio da **Não-Contradição***, i.e., para* φ *uma proposição, temos que não acontece que* φ *e não* φ*, ou seja, em formalismo lógico, não acontece que* $\varphi \wedge \neg\varphi$*.*
(c) o princípio do **Terceiro Excluso***, i.e., para* φ *uma proposição, temos que sempre acontece que* φ *ou não* φ*, ou seja, em formalismo lógico, sempre acontece que* $\varphi \vee \neg\varphi$*.*

Pensando acerca dos três princípios enunciados na última observação podemos resumir que o primeiro princípio é bem razoável para o funcionamento de matemática. O que faríamos se um objeto fosse distinto de si mesmo? Teríamos problemas de trabalhar de maneira clara com este objeto. Assim, o princípio da identidade é pouco questionado.
O segundo princípio da não-contradição também é em geral pouco questionado. Não gostaríamos que uma afirmação matemática valesse junto com a sua negação. Na maioria dos casos em que podemos pensar, uma contradição lida com um estado matemático em qual não sabemos direito o que fazer com ele. Mas gostaríamos de mencionar que existem lógicas quais admitem contradições. Estas lógicas geralmente estão chamadas de lógicas **paraconsistentes**. Vamos pensar num banco de dados qual armazena vários dados sobre pessoas entre outros, o estado civil. Se uma certa pessoa está cadastrada sob estado civil de solteira e chega uma informação de que a pessoa não é (mais) solteira, teríamos uma contradição. Na lógica clássica, temos a regra de que de uma contradição se deriva qualquer afirmação, o princípio chamado de *ex contradictione sequitur quodlibet.* Se a lógica deste banco de dados funciona classicamente, usando este princípio, todos os dados poderiam ser derivados de qualquer pessoa e isso não gostaríamos que acontecesse, ou seja, esta contradição não necessariamente deveria prejudicar outros dados desta pessoa e principalmente de outras pessoas cadastradas. Este exemplo mostra que em certas circunstâncias, contradições poderiam ser

admitidas. Assim as lógicas paraconsistentes têm as suas existências justificadas. O leitor interessado pode consultar por exemplo [5].
Enquanto o terceiro ponto do terceiro excluso, na primeira vista parece que pode ser pouco questionado também, vejamos numa segunda vista que este princípio é o, que poderia ser mais questionado. O princípio (c) afirma que uma afirmação vale ou a sua negação é válida. O seu nome já diz que uma terceira possabilidade não é possível. Mas pensando numa afirmação de uma área da matemática na qual você não é especialista, tomamos por exemplo a teoria dos grupos, e perguntamos será que vale a recíproca do Teorema de Lagrange? Como você não é especialista em teoria dos grupos, é bem provável que não sabe. Assim, pelo terceiro excluso você pode afirmar que a recíproca deste teorema vale ou não vale. Esta afirmação é um pouco digamos ariscada, pois sabendo nada do assunto, afirmar algo já é complicado. Além disso, existem exemplos de afirmações matemáticas, sobre quais uma vez não sabemos até hoje se valem ou não valem, como por exemplo a famosa conjectura de Goldbach, qual postula que todo número par maior ou igual a quatro é soma de dois números primos. Por outro lado, também existem afirmações sobre quais sabemos que não podem ser demonstradas nem as suas negações podem ser demonstradas, como por exemplo o famoso quinto postulado de Euclides sobre paralelismo de retas. Assim, poderíamos questionar a afirmação de que este postulado vale ou não vale? Mais um ponto a favor de negar ou não aceitar o terceiro excluso é que podemos demonstrar com este princípio resultados matemáticos como o seguinte, cf. [6]:

Queremos demonstrar que existem dois números irracionais, i.e., $a, b \in \mathbb{R} \setminus \mathbb{Q}$ tais que $a^b \in \mathbb{Q}$, ou seja, a existência de dois irracionais cuja potência é racional. Elaboramos a seguinte argumentação: Sabemos que $\sqrt{2}$ é irracional, ou seja não pode ser da forma $\frac{a}{b}$, para alguns $a, b \in \mathbb{Z}$. Afirmamos agora, se $\sqrt{2}^{\sqrt{2}}$ for racional então estamos prontos. Caso contrário, o número $\sqrt{2}^{\sqrt{2}}$ é irracional. Mas não temos nenhum problema com isso, pois tomamos agora simplesmente o número $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ o que é racional. Logo, em qualquer dos casos, existem $a, b \in \mathbb{R} \setminus \mathbb{Q}$ tais que $a^b \in \mathbb{Q}$.

O problema desta demonstração é que no final das contas não sabemos se $\sqrt{2}^{\sqrt{2}}$ é racional ou não. O início da lógica intuicionista de Brouwer (1881-1966) e Heyting (1898-1980) (qual entre outros peculiaridades, não aceita o terceiro excluso) foi dada por pensamentos de L.E.J. Brouwer no início do século 20, o seu estudante A. Heyting formalizou estes pensamentos e obteve uma lógica bem funcionando, chamada lógica intuicionista de Brouwer-Heyting. Existem também outras lógicas intuicionistas, quais surgiam após os pensamentos de Brouwer. Para concluir, é preciso saber que o desenvolvimento da lógica intuicionista de Brouwer-Heyting foi forçado com o surgimento de contradições principalmente na teoria dos conjuntos, qual levou para uma crise na matemática, a dita **crise dos fundamentos**, veja também o paradóxo de Russell em 2.1. Para vencer esta crise, pensava-se entre outras soluções também em mudar a lógica, pois a lógica clássica admite as ditas demonstrações por absurdo, cf. 1.4.2, quais de fato são às vezes um pouco obscuras. Claramente, a lógica intuicionista também tem desvantagens se trabalhada matematicamente. O leitor interessado pode consultar mais acerca desta lógica em [6, 10].

Observação 1.2.2. *No final desta seção, queremos ainda observar que o símbolo da igualdade, $=$, é um símbolo lógico, e sempre satisfaz quatro axiomas, quais são os seguintes:*

(a) $\forall x$ temos que $x = x$. (reflexividade)
(b) $\forall x, y$ temos que, se $x = y$ então, $y = x$. (simetria)
(c) $\forall x, y, z$ temos que, se $x = y$ e $y = z$ então, $x = z$. (transitividade)
(d) $\forall x, y$ e para qualquer função f n-ária, se $x = y$ e $f(x_1, \ldots, x, \ldots, x_n) = z$, então $f(x_1, \ldots, y, \ldots, x_n) = z$ (substituição por iguais)

1.3 Linguagem, fórmulas e tabelas de verdade

Nesta seção começamos a desenvolver fundamentos matemáticos bem simples para podermos trabalhar com a lógica clássica. De um ponto de vista ingênuo, queremos atribuir para certas afirmações de uma área a ser escolhida, um valor de verdade, digamos, os valores 0 ou 1. Podemos pensar que o valor 0 significa *falso*, enquanto o valor 1 deve significar *verdadeiro*. Para esta atribuição de valores de verdade para afirmações é preciso esclarecer quais sentenças podemos taxar? Isto leva a um problema de definir sentença. Pensando bem, se quisermos trabalhar com valores de verdade para afirmações do dia a dia, é preciso a formação de frases quais podemos taxar com valores de verdade. Para formar estas frases é preciso uma linguagem e depois precisamos saber como podemos formar fórmulas taxáveis com valores de verdade. Temos então a seguinte

Definição 1.3.1. *A* **linguagem** *L da lógica proposicional (clássica) consiste de*
(i) símbolos de proposição, como $p, q, r, s, \ldots$.
(ii) símbolos lógicos, os conectivos, como $\neg, \wedge, \vee, \rightarrow$.
(iii) símbolos auxiliares, as parenteses, como $($, $)$.

Definição 1.3.2. *Seja L uma linguagem da lógica proposicional. Definimos* **L-fórmula***,* **L-sentença***, ou equivalentemente,* **fórmula bem formada** *por recursão na seguinte maneira:*
$[atom]$ Qualquer símbolo de proposição é uma L-fórmula.
$[con]$ Sejam φ, ψ L-fórmulas. Então, $(\neg\varphi)$, $(\varphi \star \psi)$, onde $\star \in \{\wedge, \vee, \rightarrow\}$ são L-fórmulas.
Nada mais é L-fórmula.
Chamamos as fórmulas obtidas por $[atom]$, também de fórmulas **atômicas***, e as outras fórmulas, de fórmulas* **compostas***, ou,* **complexas***.*

Observação 1.3.3. *(a) As linguagens da lógica proposicional somente se distinguem nos símbolos proposicionais. Os símbolos lógicos, como também os auxiliares pertencem a todas as linguagens proposicionais.*
(b) Observe que os conectivos pertencentes da linguagem L da lógica proposicinal, são de aridades diferentes. O conectivo da negação $\neg$, é um conectivo unário, pois pela definição 1.3.2, de uma L-fórmula φ, obtemos uma nova L-fórmula $(\neg\varphi)$. Os conectivos restantes são conectivos binários, pois é preciso ter duas L-fórmulas φ e ψ para podermos obter $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ e $(\varphi \rightarrow \psi)$.
(c) As variáveis em 1.3.2 são chamadas de **meta-variáveis***. Observe que elas não fazem parte da linguagem L.*
(d) A última definição 1.3.2, dá uma recursão para a construção de fórmulas. Primeiramente, observe que nem toda sequência de símbolos forma uma L-fórmula. Além disso, observe que a definição dada de L-fórmula permite a implementação de um programa computacional para detectar quando uma sequência de símbolos é de fato uma L-fórmula.
(e) A definição 1.3.2 é importante, pois em seguida queremos dar valores de verdade para L-fórmulas. Esta atribuição de valores de verdade não é possível para qualquer sequência de símbolos de L.

Exemplo 1.3.4. *(a) Vamos demonstrar que a sequência dos símbolos $\varphi := ((p \wedge q) \vee (\neg r))$ é uma L-fórmula. De fato. Usando a definição 1.3.2, obtemos que por $[atom]$, p, q e r são L-fórmulas. Por $[con]$, obtemos que $(p \wedge q)$ e $(\neg r)$ são L-fórmulas. Novamente, uma aplicação de $[con]$, mostra que $((p \wedge q) \vee (\neg r))$ é uma L-fórmula.*
(b) Obviamente nem toda sequência de símbolos é L-fórmula. Seja dada $\chi := (p(\neg q))$. Vejamos que χ não pode ser L-fórmula, segundo definição 1.3.2. Por $[atom]$, sabemos que p e q são L-fórmulas. Usando $[con]$, temos que $(\neg q)$ é uma L-fórmula. Agora temos que a sequência dos símbolos χ, não é fórmula atômica, pois ocorre o conectivo $\neg$. Como $\neg$ é o único conectivo ocorrendo em χ, é preciso ter uma fórmula ψ, para obter com $[con]$, uma fórmula do tipo $(\neg\psi)$. Mas com os símbolos p e q não podemos formar uma nova fórmula somente usando o conectivo $\neg$. Consequentemente χ não é L-fórmula.
Nas listas de exercícios temos mais exemplos acerca de L-fórmulas.

Em seguida queremos explicar como os conectivos introduzidos acima funcionam com valores de verdade. Usamos sempre os valores de verdade, 0 e 1. Podemos pensar em 0, o falso, e em 1, o verdadeiro. Pelo princípio do terceiro excluso, somente ocorrem dois valores de verdade.

1.3.1 A negação

Tratamos primeiramente o conectivo da **negação**, $\neg$. Este conectivo é unário, e pode ser lido como *não*. Temos a seguinte tabela de verdade: Seja p um símbolo de proposição.

p	$(\neg p)$
1	0
0	1

A tabela de verdade para a negação, reflete a idéia do conectivo $\neg$ de que a negação de uma proposição verdadeira é falsa, e reciprocamente, de uma falsa é verdadeira.

1.3.2 A conjunção

Tratamos agora a **conjunção**, $\wedge$. Este conectivo é binário, e pode ser lido como *e*. Na tabela de verdade para este conectivo, vejamos que uma conjunção $(p \wedge q)$ somente é verdadeira se, p e q simultaneamente são verdadeiras. Isto reflete a nossa noção da conjunção usada no dia e dia. Sejam p, q proposições.

p	q	$(p \wedge q)$
1	1	1
1	0	0
0	1	0
0	0	0

1.3.3 A disjunção

Tratamos agora a **disjunção**, $\vee$. Este conectivo é binário, e pode ser lido como *ou*. Na tabela de verdade para este conectivo, vejamos que uma disjunção $(p \vee q)$ somente é falsa se, p e q simultaneamente são falsas. Isto reflete a nossa noção da disjunção usada no dia e dia. Sejam p, q proposições.

p	q	$(p \vee q)$
1	1	1
1	0	1
0	1	1
0	0	0

1.3.4 A implicação

Tratamos agora a **implicação**, $\rightarrow$. Este conectivo é binário, e pode ser lido como *implica*. Na tabela de verdade para este conectivo, vejamos que uma implicação $(p \rightarrow q)$ somente é falsa se, p é verdadeira e q é falsa, ou seja, se conseguirmos deduzir algo falso de uma verdade: neste caso, temos um problema, pois assim estamos perdendo a noção entre afirmações verdadeiras e falsas. Sejam p, q proposições.

p	q	$(p \to q)$
1	1	1
1	0	0
0	1	1
0	0	1

Podemos ler $(p \to q)$ de maneiras diferentes como:
(i) Se p então q, ou
(ii) p é suficiente para q, ou
(iii) q é necessário para p, ou (iv) q, se p. ou
(v) p, somente se q.

1.3.5 Tautologias, contradições e fórmulas satisfatíveis

Antes de introduzirmos novos conceitos, exibimos exemplos acerca do cálculo de valor de verdades para fórmulas. Sempre precisamos ter certeza que as fórmulas são de fato bem formadas segundo a definição 1.3.2. O teorema da recursão garante que para qualquer L-fórmula o seu valor de verdade pode ser calculado.

Exemplo 1.3.5. *(a) Seja $\varphi := (p \vee (\neg p))$. Antes do cálculo da tabela de verdade para φ, precisamos verificar que φ é de fato uma L-fórmula. Isto é feito do mesmo modo de que em 1.3.4 e deixamos os detalhes como exercício. Obtemos agora a seguinte tabela de verdade para φ.*

p	$(\neg p)$	$(p \vee (\neg p))$
1	0	1
0	1	1

Vejamos em particular que esta fórmula sempre possui valor de verdade 1.

(b) Seja $\psi := (p \wedge (\neg p))$. Observe que ψ é bem formada (verfique!) e obtemos a tabela:

p	$(\neg p)$	$(p \wedge (\neg p))$
1	0	0
0	1	0

Observe que a fórmula ψ sempre tem valor de verdade 0, na última coluna.

(c) Seja $\chi := ((\neg p) \vee q)$. Observe que χ é bem formada (exercício) e obtemos a tabela de verdade seguinte:

p	q	$(\neg p)$	$((\neg p) \vee q)$
1	1	0	1
1	0	0	0
0	1	1	1
0	0	1	1

Observe que alguns valores de verdade na última coluna da tabela da verdade são 1, mas não todos.

Introduzimos a seguinte definição.

Definição 1.3.6. *Seja φ uma L-fórmula.*
(a) Dizemos que φ é uma **tautologia** *sse na última coluna da tabela da verdade para φ somente ocorre o valor* 1.
(b) Dizemos que φ é uma **contradição** *sse na última coluna da tabela da verdade para φ somente ocorre o valor* 0.
(c) Dizemos que φ é **satisfatível** *sse na última coluna da tabela da verdade para φ ocorre pelo menos um valor* 1.

Exemplo 1.3.7. *Em exemplo 1.3.5, a fórmula φ é uma tautologia, ψ é uma contradição e χ é satisfatível.*

Observe que em nossa linguagem L não ocorre o símbolo da equivalência lógica (sintática) $\leftrightarrow$. Faremos porém a seguinte

Definição 1.3.8. *Sejam φ e ψ L-fórmulas. Abreviamos com $(\varphi \leftrightarrow \psi)$ a L-fórmula $((\varphi \to \psi) \wedge (\psi \to \varphi))$*

Observação 1.3.9. *Podemos verificar que o valor de verdade para a fórmula $(\varphi \leftrightarrow \psi)$ é* 1 *sse φ e ψ têm o mesmo valor de verdade.*

Demonstração: Exercício. ■

Em seguida, introduzimos a implicação e equivalência lógica (semântica) de seguinte modo.

Definição 1.3.10. *Sejam φ e ψ L-fórmulas.*
(a) Dizemos que φ e ψ são **logicamente equivalentes***, $\varphi \Leftrightarrow \psi$, sse $(\varphi \leftrightarrow \psi)$ é uma tautologia.*
(b) Dizemos que φ **implica logicamente** *ψ, $\varphi \Rightarrow \psi$, sse $(\varphi \to \psi)$ é uma tautologia.*

1.4 Métodos de provas na matemática

Em seguida, vamos explicar alguns métodos de demonstração dos resultados matemáticos. Primeiramente, observemos que um resultado matemático, está sendo denominado como **teorema**, **proposição**, **lema**, **observação** ou **corolário**. Além disso, este resultado pode ser enunciado em distintas formas, mas sempre se separa em **hipótese** (também chamada de premissa) e **tese** (também chamada de conclusão). A hipótese é o ponto de partida para a elaboração de uma prova matemática. Supomos que cada hipótese seja verdadeira, e isso não questionamos (observe que pela tabela de verdade, uma implicação sempre é verdadeira se o antecedente for falso, cf. 1.3.4, assim este caso não nós interessa!). Usamos assim as hipóteses (postas como verdadeiras) e com a ajuda de definições e/ou resultados já demonstrados e da lógica matemática deduzimos resultados (às vezes parciais), até chegarmos na tese do resultado. É claro, que uma certa inteligência é preciso em *descobrir* ou *inventar* um racioncínio lógico correto somente usando as hipóteses para chegarmos de fato na tese. Simbolizando um teorema matemático como sendo $\varphi \Rightarrow \psi$, temos que φ é a hipótese e ψ é a tese deste teorema. Podemos então diretamente elaborar uma demonstração usando φ e chegando em ψ. Assim, temos uma **prova direta**.
Além disso, existem alguns métodos específicos (na lógica clássica !) distintos da prova direta, para demonstrarmos os teoremas, e estes métodos estamos querendo explicitar agora.

1.4.1 Prova por contraposição

Simbolizamos um teorema matemático por $\varphi \Rightarrow \psi$. Para mostrar este teorema, podemos usar o método da **demonstração por contraposição**. Para isso, vejamos o seguinte

Exemplo 1.4.1. *Sejam φ e ψ L-fórmulas. Vamos mostrar que as fórmulas $(\varphi \to \psi)$ e $((\neg\psi) \to (\neg\varphi))$ são logicamente equivalentes. Para ver isso, elaboramos a tabela de verdade para a fórmula $\sigma := ((\varphi \to \psi) \leftrightarrow ((\neg\psi) \to (\neg\varphi)))$.*

φ	ψ	$(\varphi \to \psi)$	$(\neg\varphi)$	$(\neg\psi)$	$((\neg\psi) \to (\neg\varphi))$	σ
1	1	1	0	0	1	1
1	0	0	0	1	0	1
0	1	1	1	0	1	1
0	0	1	1	1	1	1

Vimos então que as duas fórmulas são logicamente equivalentes. Como consequência temos um novo método de demonstração matemática, chamado de método da demonstração por **contraposição**. Esta prova funciona assim: Dado um resultado da matemática, formalizado como $\varphi \Rightarrow \psi$, podemos elaborar um raciocínio qual mostra a partir da hipótese $\neg\psi$ a tese $\neg\varphi$. Se esta prova for elaborado de forma correta, sabemos pelo exemplo 1.4.1, que o teorema $\varphi \Rightarrow \psi$ é demonstrado.
Observe que às vezes, é mais fácil demonstrar um teorema pela contraposição do que diretamente. Na lógica clássica, não tem diferença mostrar um teorema direto ou por contraposição, pois vimos a equivalência lógica em exemplo 1.4.1. Na lógica intuicionista de Brouwer-Heyting porém, a afirmação da contraposição é mais fraca do que a afirmação direta. Na seção 1.5, vejamos um exemplo prático deste tipo de prova.

1.4.2 Prova por contradição

Vamos explicar o método da **prova por contradição**, também chamada de **prova por absurdo**. Para isso, introduzimos o conceito de **consistência** e **inconsistência** para um conjunto de fórmulas.

Definição 1.4.2. *Sejam $n \geq 1$ um natural e $\varphi_1, \dots, \varphi_n$ L-fórmulas.*
Dizemos que o conjunto $\{\varphi_1, \dots, \varphi_n\}$ é **consistente** *sse a fórmula $(\dots(\varphi_1 \wedge \varphi_2) \wedge \dots \varphi_{n-1}) \wedge \varphi_n)$ é satisfatível. Caso contrário, o conjunto $\{\varphi_1, \dots, \varphi_n\}$ é* **inconsistente**.

Lema 1.4.3. *Sejam $n \geq 1$ um natural e $\varphi_1, \dots, \varphi_n$ L-fórmulas. São equivalentes*
(a) O conjunto $\{\varphi_1, \dots, \varphi_n\}$ é inconsistente, e
(b) A fórmula $(\dots(\varphi_1 \wedge \varphi_2) \wedge \dots \varphi_{n-1}) \wedge \varphi_n) \to \sigma)$ é uma tautologia, para qualquer L-fórmula σ.

Demonstração: Sejam $n \geq 1$ um natural e $\varphi_1, \dots, \varphi_n$ L-fórmulas. A demonstração dividimos em duas partes.
<u>(a) $\Rightarrow$ (b)</u>: Seja $\{\varphi_1, \dots, \varphi_n\}$ inconsistente, i.e., pela definição 1.4.2, a conjunção das fórmulas $\varphi_1, \dots, \varphi_n$ não é satisfatível. Assim, a fórmula obtida é uma contradição e pela tabela de verdade da implicação, $(\dots(\varphi_1 \wedge \varphi_2) \wedge \dots \varphi_{n-1}) \wedge \varphi_n) \to \sigma)$ é uma tautologia, para qualquer que seja a fórmula σ.
<u>(b) $\Rightarrow$ (a)</u>: Seja $(\dots(\varphi_1 \wedge \varphi_2) \wedge \dots \varphi_{n-1}) \wedge \varphi_n) \to \sigma)$ uma tautologia para qualquer fórmula σ. Em particular, σ pode ser uma contradição da forma $(\varphi \wedge (\neg\varphi))$. Como uma contradição não é satisfatível, ou seja, o seu valor de verdade sempre é 0, é preciso que o valor de verdade para a L-fórmula $(\dots(\varphi_1 \wedge \varphi_2) \wedge \dots \varphi_{n-1}) \wedge \varphi_n)$ também é 0. Assim, o conjunto $\{\varphi_1, \dots, \varphi_n\}$ é inconsistente. ■

Podemos agora explicar e entender o método da prova por contradição.

Observação 1.4.4. *Queremos mostrar o resultado matemático $(\dots(\varphi_1 \wedge \varphi_2) \wedge \dots \varphi_{n-1}) \wedge \varphi_n) \Rightarrow \psi$, ou seja, $\varphi \to \psi$ é uma tautologia, onde $\varphi := (\dots(\varphi_1 \wedge \varphi_2) \wedge \dots \varphi_{n-1}) \wedge \varphi_n)$. Sempre quando as hipóteses $\varphi_1, \dots, \varphi_n$ forem verdadeiras, então ψ é verdadeira. Elaboramos a seguinte demonstração por absurdo: Supomos $\varphi_1, \dots, \varphi_n$ e $(\neg\psi)$ verdadeiras. Após alguns argumentos corretos, obtemos que o conjunto $\{\varphi_1, \dots, \varphi_n, (\neg\psi)\}$ é inconsistente. Assim podemos inferir que sempre sendo a sentança φ verdadeira, a afirmação $(\neg\psi)$ tem que ser falso (por quê?). Portanto neste caso ψ é verdadeira, e mostramos o desejado.*
Na próxima seção, exibimos um exemplo prático deste tipo de prova matemática, cf. 1.5.

1.4.3 Contra-exemplos em matemática

Em matemática, o que nós interessa é, se alguma afirmação φ vale e para ter a certeza *matemática* de que φ vale, é necessário elaborar uma demonstração ou prova matemática. Nas seções anteriores, vimos alguns métodos de demonstrações. Mas, o que acontece se tivermos alguma afirmação matemática ψ, e não sabemos se tal afirmação ψ é válida ou não? O que podemos fazer neste caso?

Temos que ter alguma intuição acerca da afirmação. Tentamos demonstra-lo, e se por acaso não conseguirmos, podemos também procurar um exemplo mostrando que a afirmação ψ não vale, ou seja, procuramos um *contra-exemplo*.

O papel de contra-exemplo sempre é refutar alguma afirmação. Observe que se tivermos um exemplo mostrando que φ não está satisfeita, então não adianta tentar demonstrar φ, pois não pode ser demonstrado mais, pois temos um exemplo refutando φ. Exemplificamos isso em seguida.

Exemplo 1.4.5. *Temos duas afirmações φ e ψ, A afirmação φ postula o seguinte: A soma de dois números inteiros pares sempre é número par. Enquanto, a afirmação ψ postula: Todo múltiplo de um número inteiro ímpar é par.*
Para poder se manifestar sobre φ e ψ, é preciso esclarecer número inteiro e números par e ímpar. Os números inteiros conhecemos do ensino médio, estes são dados pelo conjunto $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
Agora definimos números par e ímpar, do seguinte modo:
Dizemos que $a \in \mathbb{N}$ é **número par** *sse existe $k \in \mathbb{N}$ tal que $a = 2k$. Caso contrário dizemos que um número é* **ímpar**. *Aparentemente a primeira afirmação φ é verdadeira. Tente demontrstá-lo ! A segunda afirmação ψ porém é falsa, como mostra o seguinte contra-exemplo:*

Tome o número 3, e observe que 3 é ímpar, pois $3 = 2 \cdot 1 + 1$. Agora observe que $3 \cdot 3 = 9 = 2 \cdot 4 + 1$, o que é ímpar. Consequentemente, todo múltiplo de um número ímpar não pode ser par. Assim, refutamos a afirmação ψ.

1.5 Um exemplo

Elaboramos agora demonstrações distintas de uma afirmação simples da teoria dos números. Vamos mostrar o seguinte

Fato 1.5.1. *Seja $a \in \mathbb{N}$ um natural. Se a^2 é par, então a é par.*

Demonstração: 1. Prova por contraposição:
Neste tipo de prova assumimos que a é ímpar, ou seja, a é da forma $2k + 1$, para algum $k \in \mathbb{N}$. Vamos mostrar que a^2 é ímpar. Observe que
$a^2 = (2k + 1)^2 = (2k)^2 + 4k + 1^2 = 2(2k^2 + 2k) + 1$, o que de fato é um número ímpar. Por 1.4.1 mostramos então o Fato.

2. Prova por absurdo:
Supomos que para $a \in \mathbb{N}$, a^2 é par e (por absurdo) que a é ímpar. Assim, a é da forma $2k + 1$, para algum $k \in \mathbb{N}$. Como visto acima, $a^2 = 2(2k^2 + 2k) + 1$, ou seja ímpar. Contradição, pois a^2 é par e ímpar, ao mesmo tempo. Por 1.4.2, mostramos então o Fato. ∎

Fica como exercício para o estudante interessado, elaborar uma prova direta do Fato. Terminamos a introdução pequena de conceitos lógicos para a matemática. Será que vale a recíproca do fato 1.5.1? Demonstre ou refute!

Capítulo 2

Conceitos básicos da teoria ingênua de conjuntos

Neste capítulo queremos introduzir alguns conceitos básicos em conjuntos. Não tratamos aqui a teoria axiomática de conjuntos, porém uma abordagem ingênua da teoria dos conjuntos. Antes da exibição de uma axiomática para a teoria dos conjuntos, um conjunto foi pensado como uma coleção de objetos quais têm alguma propriedade. Após apareceram inconsistências na matemática, por volta de 1900, era preciso esclarecer mais o conceito de conjunto. Assim começou o desenvolvimento da axiomática. A axiomática bem conhecida, é a de Zermelo (1871-1953) e Fraenkel (1891-1965), abreviado por ZF, ou ZFC, se incluirmos o axioma da escolha. Mas existem também outras abordagens, como por exemplo a teoria dos tipos de Russell (1872-1970), ou a axiomática de von Neumann (1903-1957), Bernays (1888-1977) e Gödel (1906-1978) (NBG). Em muitas axiomáticas, conjunto e pertenência são os conceitos básicos.

O leitor interessado pode acompanhar em [2, 7, 9, 12] o assunto desta seção, além dos livros [8] e [15].

2.1 Conjunto e paradóxo de Russell

Começamos com a seguinte simples

Notação 2.1.1. *Denotamos por $x \in y$, x* pertence a y *e por $x \notin y$, x* não pertence a y.

Ingenuamente, podemos pensar que um conjunto tem a seguinte forma

$$\{x| \quad \varphi(x)\}, \text{ onde } \varphi(x) \text{ é uma propriedade do elemento } x. \qquad (*)$$

Leia $\varphi(x)$ como "x tem a propriedade φ". Por exemplo temos os seguintes conjuntos:

$a := \{n \in \mathbb{N}| \quad n$ é número par $\}$.

$b := \{n \in \mathbb{N}| \quad n$ é divisível por $3\}$, etc.

Agora observemos que o princípio ingênuo $(*)$ para conjunto pode gerar uma contradição- dependendo da propriedade φ. G.Cantor já teve uma noção de que no princípio ingênuo não toda propriedade deve ser usada. Nos textos dele, Cantor sempre falava de *propriedades bem escolhidas*. Em seguida explicamos o paradóxo de Russell, e isso na mente, sempre sabemos que trabalhando na teoria ingênua de conjuntos, as propriedades escolhidas, são sempre *bem escolhidas*.

Observação 2.1.2. *Pensamos como uma propriedade $\varphi(x) := (x \notin x)$. Pelo princípio ingênuo $(*)$, teríamos então que $R := \{x| \quad x \notin x\}$ seria um conjunto.*
Mas, agora observe que temos a seguinte contradição puramente lógica

$$R \in R \quad \textit{sse} \quad R \notin R.$$

Esta contradição chamamos de **antinomia** *ou* **paradóxo de Russell** *e o não-conjunto R de* **classe de Russell**. *No início do século 20, Bertrand Russell, escreveu para o lógico Gottlob Frege, perguntando, se R seria de fato um conjunto, e pôs com esta pergunta o programa de Frege* de água abaixo, *de deduzir a aritmética da lógica matemática.*
Com esta pergunta também os matemáticos perceberam que o conceito de conjunto - usado até então de maneira ingênua e intuitiva - é preciso ser esclarecido e fundamentado matematicamente. A antinomia de Russell deu início da dita crise dos fundamentos *em matemática. Acontece que a coleção de Russell é muito grande para ser conjunto e assim dizemos que uma coleção muito grande de objetos é uma* **classe**. *Além disso, a propriedade escolhida por Russell aparentemente não seria uma propriedade bem escolhida no sentido de Cantor.*

A próxima observação dá uma possibilidade de evitar o paradóxo de Russell, introduzindo um novo axioma.

Observação 2.1.3. *(***princípio da compreensão***) O seguinte princípio exclui certos tipos de inconsistências dentro da teoria dos conjuntos.*
Sejam a um conjunto e $\varphi(x)$ uma propriedade. Dizemos que a coleção $\{x| \quad x \in a \ \& \ \varphi(x)\}$ é novamente um conjunto.

Em exercício, mostremos que o princípio da comprêensão dissolve de fato a antinomia de Russell., ou seja, não podemos mais deduzir o paradóxo de Russell aplicando este princípio.

Em seguida, vamos trabalhar com o conceito de conjunto ingenuamente, sempre usando propriedades *bem escolhidas* e sempre lembrando que podem existir coleções quais são classes. Uma pergunta importante é sob qual critério, dois conjuntos são iguais. Temos o seguinte

Axioma da extensionalidade
Dois conjuntos a e b são iguais sse a e b contém os mesmos elementos.

Exemplo 2.1.4. *(a) Observe que $\{1, 2, 3\} = \{1, 2, 2, 3, 3, 3, 3, 3\}$, pelo axioma da extensionalidade.*
(b) Sejam a e b objetos ou conjuntos. Temos que
$\{a, b\} \neq \{a\}$ sse $a \neq b$.
Para ver isso, suponha que $a = b$, assim temos por ítem (a) que $\{a, b\} = \{a, a\} = \{a\}$, mostrando $\Rightarrow$ (observe que provamos por contra-posição!). Para ver a outra implicação, seja $a \neq b$, então no conjunto $\{a, b\}$ tem um elemento b qual não pertence a $\{a\}$, e portanto $\{a, b\} \neq \{a\}$.

Definição 2.1.5. *Sejam $n \geq 1$ um natural e $x_1, \ldots, x_n$ objetos ou conjuntos distintos.*
(a) $\{x_1, \ldots, x_n\}$ é o conjunto com os elementos $x_1, \ldots, x_n$.
(b) $\{x_1, x_2\}$ é o conjunto do **par**.
(c) $\{x_1\}$ é o conjunto **unitário**.

A demonstração da seguinte observação fica como exercício.

Observação 2.1.6. *(a) $\{\{x\}\} \neq \{x\}$.*
(b) $y \in \{x_1, \ldots, x_n\}$ sse existe um $i = 1, \ldots n$ tal que $y = x_i$. ∎

Definição 2.1.7. *Dizemos que o conjunto que não contém nenhum elemento é o* **conjunto vazio**, *e denotamo-lo por $\emptyset$.*

Observação 2.1.8. *O conjunto vazio é único.*

Demonstração: Supomos que $\emptyset$ e t sejam conjuntos vazios. Pela definição anterior ambos não contém nenhum elemento, e pela extensionalidade, $\emptyset = t$, mostrando que somente existe um único conjunto vazio. ∎

2.2 Operações sobre conjuntos

Definição 2.2.1. *Sejam a, b conjuntos.*
(a) Dizemos que a é **subconjunto de** *b, $a \subseteq b$, sse $(\forall x)\ (x \in a \to x \in b)$, ou seja, todo elemento de a é elemento de b.*
(b) Dizemos que a é subconjunto **próprio** *de b, $a \subset b$, sse $a \subseteq b$ e $a \neq b$.*

Observação 2.2.2. *(a) O estudante iniciante às vezes tem dificuldades de distinguir a pertenência $\in$ com a inclusão $\subseteq$. Observe que $x \in \{x\}$ mas não $x \subseteq \{x\}$.*
(b) Observe que a relação da inclusão $\subseteq$ é uma relação transitiva, cf. 4.1.1, i.e., para quaisquer conjuntos a, b e c temos que

$$a \subseteq b \quad \& \quad b \subseteq c \quad \Longrightarrow \quad a \subseteq c$$

Mas, obviamente a relação de pertenência $\in$ não satisfaz isso (contra-exemplo?), ou seja, não é transitiva.
(c) O axioma da extensionalidade constata que para conjuntos a e b,

$$a = b \quad sse \quad a \subseteq b \ \ e \ \ b \subseteq a.$$

(d) $\emptyset \subseteq a$, para qualquer conjunto a.

Demonstração: Vamos somente demonstrar o ítem (d) e deixamos os demais ítens para exercício. Precisamos mostrar que $\emptyset \subseteq a$ para qualquer conjunto a. Isto é pela definição 2.2.1, $\forall x(x \in \emptyset) \to (x \in a)$. Por lógica, cf. 1.3.5 (c), esta sentença é equivalente a $\forall x(\neg(x \in \emptyset) \vee (x \in a))$.
Observe que esta sentença sempre é verdadeira, ou seja, uma tautologia, pois $\emptyset$ não contém nenhum elemento e assim vale $\neg(x \in \emptyset)$. Assim, $\emptyset \subseteq a$. ∎

Definição 2.2.3. *Sejam a, b conjuntos.*
(a) Dizemos que $a \cap b := \{x| \quad x \in a \,\&\, x \in b\}$ é a **interseção** *de a e b.*
(b) Dizemos que $a \cup b := \{x| \quad x \in a$ ou $x \in b\}$ é a **união** *de a e b.*
(c) Dizemos que $\mathcal{P}(a) := \{x| \quad x \subseteq a\}$ é o **conjunto das partes** *de a.*
(d) Dizemos que dois conjuntos são **disjuntos** *sse $a \cap b = \emptyset$.*

Observação 2.2.4. *Podemos visualizar conjuntos num diagrama, chamada de diagrama de Venn, para ter alguma noção sobre o que está* acontecendo*, mas alertamos que nenhum desenho, ou seja , nenhum diagrama substitui uma demonstração matemática.*

Exemplo 2.2.5. *(a) $\mathcal{P}(\emptyset) = \{\emptyset\}$.*
(b) $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$.
(c) $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.
(d) Se $x \in a$, então $\{x\} \subseteq a$.

Temos agora um lema qual lista algumas propriedades em conjuntos.

Lema 2.2.6. *Sejam a, b e c conjuntos. Então*
(i) $a \cup a = a$ (idempotência).
(ii) $a \cup (b \cup c) = (a \cup b) \cup c$ (associatividade).
(iii) $a \cup b = b \cup a$ (comutatividade).
(iv) $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$. (distributividade)
(v) Valem as propriedades duais dos ítens (i) até (iv) para conjuntos, i.e., as afirmações obtidas substituindo $\cup$ por $\cap$.
(vi) $a \cup \emptyset = a$ e $a \cap \emptyset = \emptyset$.

Demonstração: Vamos mostrar (i), e deixamos o resto como exercício.

$$x \in a \cup a \quad \text{sse} \quad x \in a \text{ ou } x \in a \quad \text{sse} \quad x \in a.$$

Pelo axioma da extensionalidade, $a \cup a = a$. ∎

Definição 2.2.7. *Sejam a e b conjuntos.*
Dizemos que $a \setminus b := \{x| \quad x \in a \,\&\, x \notin b\}$ é a **diferença** *de a com b. Às vezes, esta diferença é denotado por $a - b$.*

Exemplo 2.2.8. *Em geral, para conjuntos a e b, $a \setminus b \neq b \setminus a$. Basta que elaboramos uma contra-exemplo. Tomemos os conjuntos $a := \{1, 2\}$ e $b := \{1\}$. Assim, temos que $a \setminus b = \{2\} \neq \emptyset = b \setminus a$.*

Definição 2.2.9. *Seja x um conjunto.*
(a) Dizemos que x é **conjunto universal** *sse x contém todos os conjuntos em discussão. Muitas vezes trabalhamos somente com subconjuntos de x, ou seja, trabalhamos em $\mathcal{P}(x)$, neste caso x é conjunto universal.*
(b) Sejam x conjunto universal e $a \in \mathcal{P}(x)$. Denotamos por $\sim a$ o conjunto $x \setminus a$, e dizemos que $\sim a$ é o **complemento de** *a* **relativo em** *x.*

O seguinte lema não é difícil de demonstrar.

Lema 2.2.10. *Sejam x um conjunto e $a \in \mathcal{P}(x)$. Então,*
(a) $\sim (\sim a) = a$,
(b) $\sim \emptyset = x$.
(c) $\sim x = \emptyset$.
(d) $a \cup (\sim a) = x$.
(e) $a \cap (\sim a) = \emptyset$.

Demonstração: Exercício para o estudante. ∎

A próxima proposição denota as leis de *de Morgan*.

Proposição 2.2.11. *(***De Morgan***) Sejam x um conjunto universal e $a, b \in \mathcal{P}(x)$. Então,*
(a) $\sim (a \cap b) = (\sim a) \cup (\sim b)$.
(b) $\sim (a \cup b) = (\sim a) \cap (\sim b)$.

Demonstração: Em exercícios. ∎

Definição 2.2.12. *Sejam a e b conjuntos.*
Dizemos que $a \triangle b := (a \setminus b) \cup (b \setminus a)$ é a **diferença simétrica** *de a e b.*

Lema 2.2.13. *Sejam a e b conjuntos. Então,*
(i) $a \triangle b = b \triangle a$.
(ii) $a \triangle \emptyset = a$.
(iii) $a \triangle a = \emptyset$.

Demonstração: Em exercícios. ∎

Em seguida, queremos generalizar união e interseção para uma família de conjuntos. Temos a seguinte definição.

Definição 2.2.14. *Sejam I um conjunto de índices e $\{a_i\}_{i \in I}$ uma família de conjuntos.*
(a) Seja a família $\{a_i\}_{i \in I}$ não vazio. Definimos a **interseção** *da família $\{a_i\}_{i \in I}$, $\bigcap_{i \in I} a_i$, como sendo o conjunto $\{x| \quad \forall i(i \in I \to x \in a_i)\}$.*
(b) Definimos a **união** *da família $\{a_i\}_{i \in I}$, $\bigcup_{i \in I} a_i$, como sendo o conjunto $\{x| \quad \exists i(i \in I \wedge x \in a_i)\}$.*

Observação 2.2.15. *Dado um conjunto não vazio a podemos abstratamente definir $\bigcup a$ e $\bigcap a$. As definições são obtidas aplicando 2.2.14 de seguinte modo:*
(i) $\bigcup a := \{x| \quad \exists b(b \in a \ \wedge \ x \in b)\}$, e
(ii) $\bigcap a := \{x| \quad \forall b(b \in a \ \to \ x \in b)\}$. ∎

Proposição 2.2.16. *(***De Morgan generalizado***) Sejam I um conjunto de índices e $\{a_i\}_{i\in I}$ uma família não vazio de conjuntos num conjunto universal x. Então*
a) $\sim (\bigcap_{i\in I} a_i) = \bigcup_{i\in I}(\sim a_i)$.
(b) $\sim (\bigcup_{i\in I} a_i) = \bigcap_{i\in I}(\sim a_i)$.

Demonstração: Exercício. ∎

Podemos pensar da interseção como o maior conjunto entre todos os conjuntos, qual contém todos os elementos comuns dos conjuntos a_i na família, ou seja, o maior conjunto que está contido em todos os a_i' s. A união por outro lado, é o menor conjunto entre todos os conjuntos, qual contém todos os elementos dos conjuntos a_i da família, ou seja, o menor conjunto que contém todos os a_i' s.

Exemplo 2.2.17. *(a) $\bigcap\{a, b\} = a \cap b$ e $\bigcup\{a, b\} = a \cup b$. Com isso, é claro que a definição 2.2.14 é de fato a generalização da definição 2.2.3 (a) e (b).*
(b) $\bigcap\{a\} = a$.

2.3 O produto Cartesiano

Definição 2.3.1. *Sejam a, b conjuntos.*
Dizemos que $\langle a; b\rangle := \{\{a\}, \{a, b\}\}$ é o **par ordenado** *segundo Kuratowski. Observe que não necessariamente, $a \neq b$, e em geral $\langle a; b\rangle \neq \langle b; a\rangle$.*

Lema 2.3.2. *Sejam a, b, c e d conjuntos. Então*

$$\langle a; b\rangle = \langle c; d\rangle \quad \textit{sse} \quad a = c \ \ e \ \ b = d.$$

Demonstração: Sejam a, b, c e d conjuntos. Vamos mostrar $\Rightarrow$ e $\Leftarrow$.
($\Rightarrow$): Seja $\langle a; b\rangle = \langle c; d\rangle$. Suponha num primeiro caso que $a = b$. Então temos que $\langle a; b\rangle = \{\{a\}, \{a, a\}\} = \{\{a\}\} = \{\{c\}; \{c, d\}\}$. Como $\{\{a\}\}$ somente contém um elemento, a saber, $\{a\}$, temos pelo axioma da extensionalidade que $\{\{c\}; \{c, d\}\}$ pode conter um só elemento. Assim, $c = d$, e como $a = b$ temos que $a = c = b = d$.
Num segundo caso, supomos que $a \neq b$, então $\langle a; b\rangle$ contém dois elementos e assim, $\langle c; d\rangle$ também contém dois elementos. Logo, $\{a\} \neq \{c, d\}$, e consequentemente, $\{a\} = \{c\}$. Assim, $a = c$. Agora é preciso ter que $\{a, b\} = \{c, d\}$, e com $a = c$, obtemos que $b = d$.
($\Leftarrow$): Sejam $a = c$ e $b = d$, então pela lógica, $\langle a; b\rangle = \langle c; d\rangle$, terminando a prova. ∎

Sabendo o que é um par ordenado podemos introduzir o produto Cartesiano.

Definição 2.3.3. *Sejam a, b conjuntos. Dizemos que $a \times b := \{\langle x; y\rangle | \quad x \in a \,\&\, y \in b\}$ é o* **produto Cartesiano** *entre a e b.*

Exemplo 2.3.4. *Sejam $a := \{0, 1\}$ e $b := \{1, 2\}$. Então, $a \times b := \{\langle 0; 1\rangle, \langle 0; 2\rangle, \langle 1; 1\rangle, \langle 1; 2\rangle\}$. Por outro lado, temos que $b \times a := \{\langle 1; 0\rangle, \langle 2; 0\rangle, \langle 1; 1\rangle, \langle 2; 1\rangle\}$.*
Isso mostra que em geral $a \times b \neq b \times a$.
Tente descobrir qual condição é necessária e suficiente para $a \times b = b \times a$ e demonstre-a.

Temos o seguinte lema.

Lema 2.3.5. *Sejam a, b e c conjuntos. Então,*
(a) $a \times (b \cup c) = (a \times b) \cup (a \times c)$.
(b) $a \times (b \cap c) = (a \times b) \cap (a \times c)$.

Demonstração: Vamos mostrar somente o ítem (a), o outro ítem será demonstrado em exercícios. Observe que usando a definição do produto Cartesiano e da união obtemos que

$\langle x; y\rangle \in a \times (b \cup c)$ sse $(x \in a)$ e $[y \in (b \cup c)]$ sse $(x \in a)$ e $[(y \in b)$ ou $(y \in c)]$ sse $\langle x; y\rangle \in a \times b$ ou $\langle x; y\rangle \in a \times c$ sse $\langle x; y\rangle \in (a \times b) \cup (a \times c)$. ■

2.4 Relações e funções

Definição 2.4.1. *Seja a um conjunto. Dizemos que r é uma* **relação** *(binária) em a sse $r \subseteq a \times a$.*

Exemplo 2.4.2. *Seja a um conjunto.*
(a) A relação vazia $r := \emptyset$ é uma relação em conjunto a, pois $\emptyset \subseteq a \times a$.
(b) Dizemos que $\nabla_a := a \times a$ é a relação **universal** *em a.*
(c) A relação $\Delta_a := \{\langle x; x\rangle | \quad x \in a\}$ é a relação **diagonal** *em a.*
(d) Em $\mathbb{N}$ temos a relação de menor ou igual $\leq_{\mathbb{N}}$, definido de maneira usual seguinte,
$\leq_{\mathbb{N}} := \{\langle n; m\rangle | \quad \exists k \in \mathbb{N}, n + k = m\}$.
(e) Em $\mathbb{Q}$ temos a relação, definida de seguinte maneira $q := \{\langle x; x^2\rangle | \quad x \in \mathbb{Q}\}$.

Definição 2.4.3. *Seja r uma relação em a.*
(a) Dizemos que $dom(r) := \{x | \quad \exists y \in a, \langle x; y\rangle \in r\}$ é o **domínio** *de r.*
(b) Dizemos que $im(r) := \{y | \quad \exists x \in a, \langle x; y\rangle \in r\}$ é a **imagem** *de r.*
Observe que $dom(r) \subseteq a$ e $im(r) \subseteq a$.

Definição 2.4.4. *Sejam a, b conjuntos e $f \subseteq a \times b$ uma relação.*
(a) Dizemos que f é uma **função** *sse $dom(f) = a$ e f é unívoca, i.e., $\forall x \in a, y_1, y_2 \in b$ $(\langle x; y_1\rangle \in f \,\&\, \langle x; y_2\rangle \in f \rightarrow y_1 = y_2)$. Denotamos uma função f como $f : a \rightarrow b, x \mapsto f(x)$.*
O seu **gráfico** *está dado pelo conjunto $\{\langle x; y\rangle | \quad x \in dom(f) = a \,\&\, y = f(x)\}$.*
(b) Dizemos que $codom(f) := b$ é o **contradomínio** *de f.*
Sejam $c \subseteq a$ e $d \subseteq b$.
(c) Dizemos que $f[c] := \{f(x) | \quad x \in c\}$ é a **imagem** *de c por f.*
(d) Dizemos que $f^{-1}[d] := \{x \in a | \quad f(x) \in d\}$ é a **imagem inversa** *de d por f.*
Denotamos por $dom(f)$ e $im(f)$, o domínio e a imagem de f, respectivamente.

Definição 2.4.5. *Seja $f : a \rightarrow b$ uma função.*
(a) Dizemos que f é uma função 1 **a** *1, ou equivalentemente,* **injetiva** *sse $\forall x_1, x_2 \in a, \forall y \in b \quad (f(x_1) = y = f(x_2) \rightarrow x_1 = x_2)$.*
(b) Dizemos que f é uma função **sobre** *b, ou equivalentemente,* **sobrejetiva** *sse $im(f) = b$.*
(c) Dizemos que f é uma **bijeção***, ou equivalentemente,* **bijetiva** *sse f é 1 a 1 e sobre b.*

Observação 2.4.6. *Seja $f : a \rightarrow b$ uma função.*
(a) Podemos dizer em palavras, que f é uma função injetiva, sse nenhum valor em b será assumido mais do que uma vez.
(b) Podemos dizer em palavras, que f é uma função sobre b, sse qualquer valor de b será assumido.
(c) Podemos dizer em palavras, que f é uma função bijetiva, sse é possível de fazer por completo pares entre elementos de a e de b usando f.

Exemplo 2.4.7. *(i) A função identidade no conjunto a, $id_a : a \rightarrow a, x \mapsto x$ é uma função bijetiva.*
(ii) A função $f : \mathbb{N} \rightarrow \mathbb{N}, n \mapsto n^3$ é uma função injetiva. Observe que f não é sobre $\mathbb{N}$, pois $2 \notin im(f)$.
(iii) A função $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^3$ é uma função bijetiva. Demonstre em detalhe esta afirmação.
(iv) A relação $q : \mathbb{R} \rightarrow \mathbb{R}_0^+, x \mapsto x^2$ é uma função sobrejetiva, mas não 1 a 1.

Observação 2.4.8. *Seja $f : a \rightarrow b$ uma bijeção. Então, existe uma bijeção $g : b \rightarrow a$.*

Demonstração: Seja $f : a \to b$ uma bijeção, então f é 1 a 1 e $im(f) = b$. Definimos agora a seguinte aplicação

$$g : b \to a, y \mapsto g(y) := x, \text{ onde } x \text{ é único valor em } a \text{ tal que } f(x) = y.$$

Observe que esta aplicação é de fato uma *boa definição*, ou seja, g é uma função. Como f é uma função 1 a 1, é claro que $g(y) = x$ é bem definido, pois x é único. Por outro lado, como $im(f) = b$, g está definido para qualquer $y \in b$. Consequentemente, g é bem definida e além disso, g é uma bijeção. ∎

Lema 2.4.9. *Seja $f : a \to b$ uma função. Então*
(a) f é sobre $im(f)$.
(b) Se f 1 a 1, então $f : a \to im(f)$ é uma bijeção.

Demonstração: Observe que f é uma função pela hipótese. Assim, $im(f) := \{y| \quad \exists x \in a, \langle x; y\rangle \in f\} \subseteq b$. Tomando $y \in im(f)$, existe $x \in a$ tal que $f(x) = y$. Assim, f é sobre $im(f)$, mostrando o ítem (a).
Como pelo ítem (a), f é sobre $im(f)$ e por hipótese, f é 1 a 1, temos por 2.4.5 (c) que f é bijeção, mostrando ítem (b). ∎

Definição 2.4.10. *(i) Seja $f : a \to b$ uma função e $c \subseteq a$.*
Dizemos que $f_{|c} : c \to b, x \mapsto f(x)$ é a **restrição de f em c**.
(ii) Seja $f : a \to b$ uma função injetiva.
Dizemos que $f^{-1} : im(f) \to a, y \mapsto f^{-1}(y) := x$, onde $f(x) = y$, é a função **inversa de f**.
(iii) Sejam$f : a \to b$ e $g : b \to c$ funções.
Dizemos que $(g \circ f) : a \to c, x \mapsto g(f(x))$ é a função **composta de g com f**.

Exercício 2.4.11. *(i) Escreva o gráfico das funções restrição, função inversa e função composta.*
(ii) Mostre que para uma função $f : a \to b$ e $c \subseteq a$ temos que $f_{|c} \subseteq f$.
(iii) Seja $f : a \to b$ uma função injetiva. Mostre que $dom(f^{-1}) = im(f)$, $im(f^{-1}) = dom(f)$ e $(f^{-1})^{-1} = f$.

Lema 2.4.12. *Sejam$f : a \to b$ e $g : b \to c$ funções.*
(a) Se f e g forem injetivas, então, $(g \circ f)$ é injetiva.
(b) Se $g_{|im(f)}$ for sobre c, então $(g \circ f)$ é sobre c.

Demonstração: Vamos mostrar o ítem (b), e deixamos o ítem (a) como exercício. Seja $g_{|im(f)}$ sobre c, i.e., $\forall z \in c\ \exists y \in im(f)$ tal que $g(y) = z$. $(*)$
Queremos mostrar que $\forall z \in c\ \exists x \in a$ tal que $g(f(x)) = z$.
Observe que por lema 2.4.9, f é sobre $im(f)$, ou seja, $\forall y \in im(f)\ \exists x \in a$ tal que $f(x) = y$. $(**)$
Tomamos agora $z \in c$, obtemos por $(*)$, $y \in im(f)$ tal que $g(y) = z$. Por $(**)$, obtemos $x \in a$ tal que $y = f(x)$. Consequentemente, $z = g(y) = g(f(x))$, ou seja, $(g \circ f)$ é sobre c. ∎

O próximo resultado, dá um critério para funções injetiva e sobrejetiva.

Proposição 2.4.13. *(a) São equivalentes:*
(i) $f : a \to b$ é injetiva.
(ii) $\exists g : b \to a$ função tal que $g \circ f = id_a$. Neste caso, dizemos que f tem uma inversa **à esquerda**.

(b) São equivalentes:
(i) $f : a \to b$ é sobrejetiva.
(ii) $\exists g : b \to a$ função tal que $f \circ g = id_b$. Neste caso, dizemos que f tem uma inversa **à direita**.

Demonstração: Vamos mostrar (a).
(i) $\Rightarrow$ (ii): Seja $f : a \to b$ injetiva. Observe que a função $f^{-1} : im(f) \to a$, cf. 2.4.10, é função inversa de f. É preciso definir a função g. Para isso, seja $x \in a$ arbitrária. Defina

$$g: b \to a, y \mapsto g(y) := \begin{cases} f^{-1}(y), & \text{se } y \in im(f) \\ x, & \text{caso contrário.} \end{cases}$$

Observe que $g \circ f = id_a$, e assim g é inversa à esquerda de f.

(ii) $\Rightarrow$ (i): Seja $g : b \to a$ tal que $g \circ f = id_a$. Vamos mostrar que f é injetiva. Para isso, tomemos $x_1, x_2 \in a$ tais que $f(x_1) = f(x_2) = y \in b$. Como $g \circ f = id_a$, temos que $g(y) = g(f(x_1)) = x_1 = g(f(x_2)) = x_2$, mostrando que f é 1 a 1.

Vejamos agora (b).
(i) $\Rightarrow$ (ii)[1] : Seja $f : a \to b$ sobre b. É preciso definir a função g. Defina

$$g : b \to a, y \mapsto g(y) := x, \text{ onde } x \text{ é tal que } x \in a \text{ e } f(x) = y.$$

Observe que esta definição é boa definição, pois f é sobre b. Além disso, observe que estamos escolhendo um $x \in a$ com a propriedade de que $f(x) = y$, e assim estamos usando o axioma de escolha. Agora, que $(f \circ g)(y) = f(g(y)) = f(x) = y$, ou seja $f \circ g = id_b$, e logo, g é inversa à direita de f.

(ii) $\Rightarrow$ (i): Seja $g : b \to a$ tal que $f \circ g = id_b$. Vamos mostrar que f é sobrejetiva. Para isso, tomemos $y \in b$. Como $f \circ g = id_b$, temos que $f(g(y)) = y$, mostrando que $y \in im(f)$, pois para $x := g(y)$ temos que $f(x) = y$. Logo, $b \subseteq im(f)$ e assim f é sobrejetiva. ■

Corolário 2.4.14. *Seja $f : a \to b$ uma função. São equivalentes*
(i) f é bijeção, e
(ii) f tem inversa à esquerda e à direita. ■

Observação 2.4.15. *Observe que a demonstração da proposição 2.4.13 nós dá uma maneira construtiva de determinar as inversas à esquerda e direita, caso existam. Mais detalhes vejamos am aula de exercícios. Este tipo de demonstrações é bom não somente porque demonstra um resultado, como também dá um modo de obter o resultado em um caso especial.* ■

2.5 Cardinalidade de um conjunto

Queremos comparar o número de elementos de dois conjuntos dados, sem uso de muitos ferramentos. Imaginemos que temos dois sacos de feijão e queremos saber qual saco tem mais grãos de feijão do que o outro. Suponhamos que não podemos contar, pois não dispomos de números. Um processo muito simples de comparar a quantidade de grãos dos dois sacos é simples e forma um algoritmo:

Denotamos por p_1 e p_2 os dois sacos de feijão. Elaboramos o seguinte processo
(a) tiramos do saco p_1 um grão, e em seguida, do saco p_2. Deixamos os dois grãos do lado.
(b) Repetimos este processo, até um pacote não conter mais elementos.
Agora podem entrar três casos:
(i) Se em p_1 não tem grão, então o saco p_2 contém mais grãos, caso exista um grão em p_2.
(ii) Se em p_1 tem um grão, mas em p_2 não, então em p_1 tem mais grãos do que em p_2.
(iii) Se nem em p_1 nem em p_2 tiver grãos, então nos dois sacos têm o mesmo número de grãos.

Observe que estamos construindo uma função, digamos f, de p_1 para p_2. O resultado é o seguinte:
Em caso (i) a função f é injetiva, mas não sobrejetiva. Em caso (ii), a função f é sobrejetiva, se colocamos os grãos restantes de p_1 em correspondência com um grão arbitrário do saco p_2. Finalmente, em caso (iii), a função f é bijetiva.

Este processo, funciona aparentemente para uma boa parte de conjuntos. Em geral, podemos definir

[1] Observe que esta demonstração depende do axioma da escolha (AC), qual é um axioma importante da teoria dos conjuntos permitindo escolher elementos dentro de um conjunto dado, cf [9].

Definição 2.5.1. *Sejam a e b dois conjuntos.*
(a) Denotamos por $|a|$ o número de elementos do conjunto a, também chamamos $|a|$ de cardinalidade de a.
(b) Dizemos que os dois conjuntos a e b têm a **mesma cardinalidade**, *ou equivalentemente, são* **equipotentes** *sse existe uma bijeção $f : a \to b$.*
(c) Dizemos que a é **finito** *sse $a = \emptyset$ ou existe um $n \in \mathbb{N}$ tal que existe uma função injetiva $f : a \to \{0, 1, \ldots, n\}$.*
(d) Dizemos que a é um conjunto **enumerável** *sse a é finito ou existe uma função $f : a \to \mathbb{N}$ bijetiva.*
(e) Dizemos que a é um conjunto **não-enumerável** *sse a não é enumerável.*

O conceito de infinito é muitas vezes difícil de entender. O matemático G. Cantor (1845-1918) foi um dos primeiros matemáticos a trabalhar com conjuntos infinitos e foi ele quem desenvolveu métodos importantes para comparar conjuntos infinitos. Um método muito importante, devido a G. Cantor, vejamos nesta seção, é o **método diagonal** de Cantor, mais precisamente vejamos dois métodos diagonais em seguida. Temos a seguinte observação, antes de explicar os infinitos $\mathbb{N}, \mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$.

Observação 2.5.2. *(a) Imaginemos que temos um saco qual contém um número infinito de objetos. Agora tiramos deste saco um número infinito de objetos. A pergunta qual fazemos é que quantos objetos restam neste saco? Pense numa solução.*
(b) A segunda observação é sobre o **Hotel de Hilbert**. *Neste hotel de Hilbert, temos um número infinito de quartos a disposição, todos numerados. Acontece que todos os quartos são ocupados, e chega mais um hôspede, qual gostaria de um quarto para si. Será que este hôspede pode ser acolhido? Parece que não, mas pensando mais um pouco podemos fazer o seguinte truque trocando hôspedes e seus quartos. Podemos pensar em mandar o hôspede do primeiro quarto para o segundo, este do segundo para o terceiro, este do terceiro para o quarto, e assim continuando. Deste modo, todos os hôspedes estão com quartos, mas agora o primeiro quarto está vazio para poder abrigar o hôspede qual chegou. O que acontece se chegam mais dois hôspedes, será que podemos abriga-los? E se chega mais um número finito k de hôspedes? Pense sobre isso e tente uma solução. Como já temos este hotel de Hilbert com infinitos quartos, o que podemos fazer se o hotel é lotado e chega mais um número infinito de hôspedes? Será que podemos arrumar um quarto para cada um destes sem mandar nenhum dos hôspedes já hospedados embora?*

Observação 2.5.3. *Seja a um conjunto infinito.*
Então existe um subconjunto infinito enumerável próprio de a.

Demonstração: Seja a infinito. Tomemos agora $x \in a$ arbitrário, e consideremos $b := a \setminus \{x\}$.
Obviamente, b ainda é infinito. Caso contrário, b finito, implicaria que a seria finito. Absurdo. Iniciamos agora o processo de escolher[2] o subconjunto infinito próprio de b. Tome $x_1 \in b$, e observe que $b \setminus \{x_1\}$ é infinito. Por recursão, tomamos $x_n \in b \setminus \{x_1, \ldots, x_{n-1}\}$, para todo $n \geq 2$.
Assim, obtemos o subconjunto $\{x_i| \quad i \in \mathbb{N}\}$ próprio de a. ■

Observação 2.5.4. *Os conjuntos $\mathbb{N}$ e $\mathbb{Z}$ têm um número enumerável de elementos, e são equipotentes.*

Demonstração: É claro que os conjuntos são infinitos. De primeira vista, poderíamos achar que em $\mathbb{Z}$ tem mais elementos do que em $\mathbb{N}$. Isto não é verdade.
Para mostrar que $\mathbb{N}$ e $\mathbb{Z}$ são equipotentes, vamos exibir uma bijeção $f : \mathbb{Z} \to \mathbb{N}$. Defina

$$f : \mathbb{Z} \to \mathbb{N}, k \mapsto f(k) := \begin{cases} 2k, & \text{se } k \geq 0 \\ -2k-1, & \text{caso contrário, ou seja, se } k < 0. \end{cases}$$

Observe que f está bem definida, ou seja, $f(k) \in \mathbb{N}$. Vejamos agora que f é sobre $\mathbb{N}$. Para isso, tome $n \in \mathbb{N}$. Assim, n pode ser par ou ímpar.

[2] O leitor atento deve ter percebido que na hora do uso da palavra *ecolher* estamos mais uma vez usando o axioma de escolha da teoria dos conjuntos

Se n for par, temos que n é da forma $2t$, para algum $t \in \mathbb{N}$. Assim, tome $k = t$, e observe que $f(t) = 2t = n$. Se n for ímpar, temos que n é da forma $2t - 1$, para algum $t > 0$. Assim, tome $k = (-t) \in \mathbb{Z}$, e observe que $f(k) = f(-t) = -2(-t) - 1 = 2t - 1 = n.$
Obviamente, f é 1 a 1. Assim f é uma bijeção e os dois conjuntos são equipotentes, ou seja, em $\mathbb{Z}$ tem tantos elementos quanto em $\mathbb{N}$.

Observação 2.5.5 (1° Método Diagonal de Cantor)**.** *Explicamos o primeiro método diagonal de Cantor, mostrando que os números naturais e as frações positivas, i.e.,* $\mathbb{Q}^+ := \{\frac{a}{b}| \quad a, b \in \mathbb{Z}^+ \ \& \ a, b \neq 0\}$*, são equipotentes. Ordenamos as frações de modo seguinte e enumeramos de direita para a esquerda via diagonal, indicado pelos números nas parenteses*[3]*, obtemos a seguinte arrumação.*

$$\begin{array}{ccccc}
\frac{1}{1}\ (1) & \frac{1}{2}\ (2) & \frac{1}{3}\ (5) & \frac{1}{4}\ (6) & \dots \\
\frac{2}{1}\ (3) & \frac{2}{2}\ (\cdot) & \frac{2}{3}\ (7) & \frac{2}{4} & \dots \\
\frac{3}{1}\ (4) & \frac{3}{2}\ (8) & \frac{3}{3}\ (\cdot) & \frac{3}{4} & \dots \\
\frac{4}{1}\ (9) & \frac{4}{2}\ (\cdot) & \frac{4}{3} & \frac{4}{4} & \dots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Assim, obtemos então a seguinte enumeração:

$$\begin{array}{cccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \dots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\frac{1}{1} & \frac{1}{2} & 2 & 3 & \frac{1}{3} & \frac{1}{4} & \frac{2}{3} & \frac{3}{2} & \frac{4}{1} & \dots
\end{array}$$

Observe que consideremos somente frações novas ocorrendo na lista. Agora é fácil de estabelecer a bijeção entre todos os números racionais e os naturais, somente colocando o número zero na frente e após cada racional positivo colocamos o mesmo número somente com sinal negativo. Assim, obtemos a seguinte enumerção:

$$\begin{array}{ccccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \dots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
0 & \frac{1}{1} & -\frac{1}{1} & \frac{1}{2} & -\frac{1}{2} & 2 & -2 & 3 & -3 & \frac{1}{3} & \dots
\end{array}$$

Assim, em $\mathbb{Q}$ tem tantos elementos do que em $\mathbb{N}$. ■

Tendo em vista as observações acima, poderíamos pensar que qualquer conjunto infinito pode ser enumerado, mas isto não é verdade. Vamos observar que existem conjuntos infinitos quais não podemos enumerar, ou seja, existe infinito não enumerável. Tomamos o conjunto dos números reais $\mathbb{R}$.

Teorema 2.5.6. *(Cantor, 2° Método diagonal) O conjunto $\mathbb{R}$ dos números reais não é enumerável.*

Demonstração: A demonstração deste teorema faz uso do segundo argumento de diagonal de Cantor. Suponha que $\mathbb{R}$ é de fato enumerável, assim, existiria uma bijeção $f : \mathbb{N} \to \mathbb{R}$. Basta mostramos que não existe uma função $f : \mathbb{N} \to \mathbb{R}$ sobre. Como $[0; 1] \subseteq \mathbb{R}$, basta ver que não temos uma função sobre $f : \mathbb{N} \to [0; 1]$. Para ver isso, tomamos uma função $f : \mathbb{N} \to [0; 1]$ arbitrária e exibimos um elemento $x \in [0; 1]$ tal que $x \notin im(f)$. Logo, f não será sobre $[0; 1]$.

Para qualquer $n \in \mathbb{N}$ escrevemos $f(n)$ em decimal:

$f(0) := 0, a_{00}a_{01}a_{02}a_{03}\dots$
$f(1) := 0, a_{10}a_{11}a_{12}a_{13}\dots$

[3] a parentese $(\cdot)$ significa que não contamos, pois o número já foi contado antes.

$f(1) := 0, a_{20}a_{21}a_{22}a_{23}\ldots$
$f(1) := 0, a_{30}a_{31}a_{32}a_{33}\ldots$
$f(1) := 0, a_{40}a_{41}a_{42}a_{43}\ldots$
$\vdots$
$f(n) := 0, a_{n0}a_{n1}a_{n2}a_{n3}\ldots$
$\vdots$

onde $a_{ij} \in \{0, 1, \ldots, 9\}$ para $i, j \in \mathbb{N}$ são os dígitos do número dezimal.

Tomemos agora o seguinte número $x := 0, b_0b_1b_2b_3\ldots \in [0; 1]$ definido como

$$b_n := \begin{cases} 1 & \text{se } a_{nn} = 2 \\ 2 & \text{se } a_{nn} \neq 2 \end{cases}$$

Obviamente, $x \in \mathbb{R}$. Pela construção temos que $x \neq f(n)$ para todo $n \in \mathbb{N}$. Assim, $x \notin im(f)$ e portanto, $[0; 1]$ não é enumerável. Consequentemente, $\mathbb{R}$ não é enumerável. ■

Capítulo 3

Axiomática de Peano, indução e recursão

Neste capítulo, explicamos como podemos justificar matematicamente os números naturais, introduzindo-os pela axiomática de Peano, às vezes conhecido sob o nome de axiomática de Dedekind-Peano. Além disso, explicamos conceitos como indução, o princípio de boa ordem e recursão. Todos estes conceitos são fundamentais para um estudo da ciência da computação.

O leitor interessado pode acompanhar vários assuntos desta seção em [4, 8, 11, 15].

3.1 A axiomática de Peano

Começamos com uma citação do matemático Leopold Kronecker:

"*Deus criou os números naturais. O resto é obra dos homens.*"

Os números naturais foram usados durante muito tempo como digamos *dado por deus* ou seja, sem nenhum fundamento matemático. No século 19, Giuseppe Peano (1858-1932) introduziu uma axiomática para fundamentar os naturais matematicamente. Peano era um lógico matemático e distinguiu entre aritmética e lógica - abodagens e ideias novas na época. Na mesma época (por volta de 1879), Gottlob Frege (1848-1925) começou a escrever e terminar o seu *Begriffsschrift*, onde a lógica matemática foi tratada de maneira simbolizada com regras lógicas e com notação bidimensional. Aparentemente, Peano não conhecia o trabalho de Frege, e trabalhou acerca da lógica matemática através de ideias de Boole e Schröder. Entre os axiomas de Peano, foram inicialmente também citados os quatro axiomas acerca da igualdade entre números, cf. 1.2.2. Porém, a igualdade pertence a lógica, i.e., a igualdade é um símbolo lógico, e os quatro axiomas são subentendidos na lógica. logo, não é preciso enunciá-los cada vez falando de uma teoria matemática. Assim, podemos resumir os axiomas de Peano em três axiomas.

Os conceitos básicos são *número natural* e assim o conjunto dos números naturais $\mathbb{N}$, *número zero*, abreviado por 0 e a função *sucessor*, abreviado por $S : \mathbb{N} \to \mathbb{N}$.

Observação 3.1.1. *(***A axiomática de Peano***) Existem um conjunto $\mathbb{N}$ dos números naturais, uma constante $0 \in \mathbb{N}$ e uma função $S : \mathbb{N} \to \mathbb{N}$, satisfazendo*

(i) $0 \notin im(S)$, i.e., não existe $n \in \mathbb{N}$ tal que $0 = S(n)$.

(ii) S é uma função injetiva.

(iii) O princípio da Indução Completa:

Se $A \subseteq \mathbb{N}$ é tal que (a) $0 \in A$ e (b) sempre quando $n \in A$, então $S(n) \in A$, então $A = \mathbb{N}$.

Observação 3.1.2. *A axiomática de Peano descreve a estrutura dos naturais. O primeiro axioma garante o elemento 0 é o como dizemos* primeiro elemento *em $\mathbb{N}$. Já os primeiro e segundo axiomas, não permitem uma certa ordem digamos* circular *dos naturais, como também a existência de um natural maior. O último*

axioma dá conta do fato de que um natural ou é 0 *ou é um sucessor de um outro natural. Este axioma é importante, pois não permite a existência de números naturais entre* n *e* $S(n)$.
Intuitivamente, podemos pensar que a função S *é simplesmente a adição "mais um".*

Notação 3.1.3. *Denotamos* $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$.

Proposição 3.1.4. *Com as notações de cima,* $im(S) = \mathbb{N}^*$.

Demonstração: Fazemos a prova por indução sobre $n \in \mathbb{N}$. Primeiramente, observe que se conseguirmos mostrar que $im(S) \cup \{0\} = \mathbb{N}$, então temos a afirmação da proposição. Tomemos agora $A := im(S) \cup \{0\}$ e usamos o axioma (iii) de 3.1.1 para mostrar que $A = \mathbb{N}$.
Num início da indução observe que $0 \in A$, pois $0 \in \{0\}$ e assim vale ítem (a) de axioma (iii) de 3.1.1.
No passo da indução, supomos como *hipótese da indução*, $n \in A$. Queremos mostrar que $S(n) \in A$. Observe que de $n \in A$, temos que $n \in \mathbb{N}$ e consequentemente, $S(n) \in im(S)$. Logo $S(n) \in A$. Pelo princípio da indução completa, $A = \mathbb{N}$, terminando a demonstração. ∎

Antes de demonstrar algumas propriedades acerca dos números naturais, enunciamos algumas definições.

Definição 3.1.5. *Seja* $n \in \mathbb{N}$ *um natural. Dizemos que* $S(n)$ *é o* **sucessor** *de* n. *Neste caso também dizemos que* n *é o* **antecessor** *de* $S(n)$.

Para poder trabalhar adequadamente com os naturais, é preciso saber da adição e da multiplicação dos naturais. Temos a seguinte

Definição 3.1.6. *(Soma de naturais) Seja* m *um natural. Definimos por recursão*

$$\begin{cases} m + 0 := m \\ m + S(n) := S(m+n) \end{cases} \tag{3.1}$$

É preciso verificar que esta definição de fato define a adição para quaisquer dois números naturais m e n. Podemos demonstrar isso por indução na próxima proposição, mas observemos que isso também segue do *Teorema da recursão* enunciado em seção 3.3.

Proposição 3.1.7. *Sejam* $m, n \in \mathbb{N}$. *Então, a soma* $m + n$ *é definida pela definição 3.1.6.*

Demonstração: Seja $m \in \mathbb{N}$ um natural fixo. Tomemos o conjunto $A := \{n \in \mathbb{N} | \quad m + n$ é definida $\}$. Observe que $A \subseteq \mathbb{N}$. Vamos usar o axioma da indução de 3.1.1. Inicialmente, observe que $0 \in A$, pois $m+0 = m$ por 3.1, e assim é definido $m+0$. No passo da indução temos por hipótese da indução que $m+n$ é definida. Vejamos que $m + S(n)$ é definida. Pela definição 3.1.6, observe que $m + S(n) = S(m + n)$, e como $m+n$ é definida, temos que $S(n+m)$ é definida, e portanto $n+S(m)$ é definida. Assim, mostramos que $A = \mathbb{N}$. ∎

Proposição 3.1.8. *(Associatividade) Sejam* $m, n, p \in \mathbb{N}$. *Então,* $(m + n) + p = m + (n + p)$.

Demonstração: Exibimos mais uma vez uma prova por indução. Sejam os naturais m e n fixos, e mostramos por indução em p que $(m + n) + p = m + (n + p)$ para todo $p \in \mathbb{N}$. Tomemos assim $A := \{p \in \mathbb{N} | \quad (m + n) + p = m + (n + p)\}$.
Início da indução: $0 \in A$, pois $(m + n) + 0 = m + n$ por definição 3.1.6. Por outro lado, temos que $m + (n + 0) = m + n$, também por 3.1.6.
Passo da indução: Temos por hipótese da indução que $n \in A$, ou seja, $(m + n) + p = m + (n + p)$. Vamos mostrar que $S(n) \in A$. Para isso, observe que usando 3.1, a hipótese de indução e novamente 3.1:
$(m + n) + S(p) = S((m + n) + p) = S(m + (n + p)) = m + S((n + p)) = m + (n + S(p))$, ou seja, $S(p) \in A$.
Pelo axioma (iii) de 3.1.1, temos que $A = \mathbb{N}$, ou seja, vale a afirmação da proposição. ∎

Proposição 3.1.9. *(Elemento neutro) Seja $m \in \mathbb{N}$. Então,*

$$m + 0 = m = 0 + m \tag{3.2}$$

Demonstração: Observe que por 3.1, temos que $m + 0 = m$. Falta mostrar que $0 + m = m$, para todo $m \in \mathbb{N}$. Para isso, tomamos $A := \{m \in \mathbb{N} | \quad 0 + m = m\}$. Observe que por 3.1, $0 + 0 = 0$ e portanto $0 \in A$. Para o passo de indução, temos usando 3.1 e a hipótese da indução o seguinte:
$0 + S(m) = S(0 + m) = S(m)$, e assim, $S(m) \in A$. Logo, vale 3.2. ∎

Observação 3.1.10. *O elemento 0 é único elemento em $\mathbb{N}$ satisfazendo 3.2.*

Demonstração: Sejam 0 e $0'$ dois elementos de $\mathbb{N}$, satisfazendo 3.2. Vamos mostrar que $0 = 0'$. Observe que para qualquer $m \in \mathbb{N}$ temos que $m + 0' = m = 0' + m$. Em particular, usando isso e 3.2 para $m = 0$, temos que $0' = 0 + 0' = 0$. ∎

Definição 3.1.11. *Definimos $1 := S(0)$.*

As provas dos próximos dois resultados deixamos como exercícios. Uma simples indução junto com os resultados obtidos anteriormente resolvem isto.

Proposição 3.1.12. *Para qualquer $n \in \mathbb{N}$, temos que $S(n) = 1 + n$.* ∎

Proposição 3.1.13. *(Comutatividade) Para quaisquer $n, m \in \mathbb{N}$, temos que $n + m = m + n$.* ∎

Falta definir a multiplicação de dois naturais. Para isso, precisamos a adição a as suas propriedades introduzidas anteriormente. Temos por recursão a seguinte

Definição 3.1.14. *(Produto de naturais) Seja m um natural. Definimos por recursão*

$$\begin{cases} m \cdot 0 := 0 \\ m \cdot S(n) := (m \cdot n) + m \end{cases} \tag{3.3}$$

Como acima é preciso demonstrar a seguinte

Proposição 3.1.15. *Sejam $m, n \in \mathbb{N}$. Então, o produto $m \cdot n$ é definida pela definição 3.1.14.* ∎

Observação 3.1.16. *Na lista de exercícios temos algumas propriedades para o produto de números naturais.*

Finalizando a seção sobre os naturais, introduzimos ainda a relação de *menor ou igual* entre números naturais, como segue.

Definição 3.1.17. *Sejam $n, m \in \mathbb{N}$ naturais. Dizemos que n é* **menor ou igual** *a m, $n \leq m \quad$ sse $\quad$ existe $k \in \mathbb{N}$ tal que $n + k = m$.*

Notação 3.1.18. *Denotamos $n < m$ para $n \leq m$ e $n \neq m$, para números naturais n e m.*

As demonstrações dos ítens da próxima observação é feito nos exercícios.

Observação 3.1.19. *A relação introduzido em 3.1.17 satisfaz*
(a) $\forall n \in \mathbb{N}, \quad n \leq n$. (reflexividade)
(b) $\forall n, m \in \mathbb{N}, \quad$ se $n \leq m$ & $m \leq n$, então $n = m$. (anti-simetria)
(c) $\forall n, m, p \in \mathbb{N}, \quad$ se $n \leq m$ & $m \leq p$, então $n \leq p$. (transitividade)
(d) $\forall n, m \in \mathbb{N}, \quad n \leq m$ ou $m \leq n$. (conexão) ∎

3.2 Indução e Boa Ordem

Na seção anterior vimos na axiomática de Peano o princípio da indução completa. Este princípio sempre apliquemos quando é preciso demonstrar alguma propriedade sobre os números naturais do tipo

$$\forall n \in \mathbb{N} \text{ vale } \ldots$$

Nesta seção, vejamos mais duas versões do princípio da indução e o princípio da boa ordem. Exibimos demonstrações quais mostram que todos estes princípios são equivalentes.

Observação 3.2.1. *(Princípio da indução 1^a forma) Seja φ uma propriedade para naturais tal que*

(i) 0 tem a propriedade φ, i.e., $\varphi(0)$, e

(ii) Se $\varphi(k)$ for verdadeira então $\varphi(k+1)$ é verdadeira.

Então, $\varphi(n)$ é verdadeira para qualquer $n \in \mathbb{N}$.

Observação 3.2.2. *(Princípio da indução 2^a forma) Seja φ uma propriedade para naturais tal que*

(i) 0 tem a propriedade φ, i.e., $\varphi(0)$, e

(ii) Se $\varphi(r)$ for verdadeira para qualquer $0 \leq r \leq k$, $k > 0$ então $\varphi(k+1)$ é verdadeira.

Então, $\varphi(n)$ é verdadeira, para qualquer $n \in \mathbb{N}$.

Proposição 3.2.3. *São equivalentes*

(a) O princípio da indução completa, cf. 3.1.1, e

(b) O princípio da indução 1^a forma, cf. 3.2.1

Demonstração: (a) $\Rightarrow$ (b): Vale o princípio da indução completa. Queremos mostrar que vale o princípio da indução 1^a forma, cf. 3.2.1. Seja φ uma propriedade, e tomemos o conjunto $A := \{n \in \mathbb{N} | \quad \varphi(n)\}$.
Observe que, como $\varphi(0)$ é verdadeira (por (i) de 3.2.1), temos que $0 \in A$.
Agora sabemos que $\varphi(k)$ é verdadeira, i.e., $k \in A$. Assim, podemos aplicar (iii) (b) de 3.1.1, e obtemos que $k+1 \in A$. Mas isto é, $A = \mathbb{N}$ e assim, $\varphi(n)$ é verdadeira para qualquer $n \in \mathbb{N}$.
(b) $\Rightarrow$ (a): Seja agora $A \subseteq \mathbb{N}$ um conjunto satisfazendo os ítens (a) e (b) de (iii) em 3.1.1. Defina então $\varphi(n) := (n \in A)$.
Como $0 \in A$, temos que $\varphi(0)$ é verdadeira. Seja agora $n \in A$, i.e., $\varphi(n)$ é verdadeira. Pela hipótese, em (a) temos que $n+1 \in A$, e assim $\varphi(n+1)$ é verdadeira. Pelo princípio da indução em (b), temos que $\varphi(n)$ é verdadeira, para qualquer $n \in \mathbb{N}$. Logo, $\mathbb{N} \subseteq A$ e consequentemente, $A = \mathbb{N}$, acabando a demonstração. ■

Uma outra equivalência dos princípios da indução é o princípio da Boa Ordem, um princípio sendo usado quando trabalhamos com números inteiros.

Observação 3.2.4. *(O princípio da Boa Ordem) Seja $A \subseteq \mathbb{Z}$ um conjunto não vazio de números inteiros não negativos. Então, existe em A um menor elemento, i.e., existe $m \in A$ tal que $m \leq a$ para todo $a \in A$.*

Vejamos agora a equivalência dos princípios.

Teorema 3.2.5. *São equivalentes:*

(a) o princípio da boa ordem, cf. 3.2.4.

(b) o princípio da indução 1^a forma, cf. 3.2.1, e

(c) o princípio da indução 2^a forma, cf. 3.2.2.

Demonstração: (a) $\Rightarrow$ (b): Vale o princípio da boa ordem, e seja φ uma propriedade satisfazendo (i) e (ii) de 3.2.1. É preciso mostrar que $\varphi(n)$ para todo $n \in \mathbb{N}$. Suponha que não, i.e., o conjunto $A := \{n \in \mathbb{N} | \quad \varphi(n)$ é falso $\}$ não é vazio. Além disso, A somente contém números não negativos e assim pelo princípio da boa ordem um menor elemento, digamos $m \in A$. Agora, $m = 0$ não pode ocorrer, pois $\varphi(0)$ é verdadeira. Assim $m > 0$, e como m é menor elemento é preciso ter que $m - 1 \notin A$, ou seja, $\varphi(m-1)$ é verdadeira.

Aplicando a hipótese (ii) de 3.2.1, temos então $\varphi(m)$ é verdadeira, o que é um absurdo pois, $m \in A$. Consequentemente, $A = \emptyset$ e mostramos 3.2.1.

(b) $\Rightarrow$ (c): Vale o princípio da indução 1^a forma, e seja φ uma propriedade satisfazendo (i) e (ii) de 3.2.2. É preciso mostrar que $\varphi(n)$ para todo $n \in \mathbb{N}$. Para isso, é preciso definirmos $\psi(n) := \forall j \in \mathbb{N},\ 0 \leq j \leq n,\ \varphi(j)$. Observe que ψ satisfaz os ítens (i) e (ii) de 3.2.1. Usando então 3.2.1, temos que $\psi(n)$ para qualquer $n \in \mathbb{N}$. Logo $\varphi(n)$ é verdadeira para qualquer $n \in \mathbb{N}$.

(c) $\Rightarrow$ (a): Vale o princípio da indução 2^a forma. Vamos mostrar que vale o princípio da boa ordem. Para isso, demonstraremos a contrapositiva da boa ordem, ou seja, se $A \subseteq \mathbb{Z}$ um conjunto não vazio de elementos não negativos não possui menor elemento, então A é vazio. Seja $A \subseteq \mathbb{N}$ sem menor elemento. Tomemos a propriedade $\varphi(n) := (n \notin A)$. Assim, observe que $0 \notin A$. Caso contrário, 0 seria o menor elemento. Seja agora $k > 0$ tal que $\varphi(r)$ para qualquer $r \in \{0, \ldots, k\}$. Observe que $\varphi(k+1)$ é verdadeira. De fato. Como $r \notin A$ para qualquer $r \in \{0, \ldots, k\}$, temos que $k+1 \notin A$. Caso contrário, $k+1$ seria o menor elemento, absurdo. Assim, mostramos que para qualquer $n \in \mathbb{N},\ n \notin A$. Logo, $A = \emptyset$. ∎

Exibimos agora alguns exemplos de demonstração por indução.

Exemplo 3.2.6. *(a) Vamos mostrar que* $\quad \sum_{k=0}^{n} k = \frac{n(n+1)}{2}. \quad \forall n \in \mathbb{N} \quad (*)$
Usamos a indução (1^a forma), cf. 3.2.1 e começamos pelo
Início da indução, $n = 0$: Observe que para o lado esquerdo, $\sum_{k=0}^{0} = 0$. Para o lado direito, calculamos $\frac{0(0+1)}{2} = 0$. Assim coincidem os dois lados e provamos a afirmação $(*)$ para $n = 0$.
Passo da indução: Vale $(*)$ para n, observe que isto é a hipótese da indução. Vejamos que $(*)$ vale também para $(n+1)$. Para isso, calculamos usando a definição da soma e a hipótese da indução:

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n^2+3n+2}{2}.$$

Por outro lado, temos que $\frac{(n+1)(n+2)}{2} = \frac{n^2+3n+2}{2}$, mostrando $(*)$ para $n+1$. Pelo princípio da indução temos que $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}. \quad \forall n \in \mathbb{N}$. ∎

(b) Definimos a série de **Fibonacci** *no seguinte modo por recursão:*

$$\begin{cases} a_0 := 1, \quad a_1 := 1 \\ a_{n+2} := a_n + a_{n+1}, \quad \forall n \geq 0 \end{cases} \tag{3.4}$$

Vamos mostrar que $\quad a_n < (\frac{7}{4})^n, \quad \forall n \geq 1 \quad (**)$
Elaboramos a prova por indução (2^a forma), cf. 3.2.2. O início da indução para $n = 1$ é trivial.
Vejamos agora o passo da indução e para isso, seja $n > 1$. Vamos mostrar que $a_{n+1} < (\frac{7}{4})^{n+1}$. Temos as seguintes hipóteses da indução: $a_k < (\frac{7}{4})^k$, $\quad$ para $n > 1$ e $2 \leq k \leq n$.
Pela definição dos números de Fibonacci, 3.4, temos que $a_{n+1} = a_{n-1} + a_n$. Então, observe que pela definição e pelas hipóteses da indução temos que

$$a_{n+1} = a_{n-1} + a_n < (\tfrac{7}{4})^{n-1} + (\tfrac{7}{4})^n = (\tfrac{7}{4})^{n-1}(1 + \tfrac{7}{4}) < (\tfrac{7}{4})^{n-1} \cdot (\tfrac{7}{4})^2 = (\tfrac{7}{4})^{n+1},$$

o que era para mostrar. ∎

(c) Queremos demonstrar que $\forall n \geq 4, \quad n! > 2^n \quad (***)$.
Observe que esta demonstração também pode ser elaborada por indução, o início da indução é para $n = 4$, e o passo segue em formato usual. Observe que a afirmação $(*)$ é equivalente com a seguinte

$$\forall n \in \mathbb{N}, \quad (n+4)! > 2^{n+4}.$$

Vamos mostrar $(***)$.
Início da indução $n = 4$: Observe que obtemos no lado esquerdo para $n = 4$, $4! = 24$ e para o lado direoto, $2^4 = 16$. Como $24 > 16$, demonstramos o início da indução.
Passo da indução $n \mapsto n+1$:
Pela hipótese da indução temos que vale $(***)$ para n, onde $n > 4$. Queremos mostrar que $(n+1)! > 2^{n+1}$.

Para isso, vamos usar a hipótese da indução. Começamos como segue, usando a definição do fatorial, a hipótese da indução e propriedades da desigualdade $>$:

$$(n+1)! = n! \cdot (n+1) > 2^n \cdot (n+1) = n2^n + 2^n > 2 \cdot 2^n = 2^{n+1}. \qquad \blacksquare$$

3.3 Recursão

Em seguida, vamos enunciar e demonstrar o *Teorema da recursão em* $\mathbb{N}$. Este teorema justifica as definições recursivas feitas anteriormente. O resultado parece que foi tal natural para o matemático Felix Haussdorff, que observou em 1914 o seguinte:

"Nos não podemos somente *deduzir* por indução, como também *definir* por indução. Significa então $f(\alpha)$ não uma afirmação sobre α, porém um objeto atribuido ao número α, uma função de $\alpha \ldots$ então podemos formular o método de definição por indução na seguinte maneira:

$f(\alpha)$ é definido para qualquer α, caso $f(0)$ é definido, e sempre se $f(\xi)$ for definido para todos os $\xi < \alpha$, então $f(\alpha)$ é definido. "

Hausdorff não deu mais explicações desta sua afirmação provavelmente achava-o tanto óbvio. Nos vamos demonstrá-lo para os números naturais. Fato é que definições por recursão são permitidos e podem ser usados na teoria da computação. Já conhecemos algumas definições recursivas. Temos então, o seguinte

Teorema 3.3.1 (Teorema da Recursão para $\mathbb{N}$)**.** *Sejam S um conjunto e $x \in S$. Seja dada a aplicação*

$$G : \mathbb{N} \times S \to S, \langle n; s \rangle \mapsto G(\langle n; s \rangle)$$

Então, existe única aplicação $H : \mathbb{N} \to S$, satisfazendo

$$\text{(i) } H(0) = x, \quad \text{e} \quad \text{(ii) } H(n+1) = G(\langle n; F(n) \rangle).$$

Demonstração: É preciso mostrar a *existência* e a *unicidade*.
(a) Existência: Consideremos o seguinte conjunto

$$F := \{X \subseteq \mathbb{N} \times S | \quad \langle 0; x \rangle \in X \,\&\, \langle n; x \rangle \in X \Rightarrow \langle n+1; G(\langle n; x \rangle) \rangle \in X\}.$$

Observe que $F \neq \emptyset$, pois $\mathbb{N} \times S \in F$. Tomemos então $M := \bigcap F = \bigcap_{X \in F} X$. Vamos mostrar que $M \in F$, i.e., $\bigcap F \subset \mathbb{N} \times S$ satisafzendo a condição seguinte

$$\langle 0; x \rangle \in \bigcap F \,\&\, \langle n; x \rangle \in \bigcap F \;\Rightarrow\; \langle n+1; G(\langle n; x \rangle) \rangle \in \bigcap F. \qquad (*)$$

Como cada $X \in F$ satisafaz $(*)$ é claro que $\bigcap F$ satisfaz $(*)$ e portanto $M \in F$. Consideremos agora o conjunto

$$P := \{n \in \mathbb{N} | \quad \text{existe único } x_n \in S \text{ tal que } \langle n; x \rangle \in M\}.$$

Temos o seguinte
Fato: $\quad P = \mathbb{N}$.
Prova do fato: Vamos fazer indução em n. Começamos pelo início da indução: É preciso mostrar que $0 \in P$. Suponha por absurdo que $0 \notin P$. Como $\langle 0; x \rangle \in M$ é preciso que existe $y \in X$ tal que $x \neq y$ e $\langle 0; y \rangle \in M$. Assim, sabemos que $M \setminus \{\langle 0; y \rangle\}$ tem a condição $(*)$, e aí, $M \setminus \{\langle 0; y \rangle\} \in F$. Logo, $M \subseteq M \setminus \{\langle 0; y \rangle\}$, o que é um absurdo. Portanto temos que $0 \in P$.
Passo da indução: Vamos mostrar que $n \in P$ implica $(n+1) \in P$. Suponha novamente que $(n+1) \notin P$. Como pela hipótese da indução $n \in P$, existe único $x_n \in S$ tal que $\langle n; x_n \rangle \in X$, para todo $X \in F$. Como $M = \bigcap F$, temos que $\langle (n+1); G(\langle n; x \rangle) \rangle \in X$, para todo $X \in F$, ou seja, $\langle (n+1); G(\langle n; x \rangle) \rangle \in \bigcap F = M$. Por hipótese, $n+1 \notin P$, e portanto existe $z \in S$ tal que $z \neq G(\langle n; x \rangle)$ e $\langle n+1; z \rangle \in M$. Logo, $M \setminus \{\langle n+1; z \rangle\} \in F$, e aí, $M = \bigcap F \subseteq M \setminus \{\langle n+1; z \rangle\}$, o que é um absurdo, mostrando que $n+1 \in P$.
Consequentemente, $P = \mathbb{N}$ e temos que $\forall n \in \mathbb{N}, \exists!\; x_n \in S, \quad \langle n; x_n \rangle \in M$.
Como $\langle n; x_n \rangle \in M$ implica que $\langle n+1; G(\langle n; x_n \rangle) \rangle \in M$, é preciso que $x_{n+1} = G(\langle n; x_n \rangle)$, pela unicidade de x_{n+1}.

Portanto, $H : N \to S, n \mapsto H(n) := x_n$ satisfaz (i) e (ii), e acabamos de demonstrar a existência da aplicação H.

(b) Unicidade da aplicação: Sejam H_1, H_2 duas aplicações satisfazendo (i) e (ii). Assim, temos por (i) que $H_1(0) = x = H_2(0)$. Além disso, para quaisquer $n \in \mathbb{N}$, se $H_1(n) = H_2(n)$, então $H_1(n+1) = H_2(n+1)$, isto por (ii). Logo, as duas aplicações H_1 e H_2 coincidem. ∎

Vejamos mais alguns exemplos de definições recursivas.

Exemplo 3.3.2. *(a) Podemos definir fatorial por recursão:*

$$\begin{cases} 0! := 1, \\ (n+1)! := (n+1) \cdot n!, \quad \forall n \geq 0 \end{cases} \tag{3.5}$$

Pelo Teorema 3.3.1, temos para $S := \mathbb{N}$, $x = 1 \in \mathbb{N}$ e $G : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \langle n; m \rangle \mapsto (n+1) \cdot m$ que existe única aplicação $H : \mathbb{N} \to \mathbb{N}$ tal que $H(0) = 1$ e $H(n+1) = (n+1) \cdot H(n)$. Assim, justificamos a definição recursiva 3.5. Observe que $H(n) = n!$.

(b) Retornamos a definição da adição dos naturais. Sabemos pela definição 3.1.6 e 3.1 como definimos a adição entre os números naturais. Esta definição se justifica pelo teorema da recursão 3.3.1.

Em detalhe, observemos que para $S := \mathbb{N}$, $x = m \in \mathbb{N}$ fixo e $G : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \langle k; n \rangle \mapsto n+1$, temos por 3.3.1 a existência de única aplicação $H_m : \mathbb{N} \to \mathbb{N}$, satisfazendo

$$H_m(0) = m, \quad e \quad H_m(n+1) = G(\langle n; H_m(n) \rangle) = H_m(n) + 1.$$

Observe que $H_m(n) = m + n$. ∎

Capítulo 4

Relações específicas, relações de equivalência, partição e fechos de relação

Neste capítulo, vamos retornar a discussão de relações. Introduzimos relações com certas propriedades, e abordamos o conceito muito importante de relação de equivalência, e a sua conexão com partições de um conjunto dado. Finalmente, vejamos como construir fechos reflexivo e transitivo de relações, conceitos importantes para matemática e a teoria da computação.

Para acompanhar os assuntos desta seção o leitor pode consultar [4, 8, 11, 15].

4.1 Relações, relação inversa e composição de relações

Relembremos que uma relação binária é simplesmente um conjunto de pares ordenados.

Definição 4.1.1. *Seja r uma relação em a.*
(a) Dizemos que r é uma relação **simétrica** *sse $\forall x, y \in a \quad \langle x; y\rangle \in r \quad \rightarrow \quad \langle y; x\rangle \in r$.*
(b) Dizemos que r é uma relação **reflexiva** *sse $\forall x \in a \quad \langle x; x\rangle \in r$.*
(c) Dizemos que r é uma relação **anti-simétrica** *sse $\forall x, y \in a \quad \langle x; y\rangle \in r \;\&\; \langle y; x\rangle \in r \quad \rightarrow \quad x = y$.*
(d) Dizemos que r é uma relação **irreflexiva** *sse $\forall x \in a \quad \langle x; x\rangle \notin r$.*
(e) Dizemos que r é uma relação **transitiva** *sse $\forall x, y, z \in a \quad \langle x; y\rangle \in r \;\&\; \langle y; z\rangle \in r \quad \rightarrow \quad \langle x; z\rangle \in r$.*
(f) Dizemos que r é uma relação **conectada, linear, total** *sse $\forall x, y \in a \quad \langle x; y\rangle \in r$ ou $\langle y; x\rangle \in r$.*

Notação 4.1.2. *Observe que às vezes, usamos a notação xry para indicar $\langle x; y\rangle \in r$, caso r seja uma relação. Pensando na relação $\leq$, sempre escrevemos $x \leq y$ em vez de $\langle x; y\rangle \in \leq$.*

Exemplo 4.1.3. *(a) Consideremos a relação vazia, $r := \emptyset$, no conjunto $a \neq \emptyset$. r é simétrica, anti-simétrica e transitiva - por vacuidade. Mas r não é reflexiva nem conectada, porém é irreflexiva.*
(b) Consideremos a relação diagonal Δ_a em a, qual vem da igualdade $=$. Quais propriedades Δ_a satisfaz? Tente descobri-las!
(c) Consideremos a relação universal em a, $\nabla_a := a \times a$. É fácil ver que ∇_a é simétrica, reflexiva, transitiva e conectada. Obviamente, ∇_a não é irreflexiva, caso a tiver mais do que um elemento. ∇_a é anti-simétrica?
(d) Consideremos em $\mathbb{N}$ a relação de menor ou igual $\leq_{\mathbb{N}}$, definido de maneira usual seguinte,
$\leq_{\mathbb{N}} := \{\langle n; m\rangle | \quad \exists k \in \mathbb{N}, n + k = m\}$. Esta relação é reflexiva, anti-simétrica, transitiva e conectada.
(e) Em $\mathbb{Q}$ consideremos a relação, definido de seguinte maneira $q := \{\langle x; x^2\rangle | \quad x \in \mathbb{Q}\}$. Assim, q não satisfaz nenhuma propriedade da definição 4.1.1.

Definição 4.1.4. *Seja r uma relação no conjunto a.*
Dizemos que $\tilde{r}$, ou às vezes, r^{-1}, é a relação **inversa** *de r sse para todo $x, y \in a$*

$$\langle x; y\rangle \in r \quad sse \quad \langle y; x\rangle \in \tilde{r}$$

O seguinte lema é simples de demonstrar.

Lema 4.1.5. *Sejam r e s relações em a. Então,*
(a) $\tilde{\tilde{r}} = r$.
(b) $\widetilde{r \cup s} = \tilde{r} \cup \tilde{s}$. ∎

Demonstração: Para verificar o ítem (a) observe o seguinte

$$\langle x; y\rangle \in r \quad \text{sse} \quad \langle y; x\rangle \in \tilde{r} \quad \text{sse} \quad \langle x; y\rangle \in \tilde{\tilde{r}}.$$

O ítem (b), mostra-se verificando as duas inclusões, $\subseteq$ e $\supseteq$. ∎

Definição 4.1.6. *Sejam r e s relações em a.*
Dizemos que $(s \circ r) := \{\langle x; z\rangle | \quad x, z \in a \ \& \ \exists y \in a \ (\langle x; y\rangle \in r \ \& \ \langle y; z\rangle \in s\}$ é a **composição** *de r e s.*

Exemplo 4.1.7. *Sejam dadas as relações $r := \{\langle 1; 2\rangle, \langle 3; 4\rangle, \langle 2; 2\rangle\}$ e $s := \{\langle 4; 2\rangle, \langle 2; 5\rangle, \langle 3; 1\rangle, \langle 1; 3\rangle\}$. Então calculamos as relações compostas seguintes.*
$s \circ r = \{\langle 1; 5\rangle, \langle 3; 2\rangle, \langle 2; 5\rangle\}$.
$r \circ s = \{\langle 4; 2\rangle, \langle 3; 2\rangle, \langle 1; 4\rangle\}$.
$r \circ r = \{\langle 1; 2\rangle\}$.
$r \circ (r \circ r) = \{\langle 1; 2\rangle\}$.

4.2 Relação de equivalência e partição

Nesta seção introduzimos relações de equivalências, e estabelecemos a conexão com partições de um conjunto. Vejamos que relações de equivalência e partições num conjunto a são em correspondência bijetiva, i.e., existe uma função bijetiva entre o conjunto das relações de equivalência num conjunto a, e o conjunto das partições deste conjunto a. Uma relação de equivalência é a generalização da igualdade. Em relações de equivalências identificamos objetos equivalentes, porém não necessariamente *iguais.* Pensando em lógica matemática, cf. 1, e na equivalência lógica definida em 1.3.10, temos já um primeiro exemplo de uma relação de equivalência definida no conjunto $Form(L)$.

Começamos com a definição.

Definição 4.2.1. *Seja r uma relação no conjunto a. Dizemos que r é uma* **relação de equivalência** *em a sse r é reflexiva, simétrica e transitiva. (cf. 4.1.1)*

Exemplo 4.2.2. *(a) O primeiro exemplo trata da relação da igualdade, $=$. Pelas propriedades acerca da igualdade listadas em 1.2.2, temos de imediato que $=$ é uma relação de equivalência.*
(b) Consideremos a equivalência lógica $\Leftrightarrow$ em $Form(L)$, já citado acima, e definida em 1.3.10, temos outro exemplo de uma relação de equivalência. Os detalhes da demonstração deste fato, devem ser feitas nos exercícios.
(c) Introduzimos em $\mathbb{Z}$ a seguinte relação $\equiv_3$, definida no seguinte modo: Para $a, b \in \mathbb{Z}$, temos que

$$a \equiv_3 b \quad sse \quad \exists k \in \mathbb{Z}, \ a - b = 3k.$$

Assim, $\equiv_3$ é uma relação de equivalência. Dizemos que a relação $\equiv_3$ é a **congruência módulo** *3. Primeiramente, observemos que $\equiv_3 \subseteq \mathbb{Z} \times \mathbb{Z}$, e assim, é de fato uma relação em $\mathbb{Z}$. Falta agora ver as propriedades exigidas pela definição 4.2.1.*
Observe que $a - a = 0 = 0k$, e assim $a \equiv_3 a$. Agora, para $a, b \in \mathbb{Z}$ tais que $a \equiv_3 b$, temos que existe $k \in \mathbb{Z}$ tal que $a - b = 3k$. Logo, observe que $b - a = 3(-k)$, e assim, temos que $b \equiv_3 a$, mostrando que a relação

é simétrica. Para demonstrar a transitividade, sejam $a, b, c \in \mathbb{Z}$ tais que $a \equiv_3 b$ e $b \equiv_3 c$. Logo, existem $k, l \in \mathbb{Z}$, tais que $a - b = 3k$ e $b - c = 3l$. Portanto, $a - b + (b - c) = a - c = 3k + 3l = 3(k + l)$. Como $k + l \in \mathbb{Z}$, temos que $a \equiv_3 c$, e terminamos a prova. ∎

Introduzimos agora alguns conceitos para relações de equivalências.

Definição 4.2.3. *Seja r uma relação de equivalência em a.*
(a) Seja $x \in a$. Dizemos que o conjunto $[x]_r := \{y \in a| \quad xry\}$ é a **classe de equivalência** *de x em r.*
(b) Dizemos que o conjunto $[a]_r := \{[x]_r| \quad x \in a\}$ é o **conjunto quociente** *de a por r.*
Observe que existem várias notações como $\overline{x}$ ou x/r, para a classe de x. Também, $\overline{a}$ ou a/r, denotam o conjunto quociente de a por r.

Exemplo 4.2.4. *Reconsideremos o exemplo 4.2.2 e classes de equivalências e conjunto quociente.*
(a) Para a relação da igualdade $=$, temos que para $n \in \mathbb{N}$, a classe $[x]_= := \{n\}$. o conjunto quociente é o seguinte, $[\mathbb{N}]_= = \{k \in \mathbb{N}| \quad n = k\} = \{\{n\}| \quad n \in \mathbb{N}\}$.
(b) As classes e o conjunto quociente para a equivalência lógica estão sendo discutidos em exercício.
(c) Para a relação da congruência módulo 3, temos que $[0]_{\equiv_3} = \{\ldots, -6, -3, 0, +3, +6, \ldots\}$, $[1]_{\equiv_3} = \{\ldots, -4, -1, +2, +5, \ldots\}$ e $[2]_{\equiv_3} = \{\ldots, -5, -2, +1, +4, \ldots\}$. O conjunto quociente somente contém três elementos, a saber $[\mathbb{Z}]_{\equiv_3} = \{[0]_{\equiv_3}, [1]_{\equiv_3}, [2]_{\equiv_3}\}$. Denotamos $[\mathbb{Z}]_{\equiv_3}$ por $\mathbb{Z}/\mathbb{Z}_3$, ou simplesmente por $\mathbb{Z}_3$. Em matemática discreta II, vejamos que o conjunto $\mathbb{Z}_3$ ainda tem uma boa estrutura, ou seja, $\mathbb{Z}_3$ tem estrutura de anel comutativo com unidade.

O próximo resultado é fundamental para o entendimento de relação de equivalência.

Lema 4.2.5. *Seja r uma relação de equivalência em a. Então,*
(a) Para todo $x \in a$, $x \in [x]_r$. Assim, $[x]_r \neq \emptyset$.
(b) Para todo $x, y \in a$, se xry, então, $[x]_r = [y]_r$.
(c) Para todo $x, y \in a$, se $\neg(xry)$, então, $[x]_r \cap [y]_r = \emptyset$.

Demonstração: Seja r uma relação de equivalência em a. Vejamos (a). Como r é reflexiva, temos que xrx e assim, $x \in [x]_r$. Para ver (b), sejam $x, y \in a$ tais que xry. Vejamos que $[x]_r = [y]_r$, verificando $\subseteq$ e $\supseteq$.
$\subseteq$: Seja $z \in [x]_r$, i.e., xrz. Precisamos mostrar yrz. Por hipótese temos que xry. Como r é simétrica, temos que zrx, e pela transitividade de r, temos que zry. Aplicando, a simetria, obtemos o desejado, i.e., yrz.
$\supseteq$: Para mostrar a inclusão recíproca, temos $z \in [y]_r$, i.e., yrz. Usando a hipótese, xry e a transitividade de r, obtemos que xrz, ou seja, $z \in [x]_r$.
Consequentemente, $[x]_r = [y]_r$.
Falta mostrar (c). Sejam $x, y \in a$ tais que $\neg(xry)$. Suponha que $[x]_r \cap [y]_r \neq \emptyset$. Assim, existe $z \in [x]_r \cap [y]_r$. Logo, temos que xrz e yrz. Pela simetria, zry. Usando a transitividade, temos que xry, contradizendo a hipótese $\neg(xry)$. Logo (usando o princípio da prova por absurdo), $[x]_r \cap [y]_r = \emptyset$. ∎

Introduzimos agora o conceito de partição.

Definição 4.2.6. *Sejam a um conjunto e $\{a_i\}_{i \in I}$ uma família de subconjuntos não vazios de a.*
(a) Dizemos que $\{a_i\}_{i \in I}$ é uma **cobertura** *de a sse $\bigcup_{i \in I} a_i = a$.*
(b) Dizemos que $\{a_i\}_{i \in I}$ é uma **partição** *de a sse $\{a_i\}_{i \in I}$ é uma cobertura de a e os elementos da família são 2 a 2 disjuntos, i.e., para quaisquer $i, j \in I$, $i \neq j$, temos que $a_i \cap a_j = \emptyset$.*

Observação 4.2.7. *Visualize os conceitos de cobertura e partição de um conjunto a através de um diagrama de Venn!* ∎

Exemplo 4.2.8. *(a) Tomemos de 4.2.4, $[\mathbb{N}]_= := \{\{n\}| \quad n \in \mathbb{N}\}$ é uma partição de $\mathbb{N}$, pois, temos que $\bigcup_{n \in \mathbb{N}} \{n\} = \mathbb{N}$ e para $n \neq m$, $\{n\} \cap \{m\} = \emptyset$.*
(b) Tomemos agora o conjunto quociente do exemplo 4.2.4, $[\mathbb{Z}]_{\equiv_3} = \{[0]_{\equiv_3}, [1]_{\equiv_3}, [2]_{\equiv_3}\}$. Assim, é fácil para verificar (cf. exercício) que isto é uma partição para o conjunto dos inteiros $\mathbb{Z}$.

Observação 4.2.9. *O último exemplo mostrou que o conjunto quociente de algumas relações de equivalência gera uma partição. Assim, podemos perguntar se isso sempre acontece. A próxima proposição estabelece a conexão entre relação de equivalência e partição. A demonstração também é construtiva no sentido que dá uma* receita *como obter a partição a partir da relação de equivalência, como também uma relação de equivalência a partir de uma partição.*

Proposição 4.2.10. *Seja a um conjunto. Toda relação de equivalência determina uma partição e vice versa, toda partição determina uma relação de equivalência.*
Podemos dizer que relação de equivalência e partição são a mesma coisa*.*

Demonstração: Seja a um conjunto.
Primeira parte: Seja r uma relação de equivalência em a. Vamos mostrar que $[a]_r := \{[x]_r| \quad x \in a\}$ é uma partição para a. Vejamos então que $\bigcup_{x\in a}[x]_r = a$. Novamente, é preciso verificar as inclusões $\subseteq$ e $\supseteq$. Seja $y \in \bigcup_{x\in a}[x]_r$. Assim, $y \in a$. Reciprocamente, para $y \in a$, temos que $y \in [y]_r$, e portanto, $y \in \bigcup_{x\in a}[x]_r$. Pelo lema 4.2.5, temos que para qualquer $x, y \in a$, ou $[x]_r = [y]_r$ ou $[x]_r \cap [y]_r = \emptyset$. Logo, $[a]_r := \{[x]_r| \quad x \in a\}$ é de fato uma partição para a.

Segunda parte: Seja $\{a_i\}_{i\in I}$ uma partição para a. É preciso definir uma relação de equivalência r em a, a partir desta partição. Definamos então r em a como segue:

$$\langle x; y\rangle \in r \quad \text{sse} \quad \exists i \in I,\ x, y \in a_i \tag{$*$}$$

Observe que r é de fato uma relação de equivalência em a. Primeiramente, é imediato que $\langle x; x\rangle \in r$, pois $x \in a_i$, para algum $i \in I$. Assim, r é reflexiva. A simetria também é imediato, pois $\langle x; y\rangle \in r$ significa que existe $i \in I$ tal que $x, y \in a_i$. Logo, $\langle y; x\rangle \in r$. Vejamos agora que r é transitiva. Para isso, sejam $x, y, z \in a$ tais que $\langle x; y\rangle \in r$ e $\langle y; z\rangle \in r$. Assim, existem $i, j \in I$ tais que $x, y \in a_i$ e $y, z \in a_j$. Como $\{a_i\}_{i\in I}$ é uma partição para a, é preciso ter por 4.2.5, $i = j$, pois $y \in a_i \cap a_j$ e assim $x, y, z \in a_i$, mostrando que $\langle x; z\rangle \in r$. Consequentemente, a definição $(*)$ determina uma relação de equivalência em a. ■

Observação 4.2.11. *A proposição 4.2.10 estabelece uma correspondência 1 a 1 e sobre, entre relações de equivalência e partições num conjunto a. Faça os detalhes.* ■

Exemplo 4.2.12. *Seja dada a seguinte partição do conjunto $a := \{1, 2, 3, 4, 5\}$, $\{\{1, 2\}; \{3\}; \{4, 5\}\}$. Observe que isto é de fato uma partição de a. A última proposição, determina uma relação de equivalência r em a. Enuncie esta relação de equivalência induzida desta partição.* ■

4.3 Fechos reflexivo e transitivo

Nesta seção falamos de fechos reflexivo e transitivo para relações. Estes fechos são usados na teoria da computação e determinam as menores relações estendendo a relação inicial qual é reflexivo e transitivo, respectivamente. Antes de entrar nas definições e construções definimos por recursão, as m-ésimas potências r^m de uma relação r.

Definição 4.3.1. *Seja r uma relação no conjunto a. Definimos por recursão*

$$\begin{cases} r^1 := r \\ r^m := r \circ (r^{m-1}), \quad \forall m > 1 \end{cases} \tag{4.1}$$

Exemplo 4.3.2. *(a) Seja $r := \{\langle x; y\rangle, \langle x; z\rangle, \langle z; y\rangle\}$ uma relação no conjunto $a := \{x, y, z\}$. Assim, temos que*
$r^2 = r \circ r = \{\langle x; y\rangle\}$. $r^3 = \emptyset$. Logo, $\forall n > 3$, $r^n = \emptyset$.
(b) Seja $s := \{\langle x; y\rangle, \langle y; z\rangle, \langle z; x\rangle\}$ uma relação no conjunto $a := \{x, y, z\}$. Assim, temos que
$s^2 = s \circ s = \{\langle x; z\rangle, \langle y; x\rangle, \langle z; y\rangle\} = \tilde{s}$.

$s^3 = s \circ (s^2) = \{\langle x; x\rangle, \langle y; y\rangle, \langle z; z\rangle\} = \Delta_a$.
$s^4 = s \circ (s^3) = \{\langle x; y\rangle, \langle y; z\rangle, \langle z; x\rangle\} = s$.
$s^5 = s \circ (s^4) = s \circ s = s^2$.
$s^6 = s \circ (s^5) = s \circ s^2 = s^3$.
$s^7 = s \circ (s^6) = s \circ s^3 = s$.

Definição 4.3.3. *Seja r uma relação no conjunto a. Dizemos que $ref(r) := r \cup \Delta_a$[1], onde Δ_a define a relação diagonal em a, é o* **fecho reflexivo** *de r.*

Observação 4.3.4. *Observe que $ref(r)$ é a menor (em sentido da inclusão) relação reflexiva contendo a relação r, i.e., $ref(r)$ é reflexiva e qualquer outra relação reflexiva contendo r contém $ref(r)$.* ■

Definição 4.3.5. *Seja r uma relação no conjunto a. Dizemos que $tra(r) := \bigcup_{k \in \mathbb{N}^*} r^k$ é o* **fecho transitivo** *de r em a.*

Exemplo 4.3.6. *Reconsiderando o exemplo 4.3.2, temos que*
(a) Para $r := \{\langle x; y\rangle, \langle x; z\rangle, \langle z; y\rangle\}$ uma relação no conjunto $\{x, y, z\}$, temos que $tra(r) = r$. Observe que r já era relação transitiva. Assim, o fecho transitivo não trouxe nada de novo.
(b) Para $s := \{\langle x; y\rangle, \langle y; z\rangle, \langle z; x\rangle\}$ uma relação no conjunto $\{x, y, z\}$, temos que
$tra(s) = \bigcup_{k \in \mathbb{N}^*} s^k = s \cup s^2 \cup s^3 \cup s^4 \cup \ldots = s \cup s^2 \cup s^3 = s \cup \tilde{s} \cup \Delta = \nabla$. ■

Vejamos na próxima proposição que o fecho transitivo de uma relação é de fato a menor (em sentido da inclusão) relação transitiva contendo r.

Proposição 4.3.7. *Seja r uma relação em a. Então, $tra(r)$ é a menor (em sentido da inclusão) relação transitiva contendo r, isto é:*

$$\begin{cases} tra(r) \text{ é transitiva} \\ r \subseteq tra(r) \\ \forall s,\ s \text{ é relação } \& \ r \subseteq s \ \& \ s \text{ é transitiva} \quad \Rightarrow \quad tra(r) \subseteq s \end{cases} \tag{4.2}$$

Demonstração: A demonstração se divide em duas partes. Na primeira parte, vamos mostrar que $tra(r)$ é transitiva. Para isso, sejam $x, y, z \in a$ tais que $\langle x; y\rangle \in tra(r)$ e $\langle y; z\rangle \in tra(r)$. Precisamos mostrar que $\langle x; z\rangle \in tra(r)$.
Como $\langle x; y\rangle \in tra(r)$, existe $k \in \mathbb{N}^*$, pela definição de $tra(r)$, tal que $\langle x; y\rangle \in r^k$.
Analogamente, como $\langle x; y\rangle \in tra(r)$, existe $l \in \mathbb{N}^*$, tal que $\langle x; y\rangle \in r^l$.
Logo, existem os seguintes *caminhos*, $x = w_1, w_2, \ldots, w_k = y$ e $y = u_1, u_2, \ldots, u_l = z$ tais que

$$xrw_2r \ldots rw_{k-1}ry \quad \text{e} \quad yru_2r \ldots ru_{l-1}rz$$

Assim, conectando estes "caminhos", obtemos que $\langle x; z\rangle \in r^{k+l}$, e como $r^{k+l} \subseteq tra(r)$ temos que $\langle x; z\rangle \in tra(r)$.

Na segunda parte, mostramos que $tra(r)$ é a menor relação transitiva contendo r. Observe que obviamente, $r \subseteq tra(r)$. Seja s uma relação transitiva contendo r, i.e., $r \subseteq s$. Vejamos que $tra(r) \subseteq s$. Para isso, sejam $x, y \in a$ tais que $\langle x; y\rangle \in tra(r)$. Logo, existe $k \in \mathbb{N}^*$, tal que $\langle x; y\rangle \in r^k$ e assim, como acima, existem $x = w_1, w_2, \ldots, w_k = y$ tais que $xrw_2r \ldots rw_{k-1}ry$. Como $r \subseteq s$, temos que $\langle x; w_2\rangle, \langle w_2; w_3\rangle, \ldots, \langle w_{k-1}; y\rangle \in s$. Usando agora o fato de que s é uma relação transitiva, temos que $\langle x; y\rangle \in s$, terminando a prova. ■

[1] veja o exemplo 2.4.2

Capítulo 5

Introdução à análise combinatória

Neste capítulo explicamos alguns conceitos básicos da análise combinatória. Boa parte deste capítulo constá em [13], mas todos estes assuntos também podem ser consultados em [4, 8, 11, 15].

5.1 Princípios básicos de contagem

Começamos pelos princípios fundamentais e básicos para poder estabelecer análises combinatórias. O próximo princípio é simples, porém importante.

Observação 5.1.1. *(Princípio da adição) Sejam dados $n \in \mathbb{N}$ e $a_1, \ldots, a_n$ conjuntos 2 a 2 disjuntos, cada conjunto com $p_1, \ldots, p_n$ elementos, respectivamente. Então, o conjunto $\bigcup_{i=1}^{n} a_i$ tem $\sum_{i=1}^{n} p_i$ elementos.*

Exemplo 5.1.2. *Queremos resolver o seguinte problema: Numa sala há cinco homens e seis mulheres e queremos formar casais homen-mulher. De quantos modos podemos fazer isso? Denotamos por $H := \{h_1, \ldots, h_5\}$ o conjunto de homens e por $M := \{m_1, \ldots, m_6\}$ o conjunto das mulheres. Agora, temos seis casais formados pelo homen h_1, seis casais formados pelo homen h_2, ..., seis casais formados pelo homen h_5. Pelo princípio da adição temos então $6 + 6 + 6 + 6 + 6 = 30$ possabilidades de formar casais homen-mulher.*

Observação 5.1.3. *(Princípio da multiplicação) Sejam dados $n \in \mathbb{N}$ e $a_1, \ldots, a_n$ conjuntos, cada conjunto com $p_1, \ldots, p_n$ elementos, respectivamente. Então, o conjunto $\prod_{i=1}^{n} a_i$ tem $\times_{i=1}^{n} p_i = p_1 \cdot \ldots \cdot p_n$ elementos.*

Podemos reformular este princípio de seguinte maneira combinatória:
Se uma decisão d_1 pode ser tomada de p_1 maneiras, uma vez tomada esta decisão, a decisão d_2 pode ser tomada de p_2 maneiras, uma vez tomadas estas decisões, a decisão d_3 pode ser tomada de p_3 maneiras, ... e uma vez tomadas as decisões, a decisão d_n pode ser tomada de p_n maneiras, então o número de maneiras de se tomarem as decisões $d_1, \ldots, d_n$ é $p_1 \cdot \ldots \cdot p_n$.

Exemplo 5.1.4. *(a) Reconsiderando o exemplo 5.1.2, podemos resolver o problema fazendo uso da observação 5.1.3, e obtemos para $n = 2$, d_1 a decisão de escolhermos um dos homens, é de cinco maneiras, e d_2 a decisão de escolhermos uma mulher é de seis maneiras. Obtemos então que podemos formar de 30 maneiras um casal. Observe que com a notação de 5.1.2, o conjunto dos possíveis casais é o seguinte $\{\langle h_1; m_1\rangle, \ldots, \langle h_1; m_6\rangle, \ldots, \langle h_5; m_6\rangle\}$.*

(b) Temos agora uma bandeira formada de quatro listras, quais devem ser coloridas usando-se apenas as cores vermelho, azul e branco, com a exigência de que listras adjacentes devem ter cores diferentes. De quantos modos podemos colorir esta bandeira?
Usando o princípio da multiplicação obtemos que a primeira listra pode ser escolhida de três modos, a

segunda listra pode ser escolhida de dois modos, a terceira listra pode ser escolhida de dois modos e a quarta e última listra podemos escolher também de dois modos.
Pelo princípio 5.1.3, temos então, $3 \cdot 2^3 = 24$ *modos de colorir a bandeira.*

(c) Vamos resolver o seguinte problema: Quantos números naturais de três algarismos distintos *na base* 10 *existem? Elaboramos o seguinte esquema:*
para o primeiro algarismo temos 9 *números à disposição (excluimos o dígito* 0*, por ser o primeiro algarismo), para o segundo algarismo também temos* 9 *números à disposição (excluimos o algarismo escolhido da primeira posição e adicionamos o número* 0*) e para o último algarismo temos agora* 8 *números à disposição (excluindo os primeiros dois dígitos). Com o princípio da multiplicação, temos então* $9 \cdot 9 \cdot 8 = 648$ *modos possíveis de formar este número.*

(d) Agora queremos saber quantos números naturais de quatro algarismos (na base 10*) menores do que* 5.000 *e divisíveis por* 5 *podem ser formados usando apenas os algarismos* $2, 3, 4, 5$ *e* 7*. Elaboramos o seguinte esquema:*
O último algarismo somente pode ser 5*, pois o número tem que ser divisível por* 5 *e o dígito* 0 *não deve ser usado, temos então uma só possibilidade. Para o penúltimo dígito, podemos usar todos os números, e temos* 5 *possibilidades, igualmente para o segundo dígito, temos* 5 *possibilidades, enquanto para o primeiro dígito, somente podemos usar* $2, 3$ *ou* 4*, pois o número deve ser menor do que* 5.000*. Pelo princípio da multiplicação, temos* $1 \cdot 5^2 \cdot 3 = 75$ *possibilidades de formar o número procurado.*

(e) O que muda se o número procurado somente deve ser divisível por 5*? Pensando bem, o que muda são somente as possibiliades do primeiro dígito, em qual agora podemos usar todos os dígitos em jogo, ou seja, todos os cinco. Temos então* $1 \cdot 5^3 = 125$ *modos de formar este número. E se quisermos formar qualquer número com estes cinco dígitos, temos* $5^5 = 3.125$ *modos.*

Vimos nesta seção que o princípio da multiplicação resolve bastante problemas combinatórias.

5.2 Permutações simples e circulares

Começamos com o seguinte resultado

Proposição 5.2.1. *Sejam dados* n *objetos. Então podemos ordena-los em* $n!$ *modos numa linha.*

Demonstração: A afirmação da proposição segue do princípio da multiplicação, cf. 5.1.3. Denotamos os n objetos de $a_1, \dots, a_n$. Assim, para ordena-los em linha, temos na primeira posição n possibilidades, pois temos todos os objetos para escolher. Na segunda posição somente restam $n - 1$ objetos, e assim adiante, cada posição seguinte, as possibilidades devem diminuir por 1, pois já usamos objetos nas primeiras posições. Chegando para a última posição resta somente uma possibilidade. Pelo princípio 5.1.3, temos $n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$ modos de ordenar os objetos numa linha. ■.

Exemplo 5.2.2. *(a) Queremos saber quantos anagramas podemos formar da palavra* $PRATICO$*. Podemos resolver esta questão na seguinte maneira:*
Cada anagrama da palavra é uma ordenação das suas letras. Neste caso, temos sete letras diferentes, e pela proposição 5.2.1, temos então $7! = 5040$ *anagramas.*

(b) Queremos agora saber quantos são os algarismos da palavra $PRATICO$*, quais começam e terminam com um consoante? Sabemos que a palavra tem quatro consoantes, a saber* P, R, T *e* C*, e três vogais* A, O *e* I*. Assim, temos para o consoante inicial* 4 *possabilidades e para o último,* 3*. As letras restantes,* 5 *podemos ordenar em linha. Pelo princípio 5.1.3, temos* $4 \cdot 3 \cdot 5! = 1440$ *modos de formar os anagramas com as exigências postas.*

(c) Queremos saber de quantos modos podemos dividir oito pessoas em duas mesas de quatro lugares cada. Uma possível solução é a seguinte:
Denotamos estas pessoas por a, b, c, d, e, f, g, h. Num primeiro passo, colocamos as oito pessoas numa fila, podemos fazer isto de $8!$ modos. Agora temos que pensar que temos duas mesas, e assim, contamos todas as permutações nas duas mesas. Por exemplo, as escolhas $abcd/efgh$ e $dcba/hgfe$ são contadas. Ou seja, contamos as permutações em cada mesa como uma possibilidade, mas na verdade corresponde a uma só possibilidade. Logo, contamos $4! \cdot 4!$ possibiliadades a mais, ou seja, precisamos dividir o resultado por $4! \cdot 4!$. Além disso, contamos também primeira mesa e segunda mesa, ou seja, $abcd/efgh$ e $efgh/abcd$, embora é a mesma escolha, portanto é preciso dividir o resultado por 2.
Resumindo, temos então $\frac{8!}{2 \cdot 4! \cdot 4!} = \frac{5 \cdot 6 \cdot 7}{1 \cdot 2 \cdot 3} = 35$ possibilidades de distribuir estas oito pessoas em duas mesas. Pense como poderia ter chegado a esta solução escolhendo outra estratégia! Em exemplo 5.2.5, apresentamos outra solução, usando resultado estabelecido em 5.2.4.

Definição 5.2.3. *Sejam a um conjunto de n elementos e $k \leq n$ um natural.*
(a) Dizemos que um subconjunto de a com k elementos é uma **combinação simples de classe k**.
(b) Definimos por $\binom{n}{k} := \frac{n!}{k! \cdot (n-k)!}$ e dizemos que $\binom{n}{k}$ é o **coeficiente binomial**. *Às vezes, usa-se também a notação C_n^k para o coeficiente binomial.*

Proposição 5.2.4. *O número das combinções simples de classe k de um conjunto de n elementos é $\binom{n}{k}$.*

Demonstração: Sejam $a := \{x_1, \ldots, x_n\}$ um conjunto com n elementos e seja k um natural tal que $k \leq n$. Queremos saber quantos subconjuntos de a com exatamente k elementos existem. Vamos pensar da seguinte maneira:

A escolha do primeiro elemento deste subconjunto podemos fazer de n modos, pois em a temos n elementos à disposição. Para o segundo elemento temos ainda $(n-1)$ elementos à disposição. Continuando assim, temos para a escolha do k-ésimo elemento ainda $n-k+1$ possibilidades. Pelo princípio da multiplicação temos então $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$ possibilidades para escolha. Mas, observe que estamos contando elementos demais. Por exemplo, estamos contando os subconjuntos $\{x_1, \ldots, x_k\}$ e $\{x_k, \ldots, x_1\}$, ou seja, estamos contando cada permutação dos elementos do subconjunto escolhido. Isto é, estamos contando para cada escolha feita do subconjunto b qualquer permutação entre os k elementos, embora o subconjunto b é um só. Assim, estamos contando $k!$ possibilidades a mais.

Logo, o número da escolha de um subconjunto b de a com k elementos é de $\frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!}$ maneiras possível. Agora observe que

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!},$$

terminando a demonstração da proposição. ■

Exemplo 5.2.5. *(a) Quantas saladas diferentes podemos elaborar adicionando 4 frutas, se tivermos 10 frutas à disposição? Nesta questão é preciso basicamente escolher 4 frutas em 10 e fazer a salada de frutas. Esta escolha pode ser feita, segundo proposição 5.2.4 de $\binom{10}{4}$ modos. Assim podemos fazer $\binom{10}{4} = 210$ saladas de frutas diferentes, escolhendo 4 frutas em 10.*

(b) Reconsideremos o exemplo 5.2.2 (c), e queremos saber de quantos modos podemos dividir oito pessoas em duas mesas de quatro lugares cada. Tendo a proposição 5.2.4 demonstrado, simplesmente escolhemos um subconunto de 4 elementos do conjunto de 8 pessoas, i.e., $\binom{8}{4}$, e estes 4 pessoas escolhidas sentamos na mesa, distribuindo o restante, também 4 pessoas na segunda mesa. Assim, temos então $\binom{8}{4}$ possibilidades de fazer isso. Somente é preciso ter atenção, pois estamos contando subconjuntos a mais: Usando a notação de 5.2.2 (c), estamos contando a escolha $\{a, b, c, d\}$ e $\{e, f, g, h\}$ duas vezes na escolha da combinação simples. Assim temos que dividir estes casos contandos por 2, e obtemos o resultado $\binom{8}{4} \cdot \frac{1}{2} = 35$, como já sabíamos.

(c) Agora queremos saber de quantos modos podemos escolher 5 pessoas incluindo pelo menos três

mulheres, num grupo de 8 *homens e* 5 *mulheres? Observe que esta escolha, temos pelo menos três mulheres, e pode ser feita das seguintes maneiras:*

(i) Escolhemos 3 *mulheres e assim* 2 *homens, ou*
(ii) Escolhemos 4 *mulheres e assim* 1 *homen, ou*
(iii) Escolhemos 5 *mulheres e assim nenhum homen.*

A escolha em (i) podemos fazer de $\binom{5}{3} \cdot \binom{8}{2} = 280$ *vezes. A escolha em (ii) podemos fazer de* $\binom{5}{4} \cdot \binom{8}{1} = 40$ *vezes. A escolha em (ii) podemos fazer de* $\binom{5}{5} \cdot \binom{8}{0} = 1$ *vez somente. (Por quê estamos multiplicando?) Concluindo esta questão, observe que os três casos, (i), (ii) e (iii), são* 2 *a* 2 *disjuntos e levam a uma possibilidade de escolha pedida. Assim, usando o princípio da adição temos* $280 + 40 + 1 = 321$ *modos de como pode ser feita a escolha pedida.*
Temos outras maneiras de obter esta solução: por exemplo podemos pensar em escolher 5 *pessoas em* 13*, e tirando todos os casos em que temos menos de três mulheres.*
Assim, temos que $\binom{13}{5} - \binom{8}{3}\binom{5}{2} - \binom{8}{4}\binom{5}{1} - \binom{8}{5}\binom{5}{0} = 321.$ ■

A próxima observação é simples para mostrar, e é deixado para exercício.

Observação 5.2.6. *Sejam* n *e* $0 \leq k \leq n$ *naturais. Então,* $\binom{n}{k} = \binom{n}{n-k}$. ■

Agora temos a seguinte

Questão 5.2.7. *Temos* n *objetos distintos, e queremos coloca-los em torno de um circunferência. De quantos modos isso é possível?*

Exemplo 5.2.8. *Se consideremos três objetos* $1, 2$ *e* 3*. Estes três objetos podemos colocar em linha de* $3!$ *modos, como demonstrado em 5.2.1. Para ordená-los numa circunferência, vamos primeiramente escrever todas as permutações de* $\{1, 2, 3\}$*. Obtemos* $3! = 6$ *modos, a saber:*

$$1-2-3,\ 3-1-2,\ 2-3-1 \quad e \quad 2-1-3,\ 3-2-1,\ 1-3-2$$

Porém observe que na escolha de $1-3-2$*, os seguintes casos* $2-1-3$ *e* $3-2-1$ *são equivalentes numa circunferência. Agora* $1-2-3$ *é um novo caso, mas ordenado numa cricunferência, os casos,* $3-1-2$ *e* $2-3-1$ *são equivalentes a este. Temos então somente* 2 *modos de ordenar três objetos em torno de uma circunferência. Obviamente, existem menos casos possiveis numa circunferência, do que numa linha.*

Vamos demonstrar a seguinte

Proposição 5.2.9. *Dados* n *objetos, temos* $(n-1)!$ *modos de colocá-los circularmente.*

Demonstração: Pela proposição 5.2.1, podemos colocar os objetos de $n!$ modos diferentes numa linha. Considerando agora posições equivalentes, quais podemos obter através de rotação, cada escolha tem n rotações e assim, as possibilidades são de $\frac{n!}{n} = (n-1)!$ modos. ■

Exemplo 5.2.10. *(a) Queremos saber de quantos modos podemos sentar* 7 *pessoas numa mesa redonda, tal que duas pessoas determinadas não fiquem um do lado do outro?*
Podemos pensar da seguinte maneira: tiramos estas duas pessoas, digamos a *e* b *das pessoas, e sentamos primeiramente as cinco pessoas restantes numa mesa de cinco lugares. Pelo que demonstramos em 5.2.9, isto é possível de* $4! = 24$ *modos. Agora podemos sentar a pessoa* a*, entre estas cinco pessoas já sentadas. Isto é possível de cinco maneiras. Para a pessoa* b *temos a restrição que ela não pode se sentar ao lado da pessoa* a*, qual já está sentada na mesa. A princípio, a pessoa* b *tem seis posições para sentar, mas com a restrição de que não pode sentar ao lado (nem direito, nem esquerdo) da pessoa* a*, restam apenas* 4 *posições legais. Assim, temos pelo princípio da multiplicação* $4! \cdot 5 \cdot 4 = 480$ *modos de sentarmos estas sete pessoas numa mesa redonda.*

(b) Mudando a restrição da seguinte maneira, queremos saber em quantos modos podemos sentar estas sete pessoas numa mesa redonda de modo que duas destas devem sentar junto, ou seja, um do lado do outro?
Podemos racioncinar de seguinte modo: Consideremos as pessoas a e b quais devem sentar um do lado do outro. Assim, podemos ter a possibilidade de sentar b ao lado direito de a, abreviamos então esta escolha por ab, ou b ao lado esquerdo de a, abreviado por ba. Agora podemos pensar que ab ou ba é uma só pessoa e sentar as agora seis pessoas na mesa redonda. Obtemos assim, $5! = 120$ possibilidades. Levando em consideração que cada uma destas possibilidades temos ab ou ba, assim duas maneiras para variar, temos pelo princípio da multiplicação, $5! \cdot 2 = 240$ modos de sentarmos estas sete pessoas numa mesa redonda. ■

5.3 Os números de Stirling segunda ordem

Em seguida, introduzimos os números de Stirling segunda ordem, quais permitem o cálculo do número de partições de um certo conjunto com n elementos, cf 4.2, e portanto também o número das possíveis relações de equivalências de um conjunto de n elementos.

Questão 5.3.1. *Seja a um conjunto de n elementos e seja $k \in \mathbb{N}$. Quantas possibilidades existem de partir este conjunto em k blocos disjuntos, ou seja, quantas k-partições existem?*

Definição 5.3.2. *Sejam $n, k \in \mathbb{N}$. Definimos por recursão:*

$$S_{n,k} := 0 \quad \text{se } n < k, \quad S_{0,0} := 1, \quad \text{e } S_{0,k} = S_{n,0} := 0.$$

$$S_{n,k} := S_{n-1,k-1} + k \cdot S_{n-1,k} \tag{5.1}$$

Dizemos que $S_{n,k}$ denotam os **números de Stirling de segunda ordem**.

Vamos mostrar que $S_{n,k}$ dá de fato o número das k-partições de um conjunto de n elementos.

Proposição 5.3.3. *Sejam $n, k > 0$ e a um conjunto de n elementos. Então, $S_{n,k}$ definido em 5.1 é o número das k-partições de a.*

Demonstração: Seja a conjunto de n elementos. Vamos classificar as k-partições a partir de um elemento fixo $x \in a$ (observe que $a \neq \emptyset$, pois $n > 0$). Temos agora dois casos:

Se $\{x\}$ for um bloco da partição para a, então, os blocos restantes são formados a partir de $(k-1)$-partição do conjunto $a \setminus \{x\}$. Assim, temos $S_{n-1,k-1}$ possibilidades.

Se $\{x\}$ não for um bloco da partição para a, então, $a \setminus \{x\}$ é partido em k blocos. Isto pode ser feito de $S_{n-1,k}$ vezes. Agora, observe que o elemento restante x, precisa ser colocado a um dos blocos para obter uma k-partição de a. Isto pode ser feito de k maneiras (!). Neste caso obtemos então $k \cdot S_{n-1,k}$ possibilidades.

Como os dois casos são disjuntos, temos pelo princípio da adição, que o número das k-partições do conjunto a de n elementos é dado por $S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$, o que era para mostrar. ■

Os números de Stirling são dados por recursão, assim possibilitando o cálculo deles. Na próxima tabela, escrevemos os números até $n = 5$.

n \ k	0	1	2	3	4	5
0	1	0	0	0	0	0
1	0	1	0	0	0	0
2	0	1	1	0	0	0
3	0	1	3	1	0	0
4	0	1	7	6	1	0
5	0	1	15	25	10	1

Exemplo 5.3.4. *Em exercício perguntamos quantas aplicações sobrejetoras de a em b existem, se a e b forem conjuntos finitos com n e m elementos, respectivamente. Seja então $f : a \to b$ uma aplicação. Primeiramente, observemos que cada aplicação f é dada de maneira única pela família $\{f^{-1}(\{y\})| \quad y \in b\}$ das imagens inversas. Isto é fácil para ver, pois observe que $f^{-1}(\{y\}) = \{x \in a| \quad f(x) = y\}$. Agora seja f uma aplicação sobrejetora, então, observe que $f^{-1}(\{y\}) \neq \emptyset$, e assim a família das imagens inversas é de fato uma partição para o conjunto a (verifique!). Agora observe que cada m-partição de a fornece uma função sobrejetora. Elabore os detalhes para calcular quantas aplicações sobrejetoras existem.*

5.4 Números binomiais, o triângulo de Pascal e o teorema binomial

Vimos na definição os coeficientes binomiais $\binom{n}{k}$. Vejamos em seguida a relação de Stifel, qual justifica o seguinte triângulo de Pascal:

$$\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\
\vdots & & & & \cdots & & & & \vdots
\end{array}$$

Proposição 5.4.1 (Relação de Stifel)**.** *Sejam n, k naturais tais que $0 \leq k \leq n$. Então, $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.*

Demonstração: Vamos elaborar uma demonstração combinatória da afirmação. Consideremos um conjunto com n objetos brancos e um objeto azul. Podemos selecionar $k+1$ objetos deste conjunto de $n+1$ elementos, de $\binom{n+1}{k+1}$ maneiras diferentes.

Por outro lado, podemos raciocinar de modo seguinte, para escolher estes subconjuntos: Estes subconjuntos são de maneira tal que o objeto azul foi escolhido, ou não.

Em caso da escolha do objeto azul, temos $1 \cdot \binom{n}{k}$ possibilidades, pois o restante dos objetos devem ser brancos.

Em caso da não-escolha do objeto azul, temos $\binom{n}{k+1}$ possibilidades, pois neste caso todos os elementos devem ser brancos.

Como os dois casos são disjuntos, temos pelo princípio da adição, $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$, demonstrando a proposição. ∎

A consequência imediata desta proposição é o seguinte

Corolário 5.4.2.

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
\vdots & & & & \cdots & & & & \vdots
\end{array}$$

∎

Proposição 5.4.3. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Demonstração: Desenvolvemos uma demostração combinatória da afirmação. Sejam a um conjunto com n elementos e $0 \leq k \leq n$. Sabemos que o número de subconjuntos com k elementos de a é dado por $\binom{n}{k}$. Assim, sabemos que o número total de subconjuntos de a é dado por $\sum_{k=0}^{n} \binom{n}{k}$.

Por outro lado, podemos formar um subconjunto de a de seguinte modo: Seja $a := \{a_1, \ldots, a_n\}$. Para tomar um subconjunto de a, temos agora duas possibilidades para o elemento a_1, escolher ou não-escolher, para o elemento a_2 temos as mesmas possibilidades, e assim adiante, ou seja, para cada $a_i \in a$ temos duas possibilidades. Pelo princípio da multiplicação, temos então $\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{n} = 2^n$ possibilidades de formar um subconjunto de a.

Logo, $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. ■

Corolário 5.4.4. *Um conjunto de n elementos tem 2^n subconjuntos, i.e., $|\mathcal{P}(a)| = 2^n$.* ■

Exemplo 5.4.5. *Vamos calcular $S := \binom{n}{1} + 2\binom{n}{2} + \ldots + n\binom{n}{n}$, para $n \geq 1$.*
Observe que $S = \sum_{k=0}^{n} k\binom{n}{k} = \sum_{k=1}^{n} k\binom{n}{k} = \sum_{k=1}^{n} \frac{n!}{(k-1)!(n-k)!} = \sum_{k=1}^{n} n\frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} = n\sum_{k=1}^{n} \binom{n-1}{k-1} = n\sum_{k=0}^{n-1} \binom{n-1}{k} = n2^{n-1}$.

Uma aplicação da relação de Stifel é dada na seguinte

Proposição 5.4.6. *Seja $n \geq 1$. Então, $\binom{k}{k} + \binom{k+1}{k} + \cdots + \binom{k+n}{k} = \binom{k+n+1}{k+1}$.*

Demonstração: Por várias aplicações da relação de Stifel, obtemos que

$\binom{k+1}{k+1} = \binom{k}{k} + \binom{k}{k+1}$,

$\binom{k+2}{k+1} = \binom{k+1}{k} + \binom{k+1}{k+1}$,

$\vdots$

$\binom{k+n}{k+1} = \binom{k+n-1}{k} + \binom{k}{k+1}$.

Somando estas igualdades e simplificando, obtemos a seguinte equação:

$\binom{k+n+1}{k+1} = \binom{k}{k+1} + \binom{k}{k} + \binom{k+1}{k} + \ldots + \binom{k+n-1}{k} + \binom{k+n}{k}$

Levando em consideração que $\binom{k}{k+1} = 0$, acabamos a prova. ■

Observação 5.4.7. *Como temos que $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{k!}$ faz sentido definir o coeficiente binomial para $n \in \mathbb{R}$ e $k \in \mathbb{N}$. Obtemos por exemplo,*

$$\binom{\frac{1}{2}}{n} = \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)}{3!} = \frac{1}{16},$$
$$\binom{-5}{4} = \frac{(-5)(-6)(-7)(-8)}{4!} = 70$$

Demosntramos usando argumento combinatória o teorema importante de Newton.

Teorema 5.4.8 (Binômio de Newton)**.** *Sejam $x, y \in \mathbb{R}$ e $n \in \mathbb{N}$. Então, temos que*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \ldots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

Demonstração: Exibimos aqui uma demonstração combinatória, mas o estudante pode (e deve) tentar exibir uma demonstração *por indução* deste teorema, usando ”no meio do caminho”também a relação de Stifel introduzido acima. (cf. exercícios).
Com as hipóteses, observe que $(x+y)^n = \underbrace{(x+y) \cdot \ldots \cdot (x+y)}_{n}$.

Vamos calcular este termo da direita, e obtemos que cada termo deste produto é obtido escolhendo-se em cada parentese a variável x ou y, e depois da escolha os multiplicando. Seja agora $k \in \{0, 1, \dots, n\}$. Se escolhermos em k parenteses a variável x, então obrigatoriamente, escolhemos em $(n-k)$ parenteses a variável y. Assim obtemos o termo $x^k y^{n-k}$. Agora, observe que esta escolha podemos fazer de $\binom{n}{k}$ vezes, pois na verdade estamos escolhendo de um conjunto com n objetos k objetos digamos do gênero x. Assim, temos que $(x+y)^n$ é a soma dos termos $\binom{n}{k} x^k y^{n-k}$, onde $k \in \{0, 1, \dots, n\}$. ■

Corolário 5.4.9. $2^n = \sum_{k=0}^{n} \binom{n}{k}$. ■

Exemplo 5.4.10. *(a) Queremos calcular os coeficientes do desenvolvimento de* $(x+y)^5$. *Sabemos por 5.4.8 que* $(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$.

(b) Queremos determinar o coeficiente do termo x^2 *no desenvolvimento de* $(x^3 - \frac{1}{x^2})^9$. *Sabemos que*

$(x^3 - \frac{1}{x^2})^9 = \sum_{k=0}^{9} \binom{9}{k} (x^3)^{9-k} (-\frac{1}{x^2})^k$.

Os termos genéricos são da froma $\binom{9}{k}(x^3)^{9-k}(-\frac{1}{x^2})^k = \binom{9}{k}\frac{(-1)^k}{x^{2k}} x^{27-3k} = (-1)^k \binom{9}{k} x^{27-5k}$. *Agora, observe que no termo* x^2 *temos que ter* $27 - 5k = 2$, *ou seja,* $k = 5$. *Assim o coeficiente da expans ao é* $(-1)^5 \binom{9}{5} = -126$.

(c) Pelo teorma 5.4.8, temos que $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$.

Em exercícios, podemos mostrar o teorema 5.4.8 aplicando o método da indução, além disso, temos vários exercícios a serem resolvidos via combinatória.

Referências Bibliográficas

[1] E. Alencar Filho, **Lógica matemática**, Editora Nobel, São Paulo, 1975.

[2] A.B. Alfonso, H.A. Feitosa e H.L. Nascimento, **Teoria dos conjuntos: sobre a fundamentação da matemática e a construção dos conjuntos númericos**, Editora Ciência Moderna, Rio de Janeiro, 2011.

[3] S. F. Barker, **Filosofia da matemática**, Zahar Editores, Rio de Janeiro, 1969.

[4] P. Blauth Menezes, **Matemática discreta para computação e informática**, Editora Bookman, 3. edição, Porto Alegre, 2010.

[5] N.C.A. da Costa, **Sistemas formais inconsistentes**, Editora da UFPR, Curitiba, 1993.

[6] D. van Dalen, **Logic and Structure**, Springer, Berlin, 1990.

[7] H.B. Enderton, **Elements of Set Theory**, Academic Press, New York, 1977.

[8] J. L. Gersting, **Fundamentos matemáticos para a ciência da computação**, Editora LTC, Rio de Janeiro, 2001.

[9] P.R. Halmos, **Teoria ingênua dos conjuntos**, Editora Ciência Moderna, Rio de Janeiro, 2001.

[10] A. Heyting, **Intuitionism. An introduction**, North Holland Publishing Co., Amsterdam, 1956.

[11] L. Lovász, J. Pelikán e K. Vesztergombi, **Discrete mathematics**, Springer, New York, 2003.

[12] F. Miraglia: **Teoria dos conjuntos, um mínimo**, EDUSP, São Paulo, 1991.

[13] A.C.O. Morgado, J.B.P. de Carvalho, P.C.P. Carvalho e P. Fernandez, **Análise combinatória e probabilidade**, Coleção de Professor de Matemática, SBM, Rio de Janeiro, 2006.

[14] C.A. Mortari, **Introdução à lógica**, Editora UNESP, São Paulo, 2001.

[15] E.R. Scheinerman, **Matemática discreta - uma introdução**, Editora Thomson, São Paulo, 2003.